NISTIR 7983

Report: Authentication Diary Study

Michelle Steves
Dana Chisnell
Angela Sasse
Kat Krol
Mary Theofanos
Hannah Wald

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 7983

Report: Authentication Diary Study

Michelle Steves
Information Access Division
Information Technology Laboratory

Dana Chisnell
Usability Works
Boston, MA

Angela Sasse
Kat Krol
University College London
London, UK

Mary Theofanos
Office of Data and Informatics
Material Measurement Laboratory

Hannah Wald
Booze Allen Hamilton
McLean, VA

February 2014

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

1 INTRODUCTION 3

2 BACKGROUND 5

2.1 AUTHENTICATION 5
2.2 USABILITY 5
2.3 ENABLING TASKS AND PRIMARY TASKS 6
2.4 FRICTION 6
2.5 THE COMPLIANCE BUDGET 7
2.6 PASSWORD FATIGUE 7
2.7 IT AND AUTHENTICATION AT NIST 8

3 METHOD 9

3.1 PARTICIPANTS 9
3.2 MATERIALS 10
3.3 SETTING 10
3.4 PROCEDURE 11
3.4.1 Briefing 11
3.4.2 Data Collection Period 12
3.4.3 Follow-Up Interviews 12

4 RESULTS 13

4.1 WHEN DID PARTICIPANTS AUTHENTICATE? 14
4.2 WHAT TYPES OF APPLICATIONS WERE USED? 15
4.2.1 Personal and work-related authentication events 15
4.2.2 Types of applications requiring authentication 16
4.2.3 Application subtypes 18
4.3 WHERE WERE THESE EVENTS TAKING PLACE? 20
4.4 INFORMATION SURROUNDING HOW THESE EVENTS OCCURRED 21
4.4.1 Devices used to authenticate 21
4.4.2 What was required for authentication? 24
4.4.3 Authentication information memorization and memory aids 29
4.4.4 Authentication problems 35
4.4.5 Actions taken after encountering authentication problems 37
4.4.6 Participant frustration ratings 37

5 VISUALIZING THE EFFECTS OF AUTHENTICATION: THE USER EXPERIENCE 41

5.1 THE "JOURNEY MAP" AS A TEMPLATE FOR USER EXPERIENCE VISUALIZATION 41
5.2 MEASURES USED IN THE USER EXPERIENCE CHART 42
5.2.1 Frustration Rating 42
5.2.2 Interviewer Rating 43
5.2.3 Calculated Disruption 43
5.2.4 Composite Rating 46
5.3 USER EXPERIENCE CHARTS 48

6 DISCUSSION 53

6.1 HOW PARTICIPANTS PERCIEVED THEIR AUTHENTICATION WORKLOAD 53
6.2 SPECIFIC "FRICTION POINTS" DESCRIBED BY OUR PARTICIPANTS 55
6.2.1 Re-authenticating due to timed lockouts 55

6.2.2 Remembering a large number of passwords and when/where each one is supposed to be used 56
6.2.3 Managing a large number of authentication elements 57
6.2.4 Management workload for infrequently used passwords 57
6.2.5 Miscellaneous friction points 58
6.3 PARTICIPANTS' FEELINGS ABOUT THE NECESSITY AND EFFECTIVENESS OF AUTHENTICATION 59
6.3.1 While all participants saw a need for organizational security at NIST, some questioned the effectiveness of current methods 59
6.3.2 Participants think organizational security measures are too demanding 60
6.3.3 Overall, participants believe SSO is the best way to address both security and usability issues 61
6.4 COPING WITH AUTHENTICATION 62
6.4.1 Coping mechanisms used by participants 62
6.4.2 What participants' coping mechanisms imply about their view of authentication and security 73
6.5 TRADING OFF PRODUCTIVITY FOR SECURITY 73
6.6 INSIGHTS REGARDING AUTHENTICATION, FRICTION, AND DISRUPTION 74
6.6.1 Authentication problems create considerable friction 74
6.6.2 Users experience friction from authentication even when there are no problems 75
6.6.3 Friction and disruption from authentication have long-term effects 78

7 RECOMMENDATIONS 80

7.1 RETHINKING ASSUMPTIONS ABOUT AUTHENTICATION 80
7.1.1 Users struggle with authentication because they are only human 80
7.1.2 More authentication is not necessarily better 81
7.2 MAKING PASSWORD-BASED AUTHENTICATION MORE USABLE 81
7.2.1 Listen to and work with users 81
7.2.2 Implement SSO 82
7.2.3 Consolidate and standardize authentication as much as possible 82
7.2.4 Encourage and support the use of password managers or vaults 83
7.3 FUTURE DIRECTIONS 83
7.3.1 Take a broader perspective 84
7.3.2 Establish best practices for implementing usable authentication 84
7.3.3 Conduct further research on habits and effects related to authentication 85

8 CONCLUSION 87

9 REFERENCES 88

APPENDIX A: STUDY MATERIALS 91

APPENDIX B: USER EXPERIENCE CHARTS FOR STUDY PARTICIPANTS 94

APPENDIX C: CATALOG OF PARTICIPANT QUOTES ON AUTHENTICATION-RELATED FRICTION POINTS, COPING STRATEGIES, AND HABITS 118

APPENDIX D: MODELING METHOD EXAMPLES 158

LIST OF TABLES

TABLE 1: NUMBER OF PARTICIPANT-RECORDED LOGINS BY APPLICATION 18

TABLE 2: AUTHENTICATION EVENTS BY LOCATION AND TYPE 21

TABLE 3: AUTHENTICATION ELEMENTS USED FOR EACH APPLICATION TYPE....26

TABLE 4: MEMORY AID USE WHERE ONE OR MORE ELEMENTS WERE MEMORIZED....30

TABLE 5: MEMORY AIDS USED WHEN MEMORIZATION NOT REPORTED....31

TABLE 6: AUTHENTICATION MEMORY AIDS USED BY PARTICIPANTS....34

TABLE 7: AUTHENTICATION PROBLEMS REPORTED....36

TABLE 8: ACTIONS TAKEN AFTER AUTHENTICATION PROBLEMS....37

TABLE 9: AUTHENTICATION PROBLEMS AND FRUSTRATION RATINGS BY APPLICATION....38

TABLE 10: INDIVIDUAL PARTICIPANTS' PROBLEM EVENTS AND AVERAGE FRUSTRATION RATINGS....39

TABLE 11: INTERVIEWER RATING MAPPING FOR ASSIGNED SCORES....43

TABLE 12: AUTHENTICATION OUTCOME FACTOR VALUES FOR CALCULATED DISRUPTION....44

TABLE 13: AUTHENTICATION PROBLEMS AND CORRESPONDING CALCULATED DISRUPTION VALUE ADJUSTMENTS....45

TABLE 16: FRUSTRATION AND PROBLEMS ASSOCIATED WITH NUMBER OF AUTHENTICATION ELEMENTS USED....78

TABLE 17: EXAMPLE KEYSTROKE LEVEL MODELING SEQUENCE OF STEPS FOR MANUALLY LOGGING INTO AN APPLICATION, WITH TIME FOR EACH STEP....158

LIST OF FIGURES

FIGURE 1: DISTRIBUTION OF AUTHENTICATION EVENTS OVER THE STUDY PERIOD 15

FIGURE 2: WORK-RELATED AND PERSONAL AUTHENTICATION EVENTS BY PARTICIPANT 16

FIGURE 3: APPLICATION TYPES REQUIRING AUTHENTICATION 17

FIGURE 4: PERSONAL AND WORK-RELATED EVENTS FOR EACH CATEGORY 18

FIGURE 5: PARTICIPANTS' AUTHENTICATION EVENTS BY LOCATION 21

FIGURE 6: DEVICE USE DURING AUTHENTICATION 23

FIGURE 7: DEVICES USED BY EACH PARTICIPANT WHILE AUTHENTICATING 23

FIGURE 8: TYPES OF ELEMENTS REQUIRED FOR AUTHENTICATION 24

FIGURE 9: AUTHENTICATION ELEMENTS USED FOR AUTHENTICATION BY APPLICATION CATEGORY 29

FIGURE 10: NUMBER OF AUTHENTICATION MEMORY AIDS USED BY PARTICIPANTS 33

FIGURE 11: NUMBER OF AUTHENTICATION PROBLEMS REPORTED BY EACH PARTICIPANT 35

FIGURE 12: USER EXPERIENCE GRAPH – P23 48

FIGURE 13: HOW USERS EXPERIENCE DISRUPTION CAUSED BY AUTHENTICATION - P23 (COMPOSITE RATING) 50

FIGURE 14: USER EXPERIENCE WITH RESPECT TO DISRUPTION CAUSED BY AUTHENTICATION - ALL PARTICIPANTS (COMPOSITE RATING) 51

FIGURE 15: HEAT MAP OF AUTHENTICATION EVENTS AND USER DISRUPTION - ALL PARTICIPANTS 52

FIGURE 16: THE WALL OF DISRUPTION CREATED BY THE ENABLING TASK OF AUTHENTICATION 76

FIGURE 17: A SAMPLE COGTOOL SCRIPT FOR THE KEYSTROKE LEVEL MODELING SEQUENCE OF STEPS FOR MANUALLY LOGGING INTO AN APPLICATION 160

EXECUTIVE SUMMARY

The purpose of authentication is to ensure that only authorized individuals have access to a particular resource or physical area. To authenticate and prove their "right to access," a person must essentially prove that they are who they claim to be (i.e., an authorized individual) by presenting elements such as ID badges, fingerprints, personal identification numbers (PINs) or – very often – a username and password. For users of information technology, authentication is an inescapable fact of daily life – and it affects them in ways that are still poorly understood.

In order to better understand users' authentication-related perceptions and behaviors, we conducted a two-part study with 25 NIST employees. In the first part of the study, we instructed our participants to record all the authentication events they encountered over a 24-hour period (in the workplace and, if they so chose, at home) using forms we provided. The second part of the study consisted of individual follow-up interviews regarding participants' experiences with authentication.

Our study was designed to answer the following questions:

- Where does authentication fit into the daily activities people carry out?
- What characteristics of authentication may interfere with the primary activity that authentication is supposed to enable? What are the friction points?
- How do people add up the cumulative costs of authenticating multiple times each day, and how do they balance them against their own perceived security needs?
- How do people perceive the *costs* of performing security tasks (particularly authentication tasks) in comparison with the *benefits* of performing those tasks?

We found that our participants were confused about what "authentication" actually meant. For example, one participant erroneously recorded unlocking his car with his remote key fob as an authentication event. Conversely, some participants did not record showing their ID badge to a guard before entering the NIST campus (although most did).

Our participants recorded an average of 23 authentication events each during the study period. Since many participants did not record authentication events outside of work, we suspect that the actual number is higher. In interviews, participants indicated that they were frustrated by the sheer number of authentication tasks they had to perform every day – especially those they had to perform repeatedly, such as unlocking work computers that auto-locked after 15 minutes. In addition, while participants were understandably frustrated by problems that interfered with the successful completion of authentication tasks, they were also frustrated by tasks that were particularly complex and/or time-consuming, even when they did not encounter problems. Participants also found it particularly effortful to manage a variety of passwords for multiple resources, especially since those passwords were often governed by different policies.

Although our participants valued organizational security and understood the benefits of authentication with regard to security, these benefits were often overshadowed by the day-to-day costs of using and managing multiple authentication elements. For that reason, many of our participants adopted behaviors to help them cope with or avoid authentication, without (from their perspective) compromising organizational security. Coping strategies included synchronizing passwords across multiple IT resources; employing password creation schemas; keeping password notes in a secure place; and employing password vaults or managers. Avoidance usually meant giving up on performing certain "extra" activities (e.g., doing additional work from home) because the cost of authenticating to do so seemed greater than the potential benefit of the activity.

Our participants are not unique in being impacted by authentication. "Password fatigue" is, in fact, a very common problem [1][13]. Expecting users to simply adapt to an excessive authentication workload is not realistic. But from the user's perspective, what is excessive? In any case, if our participants' coping and avoidance strategies are any indication, the ways in which users adapt may not be desirable from an organizational perspective. Rather than trying to force users to adapt to authentication, organizations, security experts, developers, and engineers must find ways to make authentication adapt to users – in other words, to make it more usable.

Ultimately, making authentication more usable will take time. Further research is needed on how authentication affects users and the habits they develop to cope with those effects. This kind of research is essential for developing more usable, context-sensitive authentication solutions that will keep interference with users' primary tasks to an absolute minimum. Finally, there is a need for best practices aimed at designing and implementing more usable authentication.

Until then, organizations can take steps to reduce the burden of authentication on their employees, and other users of these systems, which will improve both security and productivity. This study indicates that users prefer single sign-on (SSO) authentication; another option is standardizing password policies throughout the organization, which will make authentication elements easier for users to manage. Finally, organizations can encourage and support authentication coping mechanisms such as the use of password manager or vault applications on computers and mobile electronic devices.

1 INTRODUCTION

Users must interact with a variety of applications and systems over the course of a day, in both their professional and personal lives. Each application and system has its own set of security policies and measures. Even different systems within the same organization – say, a single company or governmental agency – tend to have separate (and sometimes conflicting) security policies that are effectively "unaware" of each other. Each policy is narrowly focused on the system or application to which it directly applies, rather than the broader technological and policy environment in which the system exists.

Fragmented security policies are one reason why workers have to manage multiple passwords – between 5 and 15, according to some researchers in the usability field [1][5][9][10]. In addition, those passwords may be governed by different and even mutually exclusive password policies. One requires a password 8 characters long, while another requires a password at least 12 characters long; one mandates that the password include special characters, while another forbids them; and one expires every six weeks while another expires every ninety days. In addition to the challenges of password management, users must handle the cumulative impact imposed by the need to authenticate multiple times per day [5].

In theory, authentication is supposed to enable users to perform their primary tasks (e.g., research, financial management) in a secure way. But from a user's perspective, authentication often *interferes* with the performance of primary tasks. Beautement *et al.* refer to this kind of interference as "friction," a term we use in this report [5].[1]

Users have developed various coping strategies for minimizing or avoiding the friction and burden associated with managing and using their portfolios of user IDs and passwords or personal identification numbers (PINs). Many try to use the same password (or different versions of the same password) across different systems [10]. Others use memory aids or technological assistants such as password management software for computers and mobile electronic devices.

The research team was interested in these coping strategies and the "friction points" that prompt people to use them. More broadly, we wanted to address a pressing research need by gathering data for user-centered models of how people interact with security as part of their daily life, as empirical research in that area is currently lacking.

Specifically, this study was designed to answer the following research questions:

- Where does authentication fit into the daily activities people carry out?

[1] **Sec. 2.3** and **Sec. 2.4** contain more detailed explanations of enabling tasks, primary tasks, and friction.

- What characteristics of authentication cause friction with the primary activity that authentication is supposed to enable? What are the friction points?

- How do people perceive the cumulative costs of performing authentication tasks for the systems and applications they use, and how do they balance them against their own perceived security needs?

- How do people perceive the *costs* of performing security tasks (particularly authentication tasks) in comparison with the *benefits* of performing those tasks?

The research team considered a few different factors in this study. A first objective was to develop an estimate of how many times in a typical day federal government knowledge workers[2] authenticate – in other words, prove who they are to persons or systems. To do this, participants were asked to record the "authentication events" they encountered during a typical workday in a diary form provided by the team (shown in **Appendix A**). It was anticipated that by examining users' security compliance from this angle, rather than focusing on the number of user IDs and passwords individuals maintain, some insights about usable security that have not been revealed by prior research could be obtained.

Second, the study examined instances in which participants reported situations that delayed or prevented successful completion of the authentication process, in order to identify circumstances attributed to delays and problems, e.g., friction. Finally, we investigated the factors that contributed to frustration, friction, and the use of coping strategies associated with daily use of authentication. Following the recording of authentication events, we conducted an interview with each the participant to examine these issues.

This report presents when, where, and how participants authenticated during the study period, as well the issues they encountered. Based on the findings, we quantified and developed a preliminary visual model of task disruption, success (or failure), and frustration – factors contributing to impact on the user. These factors include the mental and physical workload associated with recalling authentication elements such as passwords and PINs and the disruption that failure to recall those elements causes to the user's activity.

Additionally, we identify and discuss the friction points of authentication that participants reported. We also relate and discuss participants' observations about organizational security from their perspective as it relates to authentication, as well their coping mechanisms to manage the impact of authentication requirements. Insights and recommendations related to usable security were also derived from the findings.

---

[2] Knowledge workers include those who work in information technology fields.

2 BACKGROUND

This section presents key terms used in this study:

- Authentication (including authentication factors)
- Usability
- Enabling tasks and primary tasks
- Friction
- Compliance budget
- Password fatigue

The definitions of these terms are given below, as well as, a description of the general IT and authentication environment within NIST and how that environment affects the way authentication mechanisms are implemented and used there – important considerations for this study, since all of the participants were NIST employees.

2.1 AUTHENTICATION

The purpose of authentication is to ensure that only authorized individuals have access to a particular resource: that resource can be a system, application, database, or even a physical area. In essence, authentication requires that a person prove that they are who they claim to be, i.e., an authorized individual, using a set of authentication elements that employ some combination of the following three factors:

- Something you have – a physical token such as a smart card or ID
- Something you are – biometrics such as fingerprints or a facial image
- Something you know – a password, code, or PIN

While there are a variety of authentication mechanisms currently in use, the one that will perhaps be most familiar to people is the combination of a user ID and password (something you know). Displaying a picture ID to a guard or holding a passcard to a reader in order to unlock a door are also common forms of authentication (something you have). One form that is becoming more and more common is a multi-factor authentication (MFA) mechanism involving a smartcard and PIN (something you have, something you know).

2.2 USABILITY

Mary Ellen Zurko and Richard T. Simon coined the term “user-centered security” in a research paper in 1996. In their paper, they described the usability lessons they had learned from their work on a user-centered rules-based authorization engine. One of their key observations was that because “security mechanisms need to be appropriately used to maintain their effectiveness…. Mechanisms and models that are confusing to the user

will be misused." Not misused maliciously, in the classic sense, but unintentionally. Zurko and Simon strongly recommended that secure systems should be designed and tested for usability in order to reduce the potential for confusion and, by extension, inadvertent misuse [29].

A few years later, in 1999, Alma Whitten and Doug Tygar published the results of a usability study on Pretty Good Privacy (PGP) 5.0, a program that provides cryptographic privacy and authentication for e-mail and other online communication. In their paper, they presented the following criteria for usability:

> *"Security software is usable if the people who are expected to use it:*
> *(1) Are reliably made aware of the security tasks they need to perform.*
> *(2) Are able to figure out how to successfully perform those tasks.*
> *(3) Don't make dangerous errors.*
> *(4) Are sufficiently comfortable with the interface to continue using it." [27].*

2.3 ENABLING TASKS AND PRIMARY TASKS

Authentication is something that users do on the way to some other activity – for example, logging into an e-mail application in order to send a message to a co-worker. Sending the e-mail is the *primary* task, while logging into the application in order to do so is the *secondary* task that enables it. Or, as usability researchers Dirk Weirich and Martina Angela Sasse put it:

> *"In most cases, authentication to a system is an enabling task, which means it creates an overhead for the user, who is using that system as a tool to achieve a primary, real-world task." [26]*

In some cases the enabling task of authentication can be transparent: it fits into the flow of the user's primary task or happens automatically, so the user does not notice it. But in the overwhelming majority of cases, authentication is explicit – a specific set of actions that the user must take before proceeding. It is something the user *must* do before engaging in something he or she *wants* to do.

2.4 FRICTION

In a report on a study examining the factors that influence users' compliance (or non-compliance) with organizational security requirements, Beautement *et al*. explained that:

> *"Employees focus on completing their primary (production) tasks, and the behaviour required by the security (enabling) tasks often presents an obstacle on the shortest path to the primary goal. This misalignment introduces friction between security and business processes into the organizational system, and it is this friction that is at the heart of individual compliance issues." [5]*

In other words, friction occurs when security tasks interrupt the user on his or her way to completing a primary task. Because of this friction, users must spend additional time and effort to accomplish their primary goals.

2.5 THE COMPLIANCE BUDGET

Because of the friction inherent in security tasks, as described in **Sec. 2.4**, users often perceive these tasks as an obstacle to engaging in and completing their primary tasks. More than that, they see little if any return on the investment of time and effort that they put into security tasks. As Beautement *et al*. explain, users have a limited tolerance for the disruption related to security tasks:

> *"There is a limit to the amount of effort individuals are prepared to expend on security measures that do not obviously contribute to their key production tasks, and this extra non-productive effort required accumulates until a limit is reached. We have named this limit the Compliance Budget… The limit of the Compliance Budget is referred to as the compliance threshold; this being the point at which the individual no longer has the will to comply with official requirements." [5]*

For users, cost/benefit calculations related to the compliance budget are largely non-quantified, just like most of the cost/benefit calculations humans perform as they make decisions on a daily basis – for example, determining the importance and urgency of individual tasks when prioritizing the tasks that might be accomplished in a given timeframe. Users cannot quantify their compliance budget. But they are aware that security requirements and security tasks cause accumulated fatigue over time.

2.6 PASSWORD FATIGUE

Password fatigue, also referred to as *authentication fatigue*, is conceptually related to the compliance budget and compliance threshold: it is a nearly perpetual state of stress and exhaustion experienced by technology users who are overwhelmed by authentication-related demands on their time, energy, and memory [13]. Martina Angela Sasse and Angela Adams point out that this situation is exacerbated by organizational IT departments that try to address what they see as the problem of "inherently insecure" users by escalating the number and stringency of security mechanisms and policies those users must deal with [1].

"Password fatigue" is a common term in the security and IT industries, often cited as the reason why many users – even if they are relatively security-conscious – engage in behaviors that compromise the security of the systems they use, e.g., creating passwords that are easy to guess or to compromise with password-cracking software. Another possible effect of password fatigue is changing one's work habits to reduce or avoid authentication in a way that does not compromise security, but *does* have adverse effects on one's productivity.

2.7 IT AND AUTHENTICATION AT NIST

At NIST, many and varied applications and software systems[3] are required to perform the business of the organization. These applications and systems may be administered by agencies and organizations outside of NIST, e.g., other government agencies or standards bodies; and as a consequence NIST does not have control over their authentication configuration. Other systems are administered by the NIST IT system support staff, while still other (often more specialized) systems and applications may be managed by staff associated with the individual projects that make use of those applications. Users at NIST interact with multiple applications each day to do their work, each of which requires authentication. The authentication methods associated with these applications include: user ID and password, smartcard and PIN, remote token combined with smartcard and PIN, and picture ID.

As in many other organizations, the most common authentication mechanism used for logical access (i.e., access to a system or application) employs a user ID and password. Logins for a number of mission-critical applications and systems within the NIST domain are consolidated using a single sign-on (SSO) solution – for example, NIST's domain services automatically log users into e-mail and calendar clients as well as other applications. However, Windows and OSX user profile passwords are not part of the SSO solution, nor are the passwords used for hard disk encryption on laptops. Fortunately these are all governed by the same password policy. Additionally, authentication elements for a number of other applications used at NIST – such as applications managed by the Department of Commerce – are not managed through SSO, and their password policies vary.

Some applications and systems also support smartcard-based authentication. All NIST employees have a Personal Identity Verification (PIV) smartcard with an associated 6-8 digit PIN. At the time of this writing, a relatively small number of employees use this method on a regular basis, in part because not all employees are "PIV-enabled," i.e., they do not have the requisite card reader and middleware or operating system. Even employees who use smartcard authentication almost exclusively must still manage their NIST domain password, which expires every ninety days.

Logging into the NIST virtual private network (VPN) from off campus requires not only a user ID and password (or PIV card and PIN), but also a six-digit code from a NIST-issued RSA token, which changes every sixty seconds. To authenticate, users must enter their user ID, PIN and the RSA code, then their user ID and password. It takes a few seconds for the system to process each set of authentication elements once they are

[3] The reference to any commercial products in this document is not intended to imply recommendation or endorsement by National Institute of Standards and Technology, nor is it intended to imply that the products are necessarily the best available for the purpose.

submitted, and if the RSA code expires before the authentication process is completed, the user will have to authenticate again.

All NIST computers, whether they are desktops or laptops, are set to lock after fifteen minutes of inactivity, i.e., no input from the keyboard or mouse. Once the computer is locked, the user must enter his/her password – or insert a PIV card (if it had been removed) and enter the corresponding PIN – to unlock it.[4]

NIST requires authentication for *physical* access to the grounds and buildings as well as logical access to information systems. All NIST employees, contractors, and associates have a picture ID/keycard that they use as a credential for this purpose. This ID must be shown to the guards posted at NIST gates for campus access. Further, this card is also required for access, via an electronic reader, to the majority of NIST facilities.

3 METHOD

This study used a combined methods approach, drawing quantitative data from self-reports from participants about the number and types of authentication they encountered (called a *diary study*), and qualitative data from ethnographic interviews to probe participants' experiences and specific authentication incidents reported in their diaries. Ethnographic methods such as the in-depth follow-up interviews conducted, provided an excellent opportunity to understand the contexts in which participants encountered authentication, and in particular, situations in which they experienced problems, frustration, or authentication-related disruption. The interviews provided a counterpoint to the participant diaries.

3.1 PARTICIPANTS

NIST's Visualization and Usability Group (VUG) put out a call for volunteers throughout the organization via e-mail. Twenty-five NIST employees responded to that call. Of those, 22 attended briefings before the data collection started. We were able to use data from 23 participants to model the day-long snapshot of authentication that formed the critical component of our study. The remaining two participants were unable to provide authentication diary data within the requested time frame. We were able to conduct follow-up interviews with 22 of those 23 participants who provided diary information.

There were 9 women and 14 men. 11 of the participants ranged in age from 50-59; 3 were in their 40s, 5 were in their 30s, and the remaining 3 were in their 20s.

[4] Mac users were not required to use these measures until a few months prior to the study, when NIST started centrally managing security on Macs in the same manner it had been managing Windows machines.

All the participants in this study were knowledge workers. Thirteen of the participants were researchers with computer science explicitly in their title or background. Three participants were researchers with non-computer science backgrounds (e.g., physics, cognitive science). Two were information technology systems administrators. Three participants held technical supervisory positions. The remaining two participants were administrative support staff.

3.2 MATERIALS

The research team worked with NIST scientists to develop the following materials for use in this study:

- A script for briefing participants prior to the study. The script contained an explanation of the study and the definition of "authentication events" participants were supposed to record.

- A list of open-ended questions to ask in follow-up interviews conducted with participants (see **Appendix A**).

- The diary form that participants could use to capture authentication events during the course of a work day.

Since the form participants use to collect data is a key success factor in every diary study – and the research team did not want to create an additional burden for participants – every effort was made to create one that was compact, clear, and easy to complete. Several members of the NIST staff contributed to the design of the form, working from design principles and lessons learned by others at University College London's Human-Centred Security, Privacy, Identity, and Trust department who had previously conducted diary studies about usable security [10]. At the participant briefing, described more fully in **Sec. 3.4.1**, study participants received printed copies of the diary form. Each 21.59 cm by 27.94 cm (8.5 in x 11 in) page contained two entry forms. Each participant received a packet of 20 sheets, containing a total of 40 event entry form instances. Softcopy, editable versions of the form were also e-mailed to participants in Word and PDF formats. The form can be seen in **Appendix A**.

3.3 SETTING

Data collection centered on authentication events participants encountered during a normal workday at NIST. Most of the data was from authentication events on the NIST campus, but some participants were on travel or worked from home for at least part of the day. A few participants reported authentication events in their personal lives as well as in their workday; these are delineated in the presentation of the data.

3.4 PROCEDURE

3.4.1 Briefing

Participants were invited to group meetings to be briefed about the study and to receive specific instructions about how to record "authentication events". Because this diary study was about security, it was anticipated that some participants might not want to join a group briefing meeting. The option for individual briefings was available to participants. However, a majority of participants attended the group meetings. A few were briefed individually, as they were not located on the NIST Gaithersburg campus at the time of the briefing meetings rather than because of other concerns. Of the participants who were briefed individually, one was based on the NIST campus in Boulder, Colorado, while others were traveling or working from home at the time – remote briefings took place via teleconference.

In the briefing, the study was described to participants as a "day in the life of authentication" and participants were invited to be "co-researchers," helping the research team to understand the depth and breadth of the effects of authenticating. Participants were given the diary form created for the study (described in **Sec. 3.2**) and were asked to use it to record every authentication event, every time they had to prove their identity to a person or a system, during a 24-hour period.

Participants were asked to record the following information:

- The beginning and ending times of each authentication event, i.e., when it happened and how long it took
- The purpose of the authentication, e.g., first log-in of the day, re-trying authentication after a problem
- What device they were logging into
- Where they were during each authentication event (on NIST's campus or off)
- What type of application or system they were authenticating
- Whether they used any memory aids for an authentication and if so, what type
- Any problems encountered during the authentication event
- Actions taken in the event of an authentication problem
- Frustration level (on a 5-point scale, with 1 being "Not Frustrated" and 5 being "Very Frustrated"

In addition, participants were provided with examples of authentication events, e.g., VPN, NIST domain, and NIST e-mail logins. It was specified that they should focus on

authentications that were work-related; authentications outside of work were optional. Although the data was protected and anonymous, because the participants and some of the researchers worked for the same agency, we wanted to allow for as much privacy as possible.

Therefore participants were provided with blank envelopes with which to deliver their paper diaries to Mary Theofanos at NIST and instructed not to mark or label the envelopes. Alternatively, participants had the option to e-mail softcopy versions of their diaries to Dana Chisnell, a contractor employed by NIST. Finally, participants were advised that they would be contacted shortly after the diary recording portion of the study to a schedule a follow-up interview.

3.4.2 Data Collection Period

Since the briefings were held a few days before the "diary day" when participants were supposed to record their authentication events, participants were e-mailed the day before to remind them of their recording task. At that time, participants were also given instructions on how to obtain more diary forms and how to contact a researcher with any questions.

To minimize the disruption caused by the self-observation, participants were given a choice of how to document their authentication events, and were encouraged to use the tools they found most comfortable. Most participants recorded the events on the paper forms provided to them, but some participants constructed their own spreadsheets or used Portable Document Format (PDF) versions of the paper diaries. Although we offered participants the option of recording their diaries on video or audio, none of them opted for this alternative.

3.4.3 Follow-Up Interviews

Within one month after the "diary day," we met with each participant to interview them about their experiences with authentication. During this time, basic demographic information, including profession, gender, and age range, was collected from each participant.

The interview focused on retrospectively reviewing diary events to ensure the researchers understood the data collected, as well as the context for problem events. Because of the retrospective nature of the interview, participant diaries were used in combination with a list of open-ended questions (see **Sec. 3.2**), to set the framework for the exchange.

Initially, participants were asked what they thought the big insights were from their "diary day," what surprises they encountered, and what questions they had. The rest of the interview investigated:

- The number and frequency of authentications throughout the day, and how participants felt about these measures.

- How much control and autonomy participants felt they had in authentication and where they exercised it, e.g., whether they could do certain things to control how often they authenticated.

- Where participants encountered frustration, and what were the factors contributing to that frustration, i.e., what participants found frustrating and why.

- When participants authenticated during the day and why.

- How participants felt about the effectiveness of authentication, including perceived tradeoffs of security versus usability and convenience.

- How participants decided on their coping strategies, if used.

- How typical the timing of recorded authentication events was.

- What participants considered the major impediments related to authentication.

Participants' responses to these inquiries are related in **Sec. 4** and **Sec. 6**. **Appendix C** provides a catalog of participants' direct quotes.

4 RESULTS

Although we defined the term "authentication event" to participants during briefings and provided participants with examples of what we were seeking, the data participants provided on their diary forms was somewhat inconsistent across the sample. For example, one participant included unlocking his car with a remote key fob; key entries were not considered to be authentication events because a key is not usually unique to a person, nor does it serve as proof of one's identity. Events such as the key entry example that did not qualify as authentication events in this study and were excluded from the data that was analyzed. Conversely, many participants included checking with the guard as they came through the gate at the entrance to the NIST campus – which was considered to be authentication because the participant had to prove who they were with approved identification to gain entry – but seven participants did not record this type of event even though they logged on-campus events. This example illustrates that some underreporting existed; however, only the qualifying data that participants reported was included in the analysis.

Overall, participants reported a total of 528 authentication events during the diary data collection period – one 24-hour day (all reporting will reflect that period, unless otherwise noted). On average, participants authenticated 23 times during this period, with the lowest number of authentication events being 4 and the highest 40. The majority of authentication events delayed participants in the performance of their primary tasks, but usually did not prevent them from reaching their goals.

To inform a primary research objective, *Where does authentication fit into the daily activities people carry out?*, the diary data collected and reported by participants was summarized into the following groupings:

- *When* did participants authenticate?
    - Distribution of events over the study period
- *What* were the types of applications requiring authentication that were reported?
    - Personal and work-related authentication events
    - Types of applications requiring authentication
    - Application subtypes
- *Where* were these events taking place?
    - Authentication event locations
- Information surrounding *how* authentication events occurred:
    - Devices used to authenticate
    - Types of authentication factors and information required for authentication
    - Authentication memory aids
    - Authentication problems
    - Actions taken after encountering authentication problems
    - Participant frustration ratings

Several of the latter categories just given, i.e., "Authentication memory aids", "Authentication problems", and "Actions taken after encountering authentication problems", were diary reporting categories that were anticipated to give researchers insights into the research question, *What characteristics of authentication cause friction with the primary activity that authentication is supposed to enable?*

The remainder of **Sec. 4** relates aggregated diary data to inform these research questions.

4.1 WHEN DID PARTICIPANTS AUTHENTICATE?

The largest cluster of authentication events reported by participants occurred near the start of the workday – around 9:00 AM – as is evident in **Fig. 1**.

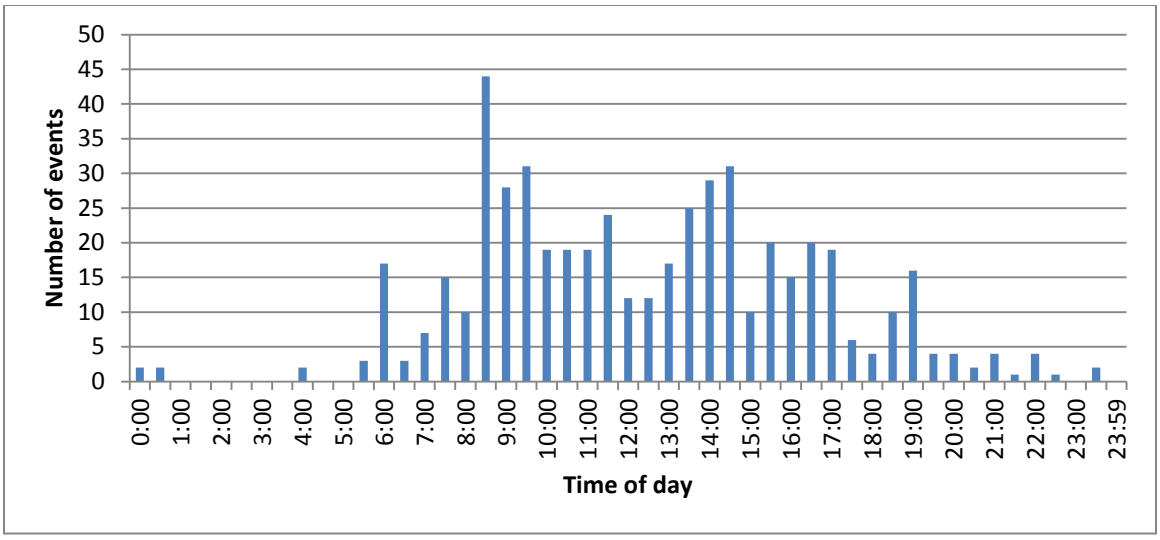


Figure 1: Distribution of authentication events over the study period

Other peak periods of authentication activity occurred later in the morning and in the early afternoon.

4.2 WHAT TYPES OF APPLICATIONS WERE USED?

In this paper we use the term "application" broadly: it can mean an actual computer application, a device, a system, a network, a website, a door that must be opened with a keycard, or even a checkpoint staffed by a human who ensures that only persons with legitimate identification are allowed onto the NIST campus. In this section, we present the types of applications participants reported encountering and authenticating to throughout the study period. Two different perspectives are given: the first differentiates between events enabling a primary task for *personal* use or one which is *work-related*. The second view presents the researcher-assigned categorization of each event by application type and subtype.

4.2.1 Personal and work-related authentication events

Although participants were invited to log events for a 24-hour period, logging events outside of work hours was optional. 18 of 23 participants logged authentication events when they were not working; however these participants typically logged fewer personal events than work-related events. It is therefore unsurprising that 81.21% of the authentication events captured in the study were work-related, while the remaining 18.79% were personal authentications. **Figure 2** shows a summary of each participant's events requiring authentication categorized as work-related and personal applications. Note that while participants were not asked to distinguish between personal or work-related events, the nature of each event was evident from the recorded data (combined with supplemental information from the interview as needed).

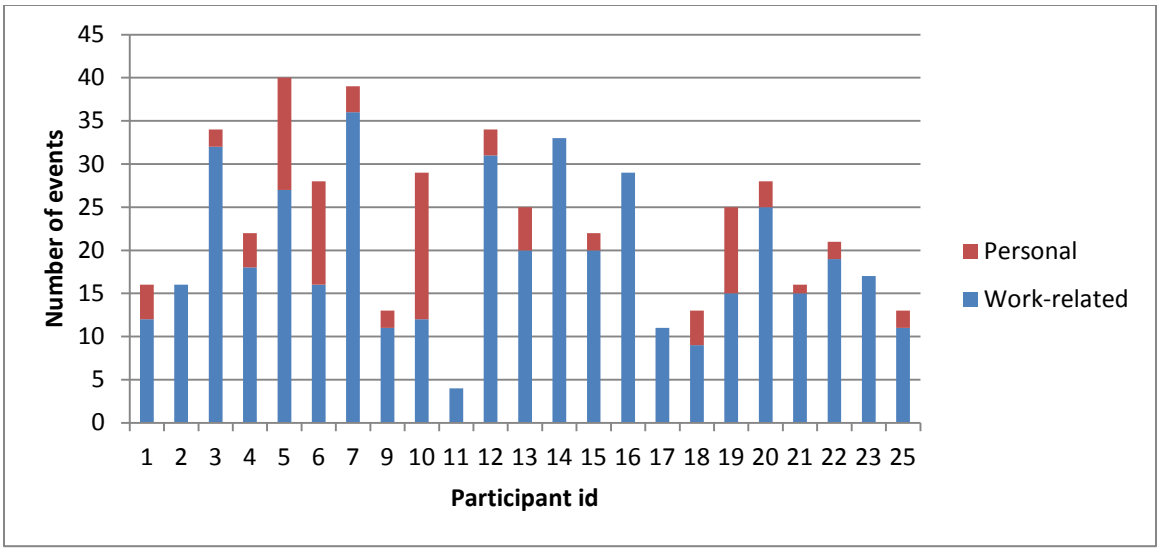


Figure 2: Work-related and personal authentication events by participant[5]

4.2.2 Types of applications requiring authentication

Figure 3 shows the categories of applications that users reported authenticating to and the percentage of each type's reported use during the data collection period.

[5] Participants "8" and "24" are absent from this figure as well as other numbers and tables that display participant labels, because their data were not included in the final study (see **Sec. 3.1**).

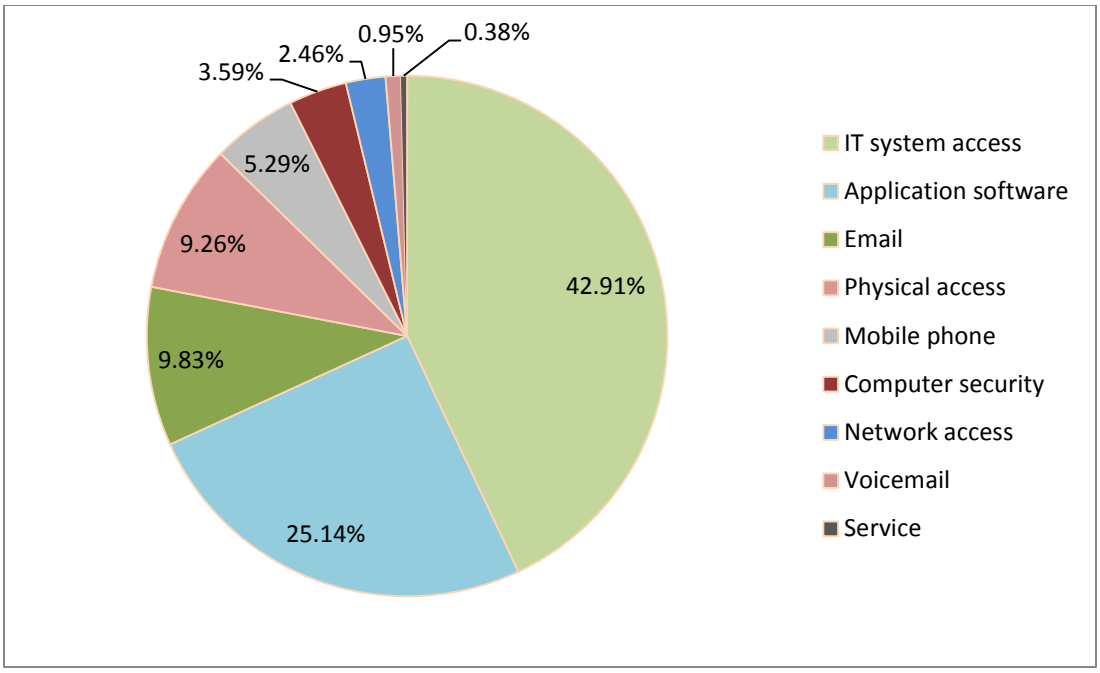


Figure 3: Application types requiring authentication

As the chart shows, the largest portion of the recorded authentications were for access to IT systems (42.91%), e.g., computer account access. The second-largest category, *Application software*, contained authentication events related to access for a plethora of packages and internet-based functionality and services (25.14%). Some examples include backup software, online banking, online shopping, e-conferencing, NIST time and attendance, applications supporting other NIST administrative functions, and Web applications. Authentication events related to e-mail access were contained in the next largest category (9.86%). Events related to physical access, such as admittance to the NIST campus[6] and buildings, were categorized as *Physical access* (9.26%). Events related to mobile phone device access was the next largest category, comprising 5.29% of all events. The *Computer security* category (3.59%) contained events that were considered specialized computer security access above and beyond those contained in the IT system category, such as computer encryption software, password vaults, and privileged account access. The *Network access* category, having 2.46% of the total events, contained events related to authentication for network access that were not abstracted from the user. The *Voicemail* category contained all events related to accessing

[6] As described at the beginning of this section, all participants who worked on the NIST Gaithersburg campus during the study period had to authenticate to a guard to gain access to the NIST campus. However, 7 of the 20 participants who recorded events as originating on the NIST campus did not record their authentication at the gate. If they had, the events in the Physical access category would represent a modestly larger percentage of the applications to which participants authenticated.

voicemail systems (0.95%). Finally, the *Service* category contained two events (0.38%), use of a library card and use of a debit card.

