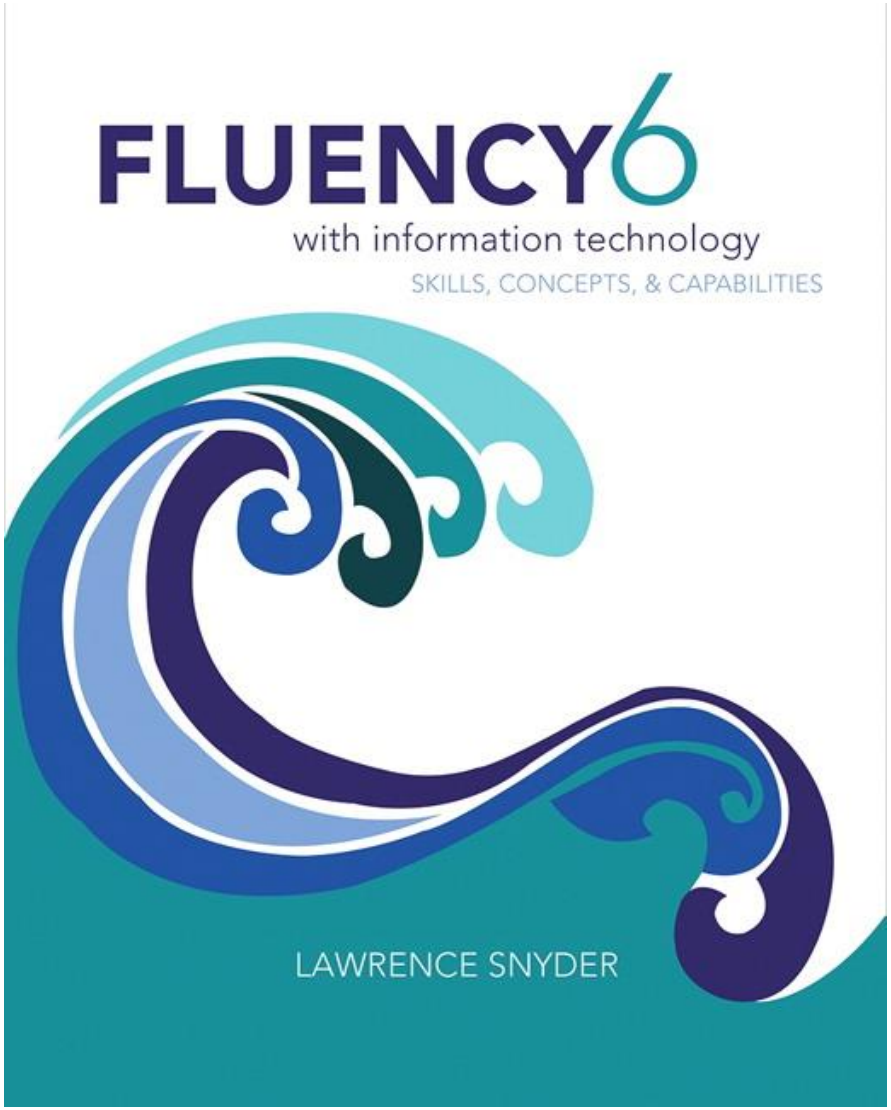

Chapter 12

Privacy and Digital Security

Learning Objectives

- Explain the meaning of privacy; discuss the issues surrounding privacy of information
- List and explain the meaning of the OECD Fair Information Practices
- Discuss the issues concerning U.S. privacy: Opt-in/Opt-out, compliance/enforcement, coverage
- List the ways a computer can be compromised
- Explain the security methods used in public key cryptosystems (PKCs)
- Perform simple encryption from cleartext to cipher text and perform the reverse decryption

Modern Devices and Privacy

- In the past, it was hard for people's privacy to be violated without their knowledge
- With modern technological devices, people's privacy can be violated without their knowing it
- Your image and your information deserves "sufficient safeguards against improper circulation"

Privacy: Whose Information Is It?

- Buying a product at a store generates a transaction, which produces information.
  - Paying with cash generally ensures anonymity
  - Paying by check, credit card, or debit card
  - Purchasing through mail order or on the Internet
  - Providing a “preferred customer” number
  - Buying a product that must be registered for a service agreement or warranty

How Can the Information Be Used?

