Chapter 13: Shhh, It's a Secret: Privacy and Digital Security

Fluency with Information Technology
Third Edition

by
Lawrence Snyder

Privacy: Whose Information Is It?

- What is privacy? Examine a transaction of buying *Dating for Total Dummies*
  - Information linking the purchase with the customer
- How can the information be used?
  - Book merchant collecting information is ordinary business practice
  - Book merchant sending advertisements to customer is ordinary business practice
  - What about merchant selling information to other businesses?

Modern Devices and Privacy

- Modern devices make it possible to violate people's privacy without their knowledge
- In 1890, Brandeis wrote that individuals deserve "sufficient safeguards against improper circulation" of their images

Controlling the Use of Information

- Spectrum of control spans four main possibilities:
  1. **No uses**. Information should be deleted when the store is finished with it
  2. **Approval or Opt-in**. Store can use it for other purposes with customer's approval
  3. **Objection or Opt-out**. Store can use it for other purposes if customer does not object
  4. **No limits**. Information can be used any way the store chooses
  5. Fifth possibility is **internal use**—store can use information to continue conducting business with you

A Privacy Definition

- 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
- Threats to Privacy: Government and business
- Voluntary Disclosure: We choose to reveal information in return for real benefits (doctor, credit card company)

Fair Information Practices

- OECD (Organization of Economic Cooperation and Development) in 1980 developed the standard eight-point list of privacy principles.
  - Limited Collection Principle
  - Quality Principle
  - Purpose Principle
  - Use Limitation Principle
  - Security Principle
  - Openness Principle
  - Participation Principle
  - Accountability Principle

Comparing Privacy Across the Atlantic

- U.S. has not adopted OECD principles
- China does not protect privacy
- European Union has European Data Protection Directive (OECD principles)
- EU Directive requires data on EU citizens to be protected at same standard even when it leaves their country

US Laws Protecting Privacy

- Privacy Act of 1974 covers interaction with government
- Interactions with business:
  - Electronic Communication 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
- These all deal with specific business sectors—not an omnibus solution

Privacy Principles: European Union

- Two points of disagreement between FTC (US) and OECD (Europe):
  - Opt-in/Opt-out
    - When can an organization use information it collects for one purpose, for a different purpose?
    - Opt-out is US standard except for highly sensitive data; Opt-in is European standard
  - Compliance/Enforcement
    - US has "voluntary compliance," EU has offices to control data

A Privacy Success Story

- Do-Not-Call List
  - Telemarketing industry's "self-policing" mechanism required individuals to write a letter or pay an on-line fee to stop telemarketing calls
  - US government set up Do-Not-Call List. Over 107,000,000 households are on the list and telemarketing industry has largely collapsed

The Cookie Monster

- *Cookie*: Record containing seven fields of information that uniquely identify a customer's session on a website. Cookie is stored on customer's hard drive.
- Abuse: Third-party cookie
  - Third party advertisers on web site enter client/server relationship with customer as page loads
  - Advertiser can set cookies, and can access cookies when user views other websites that advertiser uses

The Cookie Monster (Cont'd)

- Browser options:
  - Turn off cookies
  - Ask each time a server wants to set a cookie
  - Accept all cookies

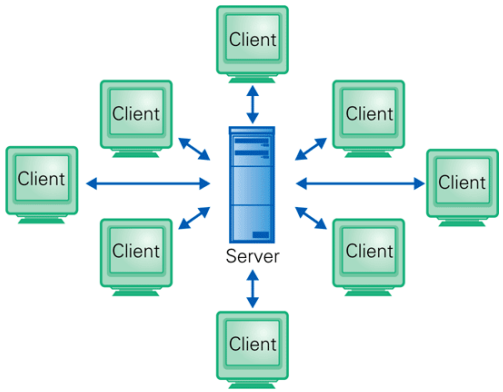

Figure 13.1 Server's view of the client/server relationship.

