Chapter 13

Shhh, It's a Secret: Privacy and Digital Security

Many countries state privacy as a right of citizens.

The U.S. Constitution does not grant privacy, but it is granted through other rights and laws.
Whose information is it?

- Paying by check, credit card, or debit card?
- Purchasing through mail order or on the Internet?
- Providing a "preferred customer" card or number?
- Buying a product that must be registered for a service agreement or warranty?
How can the information be used?

Imagine you buy a book from Amazon titled, "Dating for Dummies."

What advertisements will Amazon send in the future based on your purchase?

Who else would be interested in the information?

Could this affect your future?
Information Control Possibilities

- No Uses
- Approval or Opt-in
- Objections or Opt-out
- No Limits
Privacy

The right of people to choose freely under what circumstances and to what extent they will reveal themselves, their attitude, and their behavior to others.
Privacy Threats

- Governments
  - Surveillance / Protection
  - Political Threats
- Businesses
  - Advertisements
  - Identity Theft
- Friends and Family
Voluntary Disclosure

- We tell doctors personal facts so that we can get better treatment.
- We allow background credit checks in exchange for using credit.
- We permit employers to read out email and monitor our Internet connections and usage.
- We reveal to the government facts about ourself to enjoy citizenship.
Social Networking Disclosure

- Facebook
- MySpace
- Twitter
- Flickr
- Cy World
- Mixi
- Google Buzz
- Live Journal
- Blogger
- YouTube
- Orkut
- News article comments
OECD Fair Information Practices

- Limited Collection Principle
- Quality Principle
- Purpose Principle
- Use Limitation Principle
- Security Principle
- Openness Principle
- Participation Principle
- Accountability Principle
Privacy often comes in conflict with private or governmental interests.
Privacy Related Laws

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- U.S. Patriot Act of 2002
Other U.S. Laws Protecting Privacy

- Electronic Communications Privacy Act of 1986
- Video Privacy Protection Act of 1988
- Telephone Consumer Protection Act of 1991
- Driver's Privacy Protection Act of 1994
- Health Insurance Privacy and Accountability Act of 1996
Voluntary Compliance?

Privacy consultant Richard M. Smith discovered in November 1999 that Real Networks' JukeBox software was gathering music taste profiles based on users' unique IDs. The Company had a privacy policy, but it did not mention the unique ID or the profiling activity, until he caught them. Further, Real Networks had hired the audit firm TRUSTe.
Since the U.S. Government set up the Do-Not-Call list, more than 100 million people have registered, and the telemarketing business has largely collapsed.
Cookies are pieces of information stored with the rest of your browsers information. Each cookie lists the site that it should be sent to. When you connect to that site, the cookie is also sent. This allows sites to keep track of you by having your browser store a unique ID from the site.
Finding Cookies

Modern browsers let you control the cookie policy for your computer. Many of them also allow you to see the cookies. Many browsers can be either natively or through third party applications configured to give you the ability to edit cookies.
Many sites also include advertisements. These advertisements are often from third party websites. When your browser sees the third party request, it requests the advertisement, but also includes information about the referring site. The third party site is able to maintain cookies about you, and gives credit to the referring site.
Identity Theft

The crime of posing as someone else for fraudulent purposes.
Protecting Privacy

- Up-to-date virus checking software
- Adjust cookie settings to a comfortable level
- Read privacy statements on sites
- Avoid phishing scams
- Patronize reputable companies for downloaded files
- Be familiar with current assaults on privacy
- Lobby U.S. for better laws
Many early Internet applications used plaintext transfer methods for exchanging data. These allowed unauthorized viewing by not preventing people from seeing the traffic as it was passing by.
Cryptosystems

The process of encrypting cleartext or plaintext into cipher text for transmission, then decrypting the cipher text back into cleartext or plaintext at the destination.
XOR Encryption Operation

Encryption

0101 0110 1111 1010 Cleartext
XOR 1010 1110 0101 0010 Key
1111 1000 1010 1000 Cipher text

Decryption

1111 1000 1010 1000 Cipher text
XOR 1010 1110 0101 0010 Key
0101 0110 1111 1010 Cleartext
Imagine you have two people Alice and Bob. Alice wants to send a key to Bob, but does not want Eve, a spy to listen in on the conversation. How can this be done?

\[(g^a)^b = (g^b)^a\]
RSA Public Key Cryptosystems

p and q are prime. Compute $n = pq$.
Choose $e$ with $\gcd(e, (p-1)(q-1)) = 1$
Compute $d$ with $de \mod (p-1)(q-1) = 1$
Public key is $n$ and $e$
Private key is $p$, $q$, and $d$

Encrypt $m$ using $m^e \mod n = c$
Decrypt $m$ using $c^d \mod n = e$
Breaking RSA

- You can break the cryptosystem if you can factor the public key.
- You can break the cryptosystem if you can pretend to be the other person.
- You can break the cryptosystem if you know the private key.
Key Escrow

The idea of key escrow is that people are required to register the prime numbers $p$ and $q$. If there is ever a need to break the encryption for something like law enforcement personnel having a court approved warrant or you needing to recover encrypted data, the escrow could provide the numbers.

Who would use the service?
Backing up Personal Data

- Backup data that cannot be recreated from permanent sources.
- Backup files that have been changed since you last backed them up.
- Backup documents and files that you care about.