The chart in **Fig. 4** displays the relative number of work-related and personal events in each application category.

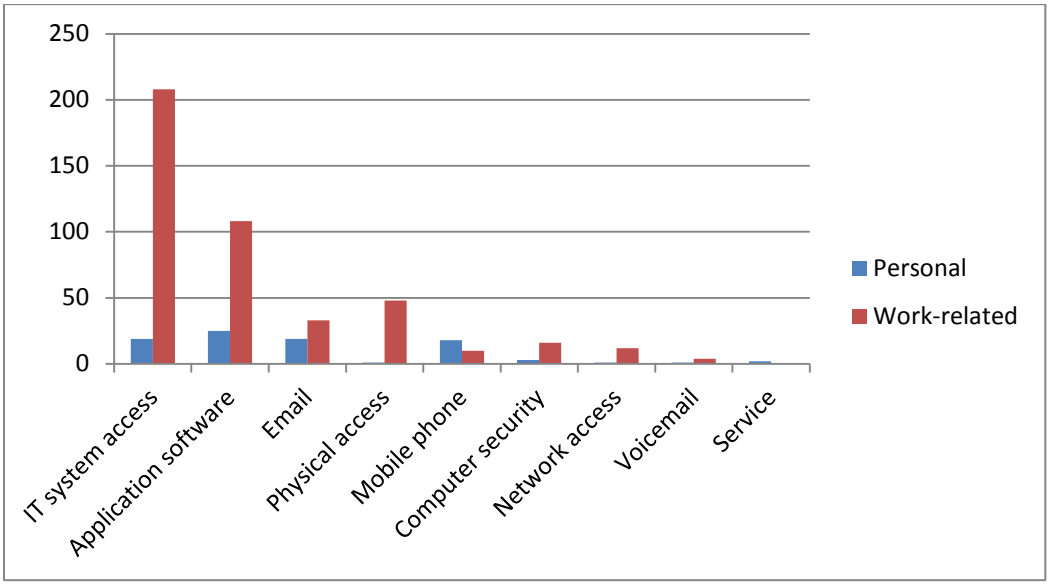


Figure 4: Personal and work-related events for each category

4.2.3 Application subtypes

There were often a variety of applications reported within each application category: these are referred to in this report as the *application subtypes*. For example, within the category *IT system access*, three specific types of system access were reported: NIST domain, local computer, and remote computer. The list of application types, subtypes, and number of participant-reported logins associated with each is provided in **Table 1**.

Table 1: Number of participant-recorded logins by application

Application type	Application Subtype	Work-related	Personal	Totals
IT system access		**208**	**19**	**227**
	Local computer	23	19	42
	NIST domain	144	0	144
	Remote computer	41	0	41
Application software		**108**	**25**	**133**

Application type	Application Subtype	Work-related	Personal	Totals
	Backup	4	0	4
	E-conferencing	15	2	17
	NIST application	32	0	32
	NIST time & attendance	21	0	21
	Not specified	0	1	1
	Online banking	0	5	5
	Online shopping	0	3	3
	IT support incident mgmt sys	3	0	3
	Web application	33	14	47
Email		**33**	**19**	**52**
	NIST e-mail	33	0	33
	Personal e-mail	0	19	19
Physical access		**48**	**1**	**49**
	Building/door entry	31	1	32
	Gated location	17	0	17
Mobile phone		**10**	**18**	**28**
	Cellular/phone account	10	18	28
Computer security		**16**	**3**	**19**
	Computer encryption	8	0	8
	OS privileged access	2	1	3
	Password manager	6	1	7
	PC security package	0	1	1
Network access		**12**	**1**	**13**
	NIST wireless network	5	0	5
	Virtual Private Network	7	0	7
	Wireless network	0	1	1

Application type	Application Subtype	Work-related	Personal	Totals
Voicemail		**4**	**1**	**5**
	Home voicemail	0	1	1
	NIST voicemail	4	0	4
Service		**0**	**2**	**2**
	Library card	0	1	1
	Purchase (debit)	0	1	1
Grand Total		**439**	**89**	**528**

As described in **Sec. 2.7**, logins for a number of applications and systems within portions of the NIST domain are consolidated using an SSO solution; for example, NIST's domain services automatically log users into the e-mail and calendar application when the client is started. This is true for other applications as well, when it is implemented. Because of this, we suspect that there were a large number of authentication events that users did not notice or report, as the actual authentication was abstracted from the user. Users would only notice these authentications if SSO either failed to work or was not available (e.g., when the user logged in remotely or from a segment of the domain where SSO was not implemented). Since users did not notice these automatic SSO-enabled authentications, they did not report them. It is likely that if SSO-enabled authentication had not been in place, participants in this study would have encountered and recorded more work-related authentication events in the *Application software*, *NIST e-mail*, and *Network access* categories.

In addition, since all NIST computers are set to lock after a certain period of inactivity and must be unlocked with a password (as described in **Sec. 2.7**) or a PIV card, it is likely that many of the work-related *IT system access* authentication events recorded by users represented unlocking their computers multiple times during the day.

4.3 WHERE WERE THESE EVENTS TAKING PLACE?

For each authentication event recorded, participants were asked to record whether they were on or off the NIST campus at the time of the event. **Figure 5** shows the number of events recorded by each participant, while distinguishing the location (i.e., whether they were on- or off-campus).

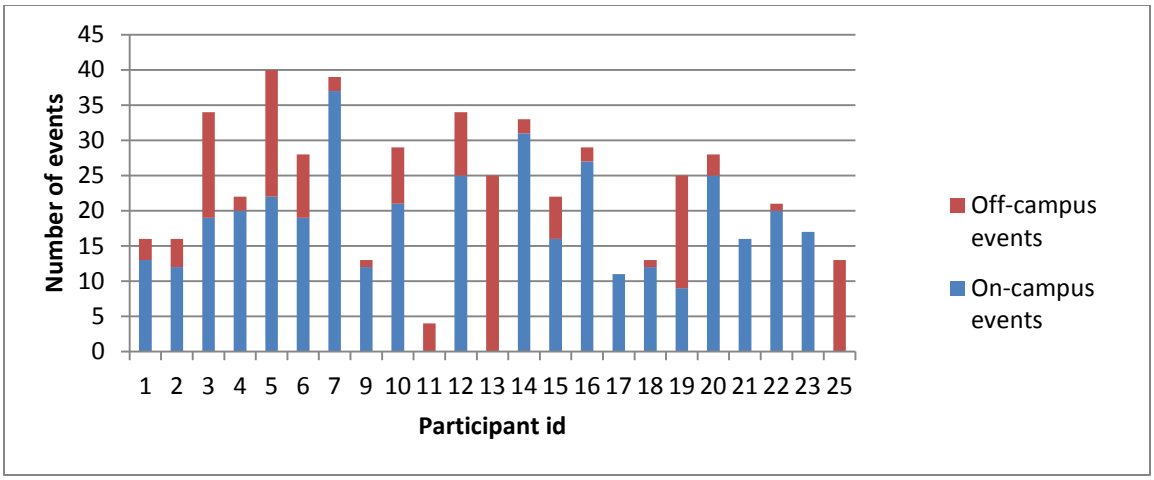


Figure 5: Participants' authentication events by location

Table 2 provides a delineation of all participants' authentication events by location (on-campus or off-campus) and type (work-related or personal). It should be noted that authentication events recorded on the NIST campus were not always work-related; likewise, not all events that were recorded off-campus were personal.

Table 2: Authentication events by location and type

Event Location	Event Type		All Types
	Personal	Work-related	
NIST	26	359	385
Off-campus	63	80	143
All Locations	89	439	528

Additionally, the data show that 72.92% of the recorded authentication events took place on-campus, while 27.08% took place off-campus. This is to be expected, given that most of our participants worked on-campus during the diary day. Two participants were telecommuting at the time of the study, and one was on work-related travel.

4.4 INFORMATION SURROUNDING HOW THESE EVENTS OCCURRED

4.4.1 Devices used to authenticate

Diary data show that participants used a number of different mechanisms, usually electronic devices, to gain access to various resources through authentication. These mechanisms included desktop computers, laptop computers, tablet computers, mobile phones, landline phones, biometric scanners (e.g., fingerprint readers), and various electronic card readers for PIV smartcards, NIST badges, debit cards, and so on. There

was also a human authentication mechanism – specifically, a guard at each gate to the NIST campus to whom participants had to display their ID badges for admittance.

As one might expect, the devices used in the vast majority of authentications were desktop and laptop computers (42.52% and 32.12% respectively). The next most commonly used authentication device types were mobile phones (10.04%) and NIST badge readers located at most building entrances (5.66%). Events using a human authenticator, i.e., authenticating to a guard at a NIST property gate, accounted for the next highest number of events, 3.10%. Note that while some building-entry badge reader devices could read NIST PIV cards at the time of this study, use of the non-PIV and PIV NIST identification cards[7] were not distinguished at gate and building entry. Biometric scanners built into computing systems or keyboards constituted 2.92% of the reported use. Tablet use accounted for 1.46% of the reported authentications.

The "Other" category contained three different electronic card reader types, i.e., credit/debit card reader, library card reader, and a membership card reader, as well as a hardware-based encrypted password vault device. This category constituted 0.91% of the reported device type use. Landline phone use accounted for another 0.91% of the total use.

PIV card readers may be attached to or integrated into a desktop or laptop computer, but for purposes of this study we asked participants to count readers as a device. PIV card readers accounted for 0.36% of the total number of reported device types used. For the two events in which participants reported using a PIV card reader, the associated device was a desktop computer, which was also counted as a device on which authentication occurred during those events. **Figure 6** shows a circle graph in which the relative sizes of the areas shown correspond to the percentages of reported device use for authentication during the study period.

[7] At the time of the study, NIST was transitioning to PIV identification cards (also referred to as badges) and many NIST employees carried both PIV and non-PIV NIST identification cards.

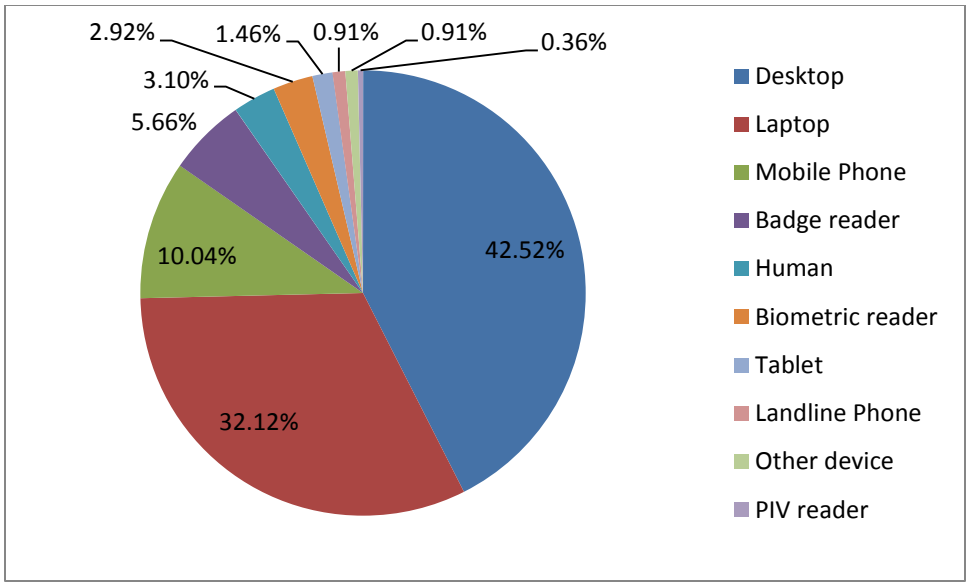


Figure 6: Device use during authentication

Figure 7 shows the relative number and device types used by each participant during authentication events.

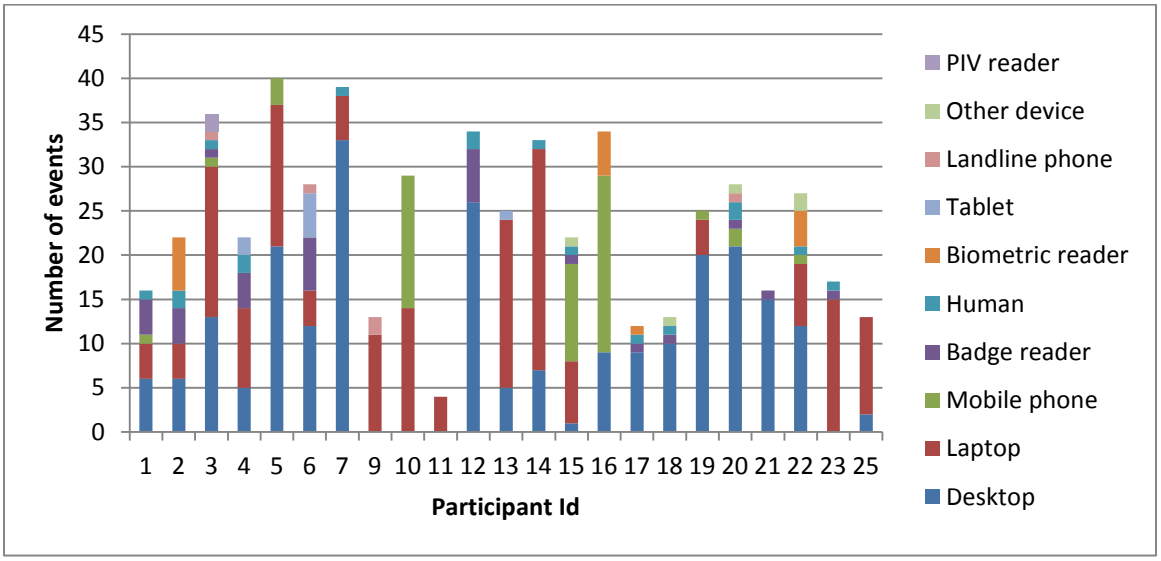


Figure 7: Devices used by each participant while authenticating

On average, participants in this study reported using 3.74 ± 1.57 SD different device types when authentication occurred during the study period. At the ends of the spectrum of device use, one participant reported authenticating via only one device type, a laptop, while another participant reported authenticating via seven different device types over the course of the day.

4.4.2 What was required for authentication?

Participants also reported the types of information and objects they were required to provide during authentication events. **Figure 8** shows the relative use of the different types of items used in the 528 application events recorded during the data collection period. The "Other" category contains information elements such as: personally identifying information (e.g., birthdate, Social Security number), challenge question responses, Google credentials, Completely Automated Public Turing Test To Tell Computers and Humans Apart (CAPTCHA), a user-selected verification image associated with an account, encoding contained on a hardware-based password vault, and encoding on electronically read cards (e.g., debit card, library card).

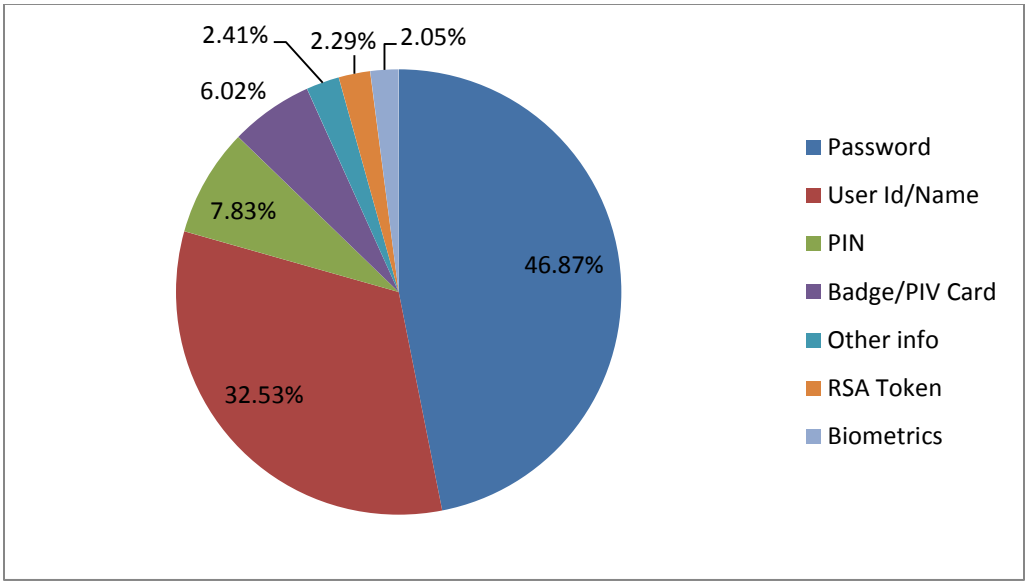


Figure 8: Types of elements required for authentication

As the chart shows, the most commonly used authentication elements were passwords (46.87%) and user IDs or user names (32.53%). This is unsurprising, given that the most common authentication mechanism used on information systems requires a user ID and password. Since the two items are almost always used together, one might expect the percentages of both elements to be equal; however, in many cases a user ID may be filled in automatically based on the previous login, so the only element a user must enter manually is a password. In such cases, it is understandable that a participant would not count the user ID as an authentication element.

The next most common were a PIN (7.83%) and a NIST badge/PIV card (6.02%). Although a PIV card and a PIN can be used together to authenticate in the same way that a user ID and password are, there were only two reported uses of a PIV card during the diary period. So even though the PIN and badge/PIV card had roughly similar reported use, in this study PINs were generally used in events that did not involve use of a PIV

card. The majority of reported badge/PIV card use was for physical access to the NIST site and buildings.

The “Other” category (2.41%) had a relatively small proportion of the elements participants reported using during the study period. The fact that VPN tokens were only used in 2.29% of authentication is to be expected: one would only need to use the token to connect remotely to the NIST network, and the fact that the vast majority of work-related authentication events took place on the NIST campus (illustrated in **Table 2**) indicates that most of the study participants did not connect remotely during the study period. Finally, biometrics accounted for 2.05% of the reported elements used for authentication.

Table 3 shows how many and which authentication elements (e.g., user IDs, VPN tokens, PIV cards) participants used to authenticate to the applications reported via diaries.

Table 3: Authentication elements used for each application type

Application Type	# Of events	Pass-Word	User ID or Name	PIN	Badge or PIV Card	Other Info	Token	Bio-metrics	Avg # of items needed
IT system access	**227**	**184**	**92**	**22**	**2**	**1**	**0**	**16**	**1.40**
Local computer	42	35	13	1	0	0	0	6	1.31
NIST domain	144	109	42	21	2	0	0	10	1.28
Remote computer	41	40	37	0	0	1	0	0	1.90
Application software	**133**	**119**	**103**	**3**	**0**	**15**	**0**	**0**	**1.80**
Backup	4	4	4	0	0	0	0	0	2.00
E-conferencing	17	12	12	0	0	6	0	0	1.76
IT support incident management sys	3	3	2	0	0	0	0	0	1.67
NIST application	32	29	16	1	0	3	0	0	1.53
NIST time & attendance	19	19	17	0	0	0	0	0	1.81
Not specified	1	1	1	0	0	0	0	0	2.00
Online banking	5	4	5	2	0	2	0	0	2.60
Online shopping	3	2	3	0	0	0	0	0	1.67
Web application	47	43	43	0	0	4	0	0	1.91

Application Type	# Of events	Pass-Word	User ID or Name	PIN	Badge or PIV Card	Other Info	Token	Bio-metrics	Avg # of items needed
Email	**52**	**52**	**48**	**11**	**0**	**1**	**12**	**0**	**2.38**
NIST e-mail	33	33	33	11	0	1	12	0	2.73
Personal e-mail	19	19	15	0	0	0	0	0	1.79
Physical access	**49**	**0**	**0**	**0**	**48**	**1**	**0**	**0**	**1.00**
Building/door entry	32	0	0	0	31	1	0	0	1.00
Gated location	17	0	0	0	17	0	0	0	1.00
Mobile phone	**28**	**11**	**0**	**17**	**0**	**0**	**0**	**0**	**1.00**
Cellular/phone account	28	11	0	17	0	0	0	0	1.00
Computer security	**19**	**19**	**14**	**0**	**0**	**0**	**0**	**0**	**1.74**
Computer encryption	8	8	8	0	0	0	0	0	2.00
OS privileged access	3	3	1	0	0	0	0	0	1.33
Password manager	7	7	4	0	0	0	0	0	1.57
PC security package	1	1	1	0	0	0	0	0	2.00
Network access	**13**	**5**	**11**	**7**	**0**	**0**	**7**	**0**	**2.31**
NIST wireless network	5	4	4	0	0	0	0	0	1.60
Virtual Private Network	7	0	7	7	0	0	7	0	3.00
Wireless network	1	1	0	0	0	0	0	0	1.00

Application Type	# Of events	Pass-Word	User ID or Name	PIN	Badge or PIV Card	Other Info	Token	Bio-metrics	Avg # of items needed
Voicemail	**5**	**1**	**2**	**4**	**0**	**0**	**0**	**0**	**1.40**
Home voicemail	1	0	0	1	0	0	0	0	1.00
NIST voicemail	4	1	2	3	0	0	0	0	1.50
Service	**2**	**0**	**0**	**1**	**0**	**2**	**0**	**0**	**1.50**
Library card	1	0	0	0	0	1	0	0	1.00
Purchase (debit)	1	0	0	1	0	1	0	0	2.00

Figure 9 below displays the information from **Table 3** in bar chart form. Specifically, it charts the number and types of authentication elements reported being used for each application category, e.g., IT system access, e-mail, Network access, and so on.

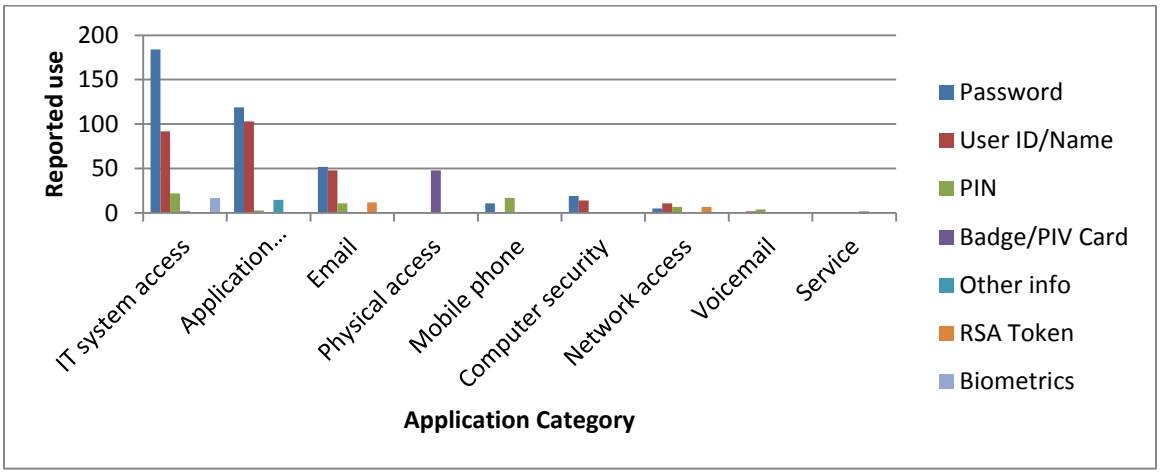


Figure 9: Authentication elements used for authentication by application category

The application categories that demanded the largest average number of elements for authentication were *IT system access* and *Application software*. Reported password use was higher than username/ID use in several categories; in these cases it is expected that the username portion of the authentication event had already been supplied by the application. For example, a locked computer session inherently has a user ID associated with it. Also of note is the fact that mobile phone users reported using both PINs and passwords to access their devices, when in fact it is possible some of these elements were mis-reported, i.e., that elements labeled as passwords were actually PINs.

4.4.3 Authentication information memorization and memory aids

Participants in this study reported using a variety of memory aids to help them avoid mistakes while performing their authentication tasks during the study period. In this case, we define a "memory aid" as anything that helped relieve some of the authentication-related pressures on participants' memories. By this definition, a memory aid could be a record of passwords and PINs, or a non-password authentication mechanism (such as a fingerprint reader) that helps minimize the need to use passwords at all. Note that authentication tasks that did not involve memory use by design, e.g., physical access using a badge and badge reader, are delineated as such. However, there were some events where the participant could provide *something they are*, such as a fingerprint, as opposed to *something they know*, like a password. In this type of event where participants *chose* to use fingerprint scanners rather than provide one or more other elements, the use of biometric information was considered a memory aid.

While all participants reported having at least some passwords and PINs memorized, all but two participants reported using some type of memory aid. Some stored their passwords in a client such as a Web browser, or wrote them down in an electronic file or on paper. Others used password manager programs or secure USB drives.[8] Participants also used strategies such as keeping a designated "root" segment of a password the same and changing a predefined part of it every time that password was about to expire**.**

4.4.3.1 Memorization reported

All participants recorded at least one event where they reported having used a memorized authentication element for authentication during the study period. Indeed, of the total 528 events, 353 events (66.86%) were reported as having at least one element that was described as memorized. Note that it was often the case where multiple elements were required for an event, the diary form did not prompt participants to note which elements were memorized, only to indicate if at least one was memorized.

For these 353 events, where one or more elements used in the event's authentication task were reported to be memorized, **Table 4** shows how many events were reported being used for the types of memory aids reported. The data reported in **Table 4** were collected from both diaries and follow-up interviews.

Table 4: Memory aid use where one or more elements were memorized

Memory Aid	Number of events
Paper note	34
Maintaining the same root or stem for passwords while varying one or more parts	8
Biometric (fingerprint)	5
Client application storage (e.g., Web browser)	5
Configuring the computer or application to use local user ID information	3
Electronic file	2
Memorable phrase	2

[8] These store passwords and/or other confidential information in encrypted form: the user must enter a "master" password to access the stored information, but the user does not have to follow any policies regarding password composition when creating this master password, nor is he/she required to change it regularly.

Memory Aid	Number of events
Total number of events in which memory aids were employed when elements were reported being memorized	**59**

As shown in **Table 4**, of these 353 events, participants reported 59 events where a memory aid was used. Put another way, participants reported a total of 294 events where the authentication task was completed by use of memory without additional aid. In the context of all events reported for the study period, this is 294 of 528 total events, or 55.5%.

4.4.3.2 Memorization not reported

For the 175 events where authentication information was not reported as being memorized, 50 events were of the type that required the participant to provide a sole physical authentication element *(something you have)*, e.g., an identification or library card; therefore information recall was not a part of the authentication task. Additionally, five events were for authentication prompts that the participant aborted without entering information (the participant did not know why the prompt appeared). And finally, eleven events were reported without indication that one or more elements were memorized or that memory aids were used. The omission of the memory aid information appeared to be an oversight by these participants, as each participant who omitted the memory aid information for these eleven events recorded the memory aid information for other events reported in their diaries.

For the remaining 109 events, participants did not report memorizing the elements required for authentication and relying on other aids to help them complete the authentication task.

Table 5 shows how often the different types of memory aids were noted as being used for events where participants did not report elements being memorized. Again, the data were extracted from both participant diaries and follow-up interviews.

Table 5: Memory aids used when memorization not reported

Memory Aid	Number of events
Client application storage (e.g., Web browser)	59
Paper note	14
Vaults and managers (e.g., IronKey, KeePass)	13

Memory Aid	Number of events
Biometric (fingerprint)	11
Electronic file	8
OAuth[9] used to attempt recovery of forgotten information	4
E-mail used to attempt recovery of forgotten information	3
Total number of memory aids employed when elements were reported not being memorized	**112***

* Note that one participant reported using two memory aids for the authentication information used in three events, relating where a password was written on paper as well as stored in an application, which resulted in three reported uses of memory aids beyond the 109 events for this category. These data show that only one participant reported using a "back-up" method for authentication retrieval for elements that were not memorized, while other participants relied on one chosen method, without reporting the use of additional methods for authentication element retrieval in the event that their primary method failed in some way.

The previous two tables show how many times, i.e., the frequency expressed in number of events, each memory aid was used in the context of authentication information memorization. The next subsection presents how many memory aids participants reported using overall and the context of authentication information memorization when it was available.

4.4.3.3 Number of memory aids used

Through their diary entries and interviews, each participant reported on the types and number of memory aids employed. **Figure 10** shows the distribution of how many memory aids participants reported using. This data were extracted from both the diary and interview data. The use of two different memory aids was the most commonly reported situation (nine participants); however two participants reported not using any memory aids, while one participant reported using five different memory aids for the various authentication elements required over the course of the study period.

[9] OAuth is an open protocol to allow secure authorization using a standard method for multiple platforms. More information is available at http://oauth.net/

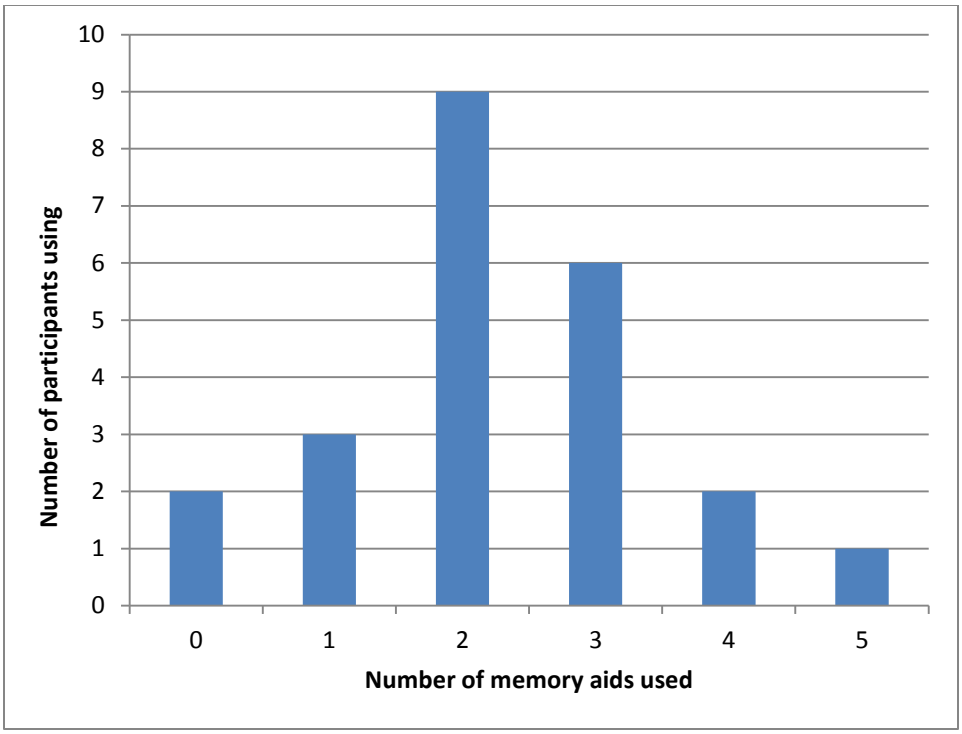


Figure 10: Number of authentication memory aids used by participants

As noted earlier, participants also reported whether one or more authentication elements for each event were memorized; this was usually associated with a password or PIN. The diary data can be viewed by which types of memory aids were noted when participants reported that one or more authentications elements were memorized or not. The next segment explores this perspective.

Table 6 shows how many participants used each memory aid that was reported being used in both the diaries and interviews. The two middle columns in the table provide insights from the diary data to distinguish which memory aids were used when one or more authentication elements were reported as being memorized. The right-most column (heavy shading) in the table provides data on memory aid use from the follow-up interviews. In particular, this data comes from the interview question, "What kinds of tricks do you use to make authentication easier or more efficient for yourself?" Often the number of participants detailing use of a particular memory aid in their diary did not match with their reported memory aid use during the later interview.

Again, events where an authentication element of the type "something you have", e.g., a identification or library card was required and no other authentication information was used, and where the element was not substituted for "something you know", e.g., a fingerprint instead of a password, were excluded from the table below.

Table 6: Authentication memory aids used by participants

Memory Aid	… when elements(s) memorized	… when elements(s) NOT memorized	Use reported during interview[10]
Client application storage (e.g., Web browser)	1	12	3
Paper note	5	6	5
Electronic file	1	3	3
Biometric (fingerprint)	1	3	3
Vaults and managers (e.g., IronKey, KeePass)	0	2	4
E-mail hints, reminders, or passwords	0	2	0
OAuth	0	1	0
Configuring the computer or application to use local user ID information	1	0	0
Maintaining the same root or stem for passwords while varying one or more parts	1	0	5
Memorable phrase	1	0	1
Using the same password across all applications (where possible)	0	0	2

From the perspective of which memory aids were reported being used by the most participants, use of client authentication information storage, e.g., Web browser storage, was the most prevalent. Use of the paper note was the next most commonly employed memory aid. Use of electronic files and biometric (fingerprint) data was next highest in reported use. In addition to the first four listed aids, password vaults, managers, e-mail, and OAuth were the types of memory aids used when authentication information was not reported being memorized – note conversely these aids were not used when information was reported being memorized (table entries are lightly shaded). Likewise, there were three memory aids used exclusively when elements were reported being memorized:

[10] The interview data did not contain detail regarding whether memorization was associated with memory aids. It is reported here to give insights into the types of memory aids and strategies participants use.

configuring the computer to use the local user ID, maintaining the same root or stem, and use of a memorable phrase (medium shading), in addition to the top four listed memory aids. Finally, two participants reported in the follow-up interviews, use of the strategy of attempting to use the same password across all applications.

The memory aids discussed in this section are part of a larger collection of coping mechanisms our participants reported using to deal with authentication. We explore these coping mechanisms – memory aids included – in more detail in **Sec. 6.4**.

4.4.4 Authentication problems

15 of the 23 participants who logged authentication event data for the study reported having one or more authentication problems during the study period. Of the 528 total events recorded, 48 (or 9.09%) were "problematic" (meaning that participants experienced some problem during those events). **Figure 11** shows the number of problems in relation to all events reported by each participant during the study period.

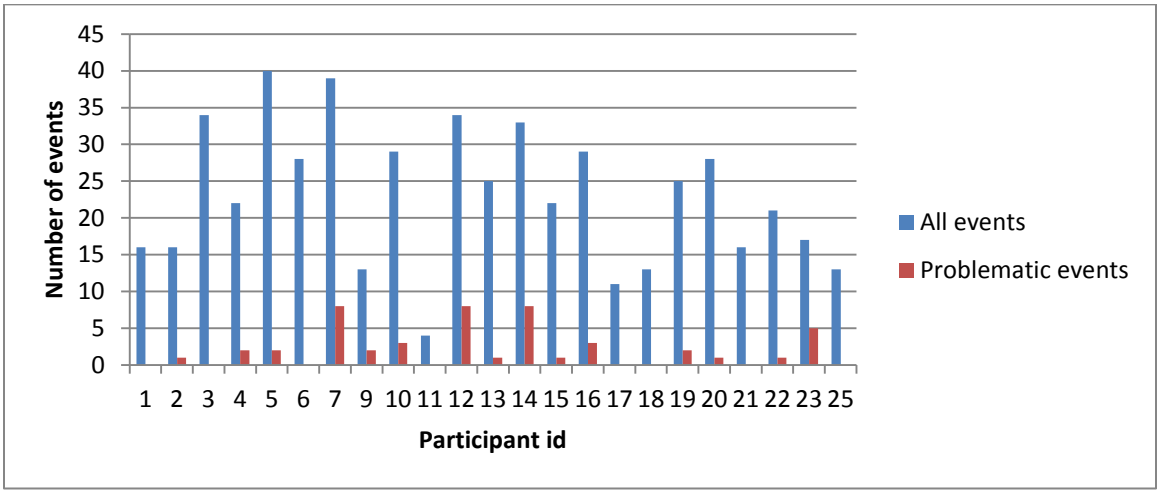


Figure 11: Number of authentication problems reported by each participant

The average number of authentication problems per participant was 2.09 $\pm$ 2.66 SD.55; three participants reported eight problems each, while eight participants did not report encountering any authentication problems during the study period.

Table 7 shows the types of problems reported by each participant, along with the number of occurrences of each type of problem (for a total of 48 authentication events with a reported problem). The most common authentication problem was mistyping one's password (50.00%), followed by using the wrong password and problems due to an unknown cause (14.58% each). As stated earlier, there were five events where the unknown cause reported by one participant was a case where an application was requesting authentication information, seemingly without cause; the participants reporting the remaining two events of unknown cause simply could not detect the cause of a failed authentication attempt.

Table 7: Authentication problems reported

Problem or issue	Number of occurrences	Percentage Of problems	Percentage of all events
Mistyped password	24	50.00%	4.55%
Unknown cause	7	14.58%	1.33%
Used wrong password	7	14.58%	1.33%
Account/password not recovered	2	4.17%	0.38%
Forgot password	2	4.17%	0.38%
Caps lock on	1	2.08%	0.19%
Could not find where to enter password	1	2.08%	0.19%
Forced to strengthen weak password	1	2.08%	0.19%
Forgot user ID	1	4.08%	0.19%
Password change required re-authentication[11]	1	2.08%	0.19%
Trouble finding (written) memory aid	1	2.08%	0.19%

[11] This often occurred when participants changed the general realm password they used for applications such as the corporate e-mail client, and then had to enter the new password on applications they had opened using the previous password.

4.4.5 Actions taken after encountering authentication problems

Participants were asked to report what actions they took after encountering a problem during authentication. 13 participants reported a total of 43 actions taken after encountering authentication problems. “Try again immediately” was the most commonly employed action by a large margin. This is not surprising given that the most common problems reported were mistyped passwords or using the wrong password. The next most common action was “dismiss pop-up,” which requires some explanation. This was the user’s solution to a problem stemming from a glitch in the PIV card middleware used by participants with the Windows XP operating system. The problem occurred when a user logged into the computer and by extension the e-mail client using his/her PIV card, removed the card to lock the computer, and later unlocked the computer with a user ID and password. The e-mail client would detect that the user ID and password, while valid, did not match the authentication information originally used to log in, and would generate a pop-up. It did not, however, require re-authentication, so dismissing the pop-up was the only action the user needed to perform.

Each action category is given in **Table 8**, along with the number of times used and the percentage of the 43 total actions.

Table 8: Actions taken after authentication problems

Strategy	# of times used	% of times used
Try again immediately	30	69.77%
Dismiss pop-up	5	11.63%
Contact NIST support	2	4.65%
Correct and resubmit	2	4.65%
Ask a colleague	1	2.33%
Give up	1	2.33%
Log out and back in	1	2.33%
Review memory aid	1	2.33%

4.4.6 Participant frustration ratings

Participants were asked to rate their level of frustration for any problems they encountered on a scale of 1 to 5, with 1 being “Not Frustrated” and 5 being “Very Frustrated.” Some participants gave a frustration rating even when they did not record

having any problems, and some did not record a frustration rating even when they *did* record problems.

Unfortunately the middle position (3) of the frustration rating scale was labeled "Neutral" on the diary form: this potentially complicates the interpretation of these results, as the qualitative interview data indicates that some participants used the numbers as a rating of the strength of the frustration they experienced. In that case, 3 would not be "Neutral" but instead would designate a level of frustration higher than 2 and lower than 4.

Table 9 shows the total number of reported authentication events for each application, as well as how many (and relative percentage) of those events were "problematic." The table also shows participants' average frustration ratings with each type of application.

Table 9: Authentication problems and frustration ratings by application

Application	# of problems	# of events	Average number of problems	Average frustration (1-5 scale)
IT system access	**21**	**227**	**9.25%**	**1.73**
Local computer	4	42	9.52%	1.69
NIST domain	16	144	11.11%	1.89
Remote computer	1	41	2.44%	1.24
Application software	**18**	**133**	**13.53%**	**1.52**
Backup	1	4	25.00%	1.50
E-conferencing	6	17	35.29%	1.71
IT support incident mgmt sys	0	3	0.00%	1.00
NIST application	2	32	6.25%	1.19
NIST time & attendance	6	21	28.57%	2.46
Not specified	0	1	0.00%	0.00
Online banking	0	5	0.00%	3.50
Online shopping	0	3	0.00%	1.00
Web application	3	47	6.38%	1.26
E-mail	**6**	**52**	**11.54%**	**1.59**
NIST e-mail	5	33	15.15%	1.96
Personal e-mail	1	19	5.26%	0.85
Physical access	**1**	**49**	**2.04%**	**1.55**
Building/door entry	1	32	3.13%	1.52
Gated location	0	17	0.00%	1.60
Mobile phone	**0**	**28**	**0.00%**	**1.08**
Cellular/phone account	0	28	0.00%	1.08
Computer security	**1**	**19**	**5.26%**	**2.00**
Computer encryption	0	8	0.00%	2.80

OS privileged access	1	3	33.33%	3.00
Password manager	0	7	0.00%	0.80
PC security package	0	1	0.00%	0.00
Network access	**2**	**13**	**15.38%**	**2.44**
NIST wireless network	2	5	40.00%	3.00
Virtual Private Network	0	7	0.00%	1.75
Wireless network	0	1	0.00%	0.00
Voicemail	**0**	**5**	**0.00%**	**1.20**
Home voicemail	0	1	0.00%	1.00
NIST voicemail	0	4	0.00%	1.25
Service	**0**	**2**	**0.00%**	**1.00**
Library card	0	1	0.00%	0.00
Purchase (debit)	0	1	0.00%	1.00

While we expected participants to assign relatively high frustration ratings to applications that frequently had authentication problems, we were surprised to note that participants indicated (sometimes considerable) frustration with certain applications even when they experienced few or no problems with those applications. For example, no participants reported experiencing authentication problems with online banking or computer encryption, but the average frustration ratings associated with these applications were among the highest on the list. Other applications that participants reported as problem-free but somewhat frustrating were the NIST VPN (1.75) and entering a gated location on the NIST campus (1.6). This data suggests that additional factors beyond an actual "problem" experienced by a participant during a specific authentication event (or not), influence the frustration rating recorded for the event.

Table 10 displays the total number of authentication events each participant recorded during the reporting period, their total number of problem events, and the average level of frustration experienced by each. If a participant did not give any frustration ratings, the relevant cell in the "Average frustration" column contains a dash (-) rather than a number.