Identity Theft

- Americans do not enjoy the *Security Principle*
  - Those who hold private information are obliged to maintain its privacy against unauthorized access and other hazards
- *Identity theft* is the crime of posing as someone else for fraudulent purposes
  - Using information about person like credit card numbers, social security numbers

Managing Your Privacy

- Purchase up-to-date anti-virus/anti-spyware software
- Adjust your cookie preferences to match your comfort level
- Read the privacy statement of any website you give information to
- Review protections against phishing scams

Managing Your Privacy (cont'd)

- Patronize reputable companies for music, software, etc.
- Be skeptical
- Stay familiar with current assaults on privacy
- Lobby for US adoption of Fair Information Practices

Encryption And Decryption

- Encryption Terminology
  - *Encryption*: Transform representation so it is no longer understandable
  - *Cryptosystem*: A combination of encryption and decryption methods
  - *Cleartext* or *Plaintext*: Information before encryption
  - *Cipher text*: Information in encrypted form
  - *One-way cipher*: Encryption system that cannot be easily reversed (used for passwords)
  - *Decryption*: Reversing encryption process

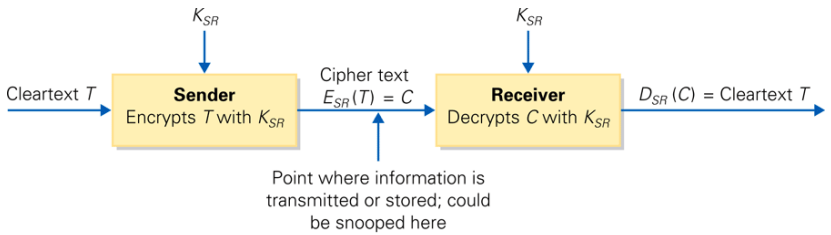

Figure 13.2 Schematic diagram of a cryptosystem. Using a key K_{SR} known only to them, the sender encrypts the cleartext information to produce a cipher text, and the receiver decrypts the cipher text to recover the cleartext.

XOR: An Encryption Operation

- Exclusive OR: Interesting way to apply a key to cleartext
- Combines two bits by rule: If the bits are the same, the result is 0; if the bits are different, the result is 1
- XOR is its own inverse (to decrypt back to original text)

Encrypting a Message

- Two students writing messages to each other decide to encrypt them
- Key is 0001 0111 0010 1101
- They use XOR encryption
- First write down ASCII representation of the letters in pairs
- XOR each resulting 16-bit sequence with their key
- If any bit sequence is XORed with another bit sequence and the result is XORed again with the same key, the result is the original bit sequence
- It makes no difference if the key is on the left or right

Cleartext					Key				Cipher Text				
Me	0100	1101	0110	0101					0101	1010	0100	1000	ZH
et	0110	0101	0111	0100					0111	0010	0101	1001	rY
@1	0100	0000	0011	0001					0101	0111	0001	1100	W^{F}_{S}
2:	0011	0010	0011	1010	⊕	0001	0111	0010	0010	0101	0001	0111	$\%^{E}_{\Sigma}$
15	0011	0001	0011	0101					0010	0110	0001	1000	$\&^{C}_{N}$
@J	0100	0000	0100	1010					0101	0111	0110	0111	Wg
oe	0110	1111	0110	0101					0111	1000	0100	1000	xH
's	0010	0111	0111	0010					0011	0000	0101	1111	0_

Figure 13.3 Encrypting the cleartext `Meet@12:15@Joe's`, using ASCII encoding of letter pairs, the key `0001 0111 0010 1101`, and the operation of exclusive OR to produce the cipher text ZHrYW$^{F}_{S}$%$^{E}_{\Sigma}$&$^{C}_{N}$WgxH0_. (Decryption works in the opposite direction, as if the "⊕" and "=" symbols of the figure were exchanged.)

