**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
- 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:
  - 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

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
<table>
<thead>
<tr>
<th>Time-of-use checks</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS approach: for narrower set of permissions, ask on each use</td>
</tr>
<tr>
<td>Proper context makes decisions clearer</td>
</tr>
<tr>
<td>But, have to avoid asking about common things</td>
</tr>
<tr>
<td>iOS app store is also more closely curated</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trusted UI for privileged actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted UI works better when asking permission (e.g., Oakland'12)</td>
</tr>
<tr>
<td>Say, “take picture” button in phone app</td>
</tr>
<tr>
<td>Requested by app</td>
</tr>
<tr>
<td>Drawn and interpreted by OS</td>
</tr>
<tr>
<td>OS well positioned to be sure click is real</td>
</tr>
<tr>
<td>Little value to attacker in drawing fake button</td>
</tr>
</tbody>
</table>