Rethinking authentication

Authentication – Just get it done?

In today's environment, there is little doubt that companies, organizations, and governments must make significant investments in developing, implementing, and supporting authentication for their digital systems. Perhaps because of this, an organization's IT support center often takes a hard line when it comes to user's authentication. Authentication tools typically take for granted that the user will do whatever it takes to authenticate. No surprise, users don't like being forced into a corner[1]. They are resourceful and very creative in making it more manageable, usually by coming up with ways that circumvent the overall security of a system. Unfortunately, as the number and complexity of authentications for each user become greater, job satisfaction for workers is likely to decrease.

All authentication is not the same

It is often assumed from the implementer's perspective that most authentication mechanisms are equivalent with another. However, from the user point of view (and from the support view), things couldn't be more different. How the user goes from identifying how to perform the work, then collecting the materials necessary to perform the work, logging onto a system, performing one or more tasks, and then logging off again could vary widely depending upon the process.

The work is also dependent upon the device used to do authentication, even varying between a mobile device and a WorkStation. Whereas a smartcard might be easily utilized in a WorkStation, the lack of a device interface may make it difficult to use with mobile equipment. Similarly, long passwords containing numbers and symbols and letters may be difficult to enter with the mobile device keyboard, but better supported at a WorkStation. Some evidence of mobile device issues is highlighted by the increased pressure of developing derived credentials, supplementing credentials typically housed in a smartcard to using them internally in a mobile device[2].

Usability in Authentication

Researchers are attempting to improve not only the security, but also the usability of many types of authentication. Increasing usability can help the user avoid stress-related workarounds. Increasingly recognized as a vital component of authentication, usability is beginning to be included in the requirements of authentication mechanisms. Usability studies have focused on the form of authenticating. Much of this work is slowly finding acceptance into the marketplace. So, are there other things that can be done to make authentication more usable?

Real world usability

Illustrating this concept using a real-world example, we have tried making the entrance door key more usable by changing the size, weight, or shape of the key. But this is not the same as considering alternatives to the lock and key. The most adaptable and user-friendly alternative to gain entry would likely be a doorman. It negates the need of a key and eliminates barriers if the hands are full, the doorman knows you and can provide germane information. However, when you consider active service 24 hours a day for a single residence, this is rather an expensive option. So, most of us choose to use a key and have a lock on the front door. Using a wireless device that allows entry without inserting a key, possibly opening the door from the car before picking up the 40 lbs. of dog food, might be helpful, but there are other concerns about the technology.

The take away from this is that depending on the usability, the expense, and the security, the implementer might opt for different solutions. This should also apply to the network or device authentication realm. Implementers usually must consider expense and security, in choosing an authentication mechanism today. However, it seems like the usability is often forgotten.

Minimizing the pain points

Usability experts are measuring the usability of different authentication methods and how they may be improved. Authentication is expected to be just a very small bump in the process of getting work done. Authentication is not the mission, not the payoff, it could be looked at as a necessary tax. So, to make the user more effective, we need to allow the user to stay focused on tasks highlighted by the employer's evaluation and minimize the impact of authentication to the overall process.

We should be improving the usability of the work process in which the authentication is being used. If we look at the user's workflow we should not see a disruption of the process in order to authenticate. An authentication disruption may consist of a required move to a different work area or stopping to consult an authentication store, whether the data is stored in a software vault or a separate hardware device. The disruption could be having to re-authenticate too often, such as a during a public presentation. In addition, establishing or updating authentication information should not occur during the workflow. These events should have their own processes that should not interrupt an in-process user workflow.

Usability of the process

Authentication permits or denies continuance of the workflow. Examine a process that accomplishes a work goal, one in which the authentication is necessary, but not the focus of the goal. By examining the steps necessary for authentication within that construct, and analyzing how they affect the process, we can begin to see how to minimize the jarring impact of authentication in the work process. By not distracting users through disjoint tasks, the overall process could be more effective and efficient and have greater user satisfaction, i.e., more usable. By aligning the authentication method or adjusting a method's parameters to be more compliant with the overall process, we identify ways to tailor authentication to increase the usability of the process.