Table 10: Individual participants' problem events and average frustration ratings

Participant	Total # of events	# Events with problems	Average frustration (1-5 scale)
1	16	0	-
2	15	1	1.53

Participant	Total # of events	# Events with problems	Average frustration (1-5 scale)
3	34	0	0.65[12]
4	22	2	1.00
5	40	2	-
6	28	0	1.64
7	39	9	1.53
9	13	2	1.00
10	29	3	5.00
11	4	0	1.00
12	34	8	2.63
13	24	1	4.67
14	34	8	3.09
15	22	1	1.05
16	29	3	3.33
17	11	0	1.60
18	13	0	1.00
19	25	2	1.00
20	28	1	1.25
21	16	0	-
22	21	1	2.76
23	17	5	3.00
25	13	0	1.08

[12] Participant 3 actually used a 0 in the frustration scale when his/her browser stored a password, which significantly lowered his/her average frustration: technically "1" should have been the lowest score recorded.

Eight participants (1, 3, 6, 11, 17, 18, 21, and 25) did not record any problems, while five participants (2, 13, 15, 20, and 22) recorded experiencing 1 authentication problem during the reporting period. Ten participants (4, 5, 7, 9, 10, 12, 14, 16, 19, and 23) recorded experiencing multiple problems. Five participants (10, 13, 14, 16 and 23) had average frustration ratings of 3.0 or higher. Note that participants' frustration level did not always correlate with the number of problems they encountered during the reporting period: for example, participant 13 reported one problem but recorded an average frustration level of 4.67, while participant 7 reported eight problems but had a much lower average level of 1.53.

5 VISUALIZING THE EFFECTS OF AUTHENTICATION: THE USER EXPERIENCE

One of the goals of this study was to understand better how authentication affected users over the course of a workday. To that end, the data captured from participants' diaries and follow-up interviews were used to quantify and chart their individual experiences during the data collection period.

As presented at the beginning of **Sec. 4**, the 23 participants reported a total of 528 application events during the data collection period, meaning they each experienced an average of 23 authentication events. After observing the results presented in **Sec. 4**, the research team members posed additional questions of the data in an attempt to break down these numbers even further: Do the authentication events tend to happen at particular times of the day? Do authentication problems occur at certain times of the day more than other times of the day?

In order to answer these questions, visualizations of the diary data were generated depicting how authentication impacted a user's day. The next sections explain how these visualizations were constructed, and the visualization for Participant 23 is displayed in **Fig. 12** in **Sec. 5.3** to illustrate the method employed. Visualizations for each participant are shown in **Appendix B**.

5.1 THE "JOURNEY MAP" AS A TEMPLATE FOR USER EXPERIENCE VISUALIZATION

The concept of a "journey map" was the starting point for this visualization. The idea for this particular tool came from a lecture by the author Kurt Vonnegut, who used journey maps to lay out the various narrative arcs a hero might travel in the course of a story [25]. Vonnegut first started sharing this idea in the 1990s. Not much later, design firms adopted a similar approach – perhaps inspired by Vonnegut's visualization of the storyline – to "map" the customer "journey" as customers encounter an organization, interact with it, and then end the relationship or start a new cycle. A discipline of design called *service design* [22][23] regularly uses a variant to depict customer experience

touch points with a particular service and factors involved in those customer interactions with the service that might be causing highs and lows.

The journey maps used in design are typically generated heuristically – that is, researchers or designers review user stories that sometimes come from ethnographic data, make inferences about why users had the experiences they reported, and then place users in the map accordingly, much like tracking the epic journey of a protagonist in a story.

The research team co-opted the concept of journey maps to model and visualize the impact of authentication. Because the factors that caused, fed, and weighted disruption could be quantified, a series of formulas to aid in the modeling of authentication events for the journey maps were generated. The visualizations helped the research team see, participant by participant, the times during the day when participants encountered and perhaps struggled with authentication.

5.2 MEASURES USED IN THE USER EXPERIENCE CHART

A chart was created for each participant, using their recorded events, with the time of day on the x-axis and a scale of what the research team called "User experience" on the y-axis. While the x-axis component is a straightforward value representing time of day, the user experience component (y-axis) is based on quantifiable measures gathered from the participants.

The user experience scale runs between +5 and -5, with +5 representing no impact on the experience (i.e., the primary task the user is performing) from authentication, 0 indicating moderate impact, and -5 representing extreme disruption. The user experience scale used here is consistent with the Service Design-based Journey Map concept, in that the positive end of the scale maps to more positive user experiences, while the negative end of the scale maps to less positive user experiences.

Four measures are shown on each participant's user experience chart. The first three measures, based on collected data, are the frustration rating the participant assigned to each event; an interviewer rating assigned by the researcher based on data from the interview with the participant; and a calculated value of effort and interruption for each event. The final measure is a composite informed by the previous three.

Note that since the scales used in the underlying measures, e.g., user-supplied frustration rating, were not already on a +5 to -5 scale, the appropriate linear transformations were applied to convert each collected data set into appropriate values for the +5 to -5 user experience scale employed in these charts. The next sections provide the details on how each measure was informed.

5.2.1 Frustration Rating

The **Frustration Rating** (red line in the user experience graphs) was taken directly from diary data supplied by the participant and mapped to a +5 to -5 scale. On this scale, a +5 means the participant reported a frustration rating of 1 ("Not Frustrated"), while a -5

means the participant reported a frustration rating of 5 (“Very Frustrated”). A zero (0) means the participant means the participant reported a frustration rating of 3.

5.2.2 Interviewer Rating

The **Interviewer Rating** (green line in the user experience graphs) was assigned by a researcher based on interview data for each event. This rating is intended to inform the impact on the primary task enabled by a given authentication event, in terms of both completion and ripple effects. The researcher assigned a score of 1-4 based on which of the following occurred during an event:

1 The need to perform authentication slightly delayed the primary task

2 Problems with authentication necessitated extra work, steps, and/or work-arounds to continue with the primary task

3 Problems with authentication prevented full completion of the primary task, i.e., some progress on the primary enabled, but full completion restricted or blocked

4 Problems with authentication caused primary task failure, i.e., the participant was unable to make any further progress on the primary task

A linear transformation was then performed on these scores to assign an appropriate representation on the user experience graph. The mapping is shown in **Table 11** below.

Table 11: Interviewer rating mapping for assigned scores

Interviewer assigned score	Interviewer rating (mapped to user experience scale)
1	4
2	1
3	-2
4	-5

5.2.3 Calculated Disruption

The **Calculated Disruption** (blue line in the user experience graphs) is a composite measure representing impact from the authentication subtask, based on three factors:

- Authentication Event Outcome: success or failure of the authentication event

- Impact on task switching: categorized assessment of how much attention the authentication enabling task might have taken, e.g., how much problem-solving was needed when a problem was encountered during the event

- Authentication information entry effort: the effort required to supply necessary authentication elements.

The research team expected that these three factors, taken together, would provide a useful view of the user experience. To the team's knowledge, this application is the first of its kind to employ these measures in this way. The value assignments used for each factor are explained below. Overall, each assignment was chosen in an effort to appropriately inform the factor, with consideration for the impact on the visualization, i.e., providing separation of significant factor differences. Therefore, other values could be determined to be more useful or representative with additional research; however, the ones used in this study were considered adequate by the research team for the visualizations provided by the user experience charts and to illustrate the method.

5.2.3.1 Authentication Event Outcomes

The authentication event outcome served as the base value for the calculated disruption composite metric. As shown in **Table 12**, the calculated disruption measure had a base value of 3 if an authentication event was successful. If the event ended in failure, however, the calculated disruption measure had a base value of -3.

Table 12: Authentication outcome factor values for calculated disruption

Authentication Event Outcome	Impact	Value
"Success"	Minor	+3
"Failure"	Major	-3

5.2.3.2 Impact on task switching

Any authentication problems encountered by a participant during an event were also factored into the Calculated Disruption measure. Each diary-reported problem (as listed in **Sec. 4.4.4**) impact was categorized as "Major" or "Minor". For each minor-impact problem, a value of 1 was added to the Calculated Disruption measure, while 1 was subtracted for each major-impact problem.[13] The categorizations and value adjustments for each problem are shown in **Table 13**. It should be noted that the participants in this

[13] The exception to this rule is the problem "Needed to correct authentication element before submitting," which is categorized as having a "Minor" impact but has a value of -1. This is because, when this problem occurred, the participant was eventually able to authenticate successfully but had to spend extra time and effort reviewing/re-entering their password in order to do so.

study reported a single problem when any problem was encountered therefore, only one value would be selected from this category per event.

Table 13: Authentication problems and corresponding calculated disruption value adjustments

Problem reported	Impact	Value
Caps lock on	Minor	+1
Needed to correct element before submitting	Minor	-1
Mistyped password	Minor	+1
Password change required re-authentication	Minor	+1
Could not find where to enter password	Major	-1
Forgot password	Major	-1
Forgot user ID	Major	-1
Lost PIV	Major	-1
Misremembered password	Major	-1
Trouble finding written memory aid	Major	-1
Unknown problem	Major	-1
Used wrong password	Major	-1
Weak password – forced to strengthen	Major	-1

5.2.3.3 Authentication Element Entry Effort

The factor pertaining to the effort required to submit authentication information was informed by adding an assigned "effort value" for each element reported being used during an authentication event. The effort factor added to the overall calculated distribution measure is always a negative value, reflecting the negative effect on the participant's primary task. As shown in **Table 14,** the value -0.5 is assigned if the user had the element memorized or had to look it up (e.g., on a handwritten note), and -0.1 if the element was contained in a mechanism such as a Web browser or PIV card. Note the relatively small value assigned to the Minor impact category reflects the relatively lower cognitive impact on the user.

Table 14: Effort values for different types of authentication elements

Authentication element status	Impact	Value
Memorized or remembered	Major	-0.5
Look up by user (e.g., RSA token, file, paper)	Major	-0.5
'Something you have,' 'something you are' or contained in mechanism (e.g., PIV card, fingerprint, browser-stored)	Minor	-0.1

Most authentications required a combination of different types of elements or information, and some required multiple elements of the same type. The following examples show how effort values were calculated depending upon the elements used in a given authentication event:

- Participant used a (one) password stored in browser (1 element contained in the mechanism): yields a calculated value of -0.1

  Calculation: $(1)_{(element)}*(-0.1)_{(assigned\ value)} = -0.1_{(calculated\ value)}$

- Participant used a memorized password (1 element memorized): yields a calculated value of -0.5

  Calculation: $(1)_{(element)}*(-0.5)_{(assigned\ value)} = -0.5_{(calculated\ value)}$

- Authenticated to VPN (2 elements memorized, 1 token element): yields a calculated value of -1.5

  Calculation: $(2)_{(elements)}*(-0.5)_{(assigned\ value)} + 1_{(token\ element)}*(-0.5)_{(assigned\ value)} = -1.5_{(calculated\ value)}$

5.2.4 Composite Rating

The **Composite Rating** (purple line in the user experience graphs) was created by a simple weighting of each of the above three measures. Since participants did not always supply a frustration rating for each event, two sets of weights were created.

- If the participant supplied a frustration rating for an event, the measures for that event were weighted as follows:
  - Frustration Rating = 20%
  - Interviewer Rating = 30%
  - Calculated Disruption = 50%

- If the participant did not supply a frustration rating for an event, the measures for that event were weighted as follows:
    - Interviewer rating = 40%
    - Calculated Disruption = 60%

In the early stages of development of the user experience graphs for this study, it seemed logical to give more weight to the user-reported frustration ratings than the Interviewer Rating or Calculated Disruption rating, since the frustration rating was the most direct measure of impact on the participant. However, after carefully reviewing the frustration ratings provided by the participants, it was discovered that participants did not apply the frustration rating consistently (see **Sec. 4.4.6**). Additionally, in the retrospective review of events during follow-up interviews, participants sometimes expressed frustration or annoyance about events they had recorded, but for which they had not recorded any frustration rating.

In contrast, the Calculated Disruption rating (as described in **Sec. 5.2.3**) could be computed consistently across all participants. Given the greater reliability of this data, the research team elected to weight it more heavily in each of the weight sets.

Likewise, the interviewer rating provided some post-collection perspective. It gave the team a gauge of how authentication affected task completion and the ripple effects of authentication problems for the user.

Note that no authentication events have a user experience rating of +5 (no impact), because all authentications have an impact – at the very least, they delay users in the performance of their primary tasks

5.3 USER EXPERIENCE CHARTS

The user experience graph shown in **Fig. 12** displays the measures in relation to each other and the effect of the assigned weights in the composite measure for Participant 23 (P23), using the technique described in the previous section. User experience graphs for each participant were generated and are shown in **Appendix B.**

Admittedly, the disruption assignments are a set of values assigned without benefit of empirical data or research-based findings on relative disruption for each disruption component used; however, one could argue that since the assignments are applied uniformly across all participants' data, that as a visualization aid, fine-tuning the value assignments would be a matter of scale adjustment rather than negating the value of the visualization.

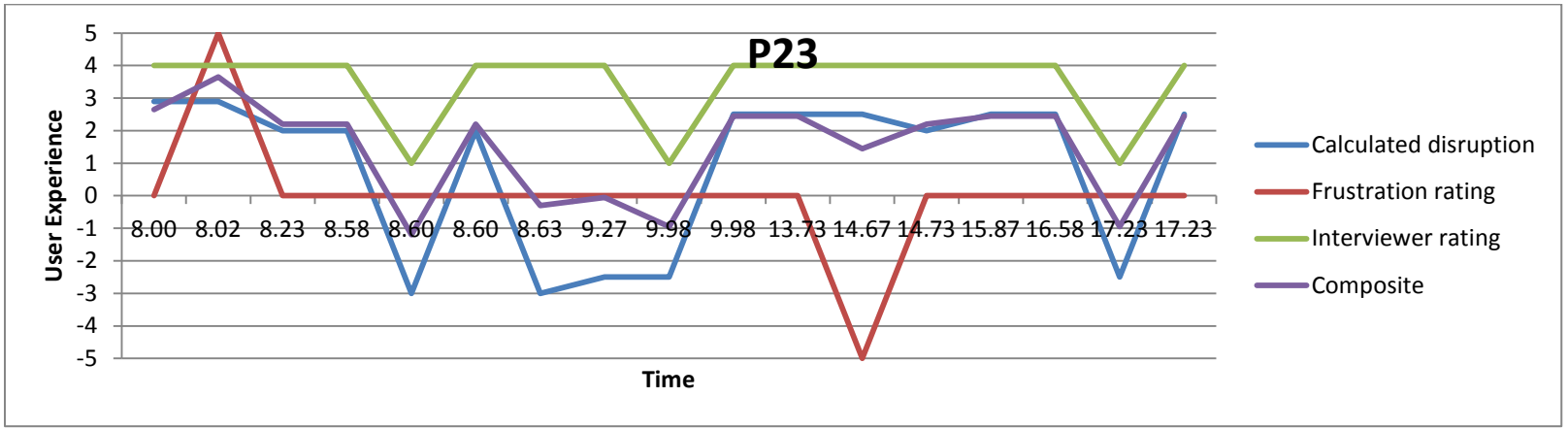


Figure 12: User experience graph – P23

This user experience graph tells the story of Participant 23's experience during the reporting period. Looking at the red frustration rating, we can see that at the beginning of the day, the participant did not experience frustration when authenticating (8:00, with a

frustration score of +5). But during the afternoon (~14:30), P23 experienced an event that caused extreme frustration (a score of -5). In a few unrelated cases, P23 experienced some authentication problems that prevented full completion of the primary task (the valleys on the green line at ~8:30, ~10:00 and ~5:30), however the participant never experienced complete primary task failure. The blue line, which indicates the amount of disruption caused by authentication events, tells us that while none of the authentication events were failures (e.g., the participant was unable to log in), P23 did have to take remedial action to recover from problems that were exacerbated by some circumstance that made providing the necessary authentication information difficult (e.g., the participant had to retrieve a memory aid). The composite (purple) line integrates the three measures together, showing us that though P23 experienced some problems and frustrations related to authentication, he/she experienced only light to moderate disruption during the day.

Figure 13 shows a different view of P23's event data. In this user experience graph, the composite rating assessment has been graphed for each event at its associated time of day. Rather than a line graph, discrete points are displayed representing the disruption for each event over the course of the day. Note that the time scale was also expanded to show the entire collection period.

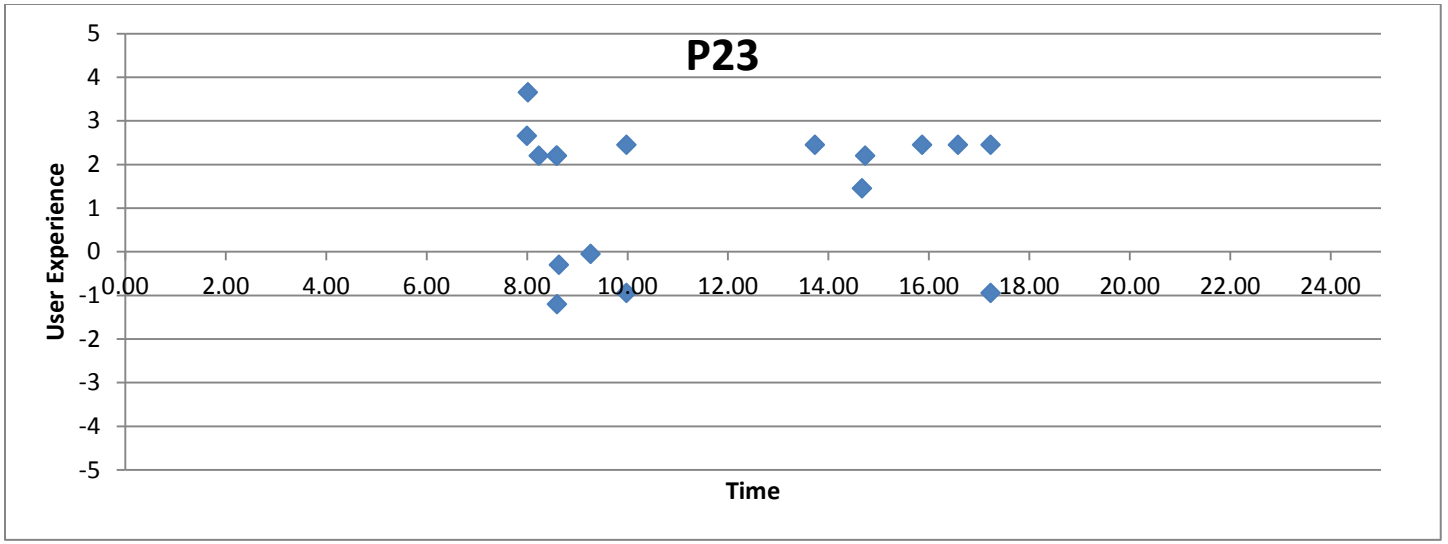


Figure 13: How users experience disruption caused by authentication - P23 (composite rating)

With this view, it is somewhat easier to locate clusters of events and the relative impact they represent over the course of the day, while the view shown in **Fig. 12** provides a good presentation of how the various ratings compare to each other. Using **Fig. 13**, it now becomes easier to discern that P23 experienced 5 mildly disruptive authentication events and 4 moderately disruptive authentication events before 10:30 AM. The authentication events that occurred after 1:30 PM were only mildly disruptive, with the exception of one event at approximately 5:30.

The view shown in **Fig. 13** was then used with the aggregated event data from all the participants using the composite rating method in order to provide an overview of the total disruption caused by authentication for all participants. The resulting graph can be seen in **Fig. 14**.

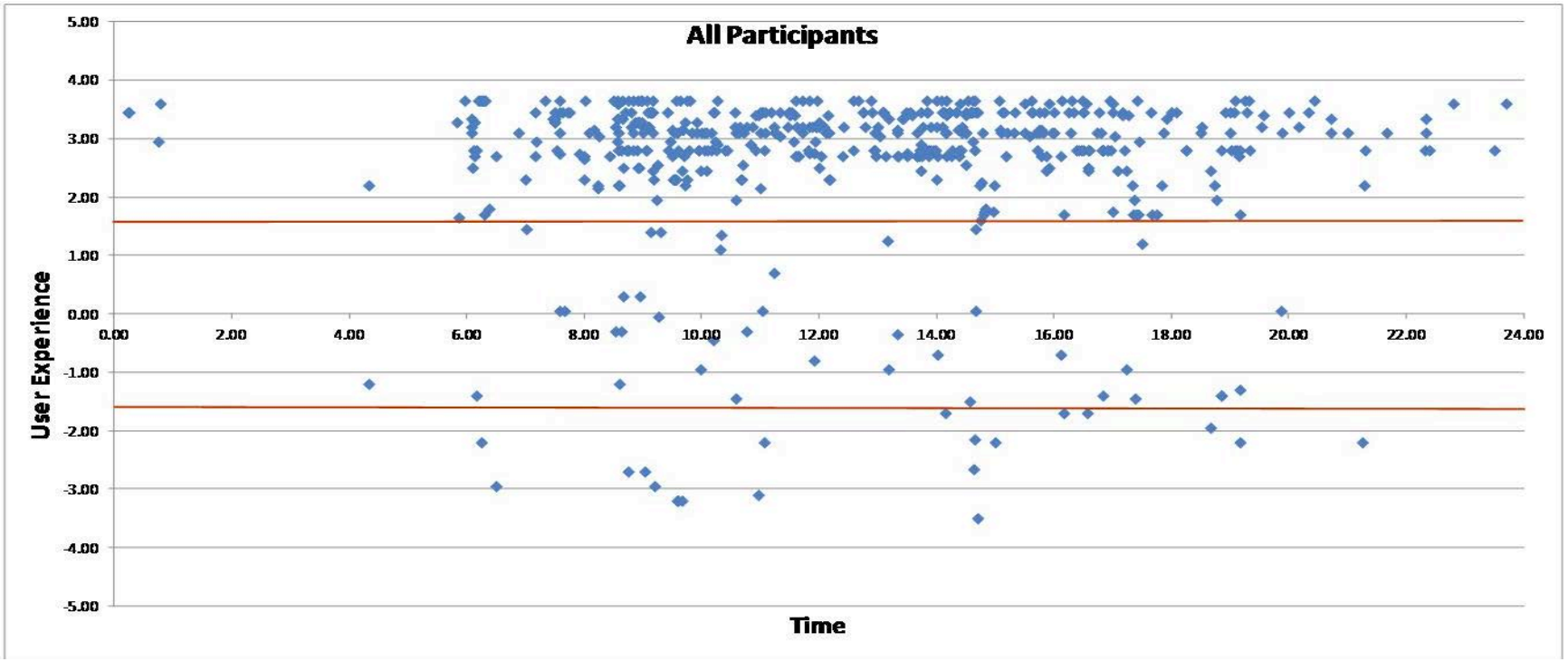


Figure 14: User experience with respect to disruption caused by authentication - all participants (composite rating)

Two horizontal lines superimposed over the graph designate ranges of disruption. The top area contains 466 (88%) of the authentication events, showing that the vast majority of events reported during the study period caused mild disruption (recall that all authentication events are at least mildly disruptive in that they delay completion of a primary activity). The middle or moderate disruption range contained 42 (8%) of the events, and finally, 21 (4%) of the events were very disruptive.

Figure 15 displays the same data for all participants in the form of a heat map representation to convey the composite disruption measure for each event across the course of the study period. Again, with respect to relative disruption, most events are in the mildly disruptive top 3rd of the graph. The highest concentrations of events occurred at 9:00 AM, 10:00 AM, 12:00 PM and 2:30 PM.

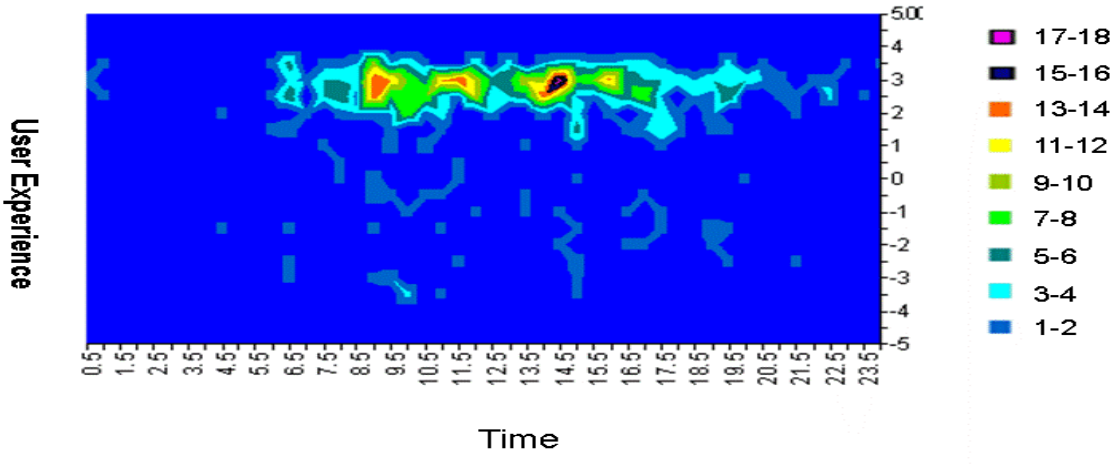


Figure 15: Heat map of authentication events and user disruption - all participants

6 DISCUSSION

This section addresses the researchers' interpretations of and insights gained from the research findings. The section presents qualitative data from the participants themselves, researcher observations regarding users' authentication-related behavior, and finally insights about authentication gained from this study.

6.1 HOW PARTICIPANTS PERCEIVED THEIR AUTHENTICATION WORKLOAD

As presented in **Sec. 4**, participants reported an average of 23 authentication events each during the data collection period. However, they did not notice (and therefore did not report) any automatic authentications facilitated by NIST's partial SSO solution. This means that the actual number of authentications was probably somewhat higher than the number reported.

Participants themselves were actually surprised at the number of authentications they reported during the data collection period. In briefing meetings before the data collection period, when the researchers gave participants diary forms (see **Appendix A** for an example) with space to record 20 authentication events, many participants asserted that they would need more diary forms because they were going to authenticate much more than 20 times. In the follow-up interviews, when researchers asked participants what surprised them most about their experiences during the data collection period, the answer was often related to their estimated vs. actual number of times authenticating. Several said they had authenticated far less than anticipated. A few said they had authenticated considerably more than they thought they would, but over-estimation was more common by far than under-estimation.

This is not because something unusual happened to participants during the data collection period. On the contrary, the day was fairly typical for most of them (except for the fact that they were recording authentication events). So where did this discrepancy between expectations and reality originate? The qualitative data suggest two principal reasons why many participants' actual authentication workload did not align with their expectations.

First, since participants taking part in the study were more aware of authenticating than was usually the case, they may have changed their behavior during the day. For example, some of them followed security policies more closely than usual: a few participants commented that during the study, they were more likely to purposely lock their computers when they left their desks than they normally did. The implications of the usual lack of awareness are significant. The qualitative data from this study suggest that authentication can become an automatic or automatized behavior: people do it habitually,

or by rote, until some significant disruption occurs (e.g., an authentication problem). Under most circumstances, participants reported they were not as mindful of authentication as they were when they recorded it for this study, reminiscent of the Hawthorne Effect.

Second, from the data in this study, we propose the theory that this discrepancy between expectations and reality is that the act (or even the prospect) of authenticating carries a notable emotional and psychological load. This may have affected participants' perceptions of the workload involved in specific authentication tasks and authentication in general: that is, participants' feelings about authentication made it seem to take more time and effort than it actually did. This emotional load is created in part by previous "catastrophic" experiences with authentication, such as when authentication problems severely delay work on a critical primary task:

> *"So a situation where authentication has been a real challenge and caused real problems, there's one example I can think of where I have a system that had completely failed, and I had to restore the system from a backup, a procedure that I've done a few times, works flawlessly without any problems. In this particular case there was some...just call it a bug that interfered with restoring the passwords to this device. These are root-level passwords, very low-level and basic passwords you log in to control a system, basically, the only account on this device, right? There's one account and it's super-user, super-privilege. That password had not been properly been reset, or it was...I think it was actually reset to a very, very, old password that...in hindsight it was a very, very old password, and it took me about three hours to figure out that that was the password that was in place and that something had happened in the configuration, and it restored a really old password or something like that. So that was very, very frustrating. The cost was actually high then. We had three hours, or two hours, of complete network failure of major component of our network, a major section of our network. So the cost was actually very high there, and it was all because the expected outcome of a restore didn't happen that way. […] The real cost is with all the people that are not able to use their systems and get their work done." (P5)*

It is understandable that a few experiences like the one described above would make a user wary about authentication and the disruption that can cause, and make authentication tasks (or even the prospect of performing authentication tasks) seem more time-consuming and effortful than they actually are.

Tension created by specific adverse experiences is only part of the emotional load related to authentication. The other part is the everyday experience of friction and disruption caused by authentication. The literature on task switching indicates that going from one

type of task to another – for example, from a creative primary task to the memory-intensive and physical task of recalling and typing in a password – has an impact on focus, concentration, and efficiency that can linger through subsequent tasks [7][16].

This issue may also be related to what is called the "Zeigarnik effect" (after the psychiatrist who first studied the phenomenon), which states that people remember uncompleted or interrupted tasks better than they remember tasks they finish [28]. Clifford Nass, a professor at Stanford University who studies multi-tasking and task switching, theorizes that users are painfully aware of disruption caused by authentication because authentication is imposed on them:

> *"I suspect that unlike multitasking, in which the task switching is voluntary and hence people have an incentive to downplay the costs, authentication is not voluntary, thereby making people aware of the cognitive cost. Also…negative experiences are much more memorable than positive experiences." [17]*

Study participants' own accounts give credence to the theory that they carried an emotional load related to authentication. They described, in detail and at length, the general and specific ways in which authentication makes their work (and their lives) more difficult than it would be otherwise. These friction points are the subject of the following section.

6.2 SPECIFIC "FRICTION POINTS" DESCRIBED BY OUR PARTICIPANTS

Participants' diaries from the data collection period provided insights into the aspects of authentication that the participants found particularly frustrating or difficult, as well as the applications for which they were most likely to have problems when authenticating. During the follow-up interviews, researchers asked participants for more detail about these "friction points." Many of them independently mentioned similar or identical issues, discussed in detail in **Secs. 6.2.1** through **6.2.5**. Many of these friction points were also identified as problematic issues for users of technology by an independent study at NIST regarding passwords [5].

6.2.1 Re-authenticating due to timed lockouts

One of the friction points most frequently mentioned by participants was that of having to authenticate to the same application over and over again, particularly because of the timed lockouts described in **Sec. 2.7**. The purpose of this measure is to make it more difficult for an attacker to exploit a user's computer (and access privileges) while the user is away from the computer.

Of the 42 local computer authentication events participants recorded during the reporting period, only 4 (or 9.52%) had problems and the average frustration rating associated with

the application was only 1.69 (see **Table 9**). However, almost half of the study participants (10) cited the timed lockout as a source of non-problem-related friction and frustration during follow-up interviews. Some participants noted that the timeout often takes effect while they are actually sitting in front of – but not actively using – their computers, which often disrupts or diverts their thought processes. Several participants expressed sentiments along the lines of "the system should know it's me." One participant said of the timed lockouts:

> *"Well, I think that if I just logged in, then it should be able to understand that I just logged in and not ask me for the password again. […] That's too much, because you shouldn't have to do extra work to authenticate. Because yeah, it can just pick up what you do." (P18)*

Periodically pressing a key or jiggling the mouse did not really alleviate the interruption and subsequent irritation caused by timed lockouts, as another participant noted:

> *"You end up having to almost set a timer in your head to go back to the computer and type something within every 10 minutes or so. And some minor studies of productivity I've been involved with indicate that it's better to be focused on a task as opposed to have lots of interruptions throughout the day." (P21)*

6.2.2 Remembering a large number of passwords and when/where each one is supposed to be used

Participants also said that having to remember all the passwords for all the different applications they used was very difficult: all but one participant in this study reported managing at least some passwords using some form of external record (e.g., handwritten note, password management software). Remembering which password corresponded to which application could be a problem as well, especially since some participants were unclear as to which passwords were synchronized and which were not:

> *"So there's the confusion of is this our BizFlow password? Is it our general realm password? Is it our Entrust password? Then they enter the password wrong. Then they think they need the password reset, but they don't because it's not actually the Entrust password that they're entering. So it's a big mess that way. […] Most users will say, "This is my e-Approval password." But e-Approval is a combination of now two different passwords, the general realm password and the Entrust password. But people think, "My e-Approval password," which will easily get them confused." (P3)*

6.2.3 Managing a large number of authentication elements

Authentication information management was also a major friction point. Again, the sheer number of passwords participants had to juggle was part of the problem (since they had to manage authentication information for many of the applications they used individually). When a password expired, participants would have to replace it with a new one, which they would have to commit to memory – and all the time and effort they put into this would cease to matter when the password expired and the cycle started again. In addition, the many applications they used could (and often did) have different password policies. A password that was acceptable for one application might not be allowed for another, which made it even more difficult to come up with compliant passwords. Passwords for different applications might also expire at different times. One participant expanded a specific example of this type of problem into a general complaint about it:

> *"[W]hen I started getting into the WebTA thing, it just so happened that it was time to change my password and WebTA makes you change your password more frequently than the NIST general domain. And every time I have to do that, I get really frustrated because I am like why can't they always be in sync. You have to think if you are going to be the responsible person, then you have to think of different passwords for everything and it is very frustrating. So when it gets to those infrequently used passwords, then I get really irritated." (P11)*

This participant touched on a related and particularly sore point: that of resetting passwords for applications that participants did not use often.

6.2.4 Management workload for infrequently used passwords

Multiple participants described the difficulties of managing a password that needs to be renewed more than it is actually used:

> *"[O]nce or twice a year I have to log into a foreign application we have here, and fill out a form, BizFlow, and I usually have to get my password reset because I don't remember what it was. I try a few times, and before I get to the right one I'm locked out." (P14)*

> *"I don't travel very often, but when I do I have to log in to something called Travel Management. And that password expires just as fast as any other password. Every single time I go to log in to submit my expense reports, first of all, my account is locked because I haven't changed my password in a few months. So then I have to figure out how to unlock it. Then I've got to go change it." (P19)*

“And e-Approval is something that I use so infrequently that each of the past few times I've had to do something in there, I've had to get my password reset, and it is very embarrassing.” (P11)

“Once again security has gotten in my way and it takes me extra time because now I got to look that one up because I don't use that one often enough.” (P17)

6.2.5 Miscellaneous friction points

Some other authentication-related friction points mentioned by participants included:

- The “human factor” – mistakes and weaknesses in the interaction because humans are forgetful or neglectful
- Being unable to re-use the same password multiple times on a single system, or across different systems
- The time and effort it takes to change passwords
- Being interrupted on the way to a task because of requirement to reset passwords
- Embarrassment at having to request support from a help desk when encountering an authentication problem
- The sheer number of authentication mechanisms and combination of requirements
- Password policies and other security rules that are not revealed until the user fails to meet them
- Drops and interruptions in connectivity to the VPN or wireless network because of some problem related to authentication

And finally, participants simply find themselves spending a great deal of time and effort on authentication:

“And it gets in the way. It definitely takes way more time out of my day, both just time having to deal with this and then the break in the flow of work.” (P19)

“In my attention it's a tiny blip, but time wise, I think it does actually still take a lot of time. There's a substantial amount of time” (P5).

6.3 PARTICIPANTS' FEELINGS ABOUT THE NECESSITY AND EFFECTIVENESS OF AUTHENTICATION

Authentication clearly created problems for the study participants (as described in **Sec. 6.2**). However, they did not think authentication should be scrapped entirely, nor did they think it was acceptable or appropriate to ignore, shortcut, or bypass NIST's organizational security requirements. Participants valued organizational security (see **Sec. 2.7**) and knew that authentication played a key role in maintaining it. They simply felt that authentication at NIST could be implemented in a more efficient and usable way.

6.3.1 While all participants saw a need for organizational security at NIST, some questioned the effectiveness of current methods

Several participants expressed the belief that following NIST security policy is an effective way to protect their own online assets and those of their co-workers. But more participants questioned whether the authentication requirements they must follow are actually effective. This is not to say that participants think the organization for which they work does not face real security risks. They had no expectation that the need to authenticate will ever go away, because there will always be "bad agents" who want to do damage for a variety of reasons. Rather, they felt that they had a part in protecting the organization from attackers – that they all shared some responsibility for organizational security. On that general point, they agreed with the organization and security specialists: however, they had specific disagreements about what security measures were actually appropriate.

Generally, participants did not fear unknown, non-specific attacks on organizational security. They also expected that most attacks (or the most serious attacks) would target the organization's servers or weaknesses in its infrastructure – not their own passwords. One participant said he had, "*Never had anyone steal my account or break in by stealing my password – that I know of*" (P7). Another echoed the sentiment, saying, "*No one has hijacked my accounts. Problems – fraud – comes from insiders, not people hacking. The emphasis may be in the wrong place*" (P20).

This is related to another belief many participants held regarding security risks: even if they followed all security policies perfectly and did everything imaginable, they could not guarantee the safety of their organizational systems. An attacker could still find and exploit some previously unknown vulnerability.

But another participant pointed out that it is unreasonable to expect security policies to be sufficiently proactive to counter unknown threats. On the contrary, security policies tend to be retroactive and implemented in response to specific security incidents:

"It's hard for the system administrators and the security people to design authentication approaches that are more flexible. It's just hard. So more of a brute force approach is what people tend to favor. Does it really make the systems more secure? I don't know. It appears not in general. It helps protect against accounts being broken into, perhaps, by coworkers or insider attacks more, but people who are still doing sophisticated attacks still seem to be able to do those and be relatively successful at them. A lot of this stuff at least some of the security requirements on laptops especially, especially when traveling – resulted more from, I think, higher level screw ups, people in upper level management having their systems being broken into." (P21)

The implication of this statement is that security policies are difficult to make flexible (i.e., responsive to actual risk assessment) and effective, which leads to burdensome polices that attempt to cover more weaknesses, both human and information-technology related.

6.3.2 Participants think organizational security measures are too demanding

In general, study participants were cautious about criticizing the state and implementation of security where they work. This may have been an artifact of an internally conducted study. Even so, participants strongly suggested that they felt they were required to authenticate too much, too often – that security policies were far more demanding than they had to be to address security risks, and may in fact have created new vulnerabilities. "*The things that move us beyond human memory, we have to use things less secure, like [password] sharing schemes. [IT] people are bound by their rules, not common sense*" (P20), as one participant put it. Some participants also expressed the belief that security policies related to authentication were so demanding as to be counterproductive:

"Going for longer and longer passwords, that just seems silly to me. I'm not sure that it actually gives you anything in terms of security, except it actually at a certain point decreases security." (P2)

"Authentication becomes a block if you don't use it frequently. It becomes an annoyance if you use it frequently." (P1)

"Human memory is limited. More security means more barriers, which makes it less usable. Close the door to attackers, but I have to put that password somewhere, which opens a window. Wish I could protect the whole house." (P3)

In addition, a number of participants worried that if the IT department found out about some of their strategies for coping with authentication (particularly schemas for password creation, as described in **Sec. 6.4.1.3**), they would prohibit these strategies through policy, technical enforcement, or both. Fortunately, this is not the case at

NIST, as its management supports this and related research in an effort to improve the usability of IT security at NIST and elsewhere. However, this is not an unreasonable concern within other organizations, given that IT departments often tend to see imposing stricter and stricter security requirements as the most effective way to deal with "inherently insecure" users [1].

Sentiments like these aside, many participants seemed resigned to dealing with the institution's security policies. As the final participant quote in **Sec. 6.3.1** implies, many considerations inevitably shape organizational security policy. Another participant summarized this situation by saying "*[It's a] cost of doing business in this environment. Just part of workday here*" *(P1).*

6.3.3 Overall, participants believe SSO is the best way to address both security and usability issues

Several participants suggested organization-wide SSO as a compromise solution that would reduce tension between the organization's need for security and their own need for usability (NIST already has partial SSO, as described in **Sec. 2.7**). A number of participants already employ authentication coping strategies that mimic SSO, such as synchronizing their passwords for multiple applications and trying to update all their passwords at the same time (see **Sec. 6.4.1.6** and **Sec. 6.4.1.7**).

Participants said they would accept having a long SSO password (longer than the ones they are currently required to use for any application) – provided that they could use it across all their work-related accounts, systems, and applications. As one participant explained it:

> *"…the strength of the single sign-on is if I only have to remember one password for my work, I don't care that that is a 12-character password. But it's just one. Right? ... Then I probably would not put it in my personal password vault or whatever, because I could keep better separation."* (P23)

However, they were aware that SSO contained the inherent risk of an attacker gaining access to the "master" password, and by extension all of a user's access privileges on every application he/she used. One participant summarized the issue by saying, "*If there's a break-in, the attacker has everything. I don't know how to balance that*" (P7).

Another participant suggested doing away with passwords entirely and using a biometrics-based SSO solution:

"We have to go to some sort of a single sign-on using biometrics. Enough of this business of trying to remember passwords and draw up rules for passwords that are designed to secure stuff when passwords themselves are not secure." (P17)

Unfortunately, some NIST users' experiences with biometric authentication – specifically, using fingerprint readers – suggests that this is not yet feasible. One participant indicated that fingerprint authentication is not a reliable alternative to passwords:

"This [authentication method] is worse, because it works by a biometric, and my finger doesn't read very well. I have to smear it with moisturizer, and then I forget what the actual password is. When it really just won't read my finger, I can't unlock it and I can't remember." (P2)

Whether it involved biometrics or not, implementing a true SSO solution at NIST would be extremely difficult (in part because of the way application ownership works within the organization – see **Sec. 2.7**).[14]

6.4 COPING WITH AUTHENTICATION

The study participants, like all users, are rational in the behavioral-economics sense: they have a high authentication workload, so they find or develop various ways to reduce the costs of individual authentication tasks. This allows them to use their authentication budget more efficiently and to greater effect than they would otherwise be able to do, all while complying with organizational security policies. In other words, they employ coping mechanisms to help them deal with the impact of authentication.

In this section, we describe specific coping mechanisms used by our participants and what participants' use of those coping mechanisms implies about how they view the relationship between authentication and security.

6.4.1 Coping mechanisms used by participants

Generally, participants' coping mechanisms reflected the desire to make authentication as automatic and unconscious as possible and minimize the amount of effort they had to spend on entering and managing authentication elements [19]. These mechanisms could be tools, behavioral strategies, or a combination of both.

---

[14] It may also not be feasible for Department of Commerce applications used within NIST, since NIST has no control over those applications.

Memory aids are perhaps the most obvious (and common) examples of coping mechanisms. As described in **Sec. 4.4.3**, all participants reported having at least some of their passwords memorized: however, all but one said that they used some kind of memory aid to help them remember their passwords. A number of them wrote their passwords down, either digitally (e.g., in an encrypted file on the computer) or by hand. These memory aids helped participants avoid the immense cognitive pressure of memorizing all their passwords or, alternatively, the impact of having to reset forgotten passwords. Some memory aids, such as password managers/vaults, not only made it easier to remember authentication information but made it easier to enter as well.

