Workplace Privacy & Security

Wrapping up Loose Ends

- Wrapping up ID Theft
- Workplace privacy & considerations
- Encryption

Next week:
- Software Failures
- Online/Electronic voting
Wrapping up ID Theft

What is Identity Theft

“Identity theft and identity fraud are terms used to refer to all types of crime in which someone **wrongfully obtains and uses another person's personal data** in some way that involves fraud or deception, typically for economic gain.”  **U.S. Dept. of Justice**

http://www.usdoj.gov/criminal/fraud/idtheft.html
Types of Identity Theft


Who's at Risk

Cost of Identity Theft

- Financial Costs:

<table>
<thead>
<tr>
<th>Year</th>
<th># of victims</th>
<th>Average Loss</th>
<th>Total Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>8.4 million</td>
<td>$6,483</td>
<td>$56.6 Billion</td>
</tr>
<tr>
<td>2006</td>
<td>9.3 million</td>
<td>$6,278</td>
<td>$55.7 Billion</td>
</tr>
<tr>
<td>2007</td>
<td>10.1 million</td>
<td>$5,720</td>
<td>$49.3 Billion</td>
</tr>
</tbody>
</table>

- Plus time to fix record (mean=25h, Avg=5hr)

http://www.privacyrights.org/ar/idtheftsurveys.htm

Sources of misused data

- Lost or stolen wallets
- Information misuse by family, friends, colleagues
- Dumpster diving
- Pretexting/social engineering
- Online scams & tracking
- Data brokers
SSN

- Social Security cards first issued 1936
- Originally used only for SS purposes
- Use of SSN has gradually increased
- SSN is a poor identification number
  - Not unique
  - Rarely checked
  - No error-detecting capability

Who's responsible for fixing problems?

- You!
- Get help from:
  - Federal Trade Commission
  - Credit Card issuer/Bank
  - Internet Service Provider
Workplace Privacy

- Employee Polygraph Protection Act 1988
  - Prohibits private employers from using lie detector tests under most conditions
  - Cannot require test for employment
- Exceptions
  - Pharmaceutical companies and security firms may give test to certain classes of employees
  - Employers who have suffered a theft may administer tests to reasonable suspects
  - Federal, state, and local governments exempt
Workplace Privacy

- What is protected?
- Email
  - Work email?
  - Private email accessed from work?
- Packet sniffers?
- Keystroke loggers?
- Telephone monitoring?
- Video monitoring?
- Location information?

Workplace Controversies

- Non-compete contract clauses
- Who owns IP you produce?
- Overtime?
- Use of contractors vs. full-time employees
- Grounds for dismissal?
Encryption

Encryption Overview

- Process of transforming a message in such a way as to conceal its meaning to all but the intended recipient
- Valuable tool for maintaining privacy
- Necessary building block for e-commerce, networking, security

- Famous Cyphers
  - The Caesar Cypher
  - The Navajo code talkers
  - Enigma
**Kryptos**

---

**Two main branches of encryption**

**Symmetric encryption**
- Single key used to encrypt and decrypt a message
- Both sender and receiver must have the key
- Problem: How does sender get key to receiver?
- If “bad guy” gets key, security is broken

**Asymmetric encryption**
- Each person has two keys: public and private
- To send R a message, encrypt it with R’s public key
- R decrypts message with R’s private key
- No need to communicate keys
PGP - Pretty Good Privacy

- An example of asymmetric encryption
- Strong encryption: virtually impossible to figure out private key, given public key
- U.S. had export restrictions on strong encryption technology

History
- Phil Zimmerman created PGP in 1991
- He made it available on Internet
- Many people downloaded PGP
- U.S. government threatened legal action
- PGP source code released in book form in 1995
- US government drops case in 1996

US approach - Government Sanctioned Security

- “Clipper”: NSA’s encryption technology
- 1993: President Clinton announced Clipper as national standard for telephone encryption
- Justice Department issued guidelines for release of keys
- Huge public outcry
- 1994: Clipper designated a voluntary standard
Do Export Restrictions Make Sense?

- We can stop the export of software, but not the sharing of the technical knowhow or the source code
- Additional burden on U.S. software industry
  - Strong encryption okay for U.S. customers
  - Weak encryption needed for foreign customers
- Reduced international competitiveness of U.S. companies
- Two federal appeals courts ruled export restrictions violated freedom of speech (1999, 2000)
- U.S. State Department dropped export restrictions
- FBI Director Louis Freeh argued for restrictions in 2004
- US passport RFID information