A technique to maximize usability of the process is to include usability studies in the mission requirements. Evaluating the usability of the process the user navigates through should identify how disruptive an authentication component is to the rest of the process. Normally, if the user must navigate a major disruption, then we normally try to improve the process. However, excuses like "oh well, it's not like we don't have to logon" allows authentication to be disruptive. As authentication becomes part of every process, it becomes important that the usability of the process includes, not excludes, authentication.

Scenarios for Use Cases

It is unlikely that each user will require a totally separate evaluation; chances are there are only a few variations for many workflows. The following paragraphs provide three different sample scenarios that lay out differences in authentication for an office worker, a researcher, and an IT administrator. These are generalized to illustrate aspects but could be tailored to support specific scenarios.

Office Worker

Looking at a typical day for an office worker often finds an incredible amount of computer access. For example, most corporate users spend a great deal of time using word processors, spreadsheets, email and messaging. To accomplish this, all users must log into their primary laptop/mobile/desktop, their email, timesheets, file server, IM, contact manager/scheduler and may even include IP telephones. Without some sort of single-sign-on capability we begin to wonder if the user can show progress for the day, especially with activity monitors which log the user off after a period of inactivity (such as reading, phone calls, or other non-keyboard activities). Another source of disruptive authentication are the patches and updates of software, OS, and peripherals, each of which require authentication. In addition, office workers may also use their authentication credentials for physically entering one or more access-controlled areas throughout the day, which may use similar credentials as their cyber access.

Researcher

The researcher may have an office where many of the same functions as the office worker are performed, perhaps with greater focus on the use of databases and algorithm manipulation or even custom programming. In addition, there may be a laboratory that may house one or more scientific instruments which have similar or other OS interfaces that must be authenticated. Each of these devices may have other logging or data storage devices that again may communicate across platforms. There is often added security due to the nature of research which may complicate all the above operations. In addition to these daily processes, a researcher is likely to perform other diverse duties including presenting complex information using tables and graphics to internal and external audiences including conferences and presentations, where interruptions for renewing authentication could be extremely detrimental when conveying complex explanations.

IT Administration

IT Administration often need access to everything which makes it difficult to address. Perhaps the most difficult area for administering network management is managing the number of people and accounts necessary for accessing the settings across the network devices. There are several factors that make this difficult. Often a factor is weak authentication schemes that are permitted on network devices due to their “out of band access”. Another factor is the now fading policy of using the same authentication across many users, many devices, and across multiple disparate locations. The degree of turnover of equipment and administrators, especially considering employees, maintenance contractors, and installation contractors also represents a difficulty. Taking these factors into consideration, the amount of changes throughout the system that are often applied when installing new or replacing existing equipment is perhaps the most worrisome. Separating IT Administration to either customer support or network support does decrease risk of compromise as does controlling remote access management, but both add complexity.

Technology options

The scenarios certainly demonstrate that this is not a simple problem. However, solutions have been developed to address, perhaps idealized, versions of these scenarios. Authentication solutions continue to be developed in three major areas: smartcards, passwords, and biometrics.

Smartcards

The U.S. Federal government has invested heavily to find the best and most flexible systems for government use. In general, the smartcard appears to be their answer. The smartcard represents a device that is quite flexible to the user but is not without its limitations and requirements. The user must have access to a card reader, drivers for the hardware-software interface, and must remember a PIN that can be changed if need requires. Most smartcards also have a wireless interface that is typically used as a physical access device. This may be the most questionable in the design; while it does remove the need to track two (or more) devices, it does not keep the user from leaving it in the computer and then exiting the area without the means for re-entry. When used for physical access the user often does not enter the PIN. However, even with this aspect removed, the response time of the process can cause a line of people waiting to authenticate. Possible safety issues concerning ingress/egress during power outages or other emergencies may arise. It can also encourage a compromise of security, the users bypassing the authentication entirely through less secure avenues or procedures. Despite these limitations, along with the large budget needed over the life of the program, secondary costs to implement a unified authentication across disparate systems, and risk of compromise, the option of smartcard authentication is often selected when cost allows.

