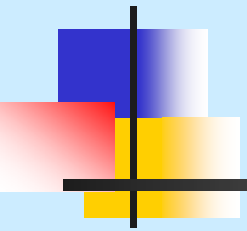
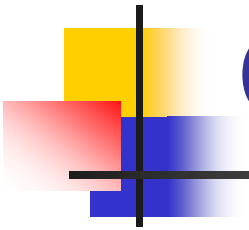


Chapter 1: Information Security Fundamentals



Objectives

- Identify the challenges for information security
- Define information security
- Explain the importance of information security
- List and define information security terminology
- Describe information security careers

Identifying the Challenges for Information Security

- Challenge of keeping networks and computers secure has never been greater
- A number of trends illustrate why security is becoming increasingly difficult
- Many trends have resulted in security attacks growing at an alarming rate

Identifying the Challenges for Information Security (continued)

- Speed of attacks
- Sophistication of attacks
- Faster detection of weaknesses
- Distributed attacks
- Difficulties of patching

- Computer Emergency Response Team (CERT) security organization compiles statistics regarding number of reported attacks

MULTICS : A Security Pioneer

- Multiplexed Information and Computing Services (MULTICS)
- Honeywell Information systems and MIT conducted a cooperative research project during the 1960s and early 1970s to develop MULTICS.
- This time-sharing system incorporated hardware and operating system software “designed with security in mind.”
- Widely touted as the most secure operating system of its time.

Laws of Inevitable Progress

- Moore's Law:

  Processing power doubles every 18 months

- Gates' Law

  Software grows to use all available memory and processing power

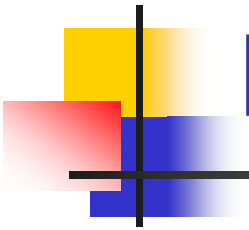
Ex:

- Multics 1969: 56,000 lines of code (PL/I)
- Windows 2000: ~55M lines of code (asm/C/C++)
- 1000x in 30 years (law predicts 1Mx, so Microsoft has work to do!)

Bugs and Vulnerabilities

- Neumann's Law:

  Number of bugs increases as square of code size
- Security vulnerabilities are approximately linear in the number of program bugs
- Windows 2000 has 965,000 times as many bugs as the Multics operating system (1974).



Motivation

- Metcalfe's Law**:**

  Value of a network is square of number of users

- Internet growth:

  1974: ~1000 hosts (10000 users?)

  2000: 200 M users

Information Protection – Why?

- Information are an important strategic and operational asset for any organization
- Damages and misuses of information affect not only a single user or an application; they may have disastrous consequences on the entire organization.
- Additionally, the advent of the Internet as well as networking capabilities has made the access to information much easier.

The Bad News

- Unnamed Law:

  Security risk is the product of the number of vulnerabilities (linear in the number of code bugs) and the value (how many people will be motivated how hard to attack you)
- Security problems are quadrillion worse today than in 1974!
- The number of suspicious probes and scans used to find vulnerable domain name servers on corporate networks shot up 280% in Jan 2001 versus December 2000. (6000 attempts vs 2200 in December). – source *Computerworld* Feb 19, 2001

The Good News

- Some small technical improvements since 1974 – firewalls, intrusion detection, virus scanners (there were no viruses in 1974)
- This means security people are much in demand and extremely well paid.
- The demand for third party security services will exceed 17.2 billion by the end of 2004 according to estimates (Computerworld Feb 26, 2001)

Top Five Jobs for 2005

- Web developer
- Security analyst
- Database Administrator
- Unix Administrator
- E-Commerce Application Development

Identifying the Challenges for Information Security (continued)

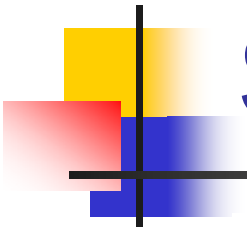
Table 1 Delay between patches and attacks