- Transaction information is a normal part of conducting business (keeping a record until our check clears)
  - The information belongs, then, to the store
- If the store decides, based on your previous purchases, to send you ads for other items, the store is using the information for the standard business practice of generating more business

How Can the Information Be Used?

- If the store sells your name to others has the information been misused?
  - Those other businesses are only trying to generate more business.
  - Is it misused if the information gets to the newspaper and is published?
  - Has the store broken the law?

Controlling the Use of Information

- Who controls the use, if any, of the transaction information?
- There are four main possibilities:
  1. **No Uses.** The information ought to be deleted when the store is finished with it.
  2. **Approval or Opt-in.** The store can use it for other purposes, but only if you approve.
  3. **Objection or Opt-out.** The store can use it for other purposes, but not if you object.
  4. **No Limits.** The information can be used any way the store chooses.

Controlling the Use of Information

- There is also a fifth possibility, *Internal Use:*
  - The store can use the information to conduct business with you (keeping your address, for example), but for no other use
  - It would not include giving or selling your information to another person or business, but it may not require your approval either

Controlling the Use of Information

- If the transaction took place in much of the developed world outside the US, the law and standards would place it between (1) and (2) on the spectrum, but very close to (1).
- If the transaction occurred in the US, the law and standards would place it between (3) and (4) on the spectrum, but very close to (4)

Controlling the Use of Information

- Many Americans assume that there is a privacy law that is close to the fifth case, internal use

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.*
- Privacy is difficult to define
- Generally, privacy concerns four aspects of our lives: our bodies, territory, personal information, and communication

A Privacy Definition

- This definition emphasizes first that it is the person who decides the *circumstances* and the *extent* to which information is revealed, not anyone else
- Second, it emphasizes that the range of features over which the person controls the information embodies every aspect of the person—themselves, their attitudes, and their behaviors

Enjoying the Benefits of Privacy

- Sometimes we want publicity, sometimes we don’t
- Strong privacy laws insure that we control the dissemination of our information

Threats to Privacy

- What are the threats to privacy?
- There are only two basic threats:
  - Government
  - Business
  - (Snooping or gossiping private parties, will be handled by security)

Threats to Privacy

- Historically, the governmental threat of spying on its citizens, worries people the most
- The business threat is a more recent worry
- There are two types of business threats:
  - Surveillance of employees
  - The use of business-related information for other purposes

Voluntary Disclosure

- In principle, a person can enjoy perfect privacy by simply deciding not to reveal anything to anyone
- It may be in our interest to reveal private information, freely in exchange for real benefits

Benefits of Voluntary Disclosure

- Doctors receive our personal information so they can help us stay healthy
- Credit card companies get our personal information to check our credit record in exchange for the convenience of paying with a card
- Employers read our email at work, because we are using the employer's computer for a job

Benefits of Voluntary Disclosure

- The government may have information on us regarding our parents' names and birthplaces, our race and ethnicity, etc. for the purpose of enjoying the rights of citizenship
- How private can we be when we reveal so much about ourselves, our attitudes, and our behavior?

Fair Information Practices

- If people or organizations are free to give or sell the information to anyone else, they are also revealing information about us.
- Our privacy is compromised
- There must be clear guidelines adopted for handling private information:
  - The Fair Information Practices principles.

OECD Fair Information Practices

- In 1980 the Organization for Economic Cooperation and Development (OECD) developed an eight-point list of privacy principles that became known as the Fair Information Practices
- They have become a widely accepted standard

OECD Fair Information Practices

- The public has an interest in these principles becoming law
- The principles also give a standard that businesses and governments can meet as a “due diligence test” for protecting citizens’ rights of privacy, thereby protecting themselves from criticism or legal action

OECD Fair Information Practices

- An important aspect of the OECD principles is the concept that the **data controller** (the person or office setting the policies) must interact with individuals about their information, if any, and must be accountable for those policies and actions!

OECD's Fair Information Practices

- 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

Table 12.1 A brief explanation of the OECD's Fair Information Practices guidelines.

