Protecting Privacy

"Most people have figured out by now you can't do anything on the Web without leaving a record"
- Holman W. Jenkins, Jr. 2000

Enhancing Privacy for Consumers

Many technologies developed over time

- Cookie disablers
- Web browsers add alert about cookies
- Software to block pop-up ads
- Security software that scan PCs and detect spyware
- Anonymizers
- Need permissions to access some web / blogs
- Self-destructing emails

Encryption

- “Cryptography is the art and science of hiding data in plain sight”
- Used to protect data in transit and also stored information
- Includes a cryptographic algorithm, and keys. A very simple one: a scrambled alphabet
- Usually the longer the key, the more difficult to break the cipher
- Government ban on export of strong encryption software in the 1990s (removed in 2000)

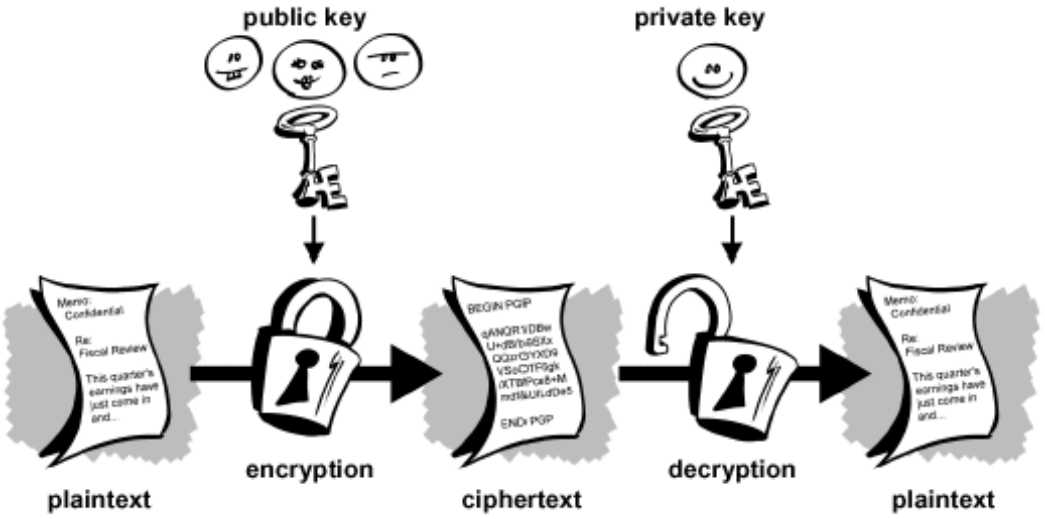
Public-Key Encryption (PKE) (1)

- Keys are secret information that is critical to the security/success of the scheme. Can be numbers, strings, etc.
- In PKE, keys come in a pair:
  - one is made public to the world, called public key
  - one is kept only to oneself, called private key
- To provides "confidentiality", i.e., only B can see the content of a received message
  - A sender encrypts with B's public key and sends it
  - B decrypts with B's private key

Public Key Encryption (2)

- To provide "authentication", we say entity A signs a document
  - To do so, A encrypts with A's private key and sends it
  - The receiver decrypts with A's public key to verify

confidentiality



Business Tools and Policies

- Audit trail of all data accesses
- Web sites pay $$$ to privacy audits companies
  - Check for info. leaks, review privacy policies, evaluate compliance to policies
- Large businesses hire a chief privacy officer
- BBB and TRUSTe seals for meeting privacy standards

Rights and Laws

Free Market View

- Freedom of consumers to make voluntary agreements
- Diversity of individual tastes and values
- Response of the market to consumer preferences
- Usefulness of contracts
- Flaws of regulatory solutions

Rights and Laws

Consumer Protection View

- Uses of personal information
- Costly and disruptive results of errors in databases
- Ease with which personal information leaks out
- Consumers need protection from their own lack of knowledge, judgment, or interest through privacy regulations

Wiretapping and E-Mail Protection

- Telephone
  - 1934 Communications Act prohibited interception of messages that is not authorized by the sender
  - 1968 Omnibus Crime Control and Safe Streets Act allowed wiretapping and electronic surveillance by law-enforcement (with court order)
- E-mail and other new communications
  - Electronic Communications Privacy Act of 1986 (ECPA) extended the 1968 wiretapping laws to include electronic communications, restricts government access to e-mail
  - Patriot Act loosens restrictions on government surveillance and wiretapping

Designing for Interception

- Communications Assistance for Law Enforcement Act of 1994 (CALEA)
  - Telecommunications equipment must be designed to ensure government can intercept telephone calls (with a court order or other authorization)
  - Rules and requirements written by Federal Communications Commission (FCC), which ruled that CALEA requirements extend to new services (cell phones and Internet phones)
  - Arguments in favor and against CALEA

Secret Intelligence Gathering

- The National Security Agency (NSA)
  - Collects and analyzes foreign intelligence data related to national security
  - Protects US Government communications
  - Prohibited from intercepting communications within the US
- Foreign Intelligence Surveillance Act (FISA) established oversight rules for the NSA
- Secret access to communications records

Discussion Questions

- What types of communication exist today that did not exist in 1968 when wiretapping was finally approved for law-enforcement agencies?
- What type of electronic communications do you use on a regular basis?