Attack Name	Impact of Attack	Date Patch First Issued	Date Attack Began	Days between Patch and Attack
Bugbear	Infected more than 2 million computers	5/16/01	9/30/02	502
Yaha	Unleashed 7,000 attacks per day as an e-mail distributed denial-of-service (DDoS) worm	5/16/01	6/22/02	402
Frethem	Spread 12 variants in the first 12 months of activity	5/16/01	06/01/02	381
ELKern	Found in more than 40 countries	5/16/01	4/17/02	336
Klez	Infected 7.2% of computers worldwide	5/16/01	4/17/02	336
Nimda	Spread worldwide in 30 minutes	10/17/00	9/18/01	336
Badtrans	Infected almost half a million computers	5/16/01	11/24/01	192
SQL Slammer	Doubled the number of infections every 8.5 seconds	7/24/02	1/25/03	185
Code Red	Doubled the number of infections every 37 minutes	6/18/01	7/19/01	31
Blaster	Infected more than 1.4 million computers	7/16/03	8/11/03	26

Identifying the Challenges for Information Security (continued)

Table 2 Number of reported incidences

Year	Reported Incidences
1988	6
1990	252
1992	773
1994	2,340
1996	2,573
1998	3,734
2000	21,756
2001	52,658
2002	82,094
2003	137,529



Security

The protection of resources (computer data and programs) from malicious or accidental modification, destruction or disclosure

Security Requirements

The main requirements (aspects) of security are:

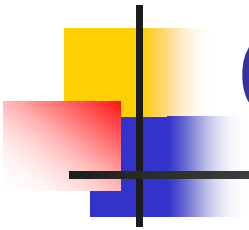
- **Confidentiality: Prevention of unauthorized disclosure of information. Or keeping unwanted parties from accessing assets of a computer system Also known as: secrecy or privacy**
- **Integrity: Prevention of unauthorized modification of information.**
- **Availability: Prevention of unauthorized withholding of information or resources. Or keeping system available**

Information Security : Example

- Consider a payroll database in a corporation, it must be ensured that:
  - Salaries of employees are not disclosed to arbitrary users of the database.
  - Salaries are modified by only those individuals that are properly authorized.
  - Paychecks are printed on time at the end of each pay period.

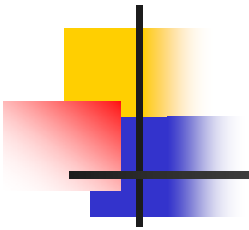
Information Security : Example

- In a military environment , it is important that:
  - The target of a missile is not given to an unauthorized user.
  - The target is not arbitrarily modified
  - The missile is launched when it is fired.



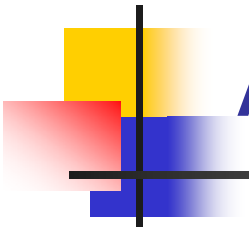
Confidentiality

- Is the concealment of information.
- The need for keeping information secret arises from the use of computers in sensitive fields such as government and industry.
- Access control mechanisms support confidentiality.
- One access control mechanism for preserving confidentiality is cryptography.
- Confidentiality also applies to the existence of data, which is sometimes more revealing than the data itself.
- Resource hiding is another important aspect of confidentiality.



Integrity

- Refers to the trustworthiness of data or resources, and is usually phrased in terms of preventing improper or unauthorized change.
- Integrity includes data integrity (the content of the information) and origin integrity (the source of the data ,often called *Authentication*)
- The aspect of integrity known as credibility is central to the proper functioning of a system.
- Integrity mechanisms fall into two categories: *Prevention* mechanisms and *Detection* mechanisms.
- Integrity includes both the correctness and the trustworthiness of the data.
- Evaluating integrity is often very difficult.



Availability

- Refers to the ability to use the information or resources desired.
- It is an important aspect of reliability.
- System design usually assumes a statistical model to analyze expected patterns of use, and mechanisms ensure availability when the statistical model holds.
- Someone may be able to manipulate use (or parameters that control use, such as network traffic) so that the assumptions of the statistical model are no longer valid. As a result the mechanisms for keeping the resources or data available will often fail.
- Attempts to block availability, called ***Denial of service access***, can be the most difficult to detect.

Compute Availability

- Availability is often expressed in terms of uptime.
- To compute the downtime for the following uptimes:

  (over the course of 1 year)

Uptime %	Downtime mins.
99	5,256
99.9	525
99.99	52.56
99.999	5.25
99.9999	0.5

Other Aspects of Security

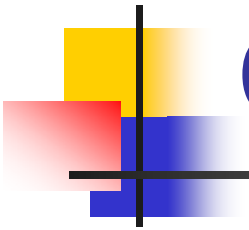
- Non-repudiation

  Ensuring that communication parties can't later deny that the exchange took place (or when the exchange took place).

