Identity numbers: mostly unhelpful
- Common US example: social security number
- Variously used as an identifier or an authenticator
  - Dual use is itself a cause for concern
- Known by many third parties (e.g., banks)
- No checksum, guessing risks
- Published soon after a person dies

"Identity theft"
- The first-order crime is impersonation fraud between two other parties
  - E.g., criminal trying to get money from a bank under false pretenses
- The impersonated "victim" is effectively victimized by follow-on false statements
  - E.g., by credit reporting agencies
- These costs are arguably the result of poor regulatory choices
- Be careful w/ negative info from 3rd parties

Backup auth suggestion: use time
- Need for backup often comes for infrequently-used accounts
- May be acceptable to slow down recovery if it reduces attack risk
  - Account recovery is a hassle anyway
- Time can allow legitimate owner to notice malicious request

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

Names and identities, cont’d
Usability and security
Logistics announcements
Usable security example areas

Writing feedback plan

If you submitted a draft of your project report by last Friday, I’ll have the writing feedback posted by tomorrow
**Project late/extension policy**

As was originally announced, you will be able to request an extension of the project due date until Monday evening 5/3.

But, to preserve an incentive to submit on time, submissions by Friday will get 10% extra credit.

**Last parts of the course**

- Thursday 4/29 is the last lecture
- And will include a break for course evaluations
- Monday 5/3 is the last lab
- No meetings or assignments during finals

**Grade weighting**

- Original plan was 60% projects, 20% psets, 10% labs, 5% lecture attendance, 5% reading questions.
- But fewer projects and psets than planned.
- I will also compute based on a rebalanced weighting, and use whichever is higher.
- E.g., 35/20/25/10/10

**Outline**

- Names and identities, cont’d
- Usability and security
- Logistics announcements
- 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, government 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

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