CSci 5271
Introduction to Computer Security
Day 24: Usability and security

Stephen McCamant

University of Minnesota, Computer Science & Engineering

Outline

Usability and security

Announcements intermission

Usable security example areas

Users are not 'ideal components'

- Frustrates engineers: cannot give users instructions like a computer
  - Closest approximation: military
- Unrealistic expectations are bad for security

Most users are benign and sensible

- On the other hand, you can't just treat users as adversaries
  - Some level of trust is inevitable
  - Your institution is not a prison
- Also need to take advantage of user common sense and expertise
  - A resource you can't afford to pass up

Don't blame users

- "User error" can be the end of a discussion
- This is a poor excuse
- Almost any "user error" could be avoidable with better systems and procedures

Users as rational

- Economic perspective: users have goals and pursue them
  - They're just not necessarily aligned with security
- Ignoring a security practice can be rational if the rewards is greater than the risk

Perspectives from psychology

- Users become habituated to experiences and processes
  - Learn "skill" of clicking OK in dialog boxes
- Heuristic factors affect perception of risk
  - Level of control, salience of examples
- Social pressures can override security rules
  - "Social engineering" attacks

User attention is a resource

- Users have limited attention to devote to security
  - Exaggeration: treat as fixed
- If you waste attention on unimportant things, it won't be available when you need it
- Fable of the boy who cried wolf

Research: ecological validity

- User behavior with respect to security is hard to study
- Experimental settings are not like real situations
- Subjects often:
  - Have little really at stake
  - Expect experimenters will protect them
  - Do what seems socially acceptable
  - Do what they think the experimenters want

Research: deception and ethics

- Have to be very careful about ethics of experiments with human subjects
  - Enforced by institutional review systems
- When is it acceptable to deceive subjects?
  - Many security problems naturally include deception

Outline

Usability and security

Announcements intermission

Usable security example areas

Exercise set 3: CCEA1/2

- Intent: not a Caesar cipher, just has 8-bit block
- What's the largest possible key space size?
- Collision dangers with block ciphers?
- Chosen-plaintext attack against block cipher

Final exam Monday 12/18

- Same room (ME 108), 8:00am-10:00am
- Similar to midterm:
  - Open-book, open-notes
  - Multiple-choice and exercise-like questions
- Slightly longer than midterm
- Comprehensive, but weighted slightly toward second half of course

Other events this week

- Exercise set 4 due Tuesday night
- Group progress meetings (a few not yet scheduled)

Upcoming project schedule

- Last progress report due next Monday
- Presentations start next Wednesday
- Planned scheduling: initially random
  - Swaps allowed with agreement of both groups
  - Trust me to generate random numbers?

Outline

Usability and security

Announcements intermission

Usable security example areas

Email encryption

- Technology became available with PGP in the early 90s
- Classic depressing study: "Why Johnny can't encrypt: a usability evaluation of PGP 5.0" (USENIX Security 1999)
- Still an open "challenge problem"
- Also some other non-UI difficulties: adoption, govt. policy

Phishing

- Attacker sends email appearing to come from an institution you trust
- Links to web site where you type your password, etc.
- *Spear phishing*: individually targeted, can be much more effective

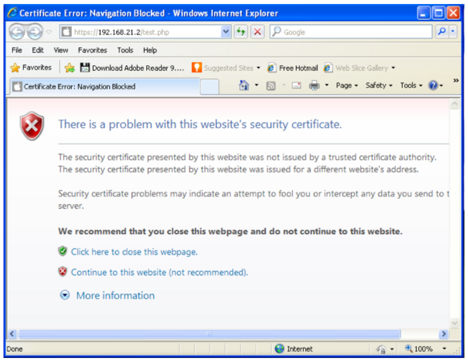
Phishing defenses

- Educate users to pay attention to X:
  - Spelling → copy from real emails
  - URL → homograph attacks
  - SSL "lock" icon → fake lock icon, or SSL-hosted attack
- Extended validation (green bar) certificates
- Phishing URL blacklists

SSL warnings: prevalence

- Browsers will warn on SSL certificate problems
- In the wild, most are false positives
  - `foo.com` vs. `www.foo.com`
  - Recently expired
  - Technical problems with validation
  - Self-signed certificates (HA2)
- Classic warning-fatigue danger