Limited Collection	There should be limits to the personal data collected; data should be collected by fair and lawful means, and with the knowledge and consent of the person whenever possible.
Purpose	The purposes for collecting personal data should be stated when it is collected; the uses should be limited to those purposes.
Quality	The data should be relevant to the purpose of collection; it should be accurate, complete, and up-to-date.
Use Limitation	Personal data should not be disclosed or used for purposes other than stated in the Purpose Principle, except with the consent of the individual or by the authority of law.
Security	Personal data should be protected by reasonable security measures against risks of disclosure, unauthorized access, misuse, modification, destruction, or loss.
Openness	There should be general openness of policies and practices about personal data collection, making it possible to know of its existence, kind, and purpose of use, as well as the contact information for the data controller.
Participation	An individual should be able to (a) determine if the data controller has information about him or her, and (b) discover what it is. If the request is denied, the individual should be allowed to challenge the denial.
Accountability	The data controller should be accountable for complying with these principles.

Privacy Worldwide

- Privacy is not enjoyed at OECD standards in much of the world
- Privacy often comes in conflict with the goals of businesses and governments:
  - Example, the United States has not adopted the OECD principles, possible because many U.S. companies profit by buying and using information in ways that are inconsistent with the OECD principles

Privacy Worldwide

- The European Union (EU) issued a benchmark law incorporating the OECD principles
  - EU Directive requires that data about EU citizens be protected by the standards of the law even when it leaves their country
- Other countries adopted it as well including Australia, Canada, Hong Kong, and New Zealand

US Approach

- US uses a *sectoral* approach
- Rather than a single privacy standard, specific regulations apply to specific sectors
- HIPAA regulates medical information privacy
- Other specific laws for auto registration, video rental, etc.

Business as Usual

- US businesses and government gathers data contrary to the OECD rules
- Patriot Act makes it a crime to say that data gathering is taking place

Business as Usual

- Almost every store and company you do business with has information about you
  - if you want to know what they are doing with that information you must read their privacy policies
  - often it says, “We use the information however we like.”

Opt-in/Opt-out

- An important test of privacy policies the opt-in/opt-out test
- When a data collector wants permission to re-purpose data, how is that attained?
- Opt-in: The subject must give explicit permission
- Opt-out: Permission is assumed unless the subject takes action to object
- Frequently, permission is assumed when the subject continues to use the collector's services

Targeted by Target

- “Big Data” is the statistical analysis of huge information archives
- The retailer Target can track the purchases of a customer who has a loyalty card
- Target can figure out if a woman is pregnant from her buying habits
  - was able to develop a ‘pregnancy prediction’ score by analyzing the customer’s purchases

Government, as Usual

- In June 2013, Edward Snowden revealed that the U.S. government was collecting complete metadata records from telephone carriers
  - it is still unknown if these allegations are true
- The government was also collecting online activity from Facebook, Microsoft, Google, etc.
- Included data to calls to other countries with OECD laws in place

Tracking

- In electronic privacy, tracking is used in two different ways
  - **online tracking**: Web site automatically sending details about your visit to other content providers (to show you ads and other products)
  - **cell phone tracking**: positioning information, used to map your physical location

Online Tracking

- We assume it is used to target advertising and marketing organizations
- But anyone could arrange to follow your "click streams"
- HTTP has a "**Do Not Track**" flag that tells Web servers your tracking preferences
  - it is up to the Web server to honor your request
- Browsers will send the flag, but you must set an option to tell them to do so

Even More Private

- “Do Not Track” is controversial because consumer behavior is very valuable, but people don’t want anyone following them around (even online)
- Two additional protections
  - National Advertising Initiative opt-out program
    - http://www.networkadvertising.org/choices/
  - DoNotTrackMe offers a free blocker
    - https://www.abine.com/index.php

Private Browsing

- “client side” facility
  - only concerns the information stored locally on your machine, not what's stored on servers
- all cookies, cached files, and history are deleted at the end of the session
- useful when using a public computer

Cell Phones

- Phone companies log cell phone calls
  - –Call details: numbers, duration, etc.
  - –Cell towers used, which determines the general location of the phones, even if "location services" (GPS) is off
- These records are kept for various periods by the phone companies

Cell Phones

- National Security Agency collects many of these records
- May keep them indefinitely
- Combine data from all phone providers
- Form a large database which invites misuse
  - No opt-out from official uses
  - Unauthorized private use by officials

