Study Guide for CSC555-ITC459-CSC459-Midterm

1. The midterm covers the following topics:

   Introduction to Information Security

   Information Security Goal

   Information Security Assurance

   Security Engineering

   The systems security engineering capability maturity model

   Access Control Goal

   Authentication

   Network Attacks and Defense

   Biometrics Systems

   Cryptography

2. The format for the midterm: Multiple choice, True/False.
3. Review the PPP.
4. Review Sample Test.

Concentrate on the goal of security engineering, password authentications, social engineering, phishing, system security issues, biometrics systems, system engineering, protocol related to the security, authentication methods, access control models, different type of algorithms in cryptography.

Sample Test for CSC459

Question 1. What are the 3 views of Security?

A) Defense, Offense, and Detection
B) Control, Deterrence, and Integrity
C) Defense, Deterrence, and Detection
D) Defense, Auditing, and Authorization
E) Confidentiality, Integrity, Availability

Correct Answer is: c.

Question 1. The process of mutual authentication involves _____.

A) A user authenticating to a system and the system authenticating to the user
B) A user authenticating to two systems at the same time
C) A user authenticating to a server and then to a process
D) A user authenticating, receiving a ticket, and then authenticating to a service

Correct Answer is: a.

Question 2. Spoofing can be described as which of the following?

A)Eavesdropping on a communication link
B)Working through a list of words
C)Session hijacking
D)Pretending to be someone or something else

Correct Answer is: d.

Question 3. If a company has a high turnover rate, which access control structure is best

A)Role based
B)Decentralized
C)Rule based
D) Discretionary

Correct Answer is: a

Question 4. Which best describes authentication

A)Registering a user
B)Identifying a user
C)Validating a user
D)Authorizing a user

Correct Answer is: c

Question 5. Which is the most important item when it comes to ensuring that security is successful in an organization

a)Senior management support
b)Biometric based smartcards for building access
c)Internal web access to policies and procedures
d)Centralized management of anti-virus on all desktop machines

Correct Answer is: a

Question 6. Which of the following best describes a value-"role based access control" offers companies in reducing administrative burdens

a)It allows users to change access rights whenever they want.
b)It ensures secure communication between computers.
c)User membership in roles can be easily revoked and new ones established as job assignments dictate.
d)enforces an enterprise-wide security policy, standards, and guidelines.

Correct Answer is: c

Question 7. An access control model should be applied in a _____ manner

a)Detective
b)Recovery
c)Corrective
d)Preventive

Correct Answer is: d

Question 8. A password is mainly used for what function?

a)Identity
b)Registration
c)Authentication
d)Authorization

Correct Answer is: c.

Question 9. What is the primary purpose of using one-way hashing on user passwords?

a)Minimizes the amount of primary and secondary storage needed to store passwords
b)Prevents anyone from reading passwords in plaintext
c)Avoids excessive processing required by an asymmetric algorithm
d)Prevents replay attacks

Correct Answer is: b.

Question 10. Which three security protocols operate at layer 4 and which transport layer protocols they can be used with?

a)TLS/SSL with UDP, DTLS with TCP, SSH with UDP
b)IPsec with TCP, PGP with UDP, SET with TCP
c)TLS/SSL with TCP, DTLS with UDP, SSH with TCP
d)SET with TCP, PGP with UDP, SSL with TCP

Correct Answer is: c.

Question 11.

When should security first be addressed in a project?

A)During requirements development.
b)During integration testing.
c)During design specifications.
d)During implementation.

Correct Answer: A

Question 12. The first phase of risk management is ____.

a. risk identification
b. design
c. risk control
d. risk evaluation

Question 13. Bit stream methods commonly use algorithm functions like the exclusive OR operation (____).

a. XOR
b. EOR
c. NOR
d. OR

Question 14 ____ functions are mathematical algorithms that generate a message summary or digest to confirm the identity of a specific message and to confirm that there have not been any changes to the content.

a. Hash
b. Map
c. Key
d. Encryption

Question 15. ____ is an integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services that enables users to communicate securely.

a. MAC
b. PKI
c. DES
d. AES

12. ANS: A
13. ANS: A
14. ANS: A
15. ANS: B

Developed and Presented By Dr. Mehrdad S Sharbaf
CSUDH
Computer Science Department

http://csc.csudh.edu/

The some of the materials are excerpted from Ian Sommerville's Book, and Ross Anderson's Book

INFORMATION SECURITY GOAL

INTRODUCTION TO INFORMATION SECURITY

- What is Information Security?
- Information Security: To make sure that the information risks and controls are in balance
- Information security initiated with Rand Report R-609 (research paper that started the study of computer security)
- Scope of computer security grew from physical security to include:
  - Safety of data
  - Limiting unauthorized access to data
  - Involvement of personnel from multiple levels of an organization

INTRODUCTION TO INFORMATION SECURITY

- The protection of information and its critical elements, including systems, software, and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, education, technology
- C.I.A. triangle was standard based on confidentiality, integrity, and availability
- C.I.A. triangle now expanded into list of critical characteristics of information

SECURITY GOALS

- Confidentiality
  - Confidentiality means that people cannot read sensitive information, either while it is on a computer or while it is traveling across a network.

SECURITY GOALS

- Integrity
  - Integrity means that attackers cannot change or destroy information, either while it is on a computer or while it is traveling across a network. Or, at least, if information is changed or destroyed, then the receiver can detect the change or restore destroyed data.

SECURITY GOALS

- Availability
  - Availability means that people who are authorized to use information are not prevented from doing so

COMPONENTS OF INFORMATION SECURITY

- Computer Security(Hardware & Software)
- Data Security
- Network Security
- Physical Security
- Information Security Management
- Policy

NSTISSC

- The National Security Telecommunications and Information Systems Security Committee (NSTISSC) was established under National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems", dated 5 July 1990.
- On October 16, 2001, President George W. Bush signed Executive Order 13231, the Critical Infrastructure Protection in the Information Age, re-designating the **National Security Telecommunications and Information Systems Security Committee** (NSTISSC) as the **Committee on National Security Systems** (CNSS).
- The **CNSS** holds discussions of policy issues, sets national policy, directions, operational procedures, and guidance for the information systems operated by the U.S. Government, its contractors or agents that either contain classified information, involve intelligence activities, involve cryptographic activities related to national security, involve command and control of military forces, involve equipment that is an integral part of a weapon or weapons system(s), or are critical to the direct fulfillment of military or intelligence missions.

NSTISSC SECURITY MODEL

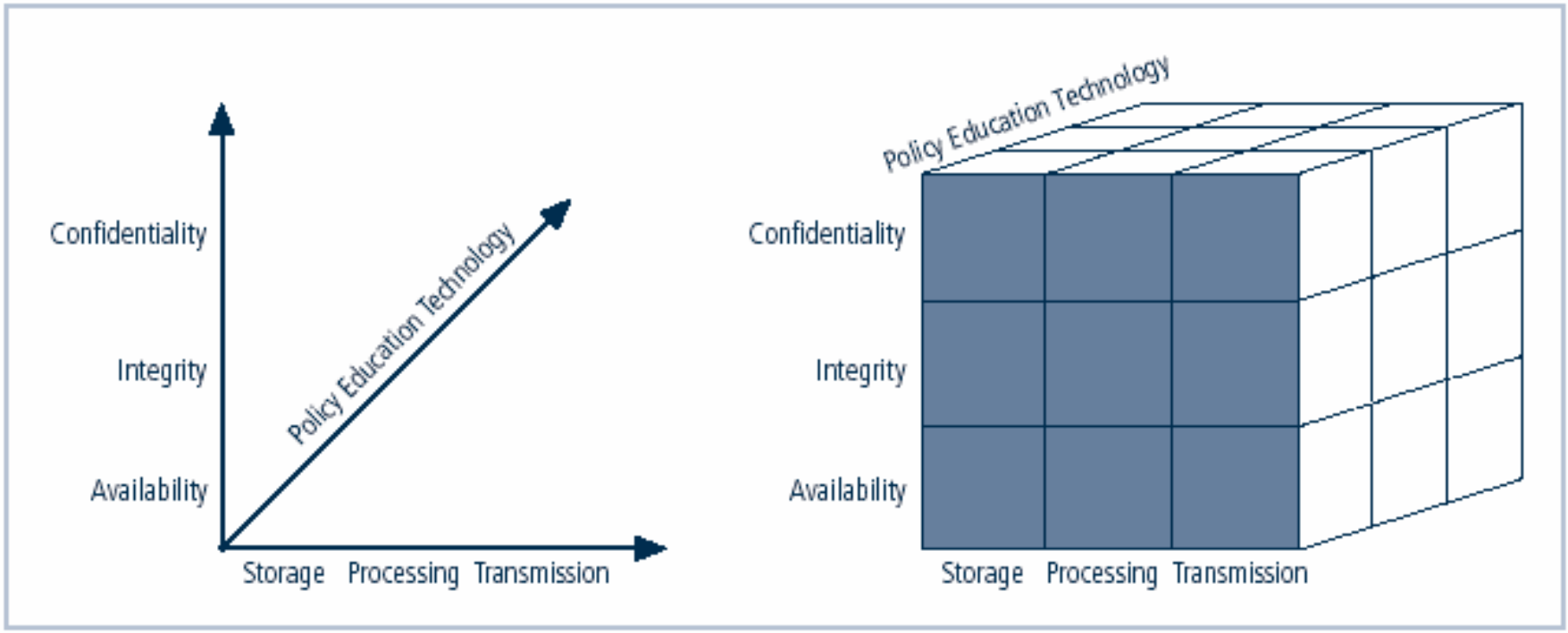


FIGURE 1-4 NSTISSC Security Model

THE THREAT ENVIRONMENT/COMPROMISES

- **The Threat Environment**
  - The threat environment consists of the types of attackers and attacks that companies face
- **Compromises**
  - Successful attacks
  - Also called incidents
  - Also called breaches

THE THREAT ENVIRONMENT/COMPROMISES

- **Employee Sabotage**
  - Destruction of hardware, software, or data
  - Plant time bomb or logic bomb on computer
- **Employee Hacking**
  - Hacking is intentionally accessing a computer resource without authorization or in excess of authorization
  - Authorization is the key

THE THREAT ENVIRONMENT/COMPROMISES

- **Malware**
  - A generic name for any “evil software”
- **Viruses**
  - Programs that attach themselves to legitimate programs on the victim’s machine
  - Spread today primarily by e-mail
  - Also by instant messaging, file transfers, etc.

THE THREAT ENVIRONMENT/COMPROMISES

- **Worms**
  - Full programs that do not attach themselves to other programs
  - Like viruses, can spread by e-mail, instant messaging, and file transfers

THE THREAT ENVIRONMENT/COMPROMISES

- **Trojan Horses**
  - A program that replaces an existing system file, taking its name
- **Trojan Horses**
  - Remote Access Trojans (RATs)
    - Remotely control the victim’s PC
  - Downloaders
    - Small Trojan horses that download larger Trojan horses after the downloader is installed

THE THREAT ENVIRONMENT/COMPROMISES

- **Trojan Horses**
  - **Spyware**
    - Programs that gather information about you and make it available to the adversary
    - Cookies that store too much sensitive personal information
    - Keystroke loggers
    - Password-stealing spyware
    - Data mining spyware

THE THREAT ENVIRONMENT/COMPROMISES

- **Trojan Horses**
  - **Rootkits**
    - Take control of the super user account (root, administrator, etc.)
    - Can hide themselves from file system detection
    - Can hide malware from detection
    - Extremely difficult to detect (ordinary antivirus programs find few rootkits)

THE THREAT ENVIRONMENT/COMPROMISES

- **Mobile Code**
  - Executable code on a webpage
  - Code is executed automatically when the webpage is downloaded
  - Javascript, Microsoft Active-X controls, etc.
  - Can do damage if computer has vulnerability

THE THREAT ENVIRONMENT/COMPROMISES

- **Social Engineering in Malware**
  - Social engineering is attempting to trick users into doing something that goes against security policies
  - Several types of malware use social engineering
    - Spam
    - Phishing
    - Hoaxes

THE THREAT ENVIRONMENT/COMPROMISES

- **Professional Hackers**
  - Motivated by thrill, validation of skills, sense of power
  - Motivated to increase reputation among other hackers
  - Often do damage as a byproduct
  - Often engage in petty crime

COUNTERMEASURES

- **Countermeasures**
  - Tools used to thwart attacks
  - Also called safeguards, protections, and controls
  - Types of countermeasures
    - Preventative
    - Detective
    - Policy toward Correction

SECURITY TOOLS

- Most of security tools are listed in my blog
- http://msharbaf.wordpress.com
- Wireshark (known as Ethereal until a trademark dispute in Summer 2006) is a fantastic open source multi-platform network protocol analyzer. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, delving down into just the level of packet detail you need.
- http://www.wireshark.org/

SECURITY TOOLS

- Nmap (“Network Mapper”) is a free and open source (license) utility for network exploration or security auditing.
- http://www.nmap.org
- Snort® is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide.
- http://www.snort.org

SECURITY TOOLS

- Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and (with appropriate hardware) can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic.
- http://www.kismetwireless.net
- Vistumbler (also known as Network Stumbler) is a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a, 802.11g, 802.11n,and 802.11ac WLAN standards.
- Vistumbler - Open Source WiFi scanner and channel scanner for windows

SECURITY POLICY

- One of the most important assets any organization possesses is its data
- Security policy is a very important component of information security
- Security policy
  - Series of documents that clearly defines the defense mechanisms an organization will employ
    - To keep information secure
  - Outlines how the organization will respond to attacks
    - Duties and responsibilities of its employees

SECURITY POLICY

- Proper development of a security policy
  - Accomplished through the security policy cycle
    - Never-ending process of identifying what needs to be protected, determining how to protect it, and evaluating the adequacy of the protection
    - Risk Identification
    - Security Policy development
    - Compliance monitoring and evaluation

Risk Identification

- Seeks to determine the risks that an organization faces against its information assets
  - Information then becomes the basis of developing the security policy itself
- Steps
  - Asset identification
  - Threat identification
  - Vulnerability appraisal
  - Risk assessment

Security Policy Development

- Policy creation
  - Consider a standard set of principles
- Policy must be implementable and enforceable
- Policy must be concise and easy to understand
- Policy must be balance protection with productivity

Compliance monitoring and evaluation

- Necessary to ensure that polices are consistently implemented and followed properly
- Involves the proactive validation that internal controls are in place and functioning as expected

COMPLIANCE MONITORING AND EVALUATION

- Change management
  - Manages the process of implementing changes
- Some of the most valuable analysis occurs when an attack penetrates the security defenses
- Incident response
  - Outlines the actions to be performed when a security breach occurs
  - Most incident responses include the composition of an incident response team (IRT)

COMPLIANCE MONITORING AND EVALUATION

- Code of ethics
  - Encourages members of professional groups to adhere to strict ethical behavior within their profession
  - Codes of ethics for IT professionals
    - Institute of Electrical and Electronics Engineers (IEEE)
    - Association for Computing Machinery (ACM)

NIST-COMPUTER SECURITY RESOURCE CENTER

- **Special Publications (800 Series)**
- Special Publications in the 800 series present documents of general interest to the computer security community. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications. This Special Publication 800 series reports on ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.
- http://csrc.nist.gov/publications/PubsSPs.html

ISO 27000 SERIES

- The ISO 27000 series standard was published in 2005, 2006, and 2009. The standard "established guidelines and general principles for initiating, implementing, maintaining, information security risk management, guidance on the development and use of measures and measurement for the assessment of the effectiveness of an implemented information security management system and controls, and improving information security management within an organization
- http://www.27000.org/

THE NEW PERSPECTIVE IN CYBER SECURITY

- Total Quality Information Security Management(TQISM Model) introduced by **Dr. Mehrdad S Sharbaf**

Developed and Presented By Dr. Mehrdad S Sharbaf
CSUDH
Computer Science Department

http://csc.csudh.edu/

The some of the materials are excerpted from Ian Sommerville's Book, and Ross Anderson's Book

SECURITY ENGINEERING

SECURITY ENGINEERING

- Tools, techniques and methods to support the development and maintenance of systems that can resist malicious attacks that are intended to damage a computer-based system or its data.

SECURITY ENGINEERING

- “Security engineering is about building systems to remain dependable in the face of malice, error, or mischance.” Ross Anderson
- Requires cross-disciplinary expertise: cryptography, computer and network security, computer and network systems and protocols, hardware (computer and network), formal methods, applied psychology, organizational methods and psychology, auditing, forensics and the law.
- Requirements not only based on confidentiality and privacy but also include critical infrastructure assurance:safety for human life and the environment, economic structures, and crime prevention and prosecution.

SECURITY ENGINEERING

- The focus of the Security Engineering discipline is:
  - tools,
  - processes, and
  - methods
- needed to
  - design,
  - implement, and
  - test
- complete systems, and to adapt existing systems as their environment evolves.

SECURITY ENGINEERING

- In my humble opinion, Security Engineering is the hardest discipline

There is requiring a cross-disciplinary knowledge of the following disciplines (at least):

- cryptography and computer security,
- hardware tamper-resistance,
- formal methods,
- psychology, legal issues and forensics,
- financial accounting and audit methods,
- software engineering (including evaluation and testing),
- system engineering and business process analysis,
- military science, and
- information theory.

And this is not a complete list!

SECURITY ENGINEERING

- A huge amount of security systems have critical assurance requirements where failure may
  - endanger human life or cause environmental damage (e.g.nuclear power plant),
  - damage the economic infrastructure (e.g.ATM machines),
  - risk personal privacy (e.g.medical record systems),
  - endanger entire business sectors (e.g.pay TV),
  - facilitate crime (e.g.burglar alarms), and
  - cause negative psychological effects (e.g. perceptions that a system is more vulnerable than it really is)

SECURITY ENGINEERING

- Things are complicated by the flawed conventional view of things:
  - "Software engineering is about ensuring that certain things happen."
    - e.g. "Alice can read this file."
  - "Information Security is about ensuring that certain things do not happen."
    - e.g. "Al Qaida cannot read this file."
- The reality is much more complicated because security requirements vary greatly from one system to another.

SECURITY ENGINEERING

- Real systems typically require tailored combinations of
  - user authentication,
  - transaction integrity and accountability,
  - fault tolerance,
  - message secrecy, and
  - covertness.
- Many (most?) system fail due to designers protecting the wrong things (or protecting the right things in the wrong way).

SECURITY ENGINEERING

- Let's look at three concrete examples to illustrate the large range of security-critical information systems.
  1. Banking.
  2. Military.
  3. Hospitals.
  4. Your home.
- After examining these examples we can attempt some definitions.

SECURITY ENGINEERING

- Example 1 – Bank
- Primary attack object – branch bookkeeping system (master customer accounts), may be centralized but principal is the same just more so because a single compromise effects more customers
- Main threat – bank employees.
- Main defense – good accounting procedures.
- Public interface – ATM, credit/debit cards plus PIN (potential attack vector), uses online/inline and offline
- cryptography.
- Internet interface for customers – Web + (TSL/SSL or VPNs), new primary attack vector (phishing).
- Both Internet and ATM depend on quality secure messaging and secure communication systems.

SECURITY ENGINEERING

- Example 2 – military
- Electronic warfare with jamming, countermeasures, counter-countermeasures are precursors of information warfare on the Internet (denial of service, ~virus, etc).
- Communications - encryption, transmission masking (low-probability-of-intercept, spread spectrum), destination masking.
- Assurance requirements (online and offline) for logistics and inventory management for VERY large systems. Frequently require access hierarchies.
- Weapons systems (particularly nuclear) often require complex multifactor and/or multi-origin access.

SECURITY ENGINEERING

- Example 3 – Hospitals
- Distributed data and delivery systems.
- Special assurance issues – can't lose data, can't store incorrect data or allow to become corrupt, i.e., reliability, and accuracy extremely important Privacy not only restricted to anonymity (hard to without special "scrubbing"), there are also role based privacy requirements.
- Availability of data/services also critical (sometimes, e.g., when in hospital). Think of DoS.

SECURITY ENGINEERING

- The main lesson is a change in mindset to enable us to design more secure systems:
  - we must learn more about how current systems work, and how have systems failed.
- We generally learn a lot more from our failures than our success.

DEFINING SECURITY BY FUNCTION

- Security can be categorized under the following functional area:
- Risk Avoidance
- Deterrence
- Prevention
- Detection
- Recovery

RISK AVOIDANCE

- An Organization should do a risk assessment that identifies what value and risk each component has to the system in whole and include strategies that reduce the likelihood of behavior/activity that can be damaging.

DETERRENCE

- Deterrence is a common method of control used by government, businesses, and individuals to scare people into thinking twice before performing an action. For example your IP address 132.208.213.10 has been recorded and all activity is subject to monitoring and logging.

PREVENTION

- Information is an asset that requires protection commensurate with its value.
- Security measures must be taken to protect information from unauthorized modification, destruction, or disclosure whether accidental or intentional.
- During the prevention phase, security policies, controls and processes should be designed and implemented.
- Security policies, security awareness programs and access control procedures, are all interrelated and should be developed early on.
- The information security policy is the cornerstone from which all else is built.

DETECTION

- Detection of a system compromise is extremely critical. With the ever increasing threat environment, no matter what level of protection a system may have, it will get compromised given a greater level of motivation and skill. There is no full proof “silver bullet” security solution.
- A defense in layers strategy should be deployed so when each layer fails, it fails safely to a known state and sounds an alarm.
- The most important element of this strategy is timely detection and notification of a compromise.
- Intrusion detection systems (IDS) are utilized for this purpose.

RECOVERY

- Recovery strategies should be developed for Information technology (IT) systems, applications and data.
- This includes networks, servers, desktops, laptops, wireless devices, data and connectivity.
- Priorities for IT recovery should be consistent with the priorities for recovery of business functions and processes that were developed during the business impact analysis

DEFINITION

- System – anything or everything; product or component thereof, operating system, communications system, applications, staff, users, customers, environment in which embedded.
- Subject – physical person in any role
- Person – human or legal entity (company)
- Principal – an entity that participates in a security system (subject, person, role, equipment, communications
- channel, group of principals)
- Role – a function assumable by different persons
- Identity - (pure) a correspondence between a name and a person (as understood by another person)
- Identity - (vernacular) a name
- Trust - believed to be trustworthy (but may not be)

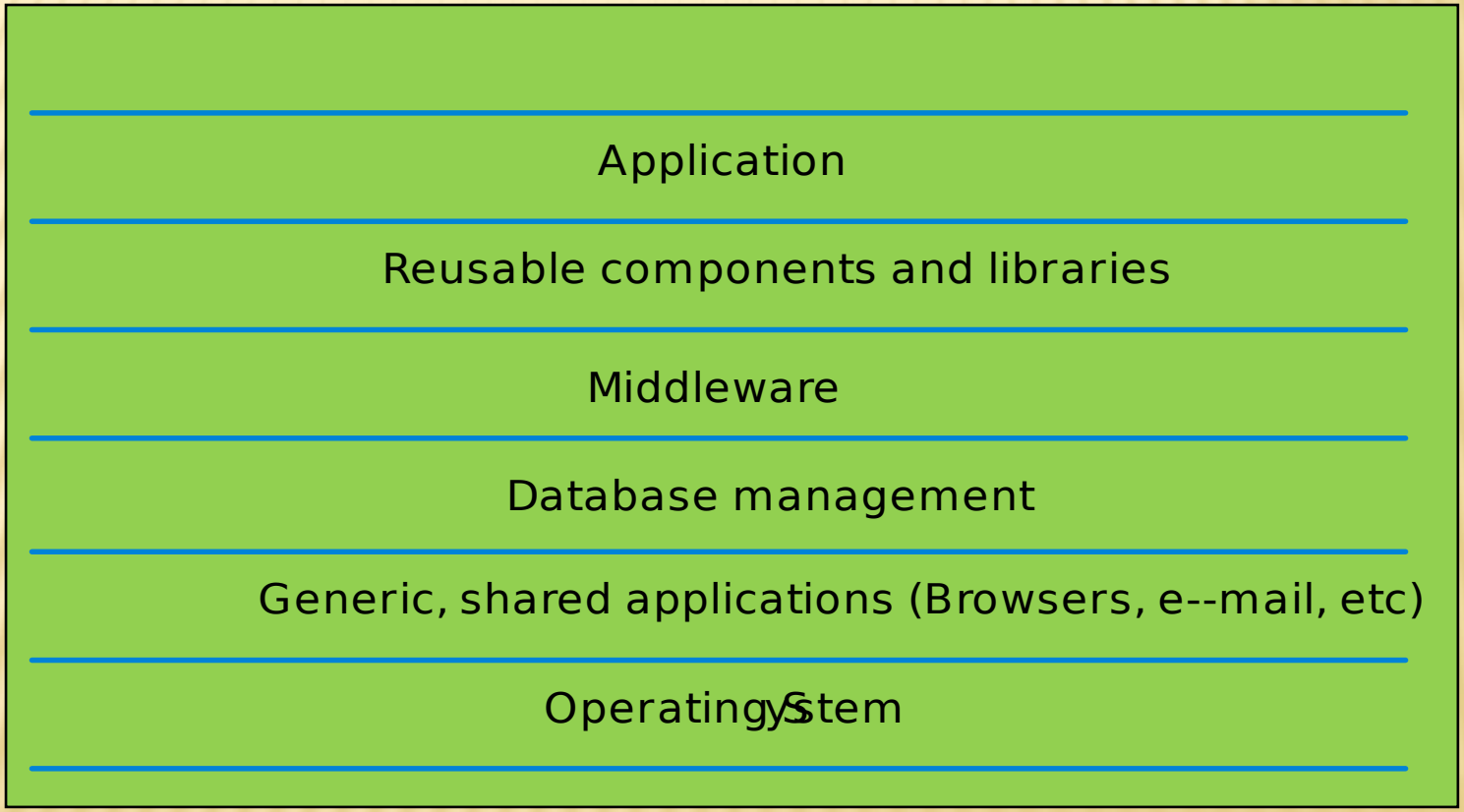
DEFINITION

- Trusted system – is a system is one whose failure can break a security policy
- Trustworthy – a system or subsystem that will not fail
- Secrecy – the effect of the mechanisms used to limit the number of principals who can access information
- Confidentiality – the obligation to protect some other person's or organization's secrets if you know them
- Privacy – the ability or right to protect your personal secrets

APPLICATION/INFRASTRUCTURE SECURITY

- Application security is a software engineering problem where the system is designed to resist attacks.
- Infrastructure security is a systems management problem where the infrastructure is configured to resist attacks.
- Let’s try to focus on application security.

SYSTEM LAYERS



SECURITY CONCEPTS

Term	Definition
Asset	A system resource that has a value and has to be protected.
Exposure	The possible loss or harm that could result from a successful attack. This can be loss or damage to data or can be a loss of time and effort if recovery is necessary after a security breach.
Vulnerability	A weakness in a computer-based system that may be exploited to cause loss or harm.
Attack	An exploitation of a systemÕs vulnerability. Generally, this is from outside the system and is a deliberate attempt to cause some damage.
Threats	Circumstances that have potential to cause loss or harm. You can think of these as a system vulnerability that is subjected to an attack.
Control	A protective measure that reduces a systemÕs vulnerability. Encryption would be an example of a control that reduced a vulnerability of a weak access control system.

EXAMPLES OF SECURITY CONCEPTS

Term	Definition
Asset	The records of each patient that is receiving or has received treatment.
Exposure	Potential financial loss from future patients who do not seek treatment because they do not trust the clinic to maintain their data. Financial loss from legal action by the sports star. Loss of reputation.
Vulnerability	A weak password system which makes it easy for users to set guessable passwords. User ids that are the same as names.
Attack	An impersonation of an authorised user.
Threat	An unauthorised user will gain access to the system by guessing the credentials (login name and password) of an authorised user.
Control	A password checking system that disallows passwords that are set by users which are proper names or words that are normally included in a dictionary.

SECURITY THREATS

- Threats to the confidentiality of a system or its data
- Threats to the integrity of a system or its data
- Threats to the availability of a system or its data

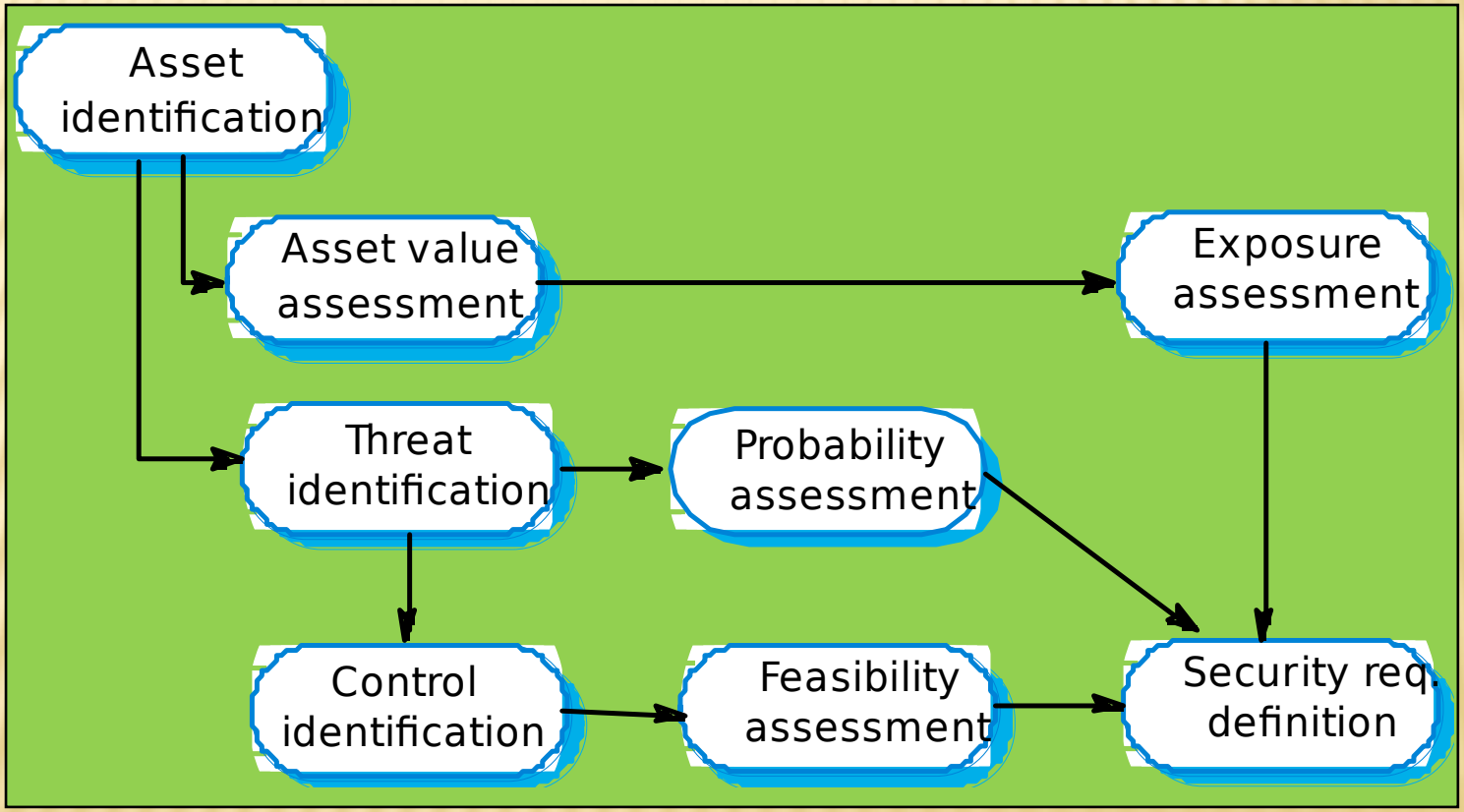
SECURITY CONTROLS

- Controls that are intended to ensure that attacks are unsuccessful. This is analogous to fault avoidance.
- Controls that are intended to detect and repel attacks. This is analogous to fault detection and tolerance.
- Controls that are intended to support recovery from problems. This is analogous to fault recovery.

SECURITY RISK MANAGEMENT

- Risk management is concerned with assessing the possible losses that might ensue from attacks on the system and balancing these losses against the costs of security procedures that may reduce these losses.
- Risk management should be driven by an organisational security policy.
- Risk management involves
  - Preliminary risk assessment
  - Life cycle risk assessment

PRELIMINARY RISK ASSESSMENT



ASSET ANALYSIS

Asset	Value	Exposure
The information system	High. Required to support all clinical consultations. Potentially safety critical.	High. Financial loss as clinics may have to be cancelled. Costs of restoring system. Possible patient harm if treatment cannot be prescribed.
The patient database	High. Required to support all clinical consultations. Potentially safety critical.	High. Financial loss as clinics may have to be cancelled. Costs of restoring system. Possible patient harm if treatment cannot be prescribed.
An individual patient record	Normally low although may be high for specific high-profile patients	Low direct losses but possible loss of reputation.

THREAT AND CONTROL ANALYSIS

Threat	Probability	Control	Feasibility
Unauthorised user gains access as system manager and makes system unavailable	Low	Only allow system management from specific locations which are physically secure.	Low cost of implementation but care must be taken with key distribution and to ensure that keys are available in the event of an emergency.
Unauthorised user gains access as system user and accesses confidential information	High	Require all users to authenticate themselves using biometric mechanism. Log all changes to patient information to track system usage.	Technically feasible but high cost solution. Possible user resistance. Simple and transparent to implement and also supports recovery.

SECURITY REQUIREMENTS

- Patient information must be downloaded at the start of a clinic session to a secure area on the system client that is used by clinical staff.
- Patient information must not be maintained on system clients after a clinic session has finished.
- A log on a separate computer from the database server must be maintained of all changes made to the system database.

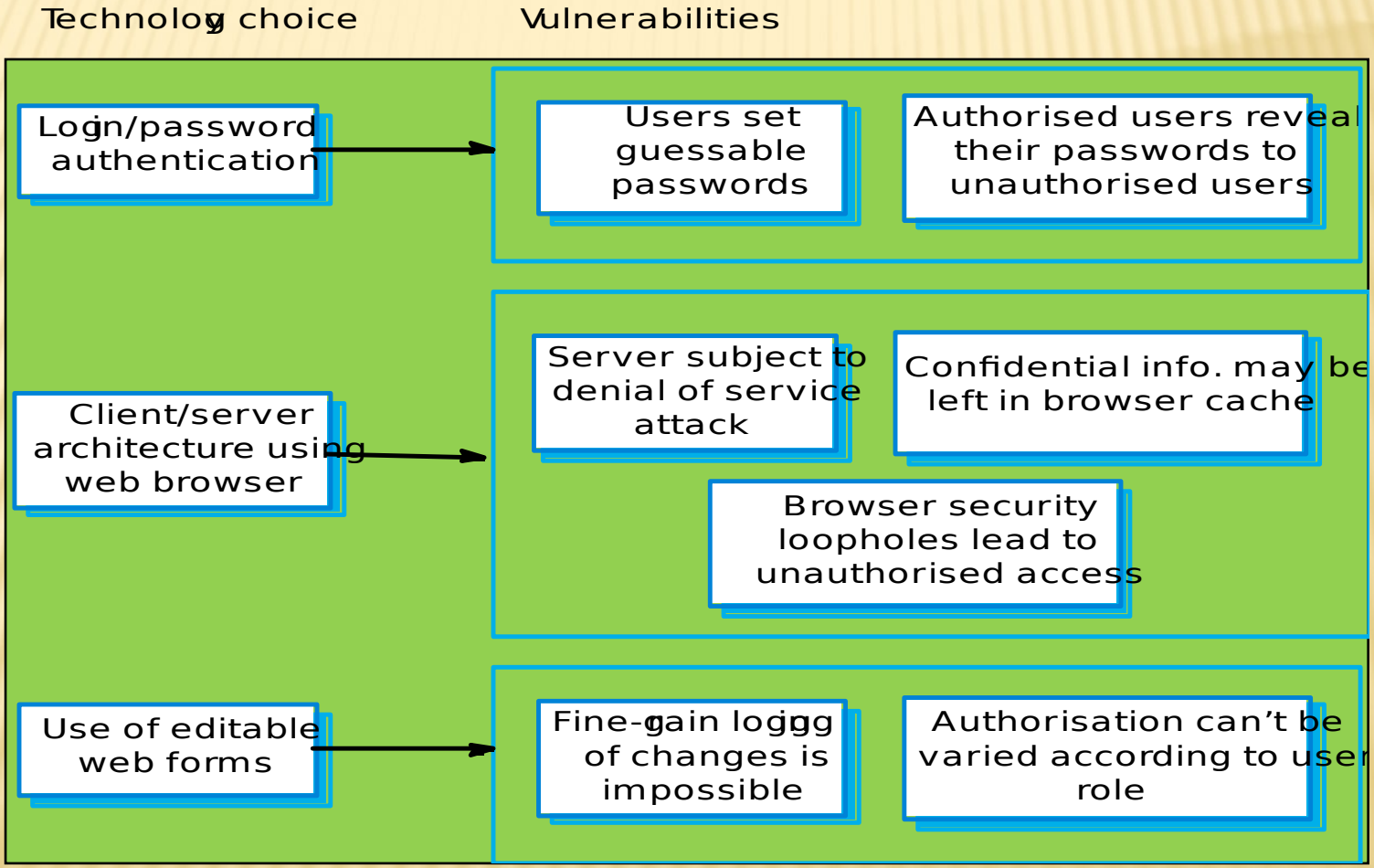
LIFE CYCLE RISK ASSESSMENT

- Risk assessment while the system is being developed and after it has been deployed
- More information is available - system platform, middleware and the system architecture and data organisation.
- Vulnerabilities that arise from design choices may therefore be identified.

EXAMPLES OF DESIGN DECISIONS

- System users authenticated using a name/password combination.
- The system architecture is client-server with clients accessing the system through a standard web browser.
- Information is presented as an editable web form.

TECHNOLOGY VULNERABILITIES



KEY POINTS

- Security engineering is concerned with how to develop systems that can resist malicious attacks
- Security threats can be threats to confidentiality, integrity or availability of a system or its data
- Security risk management is concerned with assessing possible losses from attacks and deriving security requirements to minimize losses

Developed and Presented By Dr. Mehrdad Sepehri Sharbaf
CSUDH
Computer Science Department

http://csc.csudh.edu/

The some of the materials are excerpted from Stuart Jacobs's Book, and Ross Anderson's Book

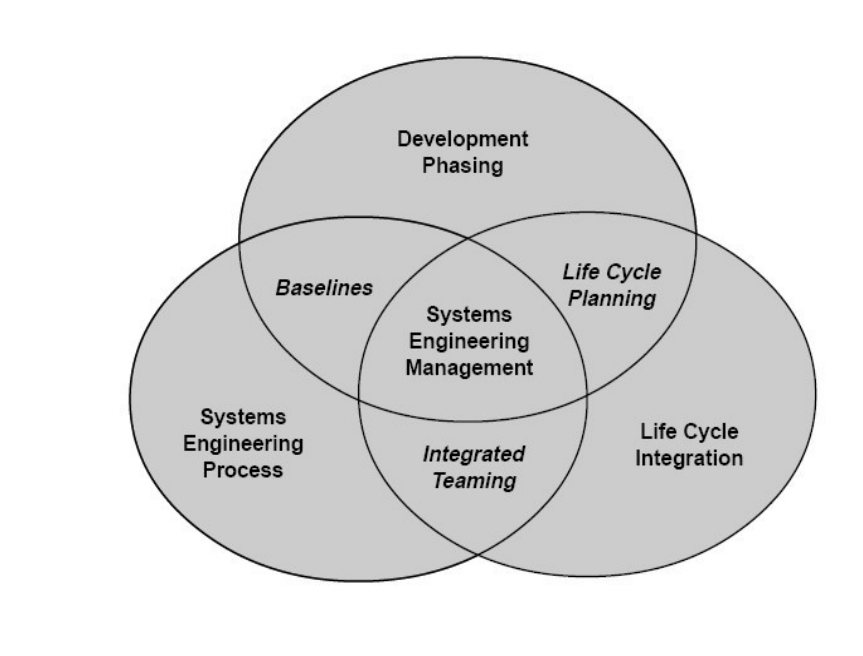
SYSTEM SECURITY ENGINEERING

SYSTEM ENGINEERING

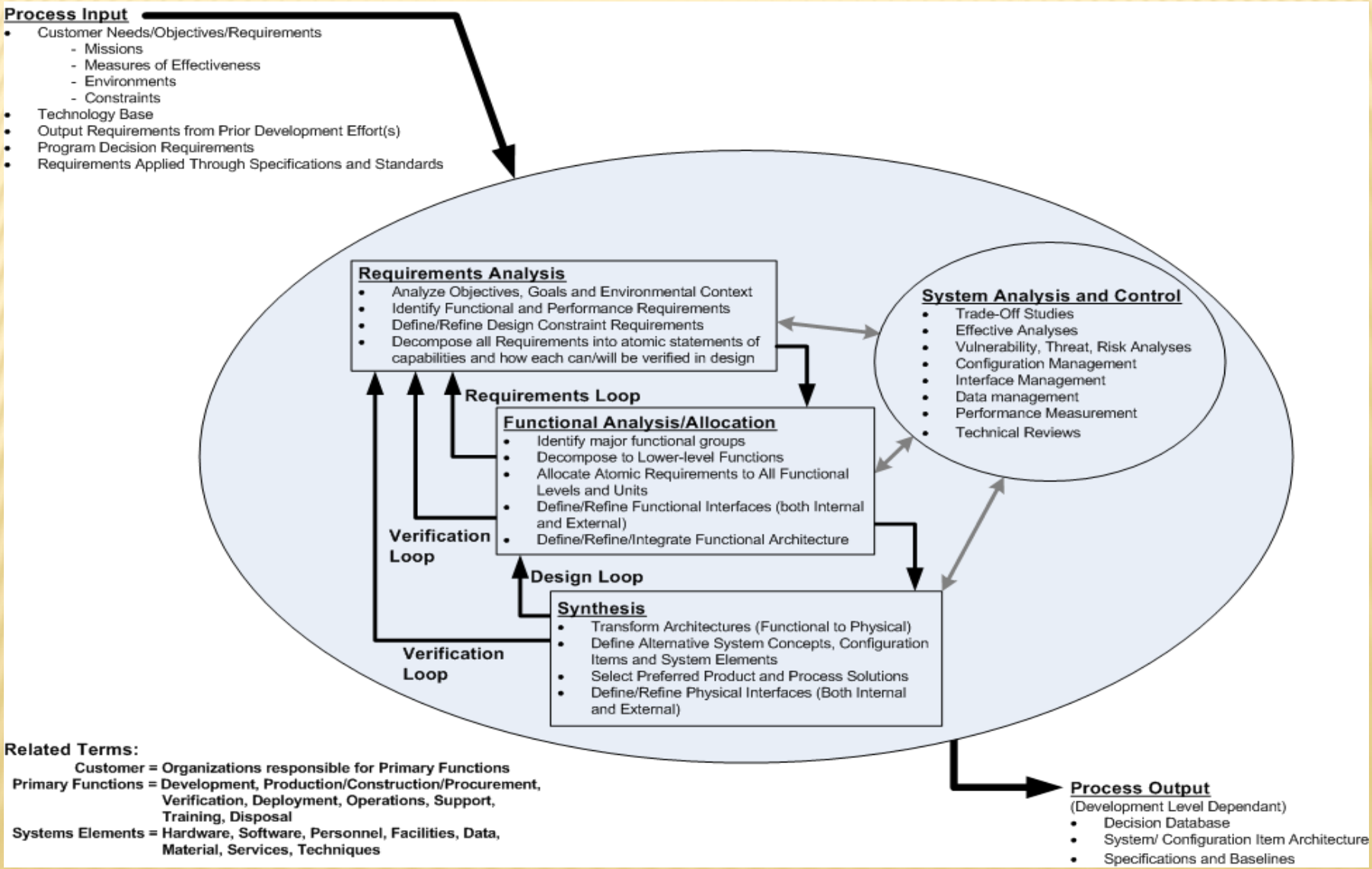
- Systems engineering is a methodical approach to the specification, design, creation, and operation of a function.
- System engineering is a robust approach to the design, creation, and operation of systems. In simple terms, the approach consists of identification and quantification of system goals, creation of alternative system design concepts, performance of design trades, selection and implementation of the best design, verification that the design is properly built and integrated, and post-implementation assessment of how well the system meets (or met) the goals. — *NASA Systems Engineering Handbook, 1995.*

SYSTEM ENGINEERING

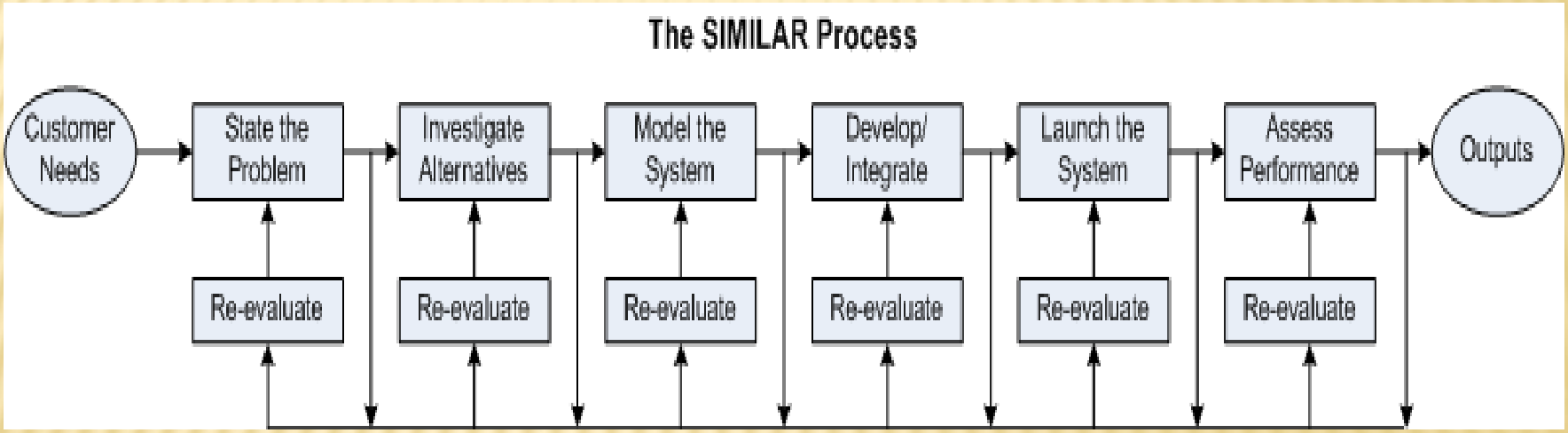
- "The Art and Science of creating effective systems, using whole system, whole life principles" OR "The Art and Science of creating optimal solution systems to complex issues and problems — *Derek Hitchins, Prof. of Systems Engineering, former president of INCOSE (UK), 2007.*



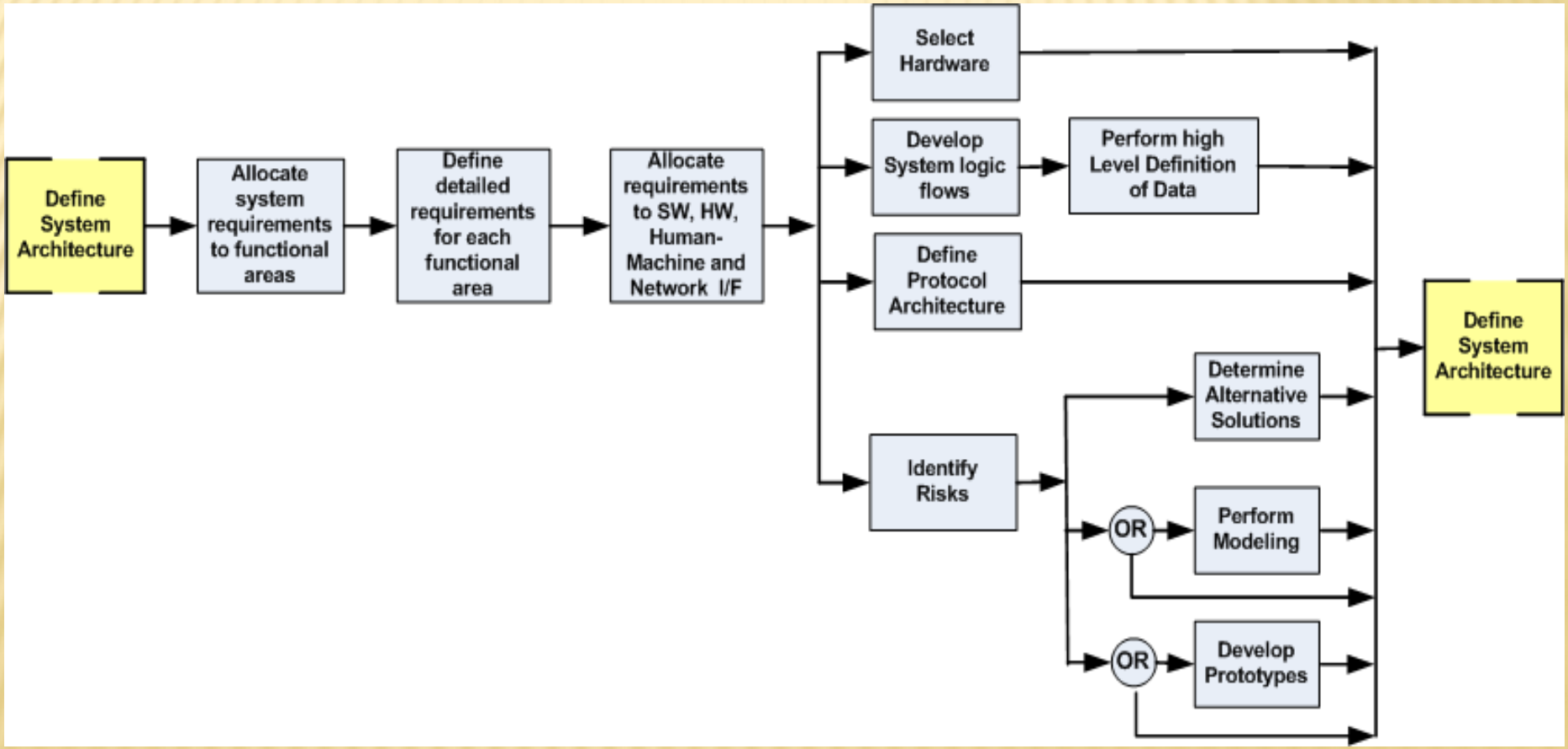
SYSTEM ENGINEERING PROCESS



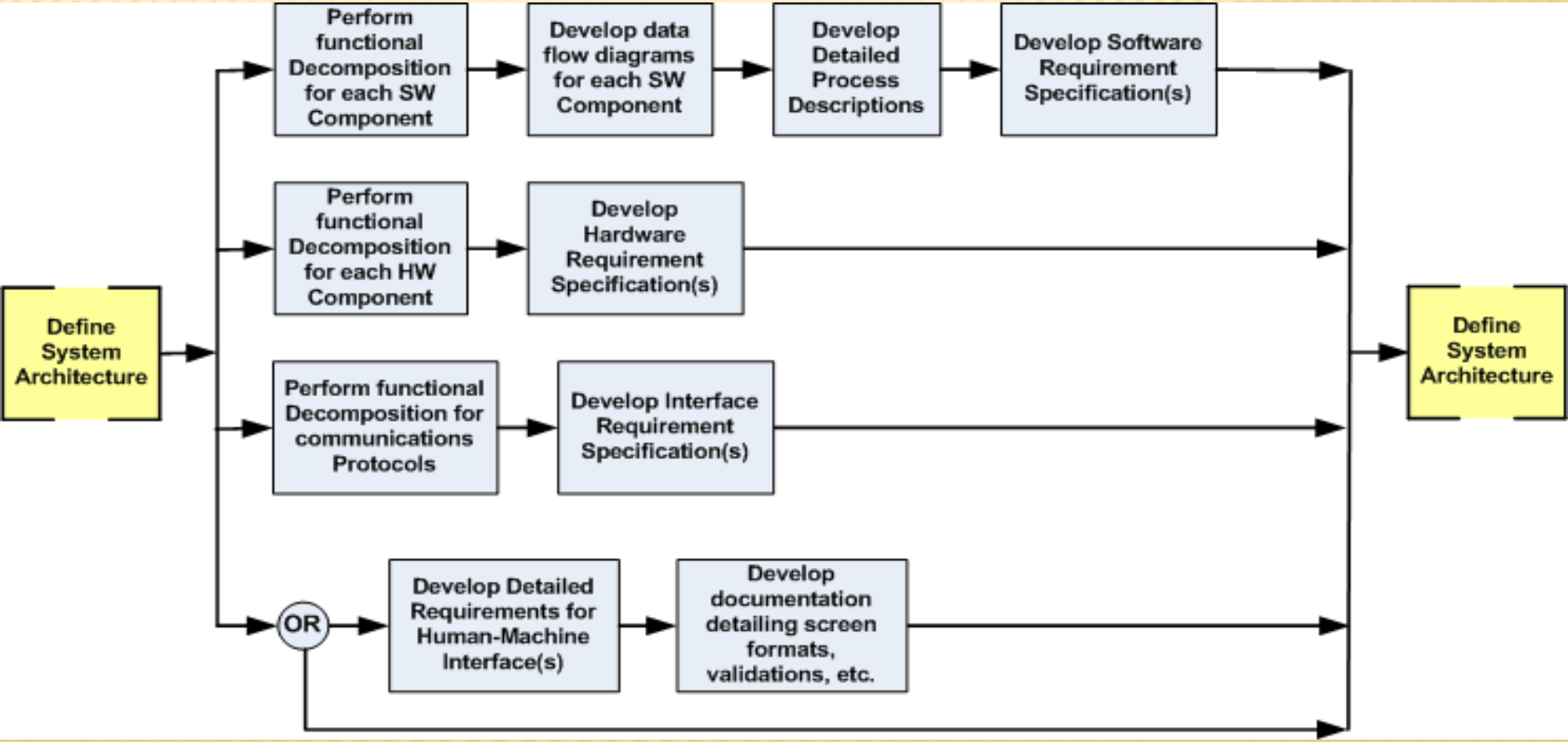
SIMILAR SYSTEM ENGINEERING PROCESS



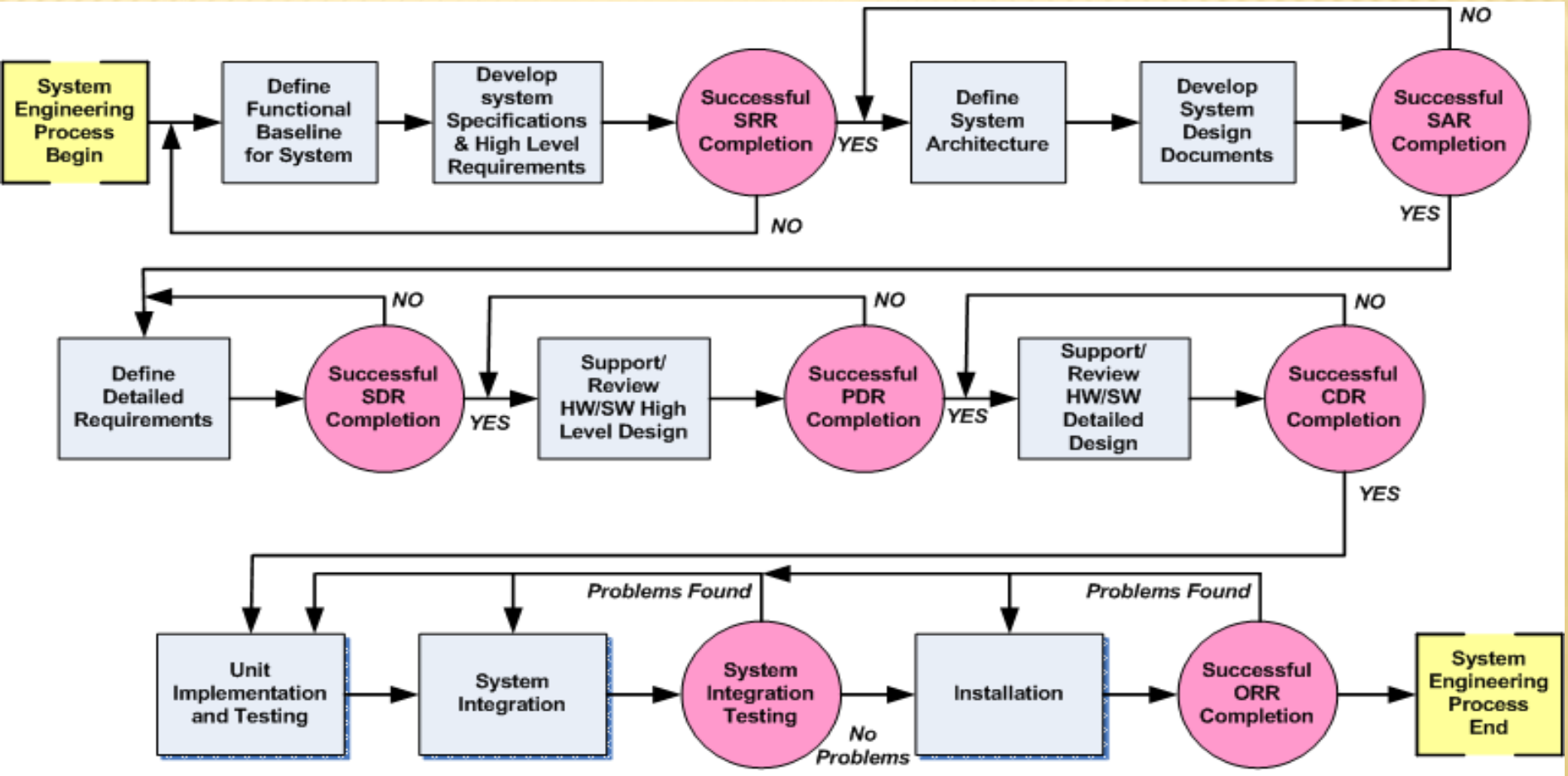
SYSTEM DEVELOPMENT ARCHITECTURE PART 1



SYSTEM DEVELOPMENT ARCHITECTURE PART 2

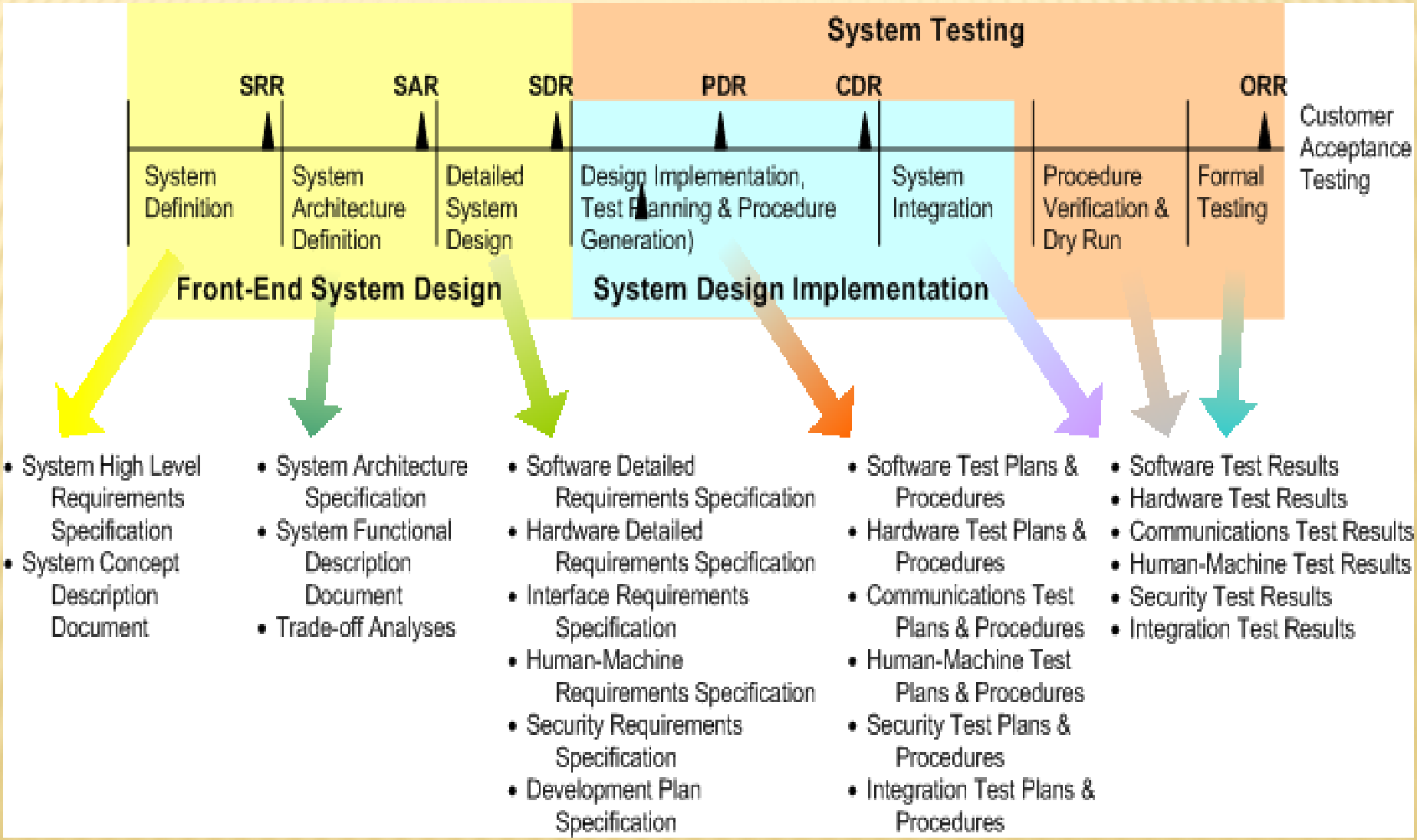


TYPICAL ENGINEERING PROCESS FOR COMPLEX SYSTEM



SRR = System Requirements Review
SAR = System Architecture Review
SDR = System Detailed Requirements Review
PDR = Preliminary Design Review
CDR = Critical Design Review
ORR = Operational Readiness Review

COMPLEX SYSTEM ENGINEERING



SYSTEMS SECURITY ENGINEERING

Definitions: Systems security engineering is a specialty engineering field strongly related to systems engineering. It applies scientific, engineering, and information assurance principles to deliver trustworthy systems that satisfy stakeholder requirements within their established risk tolerance(NIST).