Passwords

Password authentication is by far the most prevalent method of authentication, especially for small to medium business, websites and apps. It is also one of the cheapest if done right, but in general, the more secure user password, typically the more difficult to remember and therefore, the more difficult to use and support. Passwords can overwhelm and certainly side track the thought process[3] by having to remember (and not fat finger) the password. As most passwords are not displayed when entered, negotiating mobile devices and other non-standard keyboards can also add to the difficulty. Password safes diminish memory loss issues but is often a separate process that can also derail the user from their mission. While systems using passwords for authentication can often be joined, the difficulty of implementing and managing these systems becomes a cost issue for many. Passwords or PINS used for access control are typically used on a much smaller scale and are typically susceptible to compromise by observation of the users entering their authentication information or the residue left on keys. In most cases, passwords or PINs can be easily changed, though this often leaves the burden on the user to negotiate another interface, select, and remember new information, all while trying to focus on other things.

Biometrics.

Though biometrics have been around several decades, mobile devices such as smartphones or tablets and many laptops can support biometric solutions that were difficult and expensive to implement less than a decade ago. The reduction in cost and the integration of the sensors into the hardware lend themselves to use as part of the authentication system. Smartphones have in certain ways stood biometric implementation schemes on their head; instead of one system with multiple sensors, it is becoming one sensor for multiple systems. It is possible to bank, purchase, receive medical information, and even dial contacts by authenticating using biometric sensors in the smartphone. While there are several other examples, this appears to be the most accepted use of biometrics to date. The usability of these sensors is typically very high as they are often implemented specifically with the user in mind.

Developing usable authentication

We are seeing the effects of ill-fitting authentication. Indicators include frequent errors and reset requests, long authentication times, and possibly exposure of sensitive information in highly public places. In addition, impromptu authentication updates often confound the user by focusing on selecting authentication evidence while making it harder to remember the original task[4].

Many of the issues with the authentication appears to be improper or insufficient user testing, especially as a part of a work process. In rolling out new authentication schemes, developers and testers should have to manually use the creation tools and use of the authentication “under load” to gain insight as to how authentication may be better integrated and executed.

A significant concern is the number of disparate systems that the user is expected to bridge. All components of the workflow process must be reviewed, the authentication is not the only area where adjustments must be made to improve the user experience. Consider one of the two workflow process below which may facilitate better usability.

- Staged flow – Do something local, save, authenticate, save securely online. Simplest to accommodate different authentication strategies.
- Single Sign On -- the user authenticates and, then begins work.

There are many other workflows that might be applied. The more consistently applied workflow, the easier for all users.

Perhaps the hardest part is the realization that the workflow must painlessly integrate authentication. Organizations must invest in incorporating authentication to everyday, multi-system integration. Perhaps we must revisit Frank and Lillian Gilbreth’s work[5], applying it to today’s requirements rather than the plug and play approach we currently take.

References

1. Sasse, A. “**Scaring and Bullying People into Security Won’t Work**” *IEEE Security \& Privacy* no. 3 (2015): 80–83.

2. Ferraiolo, H., Cooper, D., Francomacaro, S., Regenscheid, A., Mohler, J., Gupta, S., and Burr, W. “**NIST Special Publication 800-157, Guidelines For Derived Personal Identity Verification (PIV) Credentials**” (2014):

3. Adams, A. and Sasse, M. A. “**Users Are Not the Enemy**” *Communications of the ACM* 42, no. 12 (1999): 40–46.

4. Stanton, B., Theofanos, M. F., Prettyman, S. S., and Furman, S. “**Security Fatigue**” *IT Professional* 18, no. 5 (2016): 26–32.

5. Price, B. “**Frank and Lillian Gilbreth and the Motion Study Controversy, 1907-1930**” *A mental revolution: scientific management since Taylor* (1990):