	Verizon	T-Mobile	AT&T/Cingular	Sprint	Nextel	Virgin Mobile
Subscriber Information	Post-paid: 3–5 years	5 years	Depends on length of service	Unlimited	Unlimited	Unlimited
Call detail records	1 rolling year	Pre-paid: 2 years Post-paid: 5 years	Pre-paid: varies Post-paid: 5–7 years	18–24 months	18–24 months	2 years
Cell towers used by phone	1 rolling year	Officially 4–6 months, really a year or more.	From July 2008	18–24 months	18–24 months	Not retained—obtain through Sprint
Text message detail	1 rolling year	Pre-paid: 2 years Post-paid: 5 years	Post paid: 5–7 years	18 months (depends on device)	18 months (depends on device)	60–90 days
Text message content	3–5 days	Not retained	Not retained	Not retained	Not retained	90 days (search warrant required with "text of text" request)
Pictures	Only if uploaded to Web site (customer can add or delete pictures any time)	Can be stored online and are retained until deleted or service is canceled	Not retained	Contact provider	Contact provider	Not retained
IP session information	1 rolling year	Not retained	Only retained on non-public IPs for 72 hours. If public IP, not retained.	60 days	60 days	Not retained
IP destination information	90 days	Not retained	Only retained on non-public IPs for 72 hours. If public IP, not retained.	60 days	60 days	Not retained
Bill copies (post-paid only)	3–5 years, but only last 12 months readily available	Not retained	5–7 years	7 years	7 years	n/a
Payment history (post-paid only)	3–5 years, check copies for 6 months	5 years	Depends on length of service	Unlimited	Unlimited	n/a
Store Surveillance Videos	Typically 30 days	2 weeks	Depends. Most stores carry for 1–2 months	Depends	Depends	n/a
Service Applications	Post-paid: 3–5 years	Not retained	Not retained	Depends	Depends	Not retained

Figure 12.2 Retention periods for information held by cellular phone providers.

Cookies

- Cookies are a standard computer science concept originally used by Netscape engineers to connect the identity of a client across a series of independent client/server events

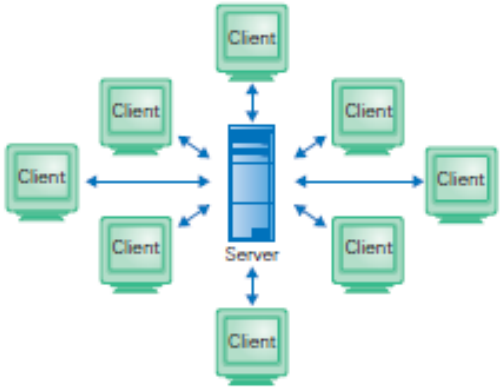

Figure 12.3 Server's view of the client/server relationship.

Cookies

- Imagine this is your bank's server, and you are a client
- The server is helping many clients, and to know who's who, the server stores an identification record called a ***cookie*** on each one

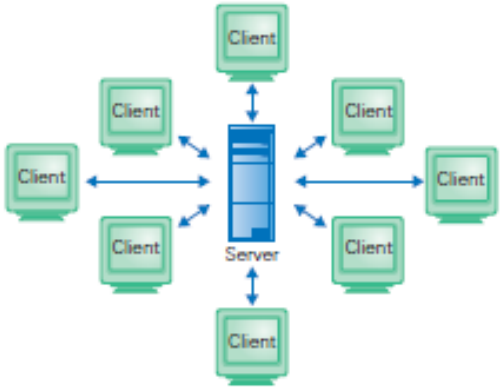

Figure 12.3 Server's view of the client/server relationship.

Cookies

- Cookies are exchanged between the client and the server on each transmission of information, allowing the server to know which of the many clients is sending information

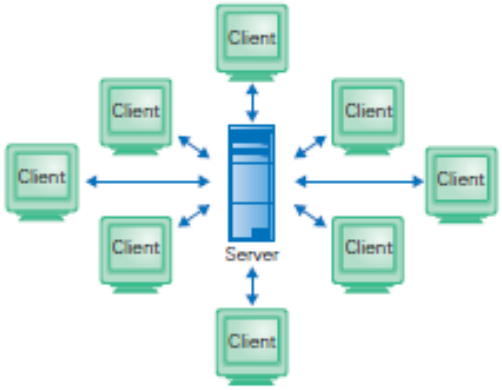

Figure 12.3 Server's view of the client/server relationship.

