Security: The Human Element

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 reduce the effective security?

Usable but not Secure

- Can the users accomplish their tasks?
- Is performance affected?

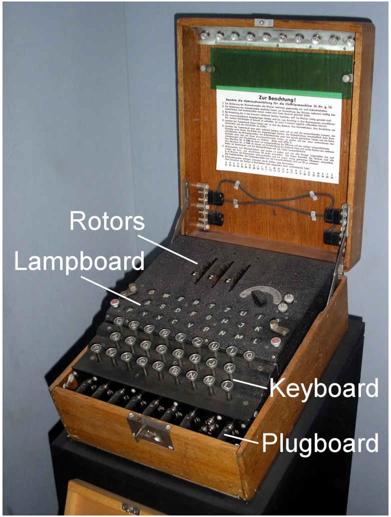
Considerations

- 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
- Close the barn door after the horse is stolen incident, not before

The German Enigma Cipher Machine



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?

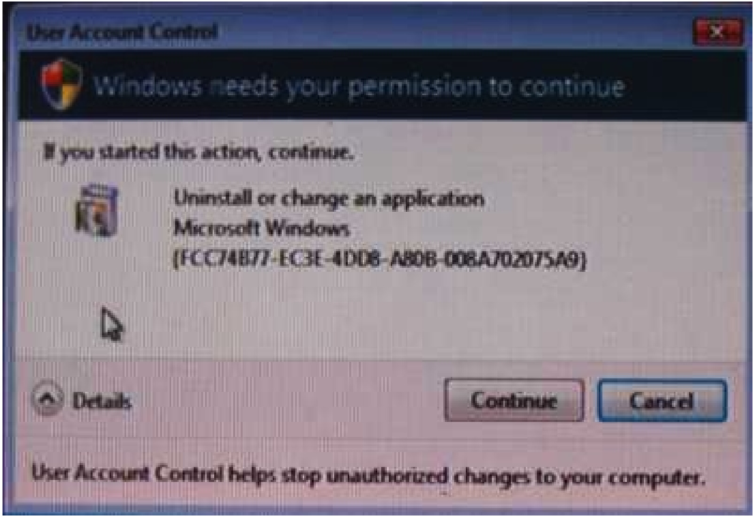
Psychological Acceptability

- 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



User Account Control

Windows needs your permission to continue

If you started this action, continue.

Uninstall or change an application
Microsoft Windows
{FCC74B77-EC3E-4DD8-A80B-008A702075A9}

User Account Control helps stop unauthorized changes to your computer.

What is going on here?

User Prompts

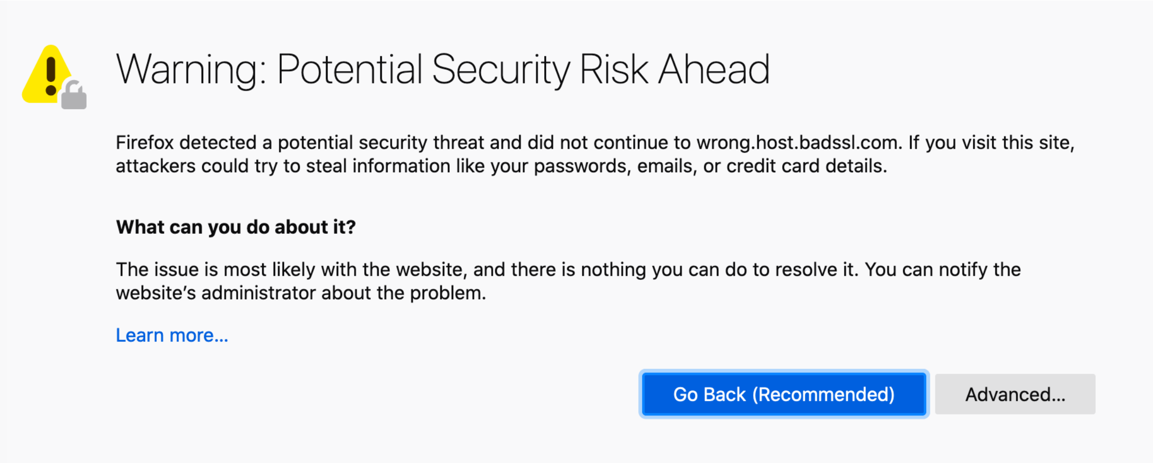
- Is something being uninstalled or changed?
- What program?
- What triggered the prompt? Is it tied to a particular user request or not?
- Warning fatigue

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?



