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

Usable Security: A Human-centric Approach

Julie Haney, PhD
Visualization & Usability Group
NIST Information Technology Laboratory

January 28, 2021

Disclaimer

Throughout the presentation, certain commercial companies or products may be identified to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor does it imply that the companies or products identified are necessarily the best available for the purpose.

About Me

B.S. and M.S. in Computer Science

⬇

Cybersecurity professional for 20+ years at the U.S. Department of Defense

⬇

PhD in Human-centered Computing

⬇

Researcher and lead of the NIST Usable Cybersecurity program

Usability

Usability

“the extent to which a system, product or service can be used by specified users to achieve specified goals with ***effectiveness***, ***efficiency*** and ***satisfaction*** in a specified context of use”

(ISO 9241-11:2018)

Effectiveness - accuracy and completeness with which users achieve specified goals

Efficiency - resources used in relation to the results achieved

Satisfaction - extent to which the user's physical, cognitive and emotional responses that result from the use of a system, product or service meet the user’s needs and expectations

Systems, Products, and Services

IT devices, SW, services

processes

policies

Recommended Security Controls for Federal Information Systems and Organizations

NIST 800-53

guidance

awareness & training

Users

end users

system administrators

security professionals

decision and policy makers

Context of Use

Intended Users

- Motivation and perceptions
- Ability, knowledge
- Biases

Tasks and Goals

- Security as primary task or not
- Personal or organizational outcome

Environment

- Technical
- Social
- Organizational
- Physical

Usable Security

Usable Cybersecurity as a Priority

> Security must be usable by persons ranging from nontechnical users to experts and system administrators. Furthermore, systems must be usable while maintaining security. In the absence of usable security, there is ultimately no effective security.

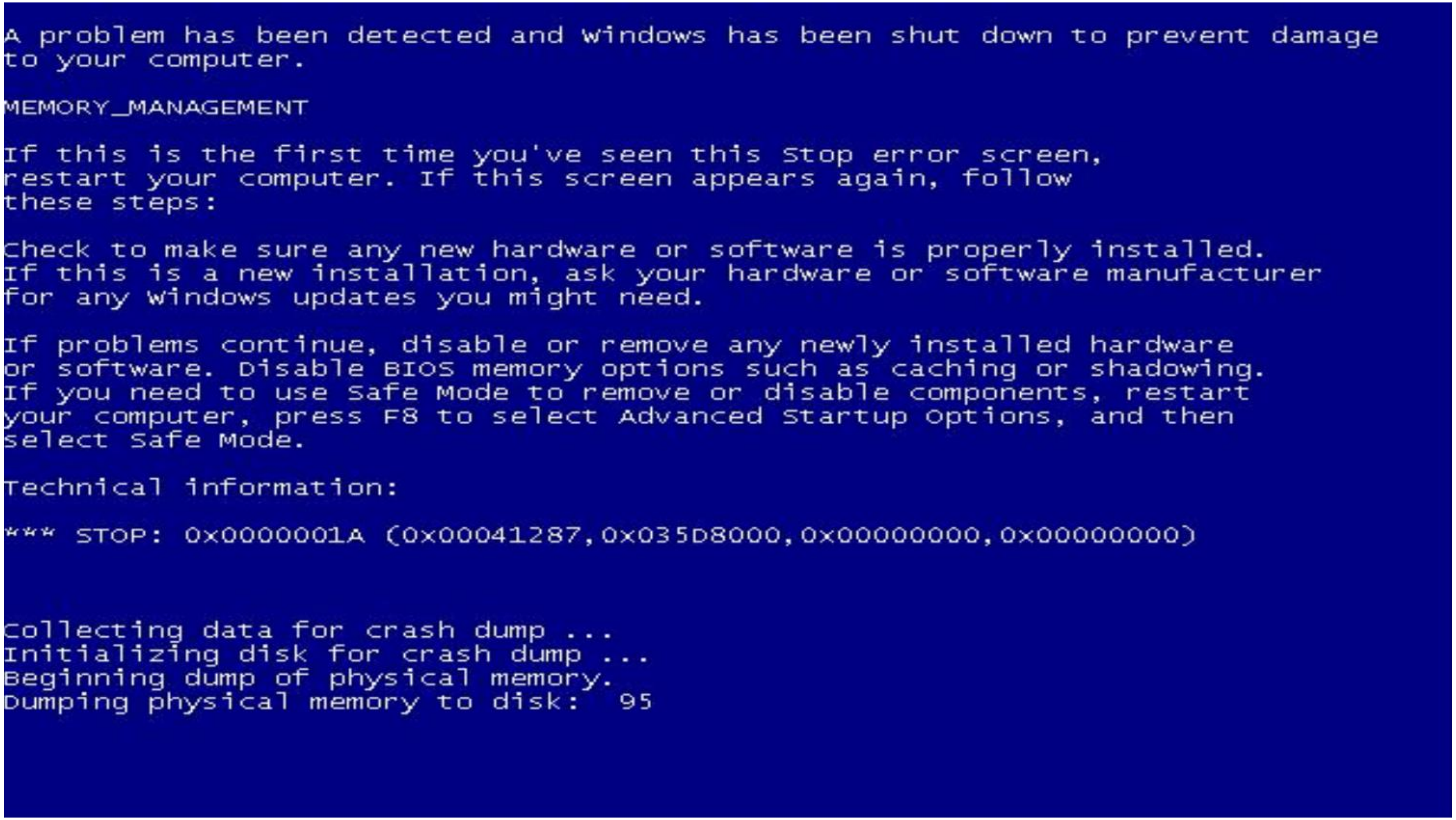
A Roadmap for Cybersecurity Research, U.S. Department of Homeland Security, 2009, p. 90