The diary and interview data provided a rich picture of how participants used memory aids as well as other mechanisms and strategies to cope with authentication. These included:

- Planning and time management
- Removing the need to re-enter authentication elements
- Employing a schema for generating passwords
- Creating memorable passwords
- Creating passwords that are easy to type
- Synchronizing passwords across multiple applications
- Proactively renewing passwords
- Using written memory aids
- Using cached or stored passwords
- Employing non-password authentication mechanisms
- Using password managers/vaults

Each of these mechanisms is described in detail in the following subsections.

6.4.1.1 Planning and time management

One strategy many participants used to cope with authentication was planning ahead. For example, one participant said that if he/she expected to receive an urgent request while working at home, he/she would sign on remotely to the NIST network well in advance.

This way he/she could go through the complex, time-consuming process of authenticating to the NIST VPN and download and install any required security software updates (a process that could take up to half an hour) at his/her leisure, rather than when he/she was under pressure to perform an urgent primary task.

On a similar note, a number of participants reported that they batched primary tasks so that they could keep to a minimum the number of times that they authenticated to a particular application. If a participant had more than one activity to perform using a given application during the day, he/she would block out time to perform all those activities at once. This batching of activities did not correspond to the natural flow of participants' work, but it allowed them to authenticate to the application they needed only once instead of doing so multiple times during the day.

This coping strategy is, essentially, changing one's work habits because of authentication. One of the problems with doing so is that it overlaps with one of the symptoms of password fatigue: trading off productivity for security [13]. As one participant described, batching primary tasks can sometimes amount to postponing them:

> *"Things get put off until when it's, 'OK, I have a block of time. It's worth it for me to get the token, to log in and to sit there and do like an hour's worth of work or half an hour or something like that.' […] But if it's for like fleeting little, 'Oh, I have this great idea' or 'I want to send this e-mail' or something, then I'm more likely to put it off until I have that sort of block of time where a log-in is worth it. […] especially if it's something that wasn't actually due. It's after hours. You've already put in your nine hours or however many hours you're doing and then you think of something of home, it definitely is less likely that you're going to get online to actually do that thing that you're thinking of. You're just going to wait until the next day." (P11)*

6.4.1.2 Removing the need to re-enter authentication elements

Study participants reported avoiding entering authentication elements in two key situations: time-outs on systems or networks, and when they perceived authenticating as more of a "hassle" than it was worth for the task they needed to do.

One common reason for having to re-authenticate was because the desktop or laptop computer the person was using had locked after 15 minutes of inactivity (as described in **Sec. 2.7**). Participants addressed this inconvenience by doing something to prevent the computer from timing out, such as jiggling the mouse, or carrying their laptop with them – although as the participant quoted at the end of **Sec. 6.2.1** pointed out, this solution was far from ideal and did little to reduce the friction and disruption caused by timed lockouts. One participant also mentioned (in jest) that software that makes the computer think the mouse is moving often enough to prevent the screen from locking or a

"drinking bird" could be employed to periodically tap a key on the computer and prevent timeouts. Another participant said that despite the appeal of "cheating" the lockout, he/she did not plan to do so:

> *"Well you have two choices. Either you can beat the system – I mean there are little devices that you can buy that you plug into USB that imitates the mouse being moved every so often, right? […] And they're very cheap. They're like five dollars or something. But I prefer not to try and beat the system, although that's tempting." (P23)*

In certain situations, participants elected to perform long tasks without the computer because doing so was more efficient than logging in, being locked out, having to log in again, and so on. In most cases, this involved working with pen and paper rather than digitally. For example, some participants reported printing documents rather than viewing digital copies on their laptop. Others said they would rather scribble things quickly on paper rather than open their machine, authenticate, and take notes digitally, or, if off campus, log into a computer, log into a virtual private network (VPN), log into the NIST network, and then log into e-mail to send a quick thought or idea.

6.4.1.3 Employing a schema for generating passwords

Because passwords must be remembered and entered, password construction often has an impact on subsequent use. For this reason, many participants used systems or schemas for generating passwords. Schemas are more of a general coping strategy than a specific one: they could be used to help facilitate password memorability, entry, management, or some combination of all three. Some specific examples of these schemas are described in **Sec. 6.4.1.4** and **Sec. 6.4.1.5**.

6.4.1.4 Creating memorable passwords

Many of the participants' reported systems for creating memorable passwords involved "chunking" them into segments. Some participants used predetermined sets of segments in a modular fashion: when updating a password, they would simply take the segments within it and reorder them. Others would take a single set of three or four characters and repeat them until they reached the required password character length.

In a number of cases, participants had a fixed segment or root that remained the same in all their passwords, ensuring that there would always be an element of the passwords that they could remember. When they needed to renew a password, participants would keep this fixed segment while changing a different part of the password, such as a prefix, suffix, and/or a single character they could increment (e.g., from "a" to "b" or from "1" to "2"). The fact that so many participants used these types of password creation strategies

is not surprising: some previous usability studies indicate that such techniques are very common [21].

Two participants described a somewhat less common strategy of using a cryptic password hint (when an application permitted it) that was effectively an "abbreviated" form of their segmented password. For example, one participant used the hint *D! #*, where "*D*" was his/her date of birth, while "*!*" and "*#*" each represented a specific password segment he/she had memorized.

These kinds of strategies do not always protect users from forgetting their passwords, in large part because they simply have so many passwords to manage. One participant admitted to having this problem:

> *"Yeah, I used to add an abbreviation to the end for each different system, but once in a while I'd forget how I'd abbreviated it." (P14)*

6.4.1.5 Creating passwords that are easy to type

Two participants reported that they used methods for creating passwords that were easy to type. Two others mentioned creating passwords based on keyboard typing patterns, moving one key in a specific direction whenever they had to renew their passwords (e.g., "a" to "s"). However, as one participant noted, this practice is often prevented by systems that perform assessments on password strength before they can be accepted and used.

Also, this method only works on conventional PC and laptop computers. It is not easy to use on mobile devices with touchscreens or small keyboards. However, some participants take this into consideration as well: one said that he/she chose a password that did not require the Shift key so that it would be easier to enter on his/her iPad.

6.4.1.6 Synchronizing passwords across multiple applications

During new hire orientation, NIST staff are given best practices training that explicitly encourages using different passwords for every application. However, several participants mentioned reusing the same passwords across multiple applications. At least one participant specifically reported that he/she used one strong password for of all the applications on which it would work. Many participants actually used different classes of passwords based on the sensitivity of the data or application protected by the password. For example, two participants reported using the strongest passwords for their online banking, and weaker passwords for commenting on blogs. This is consistent with the findings of a large-scale study of password habits conducted by Microsoft researchers Dinei Florencio and Cormac Herley [9].

Participants who used this strategy said that they often struggled with creating passwords that would comply with the different password policies (regarding length, composition, special characters, etc.) of multiple applications. Some found it very frustrating when they created what they considered a good, strong, memorable password, only to have it rejected when they tried to use it on certain applications.

One participant circumvented this by creating a "universal" password that worked for the application with the strictest password policy, then using that password on other applications with less stringent requirements. This kind of "over-fulfilling" of password requirements is common [10][21]. While it may work well most of the time within enterprises or large organizations, it may not transfer to personal online accounts (e.g., because the password character minimum for an organization is greater than the password character *maximum* for one's social networking account).

Another obstacle to keeping one's passwords synchronized is that the passwords for different applications may expire at different intervals – this was certainly the case for many NIST applications. To address this issue, many participants who synchronized passwords to some degree also used the complementary strategy of updating all their passwords on a schedule, as described in the next section.

6.4.1.7 Proactively renewing passwords

The applications used by the study participants had different password expiry intervals: some expired in less time or more time than others. For example, one application might have a "password lifetime" of 90 days, while another had a lifetime of only 30 days. To save time and effort in managing passwords, participants said they proactively updated as many passwords as possible when they received a notification that one was about to expire. In other words, many participants who had a 30-day password and a 90-day password would update both every 30 days. This was especially important for participants who tried to synchronize passwords across multiple applications.

Based on comments from participants in follow-up interviews, it seemed that the practice of updating all of one's passwords on the schedule of the one with the shortest lifetime was fairly widespread. One participant said that having to reset multiple passwords on different schedules was one reason that he/she badly wanted SSO (while acknowledging that others might not feel the same way):

> *"If you forget that one password, you're hosed, and maybe not everybody would like that, I mean because you would have to have such strict security requirements on that one password that maybe it wouldn't be worth it for everybody. But I guarantee for me I would sit down and practice that thing and practice that thing and practice that thing until it's automatized and I wouldn't forget it and I would*

be totally happy to enter a 20-digit password if I could use the same one and not have to go through this hullabaloo of calling and resetting." (P11)

A disadvantage to this strategy is that a user might have so many passwords that resetting all of them at once could be a monumental task. One of our participants noted that synchronizing all her passwords could take him/her half an hour at best: at worst it could take him/her an entire day.

6.4.1.8 Using written memory aids

Participants reported using a variety of memory aids, most of which are listed in **Sec. 4.4.3**. Many participants (16 in all, or 69.57%) reported writing passwords down or recording them in some other way: 11 (47.83%) of them said they used paper notes, and 6 (26.06%) said they wrote their passwords down in digital files such as Word or Notepad documents, while one participant used both aids; the use of written memory aids was also documented by Choong, *et al*, in [5]. It should be noted that NIST's security policy does not prohibit writing passwords down: simply that passwords in general be safeguarded, which means that writing down a password would not necessarily violate the policy.

Those participants who wrote their passwords down had different ways of doing so, and some were more systematic than others. While some participants reported saving each password in a file and encrypting it, others said they wrote down only the difficult passwords on Post-Its and carried the notes with them while they were learning and memorizing new passwords. Others said they kept an up-to-date list of their passwords in a secure location.

Though writing down passwords can reduce anxiety, it does create additional physical effort because the user has to have either the file or the piece of paper containing the passwords at hand and copy from it when entering his/her password. Digitally written passwords are somewhat less labor-intensive, since a user can simply copy and paste those passwords as needed – although as with handwritten passwords, the user may have to spend some time and effort locating the password they need first. Also, if something happens to the machine on which the digital password file is saved (e.g., hard drive failure) and the user does not have a backup or printout of that file, all the user's passwords will be lost. This creates a serious authentication problem, as one of the study participants learned from his/her own experience:

"I ended up having to change a password that day because I got locked out of an account. The reason that happened was because I had switched computers, where before, I was relying on the browser for my password. So I went to the new laptop, I didn't remember it, and I had no way of getting the password other than resetting it. The other computer was gone." (P10)

6.4.1.9 Using cached or stored passwords

Many Web browsers (e.g., Firefox, Internet Explorer) will offer to save a user's login information for a Web site when the user creates an account or enters the password for the first time. Browsers that cache login information will not only store it, but when the user visits a Web site for which the browser has stored login information, they can enter it with one click, which takes much less time and effort than entering the information manually. Macs have a "Keychain" password management utility that works in much the same way, except not just in a single Web browser but also for all browsers and applications on a machine. Slightly more than half of the study participants (12, or 52.17%) reported using cached passwords.[15]

There is, however, a significant disadvantage to browser-cached passwords: like the digitally written passwords described in **Sec. 6.4.1.9**, they will be lost if the device on which they reside is lost and the user has made no backup. This is actually a more serious issue for browser-cached passwords, because while most users have the technical knowledge necessary to transfer an encrypted Word document containing their passwords off of a computer (e.g., by putting it on a thumb drive), the same is not true for passwords cached in a browser.

6.4.1.10 Employing non-password authentication mechanisms

Some participants also used authentication methods that reduced the need to use passwords. Four participants used a biometric fingerprint reader to authenticate in 16 events (total). While one participant used his/her PIV card two times to authenticate to a NIST computer during the study period.

While not the participant who reported using a PIV card where a username-password could have been employed, one participant, P19, gave some insights into an appeal of PIV card use, but also why he/she was not using it to log into computer systems. *"I just put it in, put in the PIN, and that's it."* This participant went on to explain how the PIN composition requirements are easier than that of passwords, *"A PIN number is four to six numbers, and that's pretty easy for me to remember. It's different than 20 characters, 15 characters, of random stuff."* However, Participant 19 further explained why he/she does not use the PIV card to log into computer systems at NIST, *"I actually don't use my PIV card here at work because I forget it in the computer a lot. If I leave the building, I can't get back in because that's also my access back into the building."*

---

[15] Others may also have stored passwords in their browsers but did not report this technique because it automated the authentication process enough that they were not aware of when it was happening.

When using a fingerprint reader, in theory an individual could authenticate simply by placing his/her finger on the reader, without having to enter a password (at least for applications that supported this kind of authentication). In practice, fingerprint readers were not that reliable, as one participant pointed out:

> *"This [authentication method] is worse, because it works by a biometric, and my finger doesn't read very well. I have to smear it with moisturizer, and then I forget what the actual password is. When it really just won't read my finger, I can't unlock it and I can't remember." (P2)*

For this participant, one authentication failure – the fingerprint reader producing a false negative – led to another one: forgetting the password he/she could otherwise use as a backup, because he/she did not practice it enough to remember it.

Another participant explained that in NIST's implementation, the fingerprint reader and PIV card mechanisms are authentication system front-ends to an underlying password system. This means that while using the reader or the PIV card eliminates the daily exercise of recalling and entering complex passwords, it does not eliminate the need for password management. The participant said he/she still had to change his/her general NIST domain password every three months when it expired, which involved looking up the old domain password he/she never used just for the purpose of resetting it.

6.4.1.11 Using password management tools

A password manager or vault is a piece of software or hardware installed on a computing device, which can be a desktop computer, notebook computer, tablet, or smartphone. They store passwords[16] – in encrypted form, protected by a single "master" password – and can fill them in as appropriate when the user opens an application or visits a Web page that requires authentication information. Password management tools have multiple advantages: they take pressure off users' memory; remove the physical effort of entering authentication information (except for the master password); and prevent mistakes when recalling or entering a password. In certain circumstances, they can also automate some aspects of password management: if a user changes his/her password for a particular website, the management tool will offer to update the appropriate password in storage.

Five (21.74%) study participants reported using some kind of password management tool. Although there are a variety of password management tools on the market, the participants reported that they used the following three products:

---

[16] Some password management tools can also store other information, such as the answers to security questions, bank account and credit card numbers, identity information, and encrypted notes.

- IronKey is an encrypted USB stick with an option for a password vault.
- KeePass is a free, open-source password management tool. It can be downloaded from the Internet.
- LastPass is a free online application (a premium version is available with a paid subscription). It can be downloaded from the Internet.

One participant described how his/her password manager worked, and mentioned some of its advantages:

> *"It sits up here, as a browser extension for Mozilla or Chrome. I click this. Currently, I'm logged in. I had to log in for my master password this morning. It will automatically fill the form fields. But it stores things encrypted. I have it on my phone as well. It's very accessible." (P3)*

No password management tool worked for all the accounts and devices users had, but participants reported that use of these tools made many of their authentication tasks easier and less time consuming.

The research team developed two simulations to illustrate one of the anticipated advantages – time – of using a password manager to enter a user ID and password, rather than entering that authentication information manually. These simulations were informed by measuring the time required for a skilled user to log into a web application through a browser by entering authentication information *manually* and the time to perform the same task using the LastPass password manager, which *automatically* fills in the username and password on a Web page. The underlying modeling techniques used for the time measurements were: Goals, Operators, Methods, and Selection rules (GOMS) and its daughter technique, Keystroke-Level Modeling (KLM), referred to as GOMS-KLM.

The modeling technique GOMS-KLM reduces the interaction between a human and a computer to basic physical and cognitive actions such as pointing with the mouse, clicking, pressing keys, and mental preparation. GOMS-KLM provides numerical predictions for user performance of a set task and also estimates the amount of time a skilled user would require to accomplish that task. The task chosen was logging into a Web-based e-mail application with authentication requirements similar to that of logging into the NIST e-mail application through a Web browser. Two models, both employing GOMS-KLM, were developed to assess the time requirements for a skilled user to complete the selected task in two modes: 1) without using the LastPass and 2) to complete the task while using LastPass, which presumed that the preliminary task of logging into LastPass had already been completed (time estimate provided). The first model was built by a member of the research team, who manually specified each step of

the task according to the GOMS-KLM technique. A lengthy example is provided in Table 17, **Appendix D** The second model employed CogTool, which also uses GOMS-KLM, but may be more accurate than the manually generated GOMS-KLM estimates, as it removes the need for the researcher to be trained in the theory and use of KLM [11]. An example of a CogTool script used in this simulation is shown in **Fig. 17**, **Appendix D**.

Table 15 shows the simulation results from the two models described above for the login task in both modes (with and without LastPass), as well as an estimate of the time needed to log into LastPass initially. The results of the GOMS-KLM analyses using both the manual method and CogTool, show that using a password management tool is likely to substantially reduce the time needed for a similar authentication task. These models predict that entering the authentication information manually will take approximately 14 seconds (14.8 seconds using the researcher-developed model and 13.2 seconds using the CogTool-developed model), while using the password manager took roughly 5 seconds (5.7 seconds using the researcher-developed model and 4.6 seconds using the CogTool developed model) – meaning that the use of the password manager reduced the task time by approximately 9 seconds.

Table 15: Task completion estimates for the login task using manual authentication information entry and a password manager

Task	Model type	
	Researcher-developed model using GOMS-KLM: estimate (seconds)	**Model developed using CogTool: estimate (seconds)**
Logging into web e-mail by manually entering information (No LastPass)	14.8	13.2
Logging into web e-mail with LastPass password manager	5.7	4.6
Logging into LastPass password manager (initial login)	10.4	10.1

Note that using the password manager requires an initial login. The predicted task completion times for the initial login to LastPass are also given, just over 10 seconds. However, a user can perform this initial login shortly after starting their system, after which the password manager will remain open until the user logs out – and the user will

more than make up their investment of time in the initial password manager authentication with two or more authentications similar to the one modeled.

6.4.2 What participants' coping mechanisms imply about their view of authentication and security

As the preceding descriptions of coping mechanisms illustrate, participants clearly spent considerable time and effort trying to balance meeting security requirements with minimizing the impact of authentication on their primary tasks. Coping mechanisms were employed to make the secondary tasks of authentication as automatic and effortless as possible. But at least some of these coping mechanisms – such as using the same password across multiple applications, storing authentication information in Web browsers, and using schemas for creating passwords – suggest that participants were focused largely on following the rules to the letter without considering the security rationale behind them.

This is not to say that participants did not value organizational security: on the contrary, they did. In principle, participants accepted that authentication was an important part of protecting the assets and reputation of NIST. But in practice, participants looked for ways to reduce the impact of compliance to more manageable levels.

6.5 TRADING OFF PRODUCTIVITY FOR SECURITY

Even security-conscious users with an array of coping mechanisms can find authentication tasks too effortful. They still have limited compliance budgets (see **Sec. 2.5**), which can be exhausted by performing dozens of small authentication tasks over the course of a day. More subtly, prior bad experiences with authentication can condition users to approach future authentication tasks – particularly those that are time-consuming, complex, or otherwise difficult – with additional emotional loading. This emotional load increases the perceived time-and-effort costs of authentication (see **Sec. 6.1)**.

Either circumstance (or both) can cause users to trade security for productivity or vice-versa. The study participants felt too invested in NIST's organizational security (see **Sec. 2.7**) to deliberately do anything that would compromise it, so they traded off productivity instead. In essence, if engaging in a certain activity required going through a difficult authentication process, the participants would either engage in that activity less or just give it up completely.

For example, some participants stopped using certain devices because the effort of going through the authentication steps necessary to use them was not worth the trouble. Two participants reported giving up use of NIST laptops because of the authentication mechanism associated with the platform's disk encryption. One participant gave up using a portable cellular device because of the authentication effort. Others have not given up

entirely on using such devices, but do not use them as much as they might otherwise (for example, in between meetings).

The impact of authentication caused some participants to limit not only the devices they worked on, but from where they worked. One participant complained that "*authentication policies work against telecommuting, off-site computing and connecting*" (P21). This sentiment seems to have been shared by other participants. One stated that he/she worked from home less because of the three-step authentication process required to connect remotely to the NIST network – a process that involves entering a frequently-changing numeric code from an RSA token (see **Sec. 2.7**). Two other participants reported that they avoid traveling for the same reason. Others mentioned that when off-campus, they check their e-mails less frequently than they would otherwise because the effort and interruption of going through the necessary authentication is just not worthwhile.

Finally, authentication requirements hinder collaboration between employees at NIST and members of other organizations. One participant stressed that he/she no longer seeks to do software development work with people from other institutions because security restrictions make transferring software across organizational boundaries prohibitively difficult.

In each of the examples mentioned above, participants stated that their actions had ripple effects on their productivity, the productivity of their colleagues, and the organization overall. The participants were aware that by changing their habits to avoid dealing with authentication, they had lost out on potentially valuable opportunities. However, they felt that the time and effort required to pursue these opportunities – to overcome the friction of authentication – was not worth the potential rewards.

6.6 INSIGHTS REGARDING AUTHENTICATION, FRICTION, AND DISRUPTION

This study resulted in some valuable insights into why authentication causes friction and disruption and what factors intensify those effects. This study illustrated that 1) authentication friction and disruption are increased by authentication problems, 2) friction and disruption are increased during an authentication event as the impact increases with the addition of each authentication "cost" associated with that event, and 3) users experience friction even when there are no problems. Additionally, the study findings indicate that authentication may have more subtle, long-term effects on users than previously thought.

6.6.1 Authentication problems create considerable friction

Authentication creates friction when it delays or obstructs a user's attempt to perform a primary task (as described in **Sec. 2.4**). The greater the time and effort required to

complete an authentication task, the greater the friction it creates. Predictably, when users experience problems that interfere with the completion of authentication tasks (e.g., having to recover lost authentication information elements) both the disruption of the primary task and the degree of friction are considerable.

Many of the study participants said that they tend to experience authentication problems with applications they use infrequently. Since these applications tend to be "out of sight, out of mind" most of the time, users can easily forget to change their passwords. As a result, when they *do* use these applications, they often find that their passwords have expired, necessitating that they spend significant time and effort reinstating their accounts. Participants frequently cited these kinds of applications as a source of irritation and stress, in large part because of the need to change their passwords more frequently than they actually *use* them. As one participant said:

> *"I've even thought about setting up a reminder on my calendar every two months to remind myself to just go in and change the passwords. I don't have to deal with the whole locking out thing. […] But even that's too much work, because if I don't travel for a year, I'll change my password six times. […] There's no purpose for it other than to avoid the five to 15 minutes next year." (P19)*

A complete list of applications and the number of authentication problems reported for each is shown in **Table 9** in **Sec. 4.4.6**.

6.6.2 Users experience friction from authentication even when there are no problems

Authentication can create friction even if the user experiences no problems with it. The study participants' self-reported levels of frustration certainly tend to indicate this: consider **Table 9** (**Sec. 4.4.6**), in which participants reported frustration with authenticating to certain applications even if they did not experience problems doing so (online banking, for example). Similarly, **Table 10** (also in **Sec. 4.4.6**) shows that some participants were frustrated by authentication even if they did not experience any authentication problems during the reporting period.

Why would users be so frustrated even over authentication tasks that go smoothly? There are a few reasons, one being that authentication is a "non-productive" task that does not result in any direct benefits for the user [5]. Also, any authentication task that requires time and effort on the part of the user creates a "wall of disruption" that impedes the performance of primary tasks. This effect is illustrated in **Fig. 16.**

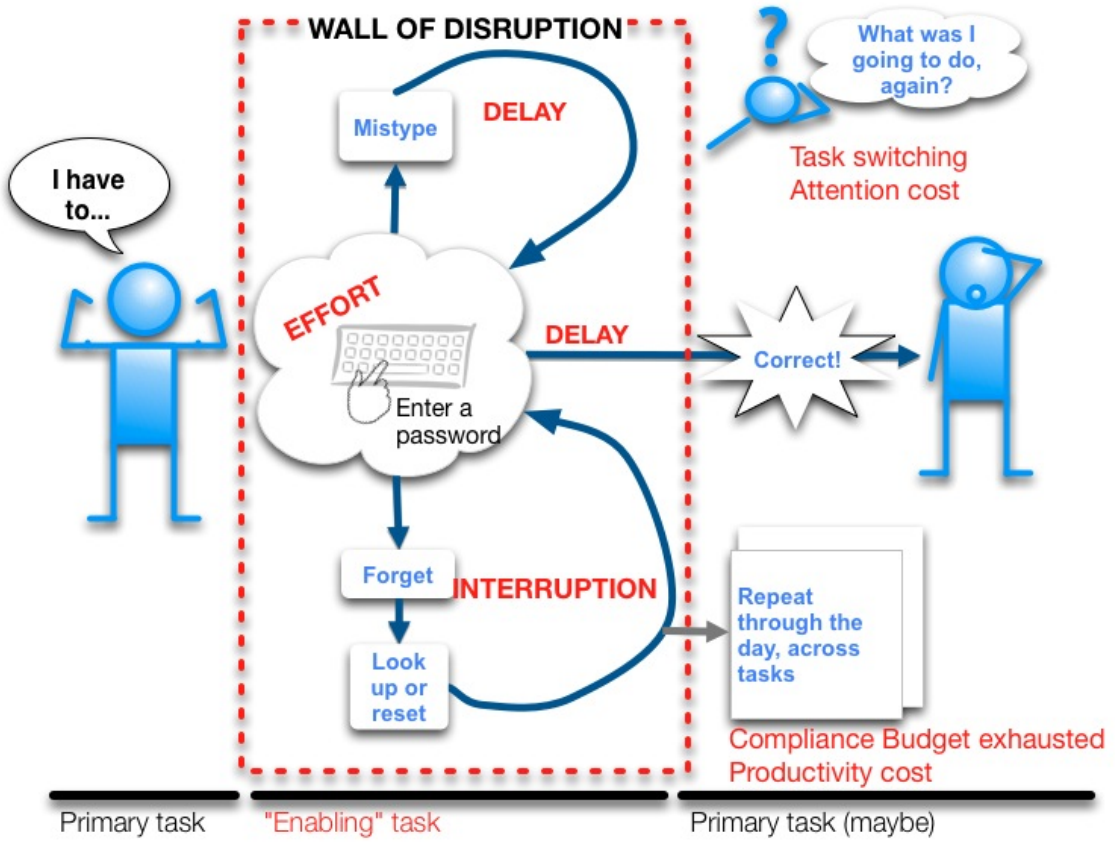


Figure 16: The wall of disruption created by the enabling task of authentication

Even a successful, problem-free authentication task is fraught with friction caused by the effort of context switching between primary tasks and authentication tasks. As noted in **Sec. 6.1**, users are painfully aware of the task-switching costs imposed upon them by authentication [17].

The higher the workload associated with a specific authentication task, the more friction and disruption it creates. Based on diary data and interview data from this study, the research team identified four essential factors that increase authentication workload (and therefore friction and disruption):

- **Difficulty accessing and/or retrieving authentication elements.** Forgetting a password and having to consult a memory aid; having difficulty finding the memory aid; losing a smartcard; having trouble reading the code on an RSA token.

- **Perceived lack of user control.** Having to follow seemingly arbitrary rules; being blocked from access to an application, resource, or system due to problems with authentication; having no control over when one authenticates (or re-authenticates), such as when the computer locks after a set period of time; being forced to create passwords that are difficult to remember and type.

- **Complexity.** Dealing with different (and conflicting) sets of password creation requirements; having passwords with different expiration timing; keeping track of which passwords are synchronized and which ones are not; having to submit a large number of elements (3 or more) to authenticate.

- **Time.** Waiting for a new password to be valid after it has been changed; spending 15 or 20 minutes getting assistance from a help desk to resolve authentication problems; re-entering a password multiple times (either because it was entered incorrectly or because of repeated prompts for authentication); making multiple attempts to recover a password; delaying work to renew a password that is about to expire.

Note that some of the example situations listed above involve more than one factor. For example, having to consult a memory aid (especially one that has been misplaced or is otherwise inconveniently located) not only involves the "Difficulty accessing and/or retrieving authentication elements" factor, but the "Time" factor as well. Time is actually a factor in all authentication tasks, because at a minimum, a user must spend some time to perform the task. All authentication tasks have some workload, and therefore a cost to the user: there is no "free" authentication.

Generally speaking, the greater the impact of any one of these factors in an authentication task (e.g., the more difficult it is to retrieve elements, the less control the user feels, the more complex the task, and the longer it takes), the more friction and frustration the user experiences. This is supported by the data displayed in **Table 9** (**Sec. 4.4.6**) and **Table 3** (**Sec. 4.4.2**): the former shows the frequency of problems and average frustration ratings for each application, and the latter shows the average number of authentication elements required to authenticate to each application. Upon comparing the two tables, the research team found that the more elements an application required for authentication, the more likely participants were to report some frustration with it, even if they experienced few or no problems. **Table 16** consolidates this information.

Table 16: Frustration and problems associated with number of authentication elements used

Authentication elements	Average frustration	Percentage of problems
1	1.58	8.20%
2	1.62	8.94%
3	2.25	6.67%
4	2.36	36.36%

This data suggest that there is a connection between labor-intensive authentication and participant frustration.

Accumulated frustration associated with a low-cost authentication task repeated many times was also high. The study participants said that performing the same small authentication task over and over was one of their major friction points (see **Sec. 6.2.1**). Both individual high-cost authentication tasks and large aggregations of low-cost tasks have the same effect in the end: friction and disruption that extends beyond the authentication task itself.

6.6.3 Friction and disruption from authentication have long-term effects

One of the most important insights that can be derived from the findings of this study is that authentication leads to an accumulation of disruption over time on any one account or application. The cost of authentication to the user goes well beyond those identified in some previous authentication diary studies [10]. The literature on task switching suggests that the negative impact of experiencing authentication as an obstacle to one primary task probably lingers through multiple subsequent primary tasks [7][16]. Consider the following example of a hypothetical NIST knowledge worker named Alice, derived from diary and interview data provided by our participants.

At the end of a two-week pay period, Alice sits down to use the NIST Time and Attendance (TA) application, where she records how many hours she spent working on her projects, performing administrative duties, and/or on leave. However, Alice has not logged in since she last renewed her password two weeks ago. Because she has not had an opportunity to "exercise" the new TA password, she does not have it memorized. She has to look it up. But because she wants to keep the password secure, she has stored it in an encrypted file. She must find the file, unlock it, and then find the right password. Alice feels annoyed because this password is not synchronized with that of other key accounts she uses – she usually tries to renew all her passwords at the same time so she can focus her attention properly and not be interrupted at different times by different systems asking for new passwords.

Part of the reason Alice is having trouble is that she cannot remember the requirements for authenticating to TA. Does this password require a number? A special character? Both? Neither? She may feel that the password rules are more stringent than is appropriate for the value of the data being protected.

Nevertheless, Alice keeps trying to authenticate to TA. She types her new password incorrectly, even though she has it right in front of her, because her fingers remember the old one or the combination of characters in the new one is difficult to type (or both). She tries to enter the password a second time, and logs on successfully.

While it is true that this scenario typically plays out in under a minute, variations of the scenario repeat throughout the day. For example, Alice may have to log in to her TA account several times before she is done because she was interrupted while recording her hours each time and the application automatically logged her out after being idle for a few minutes. Multiply the time-and-effort cost of this kind of authentication task (i.e., remembering the new password, finding the memory aid, entering the password incorrectly) by the number of mission-critical applications Alice uses, and by the number of times per day she needs to authenticate to them, and the switching costs become more evident. Alice takes longer to complete the next several tasks because she is still processing the enabling task which caused a problem.

In addition, because Alice has experienced many authentication-related problems like the one described above, she is conditioned to approach authentication anticipating possible difficulty (an issue touched on in **Sec. 6.1**). She also feels that the repeated cycle of renewing, using, and then retiring passwords never seems to end. Also, she feels guilty for being so frustrated with authentication: after all, authentication plays a key role in maintaining NIST's security, and she takes that security very seriously [14].

The result of all this is that Alice's accumulated experiences with authentication adds to the perceived costs of even the smallest authentication tasks, creating additional drains on the compliance budget and hastening the onset of physical, mental, and password fatigue [5][13]. Users' experience of fatigue affects their future perceptions of and approaches to authentication, and so forth. In effect, authentication friction and disruption create a vicious cycle.

7 RECOMMENDATIONS

As was illustrated in the preceding sections of this document, authentication entails significant costs for the study participants in terms of time and effort. Their authentication workload is high – because they have so many different authentication elements to use and manage – that they often resort to coping mechanisms to keep that workload at a manageable level. Even with these coping mechanisms, authentication creates disruption that has an impact on participants' work – not just on the primary task immediately disrupted by authentication, but on future tasks as well. For some participants, the friction and disruption from authentication prompted them to avoid certain elective activities requiring authentication, which resulted in lost productivity.

The study participants are hardly unique. Their situation is extremely common for countless other organizations and users, and has been for some time: Anne Adams and Martina Angela Sasse observed as early as 1999 that users were severely overburdened by their authentication workloads [1]. Over-authentication is already a crisis [9]. What can be done to address it? Where to start?

This section presents recommendations on how to tackle the problem of over-authentication, including changes in how specialists should think about and implement security; concrete steps that organizations, decision makers, security specialists, and even users can take to reduce the impact of authentication; and suggestions for future work in the field of usability.

7.1 RETHINKING ASSUMPTIONS ABOUT AUTHENTICATION

The findings from this study illustrate how often knowledge workers authenticate during a typical day, that the impact from those events can linger beyond the enabling task of authentication, and that coping mechanisms are employed to reduce that impact. These findings suggest that it is necessary for security professions to acknowledge and respect the limits of users. When users' cognitive limits are reached; they resort to variety of memory aids, some of which may have unintended security implications.

7.1.1 Users struggle with authentication because they are only human

Security specialists may be under the impression that users fail to practice good security behaviors because they are completely unaware of the consequences of their actions, or because they do not care about organizational security. This is not typically the case. Most users are aware, in principle, that they have a responsibility to help maintain organizational security. They also understand that part of that responsibility involves fulfilling authentication requirements. The authentication diary study participants were certainly aware of this, and took the importance of organizational security very seriously.

However, on a practical, day-to-day basis, users' principal objective is to accomplish their primary tasks. Authentication makes that more difficult than it would otherwise be, because it disrupts users' workflow (especially if it is complex, time-consuming, and/or prone to problems). The time-and-effort costs of authentication and the disruption it causes – which are both compounded by the number, type, and success or failure of authentication events – accumulate across tasks and applications over time.

Therefore, users lose sight of the value of security measures as their attention naturally gravitates to the immediate task of meeting authentication requirements as quickly and efficiently as possible (which is the reason for coping mechanisms). When users encounter authentication, they tend to see it as a hassle first and a necessity second. This is not because users are stupid, malicious, or lazy; they are simply having an instinctive human reaction to being interrupted and detoured on the way to accomplishing their goals [17].

7.1.2 More authentication is not necessarily better

Some of the study participants admitted that certain authentication coping mechanisms they used – such as writing passwords down, or using the same password for multiple accounts – had the potential to compromise organizational security. But without these coping mechanisms, it is difficult to use and manage many passwords. What choice did they have?

In security design, making the user authenticate for everything is often the path of least resistance. But taking that path adds significantly, and possibly unnecessarily, to a user's authentication burden.

7.2 MAKING PASSWORD-BASED AUTHENTICATION MORE USABLE

Making authentication more usable is, ultimately, a long-term prospect. It will require not only a major shift in perspective, but extensive research and development efforts: we suggest some possible directions for both in **Sec. 7.3**. Fortunately there are steps that organizations can take in the relatively short term to reduce their users' authentication burden.

7.2.1 Listen to and work with users

Making users more aware of and educated about the importance of organizational security and authentication's role in it can help increase users' compliance budgets [5]. Users will be more tolerant of authentication and other security policies and measures if they feel they understand the rationale behind them. The participants in this study were probably more accepting of authentication than they otherwise would have been because NIST makes it a point to foster a culture of security awareness, in no small part through

relevant education and training. However, such measures will not give users an inexhaustible compliance budget [5]. Even the most patient and security-positive users have limits.

For users juggling many authentication elements, resorting to coping mechanisms – such as writing passwords down, reusing them, caching them in browsers, or employing management tools – is a rational way to reduce the impacts of authentication on their primary tasks. But from the point of view of organizational IT and security personnel, these coping strategies can shift user behavior into unintended territory. In this reactive posture, IT ends up lagging somewhat behind user workarounds that have not been assessed for risk or compliance, a situation that may create security vulnerabilities of which users are unaware.

Organizational IT and security personnel need to support their users in this area. This means engaging users in discussions about authentication, encouraging them to share their friction points and coping mechanisms – and then following up with constructive action. Soliciting feedback from users and addressing their problems should be part of the organization's iterative security process. Robust organizational security depends upon the willing and active cooperation of users.

7.2.2 Implement SSO

Many of the study participants expressed a desire for NIST to implement organization-wide SSO. They said they would accept a password that is longer and more complex than any they are currently required to use, so long as it was the *only* one they had to use. Indeed, government employees in a much larger study regarding attitudes towards passwords expressed a preference for SSO [5].

SSO would solve many of the pressing usability problems described by our participants, such as having to manage multiple complex passwords with different composition rules and expiration schedules. While SSO may be difficult and expensive to implement for an organization, it may be a worthwhile investment, since it would significantly cut down on authentication-related friction and disruption and their subsequent costs.

7.2.3 Consolidate and standardize authentication as much as possible

If it is not feasible for an organization to implement actual SSO, the best alternative is to meet users halfway and implement a uniform password policy. Even if the policy chosen for universal application is the one with the most stringent content rules and the shortest expiration time, it will still help users by reducing the confusion and inconsistency that makes it more difficult for them to cope with their authentication workloads. If an overhaul of existing password policies is considered to be too difficult and disruptive, the

organization should at least dictate that all *future* applications and systems that use password-based authentication should have the same policy.

The lack of a uniform, consistent password policy made it that much harder for participants to create and manage the multiple passwords they used, especially if they employed the coping strategy of synchronizing passwords across multiple accounts. The fact that different passwords also expired at different times was also a source of confusion, and even those who tried to update all their passwords on the schedule of the one with the shortest expiry time found it difficult to keep up. NIST's system owners may not have intended to cause this situation, but it is the natural consequence of an environment where password policies for many applications were created in isolation from each other and may have been inherited from legacy systems.

7.2.4 Encourage and support the use of password managers or vaults

Finally, it is recommended that organizations actively support a user coping mechanism that, when practiced correctly, significantly reduces authentication burden while maintaining security: password management tools. (Individual users are also recommended to look into password managers or vaults for their personal use.) As described earlier, participants described password management tools as considerably simplifying password entry, which is especially useful for users who need to authenticate multiple times during the course of a day.

7.3 FUTURE DIRECTIONS

Although there are a number of different authentication mechanisms that employ a variety of different authentication elements (including PIV cards, RSA tokens, and biometrics), password-based mechanisms are by far the most common. They were the first authentication mechanism to be used on computers, starting with timesharing systems in the 1960s [15]. Users of these systems were required to enter a password once: to log on to the computer. This required a trivial amount of time and effort and did not overly disrupt any particular primary task. The relative few individuals who used computing resources needed only one simple password, which typically only had to be changed if there was good reason to believe it had been compromised.

Computing technology and the way we use it has changed radically since then. But we are still using passwords as our default method of authentication in essentially the same way: one password per technological asset. This was effective and appropriate in the days when a user would interact with, at most, a handful of password-protected assets on a daily basis. But now that most users interact with *dozens* of such assets – devices, applications, Web pages, networks, etc. – protecting each one with a password is no longer practical. There are simply more than most users can remember, especially with

the added complication of policies that require passwords to be longer, more complex, and subject to frequent expiration.

7.3.1 Take a broader perspective

Mary Theofanos and Ellen Cram Kowalczyk observed at a recent NIST Information Security and Privacy Advisory Board (ISPAB) meeting, that we have evolved from thinking "the user is the problem" to "technology is the solution", to the realization that "the user must be part of the solution" [24]. However this holistic approach requires us to fully understand the user and embrace the considerable social science knowledge relevant to usability and computer systems. Taking a broader perspective, allows us to build usability into our security products and processes, that span the life of a system from conception through design, implementation, and evolution. Good usability, like good security takes into account the changing nature of the threat environment, changing business goals, and differences in user needs, skills, attitudes, and experience. In addition, usable security should be tailored to organizational priorities and needs.

Authentication throughout an organization should be driven by an overall authentication strategy or approach that is driven by organizational security priorities and user needs and provides a vision for future growth. It appears in many cases that as systems are deployed that there is no overall strategy that governs the authentication mechanism offered and how it complements or prepares for the future.

7.3.2 Establish best practices for implementing usable authentication

Essentially, usability best practices must give IT and security professionals a roadmap for understanding the context of use for whatever asset they are working with and assessing how they can implement authentication in a way that fits that context. For example, does securing a transaction require making the *user* authenticate, or would it be more effective to authenticate the *transaction* itself? Is it possible to secure a system through implicit authentication, where the system satisfies itself that this is the authorized user [2]?

Sections 5 and **6** described some methodological tools (experience graphs and prototyping with CogTool) for measuring the effect of authentication on users, as well as recommendations for improving the usability of password-based authentication; these could be considered as a basis for best practices. But that is not nearly enough. Security and IT professionals need best practices that help them apply some basic principles of social science and design. Best practices should also guide the effective development and use of the modular authentication solutions we described in the previous section.

7.3.3 Conduct further research on habits and effects related to authentication

Technologies, techniques, and best practices in any field need to have a basis in empirical data. Usability is no different. However, at this time there is only a small body of usability research from which to draw for this domain.

This study makes strong methodological contributions in identifying and measuring the impact of explicit authentication on users. The experience journey maps discussed in **Sec. 5** (and shown for each participant in **Appendix B**) and their underlying measures can potentially be used by organizations to track and manage the effects of authentication on their customers or users. The experience journey maps, along with analyses that can be achieved through prototyping tools like CogTool, could be useful to IT and security professionals as they make security decisions that take user effort into account.

The research team would like to see these techniques applied by other researchers in other settings, in order to confirm their utility and validity. In addition, we welcome suggestions for any refinements that may make these tools more effective. Finally, we are interested in seeing whether these findings and insights regarding users' authentication-related perceptions and behaviors hold true elsewhere.

There is also a need for additional tools that reflect the factors involved in users' compliance budgets and the properties of disruption from authentication. Research that employs these kinds of tools will help security designers to think beyond current models and take into account the downstream effects of security burden for users, teams, and organizations.