Cookies

www.nasm.si.edu FALSE / FALSE 2052246450 CFTOKEN 89367880

- Many sites use cookies, even when the interaction is not intended to be as secure as a bank transaction (National Air and Space Museum sent the above)
- The meaning of the fields is unimportant
- The first is the server and the last is the unique information identifying the session

Cookie Abuse

- There is a loophole called a third-party cookie
- A cookie is exchanged between the client and server making the interaction private
- But, if the Web site includes ads on its page, the page may link to the ad company to retrieve the ad
- This new client/server relationship places a cookie on your computer

Cookie Abuse

- All browsers allow users to control how cookies are processed
- You could turn them off, or force the browser to ask you every time whether you will accept a cookie or not
- Turning off cookies prevents you from being able to bank online
- Simply set your browser's cookie policy to your own comfort level

The Right To Be Forgotten

- It can be hard to escape your past on-line
  - An arrest after which you were cleared
  - A minor crime you did commit, but long ago
  - A video of something “silly” you did in college
- Google will find them
- Should sources add some notation?
- Should search engines bury the link?
- A developing issue

Identity Theft

- ***Identity theft*** is the crime of posing as someone else for fraudulent purposes
  - –Using someone else's credit card
  - –Taking a loan in someone else's name
- When a data collector fails to secure the contents of a database, third parties can misuse the data
- Identity theft is a frequent result

Identity Theft

- In 2005, ChoicePoint leaked personal data on 145,000 persons
  - Or just weren't careful whom they sold to
- Initially admitted to only 32,000, later forced to admit the rest
- Over 800 identity thefts were attributed to this failure
- The US government fined ChoicePoint $10M, plus $5M in consumer redress

Digital Security

- Computer security is a topic that is in the news almost daily
- Remember the long list of “dos and don’ts” for online behavior?
  - Do check with the sender before opening an attachment you’re unsure about
  - Don’t fall for phishing emails
  - And the others from Chapter 11

The Risks: What can happen?

- **Mischief**: infecting a computer, causing a nuisance, erasing files, trashing files, etc
- **Information theft**: stealing personal information
- **Spying**: surreptitiously recording videos of the user, logging keystrokes, compromising secure online activities
- **Resource theft**: taking over a computer

Terms and Jargon

- **Malware**: software that harms computers
- **Virus**: shared program the contains code to reproduce itself
- **Worm**: program that is often embedded in an email attachment, reproduces itself and sends a copy to everyone on your contact list
- **Exploit**: when software takes advantage of bugs in commercial software
- **Trojan**: apparently benign, but malicious, program that performs unauthorized activities

What Does Malware Do?

- **Backdoors**: software that creates an access path allowing attackers to run any program on your computer
- **Trojans**: may record every key you type (trying to find passwords), extort money, watch for banking and credit card information
- **Rootkits**: infects your computer and then fights back against security systems

Plan of Action

- Turn off Bluetooth when not in use
- Keep your phone and other computers locked
- Do not automatically click on email attachments
- Never enter sensitive information in a pop-up

Plan of Action

- Thinking of getting something for nothing
  - Think again
- Know where you're going
  - –nice.com
- Be somewhat skeptical
- Use extreme care when visiting notorious sites

If Something Really Bad Happens

- Turn off your computer immediately
- Use a different computer to do a web search about what happened
- Use an external source for the OS to reboot

Plan of Action

- Run “modern” software
- Install updates often
- Install anti-virus software
- Set your Wi-Fi router to security level of at least WPA2
- Password-protect your phones and computers with appropriate passwords (chapter 11)
- Use your knowledge, be wise

Encryption

- Information sent over the Internet is succeptable to interception
- WiFi uses radio signals that can be received by anyone in range
- Wired networks can be snooped by other connected computers
- ***Encryption*** is used to keep your messages hidden from snoops

Encryption

- Your readable message is ***cleartext***
- It is transformed into gibberish known as ***ciphertext***
- Using a magic number called a key
- The two ends of communication agree on a ***key***
- This same key is used to decode the ciphertext at the receiving end
- There are many encryption algorithms

Encryption

- Example encryption algorithm:
  1. The sender breaks the message into groups of letters
  2. “Multiply” each group of letters times the key
  3. Send the “products”/results from the “multiplications” to the receiver
  4. The receiver “divides” the “products” by the key to recreate the groups
  5. Assemble the groups into the message

Encryption

- This works because the math works
- The “reversibility” of encryption makes them 2-way ciphers
  - Only the sender and receiver know the key, making the products useless numbers
- This is a secure communication
- The technique just explained is form of private key encryption, or symmetric-key cryptography

