Security: The Human Element

CS@CU

The Human Element

"Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed, but they are sufficiently pervasive that we must design our protocols around their limitations."

Network Security: Private Communication in a Public World, Kaufman, Perlman, and Speciner

Designing for Usability

- People have to use security systems

- If people make mistakes, security will be hurt

- Many systems are not designed to make it easy to do the right thing

☞ Some, in fact, make correct behavior very hard...

Secure but not Usable

- Can the users intentionally subvert your security mechanisms?

- Can they unknowingly influence the effective security?

Usable but not Secure

- Can the users accomplish their tasks?

- Is performance affected?

Considerations

- Is the user aware of the security tasks they need to perform?

- Is the user equipped to successfully perform those tasks?

- Is it possible for the user to make dangerous errors?

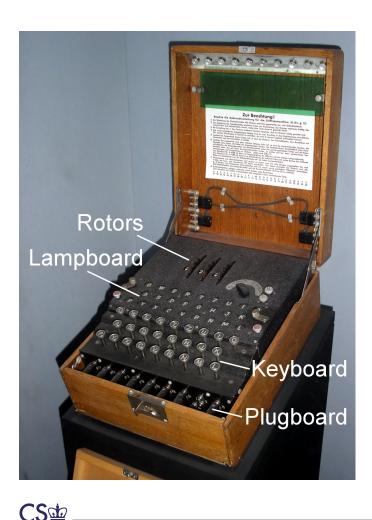- Will the user be sufficiently comfortable with the interface to continue using it?
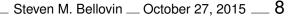
Complicating Factors

- Unmotivated user

- Lack of feedback

- Abstraction

- Weakest link

- Barn door

The German Enigma Cipher Machine

Rotors
Lampboard
Keyboard
Plugboard

- A decent (though definitely not perfect) design—but operational errors helped with its cryptanalysis

  - Easily guessed session keys ("cillies")

  - Repeated common messages ("Nothing to report")

  - Operators didn't move rotors enough ("Herivel tip")

Exploiting Errors

"That's the sort of thing we were trained to do. Instinctively look for something that had gone wrong or someone who had done something silly and torn up the rule book."

Mavis Lever, Bletchley Park cryptanalyst

Motivating Users

- Do users really care about the security rules?

- Should they?

- Do they understand how the rules really help?

- Do they see the rules as arbitrary and just getting in their way?

Psychological Acceptability

- Designed for ease of use

- Routine, automatic, correct

☞ Accurate mental model
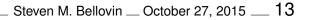
Ease of Use: The Herivel Tip

- The operator had to move three rather stiff rotors a "random" number of positions

- It's easier to move just a few clicks

- People are bad at picking random numbers

- It was hard to do the right thing

- What if they'd been told to roll dice for the number of clicks? Would they have listened?

Mental Models: Windows Vista

What is going on here?

User Prompts

- Is something being uninstalled or changed?

- What program?

- What triggered the prompt? Is it tied to a particular user request or not?

- Warning fatigue

Warning Fatigue

Dialog box

A window in which resides a button labeled "OK" and a variety of text and other content that users ignore.

From `http://www.w3.org/2006/WSC/wiki/Glossary`

What Will People Do Here?

File Permissions

Many errors...

A Few of the Interface Mistakes

- What happens if neither "Allow" nor "Deny" is checked?

- How do user and group permissions interact if they conflict?

- What is the difference between "Write" and "Modify"?

- What are "Special permissions"?

- Experiments have shown how bad it is...

Access Control Lists Are Hard

- ACLs—of the form we discussed—are not very usable

- Most people get them wrong

- However, we see them everywhere, including Facebook

- Our experiments show that most people get the Facebook privacy settings wrong

Passwords

- They seem easy...

- Users understand them

- (Supposedly) minimal maintenance costs

- However...We all know passwords are guessable

Password Policies

- Use upper and lower-case letters, numerbers, and special characters

- Do not use words found in a dictionary

- Must be at least 8–10 characters long

- Never write down or share your password

- Change your password whenever there is suspicion they may have been compromised

- Change it monthly in any event

- Never reuse a password for more than one account

- Make passwords COMPLETELY random but easy for you to remember

It Doesn't Work

- People are bad at generating random strings

- Theyre not good at remembering them

- Managing several passwords is difficult

- Most people don't know what makes a password "good"

Designing for Usable Security

- Know your users

  - Background

  - Abilities

  - Limitations

- Know the users goals and tasks

More Issues

- Consider environmental factors that may affect user behavior

- Design for robustness against potential attacks

  - Spoofability

  - Information overload

  - Warning fatigue

General Guidelines

- Make the default settings secure

- Use automation when possible

- Don't leave it to the user when things go wrong

Designing Mechanisms

- Does it behave correctly when not under attack?