Even without analytical tools such as the user experience journey maps and CogTool task analysis, the authors believe that usability researchers and organizations can gain valuable insights by conducting diary studies and follow-up interviews similar to those employed by this study. At a minimum, such studies are useful for collecting feedback and identifying the most widespread and persistent authentication issues within an organization. Studies with a larger number of participants than this one, would potentially reach a broader audience within an organization for an even broader perspective of the issues surrounding authentication.

Longer-term diary studies, spanning the course of a week or more, may also be valuable. However, the data collection methods would have to be changed slightly in order to make this feasible for study participants. Expecting participants to record every single instance of authentication over a long-term period would add significantly to their authentication burden, which is the exact opposite of what we want to accomplish, and they would probably find journaling activities difficult to sustain for more than one day. One plausible variation would be to have participants record significant authentication related events (including problems) at the end of the day, while their actual authentications

would be counted through some automated means. The data from a series of periodic interviews would be invaluable, although the number of interviews should be related to the length of the study period.

8 CONCLUSION

This study provided a very clear picture of the average government knowledge worker's authentication workload at NIST during the course of a typical day. While participants were using technology, any kind of technology at all, the impact of authentication was present. The study participants spent a considerable amount of time and effort on authentication each day. Participants tried very hard to cope with this workload in ways that they thought would preserve organizational security. It is important to note that they dealt with authentication not only at work, but also in their personal lives, on their computers and devices outside of the work environment. Organizations may not consider it incumbent to count users' personal authentication workload since they cannot control it. But it *is* an important factor that cannot be ignored, as people cannot divide their cognitive effort: they need to be able to accommodate some personal authentication events as well as work events.

We found that:

- Authentication problems create considerable friction
- Users experience authentication friction even when there are no problems
- Friction and disruption from authentication have long-term effects

These findings lead us to a set of recommendations, described in **Sec.** 7. Most importantly, the underlying assumptions about authentication must be revisited, as the human limitations of users must be respected. For NIST in particular, further implementation of SSO and incorporation of an accepted password vault or manager would help reduce the friction of authentication for NIST knowledge workers. Moreover, we believe that the findings from this study generalize to the average government knowledge worker, as the password authentication workload found here is consistent with the findings from a much larger, Department of Commerce-wide study on password related behaviors [5].

9 REFERENCES

[1] Adams, A., & Sasse, A. M. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 41-46.

[2] Almuairfi, S., Veeraraghavan, P. and Chilamkurti, N. (2011). *IPAS: Implicit Password Authentication System*. In *IEEE workshops of international conference on advanced information networking and applications* (pp. 430-435). doi: 10.1109/WAINA.2011.36

[3] Baumeister, R. F. (2003). The psychology of irrationality. In I. Brocas & J. Carrillo (Eds.), *The Psychology of Economic Decisions: Rationality and well-being* (pp. 1-15). New York, NY: Oxford University Press.

[4] Card, S. K., Thomas, T. P., & Newall, A. (1983). *The psychology of human-computer interaction*. London, UK: Lawrence Erlbaum Associates.

[5] Choong, Y., Theofanos, M., & Liu, H. (2013). *A Large-Scale Survey of Employee's Password Behaviors.* Manuscript submitted for publication.

[6] Beautement, A., Sasse, M. A., & Wonham, M. (2010). *The compliance budget: Managing security behaviour in organisations*. In *Proceedings of the 2008 workshop on New security paradigms* (pp. 47-58). doi: 0.1145/1595676.1595684

[7] Czerwinski, M., Horvitz, E., & Qilhite, S. (2004). *A diary study of task switching and interruptions*. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 175-182). doi: 10.1145/985692.985715

[8] Fitts, P. M. (1954). The information capacity of the human motor system in controlling the amplitude of movement. *Journal of experimental psychology*, *47*(6), 381.

[9] Florencio, D., & Herley, C. (2007). *A large-scale study of web password habits*. In *Proceedings of the 16th international conference on World Wide Web* (pp. 657-666). doi: 10.1145/1242572.1242661

[10] Inglesant, P. G., & Sasse, M. A. (2010). *The true cost of unusable password policies: Password use in the wild*. In P*roceedings of the 28th international conference on Human factors in computing systems*. doi: 10.1145/1753326.1753384

[11] John, B. E., Prevas, K., Salvucci, D. D., Koedinger, K. (2004) Predictive human performance modeling made easy. Proceedings of CHI 2004 (Vienna, Austria, April 2004) ACM New York. 455-462.

[12] Kieras, D. (1993). *Using the keystroke-level model to estimate execution times*. Informally published manuscript, University of Michigan, Ann Arbor, Michigan. Retrieved from http://www.pitt.edu/~cmlewis/KSM.pdf

[13] Maxwell, K. (2008). Password fatigue. In *BuzzWord by MacMillan Dictionary*. New York, NY: Macmillan Publishers Limited. Retrieved from http://www.macmillandictionary.com/buzzword/entries/password-fatigue.html

[14] McDermott, R. (2012). Emotion and security. *Communications of the ACM, 55*(2), 35-37. doi: 10.1145/2076450.2076462

[15] The M.I.T. Computation Center (1965). *The compatible time-sharing system: A programmer's guide*. (2nd ed.). Boston, MA: MIT Press.

[16] Monsell, S. (2003). Task switching. *Trends in Cognitive Sciences, 7*(3), 134-140. Retrieved from matt.colorado.edu/teaching/highcog/fall8/m3.pdf

[17] Nass, C., & Yen, C. (2010). *The man who lied to his laptop: What machines teach us about human relationships*. New York, NY: Penguin Publishing.

[18] Parkin, S., van Moorsel, A., Inglesant, P., & Sasse, M. A. (2010). *A stealth approach to usable security: helping it security managers to identify workable security solutions*. In *Proceedings of the 2010 workshop on New security paradigms* (pp. 33-50). doi: 10.1145/1900546.1900553

[19] Reason, J. (2008). *The human contribution: Unsafe acts, accidents and heroic recoveries*. Surrey, UK: Ashgate Publishing, Ltd.

[20] Sasse, M.A. and Flechais, I. (2005). Usable Security. In *Security and Usability: Designing Systems that People Can Use* (pp. 13-30). Sebastopol, CA: O'Reilly Media.

[21] Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., Christin, N., & Cranor, L. F. (2010). *Encountering stronger password requirements: User attitudes and behaviors*. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*. doi: 10.1145/1837110.1837113

[22] Shostack, L. G. (1984). Design services that deliver. *Harvard Business Review(84115)*, 133-139.

[23] Stickdorn, M. and Schneider, J. (2010). This is service design thinking. Amsterdam, BIS Publishers. Retrieved from http://www.thisisservicedesignthinking.com

[24] Theofanos, M. and Cram Kowalczyk, E. (2010). "ISPAB Panel on Usable Security". Retrieved from http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2010-11/Theofanos-Kowalczyk_usability-security_ISPAB.pdf

[25] Vonnegut, K. (Presenter). (2010). *Kurt Vonnegut on the shapes of stories*. [Web Video]. Retrieved from http://www.youtube.com/watch?v=oP3c1h8v2ZQ

[26] Weirich, D., & Sasse, M. A. (2001). *Pretty good persuasion: A first step towards effective password security in the real world*. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 137 - 143). doi: 10.1145/508171.508195

[27] Whitten, A., & Tygar, J. D. (1999). *Why Johnny can't encrypt: A usability evaluation of PGP 5.0*. In *Proceedings of the 8th conference on USENIX Security Symposium - Volume 8* (p. 14). Retrieved from http://static.usenix.org/events/sec99/whitten.html

[28] Zeigarnik, B. (1938). On finished and unfinished tasks. In W. Ellis (Ed.), *A source book of Gestalt psychology* (pp. 300-314). London, England: Kegan Paul, Trench, Trubner & Company. doi: 10.1037/11496-025

[29] Zurko, M. E., & Simon, R. T. (1996). *User-centered security*. In *Proceedings of the 1996 Workshop on New Security Paradigms* (pp. 27-33). doi: 10.1145/304851.304859

APPENDIX A: STUDY MATERIALS

A.1 DIARY FORM

Event Details			
Start Time: _____ **End Time:** _____	**Reason for Authentication** _____ First use since last logout _____ Re-try due to unsuccessful login (if re-try right after a failed login, you can skip the rest if info is the same) _____ Login after time-out Other reason: _____ **Location** _____ NIST campus _____ Offsite **Device** _____ Desktop _____ Laptop _____ Blackberry _____ Cell phone _____ Desk phone _____ iPad Other device: _____	**Type of Account/Application** For example, NIST domain, Web TA, etc. _____ **Information required for authentication** _____ User ID/Name _____ Password _____ RSA Token _____ PIN _____ PIV card Other info: _____ **Memory Aids** _____ Memorized _____ Written on a paper _____ Stored in a file _____ Remembered by the browser Other aids: _____	Any Problems? For example, mistyped password, forgot user ID, lost PIV... _____ **What are you going to do?** _____ Try again immediately _____ Contact support (e.g. ITAC) Other : _____ **Frustration Level** Not frustrated 1 2 Neutral 3 4 Very frustrated 5 **Overall comment**

A.2 FOCUS QUESTIONS FOR FOLLOW-UP INTERVIEWS

We're looking for high-level patterns here in terms of frustration, burden, or automatizing.

Indented questions are suggestions for follow-up. The focus questions can happen in any order that makes sense in the interview. Go with the participant flow.

A.1.1 Opening broad questions

- What's the biggest take-away for you from doing the day-in-the-life? Why?
- What was the biggest surprise? Why?
- What big questions do you have now?

A.1.2 Focus questions

A.1.2.1 Frequency

If this hasn't come up already:

How do you feel about the number of authentication events you documented in your day?

How close was that number to what you'd expected?

A.1.2.2 Control and autonomy

- In looking at the range of authentication devices, places, and methods you logged, tell me about how all that fits together.
- Of what you can control about authentication, how did you decide on that combination?
- What kinds of tricks do you use to make authentication easier or more efficient for yourself?

A.1.2.3 Frequency

Let's look at a couple of episodes where you marked that you were very frustrated. [*Walk through the data from the form, if you have it, up to the point of describing the problem. After you read their description, ask:*] What happened here?

- What was frustrating about it? [or, continue, if needed:] Why did you become frustrated?
- What did that event cost you?

A.1.2.4 Timing clusters

When we skimmed through your data, we saw that most of your events happened [when?]. Tell us about that. How typical is that?

A.1.2.5 Big picture: what's the hassle factor?

- Looking back at your day-in-the-life of authentication, what's your take on authentication effectiveness?
- What's the biggest hassle about it? Why?
- What do you see as the tradeoffs?

A.3 DEMOGRAPHIC SURVEY

What is your profession?

Gender ____ F _____M

Age range

__< 20

__ 21-29

__ 30-39

__ 40-49

___ 50-59

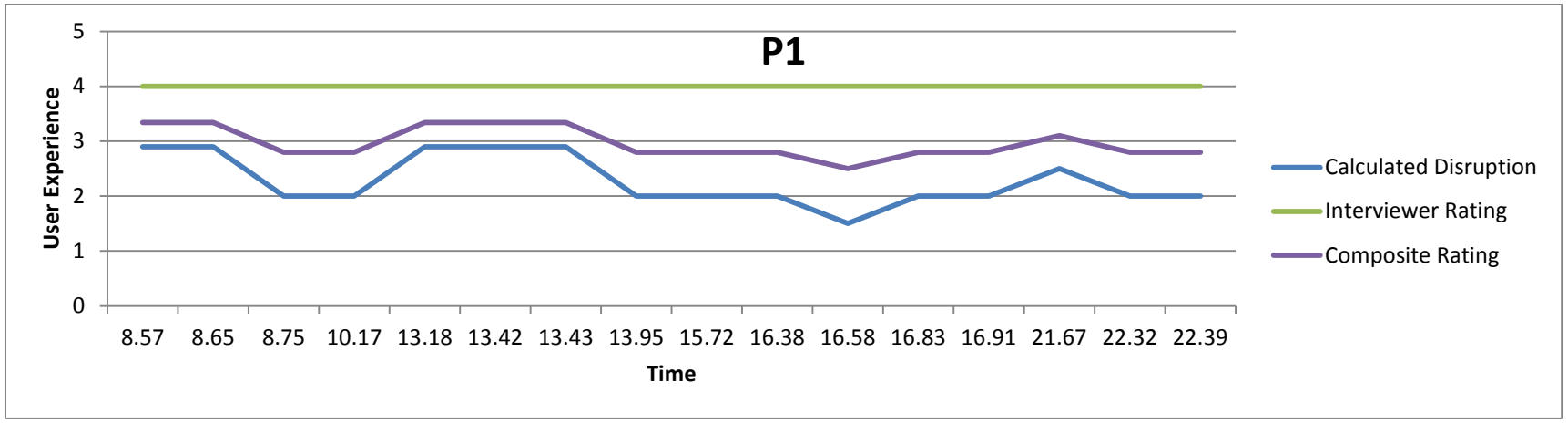
__ 60+

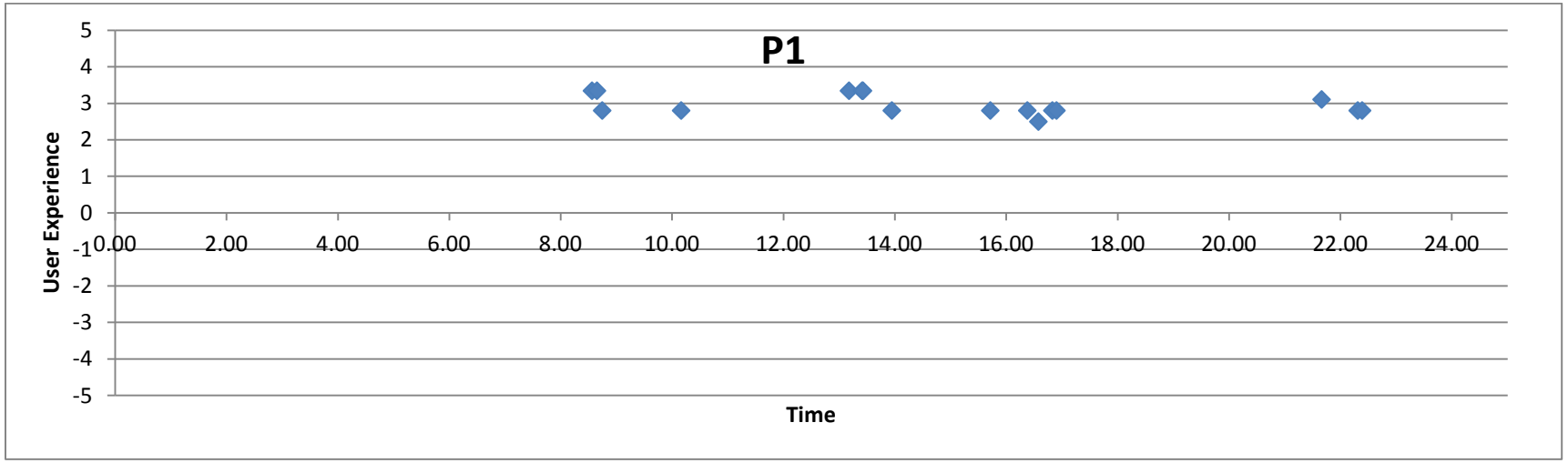
APPENDIX B: USER EXPERIENCE CHARTS FOR STUDY PARTICIPANTS

This appendix contains user experience charts (as described in **Section 5**) for each of our study participants, in the form of a line graph and a scatterplot.

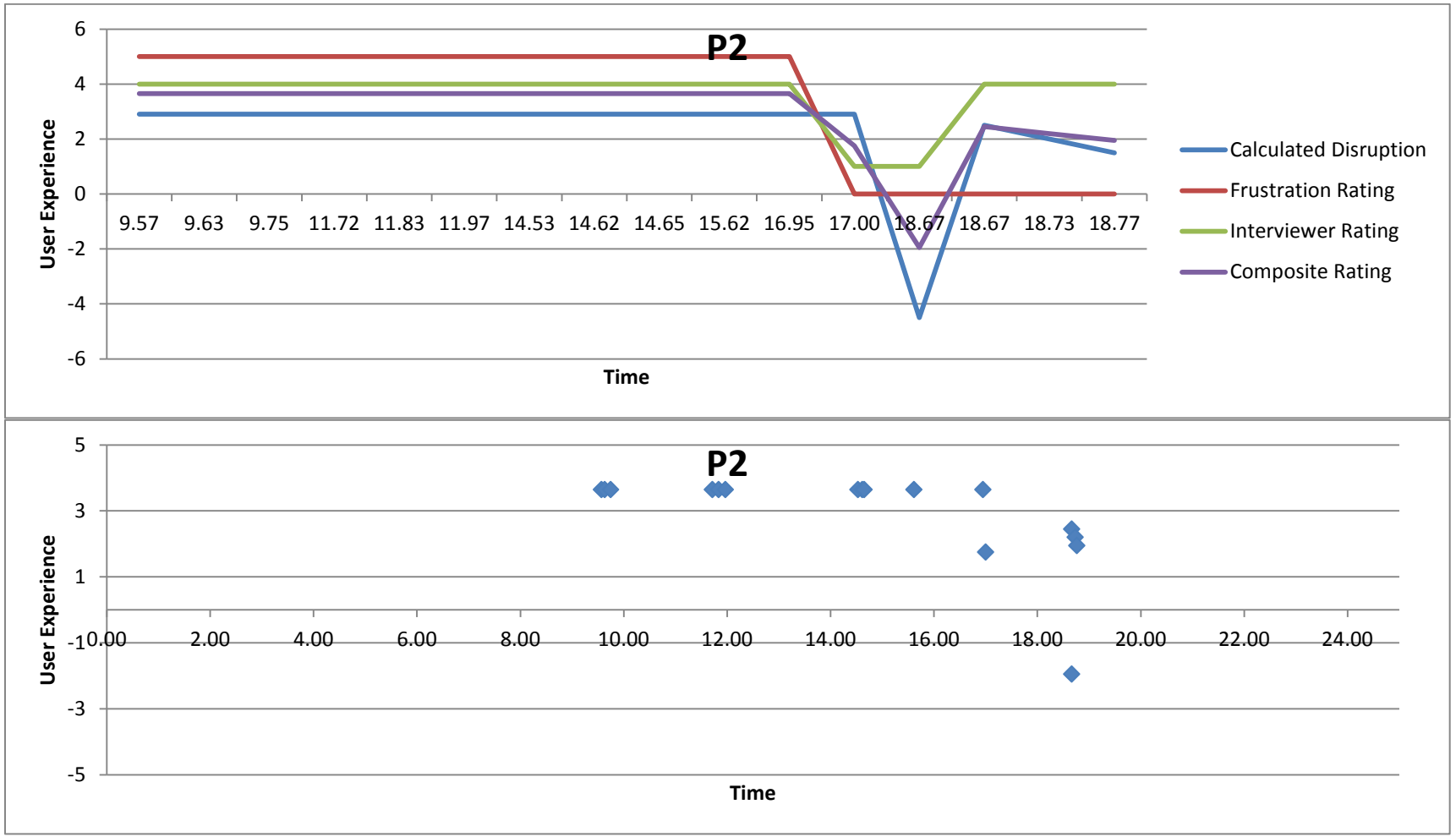
Some participants provided frustration ratings for some of their recorded authentication events but not others: in these cases, the red Frustration line on their line graph may be broken. In a few cases participants provided no frustration ratings at all, so their graphs do not include frustration lines.

User Experience Line Graph and Scatterplot – Participant 1

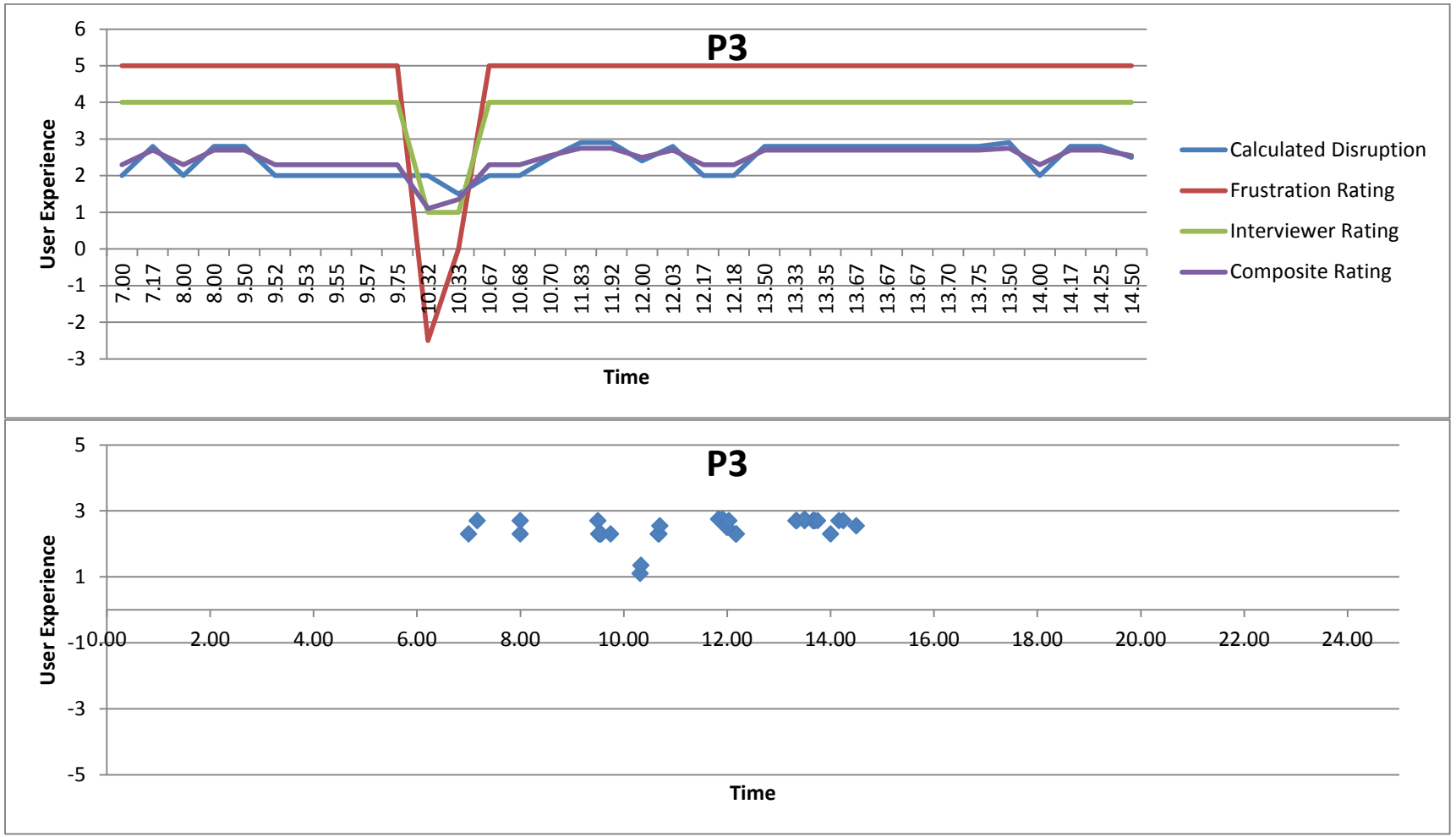




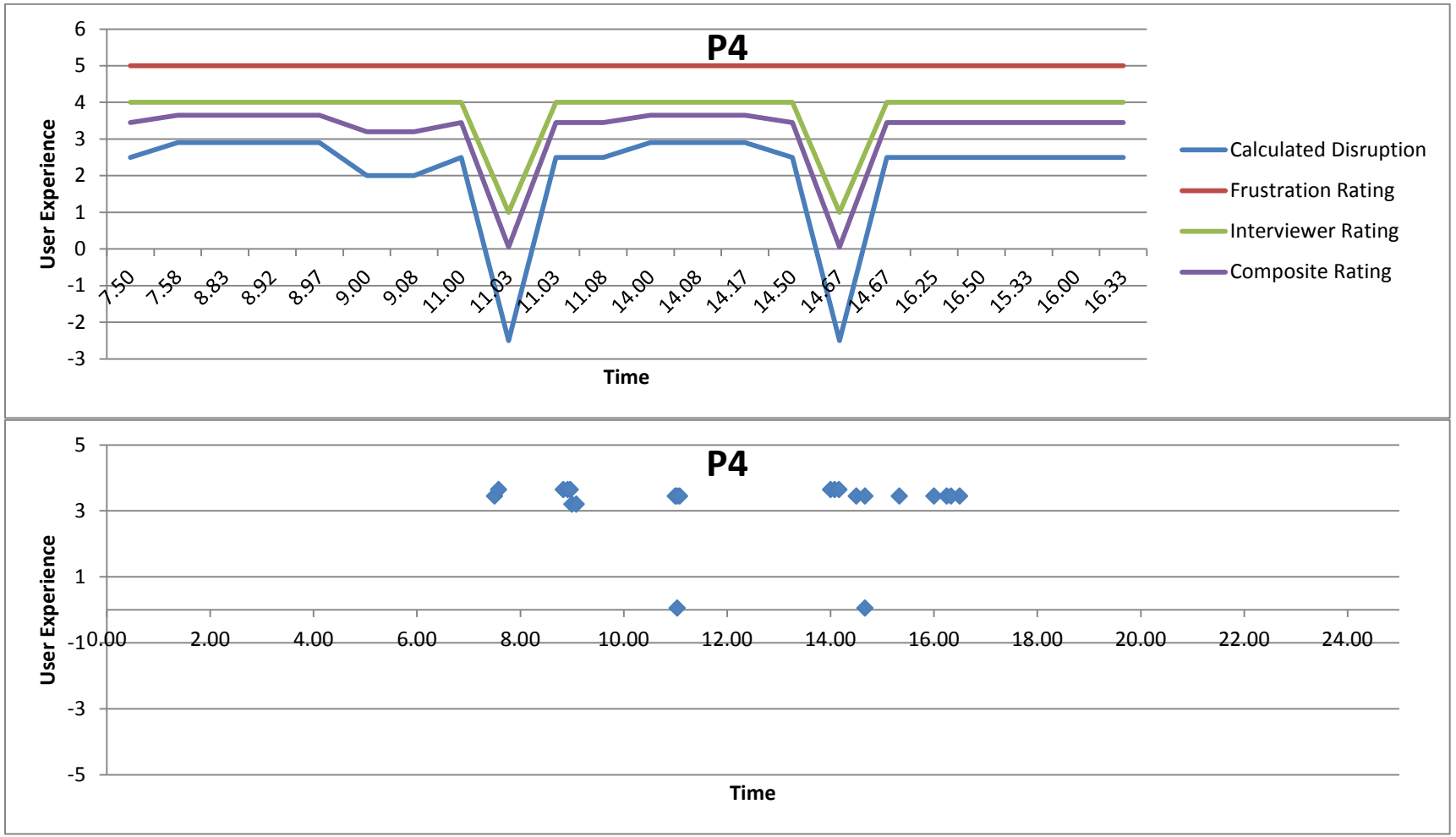
User Experience Line Graph and Scatterplot – Participant 2



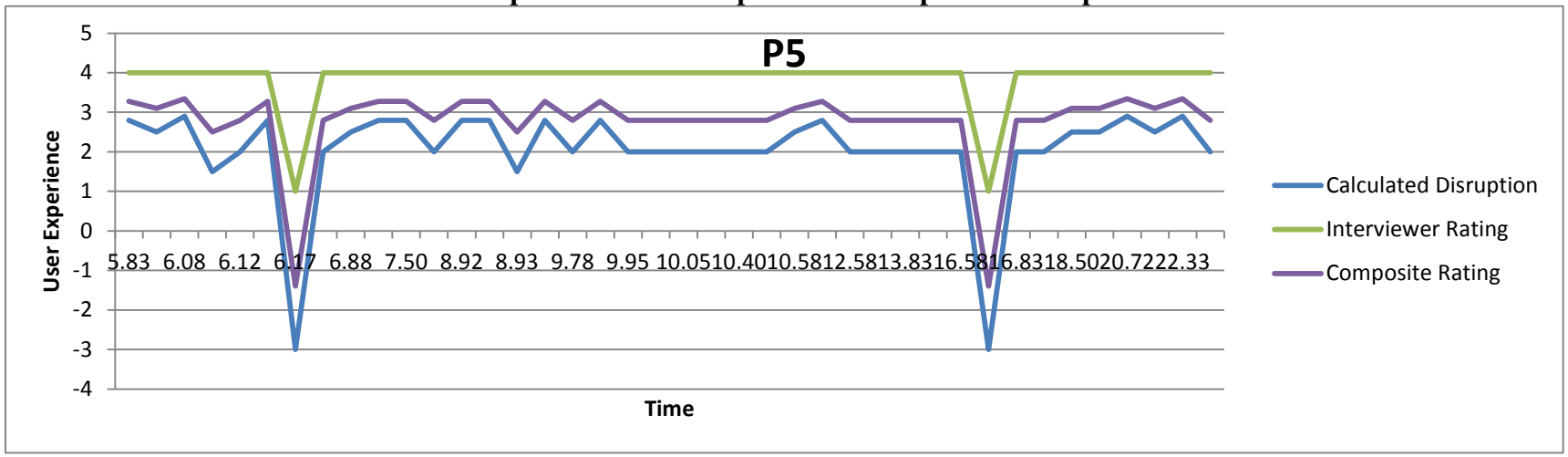
User Experience Line Graph and Scatterplot – Participant 3

