CSci 4271W
Development of Secure Software Systems
Day 27: Legal aspects and usability

Stephen McCamant
University of Minnesota, Computer Science & Engineering

Outline

Ethics and security, cont'd

Announcements intermission

Legal context for security

Usability and security

Usable security example areas

Beyond white and black hats

- In describing techniques, we posit a clear distinction of attackers and defenders
- But in real scenarios, you can't assume that attacker = bad and defender = good
- What follows are some specific situations showing more complexity

Responsible disclosure

- If you find a vulnerability in software, who should you tell about it? Two extremes:
  - Only the author/vendor ever needs to know
  - Make the information fully public right away (full disclosure)
- Security researchers often push on vendors for more and faster disclosure
- A common compromise is to give vendors a head start, but with a deadline
  - E.g., Google uses 90 days (or 7 days if being used)

Nation states

- Many governments would argue they need to break the security of criminals or foreign spies
  - "justice", "public safety", "national security", etc.
- "Cyber-warfare" has both offensive and defensive aspects
  - Compare with various ethical perspectives on killing in war

Interoperability and repair

- Vendors of devices can have economic desires to control how the devices interact with other devices or can be repaired
  - Classic example: expensive proprietary ink cartridges
- If vendors use security and cryptography techniques to implement these restrictions, is it ethical to attack them?

Copy protection and DRM

- Vendors of software and media would prefer you can't make copies to give to your friends
  - Many generations of attempts to implement such restrictions
  - Fundamentally hard, because the data must be decoded to be used
  - Keeping software from being reverse engineered is also hard
- Do the ethics depend on how competent the technique is?

Malware analysis

- Labeling software as malicious is defining it to be the evil side
  - E.g., viruses, botnet clients
- Leads to many software security concerns being inverted
- Preventing reverse engineering is a common goal of DRM software and malware

Outline

Ethics and security, cont'd

Announcements intermission

Legal context for security

Usability and security

Usable security example areas

Upcoming events

- Project 1 second submission due date is Friday
  - Sample attacks available now
  - First submission suggestions planned for late tonight
  - Clarifications and discussions on Piazza
- SRTs open now, we will also make time in Thursday's lecture for them
- The final course activity will be a lab next Monday

Outline

Ethics and security, cont'd

Announcements intermission

Legal context for security

Usability and security

Usable security example areas

Mostly US federal law

- In the US, federal law is most important in computing
  - State laws are hard to enforce across the Internet
- Other countries have their own laws that differ in details
- Treaties and international effects are sometimes also important

Benefits and costs of law/regulation

+ Enforce ethical norms on otherwise reluctant parties
  - Especially: criminals, large corporations
- Interested parties lobby for laws favorable to them
- Laws can easily fall behind technology development
- Extra costs of complying with laws

Intellectual property

- Patents: useful inventions, ~20 years
- Copyrights: fixed expressions, ~100 years
- Trademarks: business identifiers, unlimited
- Trade secrets: supplementing contracts, unlimited

Privacy?

- No law provides general protection of personal privacy
  - Gap partially filled by agency regulation
- Two major industries have specific laws:
  - FERPA in education
  - HIPAA in health care (the P doesn't stand for privacy)

CFAA

- Computer Fraud and Abuse Act of 1986
- Civil and criminal liability for "unauthorized access" to a computer
- Gradually extended to cover any computer, and many related activities
- Potentially applied to any contract or terms-of-service violation
  - Not always successfully

Example: Randal Schwartz

- Schwartz worked as a contract sysadmin several Intel divisions
- He ran a password cracking program and moved password files between machines in a division he no longer worked for
- He was convicted of three felonies under an Oregon state law
  - Similar to the CFAA, somewhat more vague

DMCA

- Digital Millennium Copyright Act of 1998
- Legally reinforces DRM by criminalizing "circumvention" and tools that perform it
- But, can violate without violating copyright
  - App stores, video game bots, garage door openers
- A narrow exemptions process is growing in application

Example: Sony BMG "rootkit"

- In 2005, sold CDs with software that modified a Windows or Mac OS to interfere with copying
- To prevent removal, the software used techniques usually used by malicious software
  - A "rootkit" is backdoor software installed on a compromised machine
  - Common techniques include hiding files and processes
- Led to a recall, class action suits, FTC settlement, etc.

Outline

Ethics and security, cont'd

Announcements intermission

Legal context for security

Usability and security

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

Ethics and security, cont'd

Announcements intermission

Legal context for security

Usability and security

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

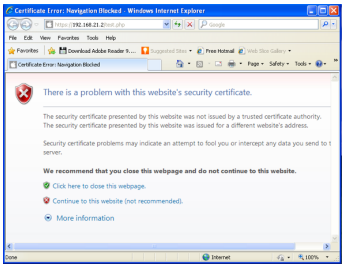
Phishing defenses

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

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

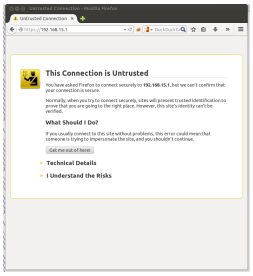
Older SSL warning



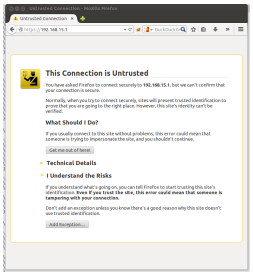
SSL warnings: effectiveness

- 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

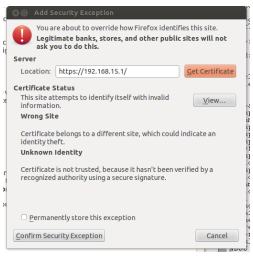
Modern Firefox warning



Modern Firefox warning (2)



Modern Firefox warning (3)



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