Encryption Example

1. Break into groups, say, ME ET ~~b~~@ ~~b~~9. (The blank is a letter, too; I have coded as ~~b~~.) These letters are, when the ASCII is converted to decimal: 7769 6984 3264 3257.
2. "Multiply" each group by the key, 13:

   7769 x 13 = 100997

   6984 x 13 = 090792

   3264 x 13 = 042432

   3257 x 13 = 042341

   (The "first zeroes" make all number six digits.)
3. Send the "products" 100997 090792 042432 042341 to the receiver.
4. The receiver "divides" by the key, 13:

   100997/13 = 7769

   090792/13 = 6984

   042432/13 = 3264

   042341/13 = 3257

   producing numbers mapped by ASCII: ME ET ~~b~~@ ~~b~~9
5. Reassembling the message, MEET @ 9.

Cryptosystem Schematic Diagram

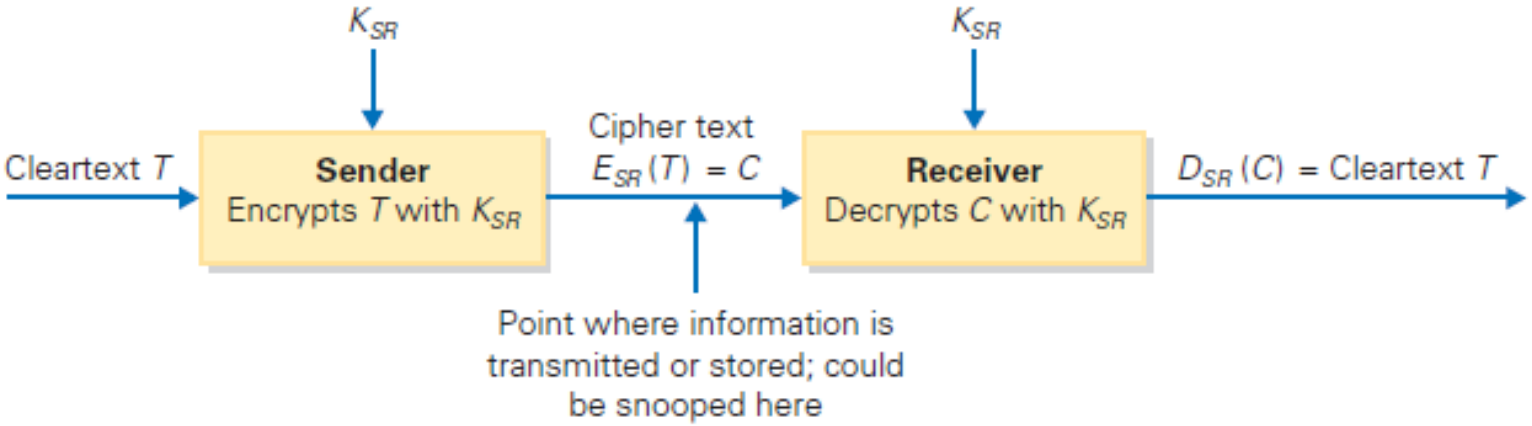

Figure 12.4 Schematic diagram of a cryptosystem. Using a key K_{SR} known only to them, the sender encrypts the cleartext information to produce a cipher text, and the receiver decrypts the cipher text to recover the cleartext. In the middle, where the content is exposed and can be snooped, it is unintelligible.

Private Key Encryption

- Real encryption systems use much longer blocks (hundreds of letters) and larger keys
- Multiplication, division are not the only operations that can be used for encryption
- All that is needed is for an operation to have an inverse (divide is the *inverse* of multiply)

Private Key Encryption

- Private key encryption works very well
- Only one small problem: The sender and receiver must agree on the key, which means they need to communicate somehow
- And communicate without interception
- Usually, they meet face-to-face (they can't email--they don't have a key yet!)

Public Key Encryption

- To avoid that face-to-face meeting, publish the key!
- Requires a key with very special properties:
  - –Encryption and decryption use different keys
  - –The encryption key cannot decrypt
- •Only the encryption key is published

Public Key Encryption Steps

- The receiver computes key *K* based on two large prime numbers
- The receiver publishes *K*, and the sender:
  1. Breaks up the message into blocks as before
  2. Cubes each block, and divides by K, keeping only the remainders
  3. Transmits the remainders

Public Key Encryption Steps

- To decrypt, the receiver:
  4. Raises each remainder to a high power determined by the prime numbers and known only to him
  5. The receiver divides by *K*, too, and saves only the remainders, which are the original blocks.
  6. The receiver assembles the message

How Do We Know It Works?