2019 Annual INCOSE Western States Regional Conference (WSRC)

Systems Security Engineering

Mehrdad Sharbaf, Ph.D.

Adjunct Professor CSUDH

Chair CLAS IEEE Computer Society Chapter

Objective

- Understand System Security Engineering processes in the development of systems.
- Evaluate the security design of systems using security engineering processes and principles.
- Develop system designs that embed security functions and provide adequate protection to system functions.
- Analyze system security risk within the context of system operations and organizational risk tolerance.
- Understand NIST SP800-160 System Security Engineering Framework, and Engineering secure systems with ISO 26702, ISO 21827 and 27001

Agenda

- Problem related to information security
- What is system engineering?
- What is system security engineering?
- System Security Engineering Processes
- Design For Security
- Security risk assessment and management
- The Systems Security Engineering Capability Maturity Model (ISO 21827)
- NIST SP800-160 System Security Engineering Framework
- System Security Engineering Assistant Tools

Problem related to information security

- How does management establish and track an information security program when:
- Current system security strategies are inadequate, and it lacks proper security engineering implementation within organization
- That impacts the organization costly, and systems fail to be certified and accredited. As systems have grown more complex and adversaries in cyberspace continue to successfully exploit numerous vulnerabilities, the need for improved secure system engineering has become acute.
- Risks are real
- Risks are nearly infinite
- The information environment is highly dynamic
- Resources are finite

Introduction to Information Security

- The protection of information and its critical elements, including systems, software, and hardware that use, store, and transmit that information
- Necessary tools: risk management, policy, awareness, training, education, technology
- C.I.A. triangle was standard based on confidentiality, integrity, and availability
- C.I.A. triangle now expanded into list of critical characteristics of information

Security Goals

- Confidentiality
  - Confidentiality means that people cannot read sensitive information, either while it is on a computer or while it is traveling across a network.

Security Goals

- Integrity
  - Integrity means that attackers cannot change or destroy information, either while it is on a computer or while it is traveling across a network. Or, at least, if information is changed or destroyed, then the receiver can detect the change or restore destroyed data.

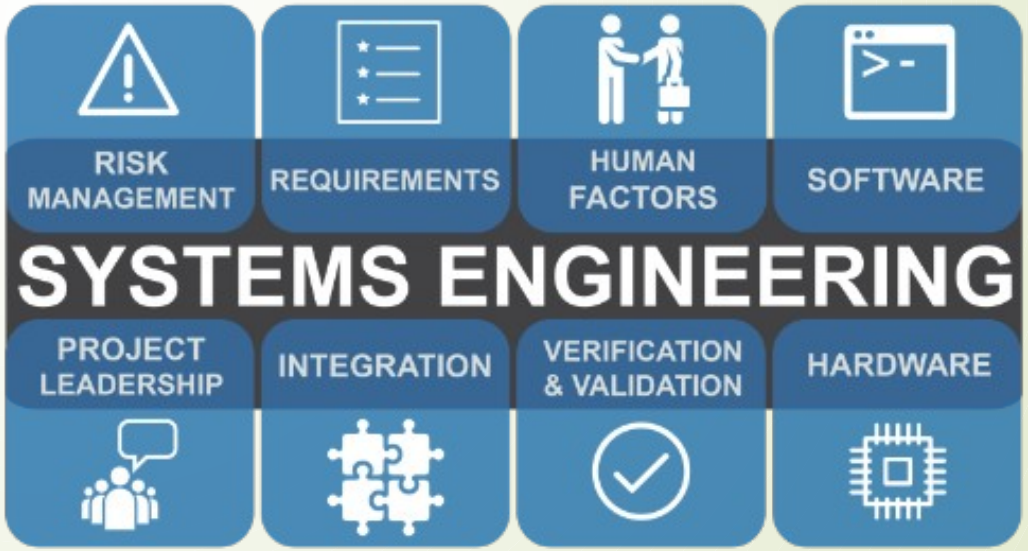
Security Goals

- Availability
  - Availability means that people who are authorized to use information are not prevented from doing so

System Engineering

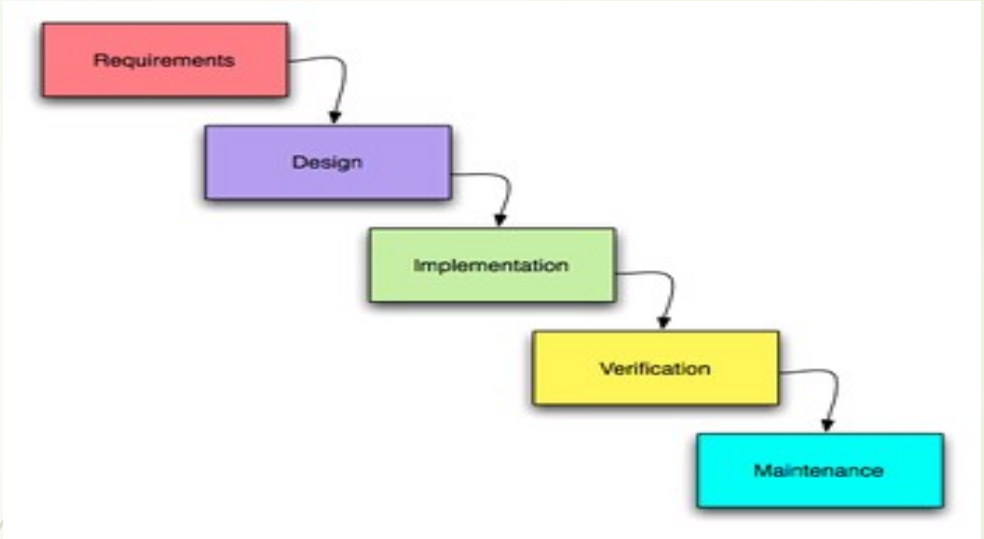
- Systems Engineering (SE) is the engineering discipline that focuses on integrating all the key elements of a system into one overall system and managing it throughout its lifecycle.
- “Systems engineering is an interdisciplinary engineering management process that evolves and verifies an integrated, life-cycle balanced set of system solutions that satisfy customer needs.” (DoD).
- Systems Engineering integrates all the disciplines and specialty groups into a team effort forming a structured development process that proceeds from concept to production to operation. Systems Engineering considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs(INCOS).

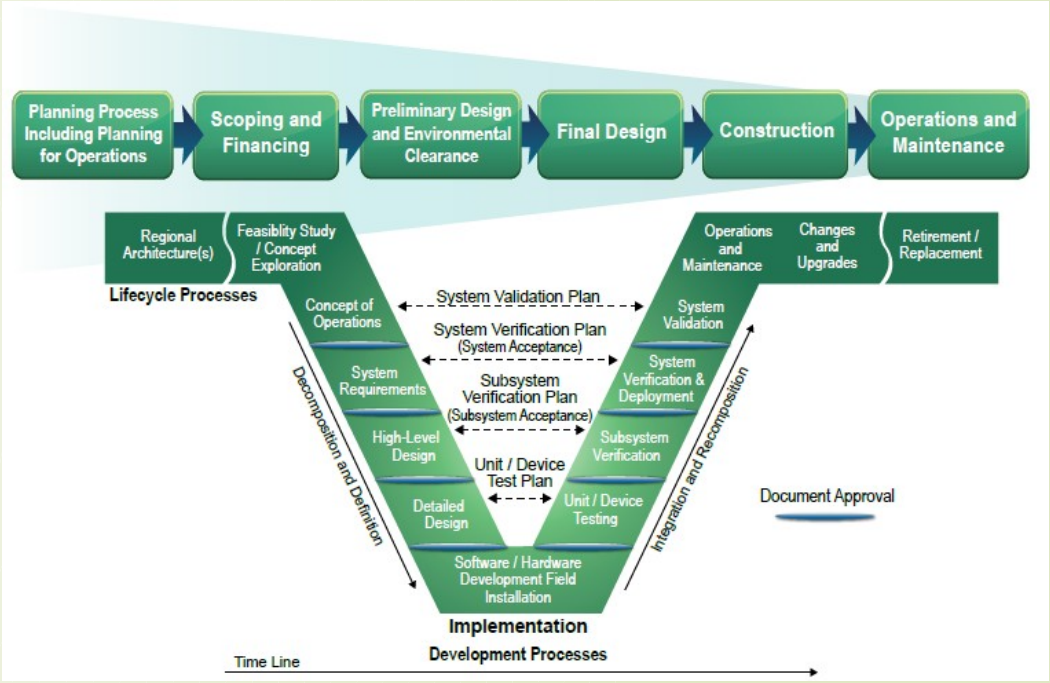
System Engineering



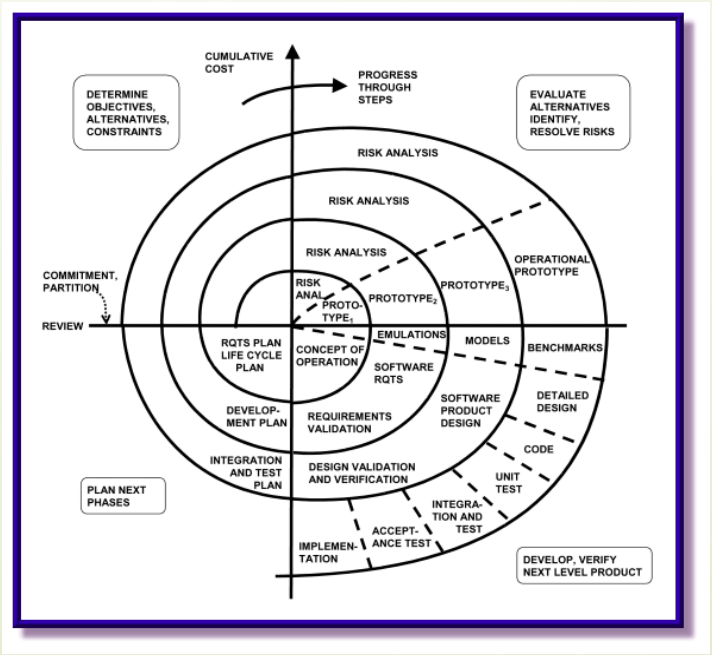
Definition of a “system”

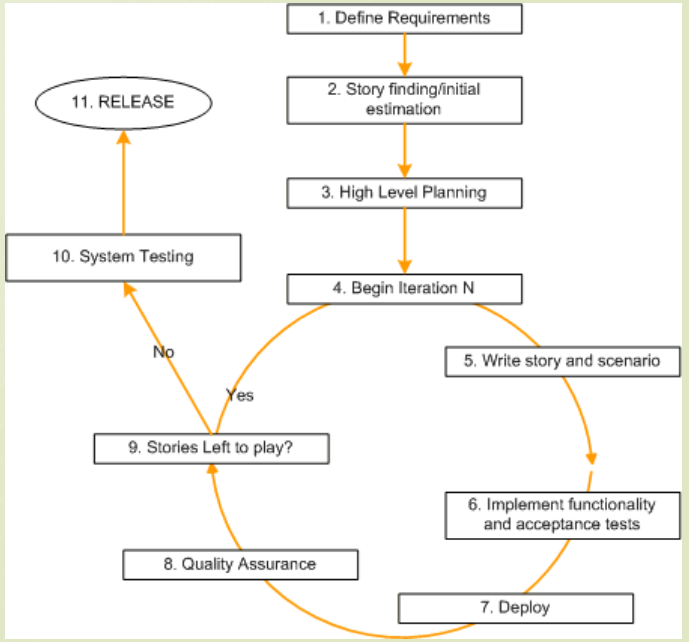
“System design is the process or art of defining the hardware and software architecture, components, modules, interfaces, and data for a computer system to satisfy specified requirements.”





Some examples of System and software development models





Systems Security Engineering

- Description: The concept of Systems Security Engineering is to serve the organization to ensure that the security requirements of systems are met under advanced adversarial attack.
- System Security Engineering (SSE) is an element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities [DoD 5200.44].

Systems Security Engineering

- The focus of the Systems Security Engineering discipline is:
  - tools,
  - processes, and
  - methods
- needed to
  - design,
  - implement, and
  - test
- complete systems, and to adapt existing systems as their environment evolves.

Process Models

- **Secure Process**
  - Set of activities performed to develop, maintain, and deliver a secure software solution
  - Activities could be concurrent or iterative
- **Process model**
  - provides a reference set of best practices that can be used for both
    - process improvement and process assessment.
  - defines the characteristics of processes
  - usually has an architecture or a structure

System Development Life Cycle (SDLC)

- A survey of existing processes, process models, and standards seems to identify the following four SDLC focus areas for secure system development
  - Security Engineering Activities
  - Security Assurance
  - Security Organizational and Project Management Activities
  - Security Risk Identification and Management Activities

SDLC

- Security Engineering Activities
  - activities needed to engineer a secure solution.

    security requirements elicitation and definition,

    secure design based on design principles for security,

    use of static analysis tools,

    reviews and inspections, security testing, etc..
- Security Assurance Activities

  verification, validation, expert review,

  artifact review, and evaluations.

SDLC

- Security Organizational and Project Management Activities
  - Organizational management
    - organizational policies, senior management sponsorship and oversight, establishing organizational roles, ….
  - Project management
    - project planning and tracking,
    - resource allocation and usage
- Security Risk Identification and Management Activities
  - Cost-based Risk analysis
  - Risk mitigation ..

Capability Maturity Models (CMM)

- CMM
  - Provides reference model of mature practices
  - Helps identify the potential areas of improvement
  - Provides goal-level definition for and key attributes for specific processes
  - Systems Security Engineering Capability Maturity Model (SSE-CMM)
    - Specifically to develop secure systems

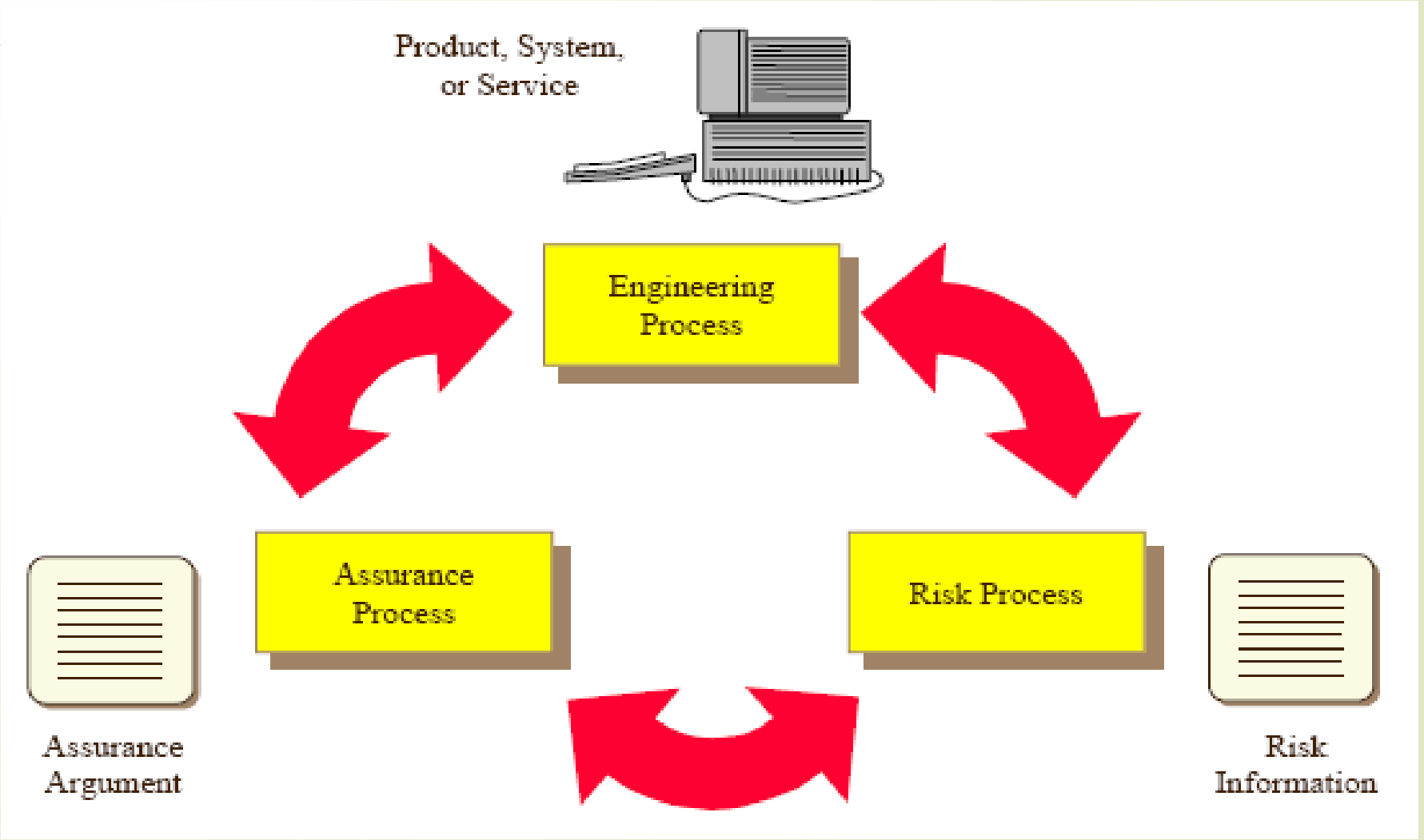
Systems Security Engineering CMM

- The SSE-CMM
  - To improve and assess the security engineering capability of an organization
- provides a comprehensive framework for
  - evaluating security engineering practices against the generally accepted security engineering principles.
- provides a way to
  - measure and improve performance in the application of security engineering principles.

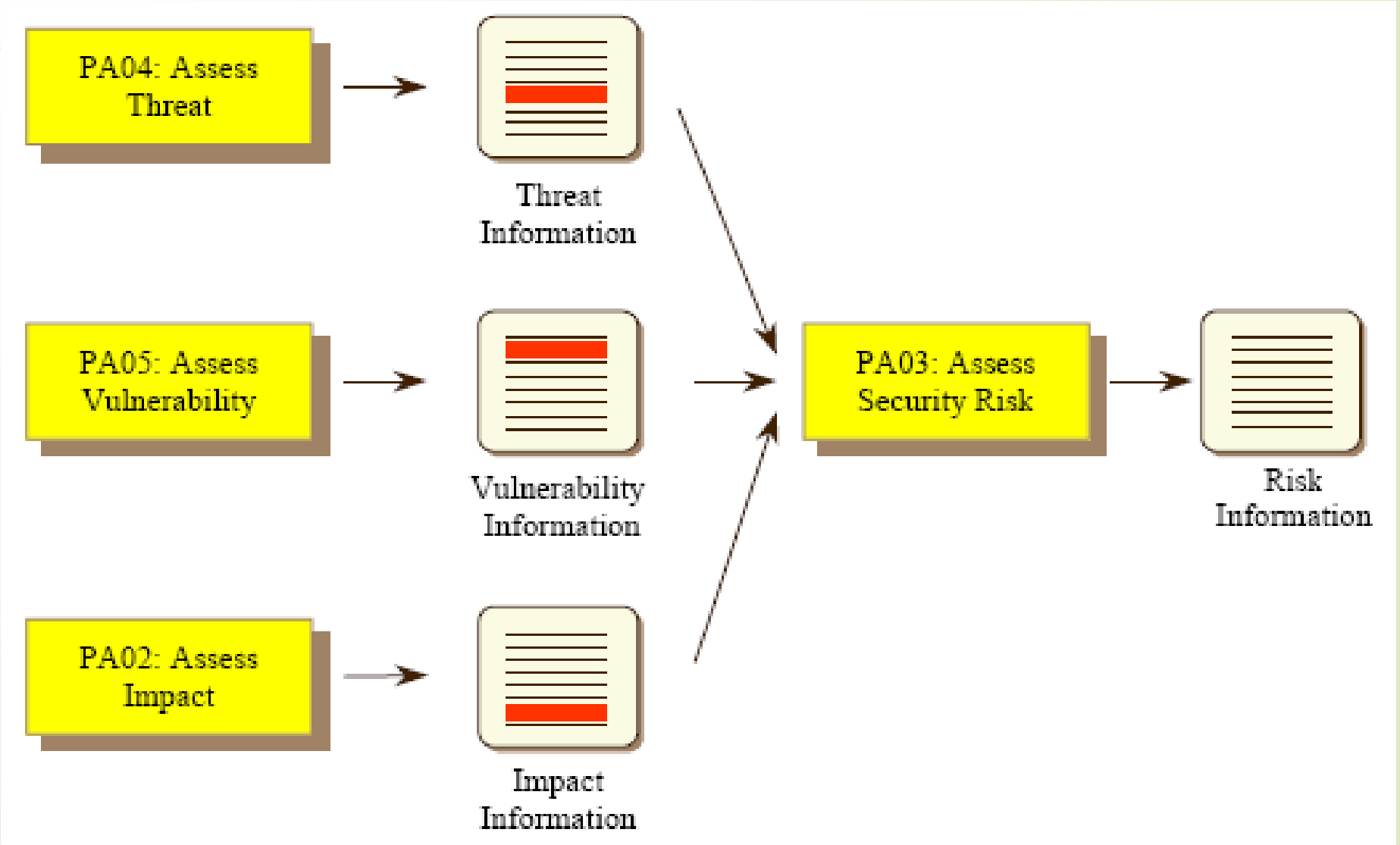
SSE-CMM

- Purpose for SSE-CMM
  - To fill the lack of a comprehensive framework for evaluating security engineering practices against the principles
- The SSE-CMM also
  - describes the essential characteristics of an organization’s security engineering processes.
    - The SSE-CMM is now ISO/IEC 21827 standard

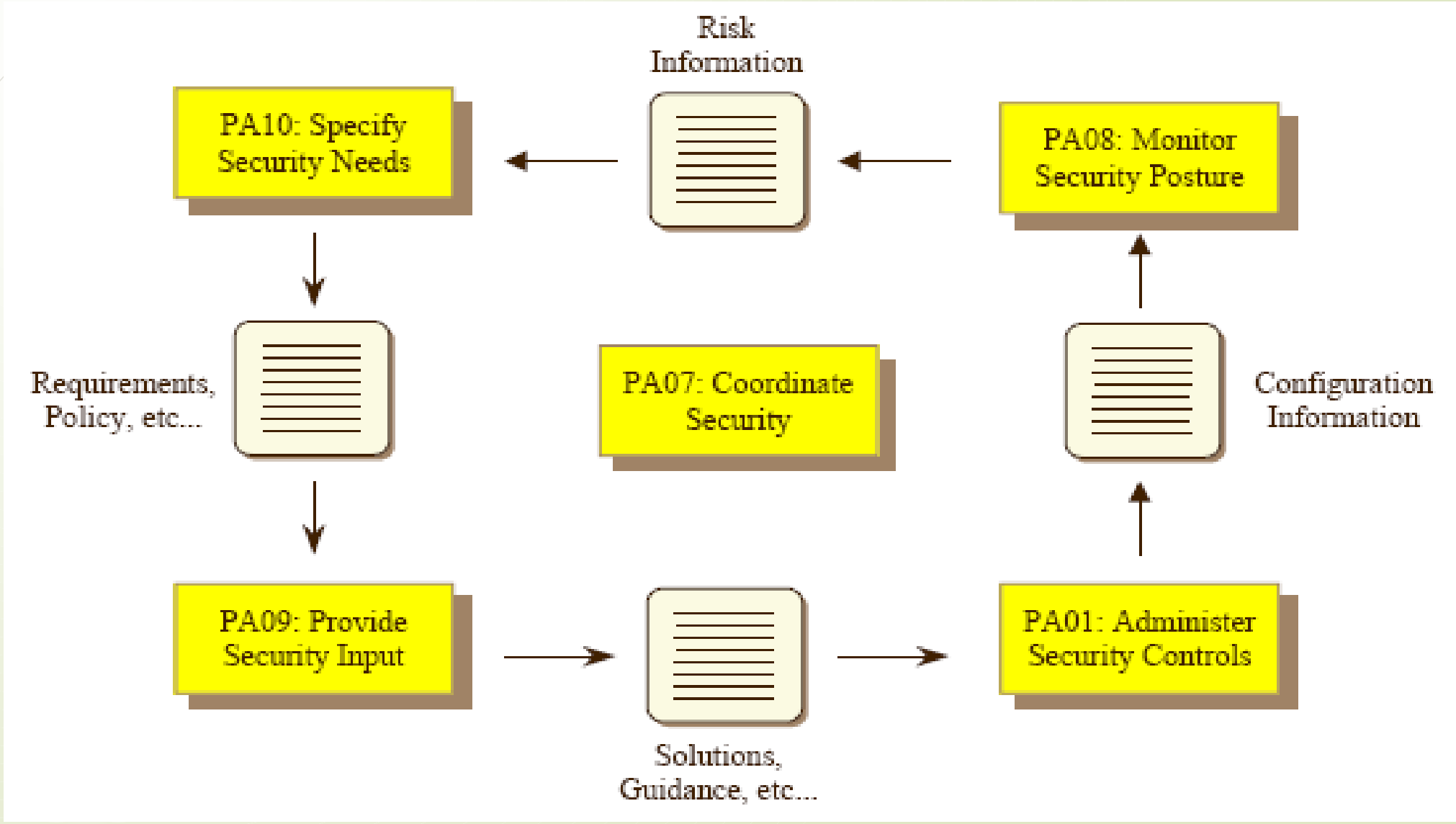
Security Engineering Process



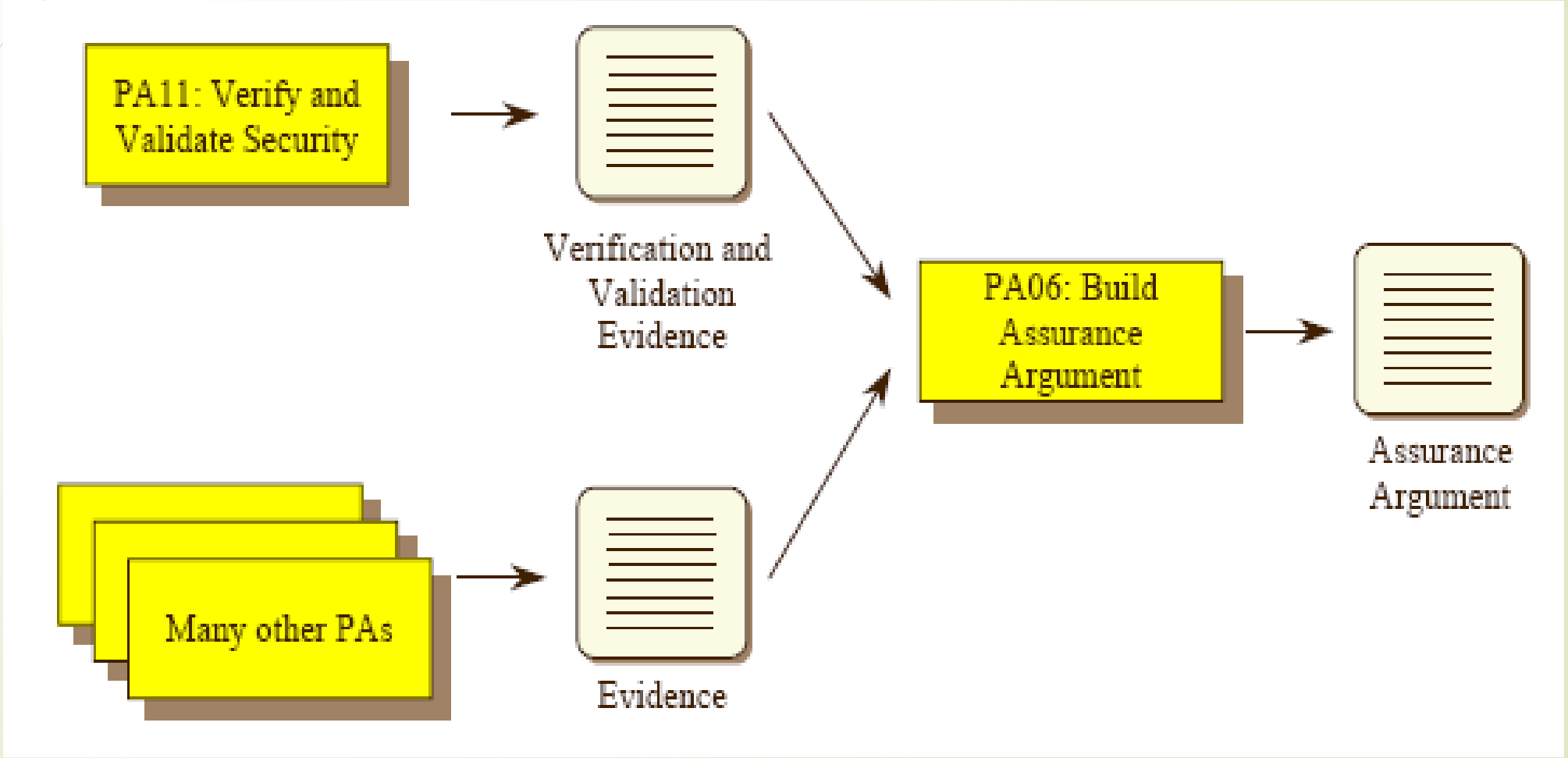
Security Risk Process



Security is part of Engineering



Assurance


PA11: Verify and Validate Security
Verification and Validation Evidence
PA06: Build Assurance Argument
Assurance Argument
Many other PAs
Evidence

Process Areas

Process Areas related to Security Engineering process areas

- PA01 Administer Security Controls
- PA02 Assess Impact
- PA03 Assess Security Risk
- PA04 Assess Threat
- PA05 Assess Vulnerability
- PA06 Build Assurance Argument
- PA07 Coordinate Security
- PA08 Monitor Security Posture
- PA09 Provide Security Input
- PA10 Specify Security Needs
- PA11 Verify and Validate Security

Process Areas related to project and Organizational practices

- PA12 – Ensure Quality
- PA13 – Manage Configuration
- PA14 – Manage Project Risk
- PA15 – Monitor and Control Technical Effort
- PA16 – Plan Technical Effort
- PA17 – Define Organization's Systems Engineering Process
- PA18 – Improve Organization's Systems Engineering Process
- PA19 – Manage Product Line Evolution
- PA20 – Manage Systems Engineering Support Environment
- PA21 – Provide Ongoing Skills and Knowledge
- PA22 – Coordinate with Suppliers

Design for security

- Architectural design - how do architectural design decisions affect the security of a system?
- Good practice - what is accepted good practice when designing secure systems?
- Design for deployment - what support should be designed into a system to avoid the introduction of vulnerabilities when a system is deployed for use?

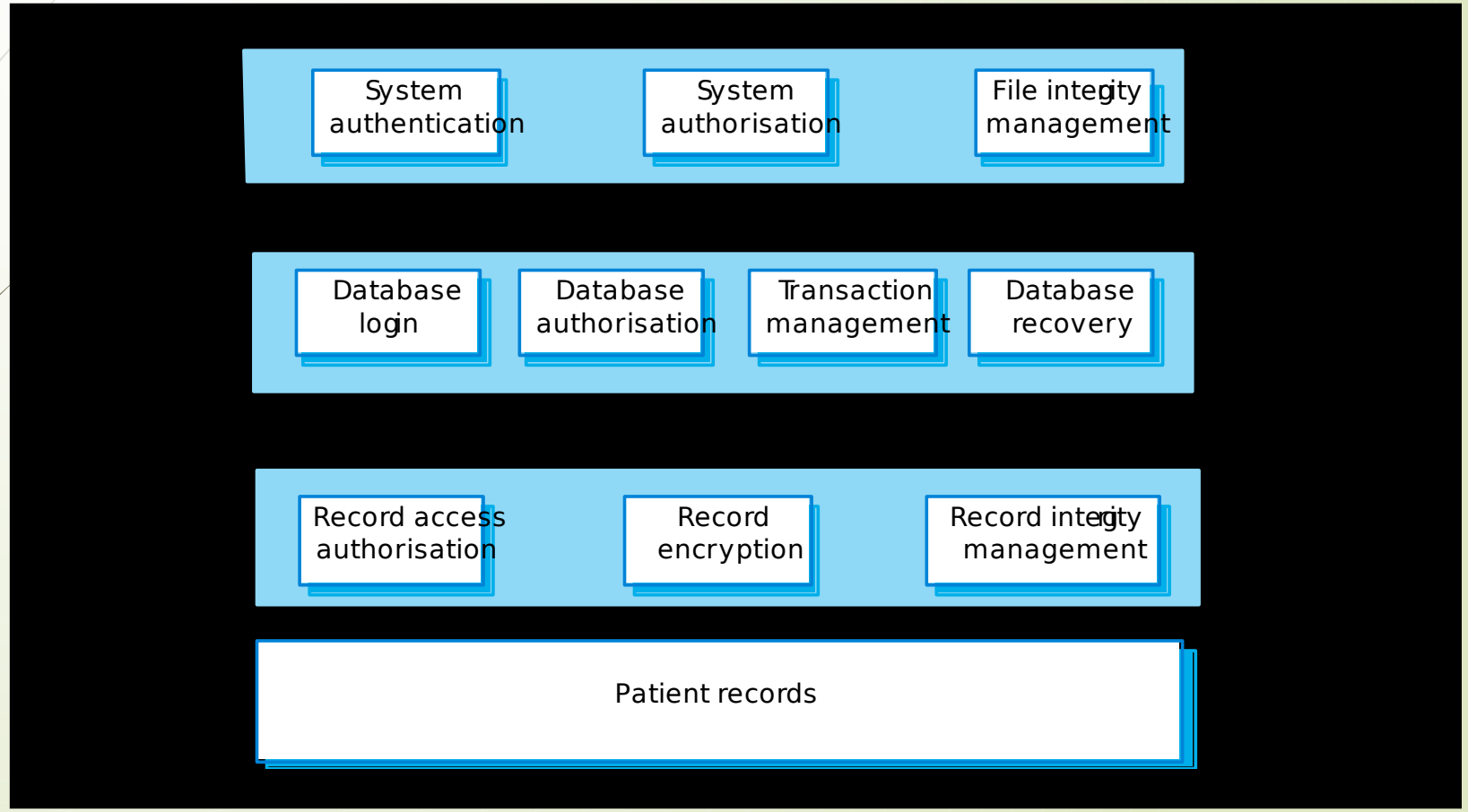
Architectural design

- Protection
  - How should the system be organized so that critical assets can be protected against external attack?
- Distribution
  - How should system assets be distributed so that the effects of a successful attack are minimized?
- Potentially conflicting
  - If assets are distributed, then they are more expensive to protect.

Protection

- Platform-level protection
- Application-level protection
- Record-level protection

Layered protection



Design guidelines

- Design guidelines encapsulate good practice in secure systems design
- Design guidelines serve two purposes:
  - They raise awareness of security issues in a software engineering team.
  - They can be used as the basis of a review checklist that is applied during the system validation process.

Design guidelines 1

- Base security decisions on an explicit security policy
- Avoid a single point of failure
- Fail securely
- Balance security and usability
- Be aware of the possibilities of social engineering

Design guidelines 2

- Use redundancy and diversity to reduce risk
- Validate all inputs
- Compartmentalize your assets
- Design for deployment
- Design for recoverability

Survivability strategies

- Resistance
  - Avoiding problems by building capabilities into the system to resist attacks
- Recognition
  - Detecting problems by building capabilities into the system to detect attacks and failures and assess the resultant damage
- Recovery
  - Tolerating problems by building capabilities into the system to deliver services whilst under attack

NIST Systems Security Engineering Initiative

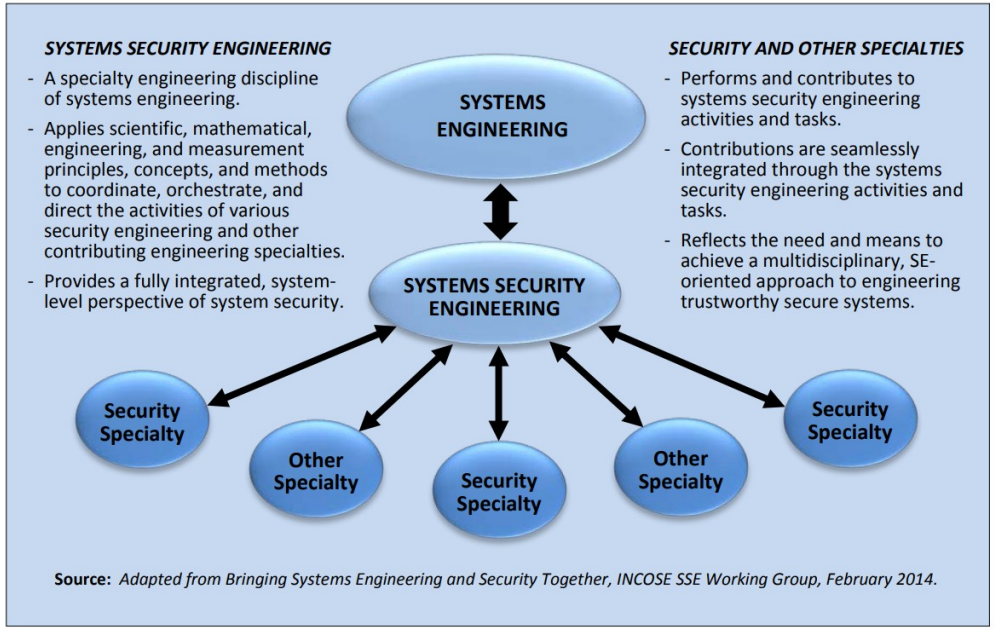
- NIST Special Publication 800-160 is the flagship publication in a series of planned systems security engineering publications.
- The series of 800-160 publications will include several important systems security engineering topics, for example: hardware security and assurance; software security and assurance; and system resiliency.
- Each topic will be addressed in the context of the system life cycle processes contained in ISO/IEC/IEEE 15288 and the security related activities and tasks that are described in SP 800-160.

NIST-Systems Security Engineering

- Systems security engineering, as an integral part of systems engineering, helps to ensure that the appropriate security principles, concepts, methods, and practices are applied during the system life cycle to achieve stakeholder objectives for the protection of assets—across all forms of adversity characterized as disruptions, hazards, and threats.
- It also helps to reduce system defects that can lead to security vulnerability and as a result, reduces the susceptibility of the system to adversity

NIST-Systems Security Engineering

- Systems security engineering leverages many security specialties and focus areas that contribute to systems security engineering activities and tasks. These security specialties and focus areas include, for example: computer security; communications security; transmission security; antitamper protection; electronic emissions security; physical security; information, software, and hardware assurance; and technology specialties such as biome

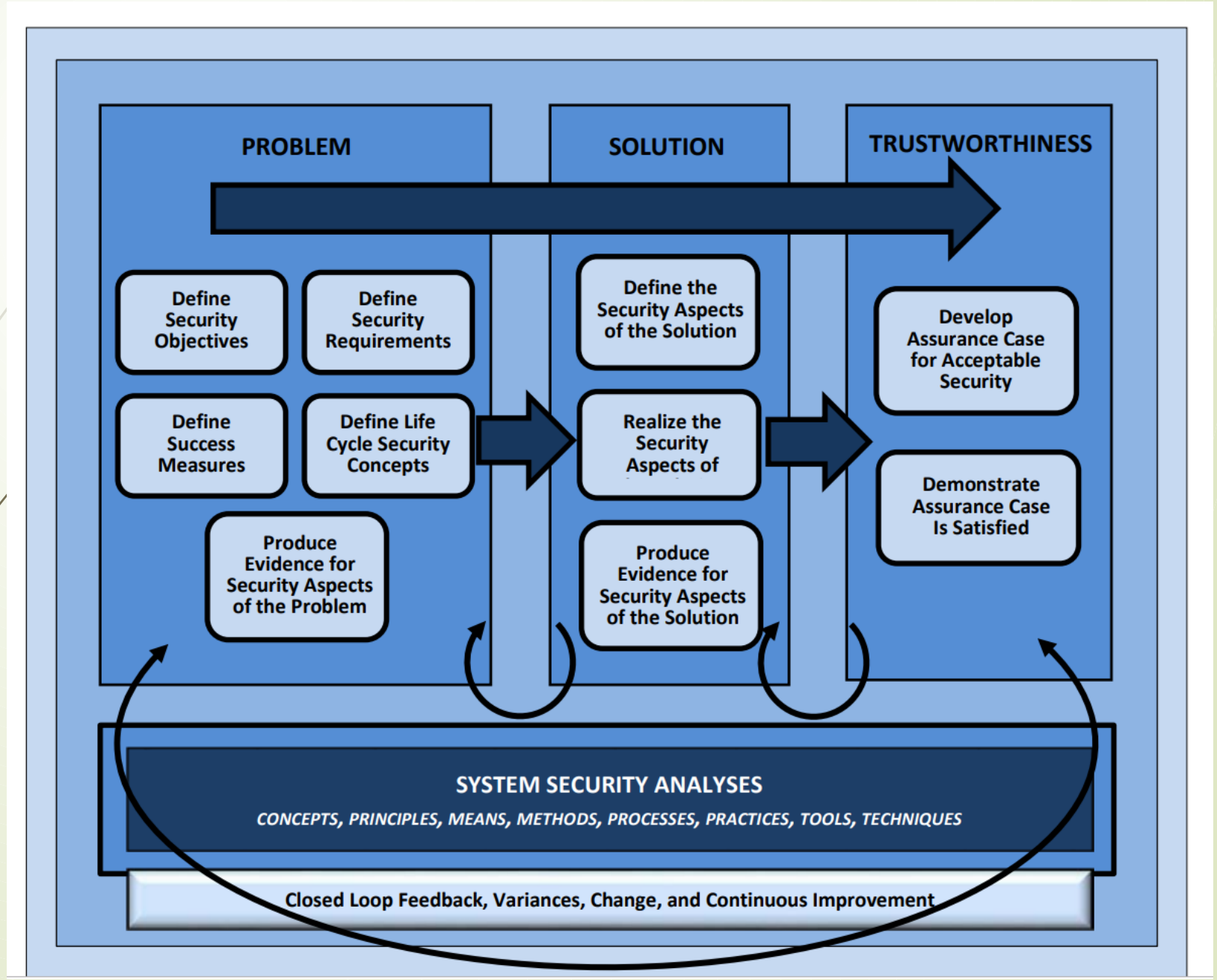


NIST-Role of Systems Security Engineering

- Engineering the security functions that provide system security capability
- Engineering the security-driven constraints for all system functions; and
- Engineering and advising for the protection of data, information, technology, methods, and assets associated with the system throughout its life cycle.
- These roles require a systems security engineering presence in all systems engineering activities in order to establish a multidisciplinary security and specialty approach to engineering—resulting in sustainably trustworthy secure systems throughout the system life cycle.

NIST-SYSTEMS SECURITY ENGINEERING FRAMEWORK

- The systems security engineering framework emphasizes an integrated, holistic security perspective across all stages of the system life cycle and is applied to satisfy the milestone objectives of each life cycle stage.
- The figure provides an overview of the systems security engineering framework and its key components.
- The framework defines three contexts within which the systems security engineering activities are conducted. These are the problem context, the solution context, and the trustworthiness context. Establishing the three contexts helps to ensure that the engineering of a system is driven by a sufficiently complete understanding of the problem articulated in a set of stakeholder security objectives that reflect protection needs and security concerns


PROBLEM
SOLUTION
TRUSTWORTHINESS
Define Security Objectives
Define Security Requirements
Define Success Measures
Define Life Cycle Security Concepts
Produce Evidence for Security Aspects of the Problem
Define the Security Aspects of the Solution
Realize the Security Aspects of
Produce Evidence for Security Aspects of the Solution
Develop Assurance Case for Acceptable Security
Demonstrate Assurance Case Is Satisfied
SYSTEM SECURITY ANALYSES
CONCEPTS, PRINCIPLES, MEANS, METHODS, PROCESSES, PRACTICES, TOOLS, TECHNIQUES
Closed Loop Feedback, Variances, Change, and Continuous Improvement

The Problem Context

- The problem context defines the basis for an acceptably and adequately secure system given the stakeholder’s mission, capability, performance needs and concerns; the constraints imposed by stakeholder concerns related to cost, schedule, risk and loss tolerance; and other constraints associated with life cycle concepts for the system
- The problem context includes:
- Determining life cycle security concepts
- Defining security objectives;
- Defining security requirements; and
- Determining measures of success.

The Solution Context

- The solution context transforms the stakeholder security requirements into design requirements for the system; addresses all security architecture, design, and related aspects necessary to realize a system that satisfies those requirements; and produces sufficient evidence to demonstrate that those requirements have been satisfied.
- The system security protection strategy is consistent with the overall concept of secure function. The concept of secure function, defined during the problem context, constitutes a strategy for a proactive and reactive protection capability throughout the system life cycle.
- The Solution Context includes:
- Defining the security aspects of the solution
- Realizing the security aspects of the solution; and
- Producing evidence for the security aspects of the solution.

The Trustworthiness Context

- The trustworthiness context is a decision-making context that provides an evidence-based demonstration, through reasoning, that the system-of-interest is deemed trustworthy based upon a set of claims derived from security objectives.
- The trustworthiness context consists of:
- Developing and maintaining the assurance case; and
- Demonstrating that the assurance case is satisfied.

SYSTEM LIFE CYCLE PROCESSES SYSTEM SECURITY IN SYSTEM LIFE CYCLE PROCESSES

- It describes the security considerations and contributions to system life cycle processes to produce the security outcomes that are necessary to achieve trustworthy secure systems.
- The security considerations and contributions are provided as systems security engineering activities and tasks and they are aligned with and developed as security extensions to the system life cycle processes in ISO/IEC/IEEE 15288, Systems and software engineering – System life cycle processes.

System Life Cycle Processes

Recursive, Iterative, Concurrent, Parallel, Sequenced Execution

Agreement Processes	Organizational Project-Enabling Processes	Technical Management Processes	Technical Processes
• Acquisition • Supply	• Life Cycle Model Management • Infrastructure Management • Portfolio Management • Human Resource Management • Quality Management • Knowledge Management	• Project Planning • Project Assessment and Control • Decision Management • Risk Management • Configuration Management • Information Management • Measurement • Quality Assurance	• Business or Mission Analysis • Stakeholder Needs and Requirements Definition • System Requirements Definition • Architecture Definition • Design Definition • System Analysis • Implementation • Integration • Verification • Transition • Validation • Operation • Maintenance • Disposal

Source: *ISO/IEC/IEEE 15288: 2015*

SSE contributes to all SE life cycle processes – with emphasis on the Technical Processes

SECURITY IN SYSTEM LIFE CYCLE PROCESSES

- Each of the system life cycle processes contains a set of system security activities and tasks that produce a set of security-oriented outcomes.
- These outcomes combine to deliver a system and a corresponding body of evidence that serves as the basis to substantiate the security and the trustworthiness of the system.
- Each life cycle process description has the following format:
- Purpose: The purpose section identifies the primary goals and objectives of the process and provides a summary of the security-focused activities conducted during the process.
- Outcomes: The outcomes section describes the security-focused outcomes achieved by the completion of the process and the data generated by the process.
- Activities and Tasks: The activities and tasks section provides a description of the security oriented work performed during the process including the security-focused enhancements to the activities and tasks.

PROCESS NAMES AND DESIGNATORS

- The following naming convention is established for the system life cycle processes. Each process is identified by a two-character designation (e.g., BA is the official designation for the Business or Mission Analysis process). The Table provides a listing of the system life cycle processes and their associated two-character designators.

ID	PROCESS	ID	PROCESS
AQ	Acquisition	MS	Measurement
AR	Architecture Definition	OP	Operation
BA	Business or Mission Analysis	PA	Project Assessment and Control
CM	Configuration Management	PL	Project Planning
DE	Design Definition	PM	Portfolio Management
DM	Decision Management	QA	Quality Assurance
DS	Disposal	QM	Quality Management
HR	Human Resource Management	RM	Risk Management
IF	Infrastructure Management	SA	System Analysis
IM	Information Management	SN	Stakeholder Needs and Requirements Definition
IN	Integration	SP	Supply
IP	Implementation	SR	System Requirements Definition
KM	Knowledge Management	TR	Transition
LM	Life Cycle Model Management	VA	Validation
MA	Maintenance	VE	Verification

SYSTEMS SECURITY ENGINEERING KEY POINTS

- Systems that possess
- resilient,
- trustworthy,
- system-level protections
- sufficient to enable achievement of mission/business objectives
- within performance parameters and risk tolerance

Analysis Classes

Static analysis examines the system without executing it and can be applied to design representations, source code, binaries, and bytecode. Tools include attack modeling, source code analyzers, obfuscated code detection, bytecode or binary disassembly, human review/inspection, origin analysis, digital signature verification, configuration checking, permission manifest analysis, development/sustainment version control, deliberate obfuscation, rebuild and compare, and formal methods.