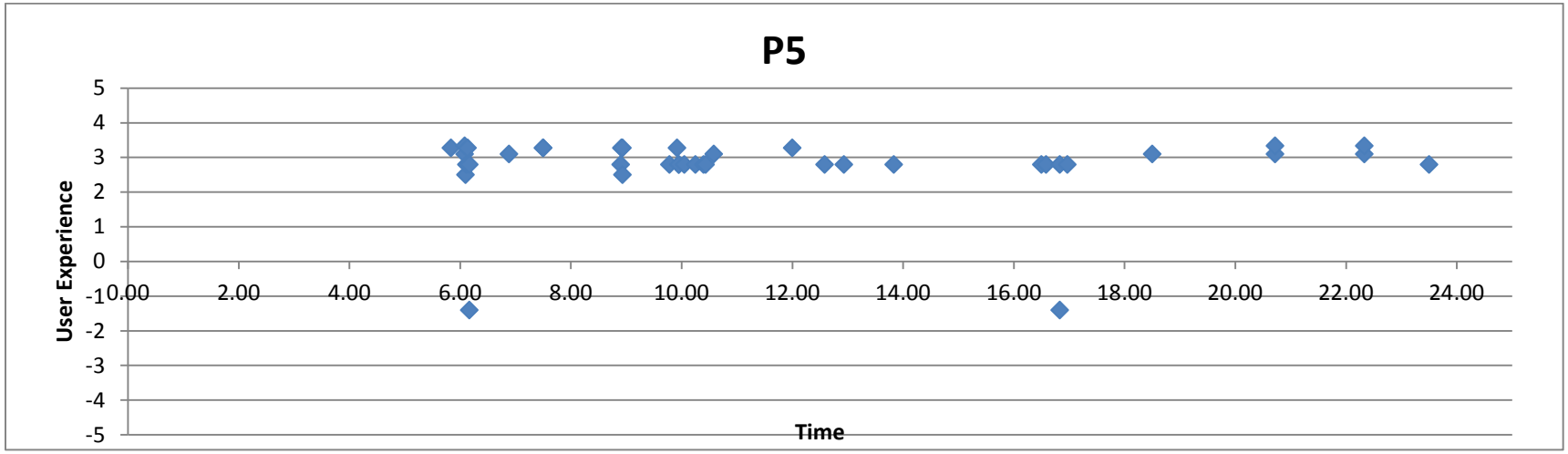


User Experience Line Graph and Scatterplot – Participant 4

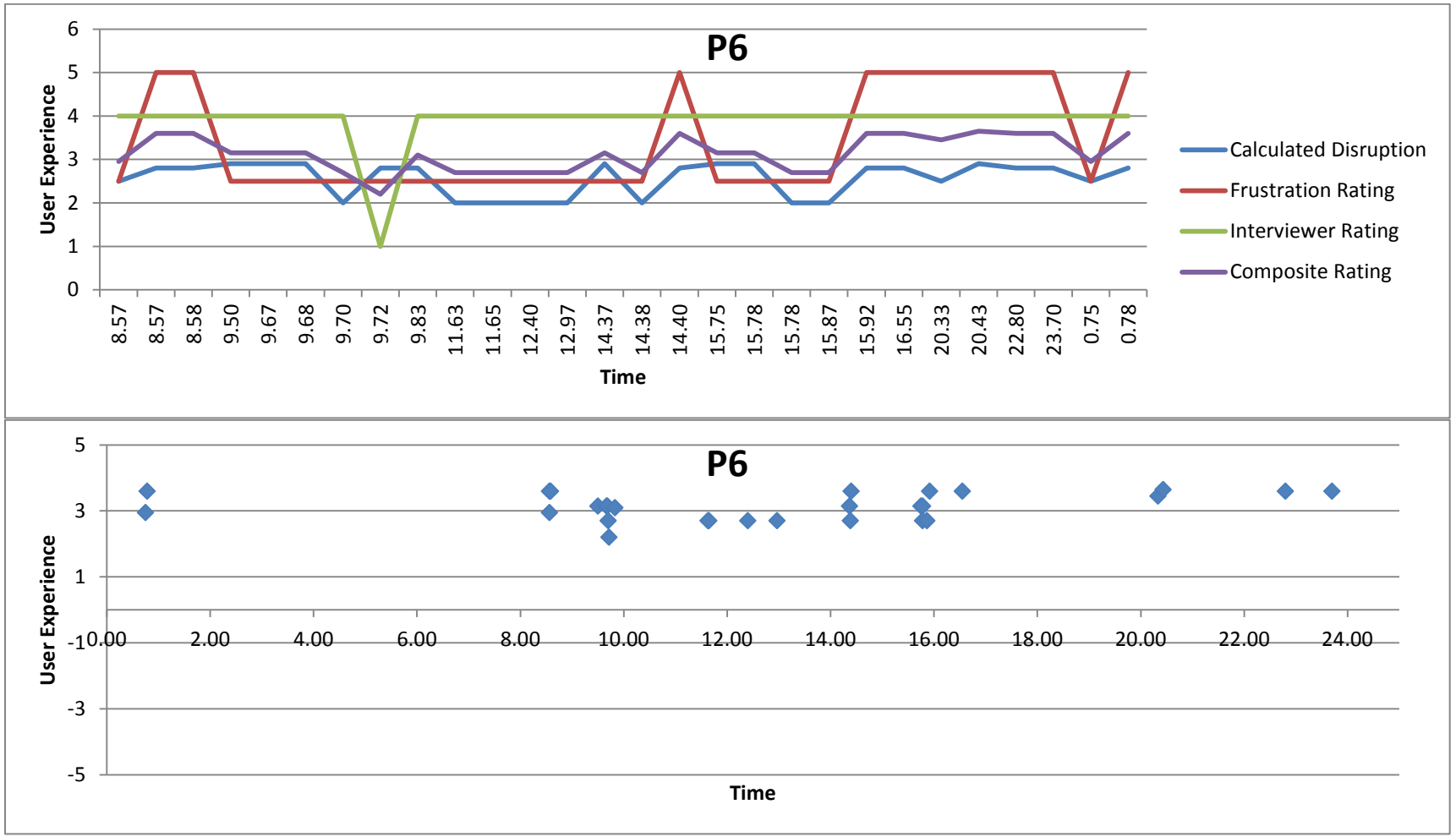


User Experience Line Graph and Scatterplot – Participant 5

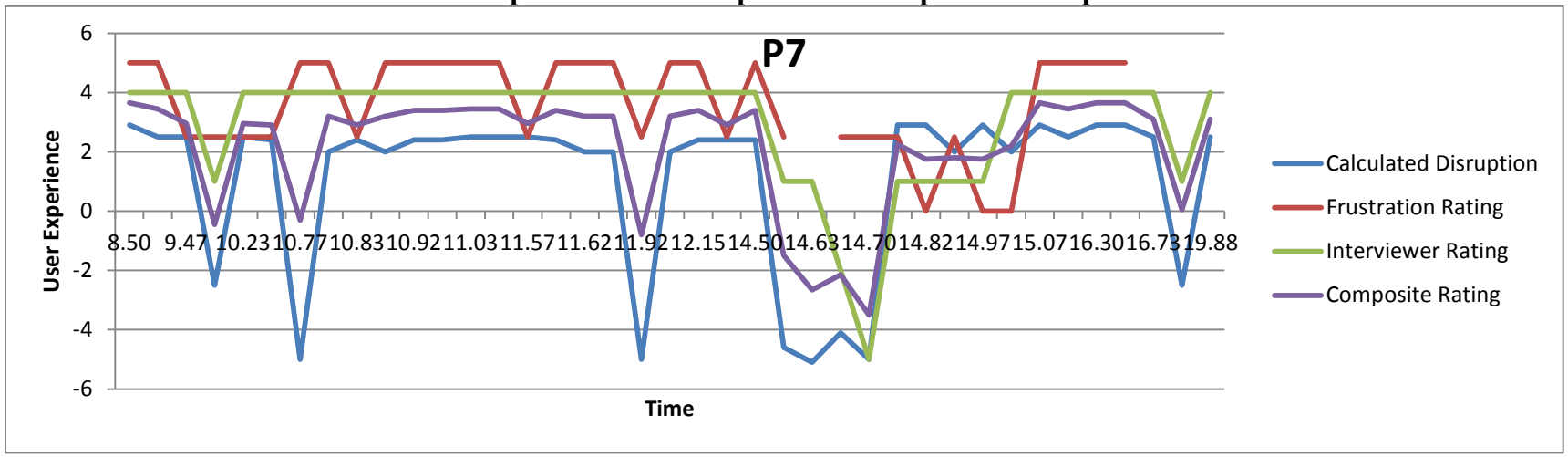


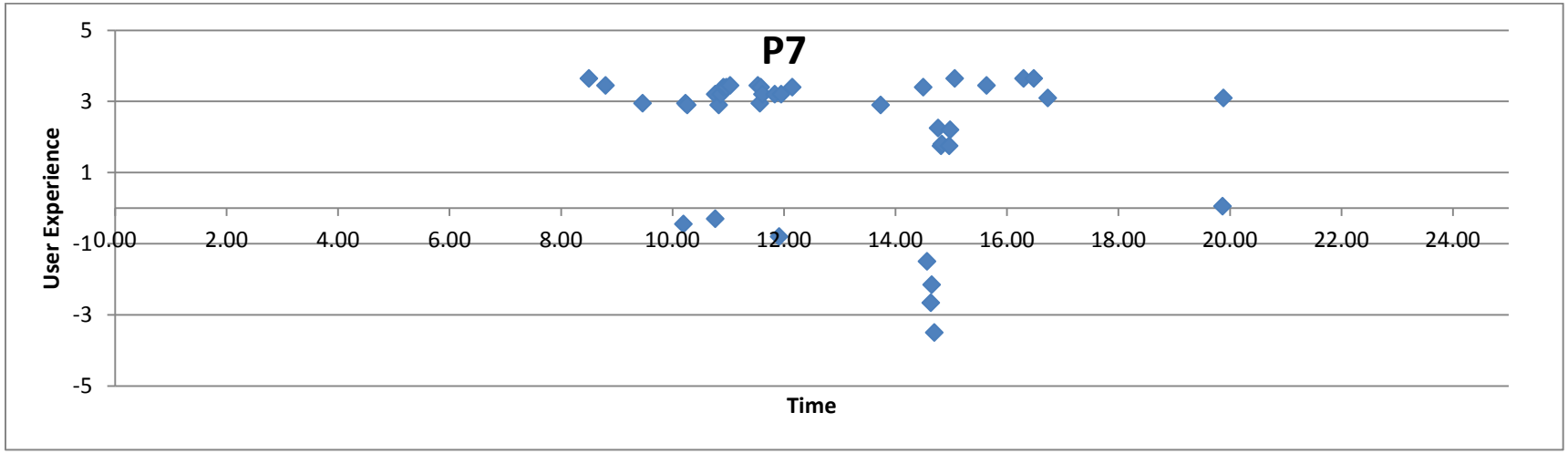


User Experience Line Graph and Scatterplot – Participant 6

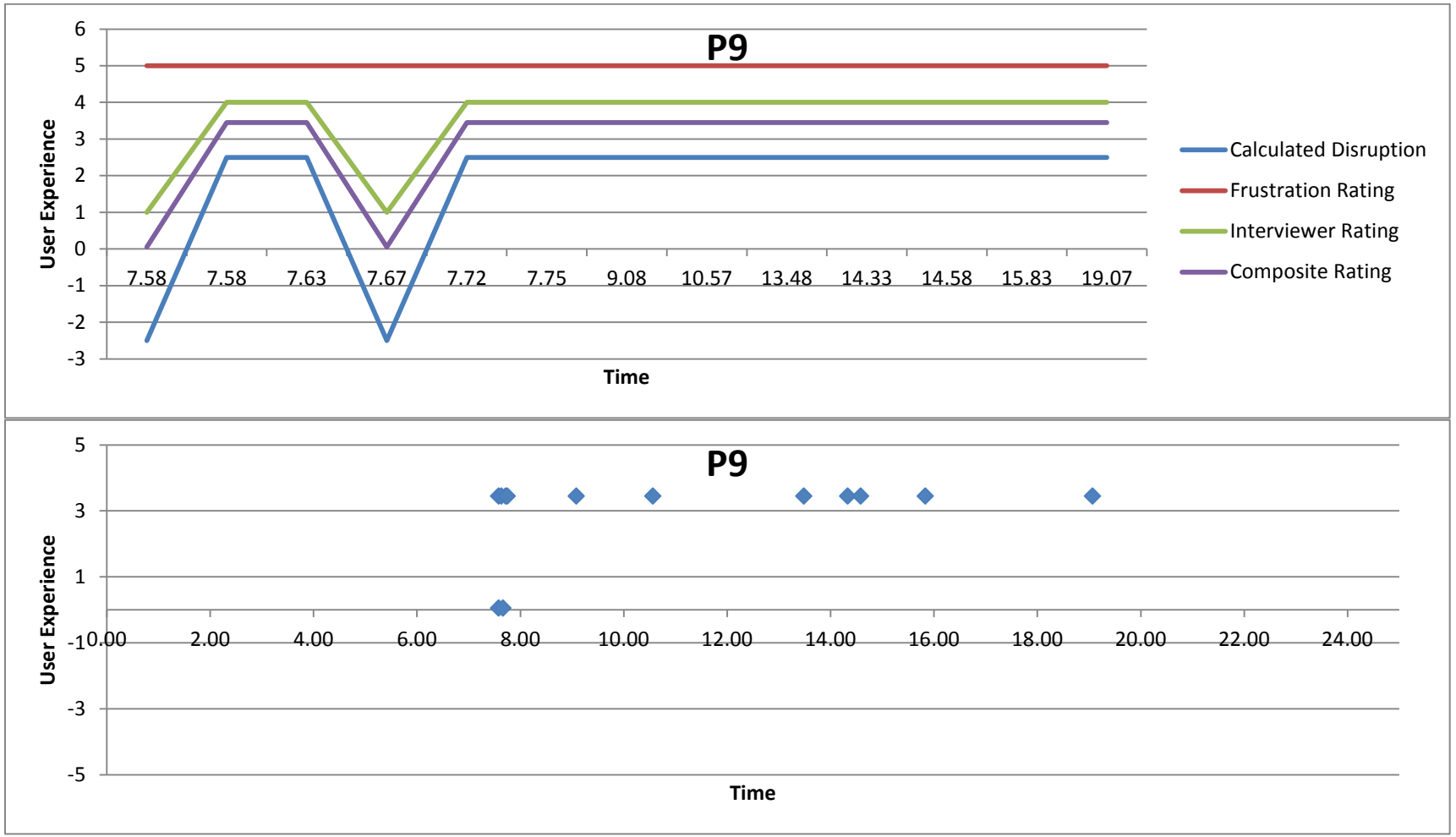


User Experience Line Graph and Scatterplot – Participant 7

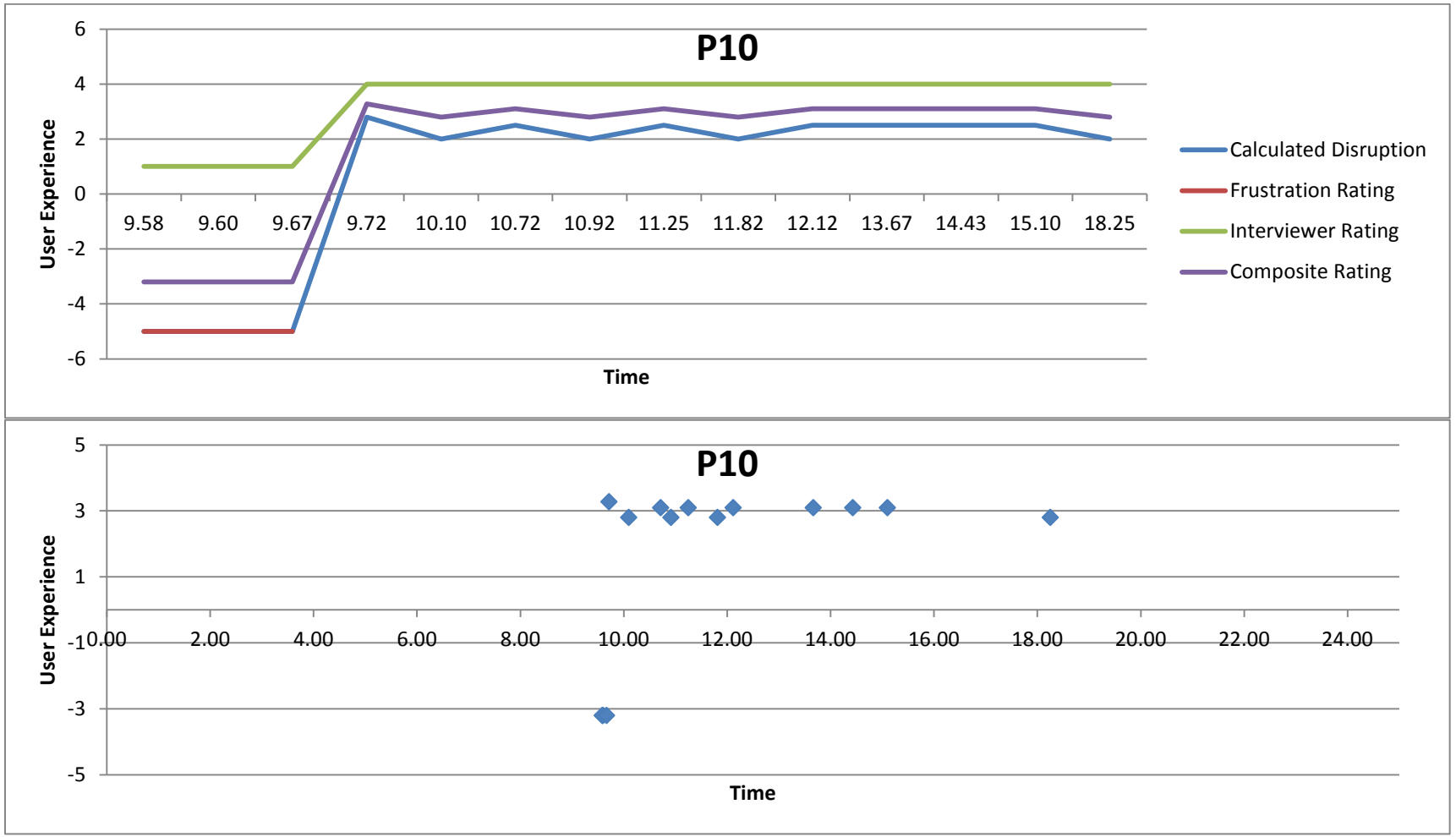




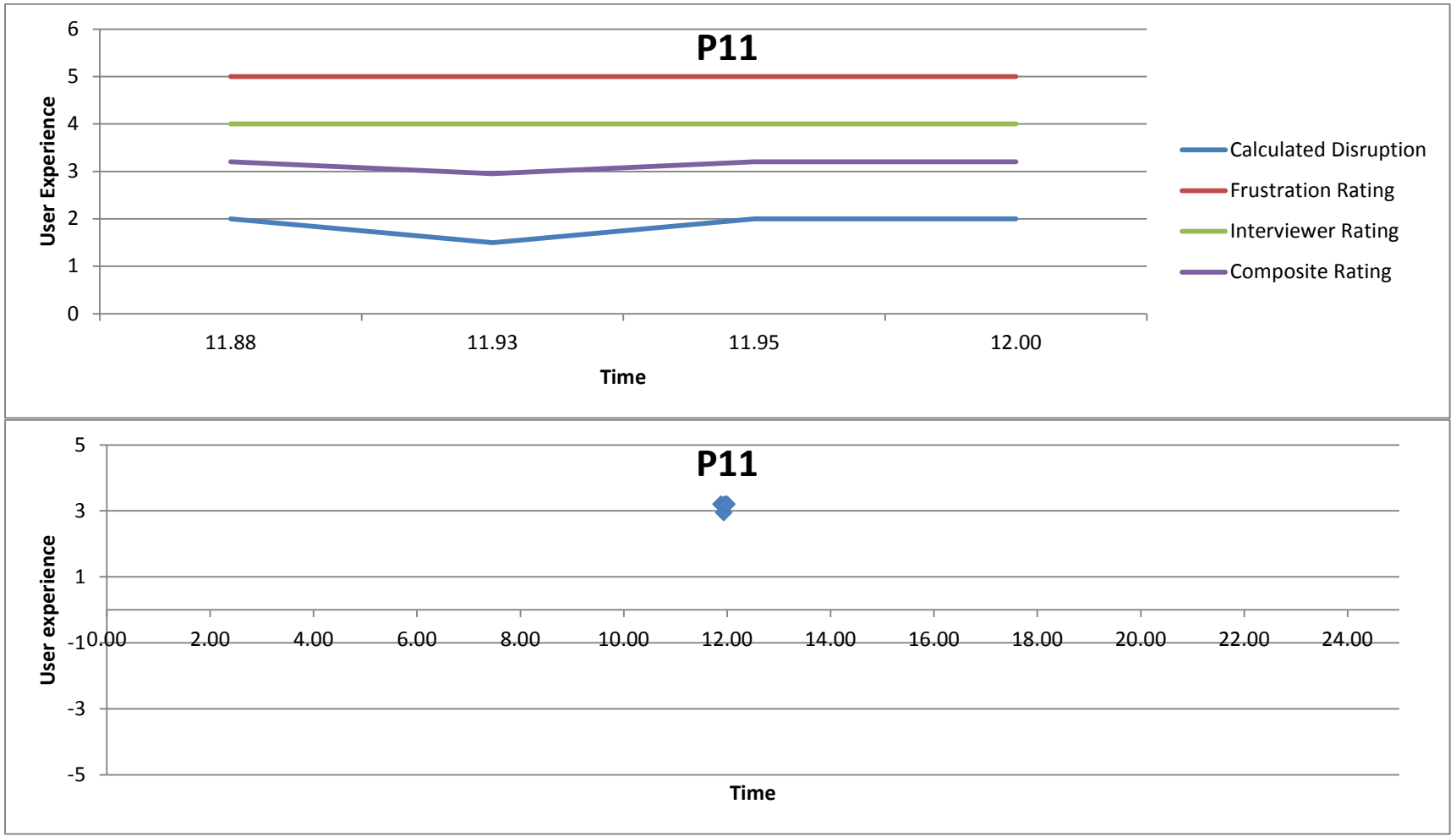
User Experience Line Graph and Scatterplot – Participant 9



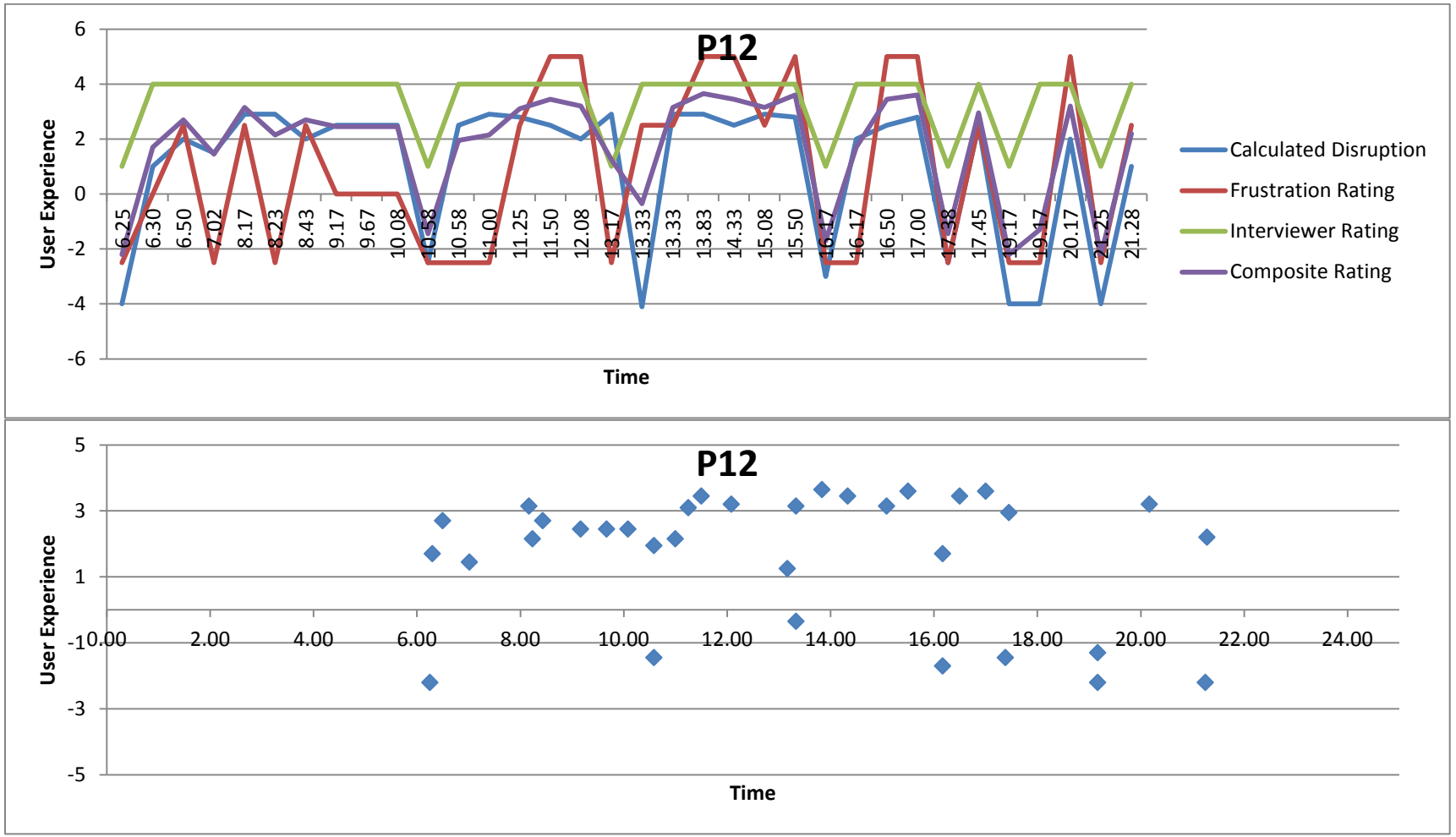
User Experience Line Graph and Scatterplot – Participant 10



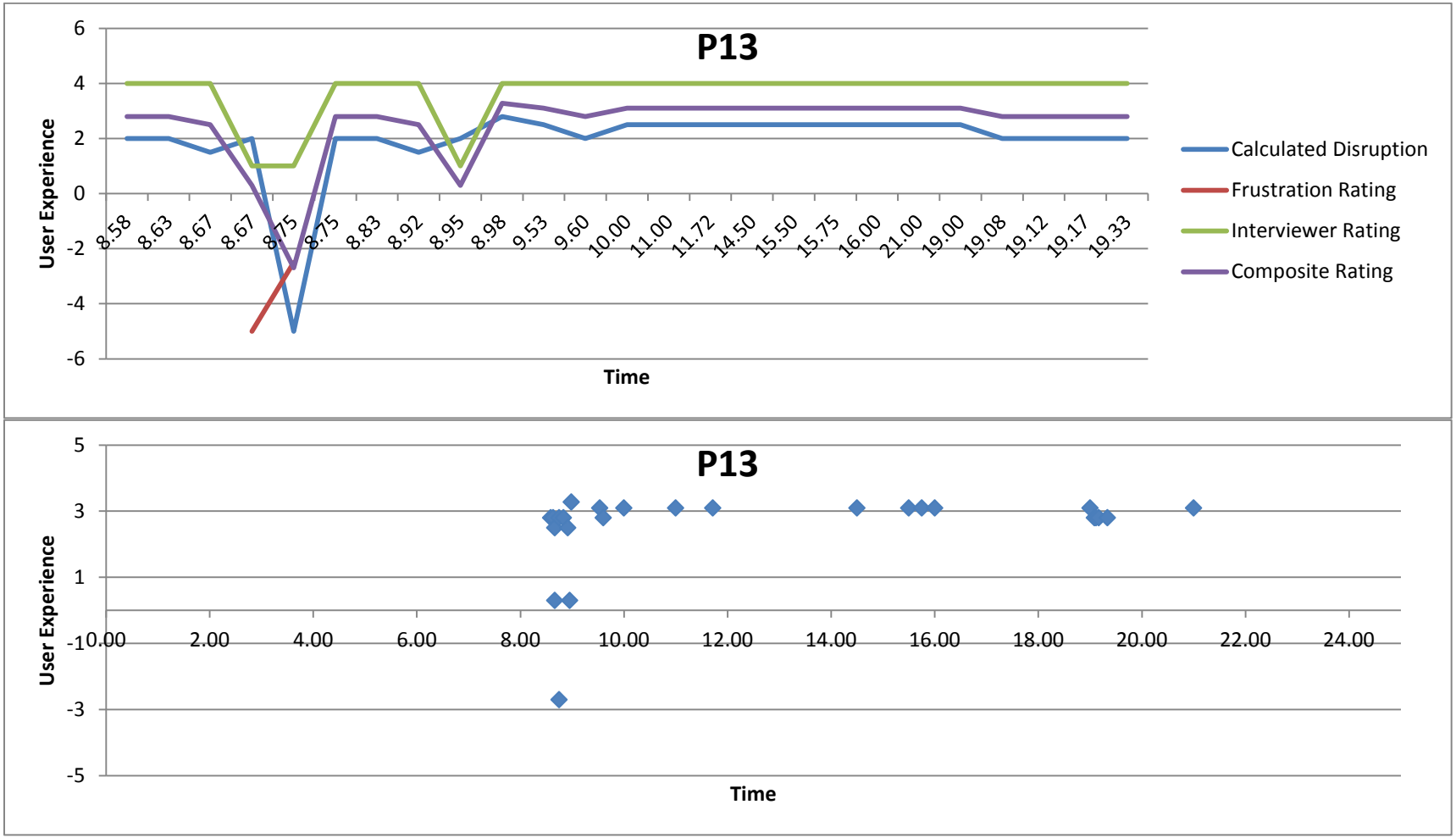
User Experience Line Graph and Scatterplot – Participant 11



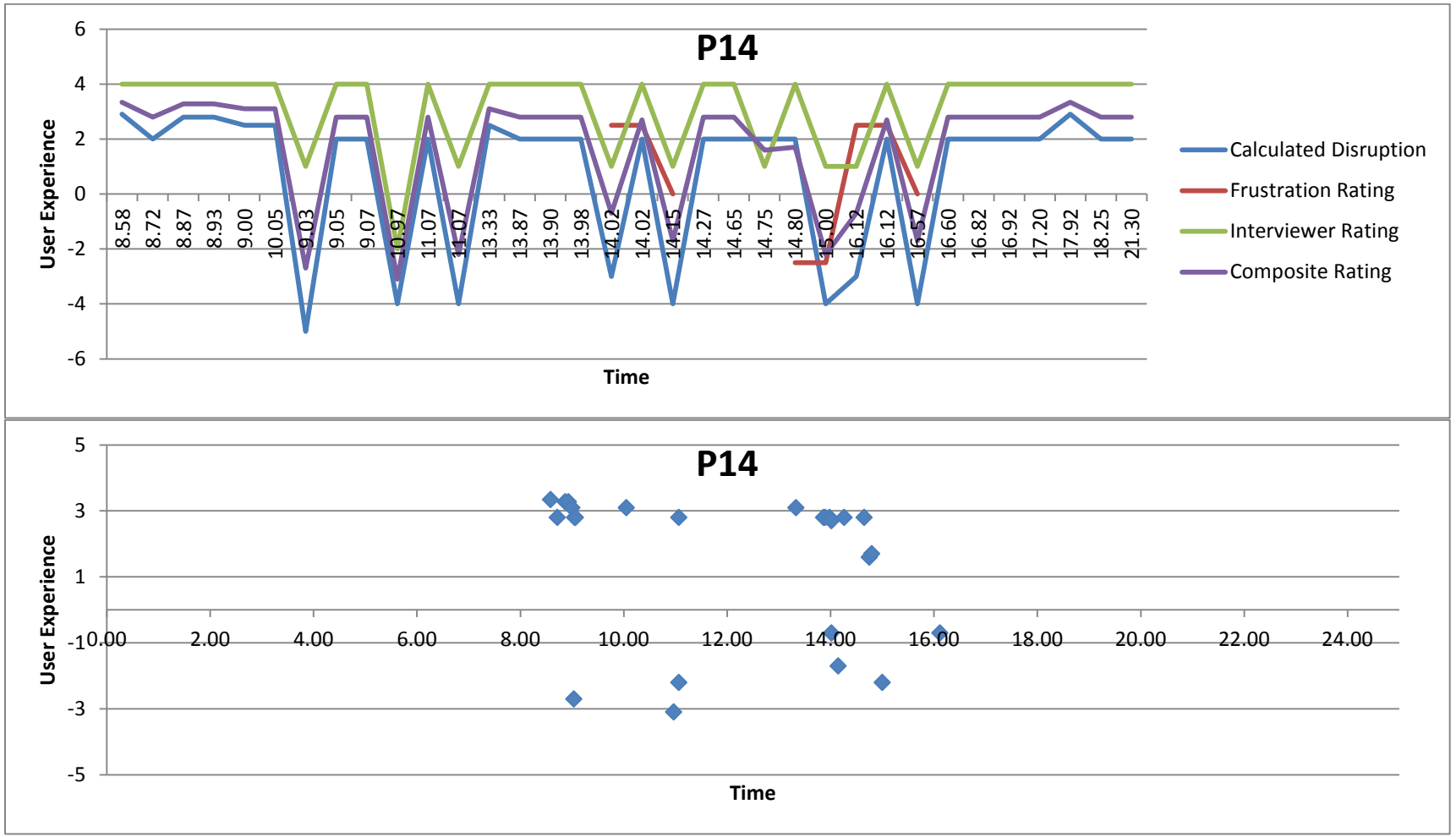
User Experience Line Graph and Scatterplot – Participant 12



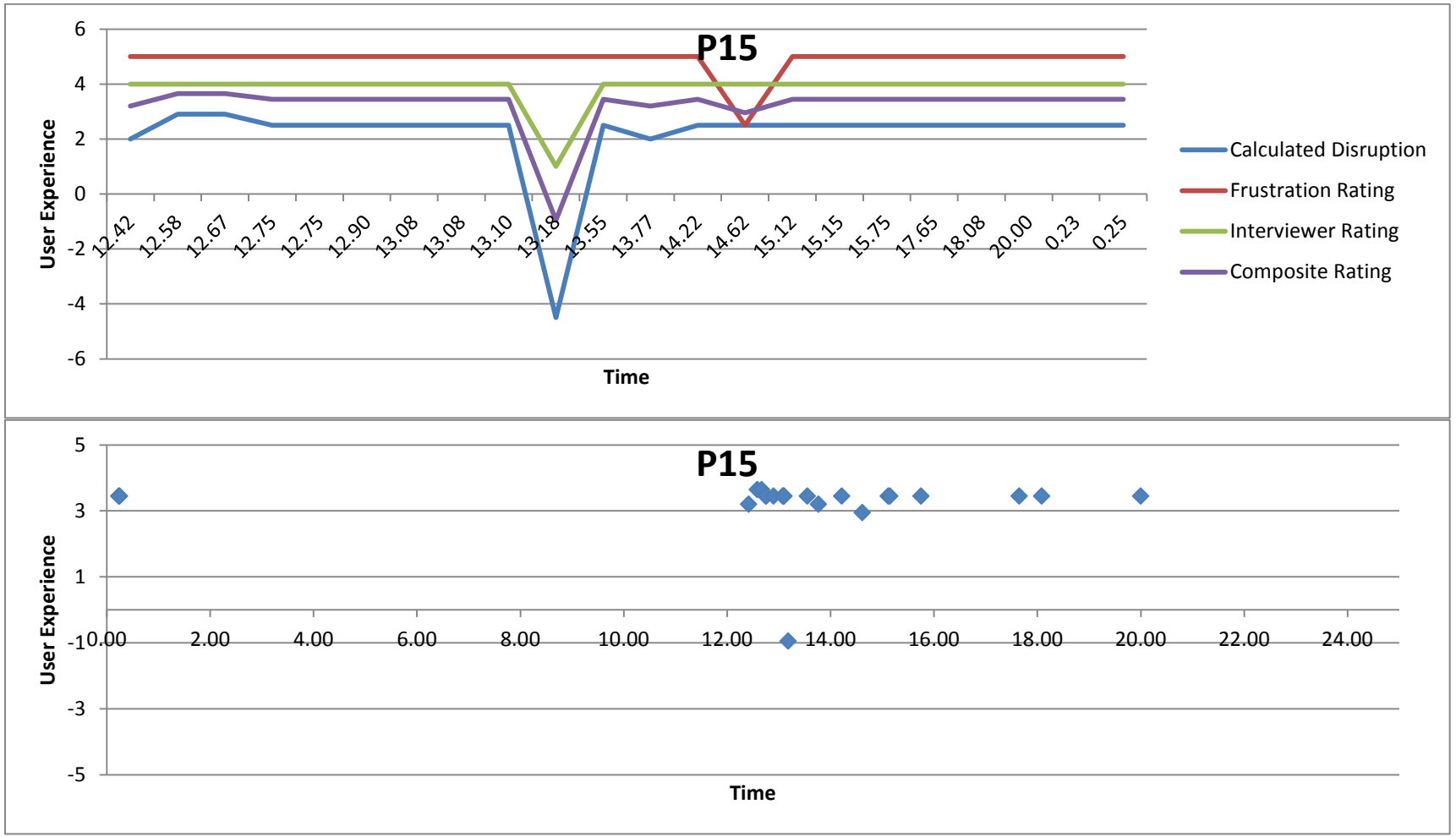
User Experience Line Graph and Scatterplot – Participant 13



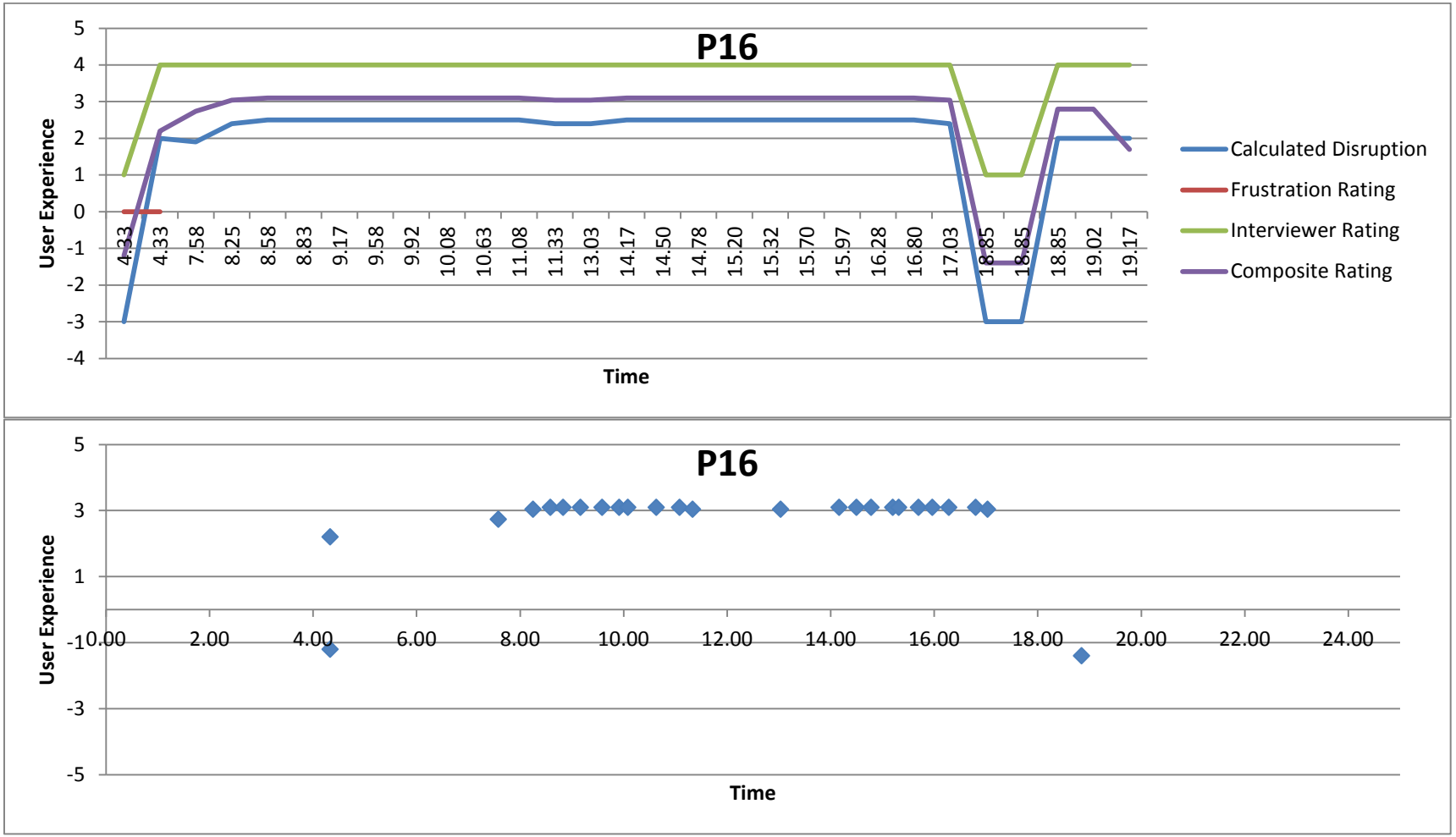
User Experience Line Graph and Scatterplot – Participant 14



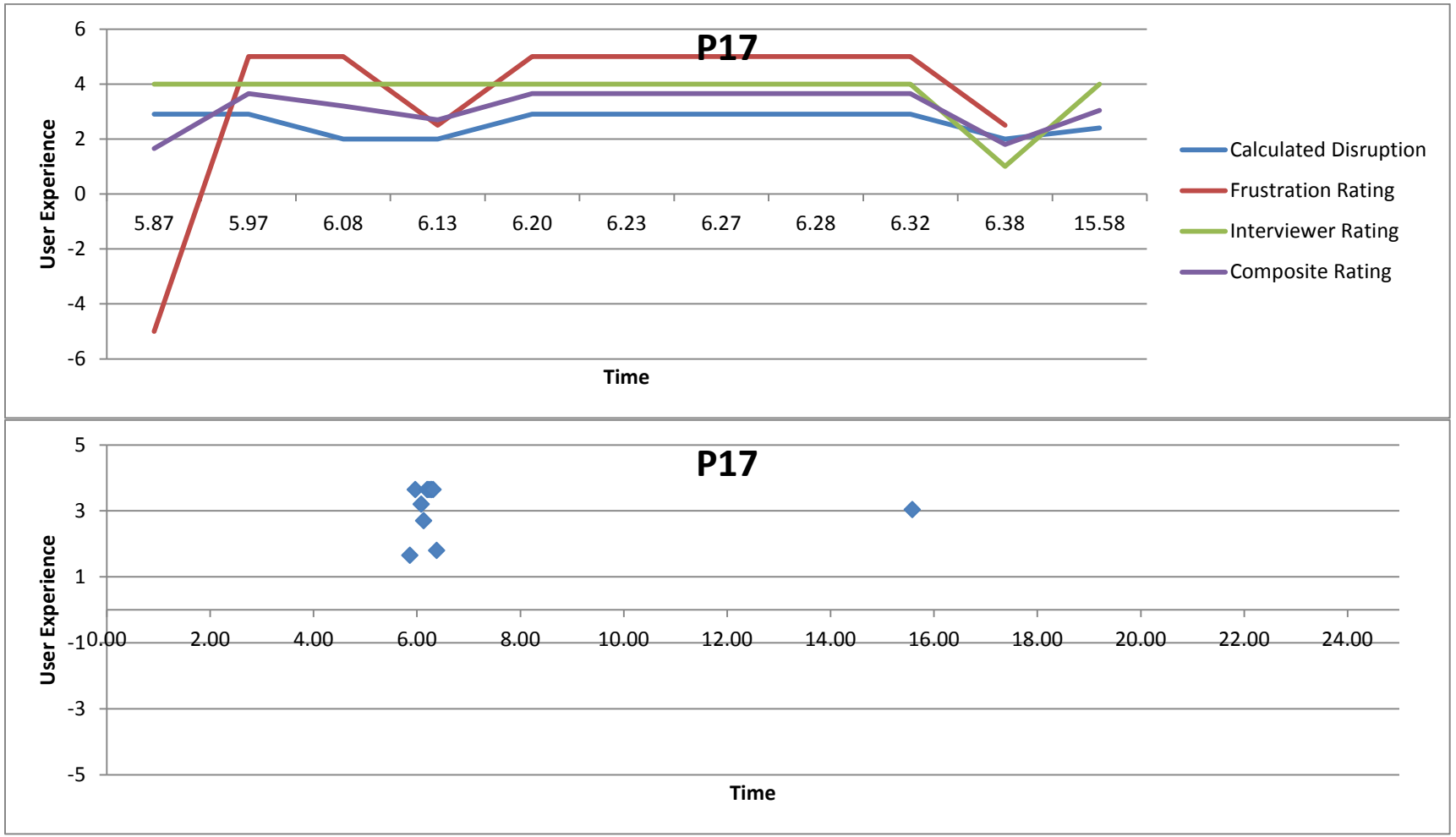
User Experience Line Graph and Scatterplot – Participant 15



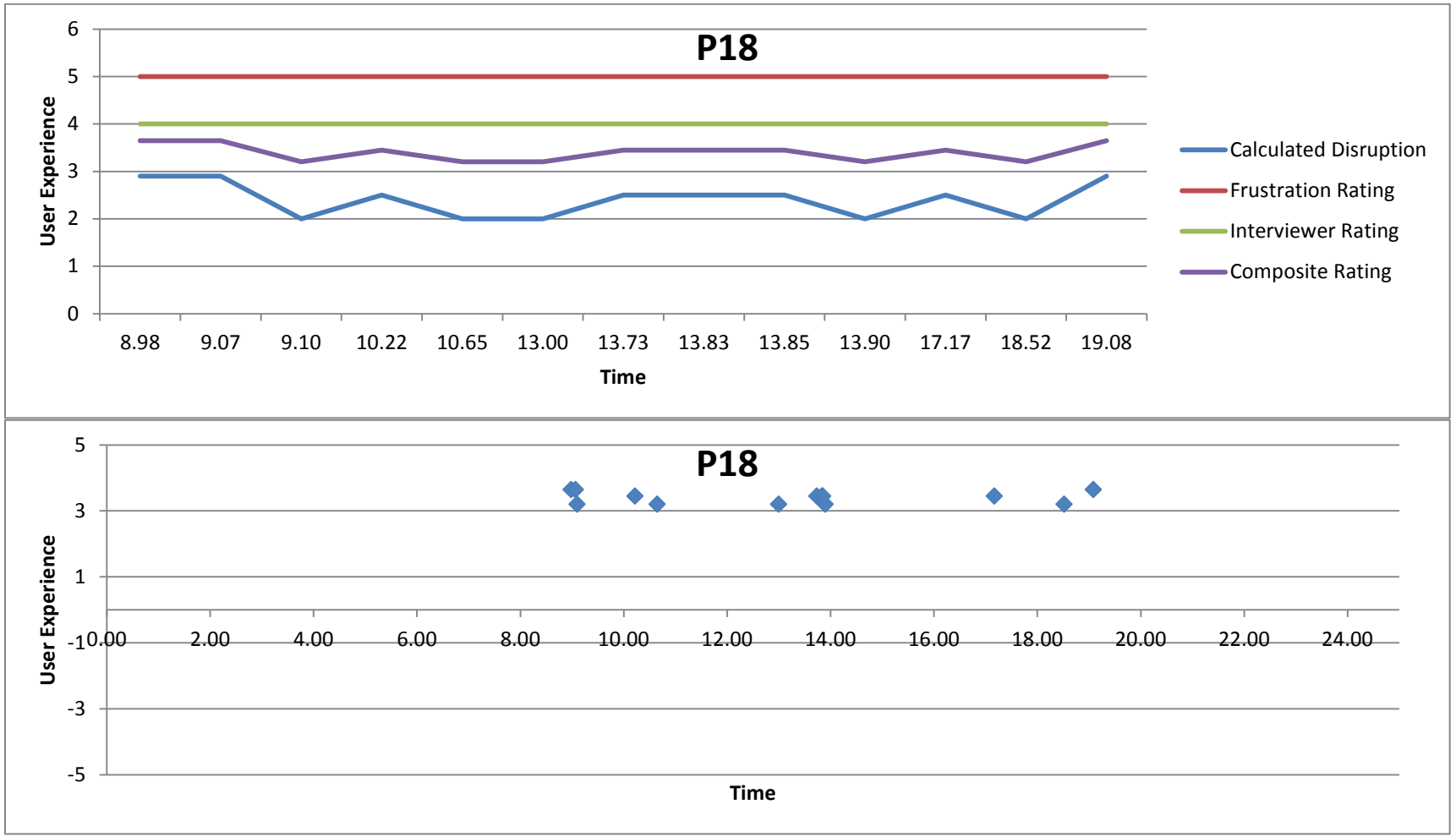
User Experience Line Graph and Scatterplot – Participant 16



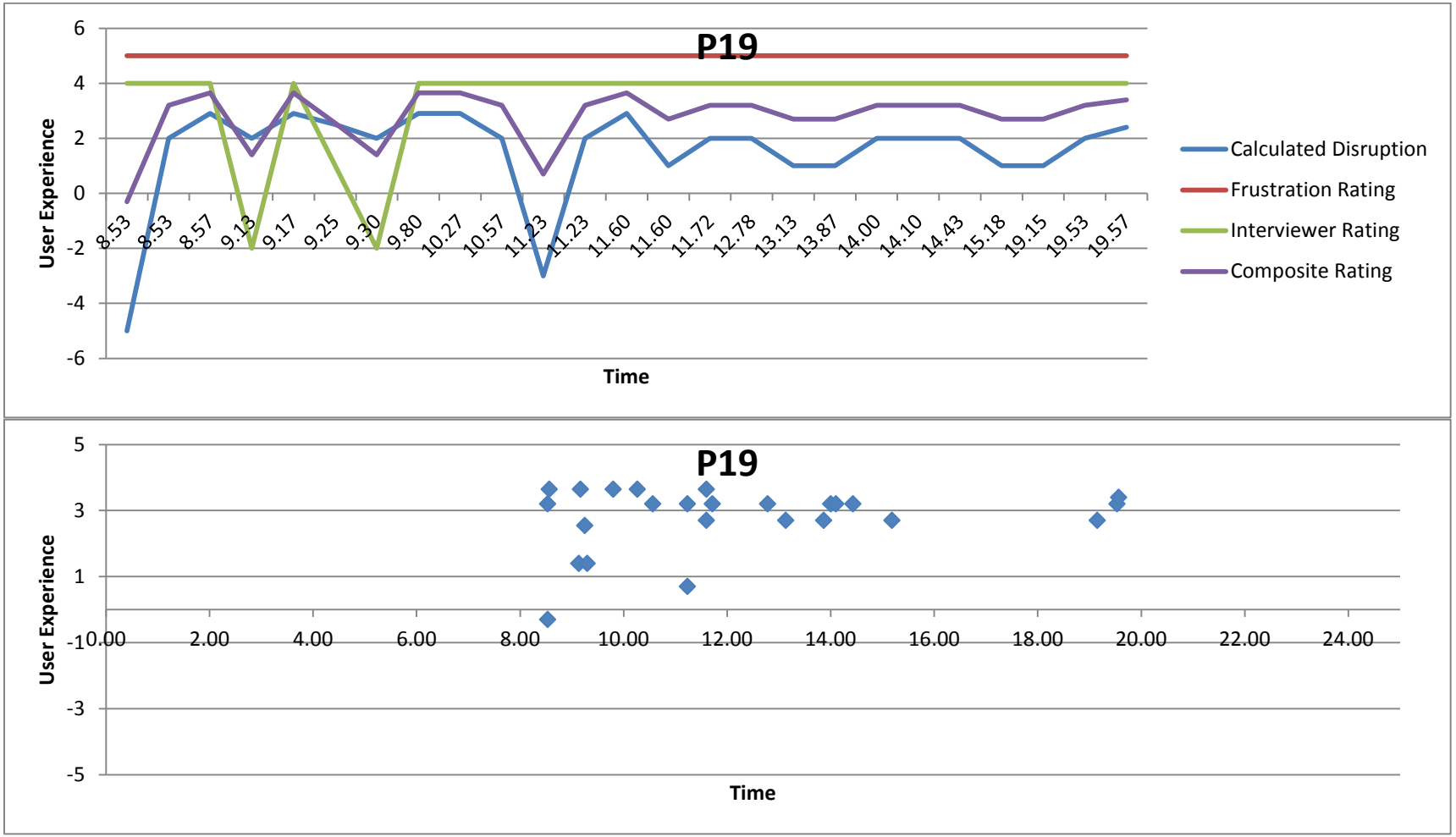
User Experience Line Graph and Scatterplot – Participant 17



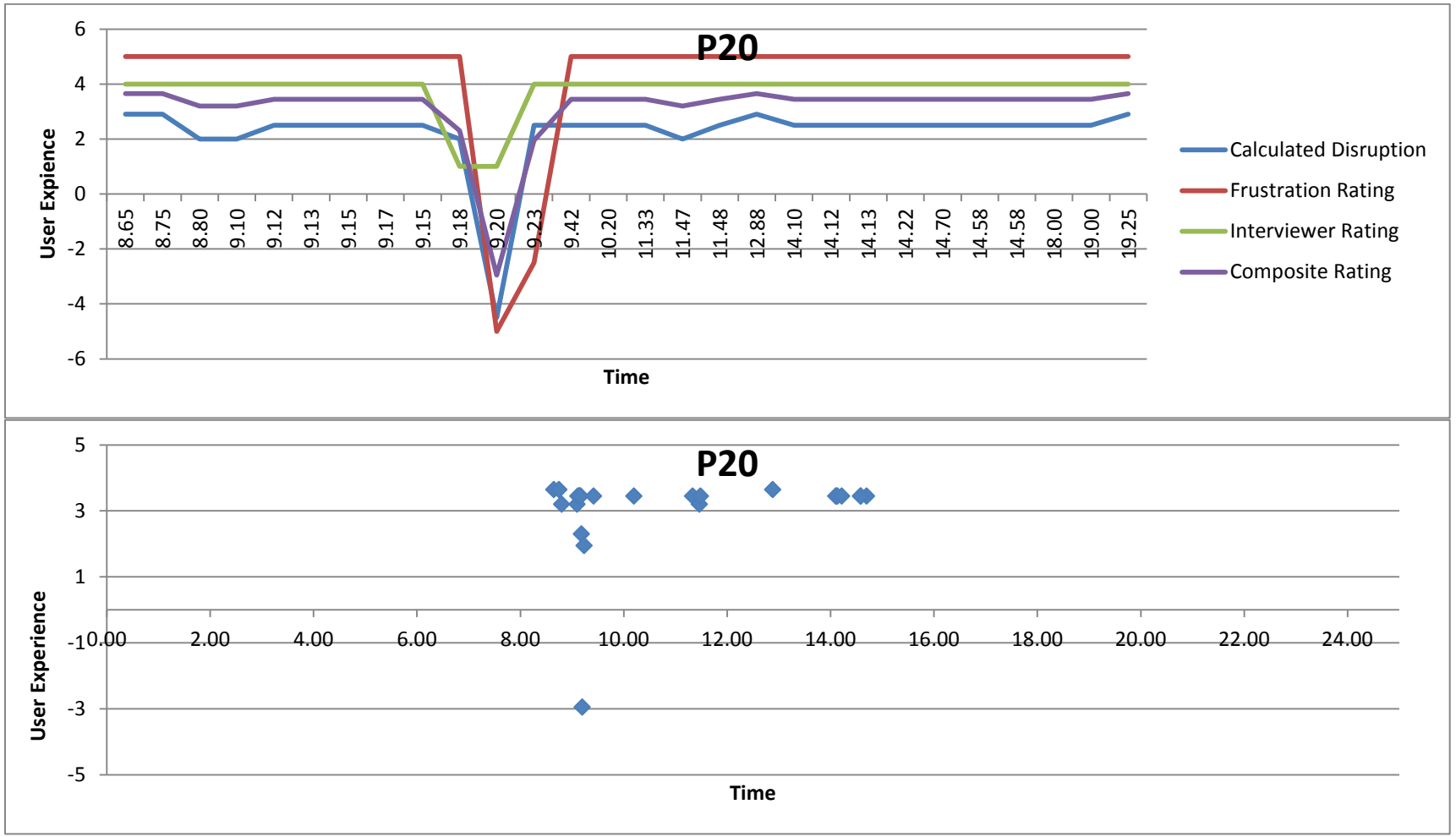
User Experience Line Graph and Scatterplot – Participant 18