- *K,* the magic public key, is just two prime numbers, *p* and *q*, multiplied together
- It is possible to figure out those two numbers from the published key in theory.
- This process, called factoring, is tough if the numbers *p* and *q* are large (60 digits apiece)
- It is impractical to factor them no matter how powerful the computer!

Redundancy Is Very, Very, Very Good

- Data can be lost
  - –Disasters: fire, flood, etc.
  - –Theft
  - –Hackers
  - –Disks simply wear out eventually
- It’s nice to have a back-up copy

Backing Up a Personal Computer

- First, you need a place to keep the copy, and you need software to make the copy
- The two easiest “places” to keep the copy are on an external hard disk or “in the cloud”
- The “cloud” company’s computers store the information for you and they take responsibility of keeping it available to you

Backing Up a Business

- Take precautions with your technology!
- Businesses archive files daily and store these backups off-site
- They have a system recovery team to clean up after a disaster strikes
- They also have system redundancy—multiple computers performing the same work, so that when one fails, another is up and running

Fault Recovery Program

- Full backup
  - A complete copy of everything written on the system as of a date and time
- Partial backup
  - Changes since the last full (or partial) backup are saved
  - “Changes” means to keep a copy of any files or folders that have been created or modified since the full backup

Fault Recovery Program

- After a disaster, recover by installing the last full backup copy
- Then make the changes saved in the partial backups in order
- Continue with each partial backup until the most recent
- That’s as close to “full recovery” as possible

Backups

- You don’t have to back up the following:
  - Information that can be recreated from some permanent source
  - Information that was saved but that has not changed
  - Information that you don’t care about

Recovering Deleted Information

- Backups are usually kept a long time
- If you accidentally delete important files, file restoration (that backup copy) is great!
- You can recover your accidentally-deleted file

Recovering Deleted Information

- Backups can also work against you
- Backups can save evidence of crimes or inappropriate behavior
- Email is hard to get rid of: when you click send
  - One copy in the sent folder
  - Another on the server
  - Eventually one in the recipient's mail box

Current Security and Privacy News

- http://www.zdnet.com/pictures/17-ways-the-internet-of-things-can-go-horribly-wrong/15/
- Malvertising Campaign Hits Major Media Sites
- US Justice Dept. Preparing to Indict Iranian Cyber Intruders for 2013 Dam Attack
- Report Says DHS, FBI Paid Ransom to Decrypt Data (March 7, 2016)
  - –According to a report from the Institute for Critical Infrastructure Technology, both the US Department of Homeland Security and the FBI have paid up in ransomware attacks. The paper does not provide specifics about the incidents.
- Seagate Phish Exposes Employee Tax Documents (March 6, 2017)
  - –A Seagate Technology employee was successfully tricked into sending all company W-2 tax documents "to an unauthorized third party."

Summary

- Revealing personal information can be beneficial, so the people and organizations that receive the information must keep it private
  - The guidelines for keeping data private have been created by several organizations, including the Organization for Economic Cooperation and Development (OECD)

Summary

- Guidelines often conflict with the interests of business and government, so some countries like the United States have not adopted them
  - Because the United States takes a sectoral approach to privacy, adopting laws only for specific business sectors or practices, much of the information collected on its citizens is not protected by OECD standards

Summary

- The Do Not Track flag should be set, and DoNotTrackMe should be installed to avoid third parties building a profile of your Web surfing behavior
- The best way to manage privacy in the Information Age is to have OECD-grade privacy laws
- There are two encryption techniques: private key and public key

Summary

- Public key cryptography (PKC) is an amazing idea built on familiar concepts
- Computer scientists have not yet proved the invincibility of the RSA scheme, but it can be “made more secure” simply by increasing the size of the key.

Summary

- Viruses and worms cause damage
  - We can reduce the chance of infection by installing and running anti-virus software
  - We must be aware of hoaxes and phishing scams
- We can implement a plan of action to ensure that our personal computers remain private and secure

Summary

- Backing up computer files is an essential safeguard
  - It ensures that your files will survive for a long time
  - Whether you want them or not