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to wrong.host.badssl.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

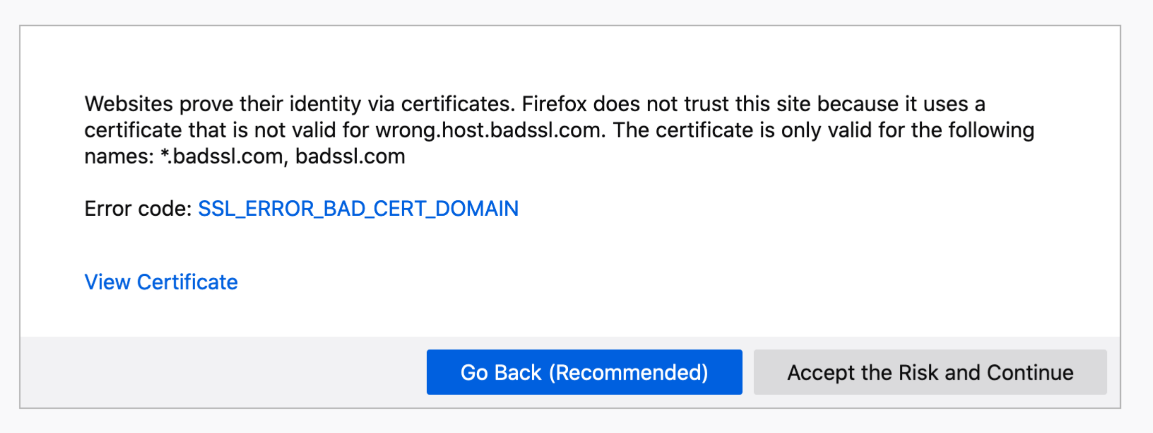
The issue is most likely with the website, and there is nothing you can do to resolve it. You can notify the website's administrator about the problem.

Learn more...

It’s a Pretty Good Screen

- It warns that there’s a possible security problem
- It says that there’s nothing users can do
- It warns of the consequences
- It does *not* simply give you a way to go ahead

If You Click “Advanced”. . .



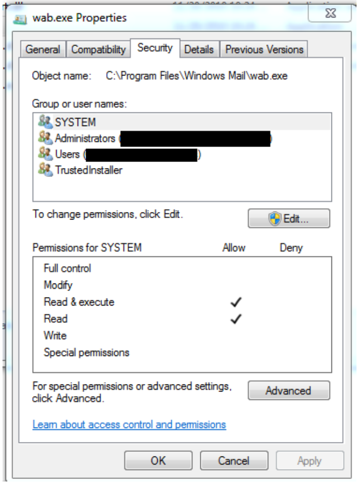
Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for wrong.host.badssl.com. The certificate is only valid for the following names: *.badssl.com, badssl.com

Error code: SSL_ERROR_BAD_CERT_DOMAIN

Still Pretty Good

- It explains the exact problem, in comprehensible terms
- It gives the recommended action
- That’s the default, if you just hit ENTER
- It lets you examine the certificate
- And you can proceed if you want
- N.B.: Not all of the advanced errors are that good

Windows File Permissions



wab.exe Properties

Object name: C:\Program Files\Windows Mail\wab.exe

Group or user names:

- SYSTEM
- Administrators ([redacted])
- Users ([redacted])
- TrustedInstaller

To change permissions, click Edit.