NIST Usable Cybersecurity

"Championing the human in cybersecurity"

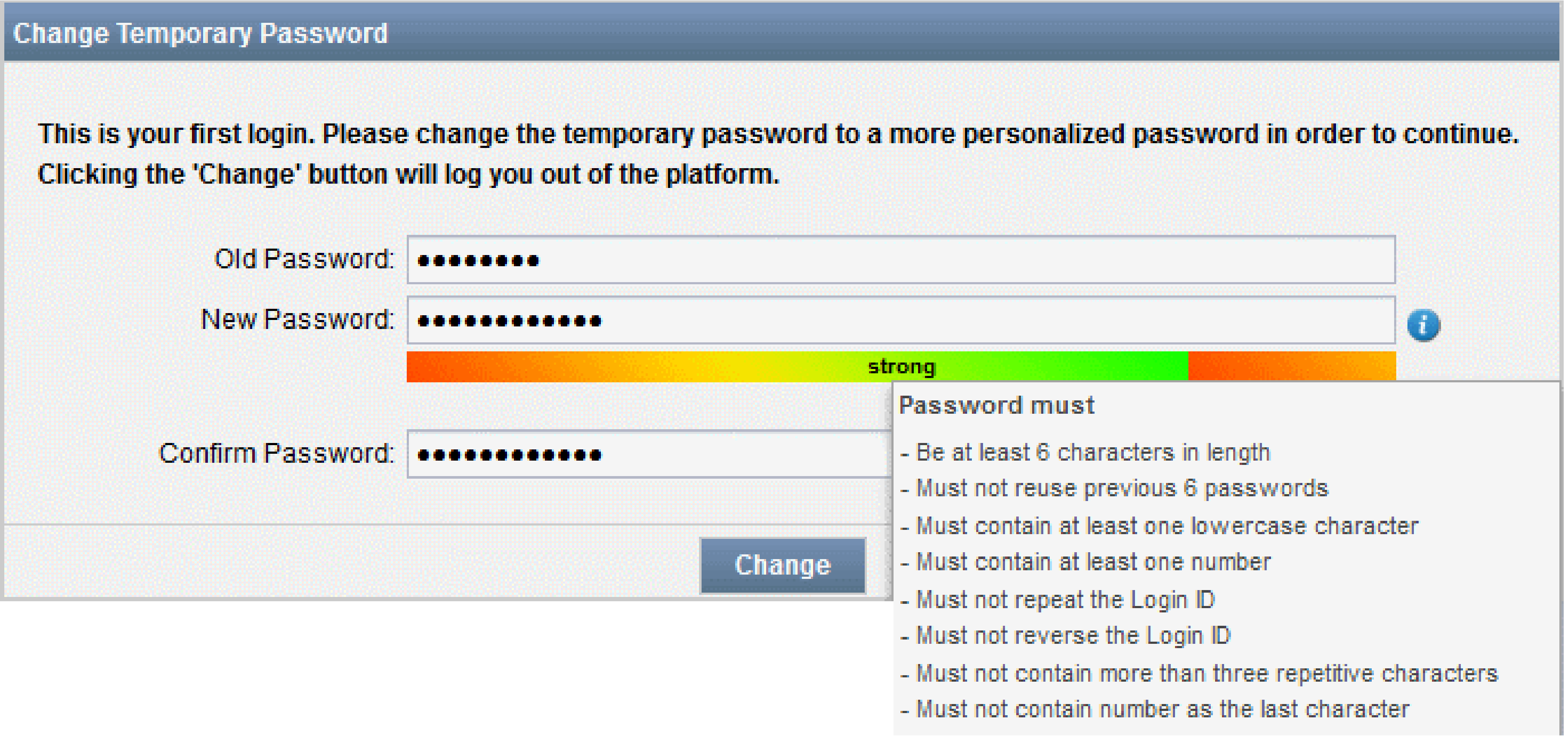
- Conduct research and usability testing at the intersection of cybersecurity and human factors – human-centered approach
- Provide actionable guidance so that the human element can be considered in cybersecurity decisions, processes, and products

A Cautionary Tale, or "How I learned the hard way"



```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

MEMORY_MANAGEMENT

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x0000001A (0x00041287,0x035D8000,0x00000000,0x00000000)



Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk:  95
```

A Classic (Un)Usable Security Example



Change Temporary Password

This is your first login. Please change the temporary password to a more personalized password in order to continue. Clicking the 'Change' button will log you out of the platform.

Old Password: ●●●●●●●●●

New Password: ●●●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●●●

Password must

- Be at least 6 characters in length
- Must not reuse previous 6 passwords
- Must contain at least one lowercase character
- Must contain at least one number
- Must not repeat the Login ID
- Must not reverse the Login ID
- Must not contain more than three repetitive characters
- Must not contain number as the last character

Security Community Pitfalls

- The blame game: thinking end users are “stupid” or “hopeless”
- Using punitive measures to get users to comply
- Putting too much burden on the user
- Not tailoring guidance/communications to the audience
- Assuming the “most secure” solution will result in the best outcome
- Making users insider threats due to poor usability
- Not considering meaningful measures of effectiveness/impact on users

Depending only the technology and not considering the individual, social, cultural, and organizational factors that may impact adoption

Usable Security Helps Organizational Security

Taking a human-centric approach to security is an important aspect of establishing and maintaining a healthy security culture

Takeaways for Organizations

- Treat people at all levels of your organization as active, capable partners in security.
- Identify stakeholders and consider their needs and context of use when deciding on organizational security technologies, procedures, or policies.
- Focus on empowering people by providing actionable, achievable guidance and an appropriate amount of information in terms they understand.
- Communicate the value of security for both individuals and the organization.

Questions?

julie.haney@nist.gov

https://csrc.nist.gov/usable-cybersecurity