Dynamic analysis examines the system execution, giving it specific inputs and examining results and/or outputs. Tools and techniques include network scanner, network sniffer, network vulnerability scanner, host-based vulnerability scanner, fuzz tester, framework-based fuzzer, negative testing, digital forensics, intrusion detection systems/intrusion prevention systems, automated monitored execution, forced path execution, firewall, man-in-the middle attack tool, debugger, and fault injection.

Hybrid analysis applies to the tight integration of static and dynamic analysis approaches.

Reference: SOAR

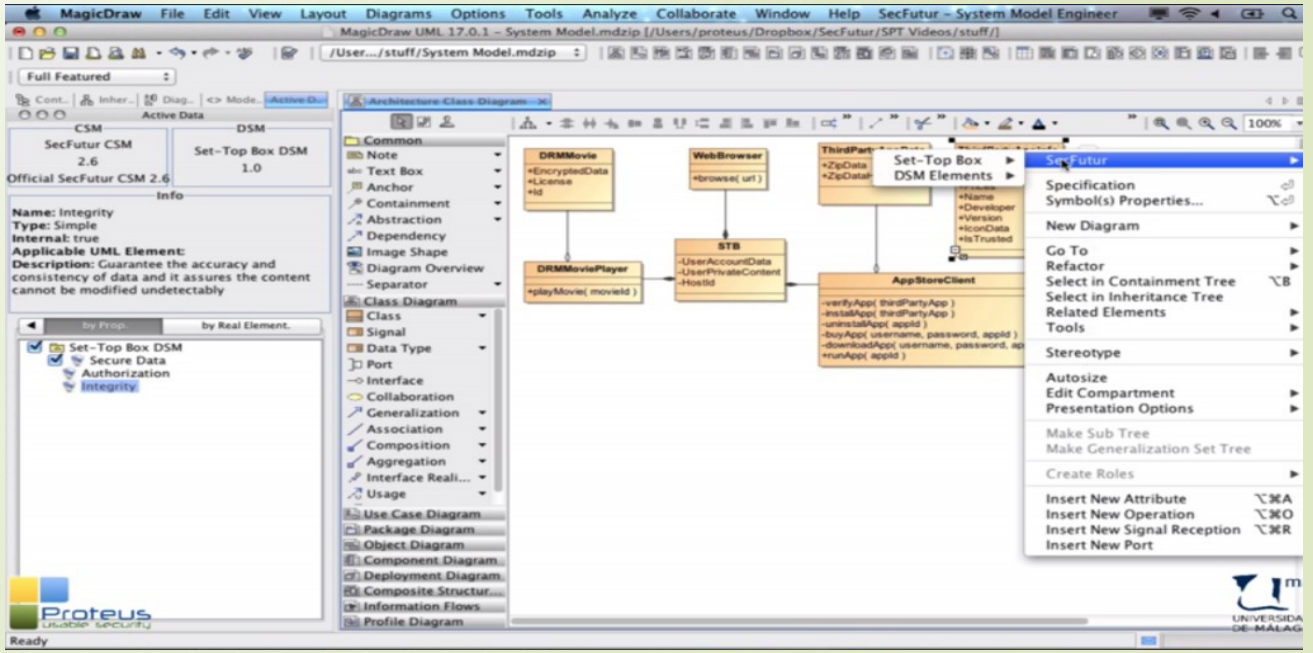
Analysis Tools

- Use a combination of tools.
- Static analysis and dynamic analysis are complementary
- Origin analysis should be used whenever third-party components are present.
- Use interactive security testing and hybrid tools if needed to get the most coverage.

Tools, Tools, Tools

System Security Engineering Assistant Tool

- System Security Engineering Assistant (S2EA) is a modelling tool that supports system engineers to adopt and deploy security mechanisms proactively by-design. S2EA follows a UML model-based paradigm and establishes a controlled and supervised modelling framework to support system engineers to create their system architectures and to integrate appropriate security mechanisms into them while ensuring design integrity.
- System Security Engineering Assistant (i85693.wixsite.com)



Tools

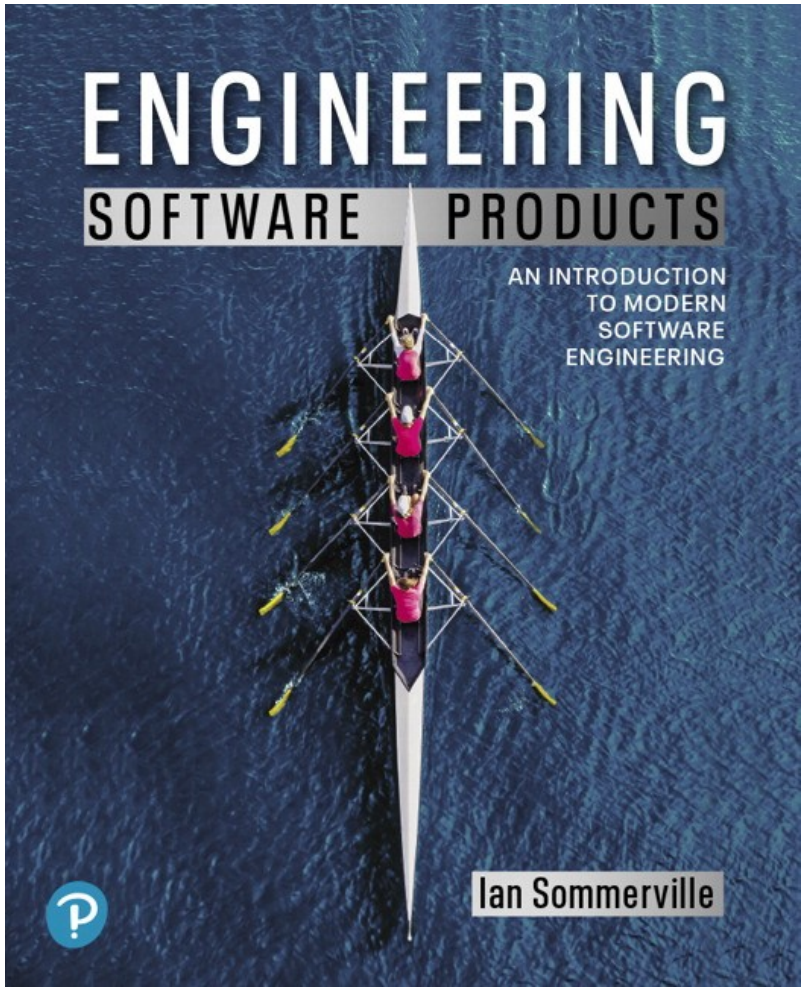
- **Top 10 Vulnerability Scanners**
- http://sectools.org/tag/vuln-scanners/
- **Top 10 Web Vulnerability Scanners**
- http://sectools.org/tag/web-scanners/
- **Top 15 Security/Hacking Tools & Utilities**
- http://www.darknet.org.uk/2006/04/top-15-securityhacking-tools-utilities/
- **Top 125 Network Security Tools**
- http://sectools.org/
- More Information about Tools, please visit my blog
- http://Msharbaf.wordpress.com

References

- [ISO/IEC 21827] International Organization for Standardization/International Electrotechnical Commission/Institute Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model, 2008
- [ISO/IEC/IEEE 15288] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE) 15288:2015, Systems and software engineering — Systems life cycle processes, May 2015.
- [ISO/IEC 15026-3] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15026-3:2015, Systems and software engineering -- Systems and software assurance -- Part 3: System integrity levels, November 2015.
- [ISO/IEC 27001] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2013, Information technology -- Security techniques -- Information security management systems -- Requirements, September 2013.
- Federal Information Security Modernization Act of 2014, (P.L. 113- 283, Title II), December 18, 2014.
- Department of Defense (DoD) Directive 8140.01, Cyberspace Workforce Management, August 2015.
- Committee on National Security Systems Instruction (CNSSI) No. 4009, Committee on National Security Systems (CNSS) Glossary, April 2015.
- System Engineering Handbook—A Guide for System Engineering Life Cycle Processes and Activities, International Council On Systems Engineering TP-2003-002-04, 4th Edition, July 2015.
- A. Madni and S. Jackson, Towards a Conceptual Framework for Resilience Engineering, IEEE Systems Journal, Vol. 3, No. 2, June 2009.
- NIST-[SP-800-160], Vol. 2, R. Ross, R. Graubart, D. Bodeau, R. McQuaid, *Systems security engineering: Cyber resiliency considerations for the engineering of trustworthy secure systems*, vol. 2, 2018.
- NIST-[SP 800-160], Vol. 1,R. Ross, R. Michael Mcevilley, Janet Carrier Oren, *Systems security engineering,* vol. 1, 2016
- NIST-[SP 800-37] National Institute of Standards and Technology Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010 (updated June 5, 2014).
- [SP 800-53A] National Institute of Standards and Technology Special Publication (SP) 800-53A Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, December 2014 (updated December 18, 2014).
- M. McEvilley, Towards a Notional Framework for Systems Security Engineering, The MITRE Corporation, NDIA 18th Annual Systems Engineering Conference, October 2015.
- R. Ross, Security Engineering: A Guide to Building Dependable Distributed Systems, Publisher: John Wiley & Sons, 2008.
- Carol C. Woody and Nancy R. Mead, Cyber Security Engineering: A Practical Approach for Systems and Software Assurance, publisher Addison-Wesley, 2017
- Stuart Jacobs, Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance, publisher IEEE Press/Wiley, 2016
- Daniel Mellado a, Carlos Blanco b, Luis E. Sánchez c, Eduardo Fernández-Medina, A systematic review of security requirements engineering, Elsevier, Computer Standards & Interfaces 32(4):153-165 · June 2010.
- Ian Alston , Simon Campbell, *Selex Galileo Ltd,* A Systems Engineering Approach For Security System Design, IEEE 2010 International Conference on Emerging Security Technologies.
- Jennier L. Bayuk, Systems Security Engineering, IEEE Security & Privacy Journal, March/April 2011, pp. 72-74, vol. 9.

Engineering Software Products

First Edition



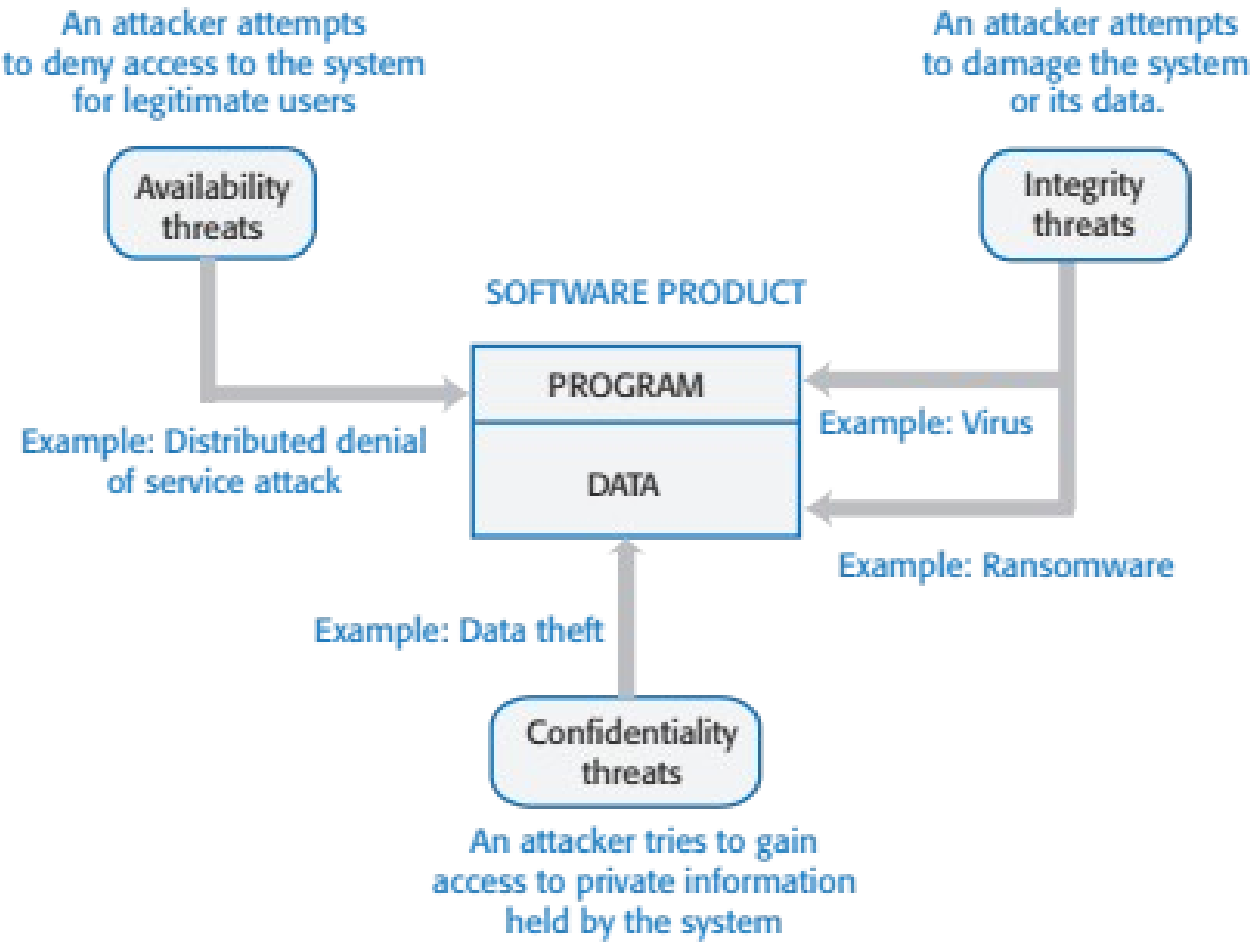
Chapter 7

Security and Privacy

Software security

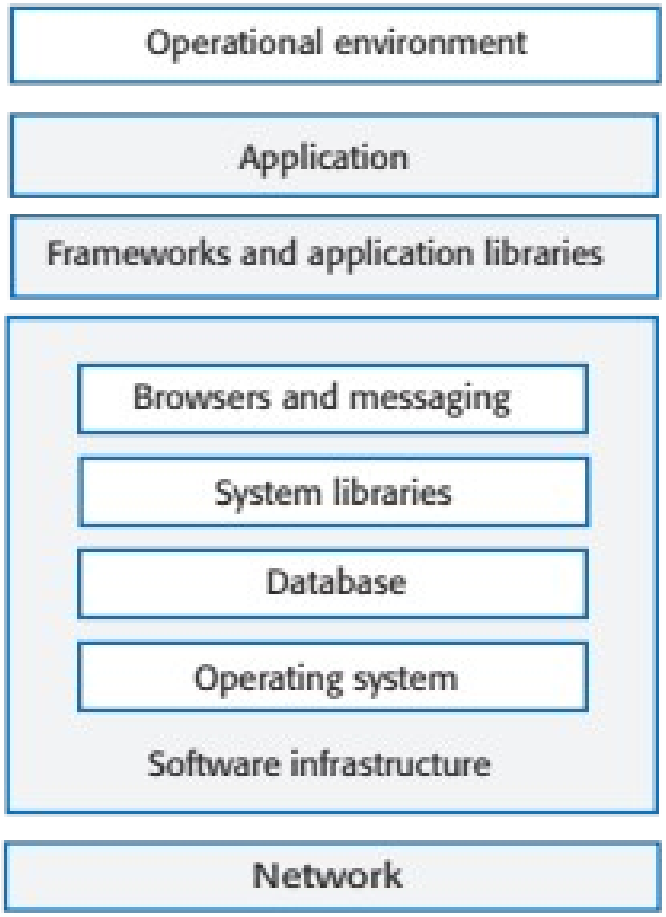
- Software security should always be a high priority for product developers and their users.
- If you don’t prioritize security, you and your customers will inevitably suffer losses from malicious attacks.
- In the worst case, these attacks could can put product providers out of business.
  - If their product is unavailable or if customer data is compromised, customers are liable to cancel their subscriptions.
- Even if they can recover from the attacks, this will take time and effort that would have been better spent working on their software.

Figure 7.1



Types of security threat

Figure 7.2



System infrastructure stack

Table 7.1 Security management

Procedure	Explanation
Authentication and authorization	You should have authentication and authorization standards and procedures that ensure that all users have strong authentication and that they have properly set up access permissions. This minimizes the risk of unauthorized users accessing system resources.
System infrastructure management	Infrastructure software should be properly configured, and security updates that patch vulnerabilities should be applied as soon as they become available.
Attack monitoring	The system should be regularly checked for possible unauthorized access. If attacks are detected, it may be possible to put resistance strategies in place that minimize the effects of the attack.
Backup	Backup policies should be implemented to ensure that you keep undamaged copies of program and data files. These can then be restored after an attack.

Operational security (1 of 2)

- Operational security focuses on helping users to maintain security. User attacks try to trick users into disclosing their credentials or accessing a website that includes malware such as a key-logging system.

Operational security (2 of 2)

- Operational security procedures and practices
  - *Auto-logout*, which addresses the common problem of users forgetting to logout from a computer used in a shared space.
  - *User command logging*, which makes it possible to discover actions taken by users that have deliberately or accidentally damaged some system resources.
  - *Multi-factor authentication*, which reduces the chances of an intruder gaining access to the system using stolen credentials.

Injection attacks

- Injection attacks are a type of attack where a malicious user uses a valid input field to input malicious code or database commands.
- These malicious instructions are then executed, causing some damage to the system. Code can be injected that leaks system data to the attackers.
- Common types of injection attack include buffer overflow attacks and SQL poisoning attacks.

SQL poisoning attacks

- SQL poisoning attacks are attacks on software products that use an SQL database.
- They take advantage of a situation where a user input is used as part of an SQL command.
- A malicious user uses a form input field to input a fragment of SQL that allows access to the database.
- The form field is added to the SQL query, which is executed and returns the information to the attacker.

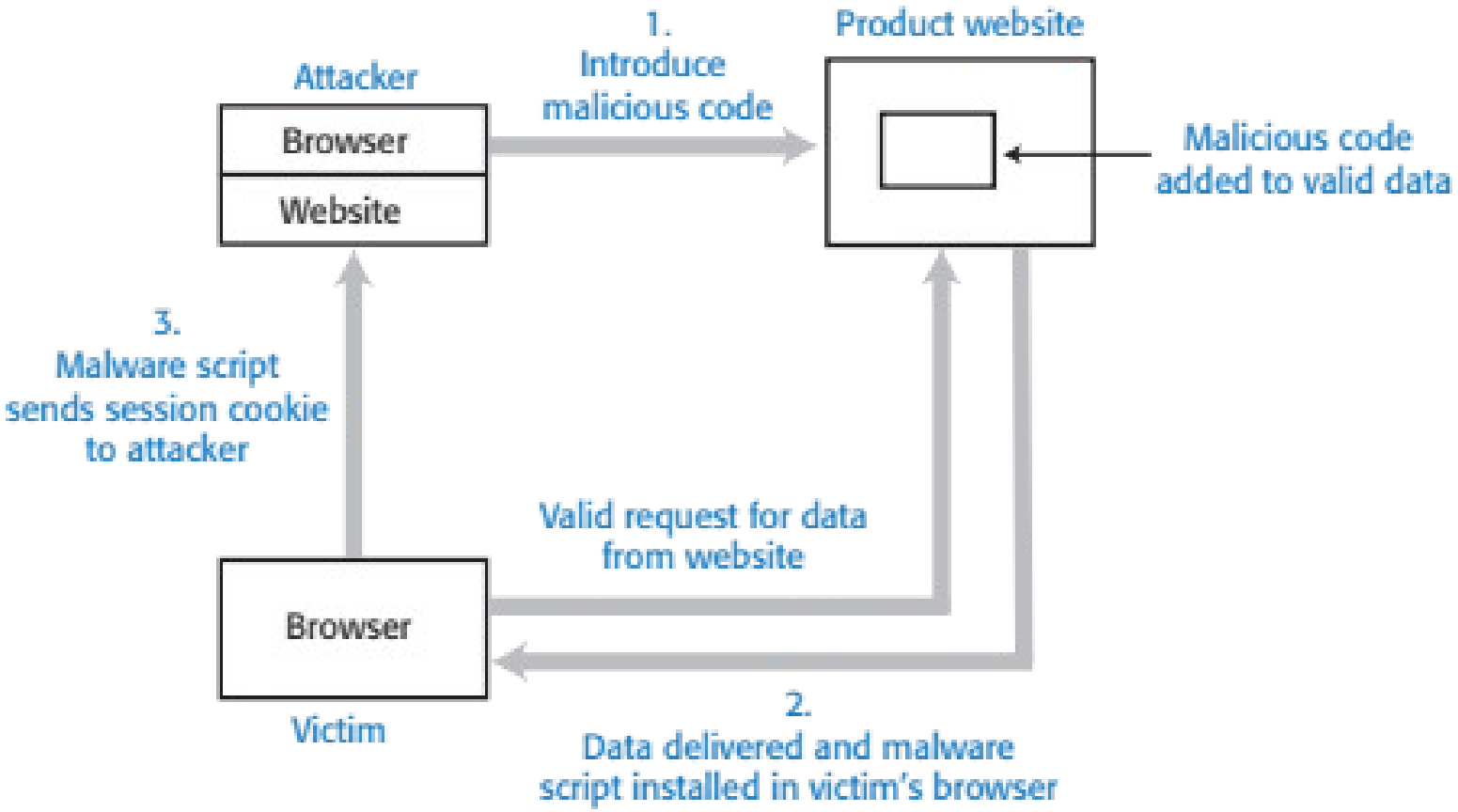
Cross-site scripting attacks (1 of 2)

- Cross-site scripting attacks are another form of injection attack.
- An attacker adds malicious JavaScript code to the web page that is returned from a server to a client and this script is executed when the page is displayed in the user's browser.

Cross-site scripting attacks (2 of 2)

- The malicious script may steal customer information or direct them to another website.
  - This may try to capture personal data or display advertisements.
  - Cookies may be stolen, which makes a session hijacking attack possible.
- As with other types of injection attack, cross-site scripting attacks may be avoided by input validation.

Figure 7.3



Cross-site scripting attack

Session hijacking attacks (1 of 2)

- When a user authenticates themselves with a web application, a session is created.
  - A session is a time period during which the user's authentication is valid. They don't have to re-authenticate for each interaction with the system.
  - The authentication process involves placing a session cookie on the user's device
- Session hijacking is a type of attack where an attacker gets hold of a session cookie and uses this to impersonate a legitimate user.

Session hijacking attacks (2 of 2)

- There are several ways that an attacker can find out the session cookie value including cross-site scripting attacks and traffic monitoring.
  - In a cross-site scripting attack, the installed malware sends session cookies to the attackers.
  - Traffic monitoring involves attackers capturing the traffic between the client and server. The session cookie can then be identified by analysing the data exchanged.

Table 7.2 Actions to reduce the likelihood of hacking

Action	Explanation
Traffic encryption	Always encrypt the network traffic between clients and your server. This means setting up sessions using https rather than http. If traffic is encrypted, it is harder to monitor to find session cookies.
Multifactor authentication	Always use multifactor authentication and require confirmation of new actions that may be damaging. For example, before a new payee request is accepted, you could ask the user to confirm their identity by inputting a code sent to their phone. You could also ask for password characters to be input before every potentially damaging action, such as transferring funds.
Short timeouts	Use relatively short timeouts on sessions. If there has been no activity in a session for a few minutes, the session should be ended and future requests directed to an authentication page. This reduces the likelihood that an attacker can access an account if a legitimate user forgets to log off when they have finished work.

Denial of service attacks (1 of 2)

- Denial of service attacks are attacks on a software system that are intended to make that system unavailable for normal use.
- Distributed denial of service attacks (DDOS) are the most common type of denial of service attacks.
  - These involve distributed computers, that have usually been hijacked as part of a botnet, sending hundreds of thousands of requests for service to a web application. There are so many service requests that legitimate users are denied access.

Denial of service attacks (2 of 2)

- Other types of denial of service attacks target application users.
  - User lockout attacks take advantage of a common authentication policy that locks out a user after a number of failed authentication attempts. Their aim is to lock users out rather than gain access and so deny the service to these users.
  - Users often use their email address as their login name so if an attacker has access to a database of email addresses, he or she can try to login using these addresses.
- If you don't lock accounts after failed validation, then attackers can use brute-force attacks on your system. If you do, you may deny access to legitimate users.

Brute force attacks (1 of 2)

- Brute force attacks are attacks on a web application where the attacker has some information, such as a valid login name, but does not have the password for the site.
- The attacker creates different passwords and tries to login with each of these. If the login fails, they then try again with a different password.
  - Attackers may use a string generator that generates every possible combination of letters and numbers and use these as passwords.
  - To speed up the process of password discovery, attackers take advantage of the fact that many users choose easy-to-remember passwords. They start by trying passwords from the published lists of the most common passwords.

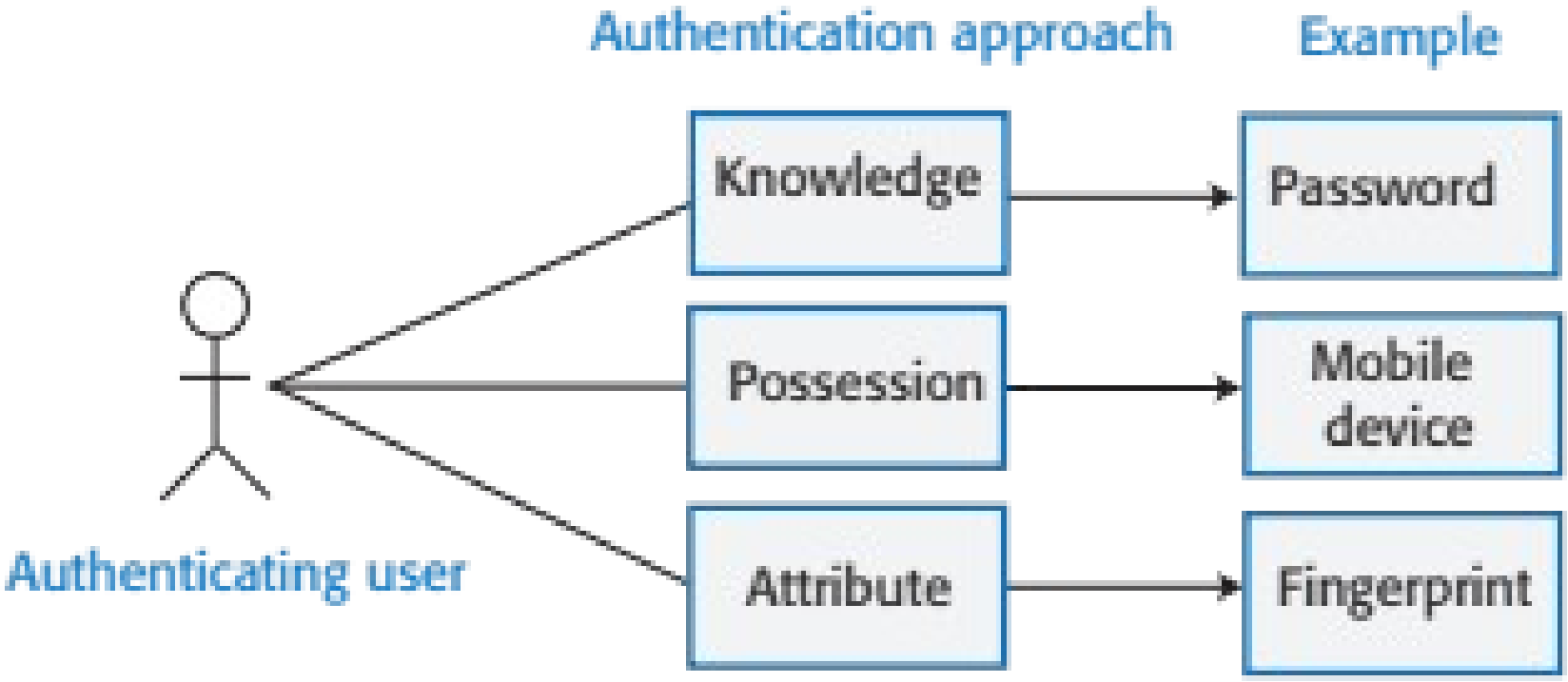
Brute force attacks (2 of 2)

- Brute force attacks rely on users setting weak passwords, so you can circumvent them by insisting that users set long passwords that are not in a dictionary or are common words.

Authentication

- Authentication is the process of ensuring that a user of your system is who they claim to be.
- You need authentication in all software products that maintain user information, so that only the providers of that information can access and change it.
- You also use authentication to learn about your users so that you can personalize their experience of using your product.

Figure 7.4



Authentication approaches

Authentication methods (1 of 2)

- Knowledge-based authentication
  - The user provides secret, personal information when they register with the system. Each time they log on, the system asks them for this information.
- Possession-based authentication
  - This relies on the user having a physical device (such as a mobile phone) that can generate or display information that is known to the authenticating system. The user inputs this information to confirm that they possess the authenticating device.

Authentication methods (2 of 2)

- Attribute-based authentication is based on a unique biometric attribute of the user, such as a fingerprint, which is registered with the system.
- Multi-factor authentication combines these approaches and requires users to use more than one authentication method.

Table 7.3 Weaknesses of password-password-based authentication

Weakness	Explanation
Insecure passwords	Users choose passwords that are easy to remember. However, it is also easy for attackers to guess or generate these passwords, using either a dictionary or a brute force attack.
Phishing attacks	Users click on an email link that points to a fake site that tries to collect their login and password details.
Password reuse	Users use the same password for several sites. If there is a security breach at one of these sites, attackers then have passwords that they can try on other sites.
Forgotten passwords	Users regularly forget their passwords, so you need to set up a password recovery mechanism to allow these to be reset. This can be a vulnerability if users' credentials have been stolen and attackers use that mechanism to reset their passwords.

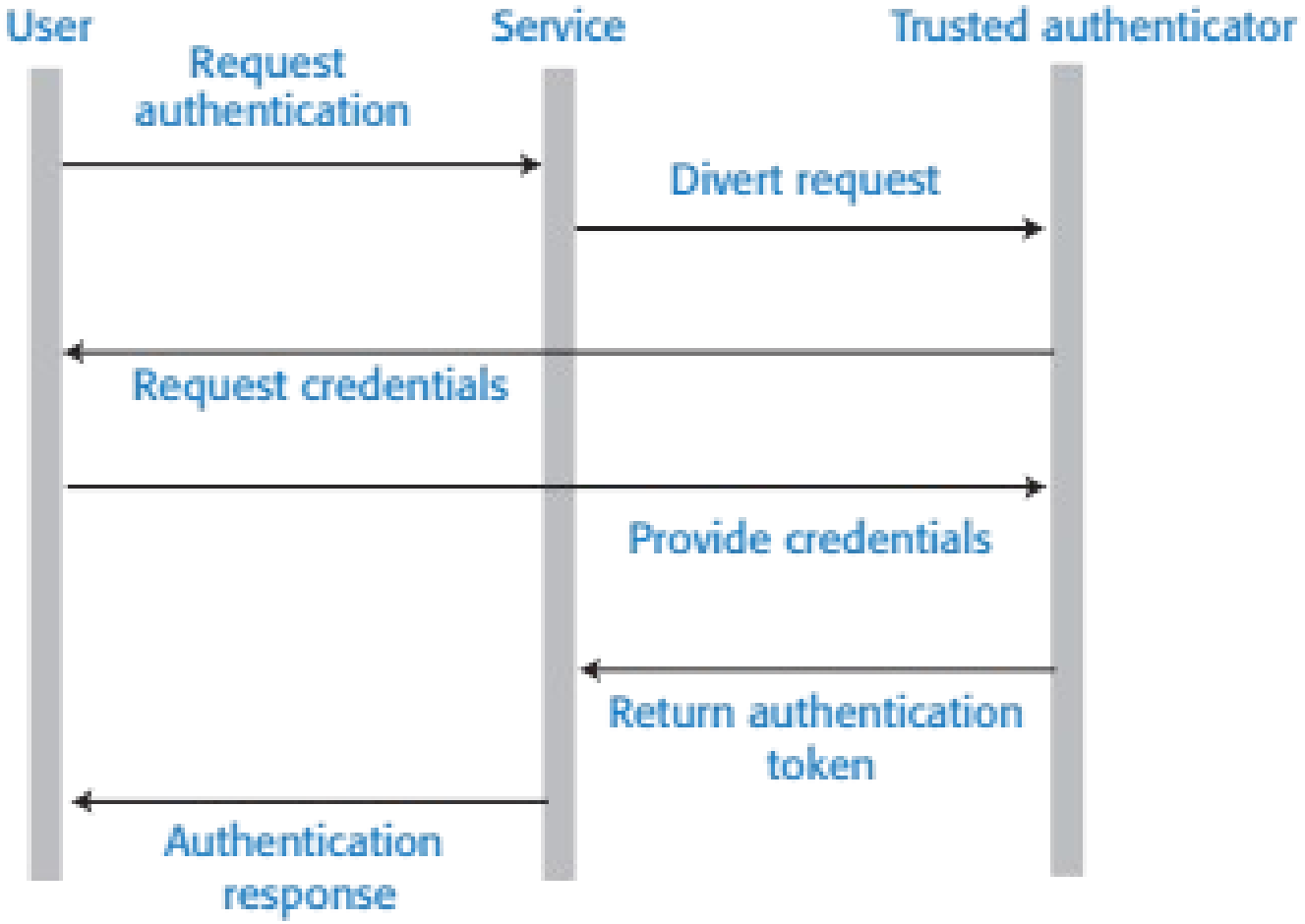
Federated identity (1 of 2)

- Federated identity is an approach to authentication where you use an external authentication service.
- ‘Login with Google’ and ‘Login with Facebook’ are widely used examples of authentication using federated identity.
- The advantage of federated identity for a user is that they have a single set of credentials that are stored by a trusted identity service.

Federated identity (2 of 2)

- Instead of logging into a service directly, a user provides their credentials to a known service who confirms their identity to the authenticating service.
- They don’t have to keep track of different user ids and passwords. Because their credentials are stored in fewer places, the chances of a security breach where these are revealed is reduced.

Figure 7.5



Federated identity

Authorization (1 of 2)

- Authentication involves a user proving their identity to a software system.
- Authorization is a complementary process in which that identity is used to control access to software system resources.
  - For example, if you use a shared folder on Dropbox, the folder's owner may authorize you to read the contents of that folder, but not to add new files or overwrite files in the folder.

Authorization (2 of 2)

- When a business wants to define the type of access that users get to resources, this is based on an access control policy.
- This policy is a set of rules that define what information (data and programs) is controlled, who has access to that information and the type of access that is allowed

Access control policies

- Explicit access control policies are important for both legal and technical reasons.
  - Data protection rules limit the access the personal data and this must be reflected in the defined access control policy. If this policy is incomplete or does not conform to the data protection rules, then there may be subsequent legal action in the event of a data breach.
  - Technically, an access control policy can be a starting point for setting up the access control scheme for a system.
  - For example, if the access control policy defines the access rights of students, then when new students are registered, they all get these rights by default.

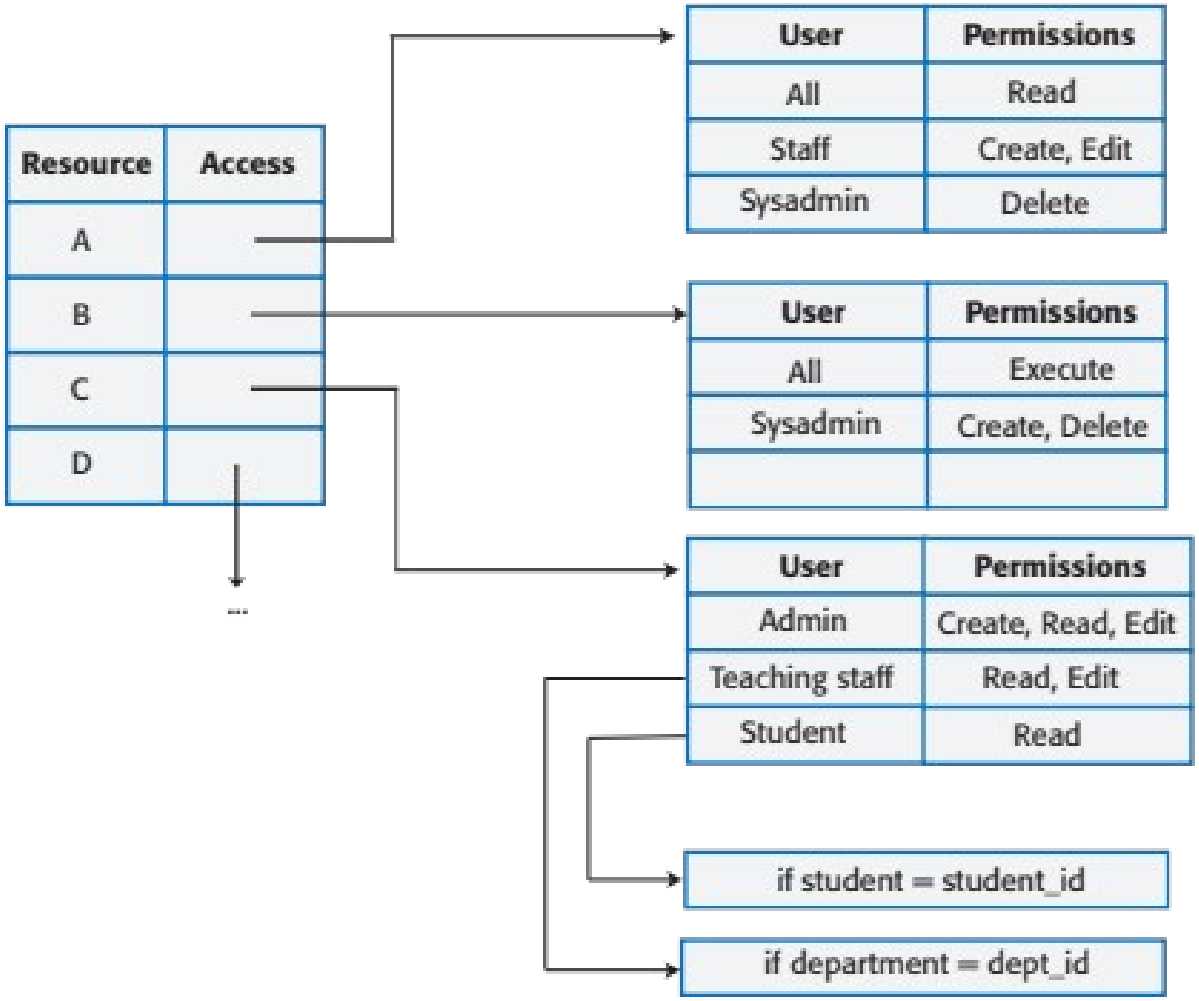
Access control lists (1 of 2)

- Access control lists (ACLs) are used in most file and database systems to implement access control policies.
- Access control lists are tables that link users with resources and specify what those users are permitted to do.
  - For example, for this book I would like to be able to set up an access control list to a book file that allows reviewers to read that file and annotate it with comments. However, they are not allowed to edit the text or to delete the file.

Access control lists (2 of 2)

- If access control lists are based on individual permissions, then these can become very large. However, you can dramatically cut their size by allocating users to groups and then assigning permissions to the group

Figure 7.8



Access control lists

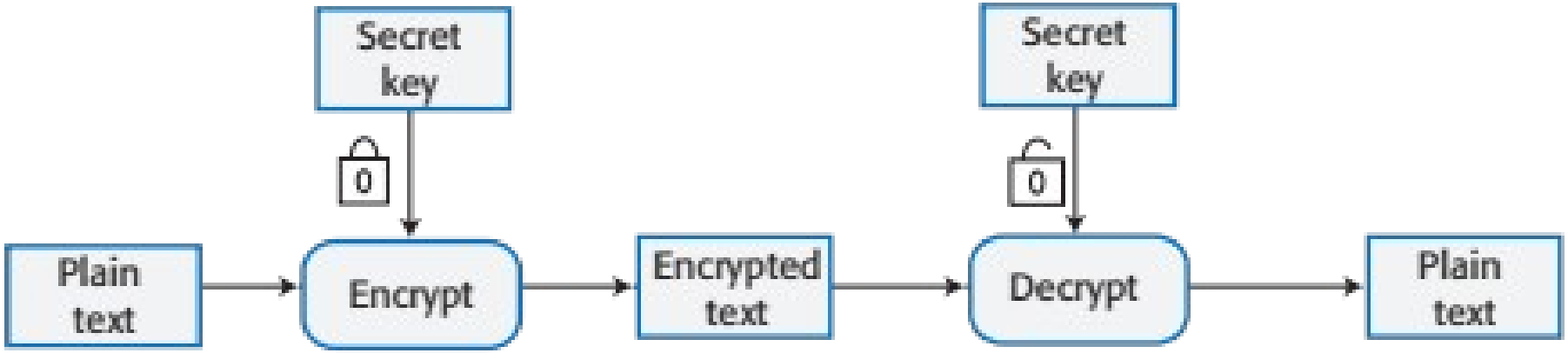
Encryption (1 of 2)

- Encryption is the process of making a document unreadable by applying an algorithmic transformation to it.
- A secret key is used by the encryption algorithm as the basis of this transformation. You can decode the encrypted text by applying the reverse transformation.
- Modern encryption techniques are such that you can encrypt data so that it is practically uncrackable using currently available technology.

Encryption (2 of 2)

- However, history has demonstrated that apparently strong encryption may be crackable when new technology becomes available.
- If commercial quantum systems become available, we will have to use a completely different approach to encryption on the Internet.

Figure 7.9

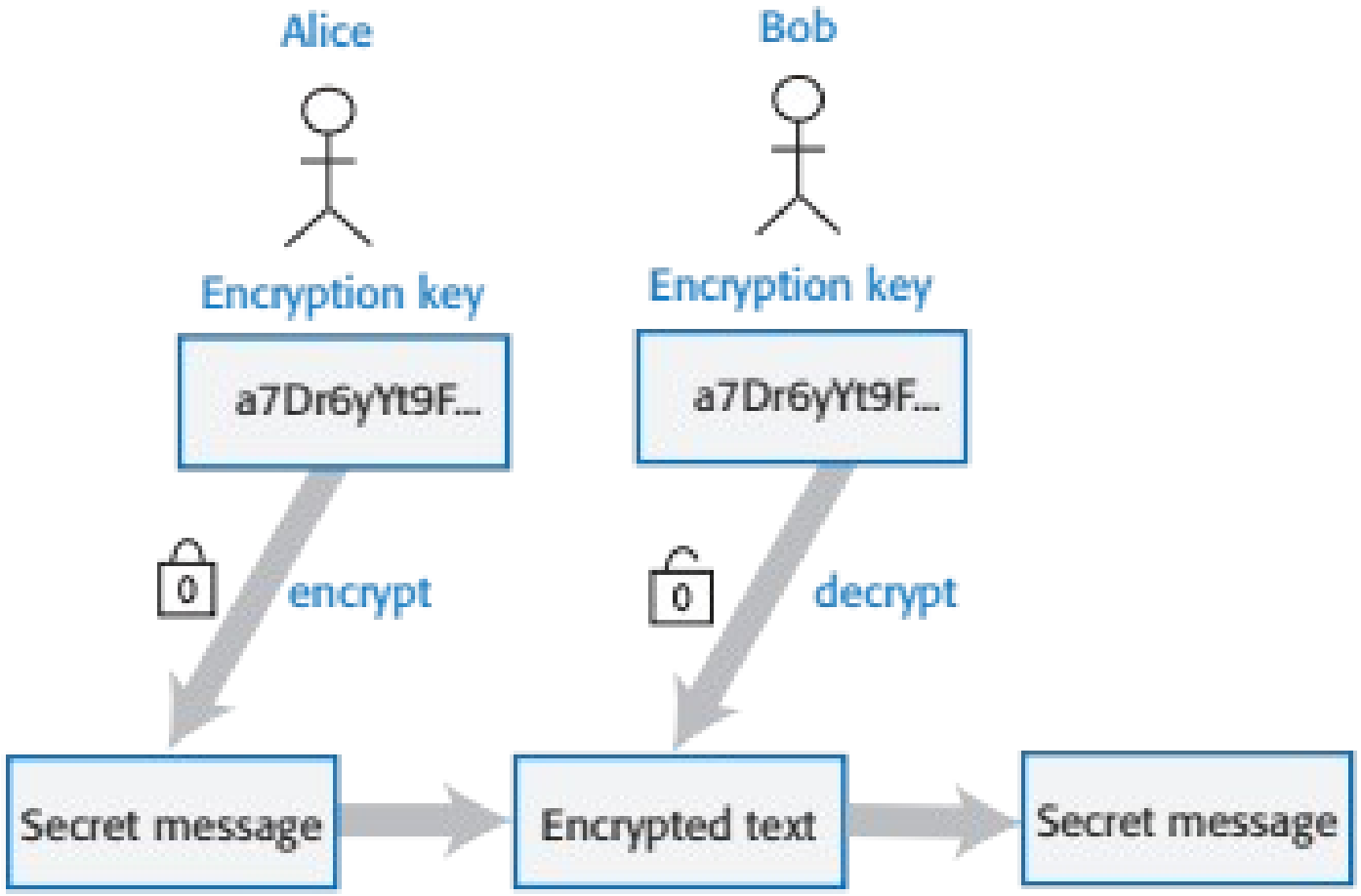


Encryption and decryption

Symmetric encryption

- In a symmetric encryption scheme, the same encryption key is used for encoding and decoding the information that is to be kept secret.
- If Alice and Bob wish to exchange a secret message, both must have a copy of the encryption key. Alice encrypts the message with this key. When Bob receives the message, he decodes it using the same key to read its contents.
- The fundamental problem with a symmetric encryption scheme is securely sharing the encryption key.
- If Alice simply sends the key to Bob, an attacker may intercept the message and gain access to the key. The attacker can then decode all future secret communications.

Figure 7.10

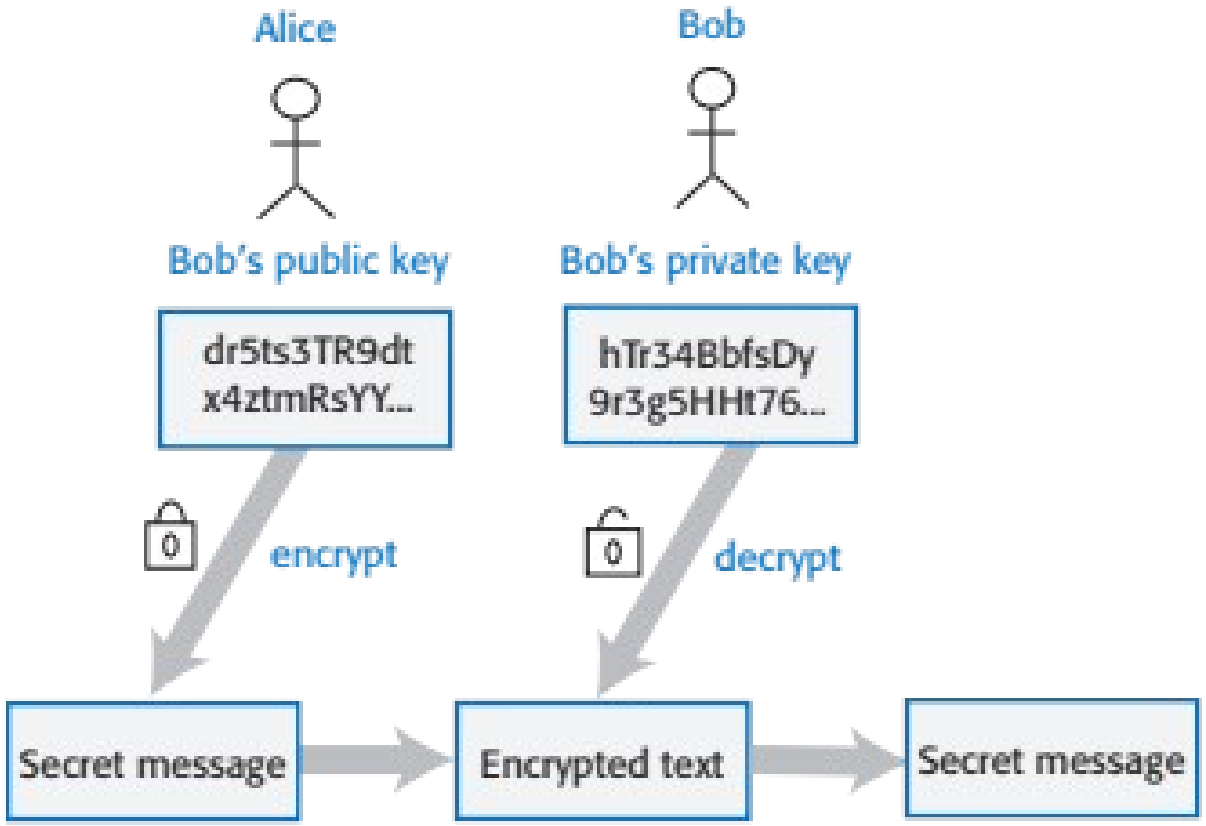


Symmetric encryption

Asymmetric encryption

- Asymmetric encryption, does not require secret keys to be shared.
- An asymmetric encryption scheme uses different keys for encrypting and decrypting messages.
- Each user has a public and a private key. Messages may be encrypted using either key but can only be decrypted using the other key.
- Public keys may be published and shared by the key owner. Anyone can access and use a published public key.
- However, messages can only be decrypted by the user's private key so is only readable by the intended recipient

Figure 7.11



Asymmetric encryption

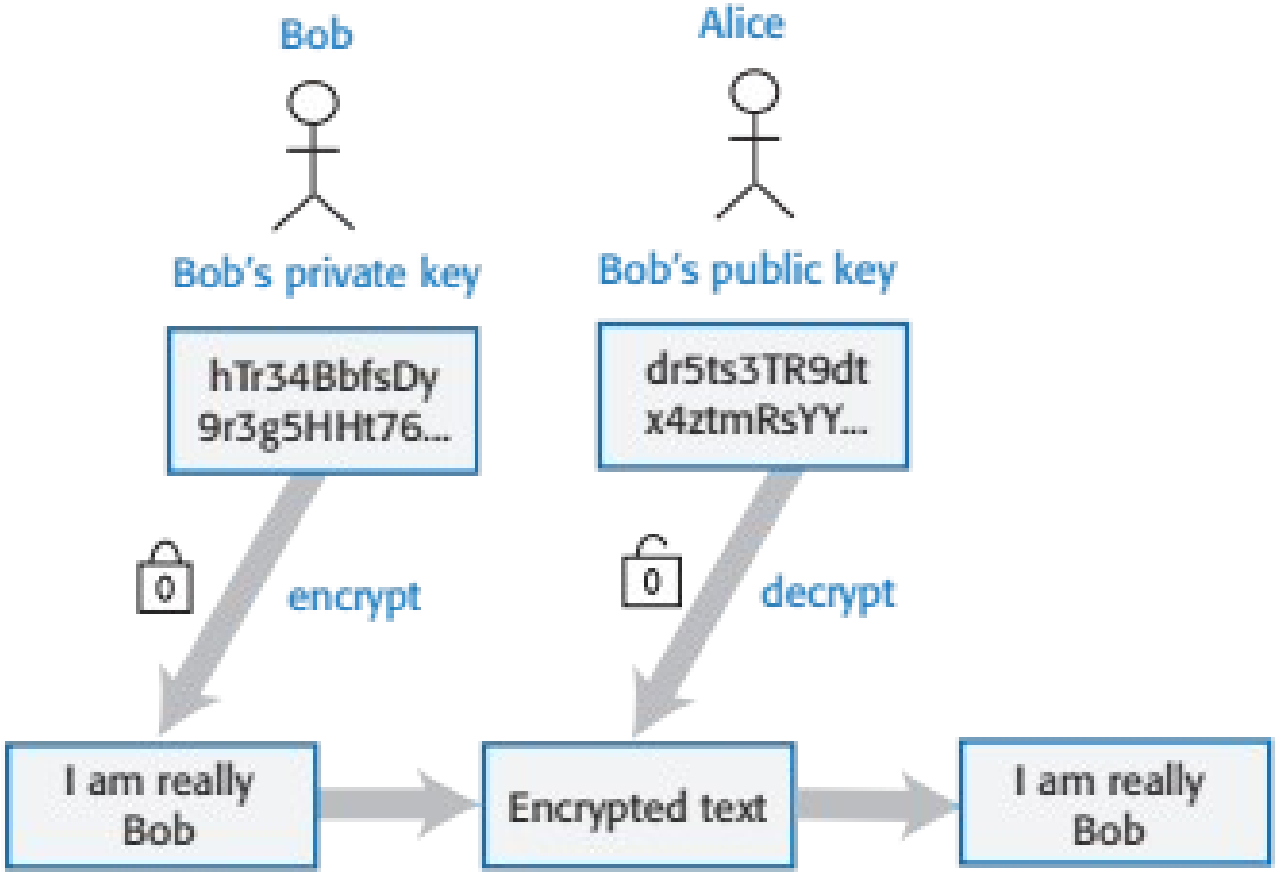
Encryption and authentication (1 of 2)

- Asymmetric encryption can also be used to authenticate the sender of a message by encrypting it with a private key and decrypting it with the corresponding public key.
- Say Alice wants to send a message to Bob and she has a copy of his public key.

Encryption and authentication (2 of 2)

- However, she is not sure whether or not the public key that she has for Bob is correct and she is concerned that the message may be sent to the wrong person.
- Private/public key encryption can be used to verify Bob's identity.
  - Bob uses his private key to encrypt a message and sends this to Alice. If it can be decrypted using Bob's public key, then Alice has the correct key.