- Does it behave correctly when under attack?

- Can it be spoofed, obscured, or otherwise manipulated?

- Do users notice it?

- Do the users know what it means?

- Do users know what they are supposed to do when they see it?

- Do they actually do it?

- Do they keep doing it over time?

- How does it interact with other indicators that may be installed on a user's computer?

Two Different Reactions

This Connection is Untrusted

You have asked Firefox to connect securely to www.████████.net, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!]

▶ **Technical Details**

▶ **I Understand the Risks**

Safari can't verify the identity of the website "www.████████.net".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "www.████████.net", which could put your confidential information at risk. Would you like to connect to the website anyway?

[Show Certificate]   [Cancel]   [Continue]

Which is right?

Safari is Worse?

- The information presented isn't understandable to most users

- What's a "certificate"?

- Easy to ignore

- Unclear, though, if Firefox's approach is better *in practice*

Experiments are Necessary

- Your instincts are probably wrong

☞ You know too much!

- Must gear things for the proper user community

- Even other programmers are users

Evaluation Methods

- Prototyping (including low-fidelity prototypes)

- Interviews

- Focus groups

- Heuristic evaluation

- Cognitive walk-through

Cognitive Walk-Through

- Task-focused: how does a user do something?

- Is each step clear?

- Do users realize that the step is needed and available?

- Do they get proper, comprehensible feedback?

Heuristic Evaluation

- Examine interface as a whole

- Evaluate according to recognized principles

- Example: clarity of indicators, consistency, real-world language, undo/redo, etc.

Dealing with Human Subjects

- Experimental design is *hard*

- Example: How do you test anti-phishing technology in the lab?

- Ethical issues: Institutional Review Boards (IRBs) at universities

Dealing with Humans...

- Sometimes, the problems with people are harder than bad interfaces

- Sometimes, the problem is security software that can't handle misbehaving insiders

- Two examples: Chelsea (formerly Bradley) Manning and Edward Snowden

- Note: this is a *technical* discussion, not a political or ethical one

The Manning Case

- Few internal access controls against trusted insiders

- Note: this was a *deliberate* policy decision, in the interests of increasing information sharing

- It's not necessarily a wrong decision per se; rather, it's a cost-benefit tradeoff

Preventing the Problem

- If someone like Manning has (correct) ACL permissions to download anything, what do you do?

- Log and audit—are the patterns unusual?

- More on logging later this semester

Snowden

- Caution: we still don't know the full story on what happened

- Apparently, Snowden was a system or network administrator

- Sysadmins have great power!

- Often, they set access policies

- Some reports say that he impersonated other users

- He could even replace software

Defenses

- None?

A *Really* Hard Problem

Logging Can the sysadmin turn off the logs?

Auditing Audit whom? The spoofed userids? Physical devices?

Token Authentication What about lost tokens?

Two-person Control Hard to do; no commercial products

Ban Removable Media Not unreasonable, but hurts productivity

Limit Access But what about the need to share?

Insider Attacks

- Insider attacks are the hardest security problem

- They have lots of knowledge of procedures and targets

- People tend to trust their colleagues—which isn't wrong

- Insiders can have lots of reasons for getting angry at their employer

Two Headlines from the Wall Street Journal

- "Departing Employees Are Security Horror"
  (`http://online.wsj.com/news/articles/`
  `SB10001424052702303442004579123412020578896`)

- "What Companies Can Do to Stop Insider Data Theft"
  (`http://online.wsj.com/news/articles/`
  `SB10001424052702304066404579125214029569216`)

Personnel Management

- The first line of defense might be management, not technical

- Background checks

- Look for worrisome behavior changes

- But how do you fire a once-trusted employee? Any back doors left behind?

Striking a Balance

- Insecurity is not a sin

- Making risk-benefit decisions is not only necessary, it's *correct*

- Taking risks is the essence of business

- But: you need to understand the risks

- And: you need to mitigate them when feasible

- There's a difference between calculated risks and recklessness

The Threat Matrix

Skill $\longrightarrow$

Opportunistic hacks   **Advanced Persistent Threats**

Joy hacks   Targeted attacks

Degree of Focus $\longrightarrow$

Insiders

- Insiders may or may not be highly skilled

- However, their attacks are *targeted*

- They have extra access and extra knowledge

- If they're also skilled, you have very serious problems