Permissions for SYSTEM	Allow	Deny
Full control		
Modify		
Read & execute	✓	
Read	✓	
Write		
Special permissions		

For special permissions or advanced settings, click Advanced.

Learn about access control and 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, including this one, are not very usable
- Most people get them wrong
- However, we see them everywhere, including Facebook for privacy settings
- 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, numbers, 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
- They’re 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

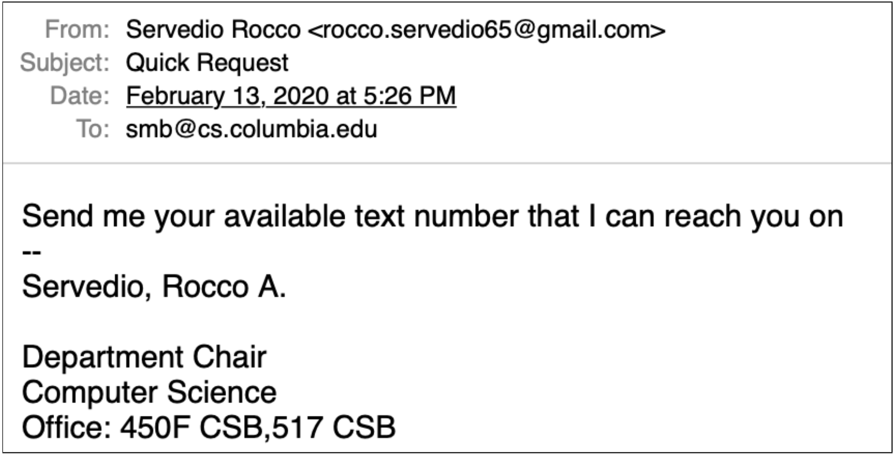
More Issues

- Consider environmental factors that may affect user behavior
- Design for robustness against potential attacks
  - Spoofability
  - Information overload
  - Warning fatigue

Phishing and Spear-Phishing

- Phishing: send emails asking people to log in to some site—but it's really a fake site
- Spear-phishing: send a message tailored to the target
- Spear-phishing may be a fake login or it may ask you to open attached malware

Spear-Phishing CS Faculty



From: Servedio Rocco <rocco.servedio65@gmail.com>
Subject: Quick Request
Date: February 13, 2020 at 5:26 PM
To: smb@cs.columbia.edu

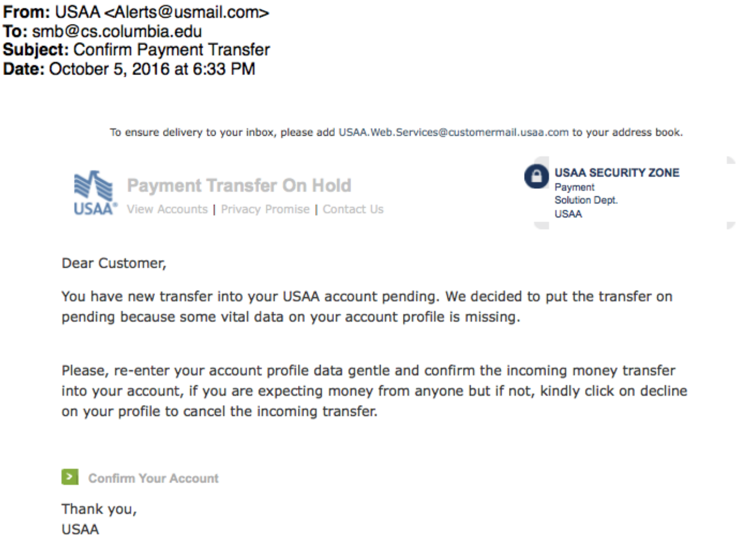
Send me your available text number that I can reach you on

--
Servedio, Rocco A.

Department Chair
Computer Science
Office: 450F CSB,517 CSB

Note the effort: actually looking up the then-department chair and his offices. I've received others purporting to be from then-Dean Boyce.