- Legitimate use

  Ensuring that resources are not used by unauthorized parties or in unauthorized ways.

- Good Performance



Goals of Security

- Prevention: take measures that prevent your assets from being damaged.
- Detection : take measures that allow you to detect when an asset has been damaged, how it has been damaged, and who has caused the damage.
- Recovery/ Response/ Reaction: take measures that allow you to recover your assets or to recover from a damage to your assets. Or continue to function correctly even if attack succeeds.

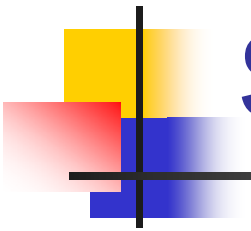
Illustration : Protection of home

- Prevention : locks at the door and bars on the windows.
- Detection : You will detect when something has been stolen if it is no longer there. A burglar alarm may be tripped when a break-in occurs.
- Reaction : you can call the police; you may decide to replace the stolen item, or the police may recover it for you.

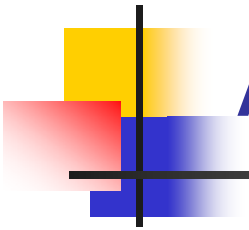
Illustration : Credit card use on the Internet

- Prevention : use encryption when placing an order; rely on merchant to perform some checks before accepting credit card order; don’t use your credit card on the Net.
- Detection :a transaction that you had not authorized appears on your credit card statement .
- Reaction : you can ask for a new credit card number; the cost of the fraudulent transaction may be recovered by the card holder, the merchant , or the card issuer.

Information Security – How? Some Mechanisms



- User authentication – to verify the identity of users wishing to access the information.
- Information authentication – to ensure information authenticity – it is supported by *signature* mechanisms.
- Encryption – to protect information when being transmitted across systems and when being stored on secondary storage.
- Intrusion detection – to prevent against impersonation of legitimate users and also against insider threats.



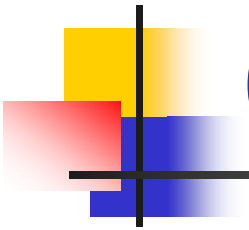
ASSETS

- Hardware
- Software
- Information (data and docs)
- People and supplies

Defining Information Security

- Information security:
  - Tasks of guarding digital information, which is typically processed by a computer (such as a personal computer), stored on a magnetic or optical storage device (such as a hard drive or DVD), and transmitted over a network .

Defining Information Security (continued)



- Ensures that protective measures are properly implemented
- Is intended to protect information
- Involves more than protecting the information itself

Defining Information Security (continued)