Figure 7.12



Encryption for authentication

TLS and digital certificates (1 of 2)

- The https protocol is a standard protocol for securely exchanging texts on the web. It is the standard http protocol plus an encryption layer called TLS (Transport Layer Security). This encryption layer is used for 2 things:
  - to verify the identity of the web server;
  - to encrypt communications so that they cannot be read by an attacker who intercepts the messages between the client and the server

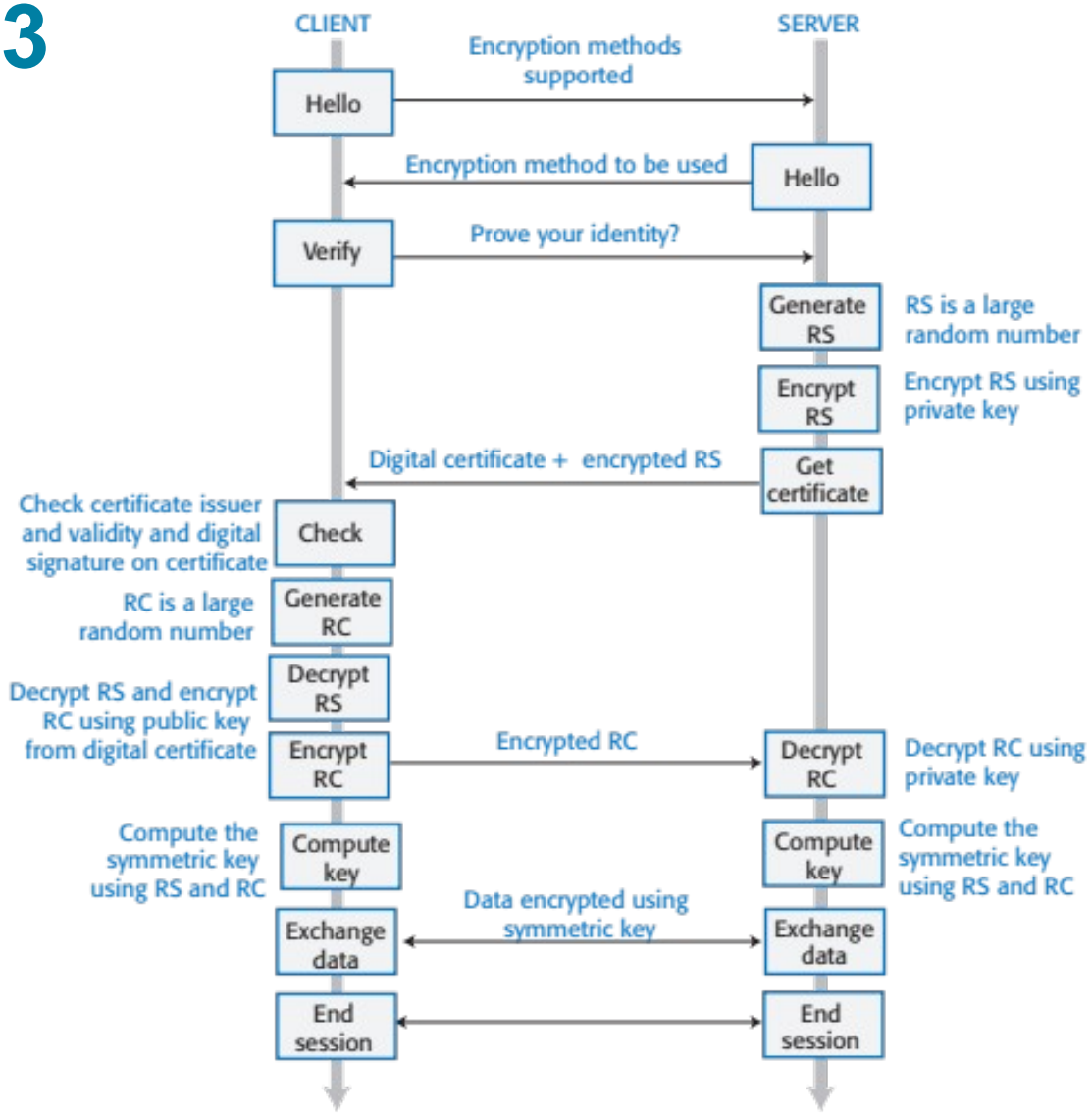
TLS and digital certificates (2 of 2)

- TLS encryption depends on a digital certificate that is sent from the web server to the client.
  - Digital certificates are issued by a certificate authority (CA), which is a trusted identity verification service.
  - The CA encrypts the information in the certificate using their private key to create a unique signature. This signature is included in the certificate along with the public key of the CA. To check that the certificate is valid, you can decrypt the signature using the CA's public key.

Table 7.5 Digital certificates

Certificate element	Explanation
Subject information	Information about the company or individual whose website is being visited. Applicants apply for a digital certificate from a certificate authority who checks that the applicant is a valid organization.
Certificate authority information	Information about the certificate authority (CA) who has issued the certificate.
Certificate information	Information about the certificate itself, including a unique serial number and a validity period, defined by start and end dates.
Digital signature	The combination of all of the above data uniquely identifies the digital certificate. The signature data are encrypted with the CA's private key to confirm that the data are correct. The algorithm used to generate the digital signature is also specified.
Public key information	The public key of the CA is included along with the key size and the encryption algorithm used. The public key may be used to decrypt the digital signature.

Figure 7.13



Using symmetric and asymmetric encryption in TLS

TLS explained (1 of 2)

- The digital certificate that the server sends to the client includes the server's public key. The server also generates a long random number, encrypts it using its private key and sends this to the client.
- The client can then decrypt this using the server's public key and, in turn, generates its own long random number. It encrypts this number using the server's public key and sends it to the server, which decrypts the message using its private key. Both client and server then have two long random numbers.

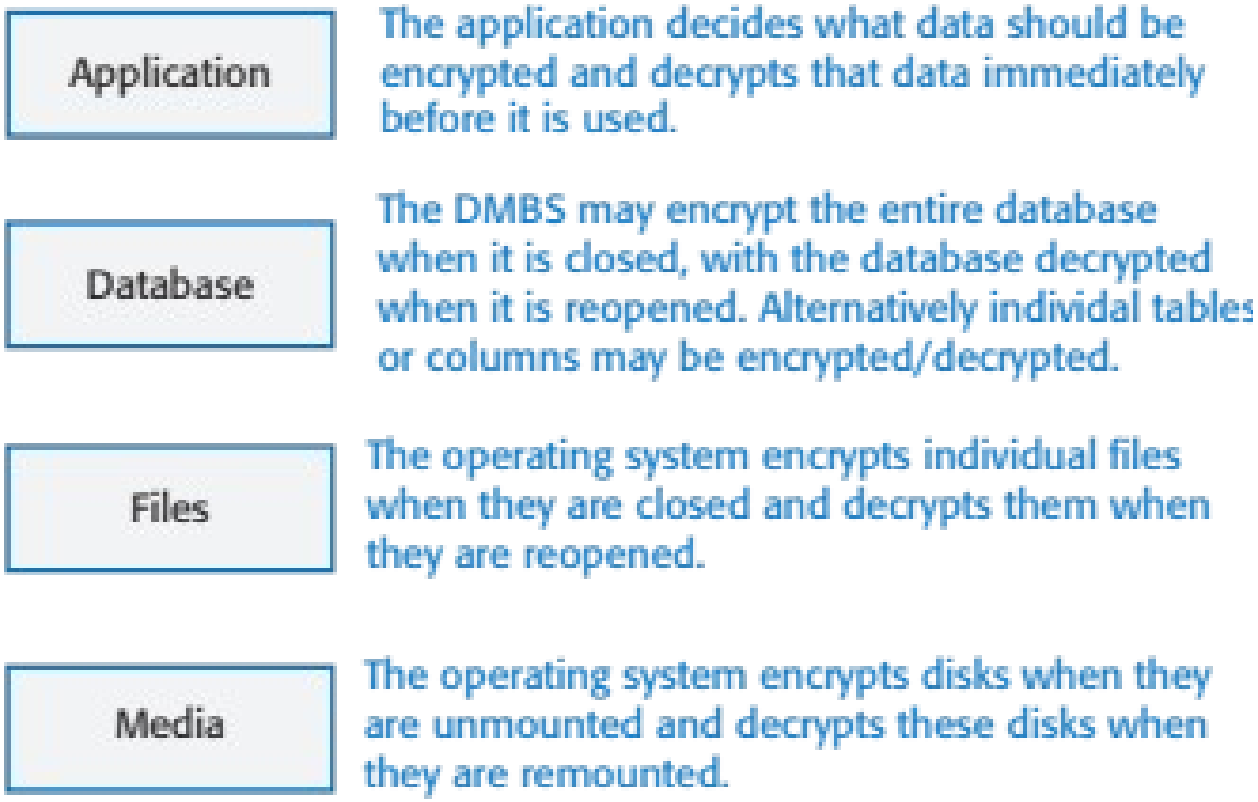
TLS explained (2 of 2)

- The agreed encryption method includes a way of generating an encryption key from these numbers. The client and server independently compute the key that will be used to encrypt subsequent messages using a symmetric approach.
- All client-server traffic is encrypted and decrypted using that computed key. There is no need to exchange the key itself.

Data encryption

- As a product provider you inevitably store information about your users and, for cloud-based products, user data.
- Encryption can be used to reduce the damage that may occur from data theft. If information is encrypted, it is impossible, or very expensive, for thieves to access and use the unencrypted data.
  - Data in transit.
    When transferring the data over the Internet, you should always use the https rather than the http protocol to ensure encryption.
  - Data at rest.
    If data is not being used, then the files where the data is stored should be encrypted so that theft of these files will not lead to disclosure of confidential information.
  - Data in use
    The data is being actively processed. Encrypting and decrypting the data slows down the system response time. Implementing a general search mechanism with encrypted data is impossible,

Figure 7.14



Encryption levels

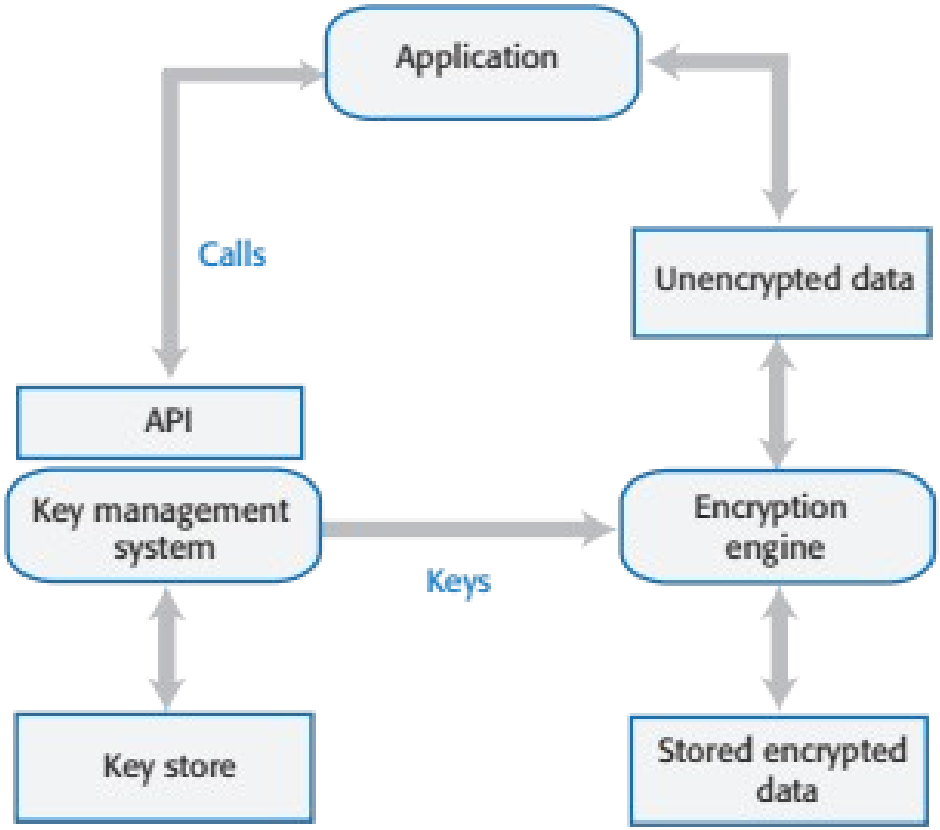
Key management (1 of 2)

- Key management is the process of ensuring that encryption keys are securely generated, stored and accessed by authorized users.
- Businesses may have to manage tens of thousands of encryption keys so it is impractical to do key management manually and you need to use some kind of automated key management system (KMS).

Key management (2 of 2)

- Key management is important because, if you get it wrong, unauthorized users may be able to access your keys and so decrypt supposedly private data. Even worse, if you lose encryption keys, then your encrypted data may be permanently inaccessible.
- A key management system (KMS) is a specialized database that is designed to securely store and manage encryption keys, digital certificates and other confidential information.

Figure 7.15



Using a KMS for encryption management

Long-term key storage (1 of 2)

- Business may be required by accounting and other regulations to keep copies of all of their data for several years.
  - For example, in the UK, tax and company data has to be maintained for at least six years, with a longer retention period for some types of data. Data protection regulations may require that this data be stored securely, so the data should be encrypted.

Long-term key storage (2 of 2)

- To reduce the risks of a security breach, encryption keys should be changed regularly. This means that archival data may be encrypted with a different key from the current data in your system.
- Therefore, key management systems must maintain multiple, timestamped versions of keys so that system backups and archives can be decrypted if required.

Privacy (1 of 2)

- Privacy is a social concept that relates to the collection, dissemination and appropriate use of personal information held by a third-party such as a company or a hospital.
- The importance of privacy has changed over time and individuals have their own views on what degree of privacy is important.

Privacy (2 of 2)

- Culture and age also affect peoples' views on what privacy means.
  - Younger people were early adopters of the first social networks and many of them seem to be less inhibited about sharing personal information on these platforms than older people.
  - In some countries, the level of income earned by an individual is seen as a private matter; in others, all tax returns are openly published.

Business reasons for privacy (1 of 2)

- If you are offering a product directly to consumers and you fail to conform to privacy regulations, then you may be subject to legal action by product buyers or by a data regulator. If your conformance is weaker than the protection offered by data protection regulations in some countries, you won't be able to sell your product in these countries.

Business reasons for privacy (2 of 2)

- If your product is a business product, business customers require privacy safeguards so that they are not put at risk of privacy violations and legal action by users.
- If personal information is leaked or misused, even if this is not seen as a violation of privacy regulations, this can lead to serious reputational damage. Customers may stop using your product because of this

Data protection laws

- In many countries, the right to individual privacy is protected by data protection laws.
- These laws limit the collection, dissemination and use of personal data to the purposes for which it was collected.
  - For example, a travel insurance company may collect health information so that they can assess their level of risk. This is legal and permissible.
  - However, it would not be legal for those companies to use this information to target online advertising of health products, unless their users had given specific permission for this.

Figure 7.16

Data protection laws

Table 7.6 Data protection principles (1 of 2)

Data protection principle	Explanation
Awareness and control	Users of your product must be made aware of what data are collected when they are using your product, and must have control over the personal information that you collect from them.
Purpose	You must tell users why data are being collected and you must not use those data for other purposes.
Consent	You must always have the consent of a user before you disclose their data to other people.
Data lifetime	You must not keep data for longer than you need to. If a user deletes an account, you must delete the personal data associated with that account.

Table 7.6 Data protection principles (2 of 2)

Data protection principle	Explanation
Secure storage	You must maintain data securely so that it cannot be tampered with or disclosed to unauthorized people.
Discovery and error correction	You must allow users to find out what personal data you store. You must provide a way for users to correct errors in their personal data.
Location	You must not store data in countries where weaker data protection laws apply unless there is an explicit agreement that the stronger data protection rules will be upheld.

Privacy policy (1 of 2)

- You should to establish a privacy policy that defines how personal and sensitive information about users is collected, stored and managed.
- Software products use data in different ways, so your privacy policy has to define the personal data that you will collect and how you will use that data.
- Product users should be able to review your privacy policy and change their preferences regarding the information that you store.

Privacy policy (2 of 2)

- Your privacy policy is a legal document and it should be auditable to check that it is consistent with the data protection laws in countries where your software is sold.
- Privacy policies should not be expressed to users in a long ‘terms and conditions’ document that, in practice, nobody reads.
- The GDPR now require software companies to include a summary of their privacy policy, written in plain language rather than legal jargon, on their website.

Key points 1 (1 of 2)

- Security is a technical concept that relates to a software system's ability to protect itself from malicious attacks that may threaten its availability, the integrity of the system and/or its data, and the theft of confidential information.
- Common types of attack on software products include injection attacks, cross-site scripting attacks, session hijacking attacks, denial of service attacks and brute force attacks.
- Authentication may be based on something a user knows, something a user has, or some physical attribute of the user.

Key points 1 (2 of 2)

- Federated authentication involves devolving responsibility for authentication to a third-party such as Facebook or Google, or to a business's authentication service.
- Authorization involves controlling access to system resources based on the user's authenticated identity. Access control lists are the most commonly-used mechanism to implement authorization.
- Symmetric encryption involves encrypting and decrypting information with the same secret key. Asymmetric encryption uses a key pair – a private key and a public key. Information encrypted using the public key can only be decrypted using the private key.

Key points 2 (1 of 2)

- A major issue in symmetric encryption is key exchange. The TLS protocol, which is used to secure web traffic, gets around this problem by using asymmetric encryption for transferring information used to generate a shared key.
- If your product stores sensitive user data, you should encrypt that data when it is not in use.
- A key management system (KMS) stores encryption keys. Using a KMS is essential because a business may have to manage thousands or even millions of keys and may have to decrypt historic data that was encrypted using an obsolete encryption key.

Key points 2 (2 of 2)

- Privacy is a social concept that relates to how people feel about the release of their personal information to others. Different countries and cultures have different ideas on what information should and should not be private.
- Data protection laws have been made in many countries to protect individual privacy. They require companies who manage user data to store it securely, to ensure that it is not used or sold without the permission of users, and to allow users to view and correct personal data held by the system.

Copyright

Developed and Presented By Dr. Mehrdad Sepehri Sharbaf
CSUDH
Computer Science Department

http://csc.csudh.edu/

The some of the materials are excerpted from Michael T. Goodrich & Roberto Tamassia's Book, and Ross Anderson's Book

ACCESS CONTROL GOAL

ACCESS CONTROL

- Access Control is one of the most popular areas of Information Security.
- It consists of many levels and mechanisms.
  - Application level.
  - Middleware.
  - Operating system.
  - Hardware controls (e.g.memory management).

These are just the basic levels.

ACCESS CONTROL

- We see the following access control mechanisms.
  - OS access controls for user authentication, isomorphic to an ACL, CL, or ACM.
  - Groups (lists of principals).
  - Roles (fixed set of permissions that principals may assume).
  - Access Control Lists.
  - Capabilities.
- There are also a lot of granularity issues.

ACCESS CONTROL

- What goes wrong with Access Control?
  - Stack smashing.
  - Race conditions and other bugs.
  - Denial of service bugs.
  - User interface failures (Trojan horse).
  - Allowing wrong programs to run as root.
  - Allowing too much privilege.
- Problems are usually caused by structural bloat where the kernel gets too big to properly manage.

TOPIC: ACCESS CONTROL

- Users and groups
- Authentication
- Passwords
- File protection
- Access control lists

- Which users can read/write which files?
- Are my files really safe?
- What does it mean to be root?
- What do we really want to control?

ACCESS CONTROL MATRICES

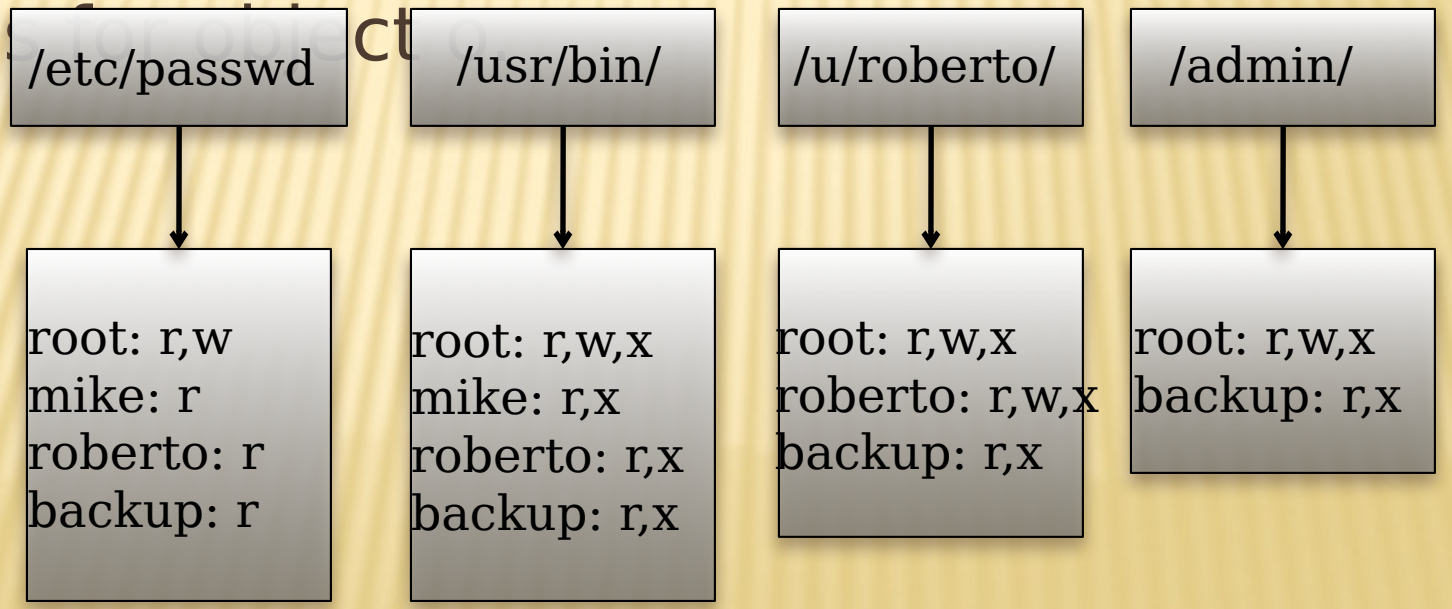
- **A table that defines permissions**.
  - Each row of this table is associated with a **subject,** which is a user, group, or system that can perform actions.
  - Each column of the table is associated with an **object,** which is a file, directory, document, device, resource, or any other entity for which we want to define access rights.
  - Each cell of the table is then filled with the access rights for the associated combination of subject and object.
  - Access rights can include actions such as reading, writing, copying, executing, deleting, and annotating.
  - An empty cell means that no access rights are granted.

EXAMPLE ACCESS CONTROL MATRIX

	/etc/passwd	/usr/bin/	/u/roberto/	/admin/
root	read, write	read, write, exec	read, write, exec	read, write, exec
mike	read	read, exec		
roberto	read	read, exec	read, write, exec	
backup	read	read, exec	read, exec	read, exec
. . .	. . .	. . .	. . .	. . .

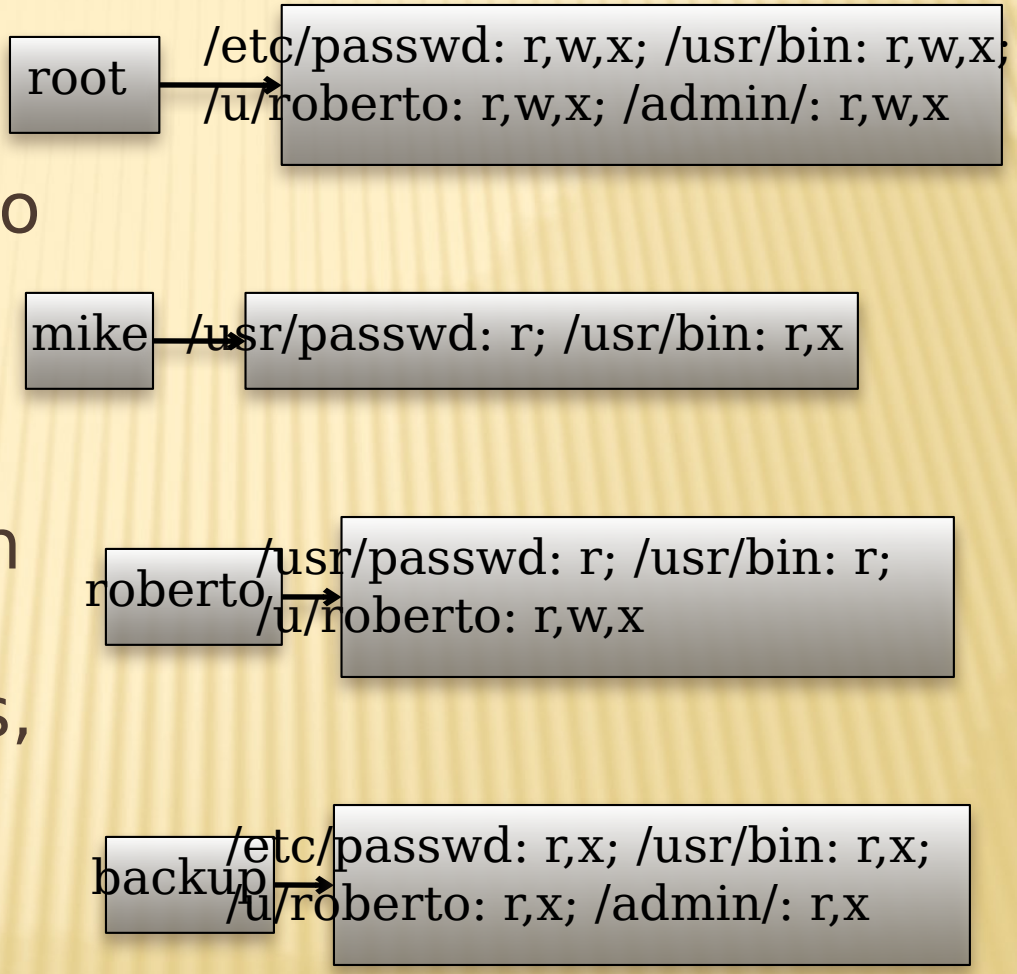
ACCESS CONTROL LISTS

- It defines, for each object, o, a list, L, called o's access control list, which enumerates all the subjects that have access rights for o and, for each such subject, s, gives the access rights that s has for object o.



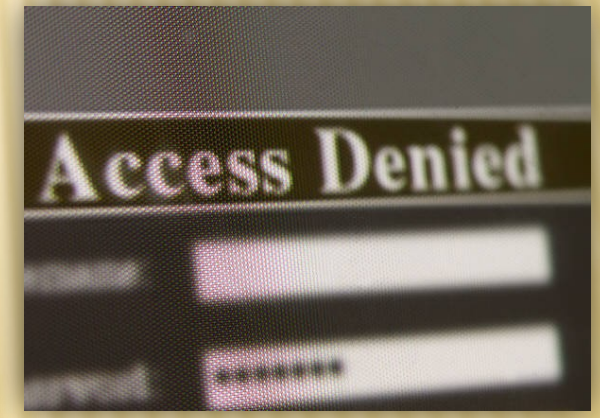
CAPABILITIES

- Takes a subject-centered approach to access control. It defines, for each subject s, the list of the objects for which s has nonempty access control rights, together with the specific rights for each such object.



ACCESS CONTROL MODELS

- Various models have been developed to formalize mechanisms to protect the confidentiality and integrity of documents stored in a computer system.
  - The Bell-La Padula (BLP) model
  - The Biba model
  - The Low-Watermark model
  - The Clark-Wilson model
  - The Chinese Wall model (The Brewer and Nash model)

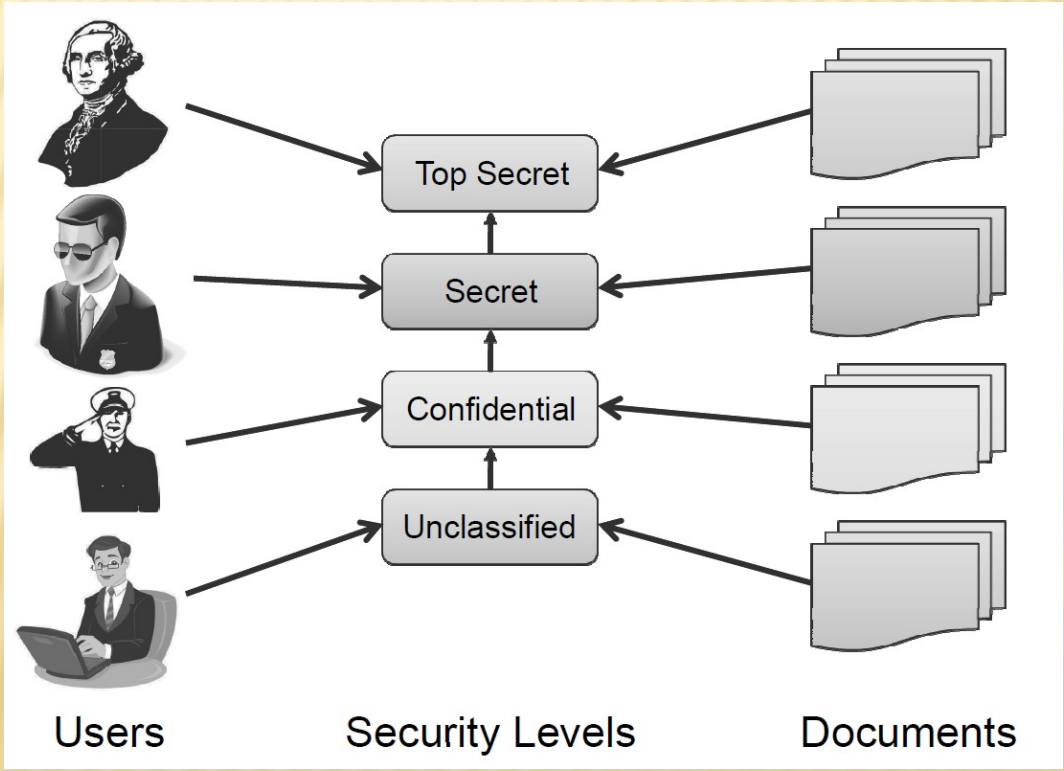


THE BELL-LA PADULA MODEL

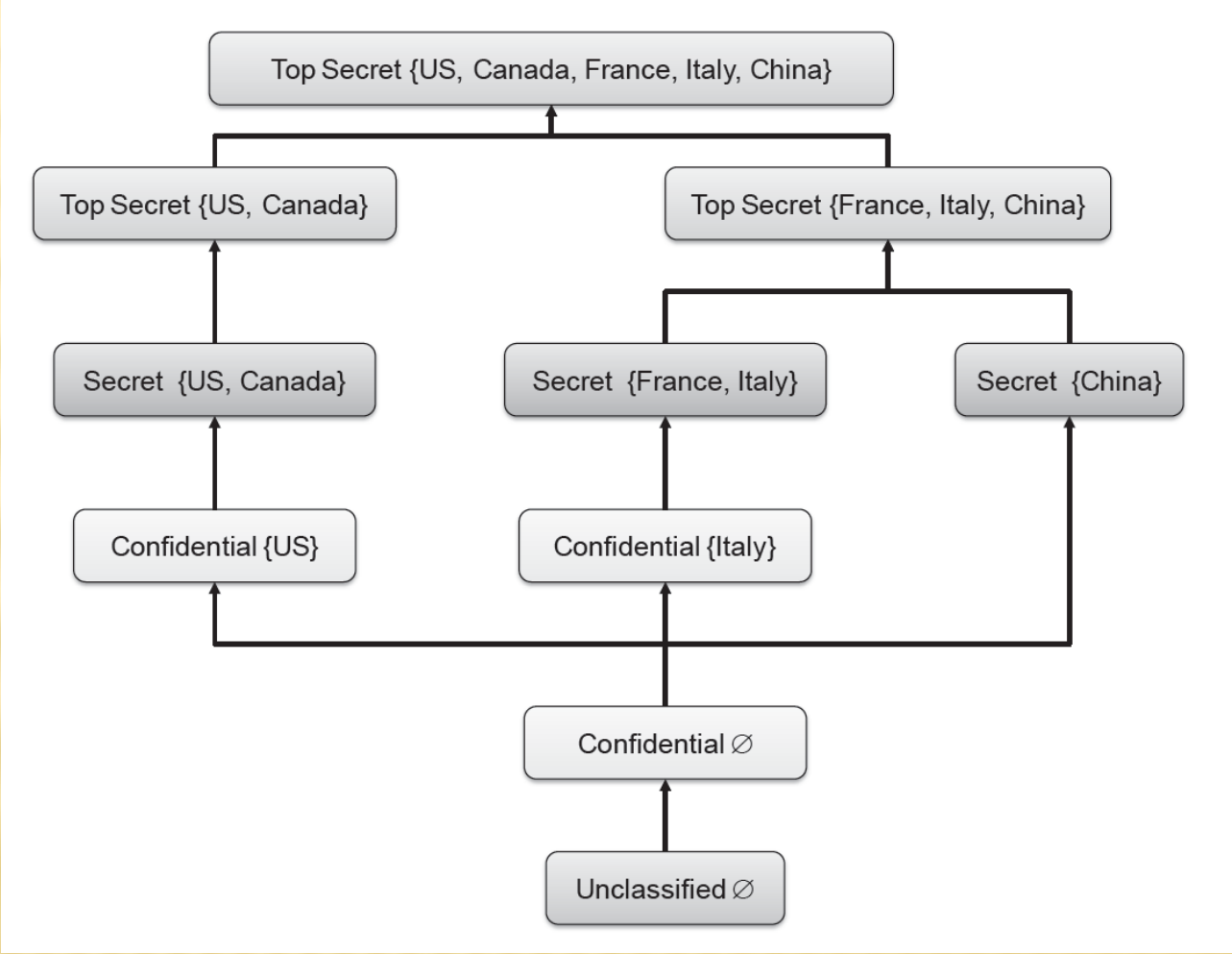
- The **Bell-La Padula (BLP) model** is a classic mandatory access-control model for protecting confidentiality.
- The BLP model is derived from the military **multilevel security paradigm,** which has been traditionally used in military organizations for document classification and personnel clearance.

THE BELL-LA PADULA MODEL

- The BLP model has a strict, linear ordering on the security of levels of documents, so that each document has a specific security level in this ordering and each user is assigned a strict level of access that allows them to view all documents with the corresponding level of security or below.



DEFINING SECURITY LEVELS USING CATEGORIES



THE BIBA MODEL

- The **Biba model** has a similar structure to the BLP model, but it addresses integrity rather than confidentiality.
- Objects and users are assigned **integrity levels** that form a partial order, similar to the BLP model.
- The integrity levels in the Biba model indicate degrees of trustworthiness, or accuracy, for objects and users, rather than levels for determining confidentiality.
  - For example, a file stored on a machine in a closely monitored data center would be assigned a higher integrity level than a file stored on a laptop.
  - In general, a data-center computer is less likely to be compromised than a random laptop computer. Likewise, when it comes to users, a senior employee with years of experience would have a higher integrity level than an intern.

THE BIBA MODEL RULES

- The access-control rules for Biba are the reverse of those for BLP. That is, Biba does not allow reading from lower levels and writing to upper levels.
- If we let I(u) denote the integrity level of a user u and I(x) denote the integrity level for an object, x, we have the following rules in the Biba model:
  - A user u can read an object x only if

    $I(u) \leq I(x)$.
  - A user u can write (create, edit or append to) an object x only if

    $I(x) \leq I(u)$.
- Thus, the Biba rules express the principle that information can only flow down, going from higher integrity levels to lower integrity levels.

THE LOW-WATERMARK MODEL

- The **low-watermark model** is an extension to the Biba model that relaxes the “no read down” restriction, but is otherwise similar to the Biba model.
- In other words, users with higher integrity levels can read objects with lower integrity levels.
- After such a reading, the user performing the reading is demoted such that his integrity level matches that of the read object.

THE CLARK-WILSON MODEL

- Rather than dealing with document confidentiality and/or integrity, the **Clark-Wilson (CW)** model deals with systems that perform transactions.
- It describes mechanisms for assuring that the integrity of such a system is preserved across the execution of a transaction. Key components of the CW model include the following:
  - **Integrity constraints** that express relationships among objects that must be satisfied for the system state to be valid. A classic example of an integrity constraint is the relationship stating that the final balance of a bank account after a withdrawal transaction must be equal to the initial balance minus the amount withdrawn.
  - **Certification methods** that verify that transactions meet given integrity constraints. Once the program for a transaction is certified, the integrity constraints do not need to be verified at each execution of the transaction.
  - **Separation of duty rules** that prevent a user that executes transaction from certifying it. In general, each transaction is assigned disjoint sets of users that can certify and execute it, respectively.

THE CHINESE WALL MODEL

- The **Brewer and Nash model,** commonly referred to as the **Chinese wall model,** is designed for use in the commercial sector to eliminate the possibility of conflicts of interest.
- To achieve this, the model groups resources into “conflict of interest classes.”
- The model enforces the restriction that each user can only access one resource from each conflict of interest class.
  - In the financial world, such a model might be used, for instance, to prevent market analysts from receiving insider information from one company and using that information to provide advice to that company’s competitor.
- Such a policy might be implemented on computer systems to regulate users’ access to sensitive or

ROLE-BASED ACCESS CONTROL

- The **role-based access control (RBAC)** model can be viewed as an evolution of the notion of group-based permissions in file systems.
- An RBAC system is defined with respect to an organization, such as company, a set of resources, such as documents, print services, and network services, and a set of users, such as employees, suppliers, and customers.

U.S. Navy image in the public domain.

RBAC COMPONENTS

- A **user** is an entity that wishes to access resources of the organization to perform a task. Usually, users are actual human users, but a user can also be a machine or application.
- A **role** is defined as a collection of users with similar functions and responsibilities in the organization. Examples of roles in a university may include “student,” “alum,” “faculty,” “dean,” “staff,” and “contractor.” In general, a user may have multiple roles.
  - Roles and their functions are often specified in the written documents of the organization.
  - The assignment of users to roles follows resolutions by the organization, such as employment actions (e.g., hiring and resignation) and academic actions (e.g., admission and graduation).
- A **permission** describes an allowed method of access to a resource**.**
  - More specifically, a permission consists of an operation performed on an object, such as “read a file” or “open a network connection.” Each role has an associated set of permissions.
- A **session** consists of the activation of a subset of the roles of a user for the purpose of performing a certain task.

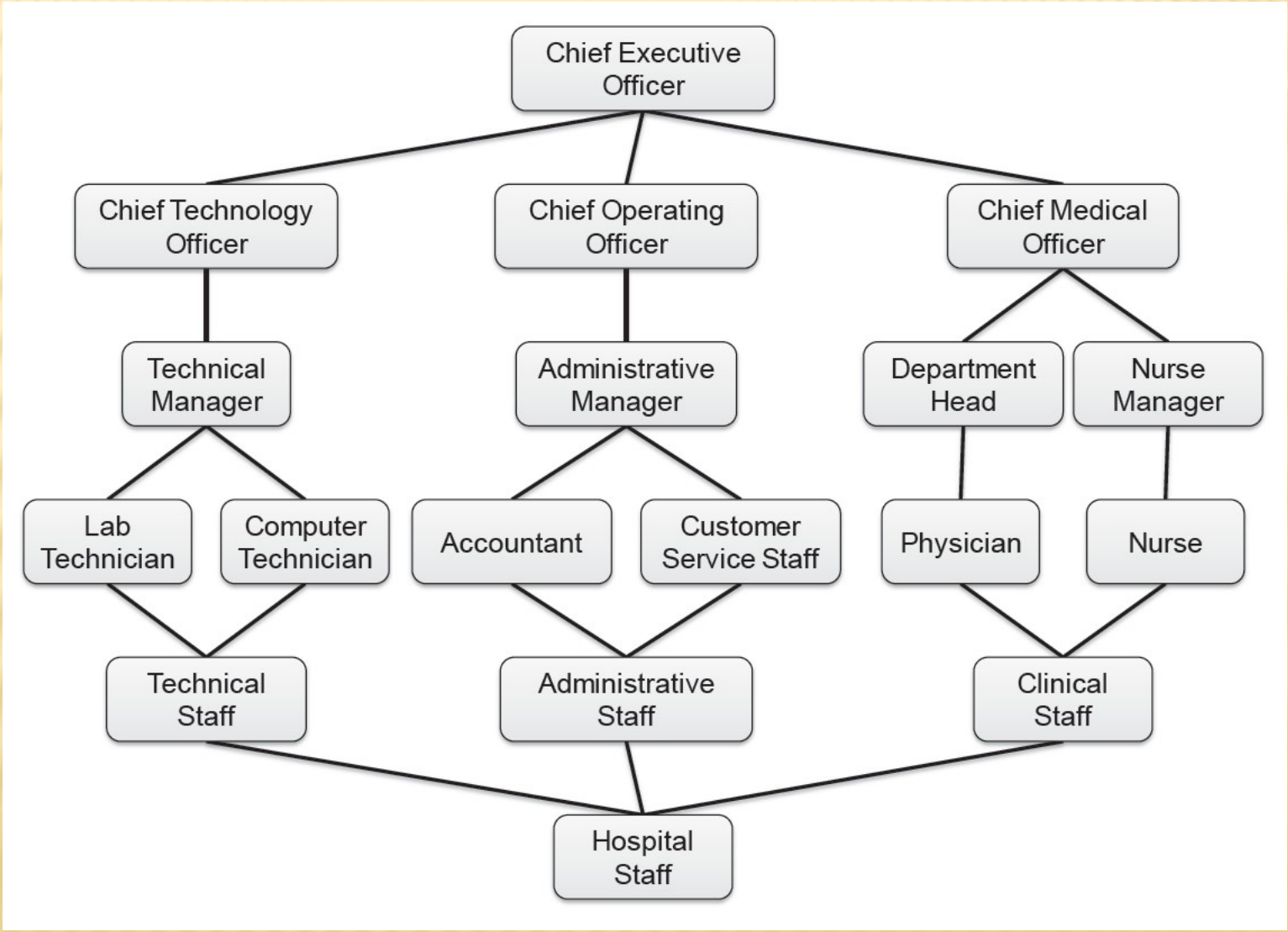
HIERARCHICAL RBAC

- In the role-based access control model, roles can be structured in a hierarchy similar to an organization chart.
- More formally, we define a partial order among roles by saying that a role R1 **inherits role R2,** which is denoted

  $R1 \geq R2$,

  if R1 includes all permissions of R2 and R2 includes all users of R1.
- When $R1 \geq R2$, we also say that role R1 is **senior** to role R2 and that role R2 is **junior** to role R1.
  - For example, in a company, the role “manager” inherits the role “employee” and the role “vice president” inherits the role “manager.”
  - Also, in a university, the roles “undergraduate student” and “graduate student” inherit the role “student.”

VISUALIZING ROLE HIERARCHY



Developed and Presented By Dr. Mehrdad Sepehri Sharbaf
CSUDH
Computer Science Department

http://csc.csudh.edu/

The some of the materials are excerpted from Firouz Forouzan's Book, and Jorge Ramió Aguirre's Book

CRYPTOGRAPHY

CRYPTOGRAPHY

Initial branch of Mathematics and currently of Computer Science and Telematics, which makes use of methods and technics with the main purpose of encrypting and/or protecting a message or file through an algorithm, using one or more keys. This gives rise to different types of cipher systems, denominated cryptosystems, that let us to assure any of these four aspects of information security: confidentiality or secret, integrity, availability and non repudiation of sender and receiver.

CRYPTOGRAPHY

Cryptography, a word with Greek origins, means "secret writing." However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.

Cryptanalysis: the art and science of decrypting messages.

Cryptology: cryptography + cryptanalysis

CRYPTOGRAPHIC STRENGTH

1. Secrecy of key
2. Difficulty of guessing the key (longer is harder)
3. Difficulty of reversing algorithm without key (breaking code)
4. Lack of back doors (decrypt without key)
5. Difficulty of using partial plaintext to find rest
6. Vulnerability of code to repeated texts

Generally, cannot prove encryption program strong, only prove weak.

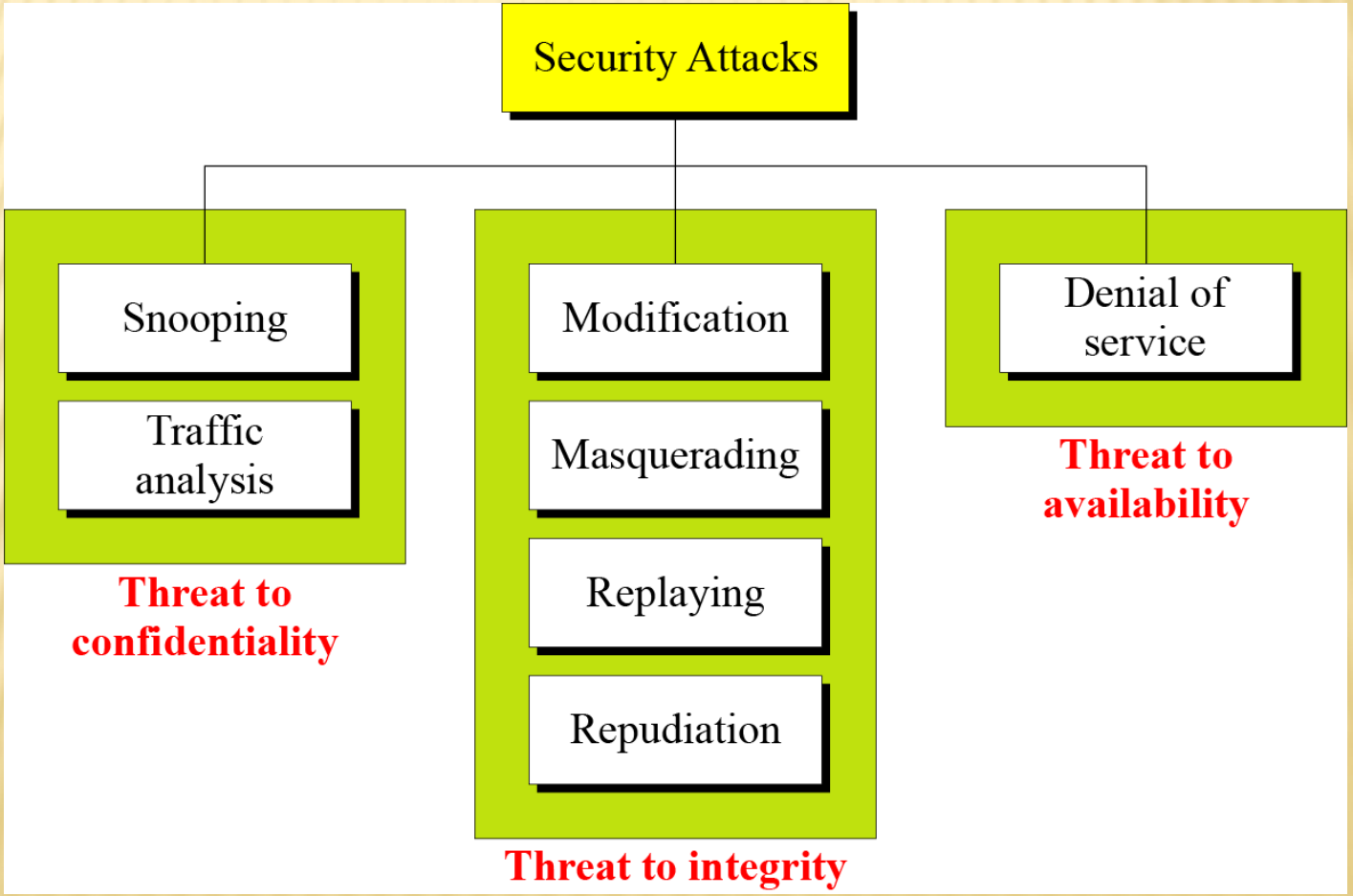
DEFINITIONS

- Plaintext: easy to understand form (original message)
- Ciphertext: difficult to understand form
- Encryption: encoding (plaintext -> ciphertext)
- Decryption: decoding (ciphertext -> plaintext)
- Cryptology: study of encryption
- Cryptography: use of encryption
- Cryptanalysis: breaking encryption

ATTACKS

The three goals of security—confidentiality, integrity, and availability—can be threatened by security attacks.

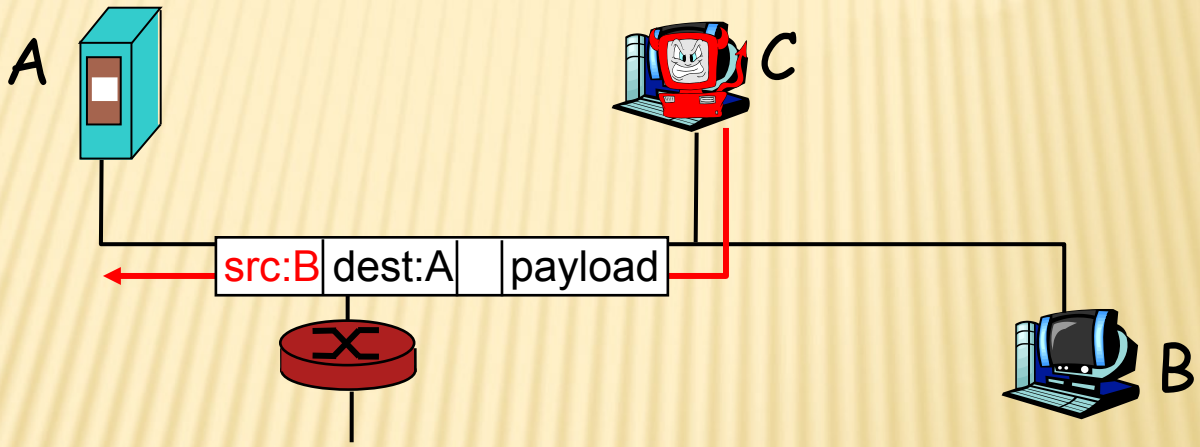
Taxonomy of attacks with relation to security goals



ATTACKS THREATENING CONFIDENTIALITY

Snooping refers to unauthorized access to or interception of data.

e.g. IP spoofing: send packet with false source address

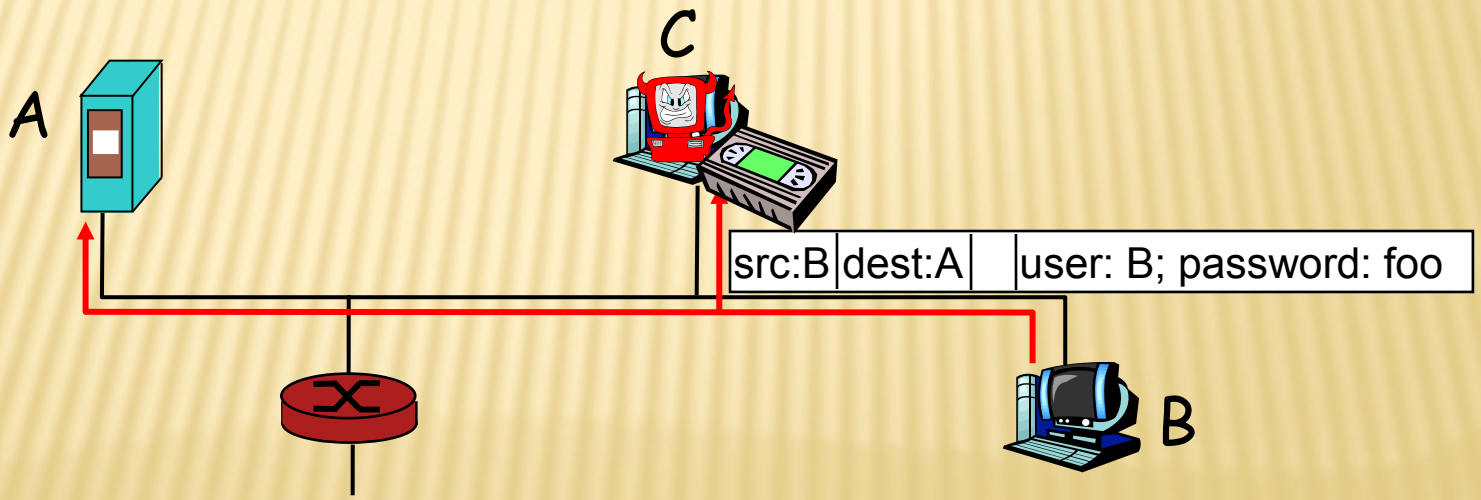


Traffic analysis refers to obtaining some other type of information by monitoring online traffic.

ATTACKS THREATENING INTEGRITY

Masquerading or spoofing happens when the attacker impersonates somebody else.

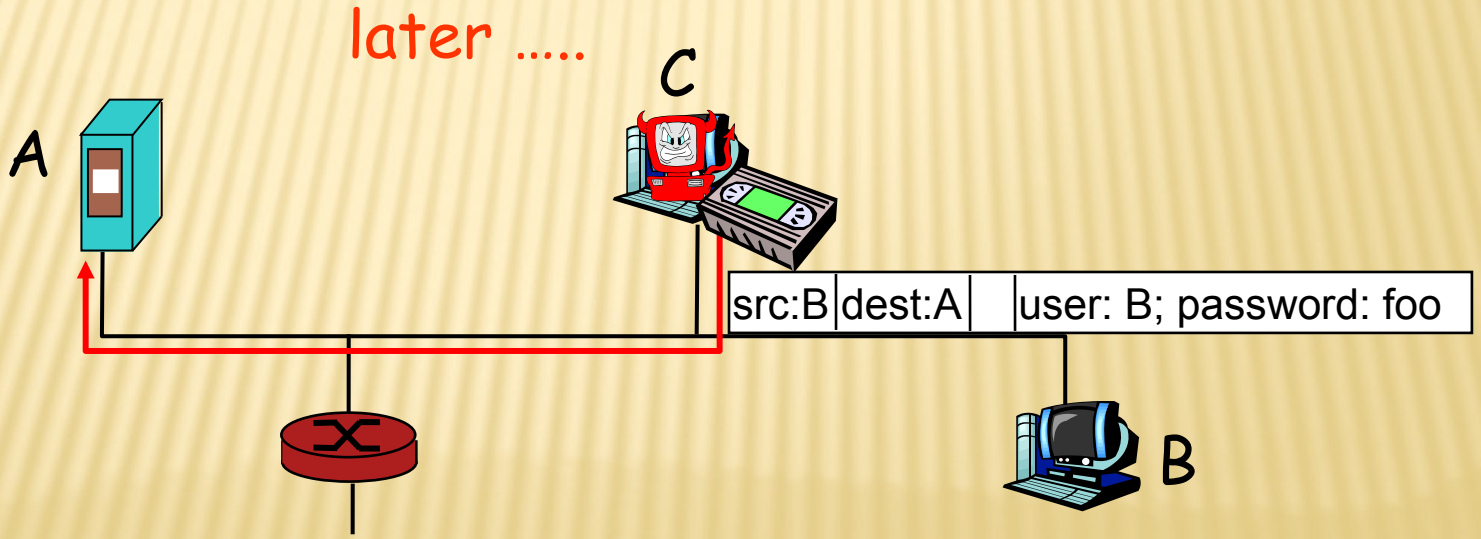
Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.



ATTACKS THREATENING INTEGRITY

Masquerading or spoofing happens when the attacker impersonates somebody else.

Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.



ATTACKS THREATENING INTEGRITY

Modification means that the attacker intercepts the message and changes it.

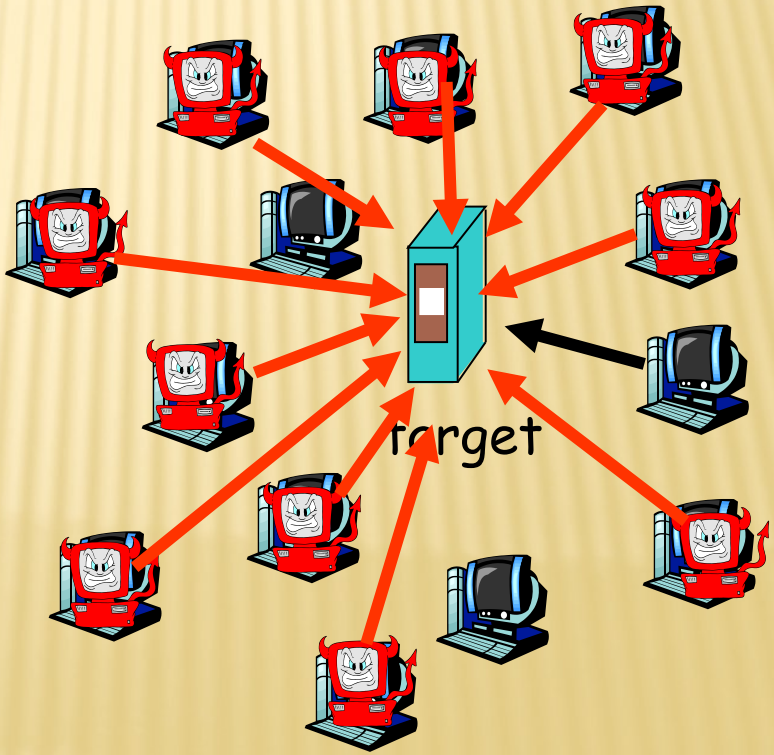
Repudiation means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

ATTACKS THREATENING AVAILABILITY

Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.

- attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

1. select target
2. break into hosts around the network
3. send packets toward target from compromised hosts



PASSIVE VERSUS ACTIVE ATTACKS

Categorization of passive and active attacks

Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

In a passive attack, the attacker's goal is just to obtain information. The attack does not modify data or harm the system, and the system continues with its normal operation.

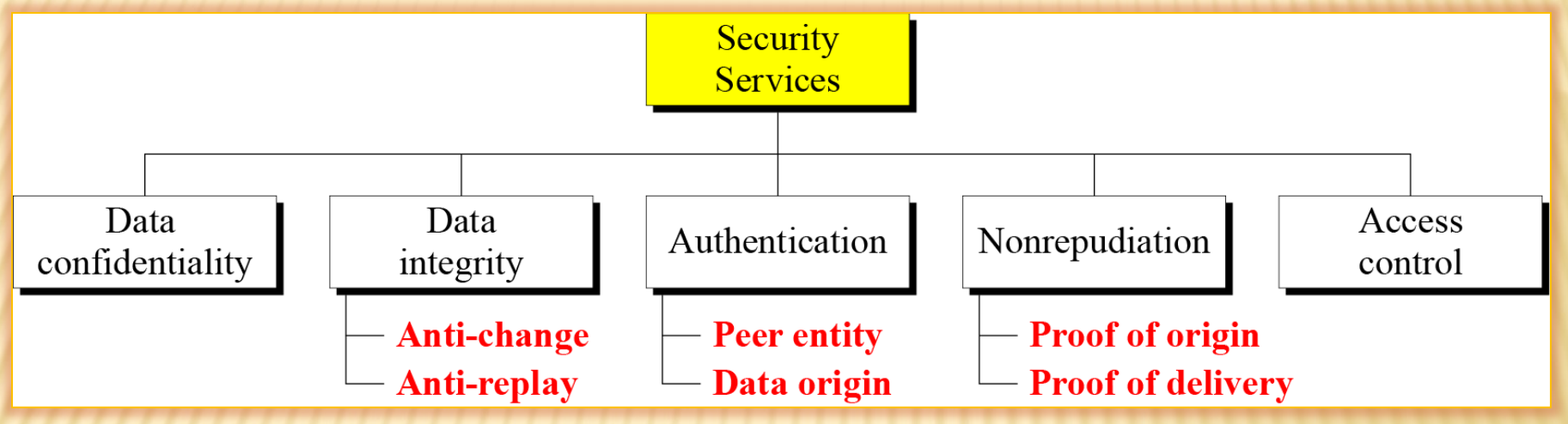
An active attack may change the data or harm the system.

SERVICES AND MECHANISMS

- The International Telecommunication Union-Telecommunication Standardization Section (ITU-T) provides some security services and some mechanisms to implement those services. Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service.

- Security Services
  Security Mechanism
  Relation between Services and Mechanisms

SECURITY SERVICES



Data confidentiality protects data from disclosure attack.

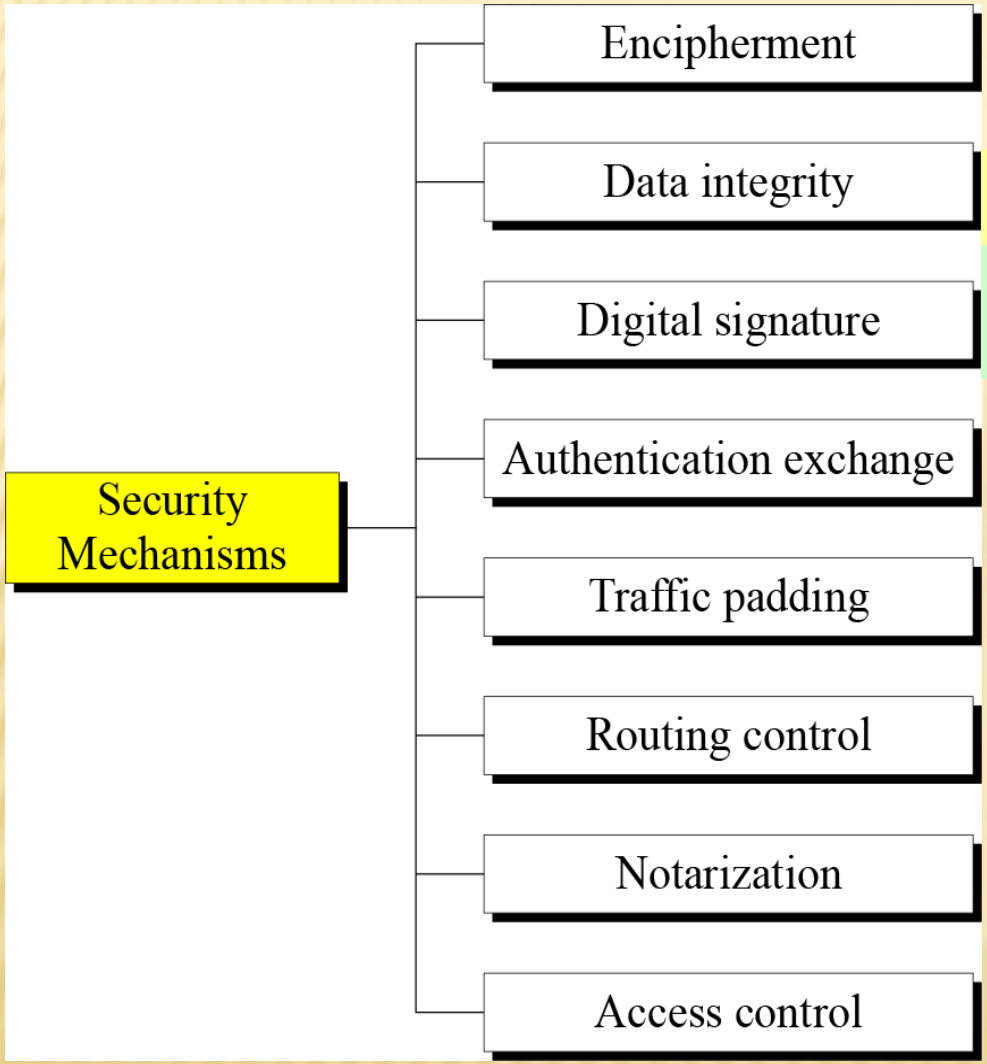
Data integrity protect data from modification, insertion, deletion, and replaying attacks.

Authentication provides proof of sender, or receiver, or source of the data.

Nonrepudiation protects against repudiation by either the sender to the reveiver.

Access control provides protection again unauthorized access to data

SECURITY MECHANISM



Hiding or covering data

Appends to data a short check value

Sender signs data, receiver verifies data

Two entities exchange msg to prove their identity to each

Insert bogus data into the data traffic to thwart traffic analysis

Continuously change routes b/w sender and receiver to prevent eavesddropping

A third trusted party controls communication

Prove and verify that a user has access right to resources

Security mechanisms

Relation between Services and Mechanisms

Relation between security services and mechanisms

Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

TECHNIQUES

Mechanisms discussed in the previous sections are only theoretical recipes to implement security. The actual implementation of security goals needs some techniques. Two techniques are prevalent today: cryptography and steganography.

Cryptography
Steganography

STEGANOGRAPHY

- Steganography is the art and science of hiding information into covert channels so as to conceal the information and prevent the detection of the hidden message.
- Today, steganography refers to hiding information in digital picture files and audio files.

STEGANOGRAPHY

- Hide a message by using the least significant bits of frames on a CD
- Kodak photo CD format's maximum resolution is 2048 by 3072 pixels, with each pixel containing 24 bits of RGB color information.
- The least significant bit of each 240bit pixel can be changed without greatly affecting the quality of the image.
- Drawbacks:
  - Overhead
  - Worthless once discovered (encryption)

STEGANOGRAPHY

- Steganography conceals the existence of the
- Steganography conceals the existence of the message
- Cryptography render the message unintelligible to outsides by various transformations of the text.
- Examples:
  - Hide a msg in an image: https://www.petitcolas.net/steganography/image_downgrading/

The image in which we want to hide another image

The image we wish to hide: ‘F15’

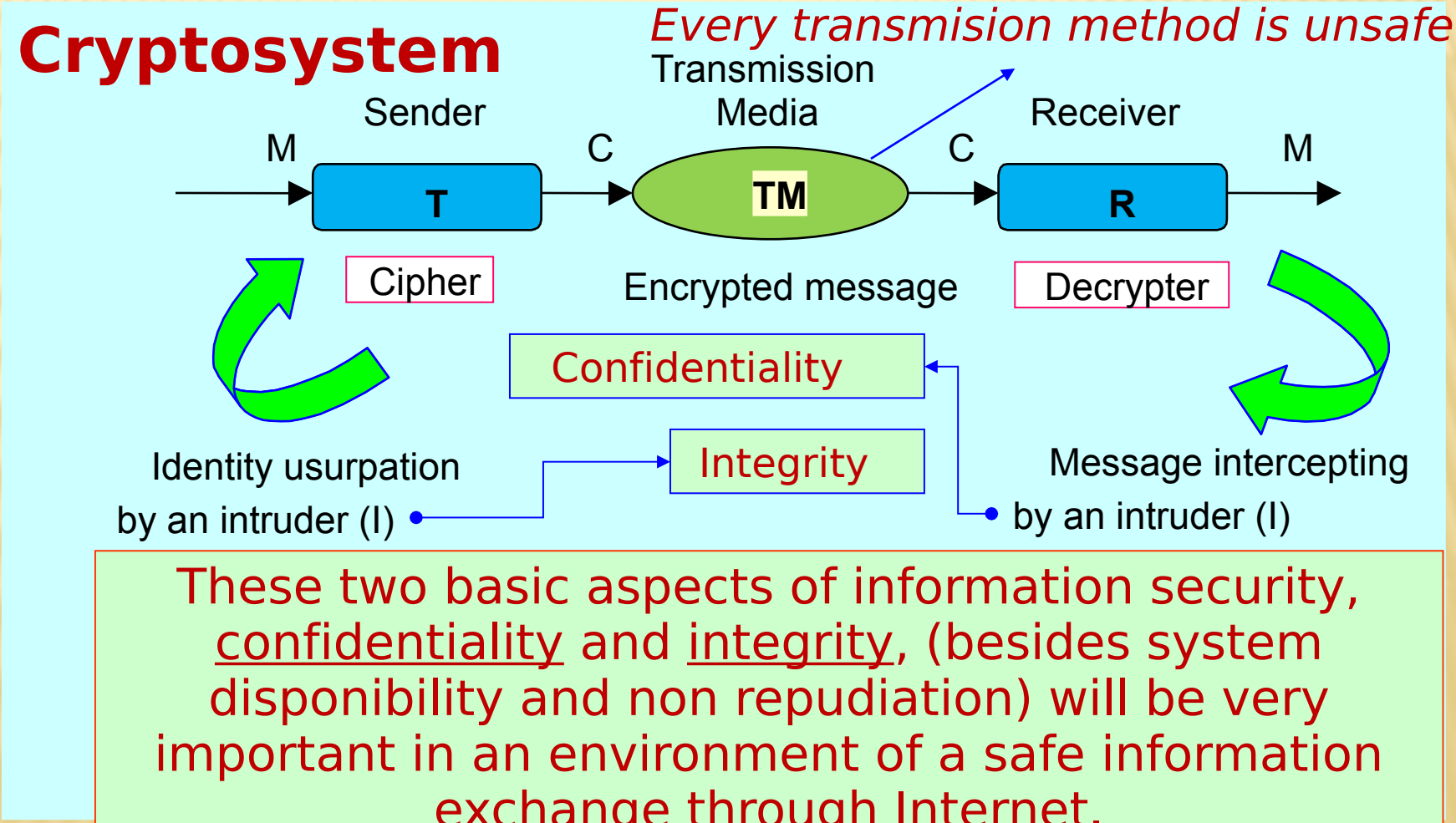
The stego-image (i.e., after the hiding process)

The image extracted from the stego-image

STEGANOGRAPHY

- Steganography is defined as "hiding information within a noise; a way to supplement (not replace) encryption, to prevent the existence of encrypted data from being detected".
- Steganography and Cryptography are cousins in the data hiding techniques.
- Cryptography is the practice of scrambling a message to an obscured form to prevent others from understanding it.
- Steganography is the study of obscuring the message so that it cannot be seen.
- More tools:
- DMOZ - Computers: Security: Products and Tools: Cryptography: Steganography (dmoz-odp.org)

CONFIDENTIALITY AND INTEGRITY



These two basic aspects of information security, confidentiality and integrity, (besides system disponibility and non repudiation) will be very important in an environment of a safe information exchange through Internet.

TYPE OF CRYPTOSYSTEMS

Classification of Cryptosystems

According to the treatment of the message they are:

Block cipher (IDEA, AES, RSA* ...) 64-128 bits

Stream cipher (A5, RC4, SEAL ...) encryption bit by bit

According the type of keys they can be:

Symmetric Systems

Asymmetric Systems

Secret key cipher

Public key cipher

(*) As we'll see in another chapter, actually systems like RSA do not encrypt by blocks: they encrypt a single number.

SYMMETRIC & ASYMMETRIC CRYPTOSYSTEMS

Symmetric Cryptosystems :

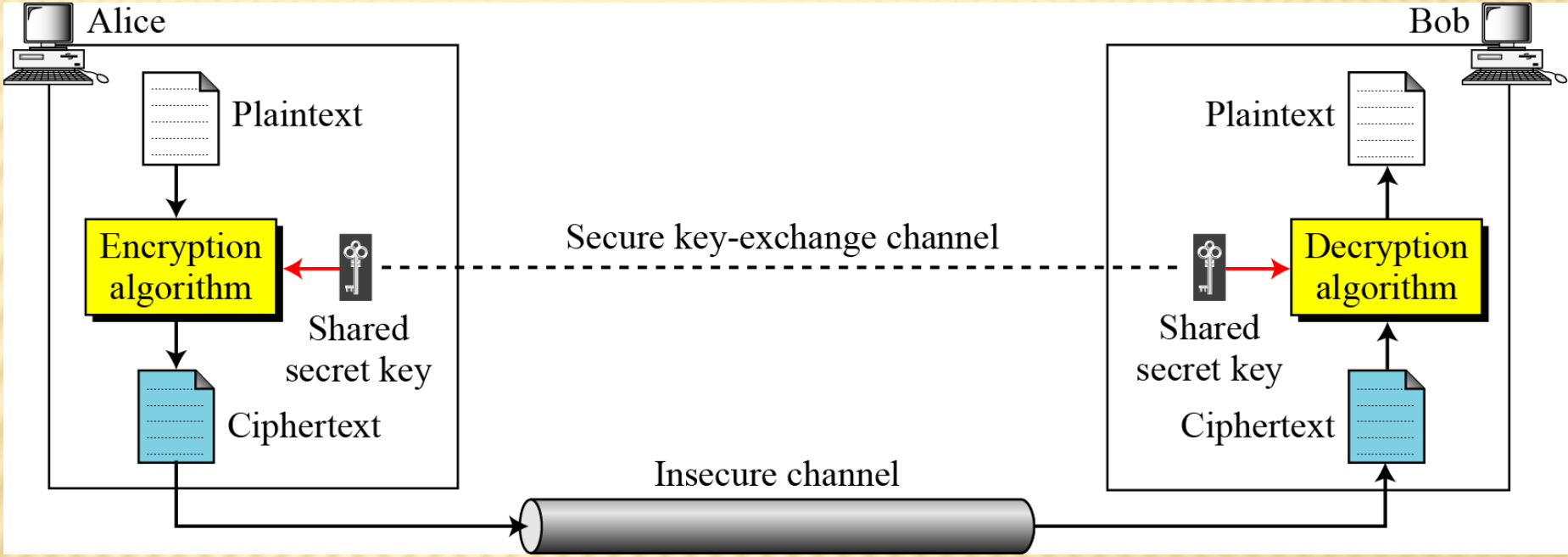
There will be a unique key (secret) that sender and receiver must share. Same key is used to encrypt and decrypt so the security just resides in maintaining the secret of the key.

Asymmetric Cryptosystems :

Every user creates a pair of keys, one private and other public, inverses of a finite field. What is encrypted in transmission with a key, is decrypted when receiving with the inverse key. The system security resides in the computing difficulty of discovering the private key through the public. For that, they use mathematical one-way functions.

Symmetric Key

General idea of symmetric-key cipher



The original message from Alice to Bob is called plaintext; the message that is sent through the channel is called the ciphertext. To create the ciphertext from the plaintext, Alice uses an encryption algorithm and a shared secret key. To create the plaintext from ciphertext, Bob uses a decryption algorithm and the same secret key.

Encryption Algorithm

If P is the plaintext, C is the ciphertext, and K is the key,

Encryption: $C = E_k(P)$ Decryption: $P = D_k(C)$

In which, $D_k(E_k(x)) = E_k(D_k(x)) = x$

We assume that Bob creates P_1; we prove that $P_1 = P$:

Alice: $C = E_k(P)$

Bob: $P_1 = D_k(C) = D_k(E_k(P)) = P$

Encryption Algorithm

Locking and unlocking with the same key

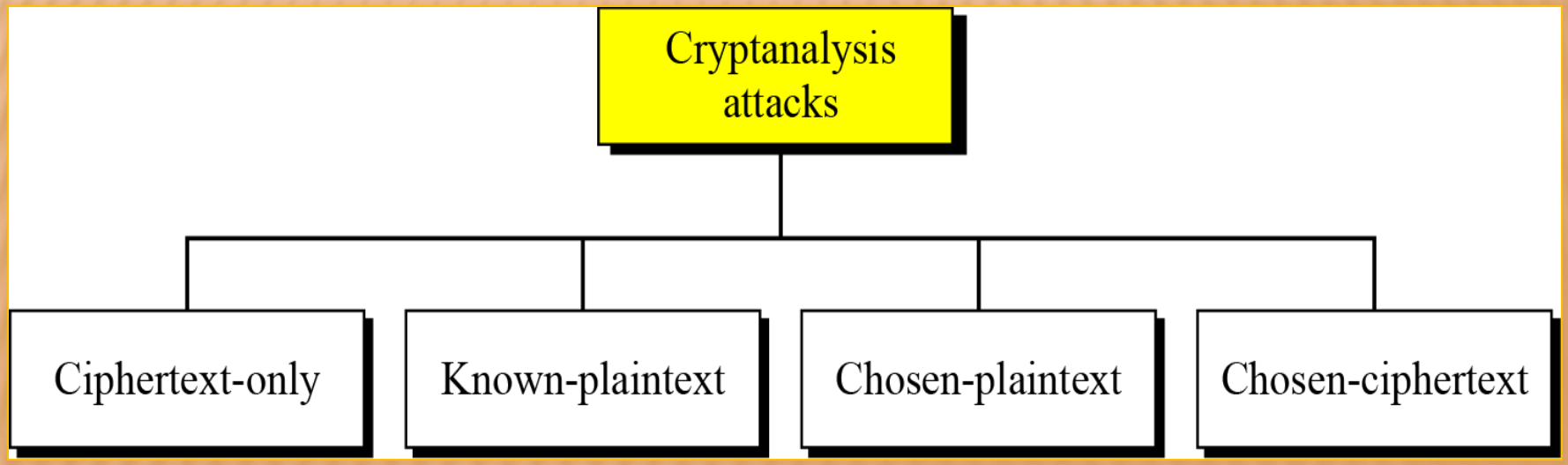
KERCKHOFF'S PRINCIPLE

- Based on Kerckhoff's principle, one should always assume that the adversary, Eve, knows the encryption/decryption algorithm. The resistance of the cipher to attack must be based only on the secrecy of the key.

CRYPTANALYSIS

- As cryptography is the science and art of creating secret codes, cryptanalysis is the science and art of breaking those codes.

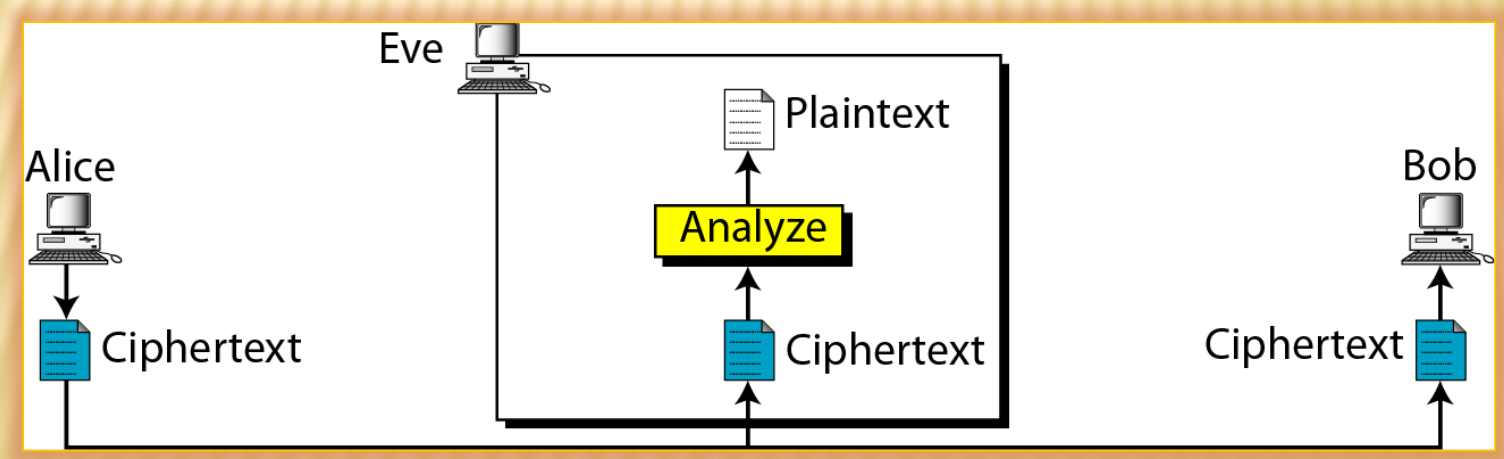
Cryptanalysis attacks



CIPHERTEXT-ONLY ATTACK

Ciphertext + algorithm ☾ key and the plaintext

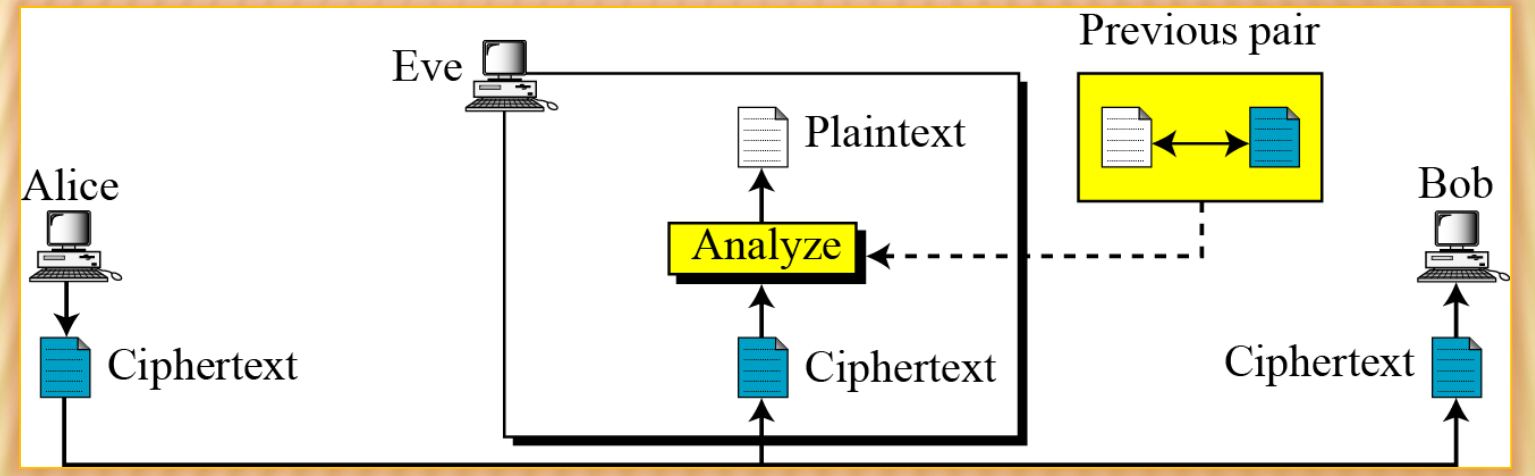
- Brute-Force attack: exhaustive key search attack
- Statistical attack: benefit from inherent characteristics of the plaintext language. E.g. E is the most frequently used letter.
- Pattern attack: discover pattern in ciphertext.



KNOWN-PLAINTEXT ATTACK

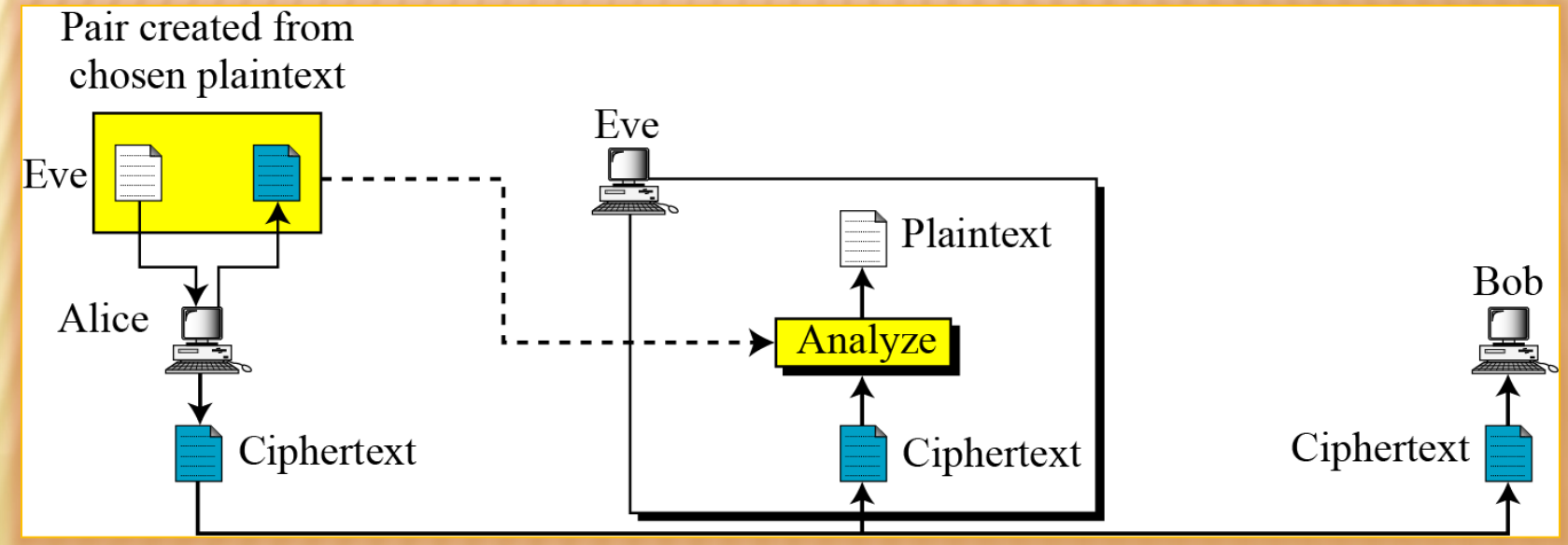
Eve has access to some plaintext/ciphertext pairs in addition to the intercepted ciphertext.

Eve uses the relationship b/w the previous pair to analyze the current ciphertext.



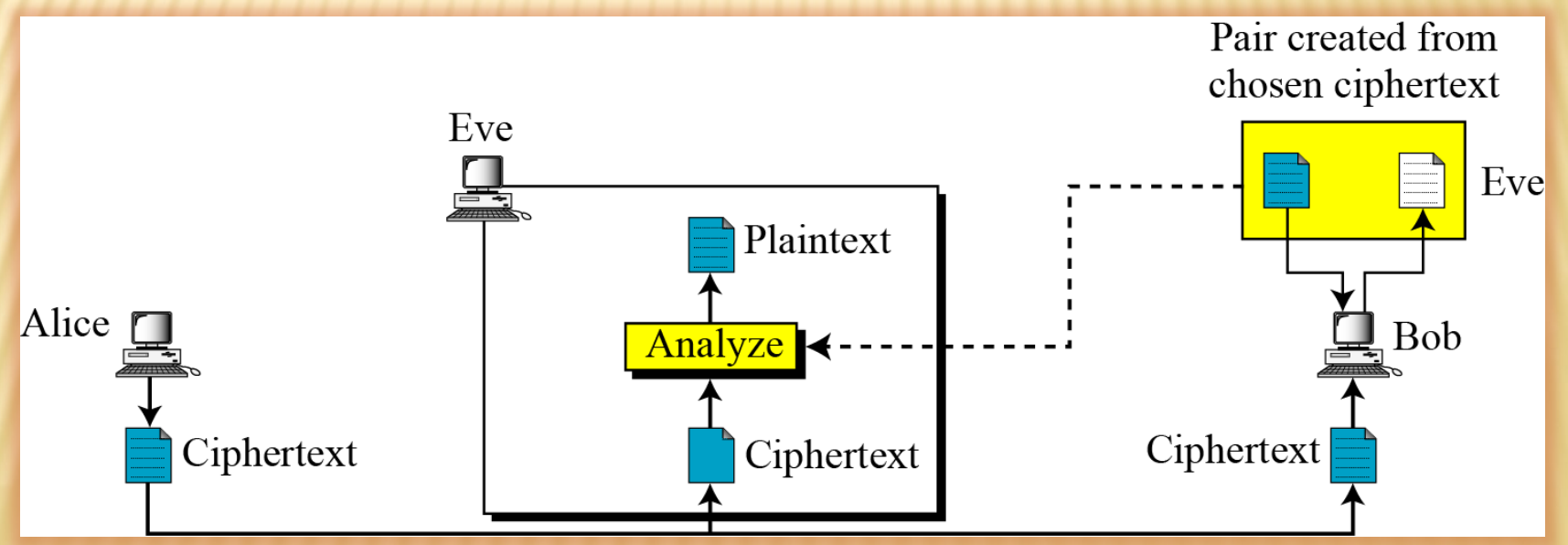
CHOSEN-PLAINTEXT ATTACK

The plaintext/ciphertext pairs have been chosen by the attacker herself.

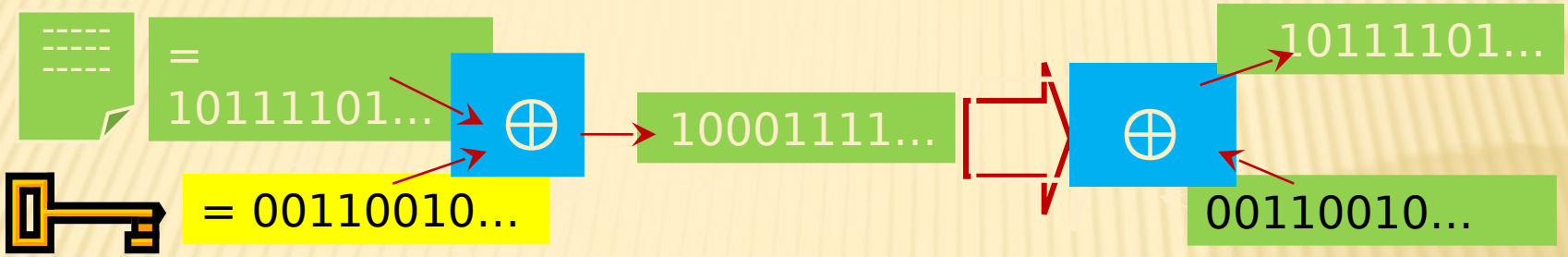


CHOSEN-CIPHERTEXT ATTACK

Eve chooses some ciphertext and decrypts to form a ciphertext/plaintext pair. This can happen if Eve has access to Bob's computer.



SIMPLE IDEA: ONE-TIME PAD



Key is a never-repeating bit sequence as long as plaintext

Encrypt by bitwise XOR of plaintext and key:
ciphertext = plaintext ⊕ key

Decrypt by bitwise XOR of ciphertext and key:
ciphertext ⊕ key = (plaintext ⊕ key) ⊕ key = plaintext ⊕ (key ⊕ key) = plaintext

Cipher achieves perfect secrecy if and only if there are as many possible keys as possible plaintexts, and every key is equally likely (Claude Shannon's result)

ADVANTAGES OF ONE-TIME PAD

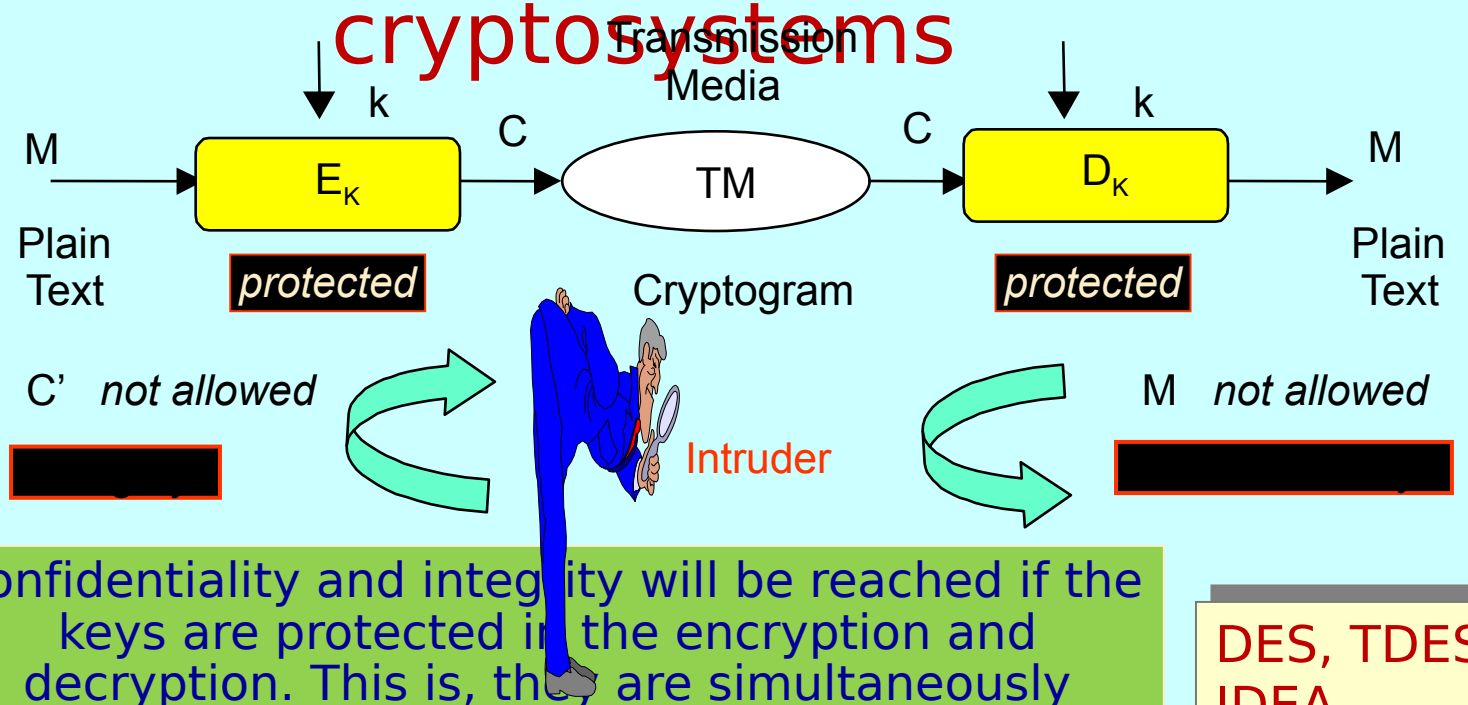
- Easy to compute
  - Encryption and decryption are the same operation
  - Bitwise XOR is very cheap to compute
- As secure as possible
  - Given a ciphertext, all plaintexts are equally likely, regardless of attacker's computational resources
  - ...as long as the key sequence is truly random
    - True randomness is expensive to obtain in large quantities
  - ...as long as each key is same length as plaintext
    - But how does the sender communicate the key to receiver?

PROBLEMS WITH ONE-TIME PAD

- Key must be as long as plaintext
  - Impractical in most realistic scenarios
  - Still used for diplomatic and intelligence traffic
- Does not guarantee integrity
  - One-time pad only guarantees confidentiality
  - Attacker cannot recover plaintext, but can easily change it to something else
- Insecure if keys are reused
  - Attacker can obtain XOR of plaintexts

SYMMETRIC CRYPTOSYSTEMS

Encryption with secret key cryptosystems



Confidentiality and integrity will be reached if the keys are protected in the encryption and decryption. This is, they are simultaneously obtained if the secret key is protected.

DES, TDES, IDEA, CAST, AES...

STREAM AND BLOCK CIPHERS

The literature divides the symmetric ciphers into two broad categories: stream ciphers and block ciphers. Although the definitions are normally applied to modern ciphers, this categorization also applies to traditional ciphers.

Stream Ciphers
Block Ciphers
Combination

SYMMETRIC KEY CRYPTOSYSTEMS

- **Stream ciphers**
  - Operate on the plaintext a single bit (or sometimes byte) at a time
  - Simple substitution
  - Poly-alphabetic substitution
  - **ORYX** is the algorithm used to encrypt data sent over digital cellular phones. t is a stream cipher based on three 32-bit Galois Linear Feedback Shift Register (LFSR)s. The cryptographic tag-team from Counterpane Systems (David Wagner, John Kelsey, and Bruce Schneier) have developed an attack on ORYX that requires approximately 24 bytes of known plaintext and about 2^{16} initial guesses.

SYMMETRIC KEY CRYPTOSYSTEMS

- **Stream ciphers**
  - **SEAL**, designed by Don Coppersmith of IBM Corp, is probably the fastest secure encryption algorithm available. The key setup process of SEAL requires several kilobytes of space and rather intensive computation involving SHA1, but only five operations per byte are required to generate the keystream. SEAL is particularly appropriate for disk encryption and similar applications where data must be read from the middle of a ciphertext stream. SEAL is patented, and can be licensed from IBM.
  - RC4 algorithm is a stream cipher from RSA Data Security, Inc. There are no known attacks against RC4. RC4 is not patented by RSA Data Security, Inc; it is just protected as a trade secret. The 40-bit exportable version of RC4 has been broken by brute force! (used by WLAN IEEE 802.11 in WEP)

SYMMETRIC KEY CRYPTOSYSTEMS

- **Block ciphers**
  - Operate on the plaintext in groups of bits. The groups of bits are called **blocks**.
  - Typical block size is 64 bits or multiple of it, e.g. 128 bits, 256 bits.
  - DES, AES
  - IDEA, developed in Zurich is generally regarded to be one of the best and most secure block algorithm available to the public today. It utilizes a 128-bit key and is designed to be resistant to differential cryptanalysis. Some attacks have been made against reduced round IDEA.

SYMMETRIC KEY CRYPTOSYSTEMS

- **Block ciphers**
  - Blowfish is a block cipher designed by Bruce Schneier, and is perhaps one of the most secure algorithms available.
  - RC5 is a group of algorithms designed by RSA that can take on a variable block size, key size, and number of rounds. RC5 generally has a 64-bit block size. David Wagner, John Kelsey, and Bruce Schneier have found weak keys in RC5, with the probability of selecting a weak key to be 2^{-10r}, where r is the number of rounds. For sufficiently large r values (greater than 10), this is not a problem as long as you are not trying to build a hash function based on RC5. Kundsen has also found a differential attack on RC5.
  - Different modes of operation

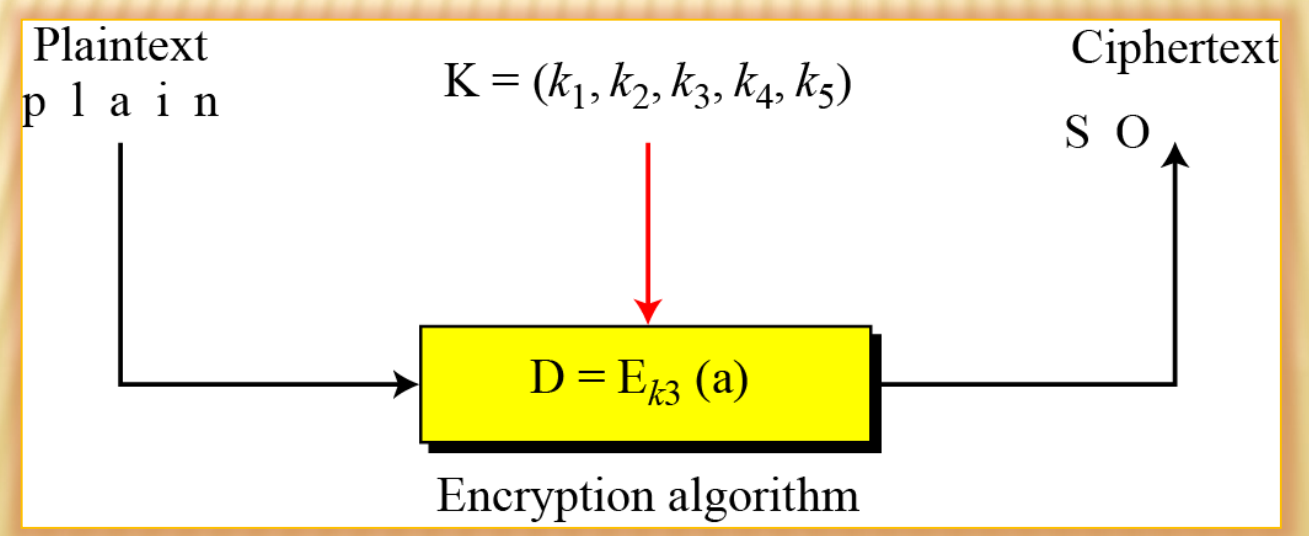
STREAM CIPHERS

Call the plaintext stream P, the ciphertext stream C, and the key stream K.

$$P = P_1P_2P_3, \ldots \qquad C = C_1C_2C_3, \ldots \qquad K = (k_1, k_2, k_3, \ldots)$$

$$C_1 = E_{k1}(P_1) \qquad C_2 = E_{k2}(P_2) \qquad C_3 = E_{k3}(P_3) \ldots$$

Stream cipher



STREAM CIPHERS

Example

Additive ciphers can be categorized as stream ciphers in which the key stream is the repeated value of the key. In other words, the key stream is considered as a predetermined stream of keys or $K = (k, k, \ldots, k)$. In this cipher, however, each character in the ciphertext depends only on the corresponding character in the plaintext, because the key stream is generated independently.

Example

The monoalphabetic substitution ciphers discussed in this chapter are also stream ciphers. However, each value of the key stream in this case is the mapping of the current plaintext character to the corresponding ciphertext character in the mapping table.

STREAM CIPHERS

Example

Vigenere ciphers are also stream ciphers according to the definition. In this case, the key stream is a repetition of m values, where m is the size of the keyword. In other words,

$$K = (k_1, k_2, \ldots k_m, k_1, k_2, \ldots k_m, \ldots)$$

Example

We can establish a criterion to divide stream ciphers based on their key streams. We can say that a stream cipher is a monoalphabetic cipher if the value of k_i does not depend on the position of the plaintext character in the plaintext stream; otherwise, the cipher is polyalphabetic.

STREAM CIPHERS

Example

- Additive ciphers are definitely monoalphabetic because k_i in the key stream is fixed; it does not depend on the position of the character in the plaintext.

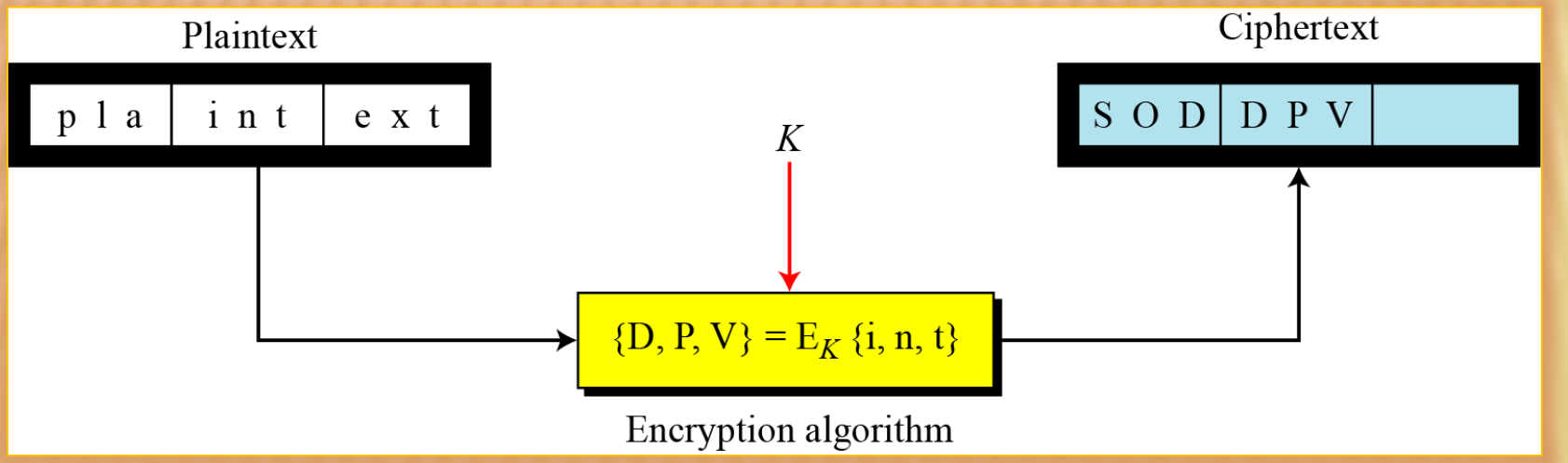
- Monoalphabetic substitution ciphers are monoalphabetic because k_i does not depend on the position of the corresponding character in the plaintext stream; it depends only on the value of the plaintext character.

- Vigenere ciphers are polyalphabetic ciphers because k_i definitely depends on the position of the plaintext character. However, the dependency is cyclic. The key is the same for two characters m positions apart.

BLOCK CIPHERS

In a block cipher, a group of plaintext symbols of size m (m > 1) are encrypted together creating a group of ciphertext of the same size. A single key is used to encrypt the whole block even if the key is made of multiple values. Figure 3.27 shows the concept of a block cipher.

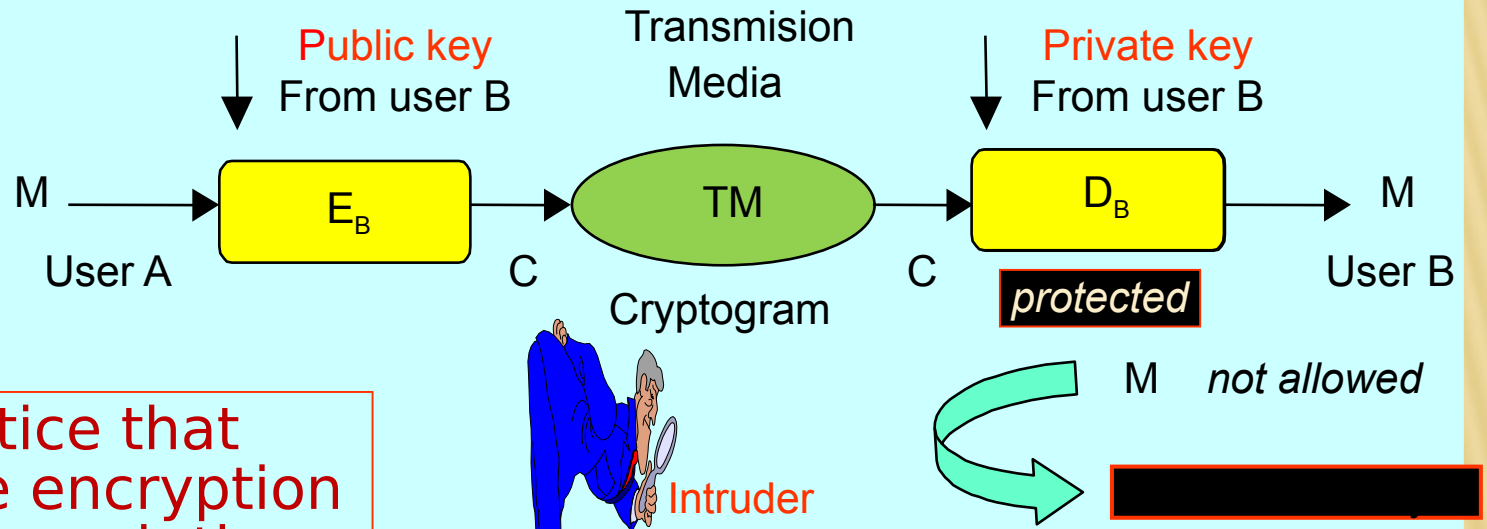
Block cipher



ASYMMETRIC CRYPTOSYSTEMS

Receiver Public Key Cipher

RSA Keys exchange



Notice that the encryption is trough the public key of receiver.

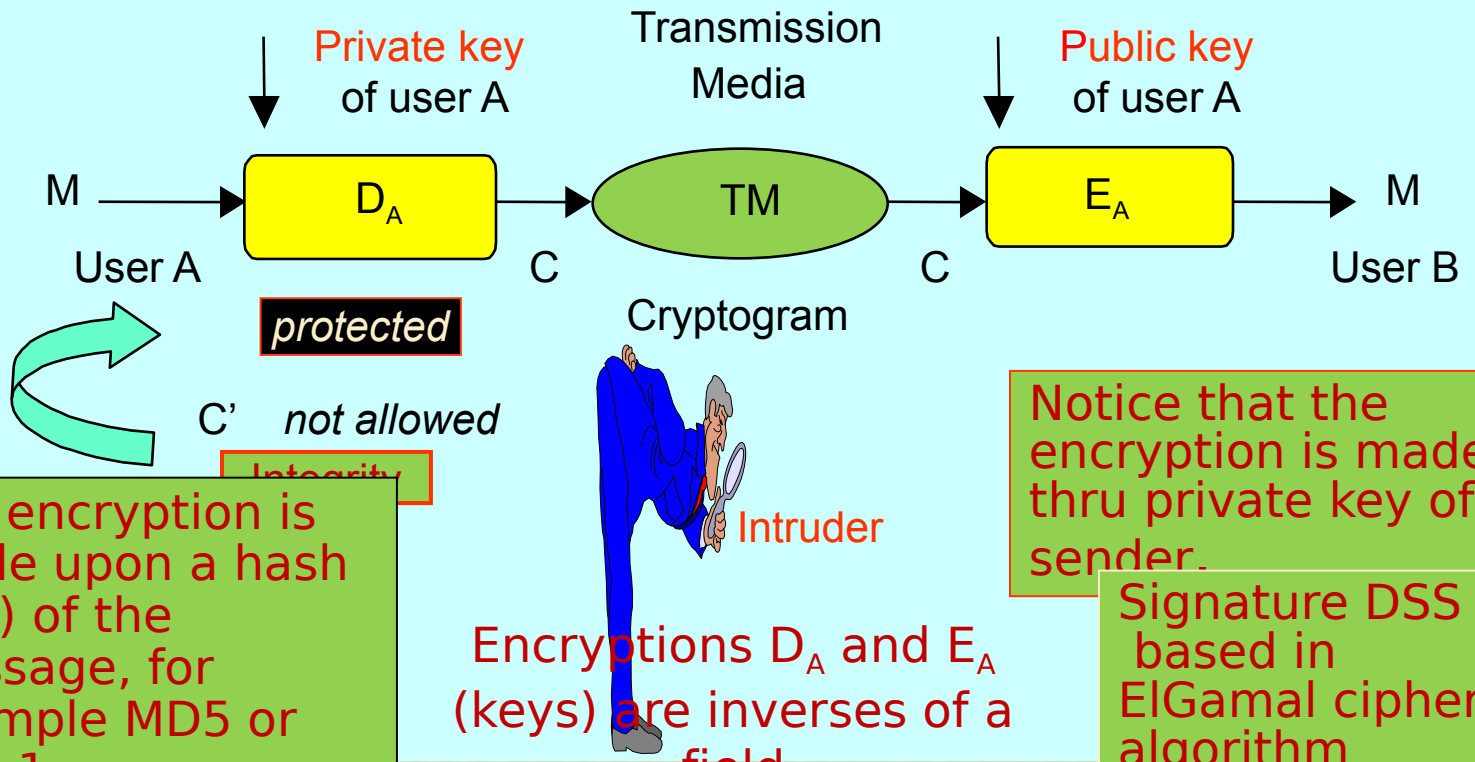
Encryptions E_B and D_B (keys) are inverses of a field

A similar system is Diffie & Hellman (DH) key agreement

ASYMMETRIC CRYPTOSYSTEMS

Encryption with private key of sender
Digital signature RSA

Signatures: RSA and DSS



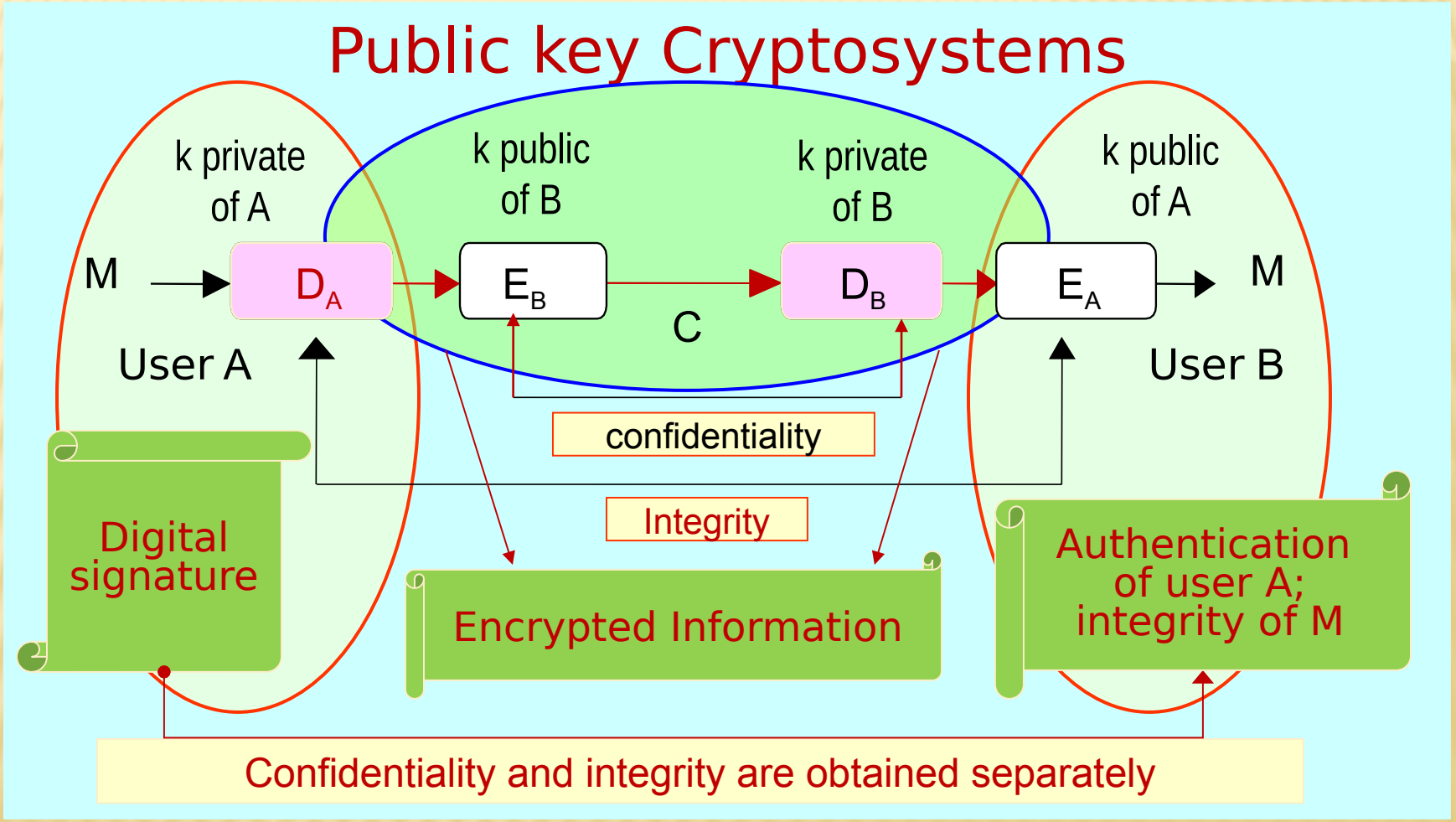
The encryption is made upon a hash H(M) of the message, for example MD5 or SHA-1

Encryptions D_A and E_A (keys) are inverses of a field

Notice that the encryption is made thru private key of sender.