Sample Phishing Email



From: USAA <Alerts@usmail.com>
To: smb@cs.columbia.edu
Subject: Confirm Payment Transfer
Date: October 5, 2016 at 6:33 PM

To ensure delivery to your inbox, please add USAA.Web.Services@customermail.usaa.com to your address book.

Payment Transfer On Hold

USAA SECURITY ZONE
Payment
Solution Dept.
USAA

Dear Customer,

You have new transfer into your USAA account pending. We decided to put the transfer on pending because some vital data on your account profile is missing.

Please, re-enter your account profile data gentle and confirm the incoming money transfer into your account, if you are expecting money from anyone but if not, kindly click on decline on your profile to cancel the incoming transfer.

Thank you,
USAA

The John Podesta/Colin Powell Hacks

- Both received spear-phishing emails
- The link to be clicked on was via bit.ly, a link-shortening service
- Both fell for it. . .

Stopping Phishing?

- *Maybe* the users should be suspicious of bit.ly links—but with HTML email, you don't see the actual link unless you try
- Once you click on it, you must:
  - Recognize that the URL is bad (even though the better ones try hard to seem plausible)—in this case, the URL started `http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?`...
  - Or check that it's https and that the certificate is right
  - (The latter will fail against a high-end attacker)
- Mental overload—you're demanding too much of users!

What’s Better?

- The root issue: password-phishing works because too many people miss the subtle indicators that distinguish between real and fake sites
- Adding more indicators won’t solve it—people just *don’t* see them
- We have to automate the recognition or use non-replayable authentication

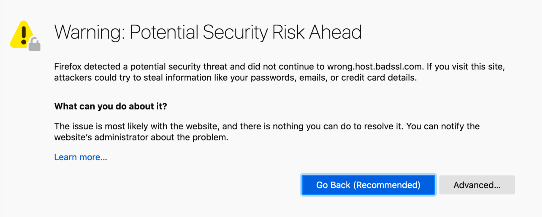
General Guidelines

- 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

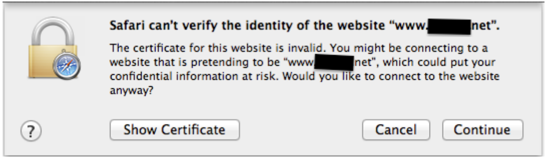


Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to wrong.host.badssl.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it. You can notify the website's administrator about the problem.



Safari can't verify the identity of the website "www.[redacted]net".

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

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

Note: this is just a *brief* overview; usable security and privacy is the subject of full-semester graduate classes

Interviews

- Very common technique
- Structured way to talk to your users—make a script first!
- Learn their needs and expectations
- Build the system to do the right thing
- Make sure users understand strengths and limits, and use it correctly
- Do your user really understand it? Is their mental model correct?
- Flesh out your understanding before more quantitative steps, e.g., surveys

Focus Groups

- Hard to execute well—not for amateurs
- Not the same as “10 interviews in one setting”
- A good technique when you have no idea where to start
- A way to understand what folks’ needs are

Cognitive Walk-Through

- Pretend to be the user
- 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, e.g., that no menu should have more than three levels
- 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

Other Human Problems

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 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?
- Manning herself wrote, “Weak servers, weak logging, weak physical security, weak counter-intelligence, inattentive signal analysis. . . a perfect storm”

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

The Clinton Email Server

- One likely reason: the official server was too secure
- If a system is too hard to use, people either won't use it or will take evasive measures
- My own opinion: the official `state.gov` email system was probably very inconvenient to use from outside networks
- Clinton was in a position to ignore the rules

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?

Two Types of Usability Problems

- The attacker will trick the user into doing something nasty—phishing and spear-phishing are common examples of this
- A user will not perform a security-sensitive operation correctly, thus leaving something vulnerable

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

Questions?

(Great horned owl, Central Park, January 26, 2022)