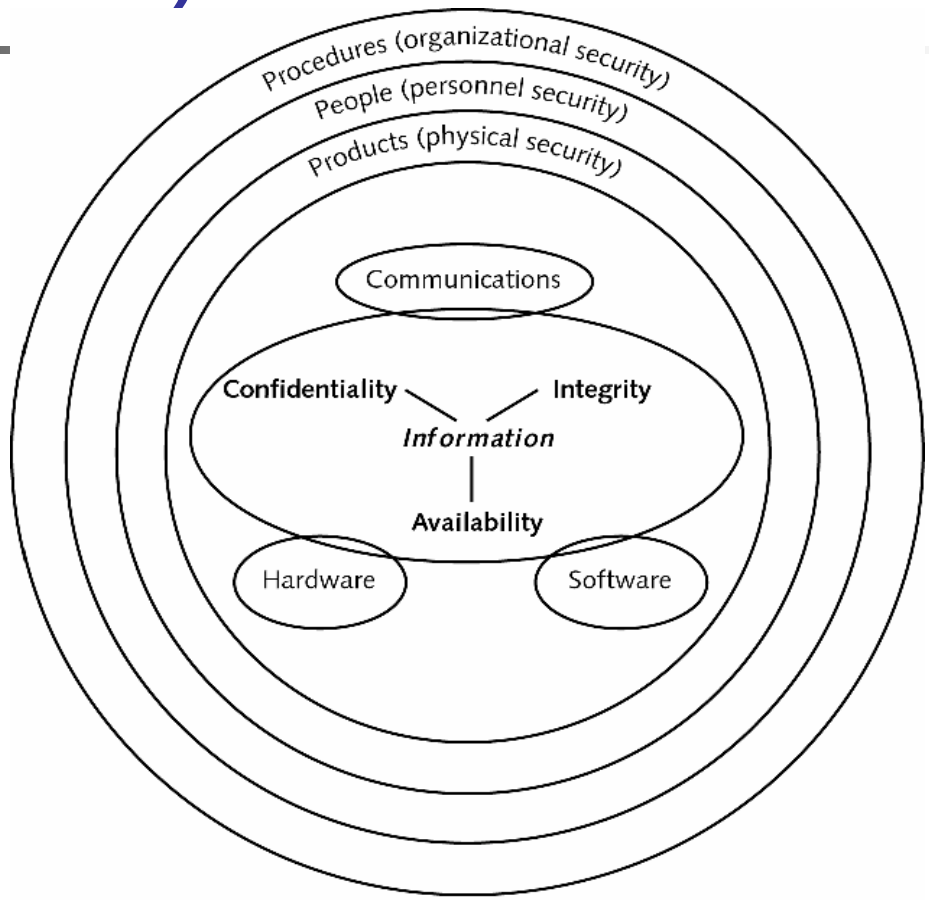


Figure 3 Information security components

Information Security is achieved through a combination of :

- Physical Security - Products (innermost layer)

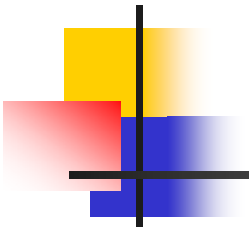
  Could be as simple as door locks, or as complicated as IDSs and Firewalls
- Personnel Security - People

  (the next layer)

  Without people implementing and properly using the security products, the data can never be protected.
- Organizational Security - Procedures

  (the final layer)

  Which include the plans and policies established by an organization to ensure that people correctly use the products to protect the information



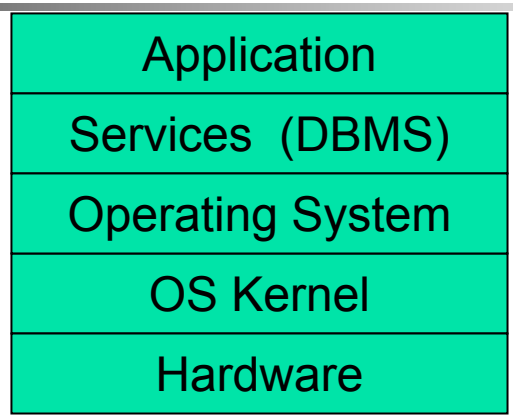
- Thus :

  Information Security protects the integrity, confidentiality, and availability of information on the devices that store, manipulate, and transmit the information through products, people, and procedures.

Defining Information Security (cont.)

- Three characteristics of information must be protected by information security:
  - Confidentiality
  - Integrity
  - Availability
- Center of diagram shows what needs to be protected (information)
- Information security achieved through a combination of three entities

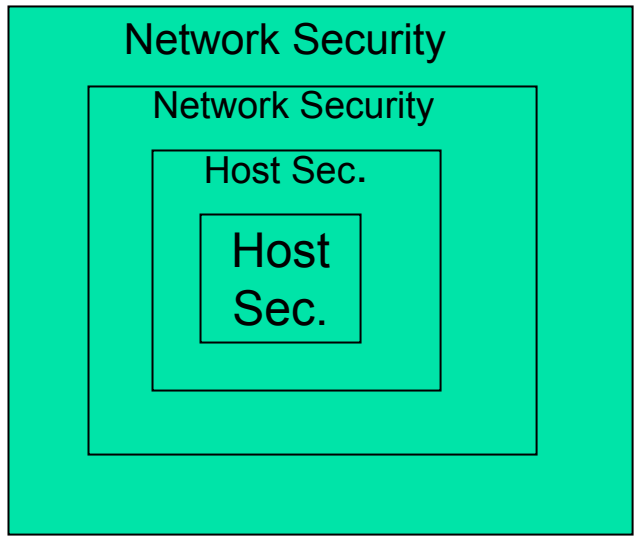
Layers Of an IT System



- Security controls can be placed in any of these layers. It is the task of the designer to find the right layer for each mechanism, and to find the right mechanism for each layer.