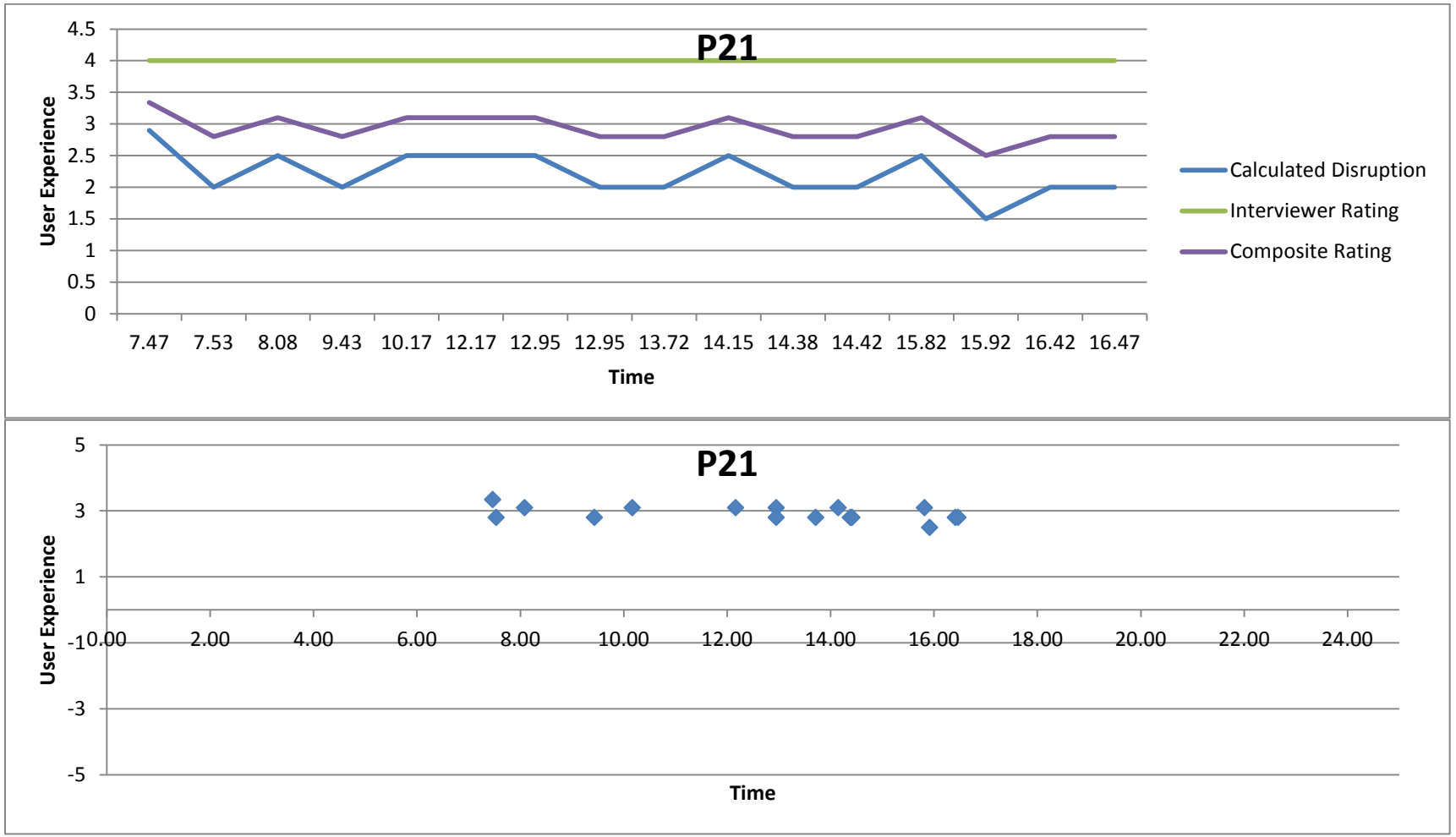
User Experience Line Graph and Scatterplot – Participant 19



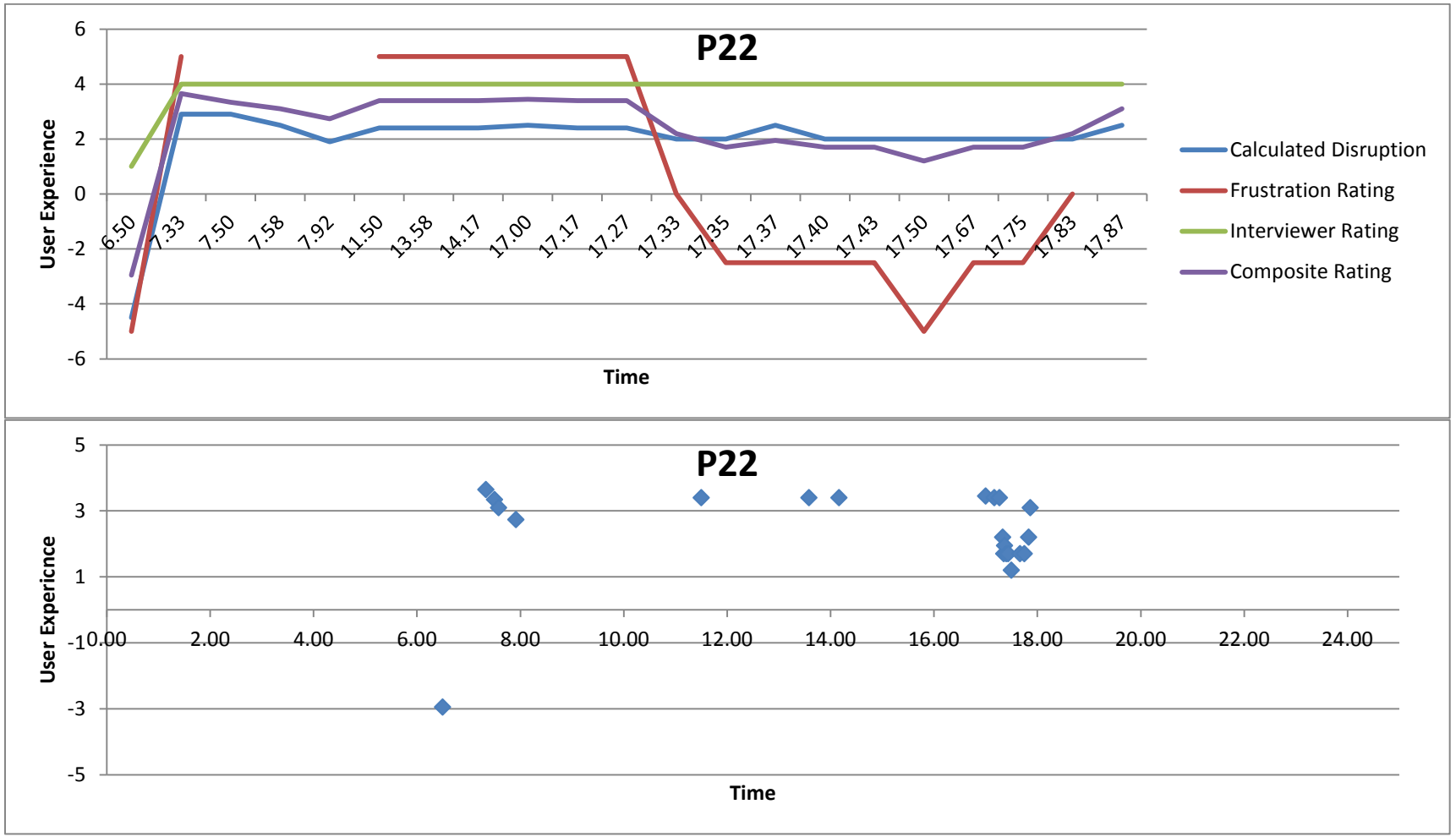
User Experience Line Graph and Scatterplot – Participant 20



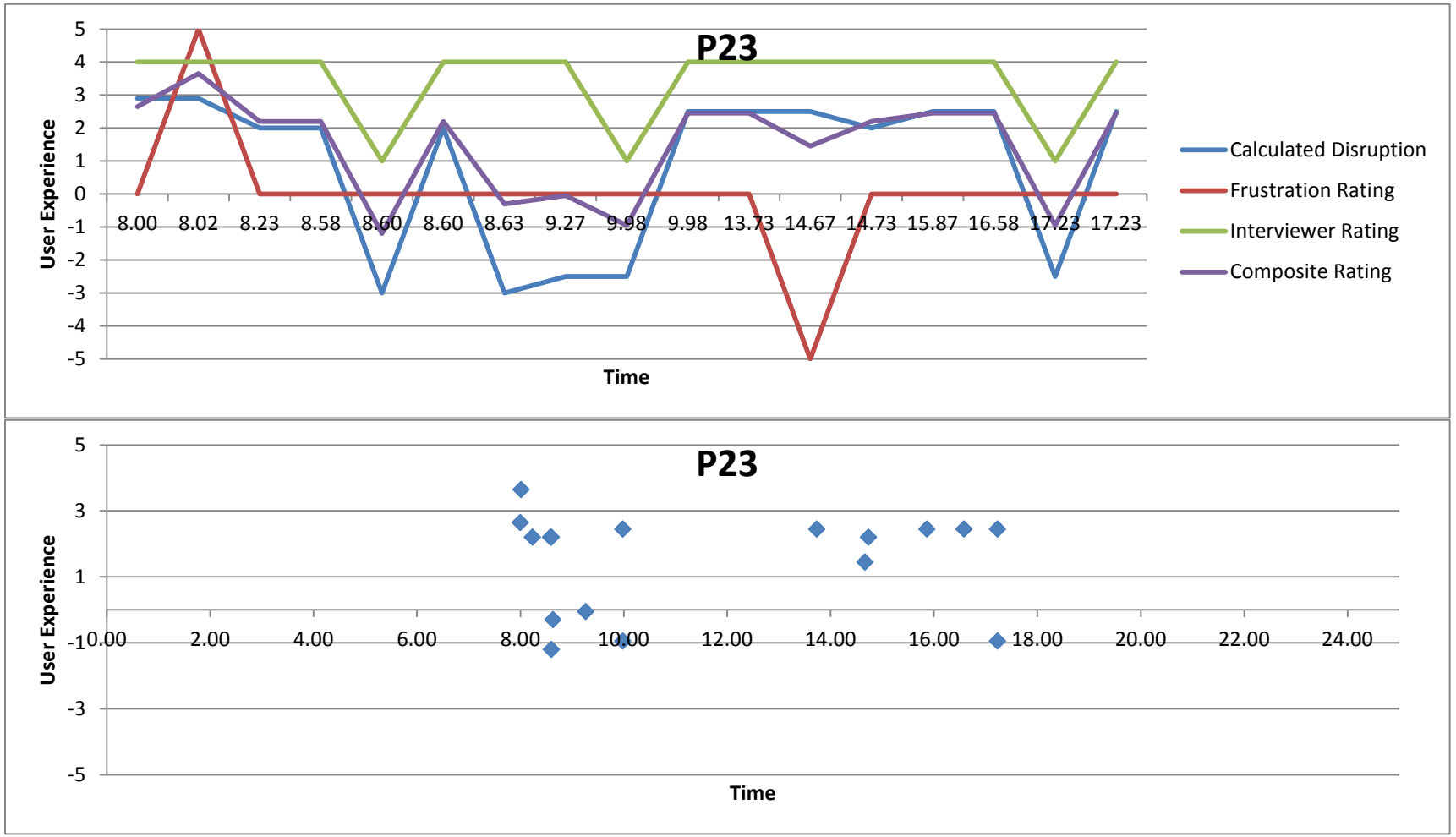
User Experience Line Graph and Scatterplot – Participant 21



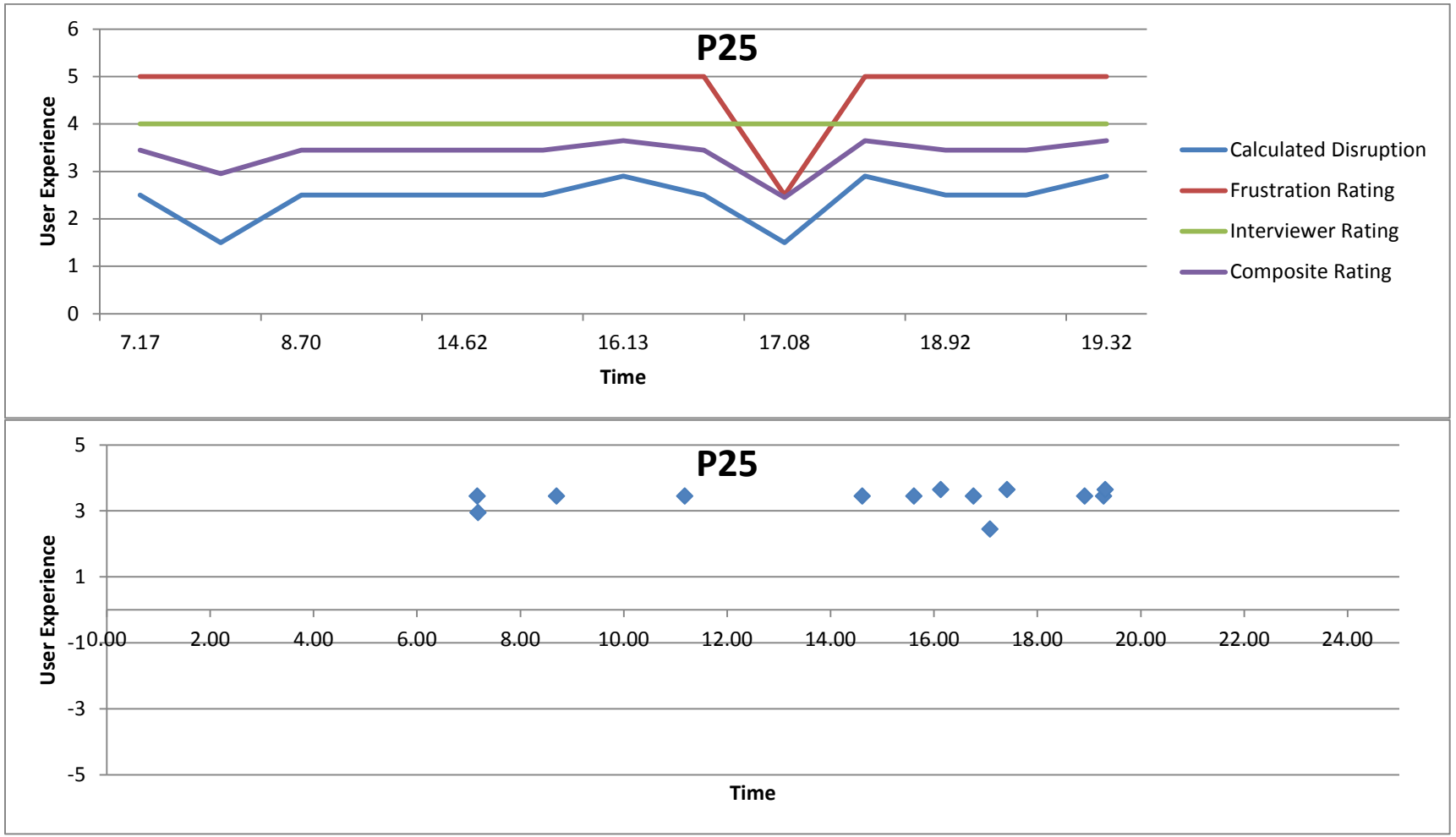
User Experience Line Graph and Scatterplot – Participant 22



User Experience Line Graph and Scatterplot – Participant 23



User Experience Line Graph and Scatterplot – Participant 25



APPENDIX C: CATALOG OF PARTICIPANT QUOTES ON AUTHENTICATION-RELATED FRICTION POINTS, COPING STRATEGIES, AND HABITS

The material in this appendix comes from follow-up interviews researchers conducted with participants following the data collection period. It consists of direct quotes (and, to a lesser extent, paraphrased statements written by researchers) regarding participants' authentication-related experiences, perceptions, and behaviors. The quotes and paraphrased statements are organized by subject category in a hierarchical format. The "top-level" categories (indicated by Roman numerals) deal with five general areas related to authentication: the entry of authentication information; the management of that information; the impact of authentication on primary tasks; authentication coping strategies; and authentication's unintended effects on work habits. Each section is further divided into parts that "drill down" into specific concepts, actions, or topics addressed by our participants. The quotes and paraphrased themselves are italicized, bulleted items appearing under the appropriate subject category (direct quotes have quotation marks, while the paraphrased statements do not). Each quote or paraphrased statement is attributed to the participant from whom it originated by means of the participant designations (e.g., P3, P17, P22) used in this study.

Some quotes appear multiple times in different categories.

I. Entering authentication elements

A. Entering authentication elements > Passwords

1. Entering authentication elements > Passwords > Mistyping passwords

a) Entering authentication elements > Passwords > Mistyping passwords > Mistyping passwords is a common problem

- *P3, P12, P14, and P23 all mention the problem of mistyping passwords in general terms.*

b) Entering authentication elements > Passwords > Mistyping passwords > The longer a password is, the easier it is to mistype

- *"I notice here, much more than other places where they only ask for an eight-character password. I tend to fat-finger it more. […] That's*

when I went out and then had to come, so of course I had to lock it again. And then come back in again and I fat-fingered again." (P2)

- *P23 says entering long (12-character) passwords can be difficult, fat-fingering is likely to occur, and this causes frustration.*

c) Entering authentication elements > Passwords > Mistyping passwords > Slowing down and putting in conscious effort when entering a password reduces the likelihood of typos and other mistakes

- *"I probably mistype it at least once every day. But again, I know what it is and I just need to either slow down. It's easy to fat finger, especially on a laptop keyboard. Maybe if I had an ergonomic one I'd type better." (P9)*

- *"It was really fascinating to have authentication fully in my consciousness as opposed to just kind of background and automatically happening. I think I typed – I made fewer typos. So there may be something about that too. I think I actually made fewer typos because it was getting 80 or 90% of my brain instead of, like, two or 3%." (P5)*

d) Entering authentication elements > Passwords > Mistyping passwords > Being watched or thinking too hard when entering passwords makes mistyping more likely

- ***"****I usually don't misspell my passwords that – I don't know. When I was trying, when I was conscious of it, I was a little more [inaudible 03:55]." (P12)*

- *"I was thinking like when I mistype passwords, usually it's only if I'm trying to login when somebody is sitting next to me. I'm either trying to type fast, or checking to see if they're watching, and that's usually when I end up having to retype my password. But other than that, I think that in all other circumstances, I don't end up mistyping." (P10)*

e) Entering a password into a system while it is loading may cause it to miss some characters being typed

- *“Now if the endpoint, this came up one time, where the endpoint and checkpoint encryption thing or whatever, for whatever reason sometimes it just kind of lags behind and you are forced to conscientiously type that thing that you know really, really, really well, very slowly and explicitly and then I would mess it up. […] sometimes there is a lag with the initial log-in screen, whatever a full disk encryption thing they have is called checkpoint endpoint security, it's the thing that pops up. Occasionally, it just seems to be running slow where it doesn't keep up with you when you are typing. And so you get to that and you have typed it like you normally do, you hit enter and somehow it's missed a couple of letters and so you can't log in and then you have to go back and literally do it so slowly and wait for it to catch up, you know, the little stars to appear. And when that happens, I usually mess up two times and then like it's very painful to do it the third time because you really, really, really have to pay attention.“ (P11)*

f) Entering authentication elements > Passwords > Mistyping passwords > Touchscreens on mobile devices make it difficult to enter passwords correctly

- ***“****There's a few times [mistyping a password], with the Blackberry, because it's touchscreen. If my hand gets wet, or something, and if I'm in a hurry, and I can't get the password in, it gets a little frustrating.*

  “In that 24-hour period I didn't actually experience that. I did want to say, that it does happen with the Blackberry. With the touchscreen, there's times, trying to enter it, that it's frustrating and you can't get it to enter correctly.” (P15)

2. Entering authentication elements > Passwords > Forgetting passwords

- *“All I had to do was go in quickly, electronically sign a form and send it on. It took me half an hour because I forgot the password.” (P15)*

- *“And e-Approval is something that I use so infrequently that each of the past few times I've had to do something in there, I've had to get my password reset, and it is very embarrassing.” (P11)*

- *“I don't remember exactly when it was, but I know I just had changed my password for a SafeBoot, and I just couldn't find where I'd written it down, and I couldn't get it right on the first ten tries.“ (P14)*

- *“Once again security has gotten in my way and it takes me extra time because now I got to look that one up because I don't use that one often enough.” (P17)*

- *“Yeah, I used to add an abbreviation to the end for each different system, but once in a while I'd forget how I'd abbreviated it.” (P14)*

B. Entering authentication elements – ID badge for physical entry

1. Entering authentication elements > ID badge for physical entry > Having consistency in how one authenticates to particular applications can help make the action automatic

    - *“[T]his that requires a hard key. When that door was shut, you have to open it with a hard key. I tried to badge into it. I held my badge up to the door, I wasn't even thinking and, again, just as an example of how when it becomes automated, you don't even think about it.” (P11)*

2. Entering authentication elements > ID badge for physical entry > It is difficult to “badge in” to a building while holding things

    - *“I fold the wallet here, and coffee, and I'm trying to hold the badge up. And then it will beep, and then I'll pull it away. And if I don't open the door in the next two seconds, I have to do it all over again because I kind of re-position myself. There's limited light. So that's kind of weird, just the sort of mechanics of it. I mean, if I hold it up to the reader and then I put things back, or I don't go in right away, it will lock me out. I have to do it all over again.“ (P12)*

3. Entering authentication elements > ID badge for physical entry > Having to show ID to a guard to get onto the NIST campus delays the start of the working day

    - *P17 says that having to show his/her ID to guards the NIST Campus gates to gain entry delays the start of his/her working day.*

C. Entering authentication elements > Biometrics

1. Entering authentication elements > Biometrics > Fingerprint readers are not reliable

- *“This one is worse, because it works by a biometric, and my finger doesn't read very well. I have to smear it with moisturizer, and then I forget what the actual password is. When it really just won't read my finger, I can't unlock it and I can't remember.” (P2)*

D. Entering authentication elements > RSA token code (to log into NIST VPN)

1. Entering authentication elements > RSA token code (to log into NIST VPN) – Logging in with the RSA token is time-consuming and effortful

- *“And then the fact that I was realizing that you have to do it so many times. You have to log in. First I have to log in to decrypt. And then, I have to log in to actually start the computer. Then I have to log in to connect to the wireless network. […] You have to put in name and password three times before you're fully hooked up. If something goes screwy without luck, you have to do it four times because you have to do it once to decrypt, once to enter in, and then once to connect to the wireless.” (P2)*

- *“For the e-mail, when I was at home, if I don't do anything on the Web page for five minutes or 10 minutes, it will log me out automatically. Which that can get frustrating because then I have to close the browser, open it up again, use the RSA key, hope I get it right the first time. And I can do that 15 or 20 times throughout the day. And a lot of times I'm just so tired of re-logging in, I'll just stop checking my e-mail. I might do it once every three or four hours instead of every 20 minutes.” (P19)*

- *“If I was home and doing that, I would get a lot more irritation. Because in order to get into webmail, you have to put in your name, password and the PIN, and the secure ID, and your name and domain, and your domain name as well. It takes like probably about 20 seconds just to put the stupid information in. And then if you get something wrong, it blanks all the fields again […] That's just irritating.” (P2)*

- *“It's a bit stupid. Well, the token is a great idea I think, but the way the webmail account is done here is I have to give, of course, my user name. I have to give my password that I use at least, but also when I use a token there is... The token has two parts. One is the PIN number which doesn't change and all these numbers that changes every minute.” (P18)*

- *“It's this extra, again, effortful stuff. I have to dig around in my bag and get the RSA ID token out and then set it on my laptop and then type out the number, make sure that you're not typing it right before changes or as it's changing or whatever. And it's not something that you just have memorized that you just can do automatically. Again, it's that sort of effortful, "I have to get the device. I have to look at it. I have to copy what it says into my computer, and then enter my password." If it was just me entering my password it wouldn't be as big of a deal. […] It's that deliberate effortful, conscientious...I really have to stop what I'm doing and think about it. Whereas if you're just doing something from muscle memory, you don't really even have to think about that.” (P11)*

2. Entering authentication elements > RSA token code (to log into NIST VPN) – Some physical aspects of the RSA token make it difficult to use

    - *“I have to dig around in my bag and get the RSA ID token out and then set it on my laptop and then type out the number, make sure that you're not typing it right before changes or as it's changing or whatever.” (P11)*

    - *“These are very low-resolution. You have to have bright light. It's frequently misread. […] If you make a simple mistake, which it is easy to do. Sevens can easily be ones. Sometimes twos look like eights. If you make a mistake, then of course you've got to reenter... [...]There aren't clear signs on it to indicate which way it ought to be held and viewed. It looks like it's intended more to be held with you left hand than right.” (P21)*

3. Entering authentication elements > RSA token code (to log into NIST VPN) – The number on the RSA token changes every minute

    - *“It changes every minute. So sometimes I'll be a little bit late, and it will be like, "OK, your pass code is invalid," because it had changed. And I*

had to type in my user name twice, my password, and it's just a lot of stuff to do. And I often make typos, so... And even if this thing still has a minute left on it, I have to wait another minute because it kind of skips that step in the pass code chain or whatever, however it works." (P19)

- *"It's a bit stupid. Well, the token is a great idea I think, but the way the webmail account is done here is I have to give, of course, my user name. I have to give my password that I use at least, but also when I use a token there is... The token has two parts. One is the PIN number which doesn't change and all these numbers that changes every minute." (P18)*

II. Managing authentication elements

A. Managing authentication elements > Passwords

1. Managing authentication elements > Passwords > Password change

a) Managing authentication elements > Passwords > Password change > Password policies vary across applications, which can make it hard to keep up with all the elements one is supposed to manage

- *"Yeah, it can be a pain. And when I'm here, everything I log into, the password policy is completely different. So even if I wanted to, the password can't be the same. Some of them have to be eight characters, some of them have to be 12. So it can't be anything more than 12. So some passwords I have are 20 characters, some are 6. And it's just hard to remember everything, so I actually load a file on my computer that just has every password listed so I can just copy and paste it." (P19)*

b) Managing authentication elements > Passwords > Password change > Password change intervals are too short for infrequently used systems

- *"And e-Approval is something that I use so infrequently that each of the past few times I've had to do something in there, I've had to get my password reset, and it is very embarrassing." (P11)*

- *"I don't travel very often, but when I do I have to log in to something called Travel Management. And that password expires just as fast as*

any other password. Every single time I go to log in to submit my expense reports, first of all, my account is locked because I haven't changed my password in a few months. So then I have to figure out how to unlock it. Then I've got to go change it." (P19)

- *"[T]he first time I have logged in at the airport, I guess, then I got the message, "Oh, change your password, it will expire in two days." I am thinking I am out of town; I am not changing right now. I don't want to have to deal with that. Where am I going to write it down. And then the next day it's "Password is expiring in one day." Then I was trying to change it and I got interrupted by something or something, I don't remember, I'd have to look back at exactly what happened. But it's just that fact that you have to change it so much more frequently for Time and Attendance." (P11)*

- *"[W]hen I started getting into the WebTA thing, it just so happened that it was time to change my password and WebTA makes you change your password more frequently than the NIST general domain. And every time I have to do that, I get really frustrated because I am like why can't they always be in sync. You have to think if you are going to be the responsible person, then you have to think of different passwords for everything and it is very frustrating. So when it gets to those infrequently used passwords, then I get really irritated." (P11)*

c) Managing authentication elements > Passwords > Password change > It can be difficult to remember a password one has recently changed/created

- *P18 says if he changes his password at the end of the week, he has a hard time remembering it on Monday. Otherwise after using the new password a couple of times, of entering, he is fine.*

- *"[T]hat's when I had the most trouble. I remember my passwords pretty well, but after I change it I need to write it down on a cheat sheet for a little while. Especially with some things like the disk encryption on the laptop. If you type the wrong password more than three times it starts delaying authentication, it starts with one minute, goes to two minutes, then four, and pretty soon you are just shut out." (P14)*

d) Managing authentication elements > Passwords > Password change > Creating a new password that complies with password policies is difficult

- *“Plus, they have to be punctuations and numbers. I use a password scheme with a slight variation, so that no one password is the same. The problem is that different secure sites have different requirements for passwords. Some of them require punctuation marks. Some of them forbid punctuation marks. So I can't even use one secure password base on all of my accounts. It's very frustrating. I manage most of my passwords by writing them down on paper.” (P7)*

- *“Then I've got to deal with finding a new password that works according to that website's password policy.” (P19)*

e) Managing authentication elements > Passwords > Password change > Reminders to change one’s password are annoying

- *“So it happens every 90 days. Actually, that's a misnomer too. They tell you it will last up to 90 days. But they start reminding you 20 days early. […] But they don't tell you, "Hey, we just thought if you are taking the next two weeks off, you might want to change it now." They don't say any of that. […] They just stick it in your face.” (P23)*

2. Managing authentication elements > Passwords > Resetting passwords

a) Managing authentication elements > Passwords > Resetting passwords > There is a confusing time lag between the creation of a new password and that new password becoming valid

- *“First I tried to login three times. Got locked out of my account. But then an administrator had to do something on there to clear that so that I could then try again and then were quite serious about my password. And once I requested to reset my password, the e-mail didn't get sent immediately. There was like a 20 minute lag. And I expected it to be sent right away. So I was like trying to login and request the request to reset it. Then I got locked out again. So I had to start over with requesting to the Admin that they clear that so that I could start again.” (P10)*

b) Managing authentication elements > Passwords > Resetting passwords > Getting a password reset is time-consuming and effortful

- *“[L]ast time I needed to sign something, I don't remember if it was a travel voucher, it was something I needed to sign. So the secretary e-mails me, tells me it's ready for my signature and e-approval. I put it off because I know I don't have time to deal with the password reset, I don't have time to do that right now, I will do it at the end of the day and then it's too late because you can't call because they are not there to reset the password for you. And so this drags out over the course of maybe a week or longer and then she in the meantime has taken the time to send me another reminder e-mail, and then I feel bad because I am wasting her time. But I just couldn't get it done because I couldn't remember the thing and I didn't have the time allocated to do the whole reset thing. And I know that sounds silly, because you're like, "How long can a phone call be?" But it takes time and especially when you have to wait for them to do. […] Especially when you have to wait for them to generate the thing, and then you have to go downstairs and pick it up. I mean that's just a whole category on its own. […] Because it has rippling effects. You know, it wasn't just affecting me, it's affecting people that I am calling. […] It's affecting her trying to send me these reminder e-mails and whoever else is doing budgeting, I haven't signed for the thing yet. I mean it really has this kind of ripple in the pond effect.” (P11)*

- *“The time cost to authenticate, if it's this automatic, non-effortful thing is minimal and I don't pay attention to it, it doesn't really frustrate me. If it is a large time cost, like me having to call and get my password reset and then you have to wait for them to generate this letter and then you have to go downstairs and pick it up, and it's like this really extended evolution. That is in a category all its own, it's very special.” (P11)*

c) Managing authentication elements > Passwords > Resetting passwords > Password synchronization does not always work the way one expects it to, which leads to authentication problems

- *“I have with the Time and Attendance, and our training software, which for some reason doesn't sync. I don't know why the training software doesn't sync our training log. I've locked myself out of that, which turned out to be a massive problem, because we created them with a second username.” (P2)*

- *“I've locked myself out on another thing. You go in. And to do the password you go to a website that supposedly syncs it. And it doesn't really sync it. The T and A system has a different password, and the travel system has a different password. […] Because apparently our computers can't pass credentials to the wireless system, although it is synced to the same password and username. You have to put it in again.” (P2)*

- *“Once you get onto the NIST network through the secure client server, then if you change your password it can update it with the NIST servers. If I change my password before I connect to the NIST network, it changes on my laptop, but on the NIST servers, it doesn't change until I reconnect to the network and they can sync up.” (P15)*

- *“So there's the confusion of is this our BizFlow password? Is it our general realm password? Is it our Entrust password? Then they enter the password wrong. Then they think they need the password reset, but they don't because it's not actually the Entrust password that they're entering. So it's a big mess that way. […] Most users will say, "This is my e-Approval password." But e-Approval is a combination of now two different passwords, the general realm password and the Entrust password. But people think, "My e-Approval password," which will easily get them confused.” (P3)*

B. Managing authentication elements > PIV card

1. Managing authentication elements > PIV card > It’s bad to leave one’s PIV card in the card reader, but it’s hard to avoid doing so

    - *“I actually don't use my PIV card here at work because I forget it in the computer a lot. If I leave the building, I can't get back in because that's*

also my access back into the building.[17] *[…] But this thing, it's just a tiny, nearly weightless piece of plastic that you often forget about. So I would forget this every single time. And I've been locked out of the building. I've been locked out of the floor. I've been reprimanded for leaving this in the computer. And there's nothing I could have done other than somehow setting reminders every two minutes to don't forget this." (P19)*

- *"When I stand up to leave, I would forget and leave my... Unless it's attached to me, I know exactly what's going to happen. My card's going to be in my system and I'm going to be locked out of the building. I'm going to run an errand or something, and get back, and realize, "Oops, I left my card in my laptop."" (P15)*

2. Managing authentication elements > PIV card > It's easy to forget the PIV card somewhere – and then it will just be too much trouble to go get it, even if you need it to do something.

    - *"Yeah, because not only do I have to have a computer and the password and PIN known, I have to have this thing physically with me. If I forget it downstairs or in my car or at work, I can't log in. I have to go downstairs or go to my car or go back to work to pick it up. […] I'll forget it in my car all the time. Sometimes I'll go get it, sometimes I'll just not check my e-mail." (P19)*

III. Authentication's impact on primary tasks

A. Authentication's impact on primary tasks > Authentication takes up a significant amount of time each day

- *"And it gets in the way. It definitely takes way more time out of my day, both just time having to deal with this and then the break in the flow of work." (P19)*

[17] Most NIST users with a PIV card still have a separate ID/physical access badge, but this participant had only the PIV card.

- *“But it's one of those things, if I spend eight hours logging into my e-mail, I'm not going to have any time to do any work. So I'd rather be doing the actual work than waste my time logging in every five minutes.” (P19)*

- *“In my attention it's a tiny blip, but time wise, I think it does actually still take a lot of time. There's a substantial amount of time. Although, you know – and I guess this is why you have to do studies for more than just one day at a time or something like that, but there are a lot of systems that I thought I was going to use on that Wednesday that I didn't end up using. And – for instance, if we had had an actual operational emergency or some sort of situation where I'd actively have to solve a problem to restore our system, I'd probably have to go into my password safe, dig out a few old passwords and things like that which would have completely slowed down the process.” (P5)*

B. Authentication’s impact on primary tasks > Authentication interrupts and distracts from the primary task

1. Authentication’s impact on primary tasks > Authentication interrupts and distracts from the primary task > Sometimes it takes so long to find one’s RSA token that one can forget what one was logging in to do in the first place

    - *“The idea was that once I had to stop and look in a bag for something like that and I'm not on my computer. I don't have three windows open. I can't do something else while waiting to login. So actually taking the time away from the computer, I walk to get my bag. Someone else stops me in the hallway. I have a conversation with them. Then soon I go back and I remember to login, but I'm like, "Oh." The strong idea I had in my head of a message that I wanted to send might have become a little more fuzzy, the idea of what I was doing. "Why did I open that other new tab and not go to the..." So there's the little things. I feel like those little things really, when you have an idea of what you want to do next and then you have to deviate from that, I think at least for my brain it throws you off a little bit.” (P3)*

2. Authentication’s impact on primary tasks > Authentication interrupts and distracts from the primary task > Authentication is a major distraction at conferences

- *“It sounds stupid to me that everybody around me gets to watch me type my 12-character password in 15 times during the conference because it times out every 15 minutes. But evidently that's not important. [It’s] not just the embarrassment, but actually I mean, if I sit next to you... If he doesn't know by the end of the conference what your password is because you've retyped it umpteen times… So it is both. If I fat-finger, then it's a few more.” (P23)*

3. Authentication’s impact on primary tasks > Authentication interrupts and distracts from the primary task > Having to re-authenticate multiple times breaks the flow of work

    - *“And it gets in the way. It definitely takes way more time out of my day, both just time having to deal with this and then the break in the flow of work.” (P19)*

    - *P18 says re-authentication can break one’s thought process.*

    - *“So basically every time I go to use the computer, which means I have a thought or something that I'm trying to keep in my head, it's locked up, and now I have to remember this 12-character password so that I can then get to what I'm trying to do to write a quick note to remind me of something.” (P23)*

    - *“You end up having to almost set a timer in your head to go back to the computer and type something within every 10 minutes or so. And some minor studies of productivity I've been involved with indicate that it's better to be focused on a task as opposed to have lots of interruptions throughout the day.” (P21)*

C. Authentication’s impact on primary tasks > Timed lockouts

1. Authentication’s impact on primary tasks > Timed lockouts > Timed lockouts interfere with work on multiple computers

    - *“The most annoying thing is, because I have several computers, and I tend to work... Let's say, I write on one computer and I program on another one, and so I tend to switch between them. Every time I switch, I have to log in because I have this 15 minute...” (P18)*

2. Authentication's impact on primary tasks > Timed lockouts > Timed lockout disconnects remote users from VPN, necessitating re-authentication

    - *"For the e-mail, when I was at home, if I don't do anything on the Web page for five minutes or 10 minutes, it will log me out automatically. Which that can get frustrating because then I have to close the browser, open it up again, use the RSA key, hope I get it right the first time. And I can do that 15 or 20 times throughout the day. And a lot of times I'm just so tired of re-logging in, I'll just stop checking my e-mail. I might do it once every three or four hours instead of every 20 minutes." (P19)*

    - *"Wednesday, when I recorded things, I was working from home and I was using my Mac laptop, and recently we were all forced by the NIST security policy to have the Mac centrally managed. That meant some encryption software being put on the system. Then the system times out fairly frequently and it also reboots if you leave it unattended for roughly 45 minutes or so. That added significantly to the amount of re-authentication I had to do. I have known for awhile that authentication issues have become excessively burdensome, I think. They are for everybody, I think, regardless of what you're doing, whether it's work or..." (P21)*

3. Authentication's impact on primary tasks > Timed lockouts > Logging out to avoid timed lockouts terminates all processes on a Mac

    - *"Yeah, and logging out is bad. Logging is out is bad because it... There's such a thing as... If you walk away from here you aren't logged out. Your account is locked, in a sense, and you press "Control - Alt - Delete" and you can get back in. On a Mac, logging out is a different thing. It means all your processes and things you had up on the screen are now terminated." (P21)*[18]

[18] This participant may be conflating "logging out" of a user account with "locking" it – the two functions do different things. "Logging out" on both Windows and OSX terminates any active processes started by the user. "Locking" a computer keeps user processes running, but they will not accept input until the computer has been unlocked. On a Mac, this option is called "sleep."