Signature DSS is based in ElGamal cipher algorithm

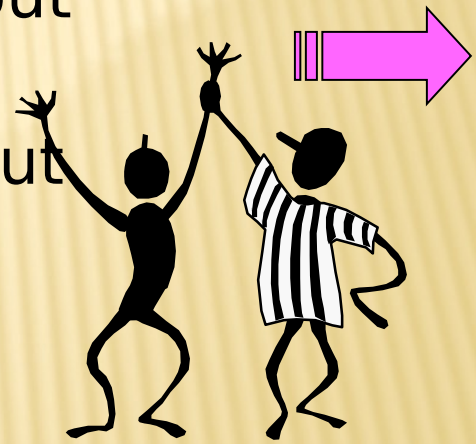
TYPES OF CIPHER WITH ASYMMETRIC SYSTEMS



SYMMETRIC OR ASYMMETRIC CIPHER?

Public key systems are very slow but they have digital signature.

Secret key systems are very fast but they do not have digital signature.

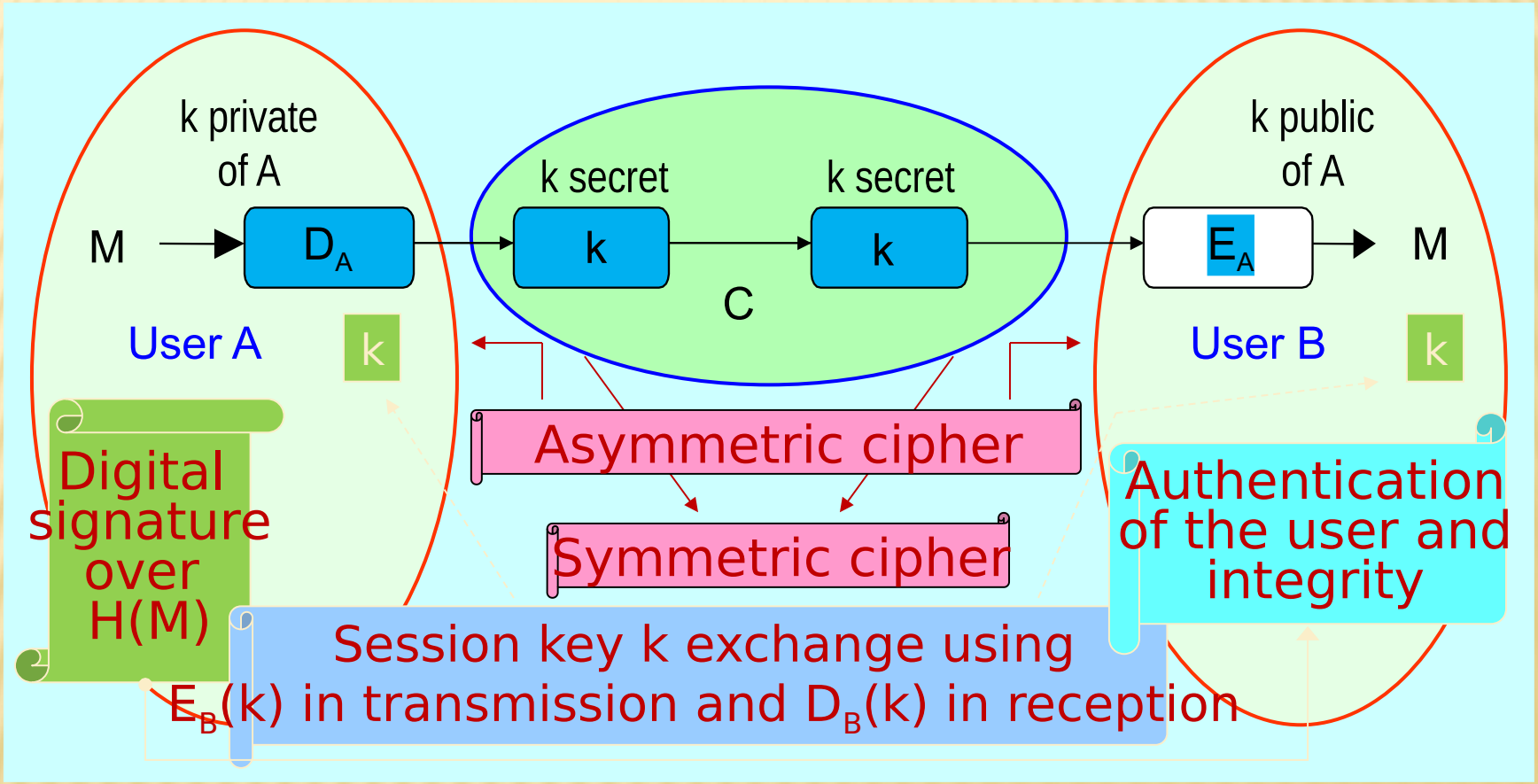


What should we do?

Information encryption:
- We´ll use secret key systems

Signature and session key exchange:
- We´ll use public key systems

HYBRID SYSTEM OF CIPHER AND SIGNATURE



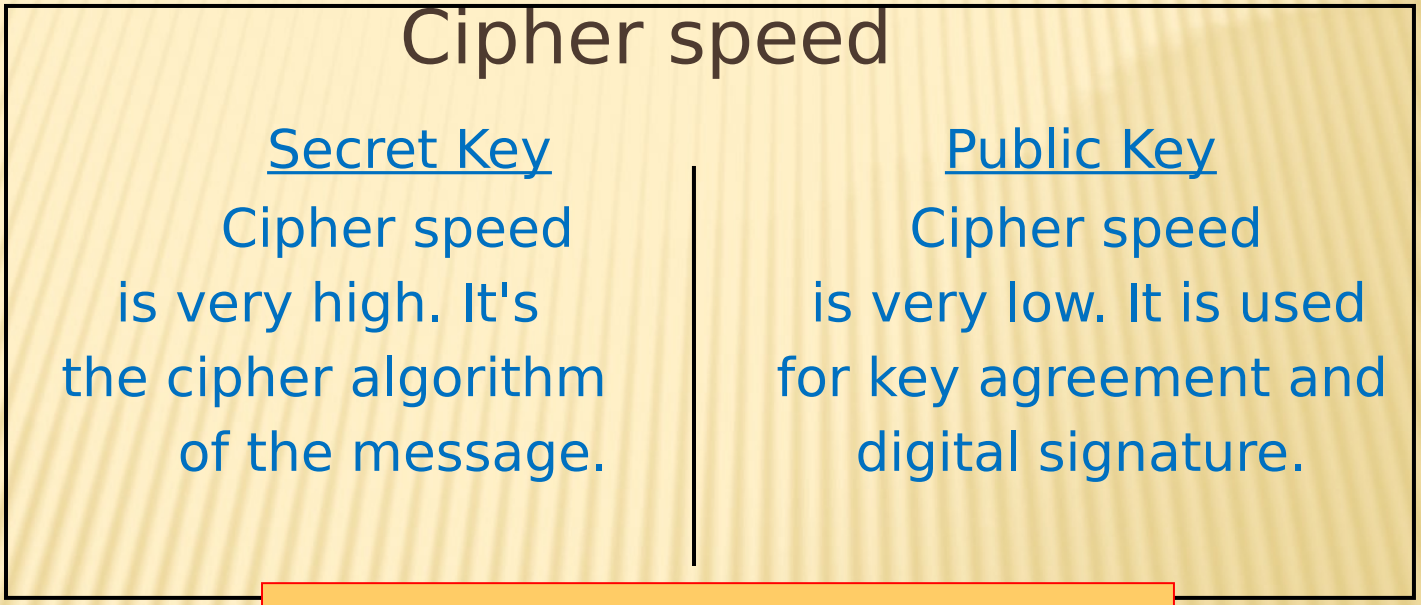
COMPARATIVE: SENDER'S AUTHENTICATION

Authentication

Secret Key	Public Key
The messsage can be authenticated but not the sender in an easy and efficient way.	Having a public key and another private, both the message and the sender can be authenticated.

Regarding authentication, symmetric systems have a heavier authentication and with only a third part of trust. Asymmetric ones allow a real digital signature, efficient and simple, where the third part of trust is just presential.

COMPARATIVE: CIPHER SPEED



Hundreds of M Bytes/seg in HW

Regarding cipher speed, symmetric systems are from 100 to 1.000 times faster than asymmetrics. In SW cipher speed is lower.

Hundreds of K Bytes/seg in HW

ummary symmetric cipher v/s asymmet

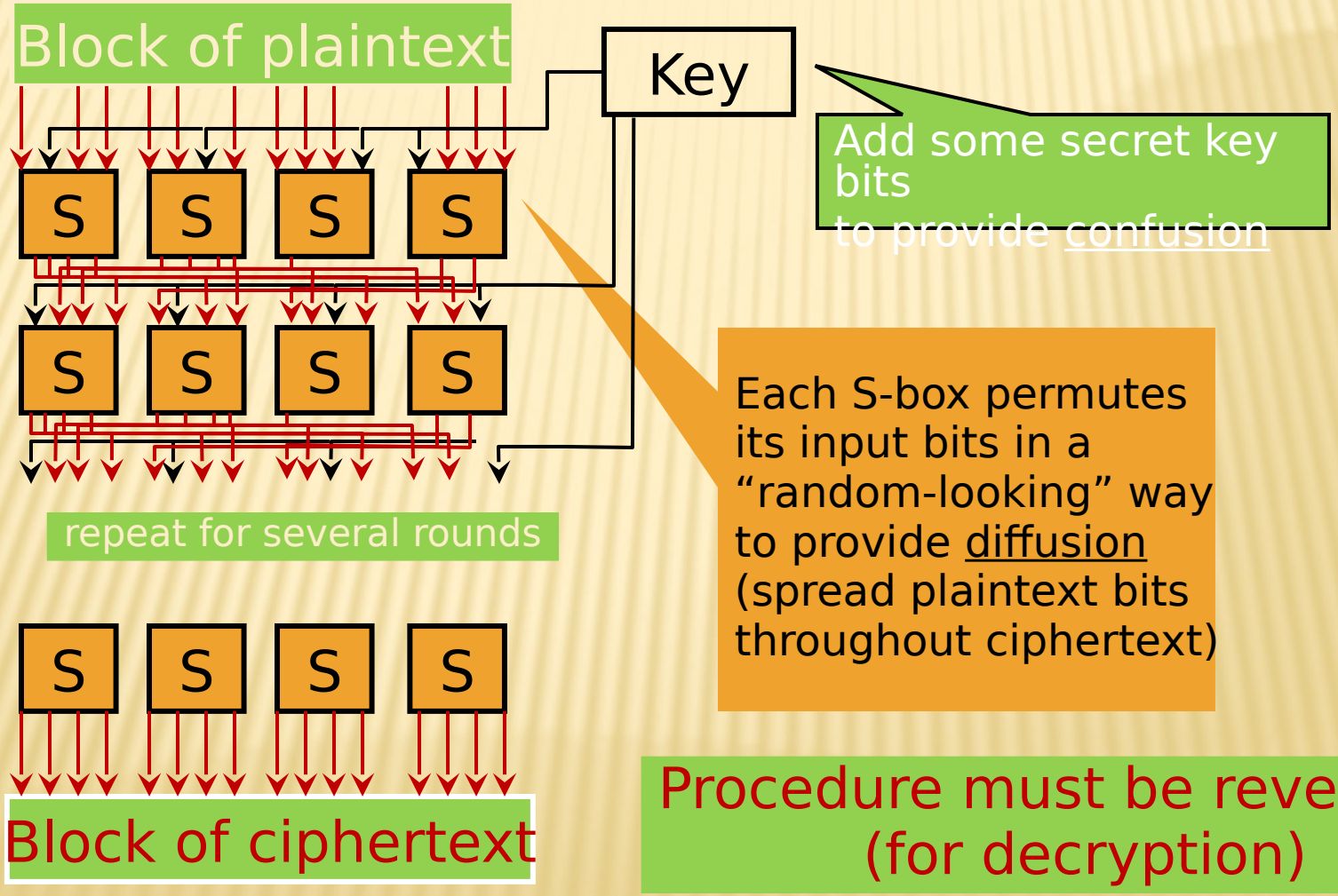
Symmetric Cipher

- Confidentiality
- Partial authentication
- No digital signature
- Keys:
  - Small lenght
  - Short lifetime (session)
  - Elevated number
- High speed

Asymmetric Cipher

- Confidentiality
- Total authentication
- With digital signature
- Keys:
  - Big lenght
  - Long lifetime
  - Number reduced
- Slow speed

BLOCK CIPHER OPERATION (SIMPLIFIED)



Procedure must be reversible (for decryption)

DESIGN PRINCIPLES

- **block size**
  - increasing size improves security, but slows cipher
- **key size**
  - increasing size improves security, makes exhaustive key searching harder, but may slow cipher
- **number of rounds**
  - increasing number improves security, but slows cipher
- **subkey generation**
  - greater complexity can make analysis harder, but slows cipher
- **round function**
  - greater complexity can make analysis harder, but slows cipher
- **fast software en/decryption & ease of**

DATA ENCRYPTION STANDARDS

- 1972 – NBS issues call for proposals
- 1974 – IBM responds with “lucifer” (DEA)
- 1976 – DES adopted
- 1986 – DES re-certification denied
- 1997 – NIST issues call for AES proposals
- 1999 – 5 submissions selected as finalists
- 2001 – Rijndahl algorithm selected

DES OVERVIEW

- Combination cipher
- 16 rounds of combined substitution and transposition
- Plaintext encrypted in 64-bit blocks
- Keys are 56 bits long (plus 8 error bits)
- Uses only arithmetic and logical operations on 64-bit numbers

AES STRUCTURE

- Apply round *n* times, where *n* depends on key size: 9 for 128, 11 for 192, 13 for 256
- Longer key sizes can be accommodated by increasing *n*.
- Each operation is very fast (add is actually an xor/shift) so algorithm is very efficient

DIGITAL SIGNATURES

How do you know that I sent that message?

- Knowing its me -- asymmetric key encryption
- Knowing its my message -- message digest (checksum)

Digital signatures can be legally equivalent to physical signatures

MESSAGE DIGESTS

Calculate function based on message content

- Irreversible (can’t go from value to message)
- Fixed size output (relatively small)
- Known method (to produce and check)
- Low collision (few texts with same value)

Common functions:

- MD2 – slow but strong
- MD4 – fast but weak
- MD5 – stronger than MD4, widely used
- SNEFRU – reportedly broken
- SHA – Similar to MD4/MD5

PICKING A CODE

- How important is the data?
- What cost for interception?
- What cost for modification?
- What cost for loss?
- Privacy of holding or privacy of sharing?
- How much delay is acceptable?
- US or Non-US?

PGP

- Freely distributed hybrid-key cryptosystem for non-commercial purposes
- 1991 version - violated RSA patent, exported without clearance
- Operation - uses Diffie/Hellman encryption for exchange of IDEA keys; digital signature MD5
- Commercial version - Network Associates (recently discontinued)
- Open-source workalike (Gnu Privacy Guard) http://www.gnupg.org/
- Available for wide variety of operating systems

WEB OF TRUST

- How do you know which is right public key?
  - Key signatures
  - Trusted introducer signature
  - Out of band verification
  - Expiring key
- Key servers

PUBLIC KEY INFRASTRUCTURE

- Organized means of handling public keys
- Key authorities
  - Trusted parties
  - Central source of distribution and cancellation
  - Division of trust
- What if authorities disagree?
- Which is most trusted?
- How do you handle lost keys?
- How do you protect against disclosure?

Developed and Presented By Dr. Mehrdad Sepehri Sharbaf
CSUDH
Computer Science Department

http://csc.csudh.edu/

The some of the materials are excerpted from Paul Reid ’s Book, John Chirillo and Scott Blaul ’s Book, and Ross Anderson’s Book

BIOMETRICS

WHO ARE YOU?

HOW ARE PEOPLE IDENTIFIED?

- People’s identity are verified and identified by three basic means:
  - Something they **have** (identity document or token)
  - Something they **know** (password, PIN)
  - Something they **are** (human body such as fingerprint or iris).
- The strongest authentication involves a combination of all three.

PERSON IDENTIFICATION

- Identifying fellow human beings has been crucial to the fabric of human society
- In the early days of civilization, people lived in small communities and everyone knew each other
- With the population growth and increase in mobility, we started relying on documents and secrets to establish identity
- Person identification is now an integral part of the infrastructure needed for diverse business sectors such as banking, border control, law enforcement.

AUTOMATIC IDENTIFICATION

Different means of automatic identification:

- **Possession-based** (credit card, smart card)
  - *“something that you have”*
- **Knowledge-based** (password, PIN)
  - *“something that you know”*
- **Biometrics-based** (biometric identifier)
  - *“something about or produced by your physical make-up”*

PROBLEMS WITH POSSESSION- OR KNOWLEDGE-BASED APPROACHES

- Card may be lost, stolen or forgotten
  - Password or PIN may be forgotten or guessed by the imposters
- ~25% of people seem to write their PIN on their ATM card
- Estimates of annual identity fraud damages:
  - $56.6 billion in credit card transactions in U.S. alone in 2005*
    - 0.25% of internet transactions revenues, 0.08% of off-line revenues
  - $1 billion in fraudulent cellular phone use
  - $3 billion in ATM withdrawals
- The traditional approaches are unable to differentiate between an authorized person and an impostor

IDENTIFICATION PROBLEMS

- Identity Theft: Identity thieves steal PIN (e.g., date of birth) to open credit card accounts, withdraw money from accounts and take out loans

3.3 million identity thefts in U.S. in 2010; 6.7 million victims of credit card fraud

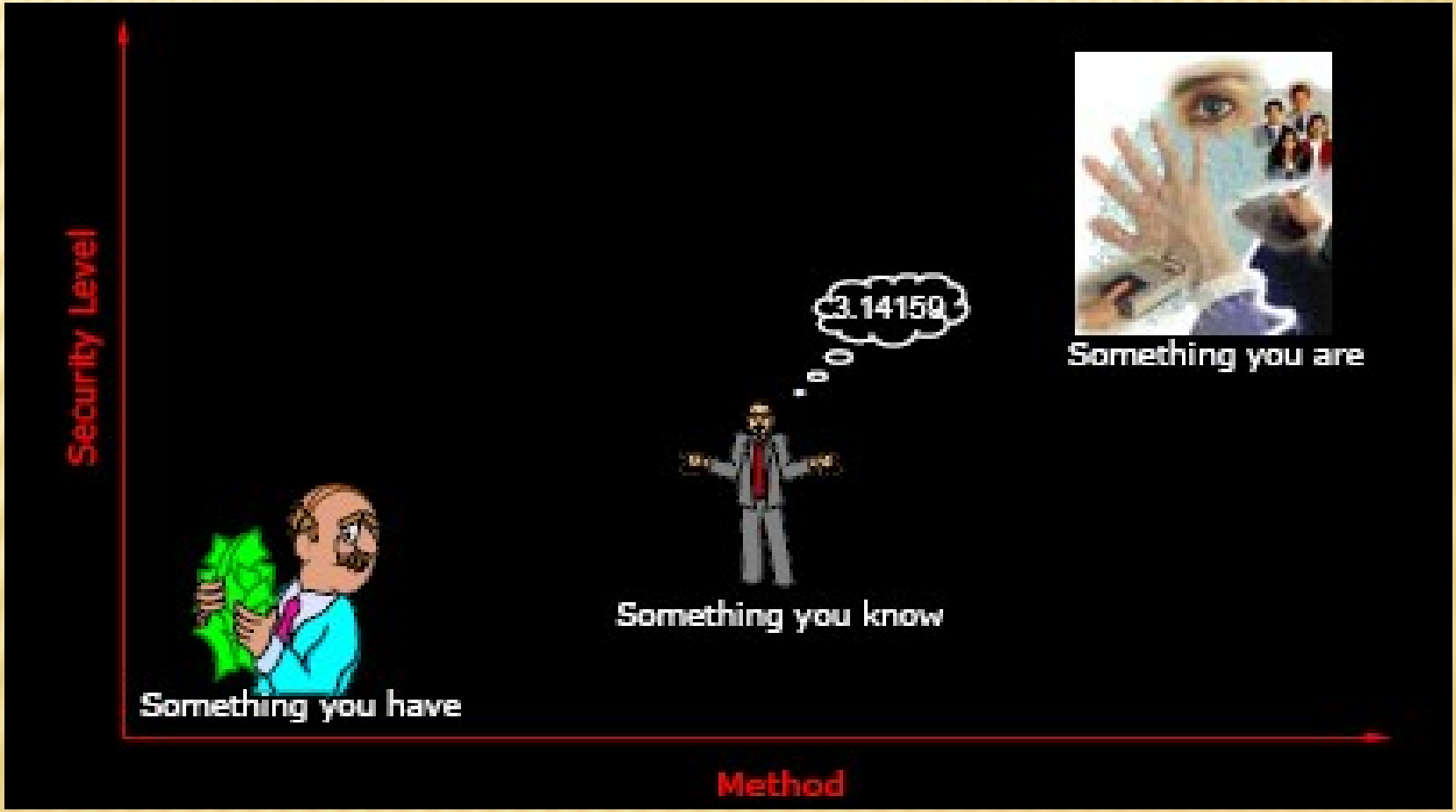
Surrogate representations of identity such as passwords and ID cards no longer suffice

WHAT ARE BIOMETRICS?

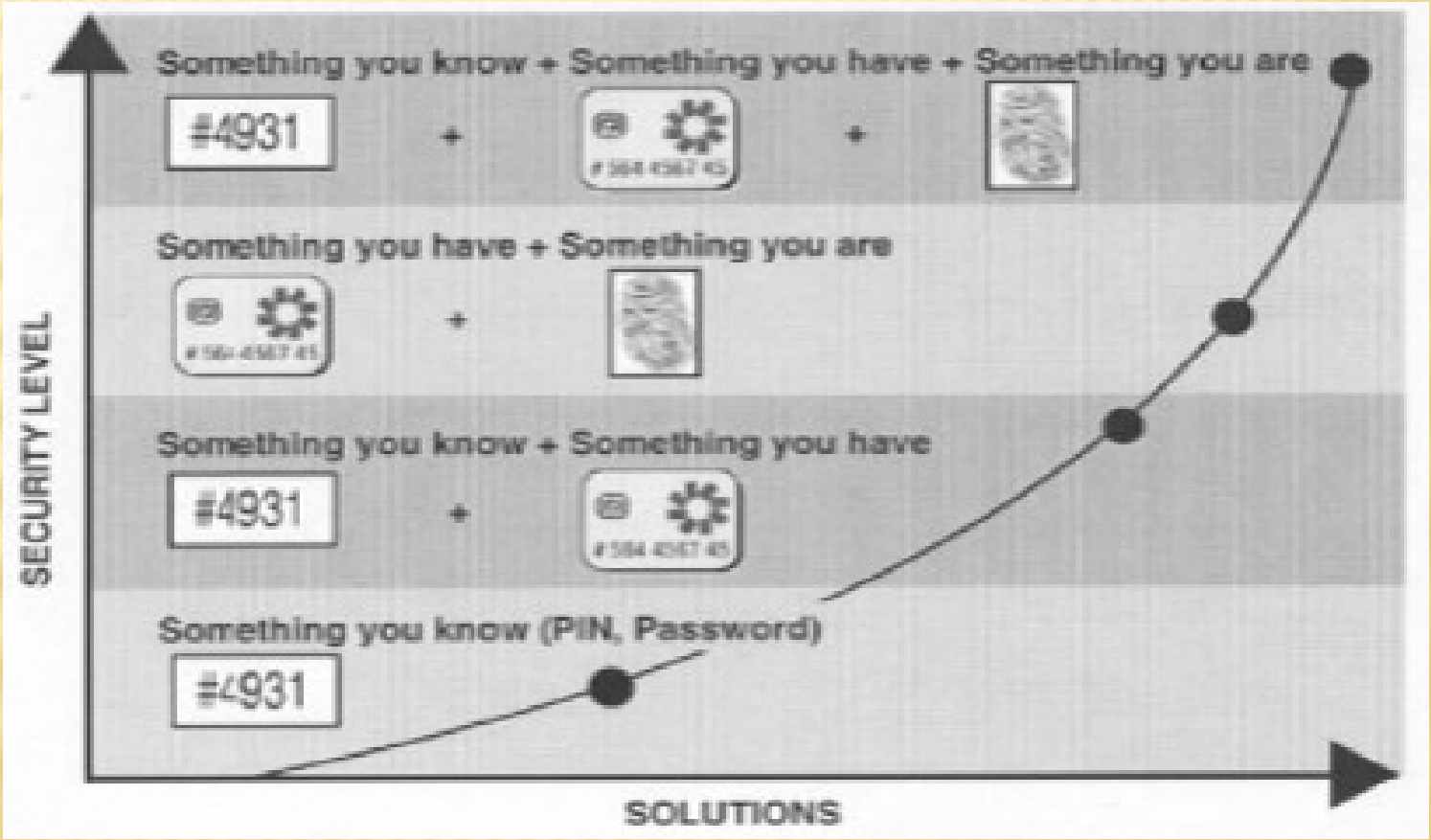
- **Biometrics** – science, which deals with the automated recognition of individuals (or plants/animals) based on biological and behavioral characteristics
- **Biometry** – mathematical and statistical analysis of biological data
- **Biometric system** – a pattern recognition system that recognizes a person by determining the authenticity of a specific biological and/or behavioral characteristic (biometric)
- **Anthropometry**–measurement techniques of human body and its specific parts
- **Forensic (judicial) anthropometry**–identification of criminals by these measurement techniques

WHY BIOMETRICS?

WHY BIOMETRICS?



MENTIONING THE OBVIOUS



REQUIREMENTS FOR AN IDEAL BIOMETRIC IDENTIFIER

1. Universality
   – Every person should have the biometric characteristic
2. Uniqueness
   - No two persons should be the same in terms of the biometric characteristic
3. Performance
   - The biometric characteristic should be invariant over time
4. Collectability
   - The biometric characteristic should be measurable with some (practical) sensing device
5. Acceptability
   - One would want to minimize the objections of the users to the measuring/collection of the biometric

IDENTIFIABLE BIOMETRIC CHARACTERISTICS

- **Biological traces**
  - DNA (DeoxyriboNucleic Acid), blood, saliva,etc.
- **Biological (physiological) characteristics**
  - fingerprints, eye irises and retinas, hand palms and geometry, and facial geometry
- **Behavioral characteristics**
  - dynamic signature, gait, keystroke dynamics, lip motion
- **Combined**
  - voice

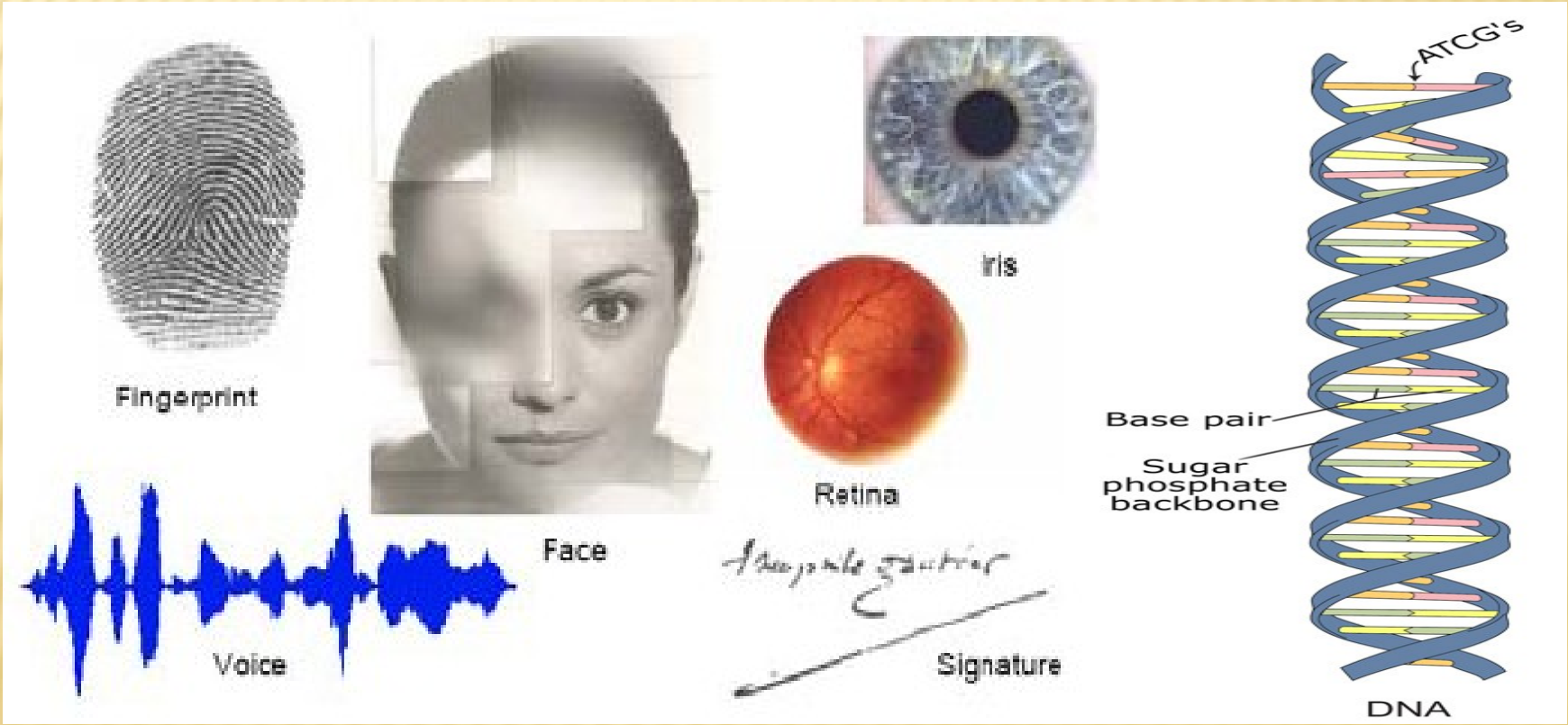
BIOMETRICS IS NOT NEW!!

- Bertillon system (1882) took a subject's photograph, and recorded height, the length of one foot, an arm and index finger
- Galton/Henry system of fingerprint classification adopted by Scotland Yard in 1900
- FBI set up a fingerprint identification division in 1924
- AFIS installed in 1965 with a database of 810,000 fingerprints
- First face recognition paper published in 1971 (Goldstein et al.)
- FBI installed IAFIS in ~2000 with a database of 47 million 10 prints; average of 50,000 searches per day; ~15% of searches are in lights out mode; 2 hour response time for criminal search

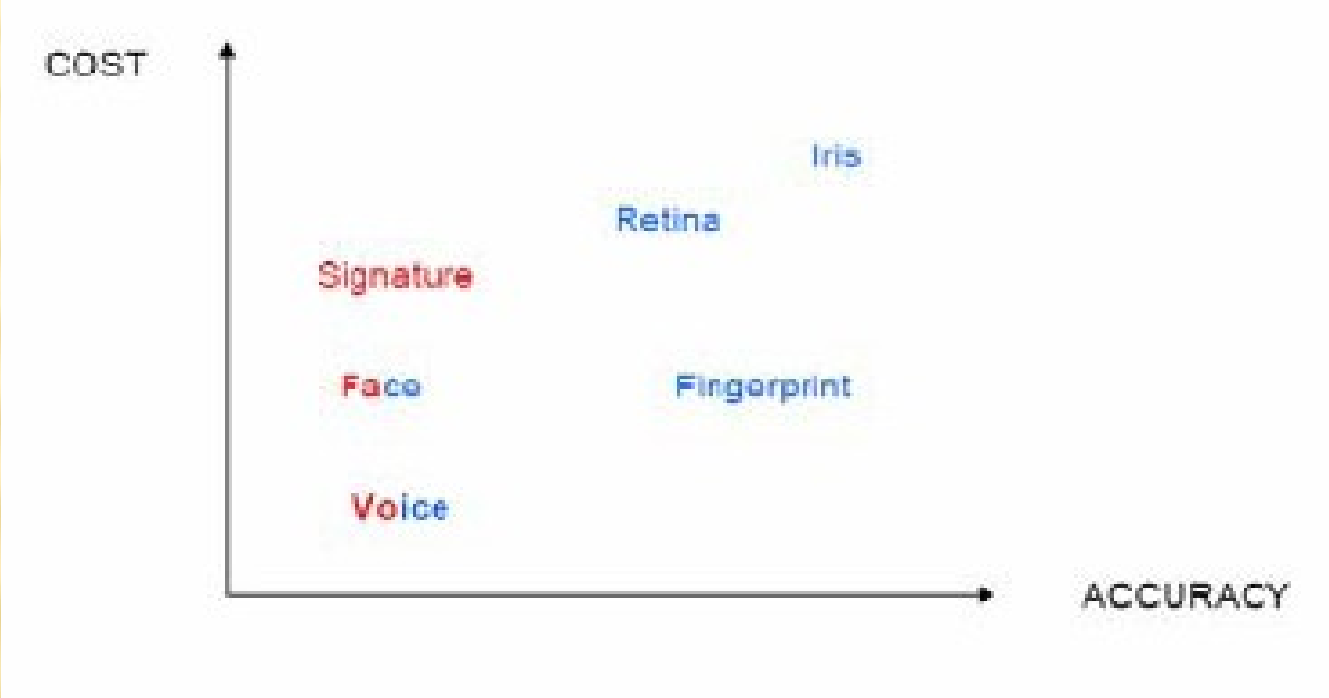
Emphasis now is to automatically perform reliable person identification in unattended mode, often remotely (or at a distance)

Biometrics

- A biometric authentication system uses the physiological (fingerprints, face, hand geometry, iris) and/or behavioral traits (voice, signature, keystroke dynamics) of an individual to identify a person or to verify a claimed identity.



COMPARISON OF BIOMETRIC TECHNIQUES



KEY BIOMETRIC TERMS AND PROCESS

WHAT IS BIOMETRIC?

- Biometrics is the automated use of physiological or behavioral characteristics to determine or verify identity.
- Automated use means using computers or machines, rather than human beings, to verify or determine physiological or behavioral characteristics.

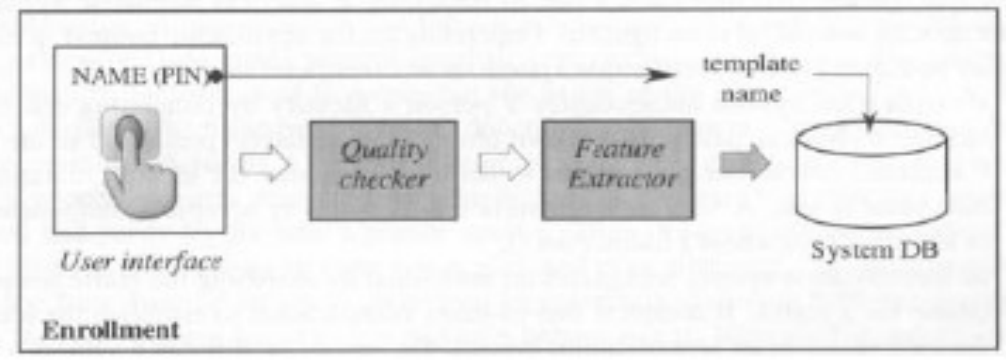
BIOMETRICS

- 2 Categories of Biometrics
  - Physiological – also known as static biometrics: Biometrics based on data derived from the measurement of a part of a person's anatomy. For example, fingerprints and iris patterns, as well as facial features, hand geometry and retinal blood vessels
  - Behavioral – biometrics based on data derived from measurement of an action performed by a person, and distinctively incorporating time as a metric, that is, the measured action. For example, voice (speaker verification)

USING BIOMETRICS
ENROLLMENT, VERIFICATION RECOGNITION

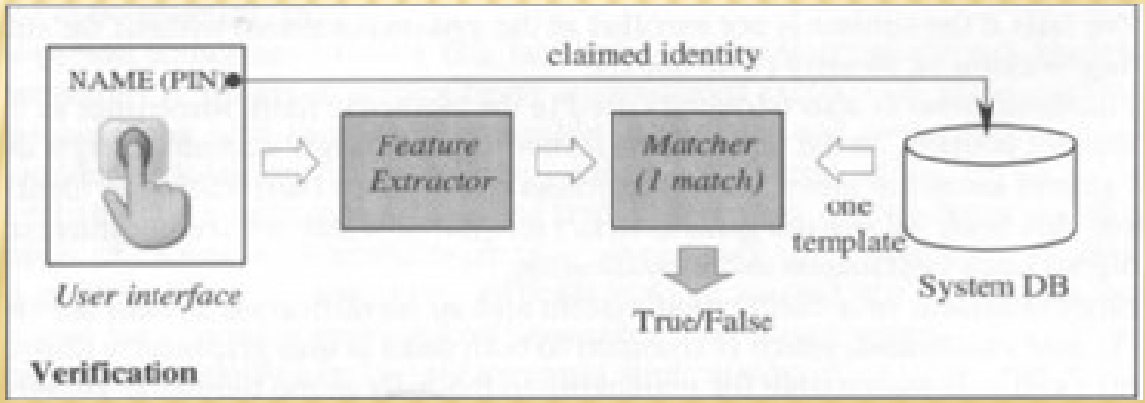
USING BIOMETRICS

- Process flow includes enrollment, and verification/identification.
- Enrollment
  - Person entered into the database
  - Biometric data provided by a user is converted into a template.
  - Templates are stored in a biometric systems for the purpose of subsequent comparison.



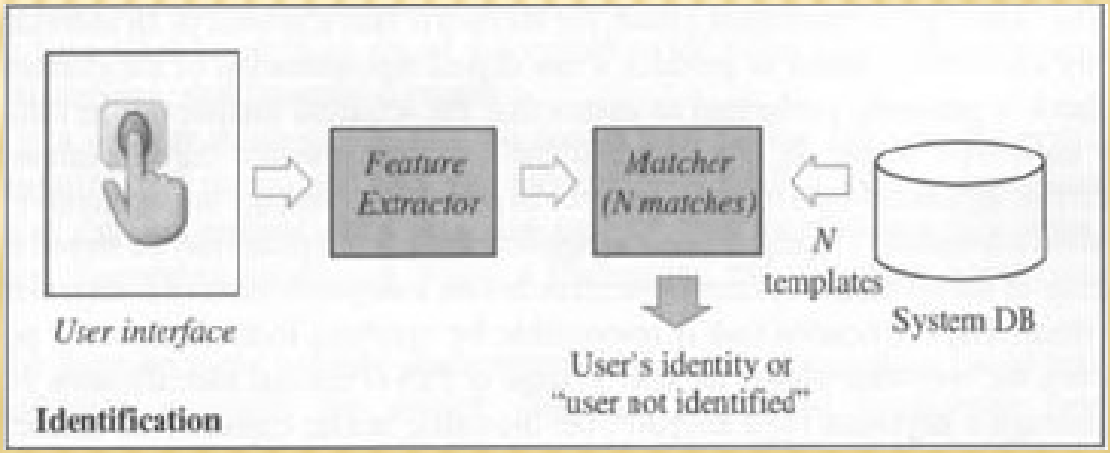
VERIFICATION VERSUS IDENTIFICATION

- Verification: Am I who I claim to be?
  - One to one comparison
  - Verification can confirm or deny the specific identification claim of a person.



IDENTIFICATION VERSUS VERIFICATION

- Identification: Who am I?
  - One to many comparison
  - can determine the identity of a person from a biometric database without that person first claiming an identity.



DISCUSSION: VERIFICATION AND IDENTIFICATION

- Verification system answers the question: “Am I who I claim to be?”
- The answer returned by the system is *match or no match*.
- Identification systems answers the question: “Who am I”
- The answer returned by the system is *an identity such as a name or ID number.*

DISCUSSION: VERIFICATION AND IDENTIFICATION

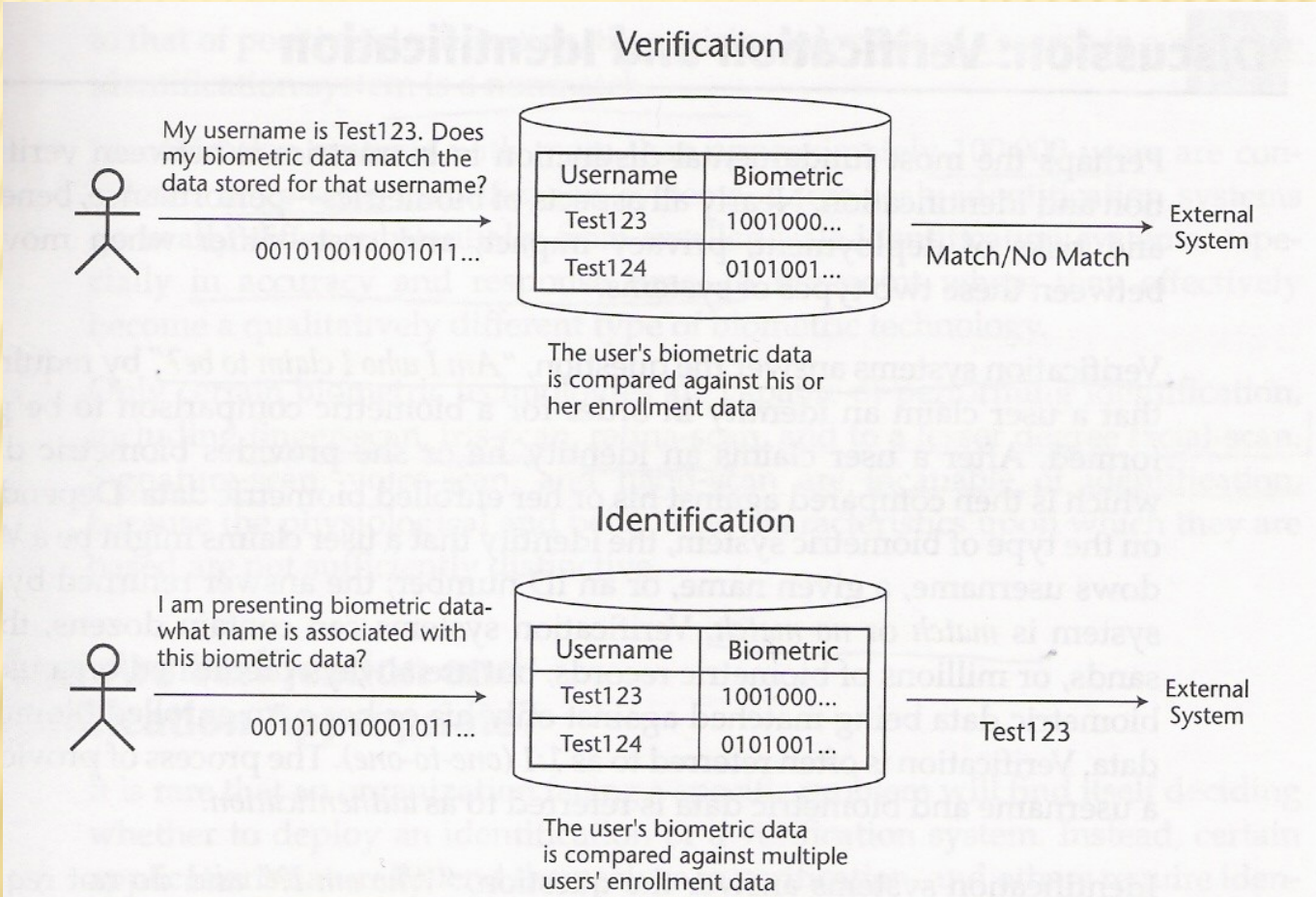


Figure 2.1 Determining versus verifying identity.

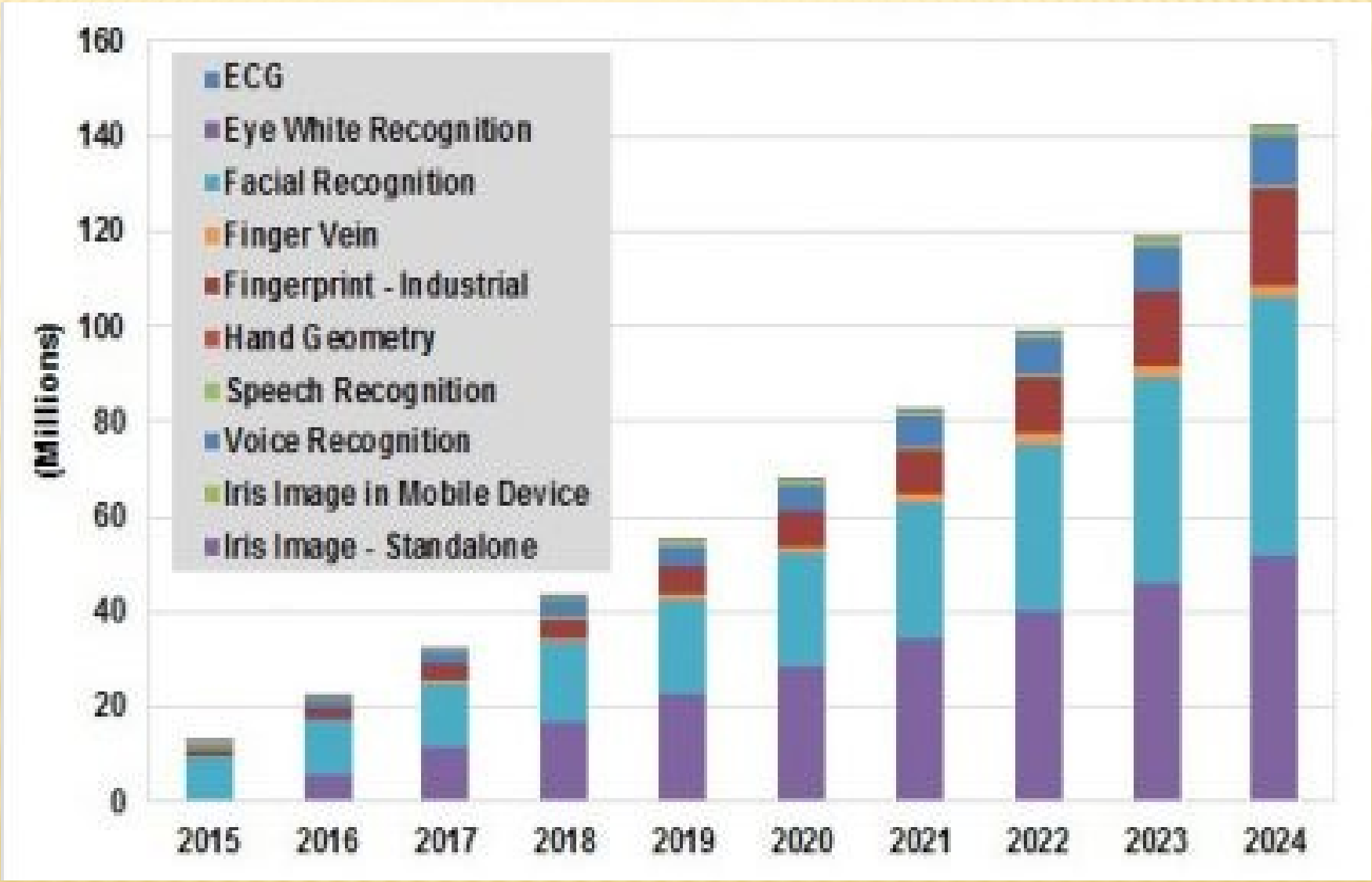
WHEN ARE VERIFICATION AND IDENTIFICATION APPROPRIATE?

- PC and Network Security -- verification
- Access to buildings and rooms – either verification (predominant) or identification
- Large-scale public benefit programs – identification
- Verification systems are generally faster and more accurate than identification systems.
- However, verification systems cannot determine whether a given person is present in a database more than once.

WHEN ARE VERIFICATION AND IDENTIFICATION APPROPRIATE?

- Identification system requires more computational power than verification systems, and there are more opportunities for an identification system to err.
- As a rule, verification systems are deployed when identification simply does not make sense (to eliminate duplicate enrollment, for instance.)

TOTAL BIOMETRICS MARKET



DIFFERENT BIOMETRICS

PHYSIOLOGICAL AND BEHAVIORAL CHARACTERISTICS

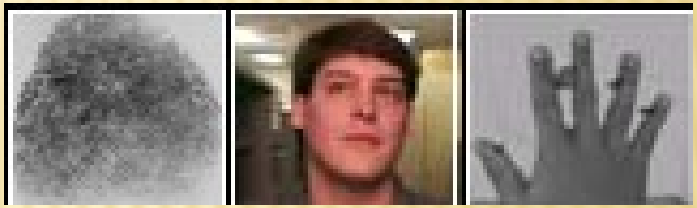
- Physiological or behavioral characteristics are distinctive, which provide basic measurement of biometrics.
- Physiological biometrics are based on direct measurements of a part of the human body, such as finger-scan, facial-scan, iris-scan, hand-scan, and retina-scan.
- Behavioral biometrics are based on measurements and data derived from an action and therefore indirectly measure characteristics of the human body, such as voice-scan and signature-scan.
- The element of time is essential to behavioral biometrics.