Layers Of Networked IT System

- Firewalls (Pr)
- IDSs (Det)
- Access Control
- Audit Logs



The Man-Machine Model of Protection mechanisms

Specific
Complex
Focus on Users

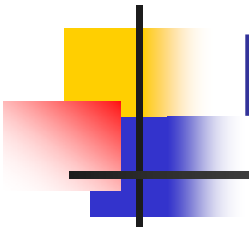
Generic
Simple
Focus on Data

ManOriented

MachineOriented

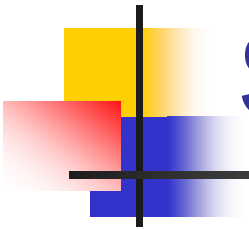
Information Security: A Complete Solution

- It consists of:
  - First defining a security policy
  - Then choosing some mechanism to enforce the policy
  - Finally providing assurance that both the mechanism and the policy are sound.



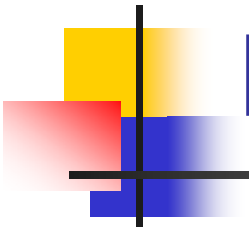
Policies and Mechanisms

- Policy says what is , and is not, allowed
- Mechanisms enforce policies



Security Assurance

- Specification
  - Requirements analysis
  - Statement of desired functionality
- Design
  - How system will meet specification
- Implementation
  - Programs/systems that carry out design



Management and Legal Issues

- Cost-Benefit Analysis
  - Is it more cost-effective to prevent or recover?
- Risk Analysis
  - Should we protect some information?
  - How much should we protect this information?
- Laws and Customs
  - Are desired security measures illegal?
  - Will people adopt them?

Understanding the Importance of Information Security

- Information security is important to businesses:
  - Prevents data theft
  - Avoids legal consequences of not securing information
  - Maintains productivity
  - Foils cyberterrorism
  - Thwarts identity theft

Preventing Data Theft

- Security often associated with theft prevention
- Drivers install security systems on their cars to prevent the cars from being stolen
- Same is true with information security—businesses cite preventing data theft as primary goal of information security

Preventing Data Theft (continued)

- Theft of data is the single largest cause of financial loss due to a security breach
- One of the most important objectives of information security is to protect important business and personal data from theft

Avoiding Legal Consequences

- Businesses that fail to protect data may face serious penalties
- Laws include:
  - The Health Insurance Portability and Accountability Act of 1996 (HIPAA)..Non-disclosure of health information
  - The Sarbanes-Oxley Act of 2002 (Sarbox) Stringent reporting requirements and internal controls on electronic financial reporting systems
  - The Cramm-Leach-Blilely Act (GLBA) Requires banks to alert customers of their policies in disclosing customer information.
  - USA PATRIOT Act 2001 is designed to broaden the surveillance of law enforcement agencies so that they can detect and suppress terrorism

Maintaining Productivity

- After an attack on information security, clean-up efforts divert resources, such as time and money away from normal activities
- A Corporate IT Forum survey of major corporations showed:
  - Each attack costs a company an average of $213,000 in lost man-hours and related costs
  - One-third of corporations reported an average of more than 3,000 man-hours lost

Maintaining Productivity (cont)

Table 1 Cost of attacks

Number of Total Employees	Average Hourly Salary	Number of Employees to Combat Attack	Hours Required to Stop Attack and Clean Up	Total Lost Salaries	Total Lost Hours of Productivity
100	$25	1	48	$4,066	81
250	$25	3	72	$17,050	300
500	$30	5	80	$28,333	483
1000	$30	10	96	$220,000	1,293

Foiling Cyberterrorism

- An area of growing concern among defense experts are surprise attacks by terrorist groups using computer technology and the Internet (cyberterrorism)
- These attacks could cripple a nation's electronic and commercial infrastructure
- Our challenge in combating cyberterrorism is that many prime targets are not owned and managed by the federal government

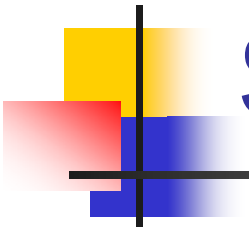
Thwarting Identity Theft

- Identity theft involves using someone's personal information, such as social security numbers, to establish bank or credit card accounts that are then left unpaid, leaving the victim with the debts and ruining their credit rating
- National, state, and local legislation continues to be enacted to deal with this growing problem
  - The Fair and Accurate Credit Transactions Act of 2003 is a federal law that addresses identity theft

Understanding Information Security Terminology

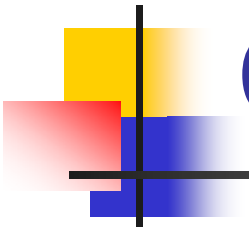
Table 2 Information security terminology