4. Authentication's impact on primary tasks > Timed lockouts > Timed lockouts make it more difficult to use laptops

    - *"But the computer locks, screen locks more often if you are idle more than five minutes. So that's an annoying thing. So I only use this for not a lot of tasks, because my main computer's here and then whenever I need to go over there, it's always locked. So I have to authenticate. So I try not to use that too much." (P4)*

5. Authentication's impact on primary tasks > Timed lockouts > Timed lockouts disrupt presentations

    - *"I'd have 150 people waiting for a presentation. I'm waiting for 15 minutes for that sucker to boot up, so I can actually use it. Then, because I'm not admin[istrator] and I can't change any setting on that box, when the screensaver kicks in, then I've got to log it all over again and reinitialize everything and start my presentation all over again and figure out where I was in the 120 slides that I use and make my way there. All the time the audience is - right? That's a combination of security and other miscellaneous things. But, like I said, it gets in the way. You're trying to do something, which should be straightforward, but you can't." (P17)*

6. Authentication's impact on primary tasks > Timed lockouts > Even preventing timed lockouts is distracting

    - *"Yes, I'm trying not to log in that often. And also, if I am logged in, I'll keep going in. Hitting 'check mail' just to make sure it doesn't time me out. And then if I don't need to, you go and you hit 'check mail.' And it blanks you out. Then you have to close the browser. Go in to reopen it, and then sign back in." (P2)*

    - *"You end up having to almost set a timer in your head to go back to the computer and type something within every 10 minutes or so. And some minor studies of productivity I've been involved with indicate that it's*

The participant was probably unfamiliar with how to "lock" a Mac. Since NIST Macs were not configured with a timed lockout until shortly before this study, the participant never had a reason to try to preemptively lock his/her computer (or, rather, put it to sleep), and logged out by accident the first time he/she tried it.

better to be focused on a task as opposed to have lots of interruptions throughout the day." (P21)

D. Authentication's impact on primary tasks > Authentication problems can lead to primary task failure

1. Authentication's impact on primary tasks > Authentication problems can lead to primary task failure > If something is wrong with the authentication for a particular application, it's impossible to use that application

- *"Well, yeah, I was just trying to do a little work over the weekend. I reflected on something I was working on, and thought of how to solve the problem, and tried to log in and couldn't." (P14)*

2. Authentication's impact on primary tasks > Authentication problems can lead to primary task failure > Even coping mechanisms may not prevent major authentication problems that cause primary task failure

- *"I don't remember exactly when it was, but I know I just had changed my password for a SafeBoot, and I just couldn't find where I'd written it down, and I couldn't get it right on the first ten tries." (P14)*

- *"I ended up having to change a password that day because I got locked out of an account. The reason that happened was because I had switched computers, where before, I was relying on the browser for my password. So I went to the new laptop, I didn't remember it, and I had no way of getting the password other than resetting it. The other computer was gone." (P10)*

E. Authentication's impact on primary tasks > Authentication creates delays and slows work down

1. Authentication's impact on primary tasks > Authentication creates delays and slows work down > Sometimes authentication takes longer than the primary task it is supposed to enable

- *"All I had to do was go in quickly, electronically sign a form and send it on. It took me half an hour because I forgot the password." (P15)*

- *“It might take me two hours to actually get back in. The actual time I'm spending dealing with the website, it can be anywhere from five minutes to 15 minutes.” (P19)*

- *“One of the aspects of security is here they have fixed IP addresses. I can't plug my laptop into our wired network, even though it's a NAIS registered computer. Can't do that, because it's on the fixed IP address. And none of the printers are connected to the wireless except for that one, are connected to the wireless printer. That one's physically connected, so you can print it. I can't print on our big printers, unless I log into this one again. I have to keep two computers running. Well, that's inane. I had been keeping notes of a meeting in someone else's office, and I'm on NAIS NET. And we were like, "OK, so we can print it off." What you had to go through to print the damn thing off! Because we couldn't hook my computer up to his printer, the wireless network doesn't access printers. And we couldn't just hook, what you would do anywhere else, which is unhook it from the back of his computer and hook it into yours. […] And it wouldn't do it. You can't do any of that, which just drives me crazy. Instead, we have to eventually e-mail it.” (P2)*

- *“So basically every time I go to use the computer, which means I have a thought or something that I'm trying to keep in my head, it's locked up, and now I have to remember this 12-character password so that I can then get to what I'm trying to do to write a quick note to remind me of something.” (P23)*

2. Authentication’s impact on primary tasks > Authentication creates delays and slows work down > Authentication delays critical, time-sensitive primary tasks

    - *“In my attention it's a tiny blip, but time wise, I think it does actually still take a lot of time. There's a substantial amount of time. Although, you know – and I guess this is why you have to do studies for more than just one day at a time or something like that, but there are a lot of systems that I thought I was going to use on that Wednesday that I didn't end up using. And – for instance, if we had had an actual operational emergency or some sort of situation where I'd actively have to solve a problem to restore our system, I'd probably have to go into my password safe, dig out a few*

old passwords and things like that which would have completely slowed down the process" (P5)

- *"So a situation where authentication has been a real challenge and caused real problems, there's one example I can think of where I have a system that had completely failed, and I had to restore the system from a backup, a procedure that I've done a few times, works flawlessly without any problems. In this particular case there was some...just call it a bug that interfered with restoring the passwords to this device. These are root-level passwords, very low-level and basic passwords you log in to control a system, basically, the only account on this device, right? There's one account and it's super-user, super-privilege. That password had not been properly been reset, or it was...I think it was actually reset to a very, very, old password that...in hindsight it was a very, very old password, and it took me about three hours to figure out that that was the password that was in place and that something had happened in the configuration, and it restored a really old password or something like that. So that was very, very frustrating. The cost was actually high then. We had three hours, or two hours, of complete network failure of major component of our network, a major section of our network. So the cost was actually very high there, and it was all because the expected outcome of a restore didn't happen that way. […] the real cost is with all the people that are not able to use their systems and get their work done." (P5)*

F. Authentication's impact on primary tasks > Authentication can require an unreasonable amount of time and effort

1. Authentication's impact on primary tasks > Authentication can require an unreasonable amount of time and effort > VPN login is complicated and takes a long time, especially if one fails to log in on the first attempt

- *"And then the fact that I was realizing that you have to do it so many times. You have to log in. First I have to log in to decrypt. And then, I have to log in to actually start the computer. Then I have to log in to connect to the wireless network. […] You have to put in name and password three times before you're fully hooked up. If something goes screwy without luck, you have to do it four times because you have to do it once to decrypt, once to enter in, and then once to connect to the wireless." (P2)*

- *“For the e-mail, when I was at home, if I don't do anything on the Web page for five minutes or 10 minutes, it will log me out automatically. Which that can get frustrating because then I have to close the browser, open it up again, use the RSA key, hope I get it right the first time. And I can do that 15 or 20 times throughout the day. And a lot of times I'm just so tired of re-logging in, I'll just stop checking my e-mail. I might do it once every three or four hours instead of every 20 minutes.” (P19)*

- *“If I was home and doing that, I would get a lot more irritation. Because in order to get into webmail, you have to put in your name, password and the PIN, and the secure ID, and your name and domain, and your domain name as well. It takes like probably about 20 seconds just to put the stupid information in. And then if you get something wrong, it blanks all the fields again […] That's just irritating.” (P2)*

2. Authentication’s impact on primary tasks > Authentication can require an unreasonable amount of time and effort > Logging in with the RSA token is particularly difficult because it always requires going out of one’s way to look something up

    - *“It's a bit stupid. Well, the token is a great idea I think, but the way the webmail account is done here is I have to give, of course, my user name. I have to give my password that I use at least, but also when I use a token there is... The token has two parts. One is the PIN number which doesn't change and all these numbers that changes every minute.” (P18)*

    - *“It's this extra, again, effortful stuff. I have to dig around in my bag and get the RSA ID token out and then set it on my laptop and then type out the number, make sure that you're not typing it right before changes or as it's changing or whatever. And it's not something that you just have memorized that you just can do automatically. Again, it's that sort of effortful, "I have to get the device. I have to look at it. I have to copy what it says into my computer, and then enter my password." If it was just me entering my password it wouldn't be as big of a deal. […] It's that deliberate effortful, conscientious...I really have to stop what I'm doing and think about it. Whereas if you're just doing something from muscle memory, you don't really even have to think about that.” (P11)*

G. Authentication's impact on primary tasks > The prospect of dealing with authentication discourages the use of course materials and other resources

- *"Once again security has gotten in my way and it takes me extra time because now I got to look that one up because I don't use that one often enough." (P17)*

H. Authentication's impact on primary tasks > Sometimes authentication encourages one to stay focused on a primary task for longer

- *"I mean, I might have continued longer than I normally would have so I wouldn't have to go back in and do it, possibly. But in a larger sense, it wouldn't, other than being an interruption. But I guess I would have stayed longer at a task rather than say going down the hall. Because I'd have to go back and do it." (P12)*

- *"I think in some ways this is actually a good thing for things like my Facebook account. So, on my NIST computer I wouldn't store my password, to add a little more friction to logging in so that I wouldn't do it. So I guess that's one. But that's kind of a benefit that it keeps me from getting distracted. […] And also, I noticed when I was going between the two laptops, so basically one of them was the only one I could use to access the Internet, and the other one was the one I was writing on. Since I locked the screen in-between times, it would keep me more focused on the writing because I wouldn't want to login and get going on the other machine, just to do a quick Google search, for example. I guess it's enough of a burden, but it made me change my work habits." (P10)*

IV. Coping mechanisms

A. Coping mechanisms > Password creation techniques

1. Coping mechanisms > Password creation techniques > Using a systematic method to create new passwords

- *"I used to write down the password for everything, and I recently switched, last year I switched, to the system where I have a system for the passwords. […] Well, basically, the ones that I use the most and the ones*

that I have to change, I do under new system. But the ones that I don't use often and I didn't have to change them, they're still written down." (P18)

2. Coping mechanisms > Password creation techniques > Employing a memorable sentence as a password mnemonic

    - *"I created a sentence. And then I can remember the sentence and use that as a device to remember what the actual password is." (P2)*

    - *"So instead, if I now have the ability to say, "Take a random phrase from a list of song lyrics," or a title of a song and they put some symbols on either side. Things that will be useful to the user and they have to remember less and can be more secure. I think that's an amazing direction." (P3)*

3. Coping mechanisms > Password creation techniques > "Chunking" a password into segments to make it easier to remember and manage

    a) Coping mechanisms > Password creation techniques > "Chunking" a password into segments to make it easier to remember and manage > Using coded password hints as a "key" to remember password segments

        - *"But if I had multiple phrases, then what I'll do is I'll switch them up, and then the password hint I will make a cryptic hint. I don't use these actual phrases, but to use an example, if it's D!#, or something like that, and then for D is my date of birth, ! Is some other phrase that I know, # is some other phrase that I know. And reusing those in combination allows me to have the password hint when that's available as an option, tell me what the cryptic phrase is." (P3)*

    b) Coping mechanisms > Password creation techniques > "Chunking" a password into segments to make it easier to remember and manage > Basing a new password on the previous one by varying some segments while keeping others the same

        - *"Some of my passwords, when I change them, I'll just have one number that will change. So it's like "applesauce5," next time it will be "applesauce6."" (P19)*

- *“When I do have to change my passwords, I don't typically change them to something drastically different than what I had. If I can change a couple characters, I do, and get away with it, if you will. I try to relate them to a commonality. All of my passwords, regardless of what I'm logging into, have some reference to something that I always will remember. I don't want to tell you exactly...” (P9)*

- *“You can append things on the end in an ordered fashion, or append things on the beginning or better yet, both the end and the beginning. But, if you do that while keeping the root, called the root word or root phrase, I mean I do use the fancy, "think of a phrase, and then you take the first number and then you switch out special symbols for the A's" and all that sort of stuff.” (P11)*

4. Coping mechanisms > Password creation techniques > Creating passwords that are easy to type

    - *“The other thing I try to do is I try to figure out what feels natural when I'm typing. I have come up with passwords that I am constantly not typing right. To me, I can recall that password, but I can't type it worth a darn, consistently well, so I just reset it to something else. Because you have to have a capital letter, so if you're hitting shift and the capital letter first and that's better for you than half-way through typing you have to hit shift and a capital letter, if that's messing you up then move it to the last letter or the beginning letter or whatever.” (P9)*

5. Coping mechanisms > Password creation techniques > Using one’s birthday (or other memorable date) for PIN creation

    - *“And then I type in my PIN, which is my six-digit PIN. […] Which I can remember because it's my birthday.” (P12)*

6. Coping mechanisms > Password creation techniques > Creating the password for the application with the strictest policy first, then using that password for all other applications

    - *“Other than that, centralizing it and creating the strongest password for centrally possible has been my tactic. Try to get it all in one bucket.“ (P3)*

- *“We go to the password that has the most strict requirements, and if you can get a password to work there it'll work everywhere else. Assuming that you already know that you've got the right punctuation that will work and stuff. E-Approval is one of the ones that has the most strict requirements for EnTrust passwords, and that's great. I always start there when I have to reset. If that one takes it, I'm safe everywhere else.” (P9)*

B. Coping mechanisms > Technological solutions

1. Coping mechanisms > Technological solutions > Employing non-password authentication mechanisms

a) Coping mechanisms > Technological solutions > Employing non-password authentication mechanisms > Biometric systems

- *“Biometrics, it would not be bad, except that it doesn't like my finger.” (P2)*
- *P23 uses a biometric fingerprint reader.*
- *“We have to go to some sort of a single sign-on using biometrics. Enough of this business of trying to remember passwords and draw up rules for passwords that are designed to secure stuff when passwords themselves are not secure.” (P17)*

b) Coping mechanisms > Technological solutions > Employing non-password authentication mechanisms > PIV card reader

- *“Because I'm in the computer security division, I do understand the need for the security. But the places where I've used card readers, I find those are just easier. Because all you need to remember are four digits. And it's physical.” (P2)*

2. Coping mechanisms > Technological solutions > Using a password manager or vault

- *“Firefox has a password storage scheme where it will remember many passwords for you. You can lock them all with one key. When I start up the Firefox, it immediately asks me for the key. Then for all of that session it will fill in passwords for me with any website that I visit.” (P6)*

- *“It sits up here, as a browser extension for Mozilla or Chrome. I click this. Currently, I'm logged in. I had to log in for my master password this morning. It will automatically fill the form fields. But it stores things encrypted. I have it on my phone as well. It's very accessible.” (P3)*

- *P19 uses a password manager: KeePass Password Safe.*

- *P23 uses an IronKey (a secure USB drive) to cope with authentication.*

- *“The other thing I found out is, I didn't realize how many passwords I had memorized. I keep them in an encrypted vault, because it got so difficult to memorize those, then I only have to remember one really good password, and I can go get...” (P15)*

3. Coping mechanisms > Technological solutions > Keeping passwords cached in a Web browser (e.g., Firefox, Internet Explorer)

    - *“I guess it was a surprise how much I really leverage cached credentials and how much I couldn't live without them, where everything, all of my passwords are stored somewhere already. And I completely depend on – I really depend on one or two passwords to protect most of them. That was a – I've known that for years, and I try to protect my passwords really well, but that was a surprise, realizing that almost every authentication I made was actually stored somewhere for me. And I couldn't live without that. If I had to truly authenticate every single time I went in to check my e-mail or every single time I wanted to log into – well, mainly e-mail. E-mail's a big one, or instant messenger or something like that. I wouldn't do it as much. I wouldn't use three different instant messenger clients, you know – Yahoo and AOL and G Talk. I wouldn't use them all. I would really limit myself.” (P5)*

    - *P12 keeps some of his/her passwords in the browser cache.*

    - *P17 has some passwords stored in his/her browser cache and others written down.*

C. Coping mechanisms > Keeping a list of passwords for reference

1. Coping mechanisms > Keeping a list of passwords for reference > Writing digitally (e.g., in an encrypted Notepad file or Word document)

    - *“I have a one-password file that I just store passwords in plain text, but then that gets encrypted with a really long key that I have to remember. That one file I use to store all the passwords of my whole life and I keep that backed up in a couple of different places.” (P6)*

    - *P9 stores passwords on her phone just in case.*

    - *“Yeah, it can be a pain. And when I'm here, everything I log into, the password policy is completely different. So even if I wanted to, the password can't be the same. Some of them have to be eight characters, some of them have to be 12. So it can't be anything more than 12. So some passwords I have are 20 characters, some are 6. And it's just hard to remember everything, so I actually load a file on my computer that just has every password listed so I can just copy and paste it.” (P19)*

2. Coping mechanisms > Keeping a list of passwords for reference > Writing passwords on paper

    - *“And everything has to get written down because you can't remember. Once you get above five or six then you start writing things down.” (P17)*

    - *“I do keep a hard copy printout of all my passwords in my fire safe at home. So, if things get really desperate, I could go there. But, I feel like I shouldn't keep it in the desk drawer here, which I know some people do, because these cabinets actually don't really lock. I have the keys that you can just pop it right open. So, this one does.” (P11)*

    - *“It [voice-mail] requires a PIN, and the paper is taped onto the phone.“ (P6)*

    - *P12 keeps some passwords written down in his/her wallet.*

    - *P17 has some passwords stored in his/her browser cache and others written down.*

    - *“Plus, they have to be punctuations and numbers. I use a password scheme with a slight variation, so that no one password is the same. The*

problem is that different secure sites have different requirements for passwords. Some of them require punctuation marks. Some of them forbid punctuation marks. So I can't even use one secure password base on all of my accounts. It's very frustrating. I manage most of my passwords by writing them down on paper." (P7)

- *"**Respondent:** Yeah, usually I write down my password when I change it, until I get used to the new one. […] Well, I have scraps of paper laying around with the password written down. **Interviewer:** The question is, do you destroy it, or do you still keep it? **Respondent:** I keep it." (P14)*

- *"[T]hat's when I had the most trouble. I remember my passwords pretty well, but after I change it I need to write it down on a cheat sheet for a little while. Especially with some things like the disk encryption on the laptop. If you type the wrong password more than three times it starts delaying authentication, it starts with one minute, goes to two minutes, then four, and pretty soon you are just shut out." (P14)*

3. Coping mechanisms > Keeping a list of passwords for reference > Looking up passwords in a system for which one has administrative privileges

    - *P14 has administrator rights for some systems, so he/she can look up forgotten passwords on those systems instead of having to reset them.*

D. Coping mechanisms > Organizing, centralizing, and/or consolidating passwords

1. Coping mechanisms > Organizing, centralizing, and/or consolidating passwords > Using a password manager or vault

    - *"Firefox has a password storage scheme where it will remember many passwords for you. You can lock them all with one key. When I start up the Firefox, it immediately asks me for the key. Then for all of that session it will fill in passwords for me with any website that I visit." (P6)*

    - *"It sits up here, as a browser extension for Mozilla or Chrome. I click this. Currently, I'm logged in. I had to log in for my master password this morning. It will automatically fill the form fields. But it stores things encrypted. I have it on my phone as well. It's very accessible." (P3)*

- *P19 uses a password manager: KeePass Password Safe.*
- *P23 uses an IronKey (a secure USB drive) to cope with authentication.*
- *"The other thing I found out is, I didn't realize how many passwords I had memorized. I keep them in an encrypted vault, because it got so difficult to memorize those, then I only have to remember one really good password, and I can go get..." (P15)*

2. Coping mechanisms > Organizing, centralizing, and/or consolidating passwords > Synchronizing one password across multiple applications

- *"**Interviewer:** Right. So which one do you change first? Do you change the main NIST password first and then you change the other ones to keep them on the same...? **Respondent:** Yeah, I change the ones first that I have to, and then when I log into something and notice that it's behind, I update it. **Interviewer**: Right, OK. Do you do all of them in one go or do you basically next time when you need that one, bring it in line with the others? **Respondent:** Yeah, usually next time I need it, I bring it in line." (P14)*
- *"Other than that, centralizing it and creating the strongest password for centrally possible has been my tactic. Try to get it all in one bucket." (P3)*
- *P14 tries to keep the passwords for several different applications the same.*
- *"[W]hen they sent an e-mail to say, "Hey, you have several, you know, how many days to change your password," and so I change it. And then I would go and change everything else so that I would have one password. […] But if one system sent it, I changed it for everything, for everything so that I had to remember only one password. " (P4)*
- *"We go to the password that has the most strict requirements, and if you can get a password to work there it'll work everywhere else. Assuming that you already know that you've got the right punctuation that will work and stuff. E-Approval is one of the ones that has the most strict requirements for EnTrust passwords, and that's great. I always start there when I have to reset. If that one takes it, I'm safe everywhere else." (P9)*

3. Coping mechanisms > Organizing, centralizing, and/or consolidating passwords > Having categories of passwords for different kinds of applications

    - *“From even the experts that I have talked to, it's very rare that anybody does more than three classes of passwords. Usually those are the three, the different variants strengths, often related - not always - but usually longer. Then if one doesn't fit, then they'll either bump it up to the stronger, if it's a requirement, which is really infuriating. Sometimes the system you don't feel calls for that strength.“ (P23)*

    - *“Well, for a lot of my personal stuff, all my banking passwords are the same. I'll have categories, so anything that deals with money is this password.” (P19)*

E. Coping mechanisms > Using alternative channels to reduce or avoid the need for authentication

1. Coping mechanisms > Using alternative channels to reduce or avoid the need for authentication > E-mailing instead of directly accessing a system

    - *“One of the aspects of security is here they have fixed IP addresses. I can't plug my laptop into our wired network, even though it's a NAIS registered computer. Can't do that, because it's on the fixed IP address. And none of the printers are connected to the wireless except for that one, are connected to the wireless printer. That one's physically connected, so you can print it. I can't print on our big printers, unless I log into this one again. I have to keep two computers running. Well, that's inane. I had been keeping notes of a meeting in someone else's office, and I'm on NAIS NET. And we were like, "OK, so we can print it off." What you had to go through to print the damn thing off! Because we couldn't hook my computer up to his printer, the wireless network doesn't access printers. And we couldn't just hook, what you would do anywhere else, which is unhook it from the back of his computer and hook it into yours. […] And it wouldn't do it. You can't do any of that, which just drives me crazy. Instead, we have to eventually e-mail it.” (P2)*

- *“Our administrative assistants no longer allow us to go to the travel website, because we apparently muck it up. This is the reason we say, "They create our names and passwords in those, and then they just log in as us. […] When I was at [another agency], we had this struggle. Our administrative assistant just never let us put our own time in, because she said we screwed it up too much. And she had to spend too much time fixing it. We would just send it to her in an e-mail, and then she would log in as us and put in our time.” (P2)*

2. Coping mechanisms > Using alternative channels to reduce or avoid the need for authentication > Going non-digital whenever possible

    - *“I mean at some point I just got so infuriated that I just started printing out the documents I wanted and carrying them in because I got tired of the stupid 15-minute timeout.“ (P23)*

3. Coping mechanisms > Using alternative channels to reduce or avoid the need for authentication > Checking e-mail on a BlackBerry rather than a computer

    - *“Some people like to get e-mail on their BlackBerry, for example, because they don't have to boot up the computer...“ (P9)*[19]

    - *“It's funny, because I'll sit here and I can do my e-mail on my desktop, but most of the time, if I'm working on a document or something, I just have the Blackberry in front of me. It typically gets e-mail before I get it on my desktop. I'll just look at the e-mail on my Blackberry and keep working on whatever document I'm doing on my desktop. I'm not sure why I do it. I guess it's a convenience thing because I don't have to close the document and open up... Bring up Outlook. I find it less interruption on the work flow. [...] I don't have to interrupt the work I'm working on [...] the Blackberry is like a prescreening. I don't need to see that now. I don't need to see that. Ooh, that one I need to see it now. A lot of times I'll pop up Outlook and say, "OK, I need to see what this was," and deal with it. It is*

[19] The hard drives on NIST laptops are encrypted with SafeBoot, which prompts the user for a user ID and password during the boot process. Checking NIST e-mail on a BlackBerry is a way to avoid the SafeBoot authentication prompt.

easier to respond on a big keyboard than the Blackberry. The more I'm talking about it, it's a prescreening of the e-mail to decide I don't really need to interrupt what I'm doing." (P15)

4. Coping mechanisms > Using alternative channels to reduce or avoid the need for authentication > Using Linux instead of Windows on one's work PC[20]

    - *P14 Uses Linux rather than Windows because the virus threat to Linux is lower.*

F. Coping mechanisms > Planning and time management

1. Coping mechanisms > Planning and time management > Doing other things while waiting for a slow authentication process

    - *"If you count from the first time it asks you for it to the second time it asks you for it, I have no idea how long that takes. Because it takes so long, I generally go and get a bite to eat." (P2)*

2. Coping mechanisms > Planning and time management > Carrying things in a bag to have one hand free to use the door card reader comfortably

    - *"Like if I'm carrying my lunch or coffee or books or whatever, and trying to do it, it's frustrating. So I've just adapted. I just know in advance not to carry all this stuff in. […] Local trips, yeah. Or I'll take a big bag. Like this morning, I had a bunch of papers, I just put them like with my coffee. And just kept one hand free." (P12)*

3. Coping mechanisms > Planning and time management > Authenticating ahead of time to avoid work delays/interruptions

    - *"So it's something where if it's important, if I were expecting an e-mail that I had to respond to right away, I might log in, in advance, to get all that taken care of. But just to read my e-mail, I'll be here again tomorrow morning." (P14)*

---

[20] NIST computers running Linux are configured with the same security and authentication measures as computers running Windows or OSX – for example, they lock after 15 minutes of inactivity.

- *“I'll take it home Thursday night and I'll telework Friday. A lot of times I'll just... I like to boot it up Thursday, because they do security scans, too. I'll boot it up, log back into the network, and then that way it can do its scan or anything before Friday so it's not doing it while I'm trying to work. I've turned it on and come in Friday morning and it's still at the SafeBoot because I forgot... I got busy doing something else. It will sit overnight.” (P15)*

4. Coping mechanisms > Planning and time management > Batching primary tasks to keep the number of authentication tasks to a minimum

    - *“I mean, I might have continued longer than I normally would have so I wouldn't have to go back in and do it, possibly. But in a larger sense, it wouldn't, other than being an interruption. But I guess I would have stayed longer at a task rather than say going down the hall. Because I'd have to go back and do it.” (P12)*

    - *“If I am at home, I try to... Well, I try not to do it multiple times, basically, because I know that it's going to take me, to frustrate me to some degree so I would check it if necessary but try to batch together.” (P18)*

    - *P21 sees some advantages of batching.*

5. Coping mechanisms > Planning and time management > Leaving the Outlook calendar open for quick access the next day

    - *“But every morning, to see that; they force us to use that for our corporate time keeping. Every morning when I come in to see what I've got scheduled for that day, I have to authenticate myself to Outlook. I have to log into this machine and then tell Outlook because it's always logged out. […] Now, if I'm really smart, I will leave it at the end of the day with the calendar showing the next day's schedule. So I can look over there and see it without having to log in.” (P7)*

G. Coping mechanisms > Miscellaneous coping strategies

1. Coping mechanisms > Miscellaneous coping strategies > Carrying laptop around (and periodically pressing a key or moving the mouse) to avoid re-authentication due to timed lockout

- *"[T]he benefit I have is I had a lot of meetings that day and I take my laptop with me, and I just close it and take it. It doesn't really require me to – I don't lock the screen because I'm not leaving it anywhere. I just go from one room to another and take it with me, versus people who leave to go to meetings. They need to lock their computer. And then when they come back from the meeting, log back in." (P9)*

2. Coping mechanisms > Miscellaneous coping strategies > Ignoring unnecessary requests for credentials rather than following up

    - *"Windows pops up this box that says it needs my current credentials and that I should lock the screen and log back in. Well, this started happening a while ago, maybe a couple of months, once in a while, and I see no reason why I need to log out and back in, because I had access to everything I need. So, I tried it once I think, and I didn't notice anything different, so I just ignored it and dismissed the little popup. […] Yeah, there's a little circle with an X and I just click on it. […] some days it pops up more than others. This day it happened quite a bit." (P14)*

3. Coping mechanisms > Miscellaneous coping strategies > Deducing the password for a particular application by looking at the policy

    - *"[B]ecause one way I remember my passwords, especially for things where the password policies are a little bit more complicated, is I'll look at the password policy itself. And then from that I can kind of deduce what my password is. […] if I see what the password policy is, I might be able to narrow it down to a few that I can try." (P19)*

4. Coping mechanisms > Miscellaneous coping strategies > Periodically clicking the mouse or pressing a key to prevent timed lockout

    - *"You end up having to almost set a timer in your head to go back to the computer and type something within every 10 minutes or so. And some minor studies of productivity I've been involved with indicate that it's better to be focused on a task as opposed to have lots of interruptions throughout the day." (P21)*

V. Authentication's unintended effects on work habits

A. Authentication's unintended effects on work habits > Postponing tasks to put off or avoid difficult authentication

- *"[L]ast time I needed to sign something, I don't remember if it was a travel voucher, it was something I needed to sign. So the secretary e-mails me, tells me it's ready for my signature and e-approval. I put it off because I know I don't have time to deal with the password reset, I don't have time to do that right now, I will do it at the end of the day and then it's too late because you can't call because they are not there to reset the password for you. And so this drags out over the course of maybe a week or longer and then she in the meantime has taken the time to send me another reminder e-mail, and then I feel bad because I am wasting her time. But I just couldn't get it done because I couldn't remember the thing and I didn't have the time allocated to do the whole reset thing. And I know that sounds silly, because you're like, "How long can a phone call be?" But it takes time and especially when you have to wait for them to do. […] Especially when you have to wait for them to generate the thing, and then you have to go downstairs and pick it up. I mean that's just a whole category on its own. […] Because it has rippling effects. You know, it wasn't just affecting me, it's affecting people that I am calling. […] It's affecting her trying to send me these reminder e-mails and whoever else is doing budgeting, I haven't signed for the thing yet. I mean it really has this kind of ripple in the pond effect." (P11)*

- *"So it's something where if it's important, if I were expecting an e-mail that I had to respond to right away, I might log in, in advance, to get all that taken care of. But just to read my e-mail, I'll be here again tomorrow morning." (P14)*

- *"Things get put off until when it's, "OK, I have a block of time. It's worth it for me to get the token, to log in and to sit there and do like an hour's worth of work or half an hour or something like that." […] But if it's for like fleeting little, "Oh, I have this great idea" or "I want to send this e-mail" or something, then I'm more likely to put it off until I have that sort of block of time where a log-in is worth it. […] especially if it's something that wasn't actually due. It's after hours. You've already put in your nine hours or however many hours you're doing and then you think of something of home, it*

definitely is less likely that you're going to get online to actually do that thing that you're thinking of. You're just going to wait until the next day." (P11)

- *"[W]hen I'm at home, if I'm downstairs, and even if I have my work laptop there which I do. I have a property password, if I have my work laptop there and I think, "Oh, I need to send this e-mail," if I have to go upstairs into my office and get my RSA token, I am likely to just scribble a note on a piece of paper and remember it the next day, hopefully. So, it definitely changes my behavior. That's a good question. I had not thought of that. Same thing, like it makes me less likely to, if I'm at the airport and I close my laptop to go to the restroom or whatever, and I have 15 minutes before the plane's going to board or 10 minutes or something like that, if I have to re-authenticate and dig out that RSA token, again, then it'll make me less likely to take advantage of just a few minutes because it's that, again that kind of level of effort. […] I mean if there's something I have to get done, then of course, I will do it. But, as far as, "Oh, let me just taking advantage of every last second," you're less likely to do that because there's a cost associated with taking advantage of that time. […] We know people are sensitive to small, local costs and when I hear myself describing the fact that, oh, well me going upstairs to get the thing is going to prevent me from doing one e-mail, it sounds kind of silly, but that's what happens." (P11)*

- *"Well, let's say I'm working on a Word document and I have to refer to somebody's e-mail just to see one of their comments or an attachment of something I sent myself or somebody sent me. I'd have to really stop my work for five minutes. And if I'm on a roll with something, it's… […] Yeah. It just breaks everything. So instead of having to stop, go do this and then come back, and then try and get back in the flow of things, I'll just keep going. I'll just skip it and maybe come back later. [...] Every time I do that and wait for incentives here to check my e-mail, I'll get like five or six e-mails that probably people would have preferred a more immediate response." (P19)*

B. Authentication's unintended effects on work habits > Doing things less frequently

1. Authentication's unintended effects on work habits > Doing things less frequently > Checking e-mail less frequently, especially when working remotely

- *“But it's one of those things, if I spend eight hours logging into my e-mail, I'm not going to have any time to do any work. So I'd rather be doing the actual work than waste my time logging in every five minutes.” (P19)*

- *“For the e-mail, when I was at home, if I don't do anything on the Web page for five minutes or 10 minutes, it will log me out automatically. Which that can get frustrating because then I have to close the browser, open it up again, use the RSA key, hope I get it right the first time. And I can do that 15 or 20 times throughout the day. And a lot of times I'm just so tired of re-logging in, I'll just stop checking my e-mail. I might do it once every three or four hours instead of every 20 minutes.” (P19)*

- *“**Respondent:** And I just work away, and I have to consciously remember to check e-mail. And then whenever I do that, it's already locked, because it's usually locked in five minutes or something. It's just some ridiculous amount of time like that, so... **Interviewer**: Do you think...I mean is that...so you probably...overall you check your e-mail less frequently because of that. **Respondent**: Yeah.” (P4)*

- *“Yeah, because not only do I have to have a computer and the password and PIN known, I have to have this thing physically with me. If I forget it downstairs or in my car or at work, I can't log in. I have to go downstairs or go to my car or go back to work to pick it up. […] I'll forget it in my car all the time. Sometimes I'll go get it, sometimes I'll just not check my e-mail.” (P19)*

- *“Well, let's say I'm working on a Word document and I have to refer to somebody's e-mail just to see one of their comments or an attachment of something I sent myself or somebody sent me. I'd have to really stop my work for five minutes. And if I'm on a roll with something, it's… […] Yeah. It just breaks everything. So instead of having to stop, go do this and then come back, and then try and get back in the flow of things, I'll just keep going. I'll just skip it and maybe come back later. [...] Every time I do that and wait for incentives here to check my e-mail, I'll get like five or six e-mails that probably people would have preferred a more immediate response.“ (P19)*

2. Authentication’s unintended effects on work habits > Doing things less frequently > Checking bank account balance less frequently

    - *“You know, like my bank – when I log into online banking or something – that's never stored anywhere. That's always out of my memory. Real time dynamically all the time, and of course, as a result, I don't log into my bank. Well, you know, you don't need to log into your bank 15 times a day to check your balances or whatever.” (P5)*

3. Authentication’s unintended effects on work habits > Doing things less frequently > Working from home less often

    - *“[T]here are lots of things that harm productivity, such as the inconvenience associated with working from home. I would probably do more work from home if there weren't so many security issues associated with that.” (P6)*

4. Authentication’s unintended effects on work habits > Doing things less frequently > Using a laptop less (because of timed lockouts)

    - *“But the computer locks, screen locks more often if you are idle more than five minutes. So that's an annoying thing. So I only use this for not a lot of tasks, because my main computer's here and then whenever I need to go over there, it's always locked. So I have to authenticate. So I try not to use that too much.“ (P4)*

5. Authentication’s unintended effects on work habits > Doing things less frequently > Doing “a little extra work” less often

    - *“Things get put off until when it's, "OK, I have a block of time. It's worth it for me to get the token, to log in and to sit there and do like an hour's worth of work or half an hour or something like that." […] But if it's for like fleeting little, "Oh, I have this great idea" or "I want to send this e-mail" or something, then I'm more likely to put it off until I have that sort of block of time where a log-in is worth it. […] especially if it's something that wasn't actually due. It's after hours. You've already put in your nine hours or however many hours you're doing and then you think of something of home, it definitely is less likely that you're going to get online*

to actually do that thing that you're thinking of. You're just going to wait until the next day." (P11)

- *"[W]hen I'm at home, if I'm downstairs, and even if I have my work laptop there which I do. I have a property password, if I have my work laptop there and I think, "Oh, I need to send this e-mail," if I have to go upstairs into my office and get my RSA token, I am likely to just scribble a note on a piece of paper and remember it the next day, hopefully. So, it definitely changes my behavior. That's a good question. I had not thought of that. Same thing, like it makes me less likely to, if I'm at the airport and I close my laptop to go to the restroom or whatever, and I have 15 minutes before the plane's going to board or 10 minutes or something like that, if I have to re-authenticate and dig out that RSA token, again, then it'll make me less likely to take advantage of just a few minutes because it's that, again that kind of level of effort. […] I mean if there's something I have to get done, then of course, I will do it. But, as far as, "Oh, let me just taking advantage of every last second," you're less likely to do that because there's a cost associated with taking advantage of that time. […] We know people are sensitive to small, local costs and when I hear myself describing the fact that, oh, well me going upstairs to get the thing is going to prevent me from doing one e-mail, it sounds kind of silly, but that's what happens." (P11)*

C. Authentication's unintended effects on work habits > Collaborating with people from other institutions less (or not at all)

- *"[I]t's very difficult to do real collaborative work with anyone who is not a NIST employee. I have research collaborations with people in other institutions, but it is just extremely difficult to share files with them, to transfer software you're writing, and that sort of thing. To me, the way that security impacts work is not that I waste a few seconds typing in a password, but it is these things that you just can't do because of the limitations of security policy. […] I can think of cases when I have thought it would be really nice to include some person at another university on a software development project, but then I realize it is going to be such a tremendous pain to organize that." (P6)*

D. Authentication's unintended effects on work habits > Being discouraged from traveling

- *“Also, another really annoying thing is when you go on foreign travel, you can't take your own laptop. You must take a laptop that you borrow from the IT support group, which is not configured with your software. That's a real problem if the purpose of your travel is that you want to share software with people that you're working with.” (P6)*

- *“Well, I may not travel as much because you have to take a laptop for the meetings and so forth and I just didn't want to deal with it.” (P12)*

E. Authentication’s unintended effects on work habits > Giving up on devices

1. Authentication’s unintended effects on work habits > Giving up on devices > PIV card

    - *“I actually don't use my PIV card here at work because I forget it in the computer a lot. If I leave the building, I can't get back in because that's also my access back into the building. […] But this thing, it's just a tiny, nearly weightless piece of plastic that you often forget about. So I would forget this every single time. And I've been locked out of the building. I've been locked out of the floor. I've been reprimanded for leaving this in the computer. And there's nothing I could have done other than somehow setting reminders every two minutes to don't forget this.” (P19)*

2. Authentication’s unintended effects on work habits > Giving up on devices > Laptop

    - *“I don't have a laptop. I don't have a laptop, which that was another – which one of the reasons why I gave up the laptop was the password thing for the SafeBoot. I had all kinds of trouble with that, but that's another story. […] Yeah. Yeah, that was one of the reasons why I didn't want to deal with the laptop anymore because I could not remember my SafeBoot code. I could not remember it. I could not remember it.” (P12)*

    - *“If I had a NIST laptop I would have to log in twice, once when you turn it on because the hard drive's encrypted, and then again to actually get into Windows or the operating system. […] So I never wanted a NIST laptop for that reason. I don't want to have to log in more times than I need to. That goes to the whole password security policy that we have here, is everything that leaves NIST has to be encrypted.“ (P19)*

3. Authentication’s unintended effects on work habits > Giving up on devices > Mobile devices

    - *“I don't have a mobile device for work. I don't bother. I don't have one for my personal either. I mean I have a phone and text. I guess mainly my thing is, again, I just try to keep my environment simple. I don't need a lot of gadgets that I have to then deal with and manage and all that.” (P9)*

APPENDIX D: MODELING METHOD EXAMPLES

Two models based on the GOMS-KLM technique were developed to model a login task similar to one NIST employees execute. The first model was developed by a member of the research team by manually modeling the task using the prescribed GOMS-KLM technique. For this model, the researchers broke the task of logging in to an e-mail app down to its most basic elements as prescribed by GOMS-KLM. GOMS-KLM includes standard durations (in seconds) for each of these actions, which were used in the task breakdown for this model. **Table 17** shows an example of a GOMS-KLM sequence for the manual login, with each action and its associated time.

Table 17: Example Keystroke Level Modeling sequence of steps for manually logging into an application, with time for each step

Step	Activity	GOMS-KLM Task Symbol	Time (in seconds)
1	Mentally prepare	M	1.35
2	Home hand on mouse	H	0.4
3	Position the cursor over the bookmark	P	1.1
4	Click mouse	P1	0.2
5	Position the cursor over the userid field	P	1.1
6	Click mouse	P1	0.2
7	Home hands on the keyboard	H	0.4
8	Recall userid	M	1.35
9	Enter userid (8 characters)	8 (K)	1.76
10	Home hand on the mouse	H	0.4
11	Position the cursor over the password field	P	1.1
12	Click mouse	P1	0.2
13	Home hands on the keyboard	H	0.4
14	Recall password	M	1.35

Step	Activity	GOMS-KLM Task Symbol	Time (in seconds)
15	Enter password (8 characters)	8 (K)	1.76
16	Home hand on the mouse	H	0.4
17	Position the cursor over the submit button	P	1.1
18	Click mouse	P1	0.2
	Total Time		14.77

For the second model, the research team used CogTool, a prototyping tool that predicts the amount of time required for a skilled user of an interface to perform a particular task based on data provided to the tool. The team performed the actions necessary to log into the selected e-mail app (manually and with LastPass) and took a screenshot at each step. This sequence of screenshots was then entered into CogTool, along with specifications for the buttons and fields used for interactions at each stage (e.g., the number of characters to be typed into a certain field). CogTool then assigned cognitive and physical components of the task based on the screenshots and information provided. While it used standardized GOMS-KLM durations for each task as a baseline, it also calculated its own times where possible. These calculations, which were based on Fitts' Law [8], took into account the distance to and size of the target object users needed to click to complete an activity. **Figure 17** below shows CogTool's script for the login task. CogTool developers assert that CogTool is at least as accurate as GOMS-KLM-only models, and perhaps more so [11].

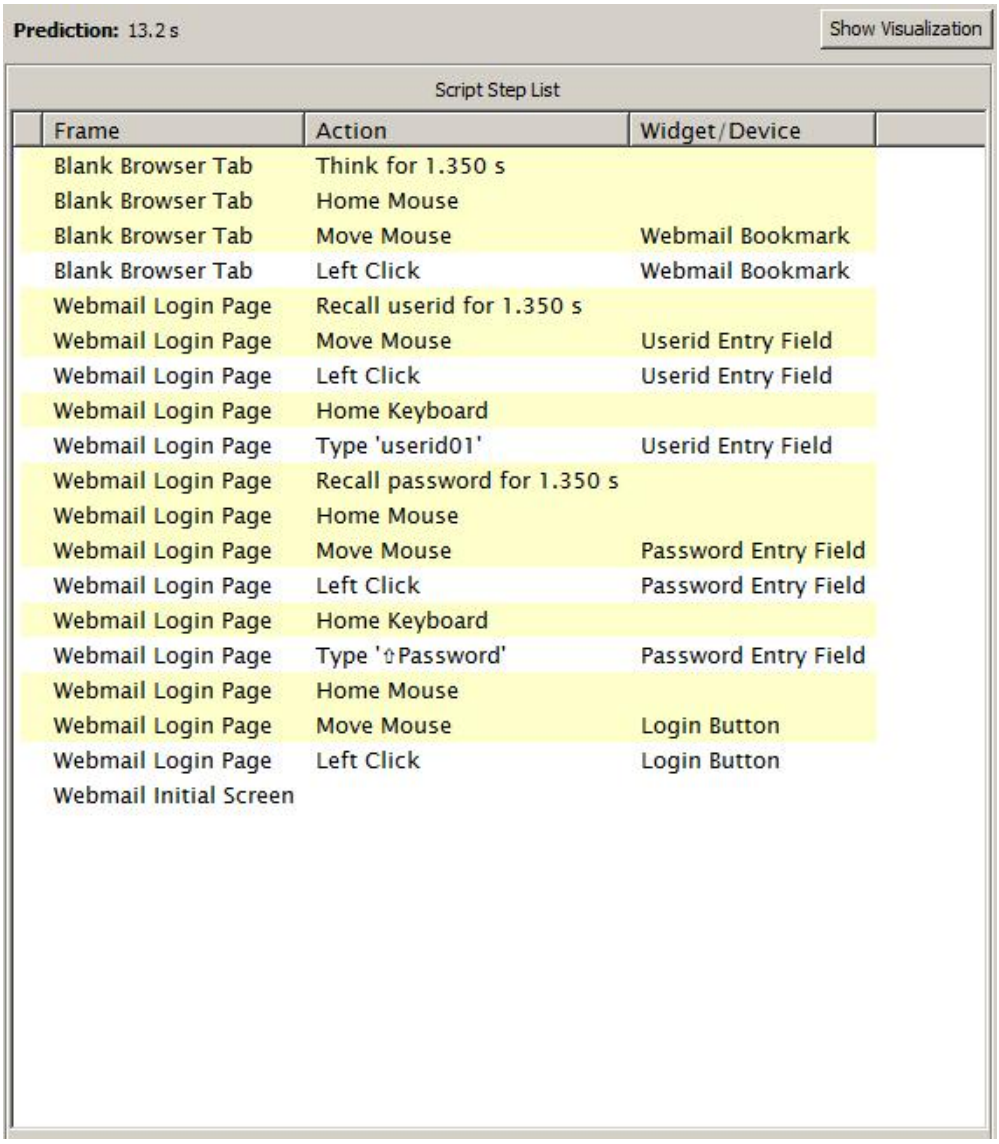


Figure 17: A sample CogTool script for the Keystroke Level Modeling sequence of steps for manually logging into an application