DNA (DEOXYRIBO NUCLEIC ACID) THE ULTIMATE BIOMETRIC

- One-dimensional unique code for one's individuality, but identical twins have identical DNA patterns
- Issues limiting the utility of DNA
  - Contamination
  - Access
  - Automatic real-time recognition issues
  - Privacy issues: information about susceptibilities of a person to certain diseases could be gained from the DNA pattern

BEHAVIORAL VS PHYSICAL TRAITS

- Physical Characteristics
  - Iris
  - Retina
  - Vein Pattern
  - Hand Geometry
  - Face
  - Fingerprint
  - Ear shape
- Behavioral Characteristics
  - Keystroke dynamics
  - Signature dynamics
  - Walking Gait
  - Voice



FINGERPRINTS

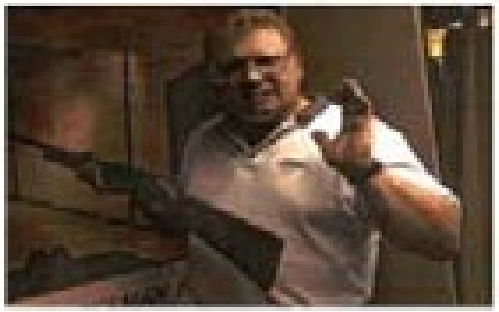
Fingerprint at check-out counter

Disney World

Smart card

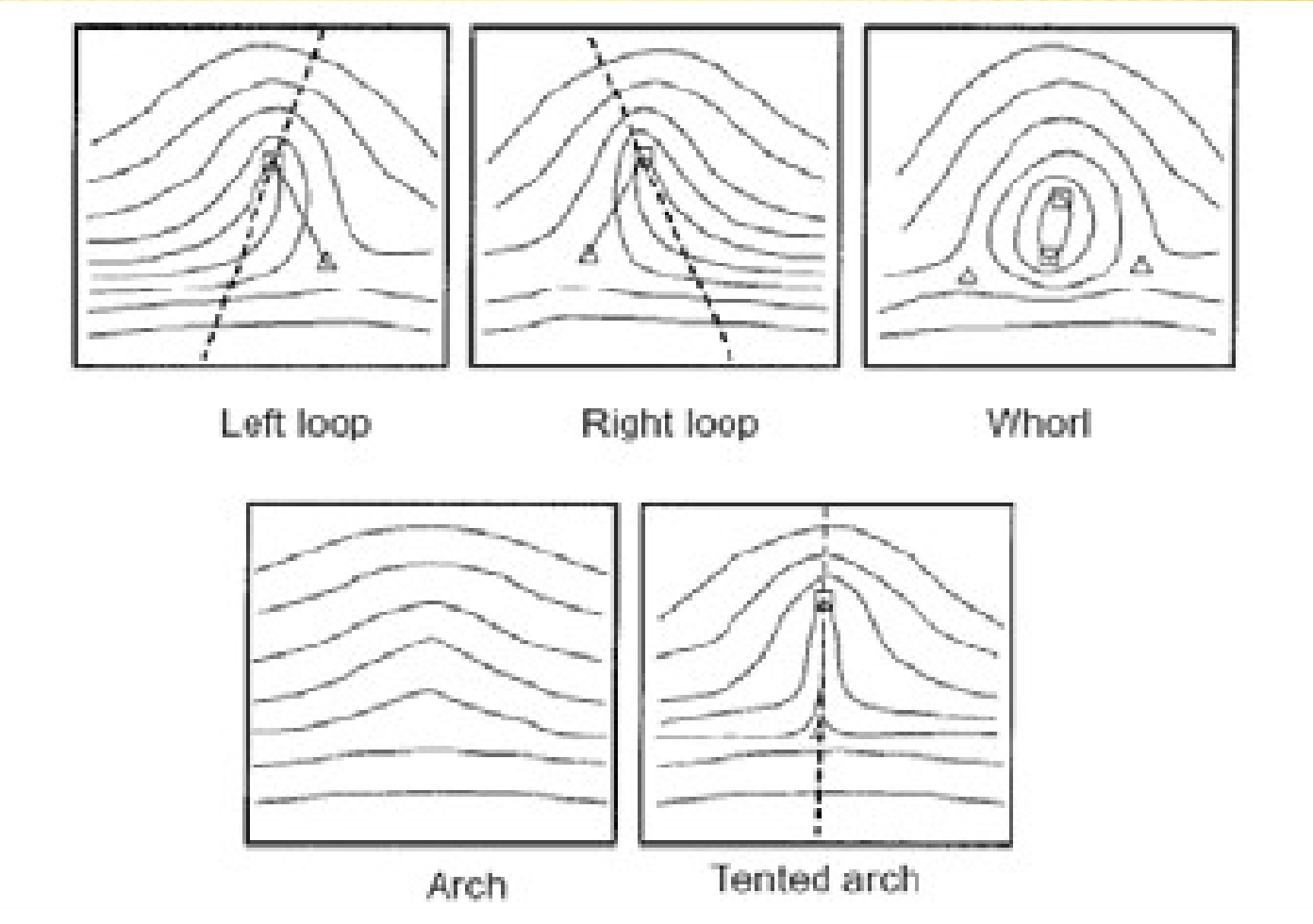
Smart PDA

Cell phone with Fingerprint sensor

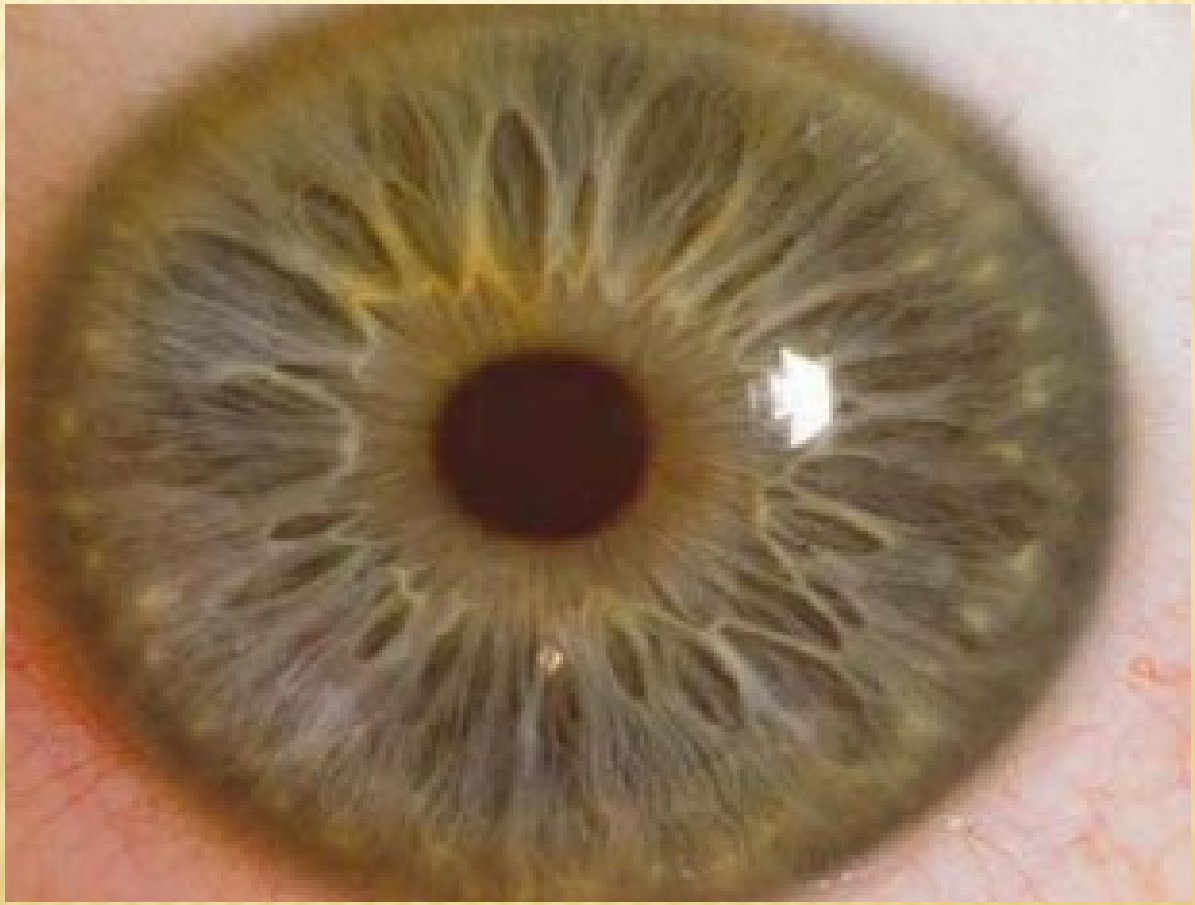


Smart gun

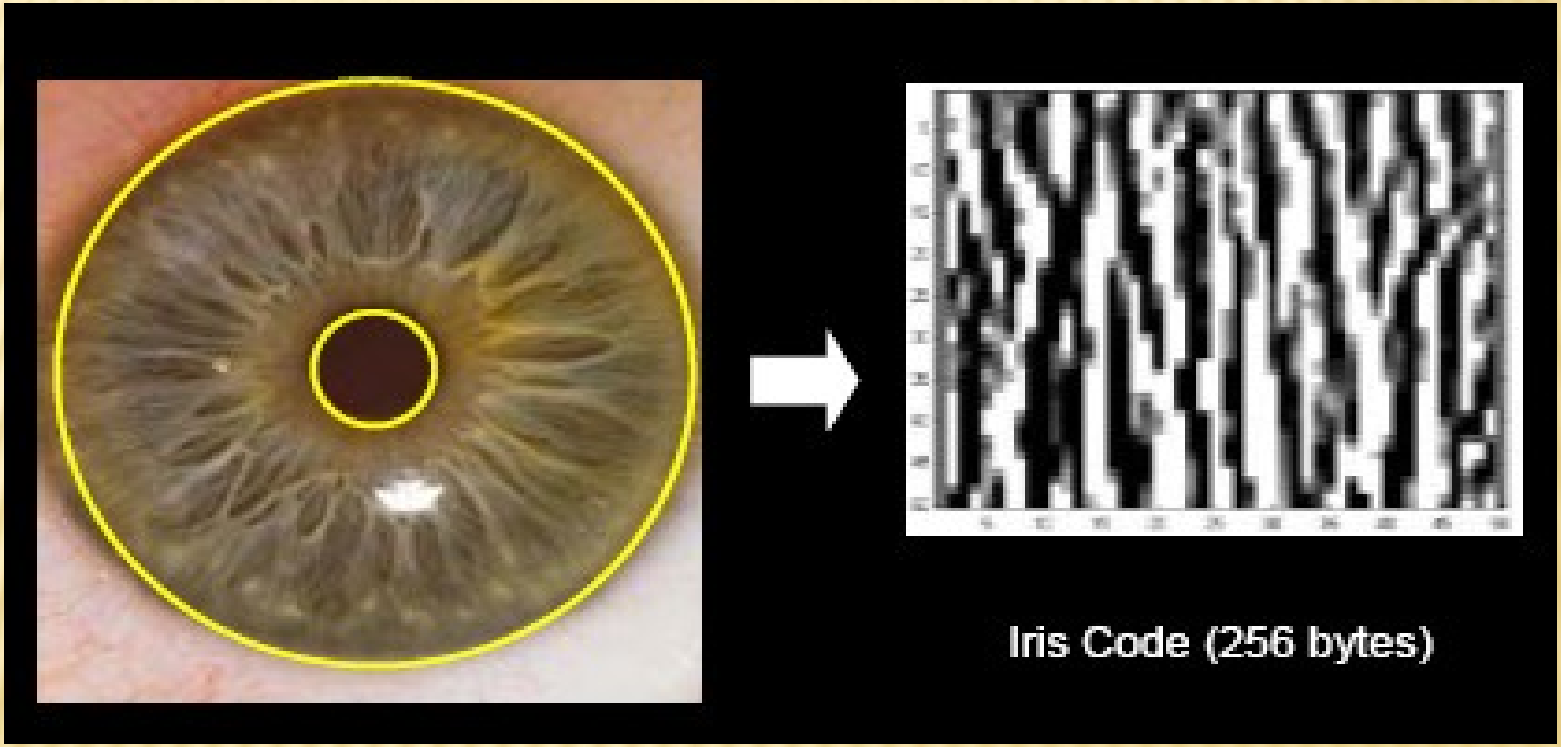
FINGERPRINT FEATURES



IRIS RECOGNITION: EYE

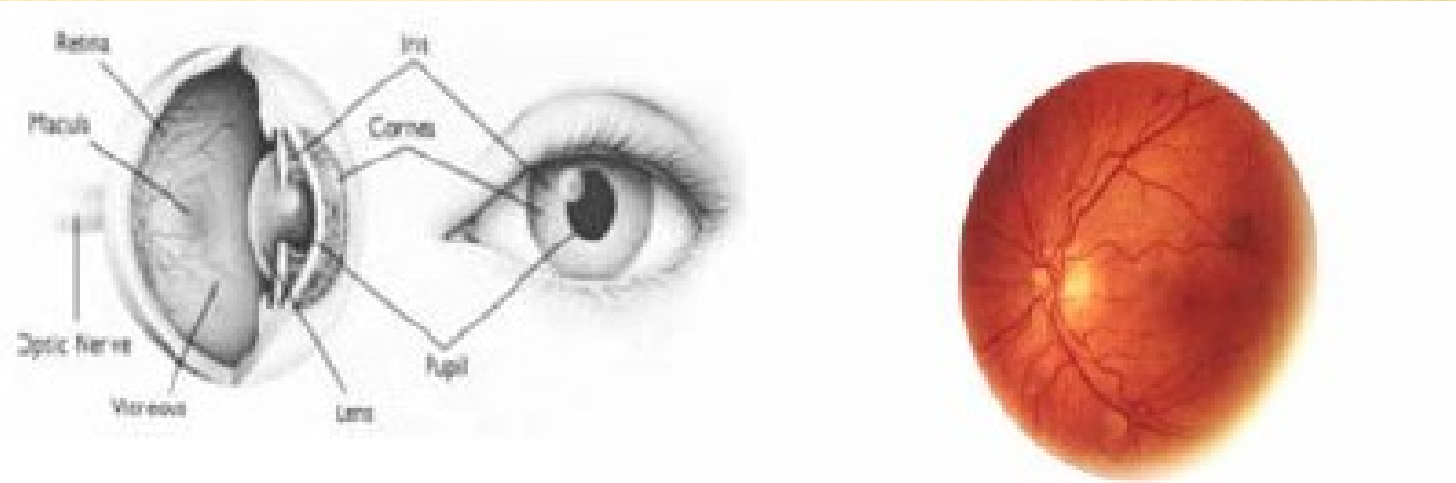


IRIS CODE



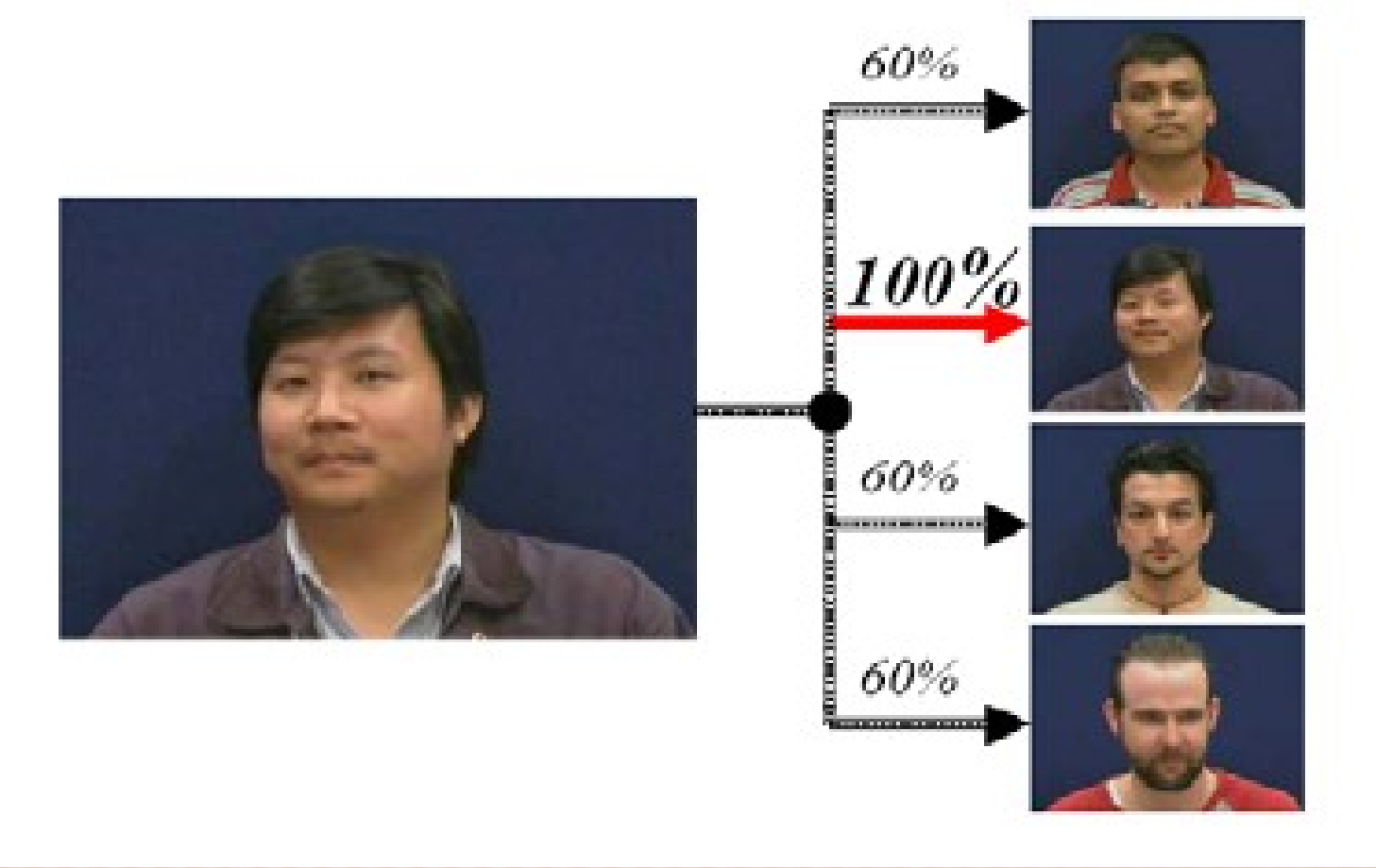
NATIONAL GEOGRAPHIC 1984 AND 2002

RETINA

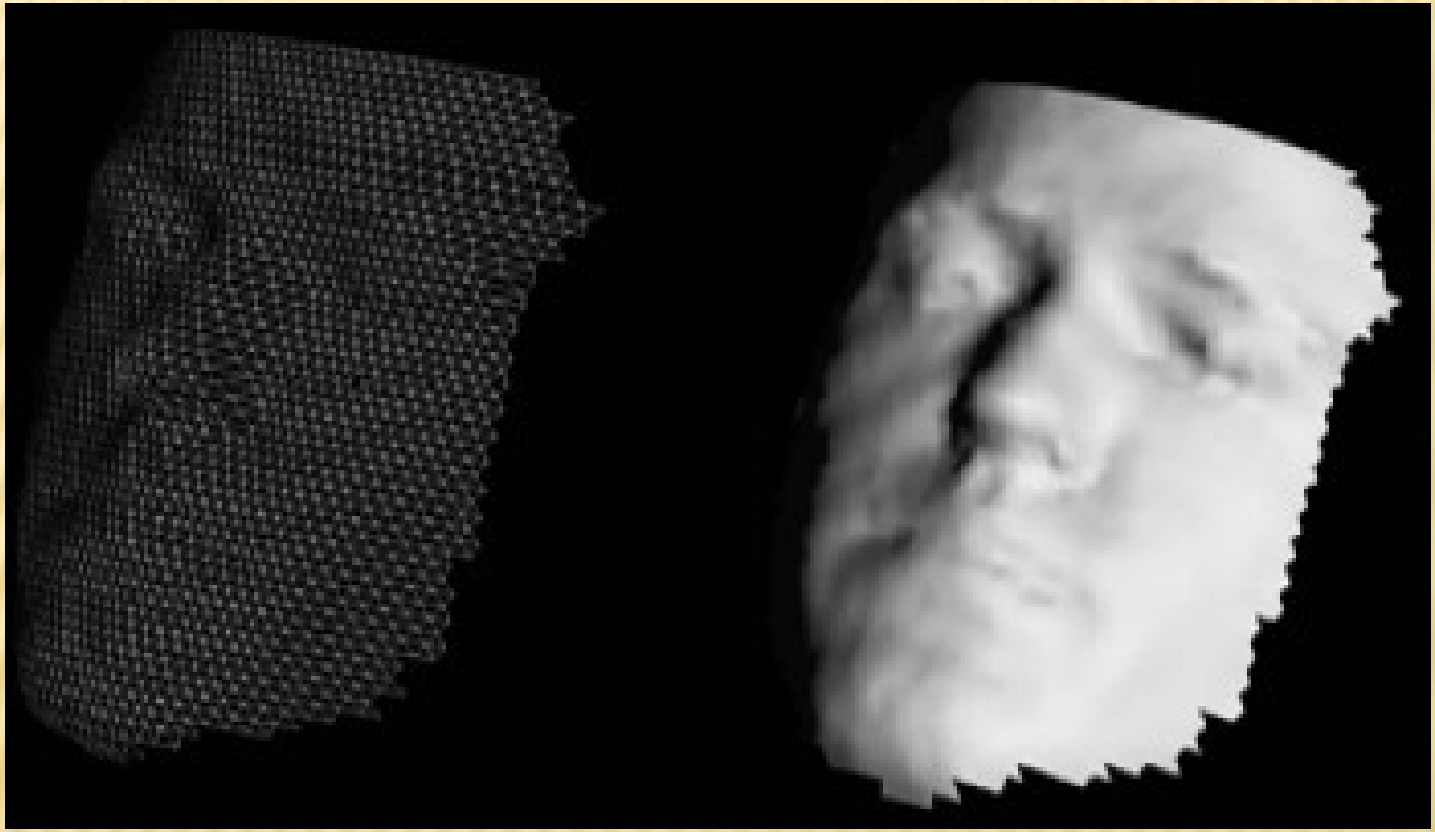


Every eye has its own totally unique pattern of blood vessels.

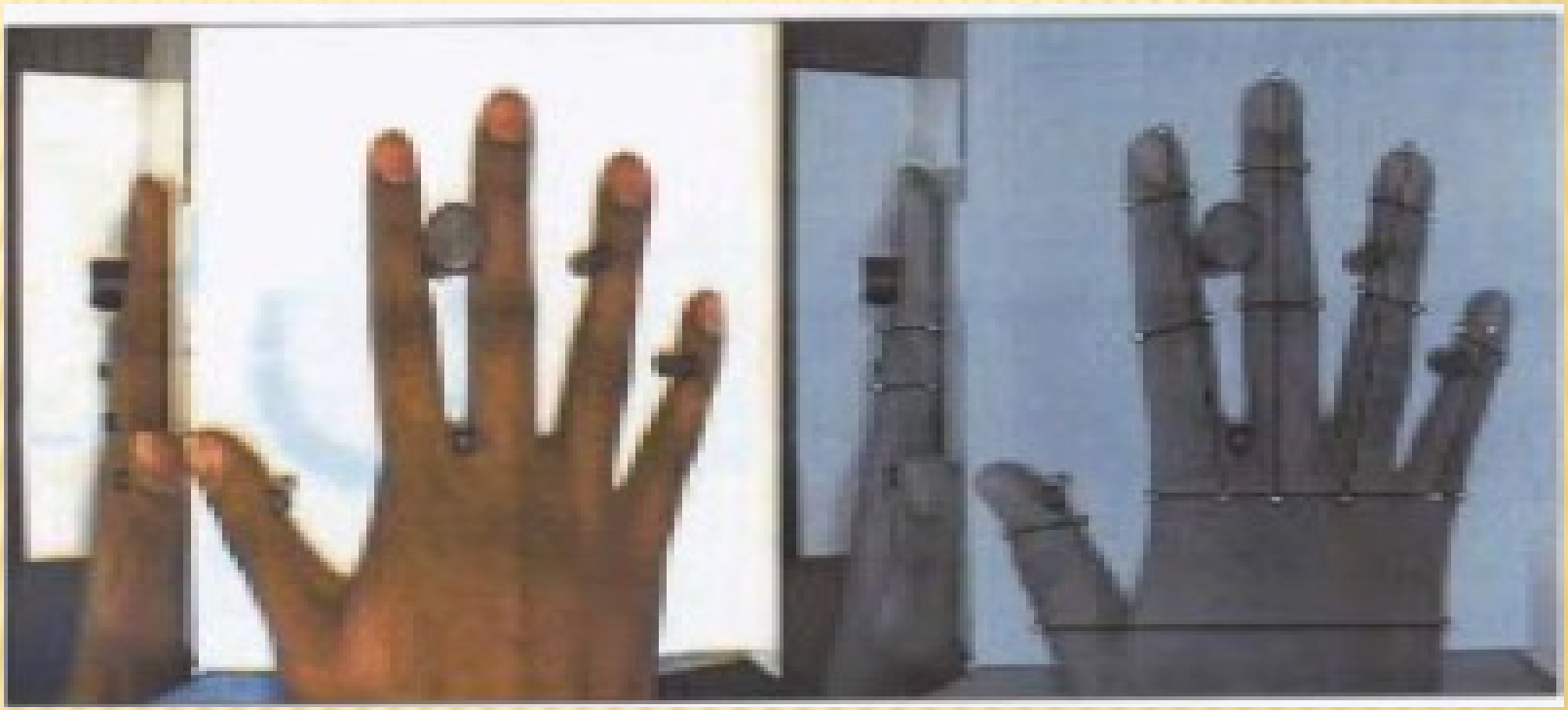
FACE RECOGNITION: CORRELATION



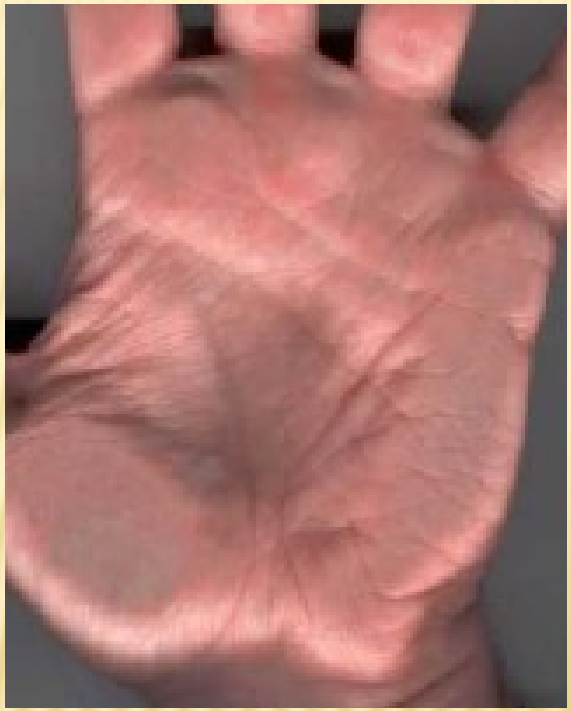
FACE RECOGNITION: 3D



HAND



PALM



VEIN

EAR

MARKET SHARE

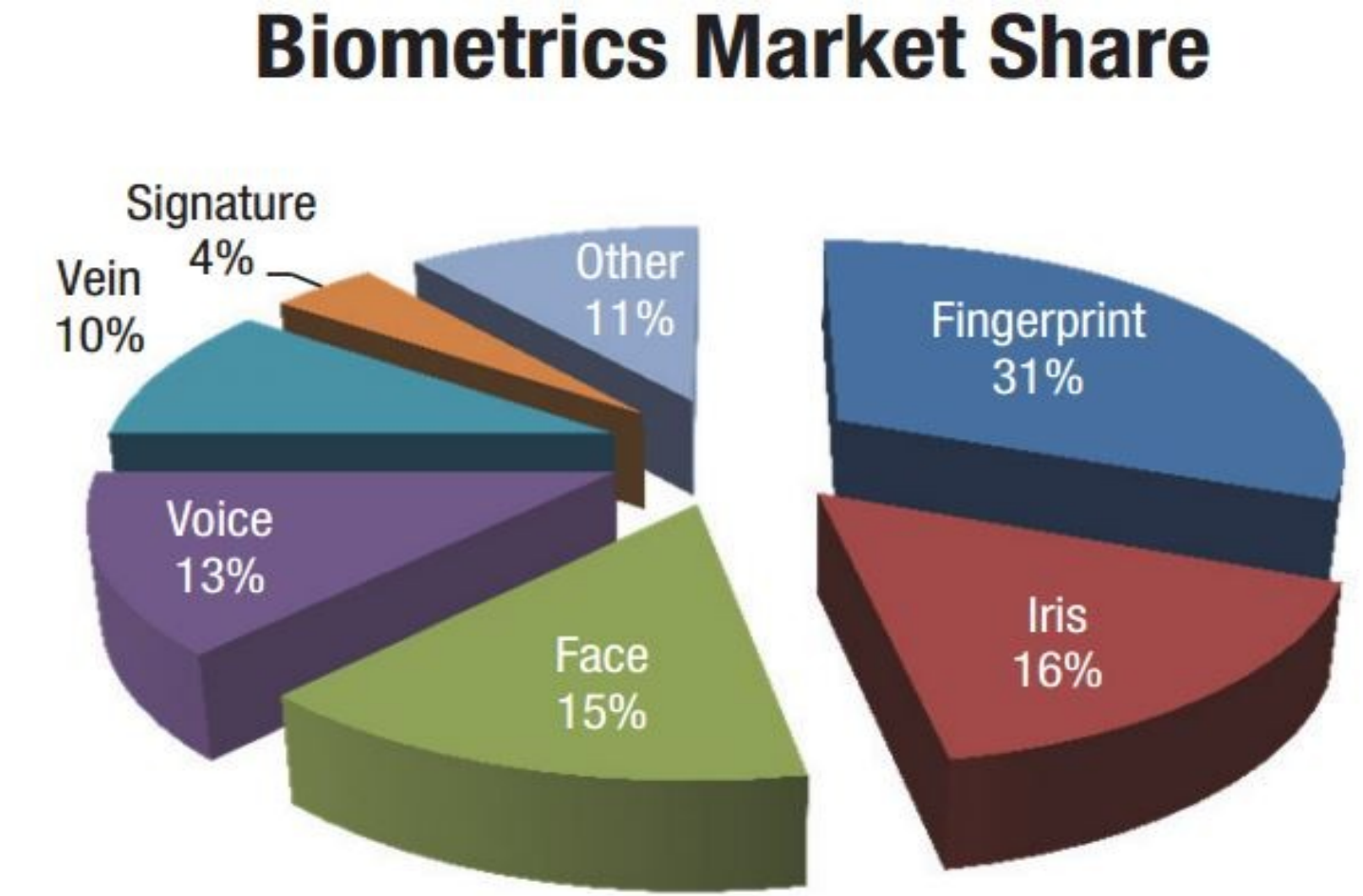


Figure 1: Biometrics market share by system type

BIOMETRIC APPLICATIONS

BIOMETRIC APPLICATION

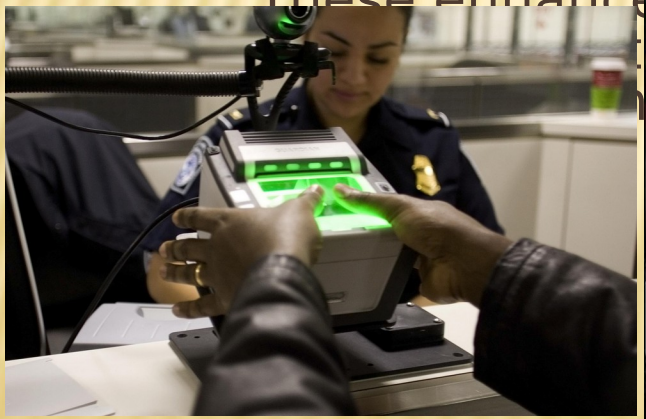
- Biometric technology is used for many applications
  - Providing time and attendance functionality for a small company
  - Ensuring the integrity of a 10 million-person voter registration database
- The benefit of using biometrics include increased security, increased convenience, reduced fraud or delivery of enhanced services.

UCSD BIOMETRIC SODA MACHINE

US-VISIT
www.dhs.gov/us-visit

Homeland Security

*As part of the enhanced procedures, most visitors traveling on visas will have two fingerprints scanned by an inkless device and a digital photograph taken. All of the data and information is then used to assist the border inspector in determining whether or not to admit the traveler. These enhanced procedures



NATIONAL BIOMETRIC ID CARDS

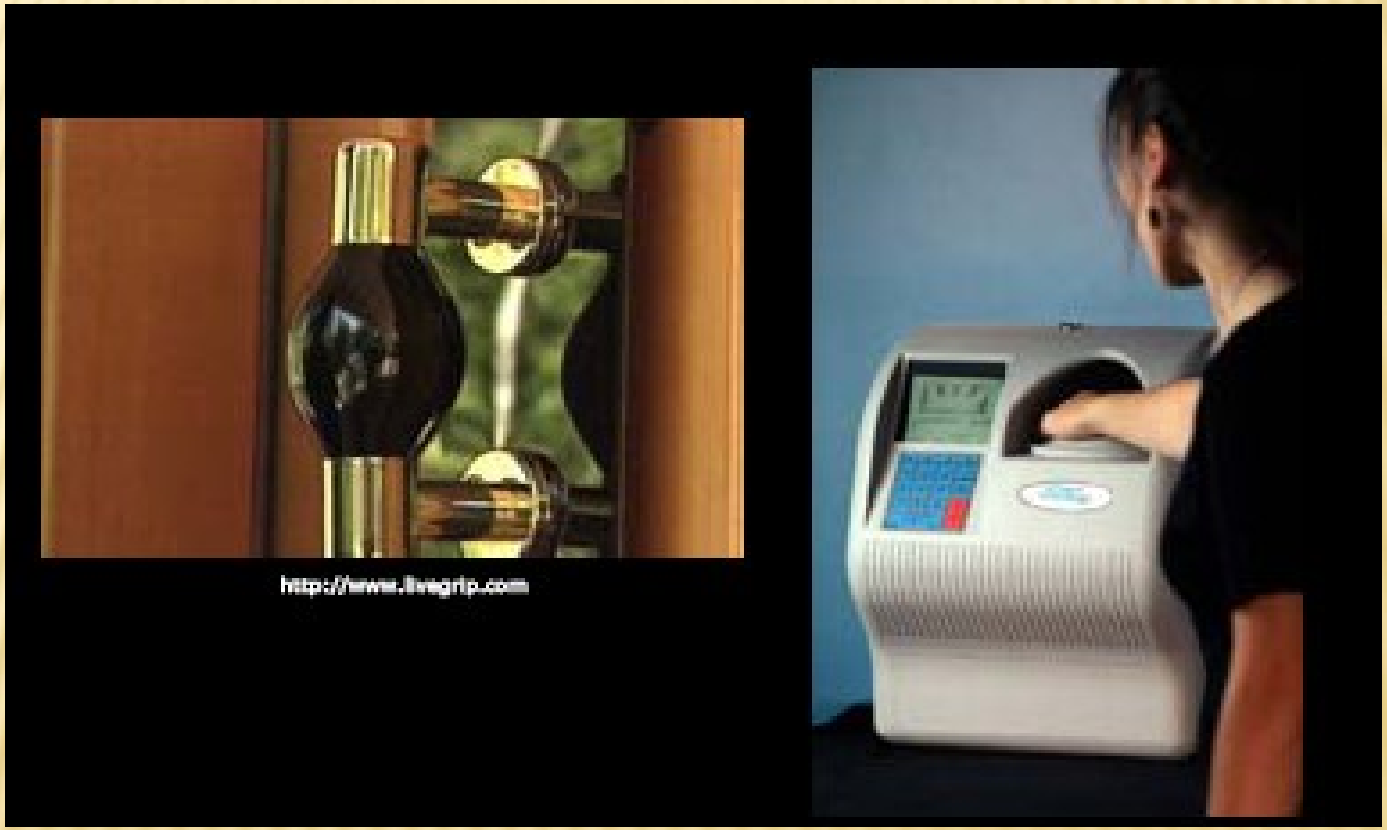
U.K. to consider national biometric ID cards, database

By Laura Rohde, COMPUTERWORLD (Nov 29, 2003)-

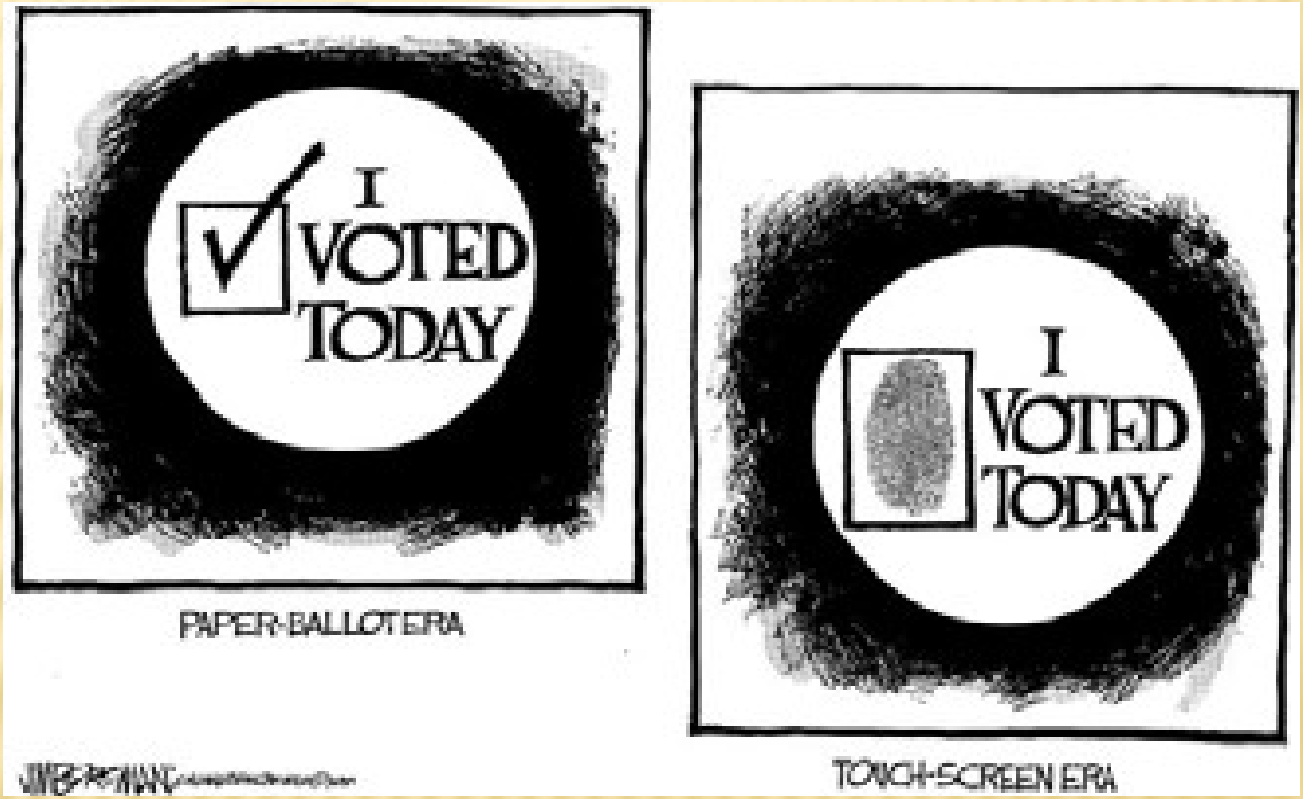
The U.K. government is set to consider legislation next year for the establishment of compulsory biometric identity cards and a central database of all U.K. subjects, it was announced by the government this week.

The information that the government is considering for inclusion on the card includes personal details such as a person's home address and telephone number, his National Insurance number (the equivalent of the U.S. Social Security number), medical information and criminal convictions, as well as the biometric information, most likely in the form of an iris, fingerprint or palm print scan.

ACCESS CONTROL



DID YOU VOTE?


I VOTED TODAY
PAPER-BALLOT ERA
I VOTED TODAY
TOUCH-SCREEN ERA

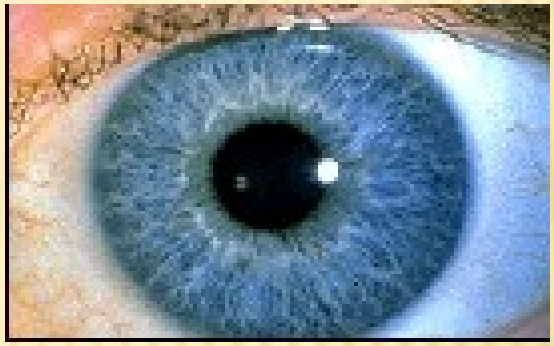
APPLICATIONS

- Video Surveillance (On-line or off-line)

FINGERPRINT SYSTEM AT GAS STATIONS

"Galp Energia SGPS SA of Lisbon won the technology innovation award for developing a payment system in which gasoline-station customers can settle their bills simply by pressing a thumb against a glass pad. Scanning technology identifies the thumbprint and sends the customer's identification information into Galp's back-office system for payment authorization."
THE WALL STREET JOURNAL,
November 15, 2004

USING IRIS SCANS TO UNLOCK HOTEL ROOMS



The Nine Zero hotel in Boston just installed a new system which uses digital photos of the irises of employees, vendors and VIP guests to admit them to certain areas, the same system used in high-security areas at airports such as New York's JFK.

FINGERPRINT SYSTEM AT BORDER CROSSINGS

"Foreigners entering the United State in three cities, including Port Huron, were fingerprinted, photographed and subjected to background checks on Monday in a test of a program that will eventually be extended to every land border crossing nationwide."

Lansing State Journal, Nov. 16, 2004

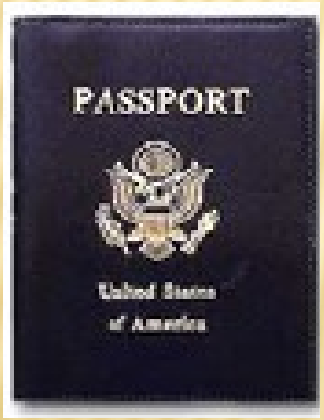
NEW PASSPORTS

"ICAO TAG-MRTD/NTWG RESOLUTION N001 - Berlin, 28 June 2002

ICAO TAG-MRTD/NTWG endorses the use of face recognition as **the globally interoperable biometric** for machine assisted identity confirmation with machine readable travel documents.

ICAO TAG-MRTD/NTWG further recognizes that Member States may elect to use fingerprint and/or iris recognition as additional biometric technologies in support of machine assisted identity confirmation.

***Endorsement:* Unanimous"**



The new passports have an embedded contactless (ISO 14443) "smart-card" chip that stores personal information and a biometric template. Two problems: reliability and privacy

WANT TO CHARGE IT? YOU'LL HAVE TO TALK TO YOUR CREDIT CARD

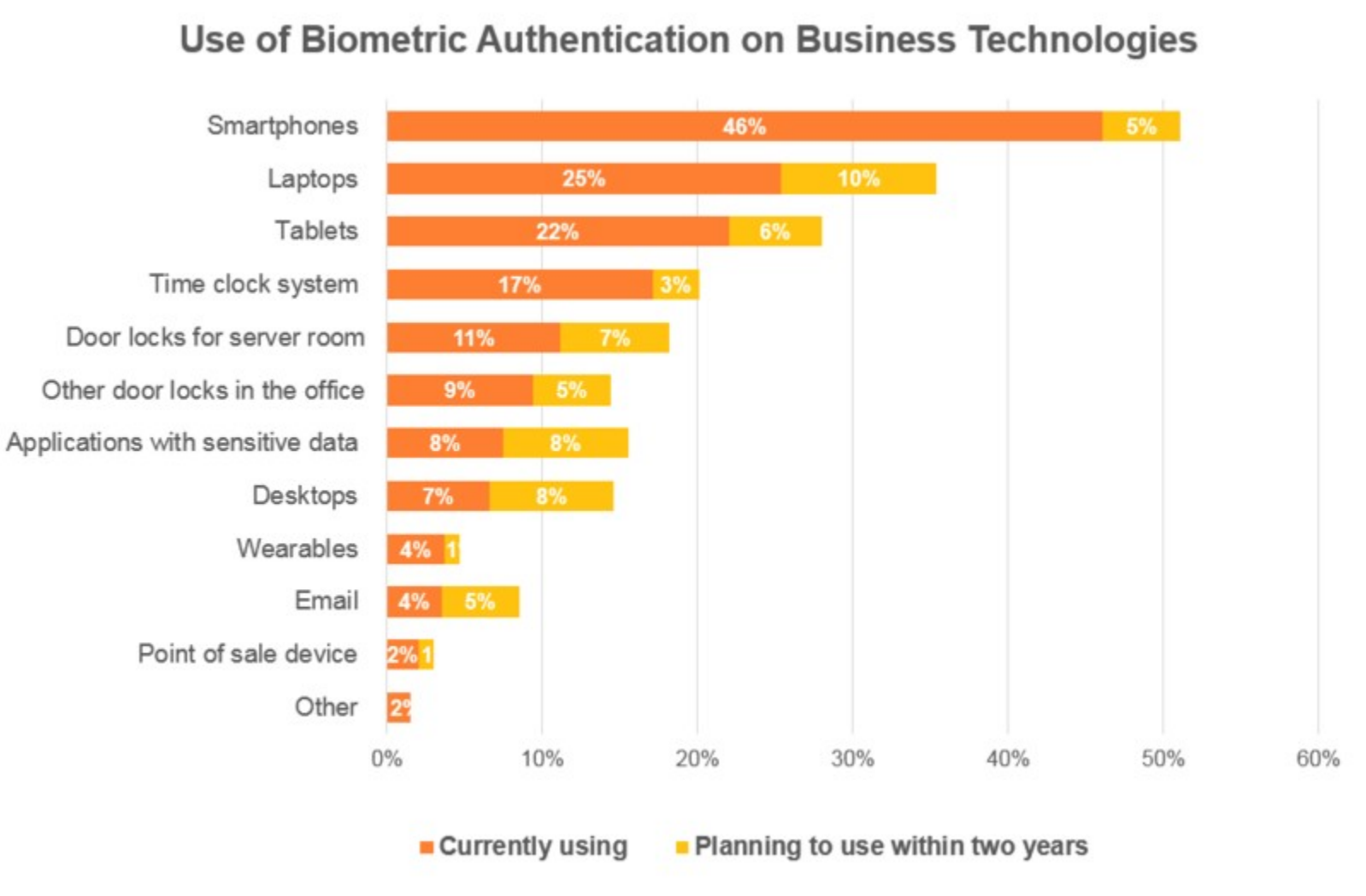
Beepcard, a company in California, has designed a credit card that works only when it recognizes the voice of its rightful owner. Enclosed in the card is a tiny microphone, a loudspeaker and a speech recognition chip that compares the spoken password with a recorded sample. If the voices match, the card emits a set of beeps that authorize a transaction over the telephone or the Internet. If the voices do not match, the card will not beep.

The system tolerates some variations in voice to accommodate cold or background noise. But it might not work if there is a blaring music in the background.

BIOMETRICS FOR PERSONALIZATION

- Automatic personalization of vehicle settings:
  - Seat position
  - Steering wheel position
  - Mirror positions
  - Lighting
  - Radio station preferences
  - Climate control settings
- URLs at your fingertips

DOMAINS OF APPLICATION



KEY TERMS

TEMPLATE (1)

- A template is a small file derived from the distinctive features of a user's biometric data, used to perform biometric matches.
- Templates, is calculated during enrollment or verification phase. The template be understood as a compact representation of the collected feature data, where useless or redundant information is discarded.
- Biometric systems store and compare biometric templates, NOT biometric data.

TEMPLATE (2)

- Most template occupy less than 1 kilobyte, and some of them are as small as 9 bytes; size of template differs from vendor to vendor.
- Templates are proprietary to each vendor and each technology, and there is no common biometric template format.
- This is beneficial from a privacy perspective, but the lack of interoperability deterred some would-be users.

TEMPLATES

- Biometric data CAN NOT be reconstructed from biometric templates.
- Templates are extractions of distinctive features and not adequate to reconstruct the full biometric image or data.
- Unique templates are generated every time a user presents biometric data. For example, two immediately successive placement of a finger on a biometric device generate entirely different templates which are processed by vendor's algorithm and recognizable as being from the same person,but are not identical.

BIOMETRIC TEMPLATES VERSUS IDENTIFIABLE BIOMETRIC DATA

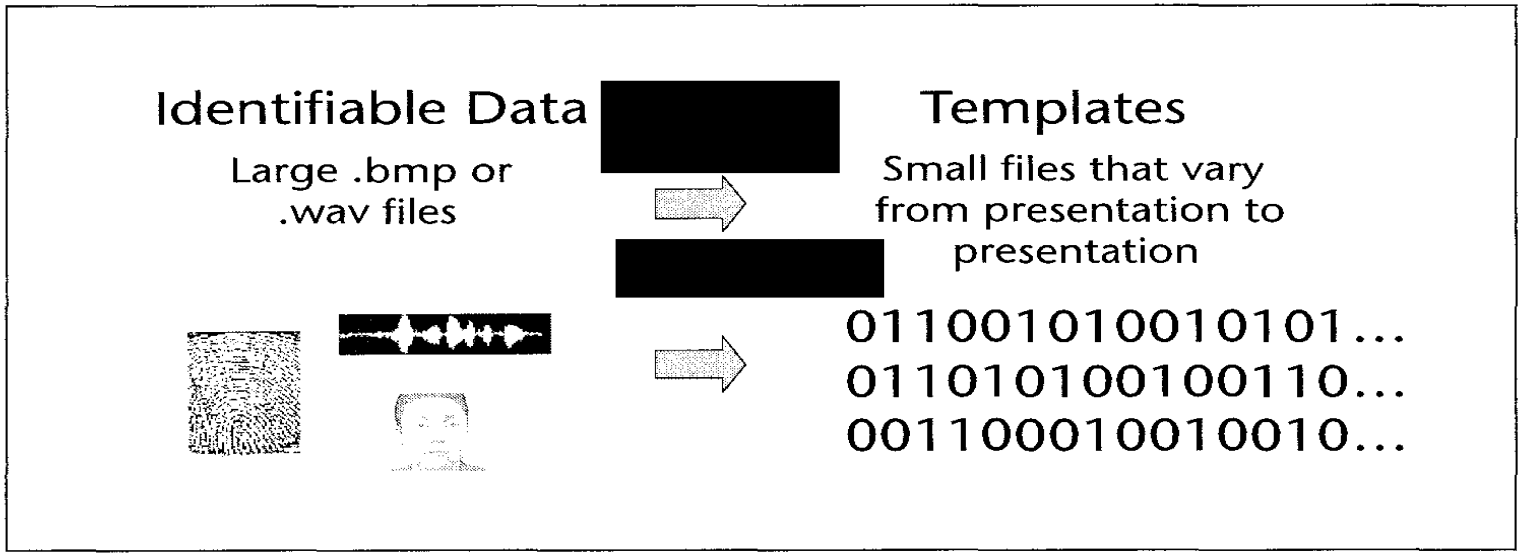
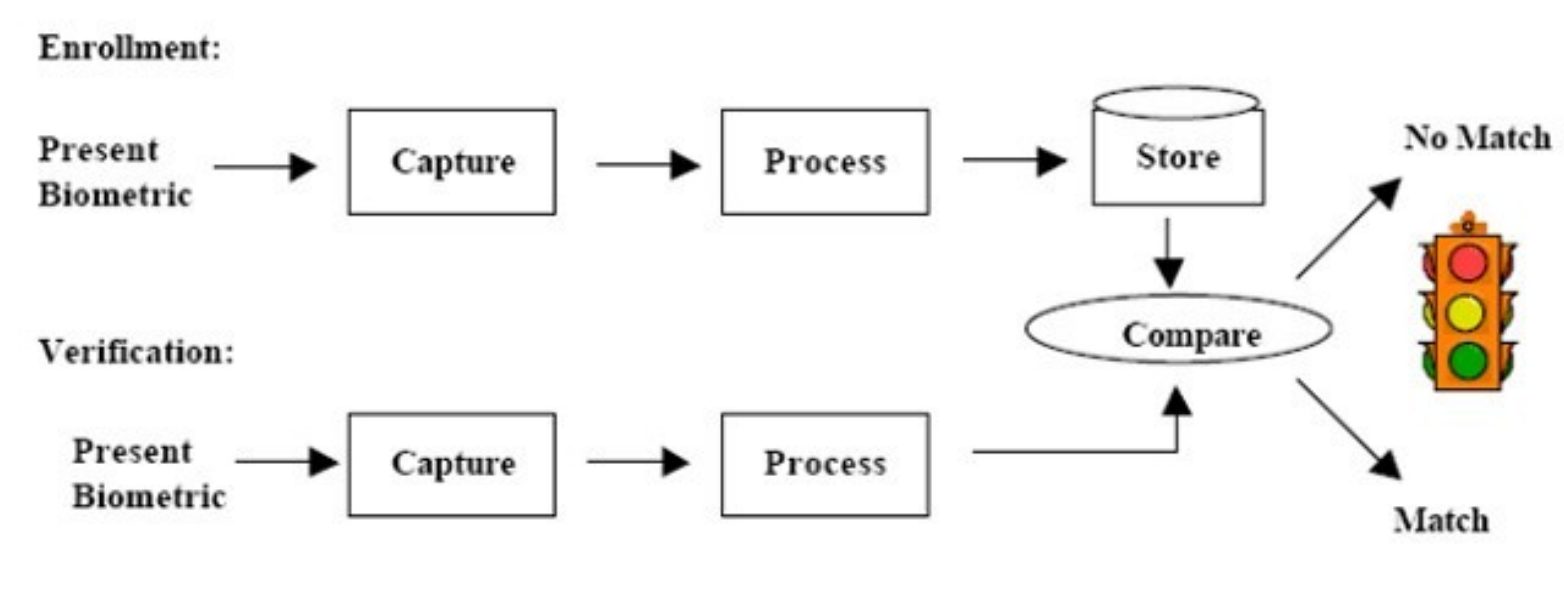


Figure 2.3 Biometric templates versus identifiable biometric data.

Depending on when they are generated, templates can be referred to as enrollment templates or match templates.

THE TWO STAGES OF A BIOMETRIC SYSTEM



ENROLLMENT AND TEMPLATE CREATION (1)

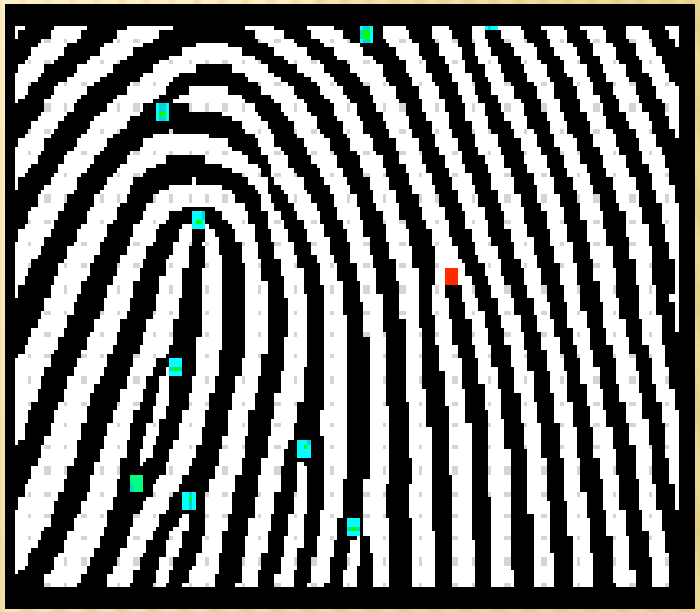
- Enrollment is a process to acquire, assess, process, and store user's biometric data in the form of a template.
- Stored templates are used for subsequent verification and identification.
- Quality enrollment is a critical factor in the long-term accuracy of biometric system.

ENROLLMENT AND TEMPLATE CREATION (2)

- Presentation is the process by which a user provides biometric data to an acquisition device – the hardware used to collect biometric data.
- For example, looking in the direction of a camera, placing a finger on a platen, or reciting a passphrase.

ENROLLMENT AND TEMPLATE CREATION (3)

- Biometric data are converted to templates through feature extraction.
- Feature extraction is the automated process of locating and encoding distinctive characteristics from biometric data in order to generate a template.
- Feature extraction removes noises and unwanted data, and digitize biometric traits.



ENROLLMENT AND TEMPLATE CREATION (4)

- A user may need to present biometric data several times in order to enroll.
- Enrollment score or quality score indicates the enrollment attempt is successful or not.
- If the user's biometric data contains highly distinctive features or an abundance of features, there will likely be a high enrollment score.
- Vendor's feature extraction processes are generally patented and are always held secret.

HOW BIOMETRIC MATCHING WORKS

- Verification/Identification template is compared with enrollment templates.
- The comparison renders a score, or confident value.
- The score is compared with threshold.
- If the score exceeds the threshold, the comparison is a match, non-match otherwise.

BIOMETRIC ALGORITHM

- A biometric algorithm is a recipe for turning raw data - like physical traits – into a digital representation in the form of a template. It also allows the matching of an enrolled template with a new template just created for verifying an identity, called the live template.

BIOMETRIC MATCHING

- Matching is the comparison of enrolled biometric templates with a new template just created for verification to determine their degree of similarity or correlation.
- In verification systems, a verification template is matched against a user's enrollment template or templates (multiple).
- In Identification systems, the verification template is matched against dozens, thousands, even millions of enrollment templates.

BIOMETRIC MATCHING – SCORING

- Biometric systems utilize proprietary algorithms to process templates and generate scores.
- Some of them use a scale of 1 to 100, others use a scale of -1 to 1.
- Traditional authentication methods such as password offer on a yes’/no response.
- In biometric system, there is no 100 percent correlation between enrollment and verification templates.

BIOMETRIC MATCHING –THRESHOLD

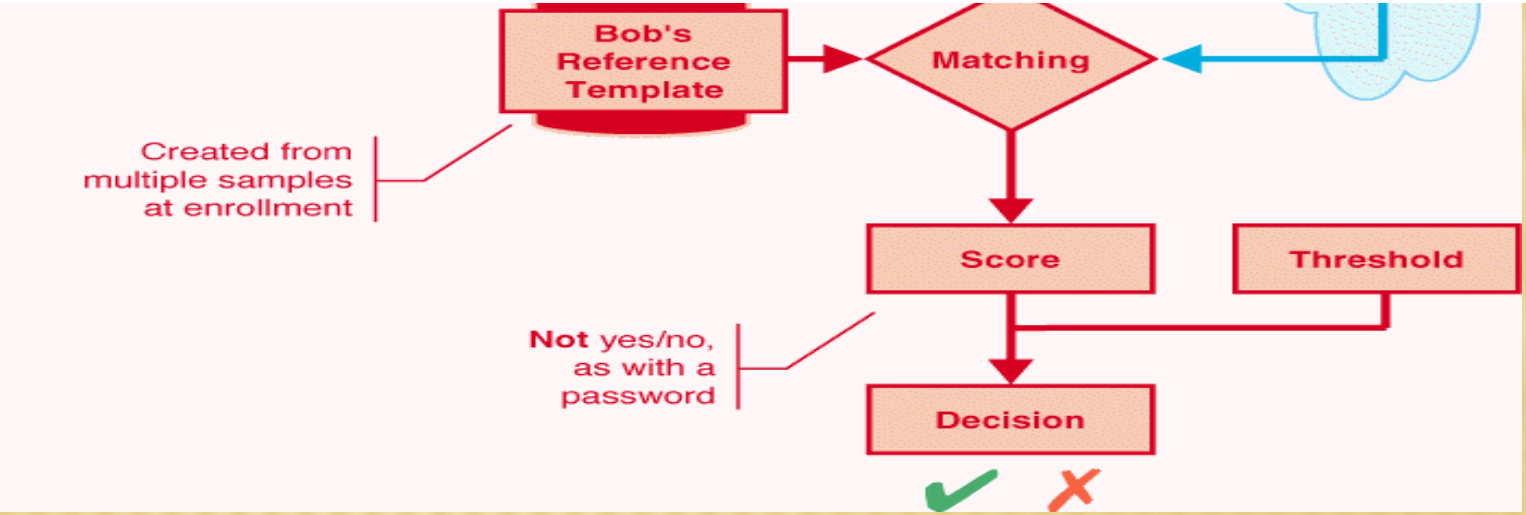
- A threshold is a predefined number, which establishes the degree of correlation necessary for a comparison to be deemed a match.
- Thresholds can vary from user to user, from transaction to transaction, and from verification to verification attempt.
- System can be either highly secure for valuable transaction or less secure for low-value transaction, depending on their threshold settings.
- Traditional authentication can not offer such flexibility.