Term	Example in Amanda's Scenario	Example in Information Security
Asset	Car stereo	Employee database
Threat	Steal stereo from car	Steal data
Threat agent	Thief	Attacker, virus, tornado
Vulnerability	Hole in fence	Software defect
Exploit	Climb through hole	Send virus to unprotected e-mail server
Risk	Transfer to insurance company	Educate users



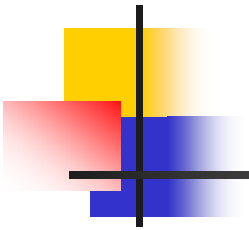
Security Threats

- Vulnerability: weakness in security system that could be exploited for loss or harm (e.g. bugs)
- Exposure: potential loss or harm
- Attack: exploitation of vulnerability
- A threat is a potential violation of security.
- The three security services-confidentiality, integrity, and availability- counter threats in the security of a system.



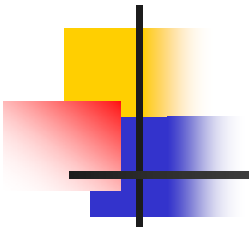
Classes of Threats

- Disclosure or unauthorized access to information- Snooping, Trojan horse
- Deception or the acceptance of false data – Modification, spoofing, repudiation of origin, denial of receipt
- Disruption or the interruption or prevention of correct operation - Modification
- Usurpation or unauthorized control of some part of a system – Modification, spoofing, delay, denial of service



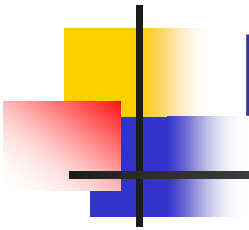
Interruption

- Data is
  - Lost
    - Unusable
    - Unavailable
- Denial of Service, DOS
- Ways this can happen:
  - Malicious destruction
  - Accident (erasure or natural disaster)
  - Malfunction



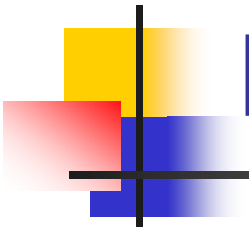
Interception

- Some unauthorized party has gained access to an asset.
- Illicit copying of programs or data files.
- Wiretapping/Eavesdropping
- Snooping is a form of disclosure
- It is passive.



Modification

- Covers three classes of threats.
- Unlike snooping, it is active
- Changing values in a database
- Replacement of a program
- Virus/Trojan horse
- Changing web-pages

