CSE 484 / CSE M 584: Computer Security and Privacy

Usable Security [finish] & Physical Security

Spring 2016

Franziska (Franzi) Roesner
franzi@cs.washington.edu

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Question

- **Q.** What are the root causes of usability issues in computer security?

Why is Usable Security Hard?

1. Lack of intuition
   - See a safe, understand threats. Not true for computers.
2. Who's in charge?
   - Doctors keep your medical records safe, you manage your passwords.
3. Hard to gauge risks
   - "It would never happen to me!"
4. No accountability
   - Asset-holder is not the only one you can lose assets.
5. Awkward, annoying, or difficult
6. Social issues

Question

- **Q.** What approaches can we take to mitigate usability issues in computer security?

Response #1: Education and Training

- Education:
  - Teaching technical concepts, risks

- Training
  - Change behavior through:
    - Drill
    - Monitoring
    - Feedback
    - Reinforcement
    - Punishment

- May be part of the solution – but not the solution

Response #2: Security Should Be Invisible

- Security should happen
  - Naturally
  - By Default
  - Without user input or understanding

- Recognize and stop bad actions
- Starting to see some invisibility
  - SSL/TLS
  - VPNs
  - Automatic Security Updates
  - User-driven access control

Response #2: Security Should Be Invisible

- "Easy" at extremes, or for simple examples
  - Don't give everyone access to everything
- But hard to generalize
- Leads to things not working for reasons user doesn't understand
- Users will then try to get the system to work, possibly further reducing security
  - E.g., "dangerous successes" for password managers

Response #3: "3 Word UI": "Are You Sure?"

- Security should be invisible
  - Except when the user tries something dangerous
  - In which case a warning is given
- But how do users evaluate the warning? Two realistic cases:
  - Always heed warning. But see problems / commonality with Response #2 ("security should be invisible")
  - Always ignore the warning. If so, then how can it be effective?

Response #4: Focus on Users, Use Metaphors

- Clear, understandable metaphors:
  - Physical analogs; e.g., red-green lights
- User-centered design: Start with user model
- Unified security model across applications
  - User doesn’t need to learn many models, one for each application
- Meaningful, intuitive user input
  - Don’t assume things on user’s behalf
  - Figure out how to ask so that user can answer intelligently

Response #5: Least Resistance

- “Match the most comfortable way to do tasks with the least granting of authority”
  - Ka-Ping Yee, Security and Usability
- Should be “easy” to comply with security policy
- “Users value and want security and privacy, but they regard them only as secondary to completing the primary tasks”
  - Karat et al, Security and Usability

Now: Physical Security

- Relate physical security to computer security
  - Locks, safes, etc
- Why?
  - More similar than you might think!
  - Lots to learn:
    - Computer security issues are often abstract; hard to relate to
    - But physical security issues are often easier to understand
  - Hypothesis:
    - Thinking about the "physical world" in new (security) ways will help you further develop the "security mindset"
    - You can then apply this mindset to computer systems, …

Lockpicking

- The following slides will not be online.
- But if you're interested in the subject, we recommend:
  - Blaze, "Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks"
  - Blaze, "Safecracking for the Computer Scientist"
  - Tool, "Guide to Lock Picking"
  - Tobias, "Opening Locks by Bumping in Five Seconds or Less"
- Careful: possessing lock picks is legal in Washington State, but not everywhere!