Breaking the Code

- Longer text is easier to decode
  - Notice what bit sequences show up frequently
  - Knowledge of most frequent letters in the cleartext language
    - e is the most common letter in English
- Smarter byte-for-byte substitutions
  - Group more than two bytes
  - Be sure not to exchange the key over unsecured connection

Public Key Cryptosystems

- People who want to securely receive information publish a key that senders should use to encrypt messages
- Key is chosen so only receiver can decode

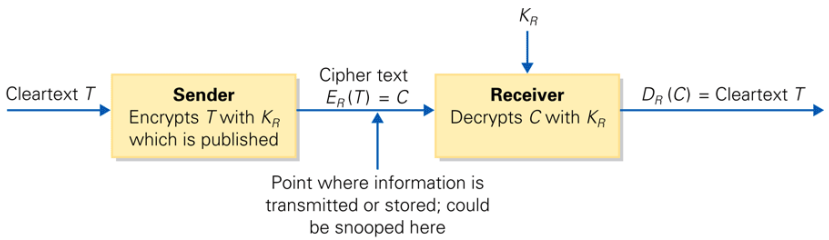

Figure 13.4 Public key cryptosystem. The sender uses the receiver's public key K_R to encrypt the cleartext, and only the receiver is able to decrypt it to recover the cleartext.

Code Cracker's Problem

- How is it secure when the key is published?
- All that is sent is the remainder
  - Bits left over from dividing manipulated data by the key
- So how can the receiver decrypt?

RSA Public Key Cryptosystem

- Relies on prime numbers
- Any number can be factored into primes in only one way
- Choosing a Key:
  - Key has special properties
    - Must be the product of two different prime numbers, *p* and *q*
      - $K_R = pq$
    - *p* and *q* must be about 64 or 65 digits long to produce a 129-digit public key
    - *p* and *q* must also be 2 greater than a multiple of 3

Encrypting a Message

- Divide cleartext into blocks
- Cube the blocks
- Divide the cubes by the public key
- Transmit the remainders from the divisions

The Decryption Method

- Compute the quantity s = (1/3)(2(p-1)(q-1) + 1)
- If the cipher text numbers C are each raised to the s power, C^s, and divided by the key K_R, the remainders T are the cleartext
- That is for some quotient d that we don't care about:
  - $C^s = K_R * d + T$

Summarizing the RSA System

- Three steps:
  - Publishing
  - Encrypting
  - Decrypting
- As long as *p*, *q*, and *s* are kept secret, code can't be cracked
  - If the key is large enough, factoring to find p and q can't be done in any reasonable amount of time even by software

Strong Encryption Techniques

- A communicating party can use the technology to protect their communication so no one else can read it, period
- Government agencies would like this technology kept out of the hands of "bad guys"
- What if cryptography software vendors had to give government a way to break such codes?

Strong Encryption Techniques

- Trapdoor Technique:
  - Way to bypass security while software is encrypting the cleartext. Send cleartext to law-enforcement officials when cipher text is sent.
- Key escrow:
  - Require software to register key with a third party, who holds it in confidence. If there is a need to break the code, the third party provides the key.
- These two schemes could be abused

Redundancy Is Very, Very, Very Good

- Precautions against data disasters include backups and system redundancy (having a hot spare up and running)

A Fault Recovery Program for Business

- Keep a full copy of everything written on the system as of some date and time—full backup
- Create partial backups—copies of changes since last full backup
- After disaster, start by installing the last full backup copy
- Re-create state of system by making changes stored in partial backups, in order
- All data since last backup (full or partial) will be lost

Backing Up a Personal Computer

- How and What to Back Up
  - You can buy automatic backup software that writes to writeable CD/DVD or HDD
  - For manual backups, you do not have to backup data that
    - Can be re-created from some permanent source, like software
    - Was saved before but has not changed
    - You don’t care about

Recovering Deleted Information

- Backups also protect from accidental deletions
- Can save evidence of crime or other inappropriate behavior
- Remember that two copies of email are produced when sender hits send—one in sent mail file and one somewhere else, which the sender probably can't delete