Older SSL warning


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://192.168.21.2/test.php
Google
File
Edit
View
Favorites
Tools
Help
Favorites
Download Adobe Reader 9....
Suggested Sites
Free Hotmail
Web Slice Gallery
Certificate Error: Navigation Blocked
Page
Safety
Tools
Done
Internet
100%

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to t
server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

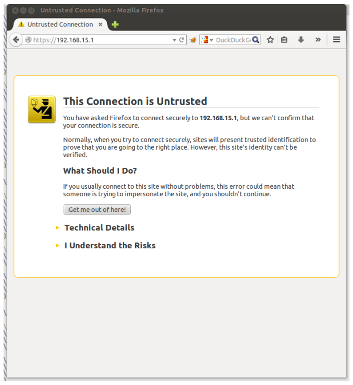
Continue to this website (not recommended).

More information

SSL warnings: effectiveness

- Early warnings fared very poorly in lab settings
- Recent browsers have a new generation of designs:
  - Harder to click through mindlessly
  - Persistent storage of exceptions
- Recent telemetry study: they work pretty well

Modern Firefox warning



This Connection is Untrusted

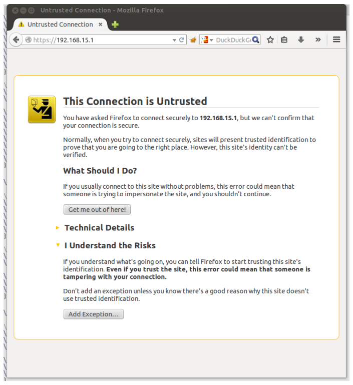
You have asked Firefox to connect securely to **192.168.15.1**, but we can't confirm that your connection is secure.

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.

Modern Firefox warning (2)



This Connection is Untrusted

You have asked Firefox to connect securely to **192.168.15.1**, 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.

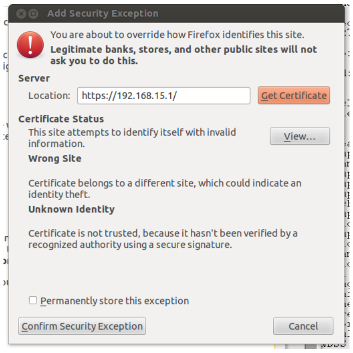
What Should I Do?

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.

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Modern Firefox warning (3)



You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://192.168.15.1/

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

Certificate belongs to a different site, which could indicate an identity theft.

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature.

□ Permanently store this exception

Confirm Security Exception

Spam-advertised purchases

- “Replica” Rolex watches, herbal `V!@gr@`, etc.
- This business is clearly unscrupulous; if I pay, will I get anything at all?
- Empirical answer: yes, almost always
  - Not a scam, a black market
  - Importance of credit-card bank relationships

Advance fee fraud

- “Why do Nigerian Scammers say they are from Nigeria?” (Herley, WEIS 2012)
- Short answer: false positives
  - Sending spam is cheap
  - But, luring victims is expensive
  - Scammer wants to minimize victims who respond but ultimately don’t pay

Trusted UI

- Tricky to ask users to make trust decisions based on UI appearance
  - Lock icon in browser, etc.
- Attacking code can draw lookalike indicators
  - Lock favicon
  - Picture-in-picture attack

Smartphone app permissions

- Smartphone OSes have more fine-grained per-application permissions
  - Access to GPS, microphone
  - Access to address book
  - Make calls
- Phone also has more tempting targets
- Users install more apps from small providers

Permissions manifest

- Android approach: present listed of requested permissions at install time
- Can be hard question to answer hypothetically
  - Users may have hard time understanding implications
- User choices seem to put low value on privacy

Time-of-use checks

- iOS approach: for narrower set of permissions, ask on each use
- Proper context makes decisions clearer
- But, have to avoid asking about common things
- iOS app store is also more closely curated

Trusted UI for privileged actions

- Trusted UI works better when asking permission (e.g., Oakland'12)
- Say, "take picture" button in phone app
  - Requested by app
  - Drawn and interpreted by OS
  - OS well positioned to be sure click is real
- Little value to attacker in drawing fake button