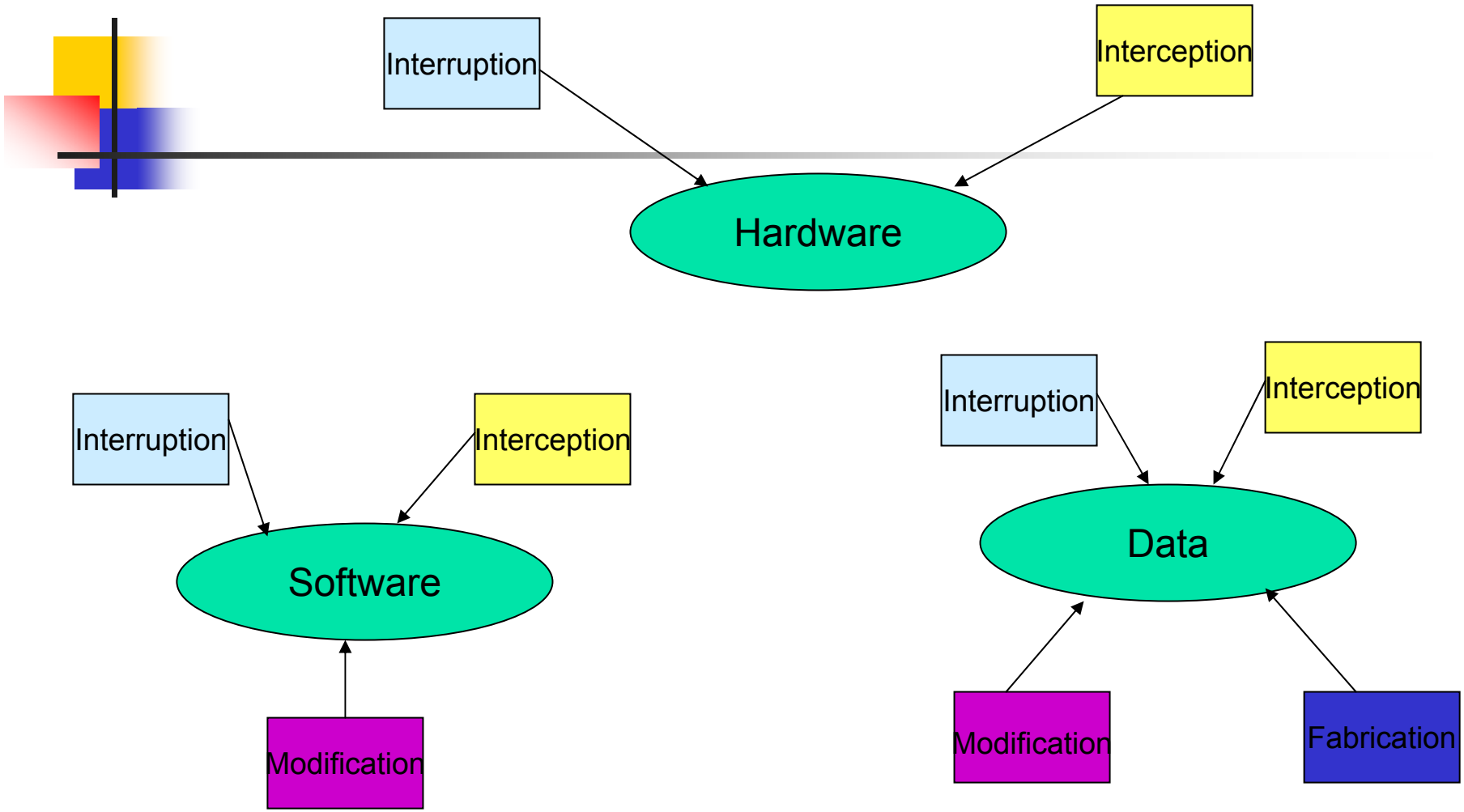


Fabrication

- By authorized or unauthorized parties.
- *Masquerading or spoofing*, an impersonation of one entity by another, is a form of both deception and usurpation.
- Examples:
  - Impersonation
  - Bogus sources or spam

Classes of Vulnerabilities

- Hardware Threats
- Software Threats
  - Software Deletion
  - Software Theft
- Data threats
  - Data Confidentiality
  - Data Integrity


Interruption
Interception
Hardware
Interruption
Interception
Software
Modification
Interruption
Interception
Data
Modification
Fabrication

Cost of Losses

- Priceless – trade secrets
- Dollar value of assets
- Plus cost to replace/fix, time
- Loss of “face” or confidence
- Liability

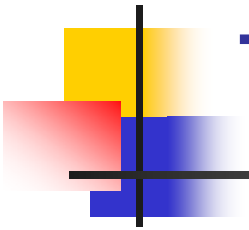
- $377.8 million cybercrime according to San Francisco based Computer Security Institute (CSI) and a team at FBI’s San Francisco office
  - Information theft: $153.2M
  - Fraud: 91.2 M
  - Viruses: 45.3 M
  - Insider Internet Abuse: 35M

Why Aren't All Computer Systems Secure?

- Partly due to hard technical problems.
- But also due to cost/benefit issues
- Security costs
- Security usually only pays off when there's trouble
- Ignorance also plays a role (unsophisticated users on the Internet)

The Principle of Adequate Protection

- Computer items must be protected only until they lose their value. They must be protected to a degree consistent with their value.
- So worthless things need little protection
- And things with timely value need only be protected for a while.



Tomorrow?

- Will security become more important?
- Yes !
- Why?
  - More money on the network
  - More sophisticated criminals
  - More leverage from computer attacks
  - More complex systems

Surveying Information Security Careers

- Information security is one of the fastest growing career fields
- As information attacks increase, companies are becoming more aware of their vulnerabilities and are looking for ways to reduce their risks and liabilities

Surveying Information Security Careers (cont.)

- Sometimes divided into three general roles:
  - Security manager develops corporate security plans and policies, provides education and awareness, and communicates with executive management about security issues
  - Security engineer designs, builds, and tests security solutions to meet policies and address business needs
  - Security administrator configures and maintains security solutions to ensure proper service levels and availability