BIOMETRIC MATCHING – DECISION

- The result of the comparison between the score and the threshold is a decision.
- The decisions a biometric system can make include *match*, *non-match*, and *inconclusive*.

BIOMETRIC MATCHING: PROCESS FLOW

- The user submits a sample (biometric data) via an acquisition device (for example, a scanner or camera)
- This biometric is then processed to extract information about distinctive features to create a trial template or verification template
- Templates are large number sequences. The trial/match template is the user's "password."
- Trial/match template is compared against the reference template stored in biometric database.



OVERVIEW OF BIOMETRICS

Biometric	Acquisition Device	Sample	Feature Extracted
Iris	Infrared-enabled video camera, PC camera	Black and white iris image	Furrows and striations of iris
Fingerprint	Desktop peripheral, PC card, mouse chip or reader embedded in keyboard	Fingerprint image (optical, silicon, ultrasound or touchless)	Location and direction of ridge endings and bifurcations on fingerprint, minutiae
Voice	Microphone, telephone	Voice Recording	Frequency, cadence and duration of vocal pattern
Signature	Signature Tablet, Motion-sensitive stylus	Image of Signature and record of related dynamics measurement	Speed, stroke order, pressure and appearance of signature
Face	Video Camera, PC camera, single-image camera	Facial image (optical or thermal)	Relative position and shape of nose, position of cheekbones
Hand	Proprietary Wall-mounted unit	3-D image of top and sides of hand	Height and width of bones and joints in hands and fingers
Retina	Proprietary desktop or wall mountable unit	Retina Image	Blood vessel patterns and retina

STRENGTHS, WEAKNESSES AND USABILITY OF BIOMETRICS

Biometric	Strengths	Weakness	Usability
Iris	• Very stable over time • Uniqueness	• Potential user resistance • Requires user training • Dependant on a single vendor's technology	• Information security access control, especially for Federal Institutions and government agencies • Physical access control (FIs and government) • Kiosks (ATMs and airline tickets)
Fingerprint	• Most mature biometric technology • Accepted reliability • Many vendors • Small template (less than 500 bytes) • Small sensors that can be built into mice, keyboards or portable devices	• Physical contact required (a problem in some cultures) • Association with criminal justice • Vendor incompatibility • Hampered by temporary physical injury	• IS access control • Physical access control • Automotive
Optical	• Most proven over time • Temperature stable	• Large physical size • Latent prints • CCD coating erodes with age • Durability unproven	

STRENGTHS, WEAKNESSES AND USABILITY OF BIOMETRICS

Biometrics	Strengths	Weakness	Usability
Silicon	• Small physical size • Cost is declining	• Requires careful enrollment • Unproven in sub optimal conditions	
Ultrasound	• Most accurate in sub optimal conditions	• New technology, few implementations • Unproven long term performance	
Voice	• Good user acceptance • Low training • Microphone can be built into PC or mobile device	• Unstable over time • Changes with time, illness stress or injury • Different microphones generate different samples • Large template unsuitable for recognition	• Mobile phones • Telephone banking and other automated call centers
Signatures	• High user acceptance • Minimal training	• Unstable over time • Occasional erratic variability • Changes with illness, stress or injury • Enrollment takes times	• Portable devices with stylus input • Applications where a “wet signature” ordinarily would be used.

STRENGTHS, WEAKNESSES AND USABILITY OF BIOMETRICS

Biometrics	Strengths	Weakness	Usability
Face	• Universally present	• Cannot distinguish identical siblings • Religious or cultural prohibitions	• Physical access control
Hand	• Small template (approximately 10 bytes) • Low failure to enroll rate • Unaffected by skin condition	• Physical size of acquisition device • Physical contact required • Juvenile finger growth • Hampered by temporary physical injury	• Physical access control • Time and attendance
Retina	• Stable over time • Uniqueness	• Requires user training and cooperation • High user resistance • Slow read time • Dependent on a single vendor's technology	• IS access control, especially for high security government agencies • Physical access control (same as IS access control)

ACCURACY IN BIOMETRIC SYSTEMS

HOW TO EVALUATE PERFORMANCE OF A SPECIFIC TECHNOLOGY?

- False acceptance rate
- False rejection rate
- Failure-to-enroll rate
- No single metric indicates how well a biometric system or device performs: Analysis of all three metrics is necessary to assess the performance of a specific technology.

FALSE ACCEPTANCE RATE

- If John Smith enters Jane Doe's username or ID, presents biometric data, and successfully matching as Jane Doe.
- This is classified as false acceptance.
- The probability of this happening is referred to as false acceptance rate (FAR)[stated as: percentage, fraction]
- This is because two people have *similar enough biometric characteristics* – a fingerprint, a voice, or a face – that the system finds a *high degree of correlation* between the users' template.

FALSE ACCEPTANCE RATE

- FAR can be *reduced* by adjusting the thresholds but the false rejection rate will increase.
- A system with a false acceptance rate of *0 percent*, but false rejection rate of *50 percent*, is secure but unusable.
- False acceptance rate is the most critical accuracy metric because an imposter break-in will certainly be a more attention-getting event than other failings of a biometric system.
- The most important false match metric in real-world deployments is the *system false match rate*.

FALSE REJECTION RATE

- If John Smith enters his username or ID, presents his biometric data to a biometric system, and fails to match.
- This is classified as false rejection.
- The probability of this happening is the false rejection rate (FRR).
- This can be attributed to changes in user's biometric data, changes in how a user presents biometric data, and changes in the environment in which data is presented.
- High FRR will result in lost productivity, frustrated users, and an increased burden on help desk or support personnel.

REASONS OF FRR

- Changes in user’s biometric data
  - Voice-scan system is influenced by sore throats
  - Facial-scan system is affected by changes in weight
  - Fingerprint changes over time, scars, aging and general wear.

ACCEPTANCE AND REJECTIONS

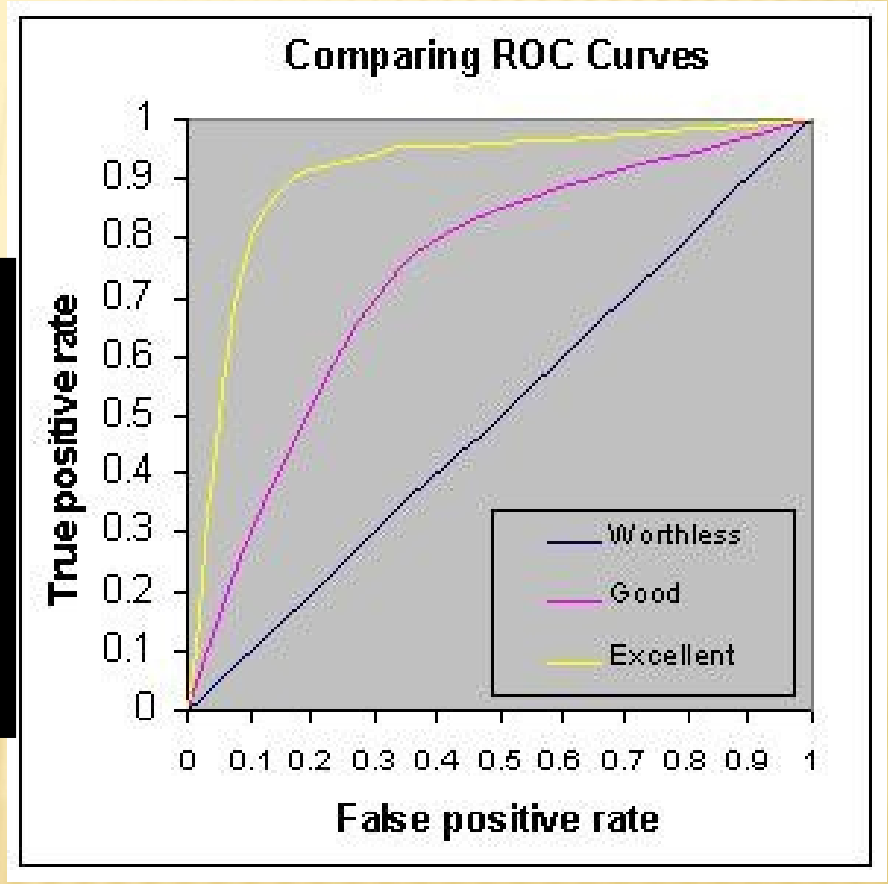
- If someone else is trying to verify as you, the system would try to match the two templates.
  - If the two templates were to match – this is classified as false acceptance.
  - If your authentication template fails to match your enrolled template, then this is referred to as a false rejection.
  - If you are new and fail to enroll to a biometric system, this is called – failure to enroll (FTE).

ACCURACY RATES

- Single False Acceptance Rate vs. System False Acceptance Rate
  - If the FAR is 1/10,000 but you have 10,000 templates on file — odds of a match are very high
- Ability to Verify (ATV) rate:
  - % of user population that can be verified
  - ATV = (1-FTE)(1-FRR)

RECEIVER OPERATING CHARACTERISTIC (ROC) CURVE

- Cost/benefit analysis of decision making.
- Tradeoff b/w true acceptance rate and false rejection rate.



Legitimate users get accepted. → True acceptance rate

Legitimate users get rejected. → False rejection rate

THE FUTURE OF BIOMETRICS

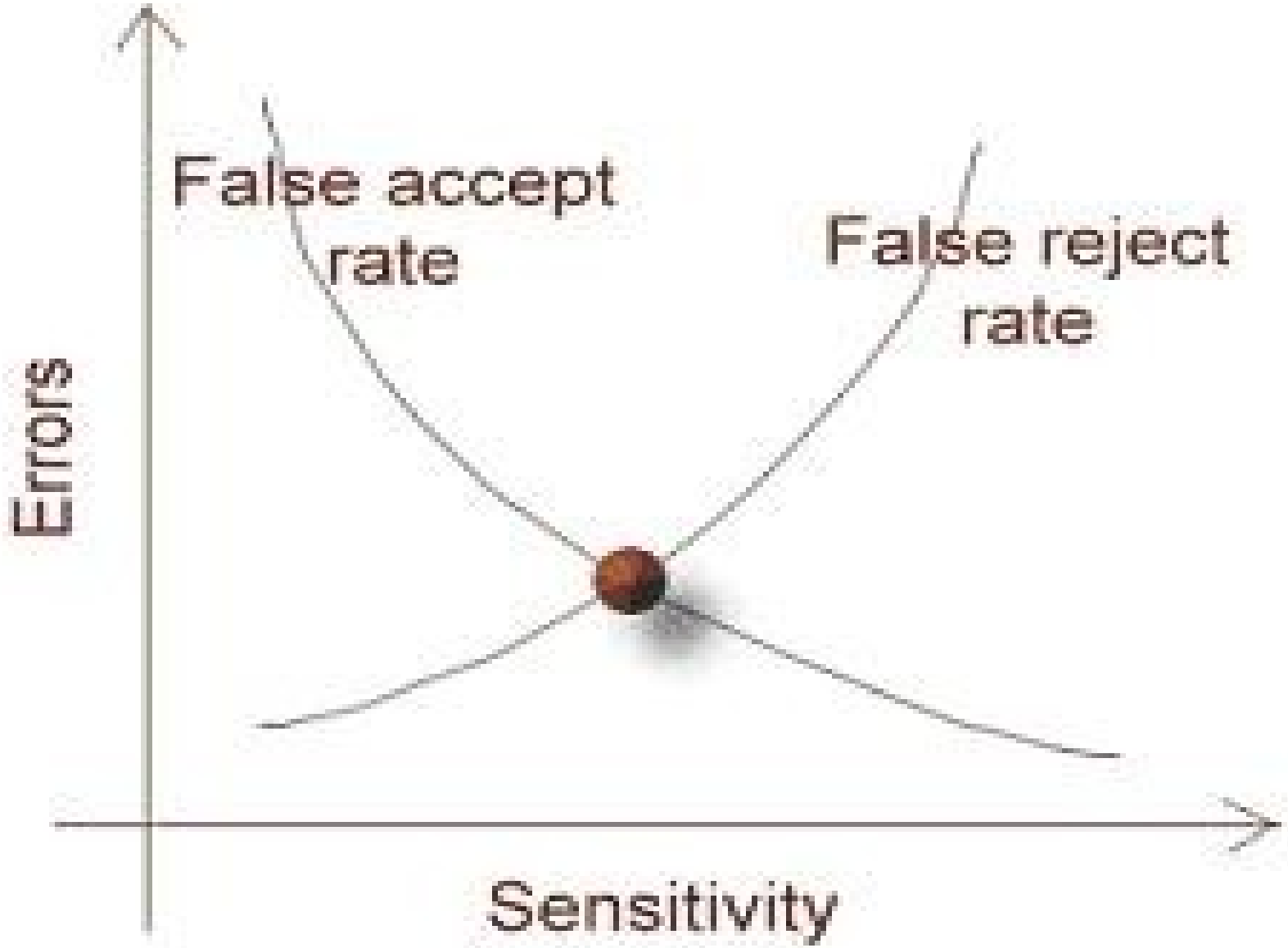
OPERATION AND PERFORMANCE

- In a typical IT biometric system, a person registers with the system when one or more of his physical and behavioral characteristics are obtained. This information is then processed by a numerical algorithm, and entered into a database.
- The algorithm creates a digital representation of the obtained biometric – a template.
- If the user is new to the system, he or she enrolls, which means that the digital template of the biometric is entered into the database.
- Each subsequent attempt to use the system, or authenticate, requires the biometric of the user to be captured again, and processed into a digital template. That template is then compared to those existing in the database to determine a match.
- The process of converting the acquired biometric into a digital template for comparison is completed each time the user attempts to authenticate to the system.
- The comparison process involves the use of a Hamming distance. This is a measurement of how similar two bit strings are.

- For example, two identical bit strings have a Hamming Distance of zero, while two totally dissimilar ones have a Hamming Distance of one.
- Thus, the Hamming distance measures the percentage of dissimilar bits out of the number of comparisons made.
  - Ideally, when a user logs in, nearly all of his/her features match;
  - However, if someone else tries to log in, who does not fully match, the system will not allow the new person to log in.
- Current technologies have widely varying Equal Error Rates, varying from as low as 60% and as high as 99.9%.

- Performance of a biometric measure is usually referred to in terms:
  - false accept rate (FAR)- percent of invalid users who are incorrectly accepted as genuine users,
  - false non match or reject rate (FRR)- percent of valid users who are rejected as impostors ,
  - failure to enroll rate (FTE or FER).
- In real-world biometric systems the FAR and FRR can typically be traded off against each other by changing some parameter.

- One of the most common measures of real-world biometric systems is the rate at which both accept and reject errors are equal:
  - the equal error rate (EER),
  - also known as the cross-over error rate (CER).
- The lower the EER or CER, the more accurate the system is considered to be.
- An EER is desirable for a biometric system because it balances the sensitivity of the system.


False accept rate
False reject rate
Errors
Sensitivity

Biometrics	Univer-sality	Unique-ness	Perma-nence	Collect-ability	Perfor-mance	Accept-ability	Circum-vention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke Dynamics	L	L	L	M	L	M	M
Hand vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial Thermogram	H	H	L	H	M	H	H
DNA	H	H	H	L	H	L	L

H=High, M=Medium, L=Low

ISSUES AND CONCERNS

- Excessive concern with the biometric may have the an eclipsing effect on the performance of the technology that one could:
  - plant DNA at the scene of the crime
  - associate another's identity with his biometrics, thereby impersonating without arousing suspicion
  - interfere with the interface between a biometric device and the host system, so that a "fail" message gets converted to a "pass".

IDENTITY THEFT AND PRIVACY ISSUES

- Concerns about Identity theft through biometrics use have not been resolved. If their iris scan is stolen, though, and it allows someone else to access personal information or financial accounts, the damage could be irreversible.
- Often, biometric technologies have been rolled out without adequate safeguards for personal information gathered about individuals.
- Also, the biometric solution to identity theft is only as good as the information in the database that is used for verifying identity.
- There are problems of getting accurate and usuable initial information (enrollment) -- witness the current troubles with the No fly list of the Dept of Homeland security.
- Presumably after the initial information is correctly stored, future computer error or vandalism (hacking) would prevent biometrics from being 100% foolproof against identity theft.
- Because biometrics are touted as a way to restrict criminality, privacy advocates fear biometrics may be used to diminish personal liberties of law abiding citizens as well.
- .

SOCIOLOGICAL CONCERNS

- As technology advances, more private companies and public utilities are using biometrics for safe, accurate identification. However, these advances are raising more concerns like:
  - Physical - Some believe this technology can cause physical harm to an individual using the methods, or that instruments used are unsanitary. For example, there are concerns that retina scanners might not always be clean.
  - Personal Information - There are concerns whether our personal information taken through biometric methods can be misused, tampered with, or sold, e.g. by criminals stealing, rearranging or copying the biometric data. Also, the data obtained using biometrics can be used in unauthorized ways without the individual's consent.
- Society fears in using biometrics will continue over time. As the public becomes more educated on the practices, and the methods are being more widely used, these concerns will become more and more evident.
- This technology is being used at border crossings that have electronic readers that are able to read the chip in the cards and verify the information present in the card and on the passport.
- This method allows for the increase in efficiency and accuracy of identifying people at the border crossing. CANPASS, by Canada Customs is currently being used by some major airports that have kiosks set up to take digital pictures of a person’s eye as a means of identification.

CONCLUSIONS

- Despite these misgivings, biometric systems have the potential to identify individuals with a very high degree of certainty.
- Forensic DNA evidence enjoys a particularly high degree of public trust at present
- Also substantial claims are being made in respect of iris recognition technology, which has the capacity to discriminate between individuals with identical DNA, such as monozygotic twins.

Developed and Presented By Dr. Mehrdad Sepehri Sharbaf
CSUDH
Computer Science Department

http://csc.csudh.edu/

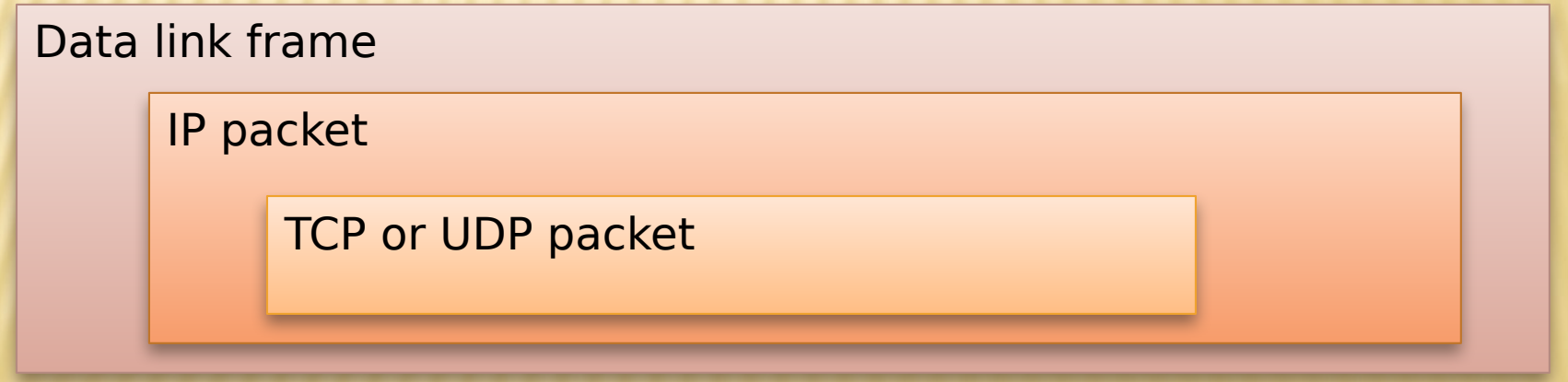
The some of the materials are excerpted from Michael T. Goodrich & Roberto Tamassia,'s Book, and Ross Anderson's Book

ATTACK ON NETWORK AND DEFENSE

NETWORKS: IP AND TCP

INTERNET PROTOCOL

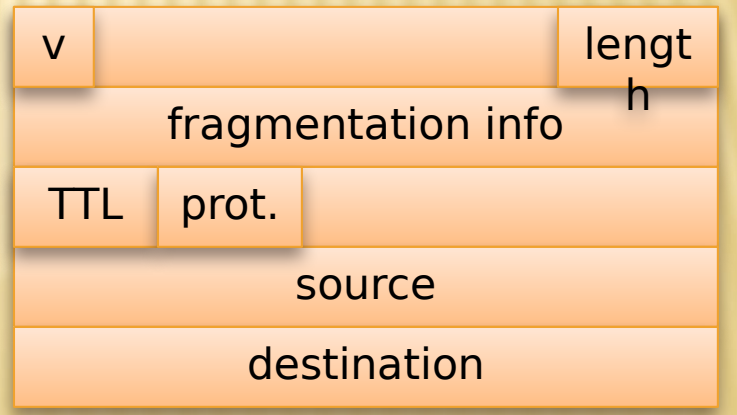
- Connectionless
  - Each packet is transported independently from other packets
- Unreliable
  - Delivery on a best effort basis
  - No acknowledgments
  - Packets may be lost, reordered, corrupted, or duplicated
- IP packets
  - Encapsulate TCP and UDP packets
  - Encapsulated into link-layer frames



IP ADDRESSES AND PACKETS

- IP addresses
  - IPv4: 32-bit addresses
  - IPv6: 128-bit addresses
- Address subdivided into network, subnet, and host
  - E.g., 128.148.32.110
- Broadcast addresses
  - E.g., 128.148.32.255
- Private networks
  - not routed outside of a LAN
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16

- IP header includes
  - Source address
  - Destination address
  - Packet length (up to 64KB)
  - Time to live (up to 255)
  - IP protocol version
  - Fragmentation information
  - Transport layer protocol information (e.g., TCP)



IP ADDRESS SPACE AND ICANN

- Hosts on the internet must have unique IP addresses
- Internet Corporation for Assigned Names and Numbers
  - International nonprofit organization
  - Incorporated in the US
  - Allocates IP address space
  - Manages top-level domains
- Historical bias in favor of US corporations and nonprofit organizations

- Examples

003/8 May 94 General Electric
009/8 Aug 92 IBM
012/8 Jun 95 AT&T Bell Labs
013/8 Sep 91 Xerox Corporation
015/8 Jul 94 Hewlett-Packard
017/8 Jul 92 Apple Computer
018/8 Jan 94 MIT
019/8 May 95 Ford Motor
040/8 Jun 94 Eli Lily
043/8 Jan 91 Japan Inet
044/8 Jul 92 Amateur Radio Digital
047/8 Jan 91 Bell-Northern Res.
048/8 May 95 Prudential Securities
054/8 Mar 92 Merck
055/8 Apr 95 Boeing
056/8 Jun 94 U.S. Postal Service

A TYPICAL UNIVERSITY'S IP SPACE

- Most universities separate their network connecting dorms and the network connecting offices and academic buildings
- Dorms
  - Class B network 138.16.0.0/16 (64K addresses)
- Academic buildings and offices
  - Class B network 128.148.0.0/16 (64K addresses)
- CS department
  - Several class C (/24) networks, each with 254 addresses

IP ROUTING

- A router bridges two or more networks
  - Operates at the network layer
  - Maintains tables to forward packets to the appropriate network
  - Forwarding decisions based solely on the destination address
- Routing table
  - Maps ranges of addresses to LANs or other gateway routers

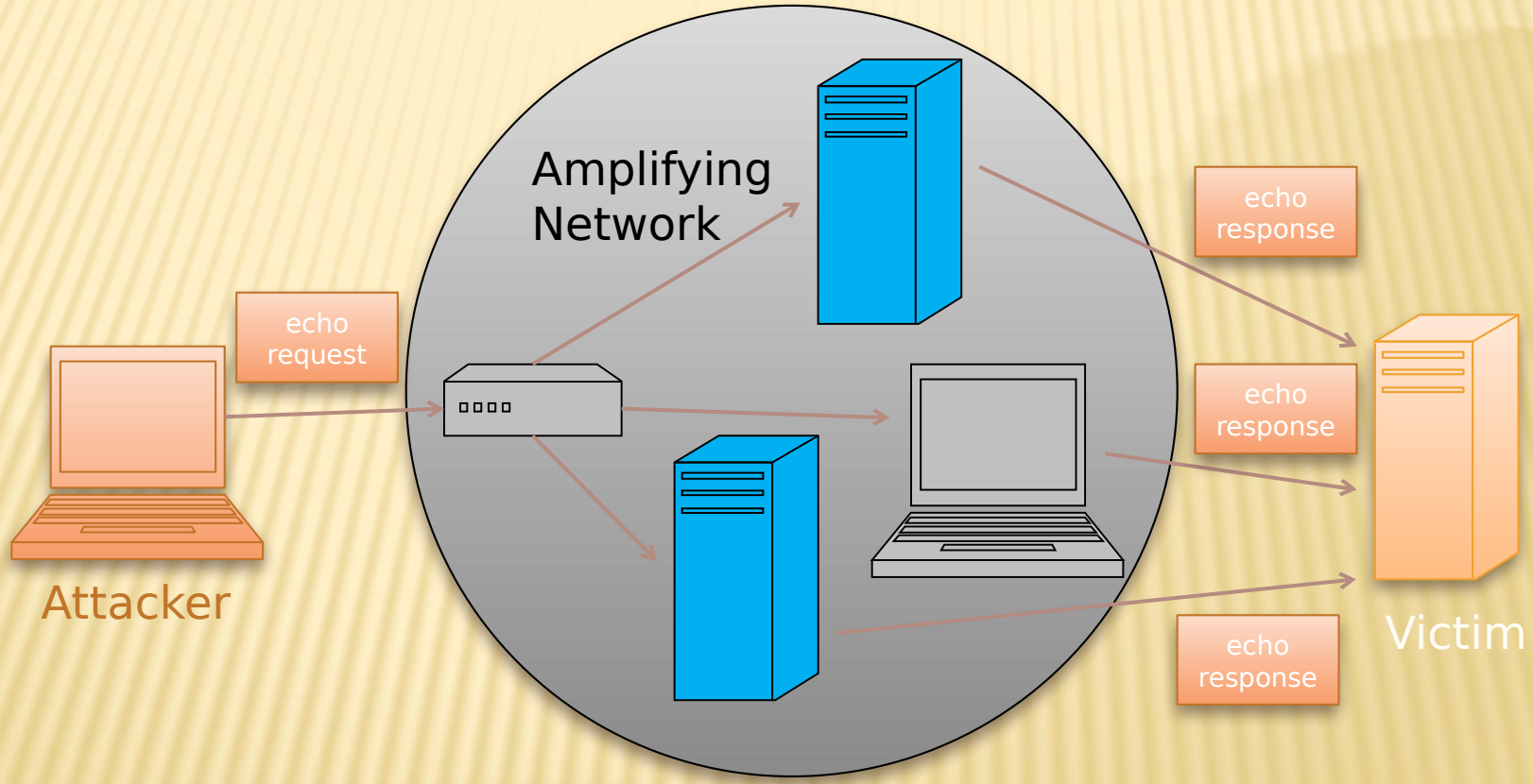
INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

- Internet Control Message Protocol (ICMP)
  - Used for network testing and debugging
  - Simple messages encapsulated in single IP packets
  - Considered a network layer protocol
- Tools based on ICMP
  - Ping: sends series of echo request messages and provides statistics on roundtrip times and packet loss
  - Traceroute: sends series ICMP packets with increasing TTL value to discover routes

ICMP ATTACKS

- Ping of death
  - ICMP specifies messages must fit a single IP packet (64KB)
  - Send a ping packet that exceeds maximum size using IP fragmentation
  - Reassembled packet caused several operating systems to crash due to a buffer overflow
- Smurf
  - Ping a broadcast address using a spoofed source address

SMURF ATTACK



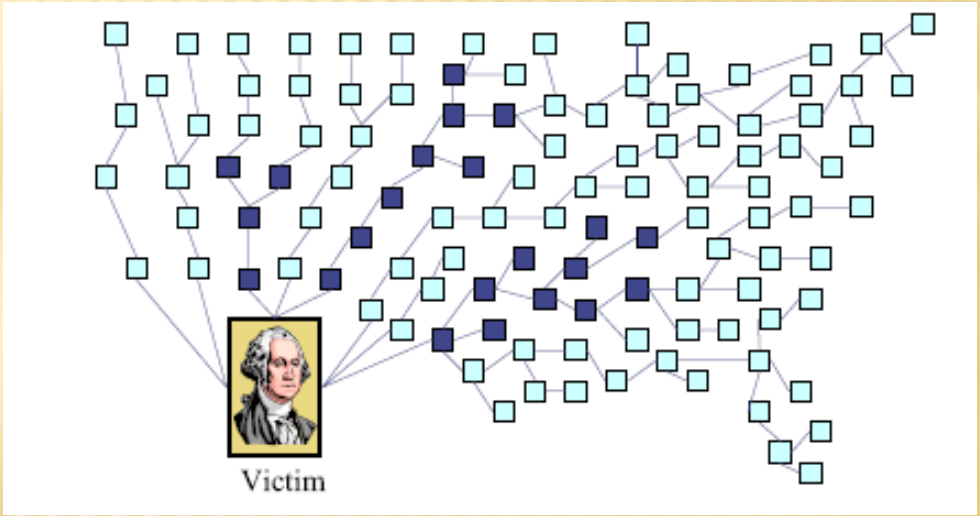
IP VULNERABILITIES

- Unencrypted transmission
  - Eavesdropping possible at any intermediate host during routing
- No source authentication
  - Sender can spoof source address, making it difficult to trace packet back to attacker
- No integrity checking
  - Entire packet, header and payload, can be modified while en route to destination, enabling content forgeries, redirections, and man-in-the-middle attacks
- No bandwidth constraints
  - Large number of packets can be injected into network to launch a denial-of-service attack
  - Broadcast addresses provide additional leverage

DENIAL OF SERVICE ATTACK

- Send large number of packets to host providing service
  - Slows down or crashes host
  - Often executed by botnet
- Attack propagation
  - Starts at zombies
  - Travels through tree of internet routers rooted
  - Ends at victim
- IP source spoofing
  - Hides attacker
  - Scatters return traffic from victim

Source:
M.T. Goodrich, Probabalistic Packet Marking for Large-Scale IP Traceback, IEEE/ACM Transactions on Networking 16:1, 2008.



IP TRACEBACK

- Problem
  - How to identify leaves of DoS propagation tree
  - Routers next to attacker
- Issues
  - There are more than 2M internet routers
  - Attacker can spoof source address
  - Attacker knows that traceback is being performed
- Approaches
  - Filtering and tracing (immediate reaction)
  - Messaging (additional traffic)
  - Logging (additional storage)
  - Probabilistic marking

PROBABILISTIC PACKET MARKING

- Method
  - Random injection of information into packet header
  - Changes seldom used bits
  - Forward routing information to victim
  - Redundancy to survive packet losses
- Benefits
  - No additional traffic
  - No router storage
  - No packet size increase
  - Can be performed online or offline

TRANSMISSION CONTROL PROTOCOL

- TCP is a transport layer protocol guaranteeing reliable data transfer, in-order delivery of messages and the ability to distinguish data for multiple concurrent applications on the same host
- Most popular application protocols, including WWW, FTP and SSH are built on top of TCP
- TCP takes a stream of 8-bit byte data, packages it into appropriately sized segment and calls on IP to transmit these packets
- Delivery order is maintained by marking each packet with a sequence number
- Every time TCP receives a packet, it sends out an ACK to indicate successful receipt of the packet.
- TCP generally checks data transmitted by comparing a checksum of the data with a checksum encoded in the packet

PORTS

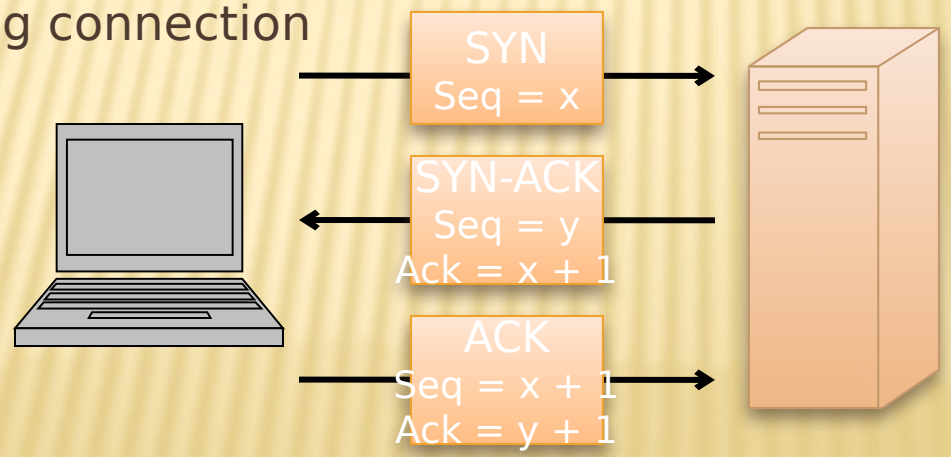
- TCP supports multiple concurrent applications on the same server
- Accomplishes this by having ports, 16 bit numbers identifying where data is directed
- The TCP header includes space for both a source and a destination port, thus allowing TCP to route all data
- In most cases, both TCP and UDP use the same port numbers for the same applications
- Ports 0 through 1023 are reserved for use by known protocols.
- Ports 1024 through 49151 are known as user ports, and should be used by most user programs for listening to connections and the like
- Ports 49152 through 65535 are private ports used for dynamic allocation by socket libraries

TCP PACKET FORMAT

Bit Offset	0-3	4-7	8-15	16-18	19-31
0	**Source Port**			**Destination Port**	
32	**Sequence Number**				
64	**Acknowledgment Number**				
96	Offset	Reserved	Flags	**Window Size**	
128	Checksum			Urgent Pointer	
160	Options				
>= 160	Payload				

ESTABLISHING TCP CONNECTIONS

- TCP connections are established through a three way handshake.
- The server generally has a passive listener, waiting for a connection request
- The client requests a connection by sending out a SYN packet
- The server responds by sending a SYN/ACK packet, indicating an acknowledgment for the connection
- The client responds by sending an ACK to the server thus establishing connection



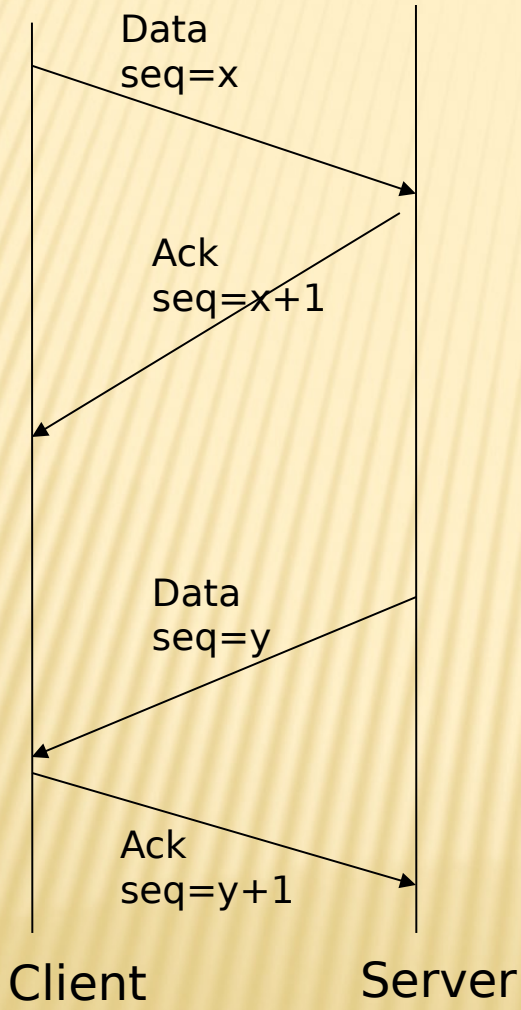
SYN FLOOD

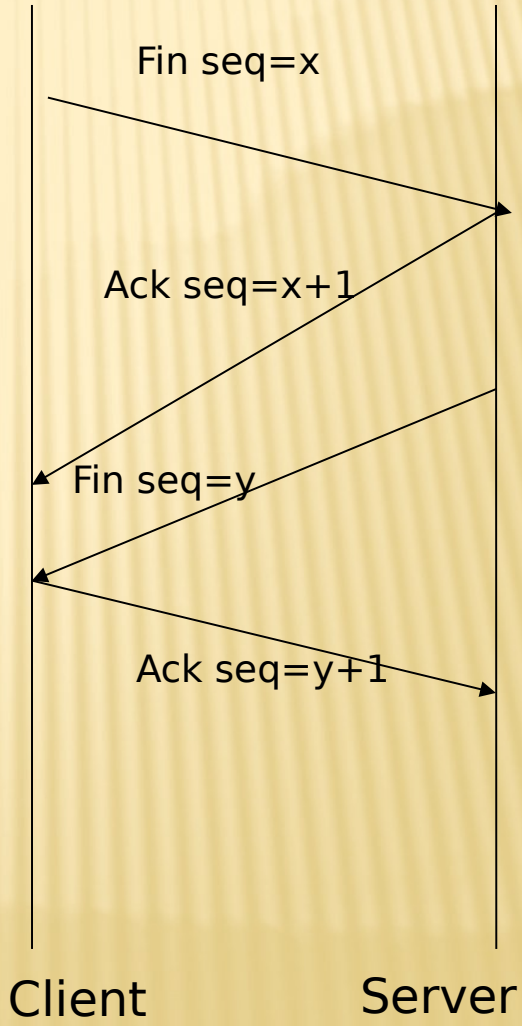
- Typically DOS attack, though can be combined with other attack such as TCP hijacking
- Rely on sending TCP connection requests faster than the server can process them
- Attacker creates a large number of packets with spoofed source addresses and setting the SYN flag on these
- The server responds with a SYN/ACK for which it never gets a response (waits for about 3 minutes each)
- Eventually the server stops accepting connection requests, thus triggering a denial of service.
- Can be solved in multiple ways
- One of the common way to do this is to use SYN cookies

TCP DATA TRANSFER

- During connection initialization using the three way handshake, initial sequence numbers are exchanged
- The TCP header includes a 16 bit checksum of the data and parts of the header, including the source and destination
- Acknowledgment or lack thereof is used by TCP to keep track of network congestion and control flow and such
- TCP connections are cleanly terminated with a 4-way handshake
  - The client which wishes to terminate the connection sends a FIN message to the other client
  - The other client responds by sending an ACK
  - The other client sends a FIN
  - The original client now sends an ACK, and the connection is terminated

TCP DATA TRANSFER AND TEARDOWN





TCP CONGESTION CONTROL

- During the mid-80s it was discovered that uncontrolled TCP messages were causing large scale network congestion
- TCP responded to congestion by retransmitting lost packets, thus making the problem was worse
- What is predominantly used today is a system where ACKs are used to determine the maximum number of packets which should be sent out
- Most TCP congestion avoidance algorithms, avoid congestion by modifying a congestion window (cwnd) as more cumulative ACKs are received
- Lost packets are taken to be a sign of network congestion
- TCP begins with an extremely low cwnd and rapidly increases the value of this variable to reach bottleneck capacity
- At this point it shifts to a collision detection algorithm which slowly probes the network for additional bandwidth
- TCP congestion control is a good idea in general but allows for certain attacks.

OPTIMISTIC ACK ATTACK

- An optimistic ACK attack takes advantage of the TCP congestion control
- It begins with a client sending out ACKs for data segments it hasn’t yet received
- This flood of optimistic ACKs makes the servers TCP stack believe that there is a large amount of bandwidth available and thus increase cwnd
- This leads to the attacker providing more optimistic ACKs, and eventually bandwidth use beyond what the server has available
- This can also be played out across multiple servers, with enough congestion that a certain section of the network is no longer reachable
- There are no practical solutions to this problem

SESSION HIJACKING

- Also commonly known as TCP Session Hijacking
- A security attack over a protected network
- Attempt to take control of a network session
- Sessions are server keeping state of a client’s connection
- Servers need to keep track of messages sent between client and the server and their respective actions
- Most networks follow the TCP/IP protocol
- IP Spoofing is one type of hijacking on large network

IP SPOOFING

- IP Spoofing is an attempt by an intruder to send packets from one IP address that appear to originate at another
- If the server thinks it is receiving messages from the real source after authenticating a session, it could inadvertently behave maliciously
- There are two basic forms of IP Spoofing
  - Blind Spoofing
    - Attack from any source
  - Non-Blind Spoofing
    - Attack from the same subnet

BLIND IP SPOOFING

- The TCP/IP protocol requires that “acknowledgement” numbers be sent across sessions
- Makes sure that the client is getting the server’s packets and vice versa
- Need to have the right sequence of acknowledgment numbers to spoof an IP identity

NON-BLIND IP SPOOFING

- IP Spoofing without inherently knowing the acknowledgment sequence pattern
  - Done on the same subnet
  - Use a packet sniffer to analyze the sequence pattern
    - Packet sniffers intercept network packets
    - Eventually decodes and analyzes the packets sent across the network
    - Determine the acknowledgment sequence pattern from the packets
    - Send messages to server with actual client's IP address and with validly sequenced acknowledgment number

PACKET SNIFFERS

- Packet sniffers “read” information traversing a network
  - Packet sniffers intercept network packets, possibly using ARP cache poisoning
  - Can be used as legitimate tools to analyze a network
    - Monitor network usage
    - Filter network traffic
    - Analyze network problems
  - Can also be used maliciously
    - Steal information (i.e. passwords, conversations, etc.)
    - Analyze network information to prepare an attack
- Packet sniffers can be either software or hardware based
  - Sniffers are dependent on network setup

DETECTING SNIFFERS

- Sniffers are almost always passive
  - They simply collect data
  - They do not attempt “entry” to “steal” data
- This can make them extremely hard to detect
- Most detection methods require suspicion that sniffing is occurring
  - Then some sort of “ping” of the sniffer is necessary
  - It should be a broadcast that will cause a response only from a sniffer
- Another solution on switched hubs is ARP watch
  - An ARP watch monitors the ARP cache for duplicate entries of a machine
  - If such duplicates appear, raise an alarm
  - Problem: false alarms
    - Specifically, DHCP networks can have multiple entires for a single machine

STOPPING PACKET SNIFFING

- The best way is to encrypt packets securely
  - Sniffers can capture the packets, but they are meaningless
    - Capturing a packet is useless if it just reads as garbage
  - SSH is also a much more secure method of connection
    - Private/Public key pairs makes sniffing virtually useless
  - On switched networks, almost all attacks will be via ARP spoofing
    - Add machines to a permanent store in the cache
    - This store cannot be modified via a broadcast reply
    - Thus, a sniffer cannot redirect an address to itself
- The best security is to not let them in in the first place
  - Sniffers need to be on your subnet in a switched hub in the first place
  - All sniffers need to somehow access root at some point to start themselves up

PORT KNOCKING

- Broadly port knocking is the act of attempting to make connections to blocked ports in a certain order in an attempt to open a port
- Port knocking is fairly secure against brute force attacks since there are 65536^k combinations, where k is the number of ports knocked
- Port knocking however if very susceptible to replay attacks. Someone can theoretically record port knocking attempts and repeat those to get the same open port again
- One good way of protecting against replay attacks would be a time dependent knock sequence.

USER DATAGRAM PROTOCOL

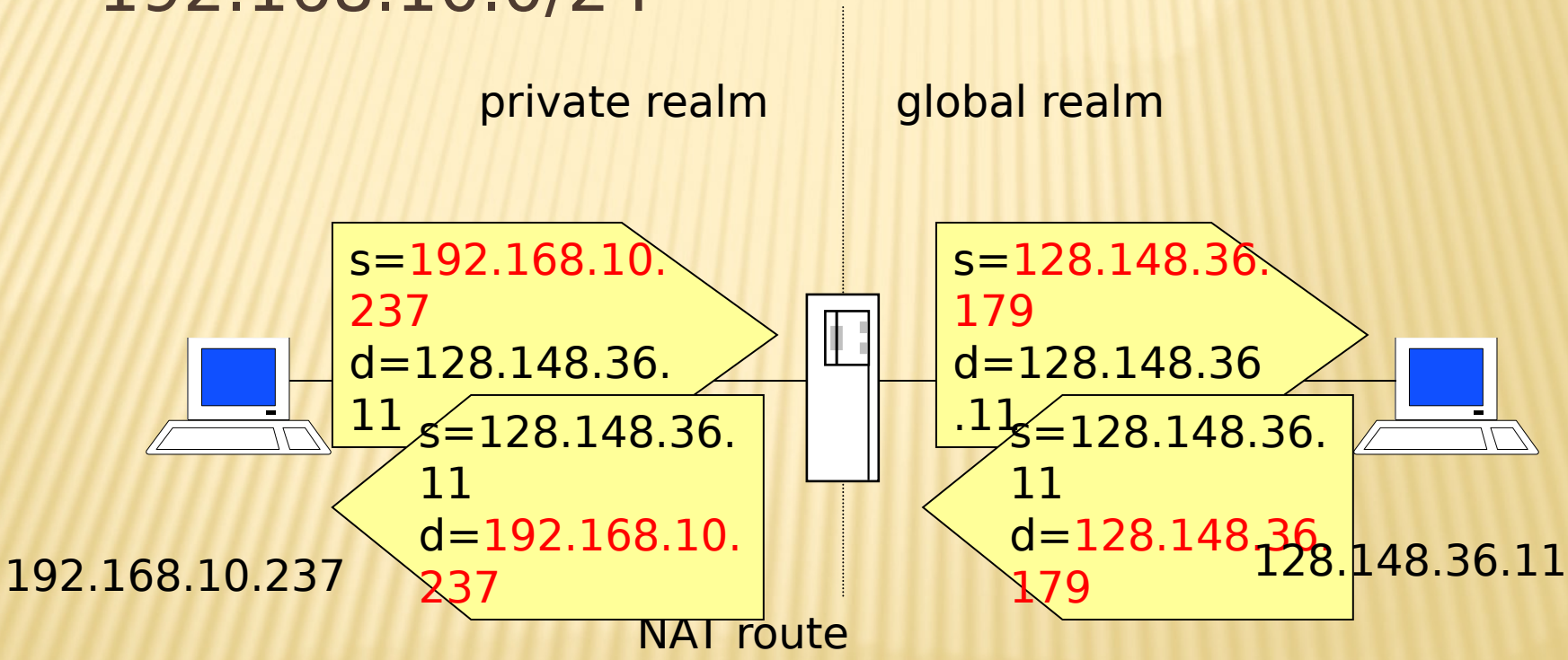
- UDP is a stateless, unreliable datagram protocol built on top of IP, that is it lies on level 4
- It does not provide delivery guarantees, or acknowledgments, but is significantly faster
- Can however distinguish data for multiple concurrent applications on a single host.
- A lack of reliability implies applications using UDP must be ready to accept a fair amount of error packages and data loss. Some application level protocols such as TFTP build reliability on top of UDP.
  - Most applications used on UDP will suffer if they have reliability. VoIP, Streaming Video and Streaming Audio all use UDP.
- UDP does not come with built in congestion protection, so while UDP does not suffer from the problems associated with optimistic ACK, there are cases where high rate UDP network access will cause congestion.

NETWORK ADDRESS TRANSLATION

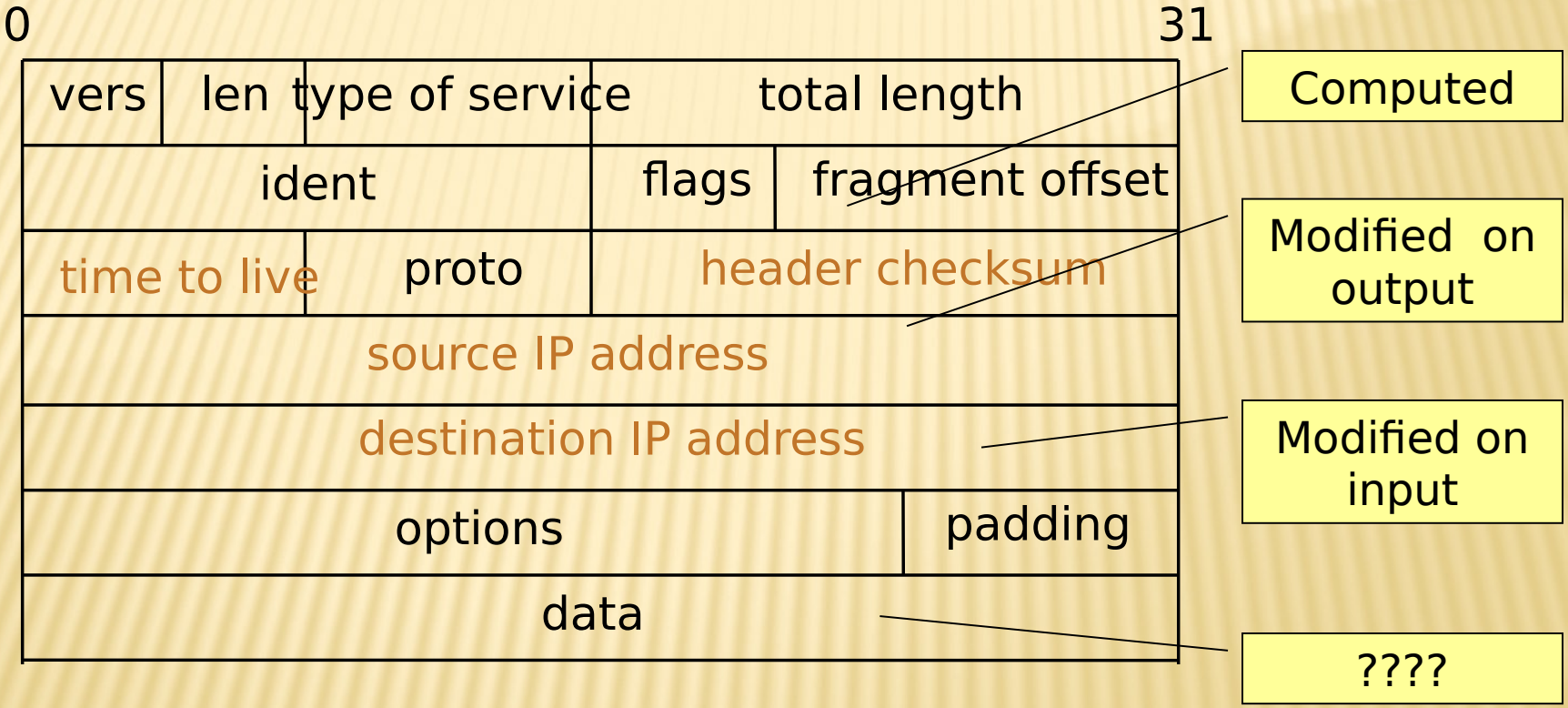
- Introduced in the early 90s to alleviate IPv4 address space congestion
- Relies on translating addresses in an internal network, to an external address that is used for communication to and from the outside world
- NAT is usually implemented by placing a router in between the internal private network and the public network.
- Saves IP address space since not every terminal needs a globally unique IP address, only an organizationally unique one
- While NAT should really be transparent to all high level services, this is sadly not true because a lot of high level communication uses things on IP

TRANSLATION

- Router has a pool of private addresses 192.168.10.0/24



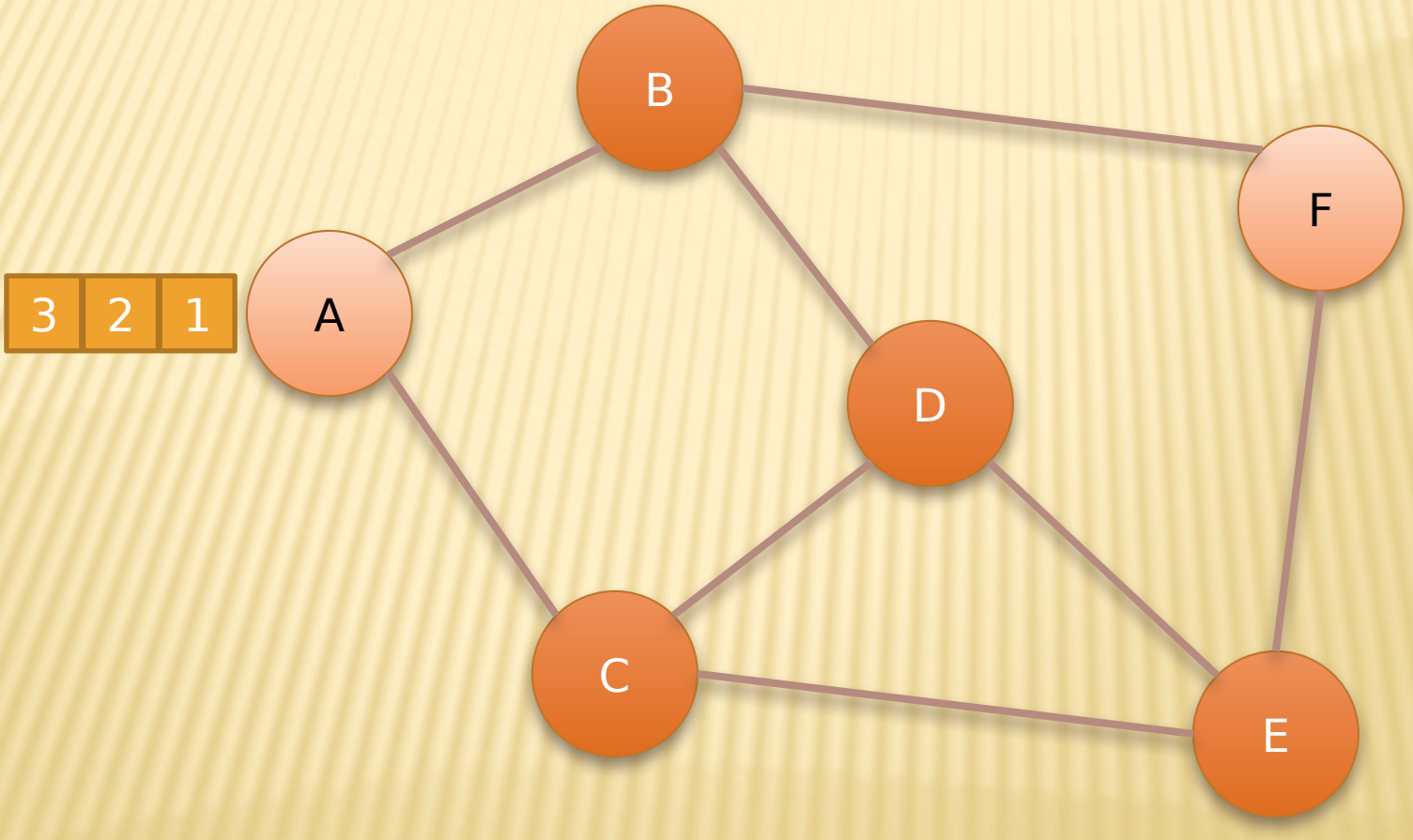
IP PACKET MODIFICATIONS



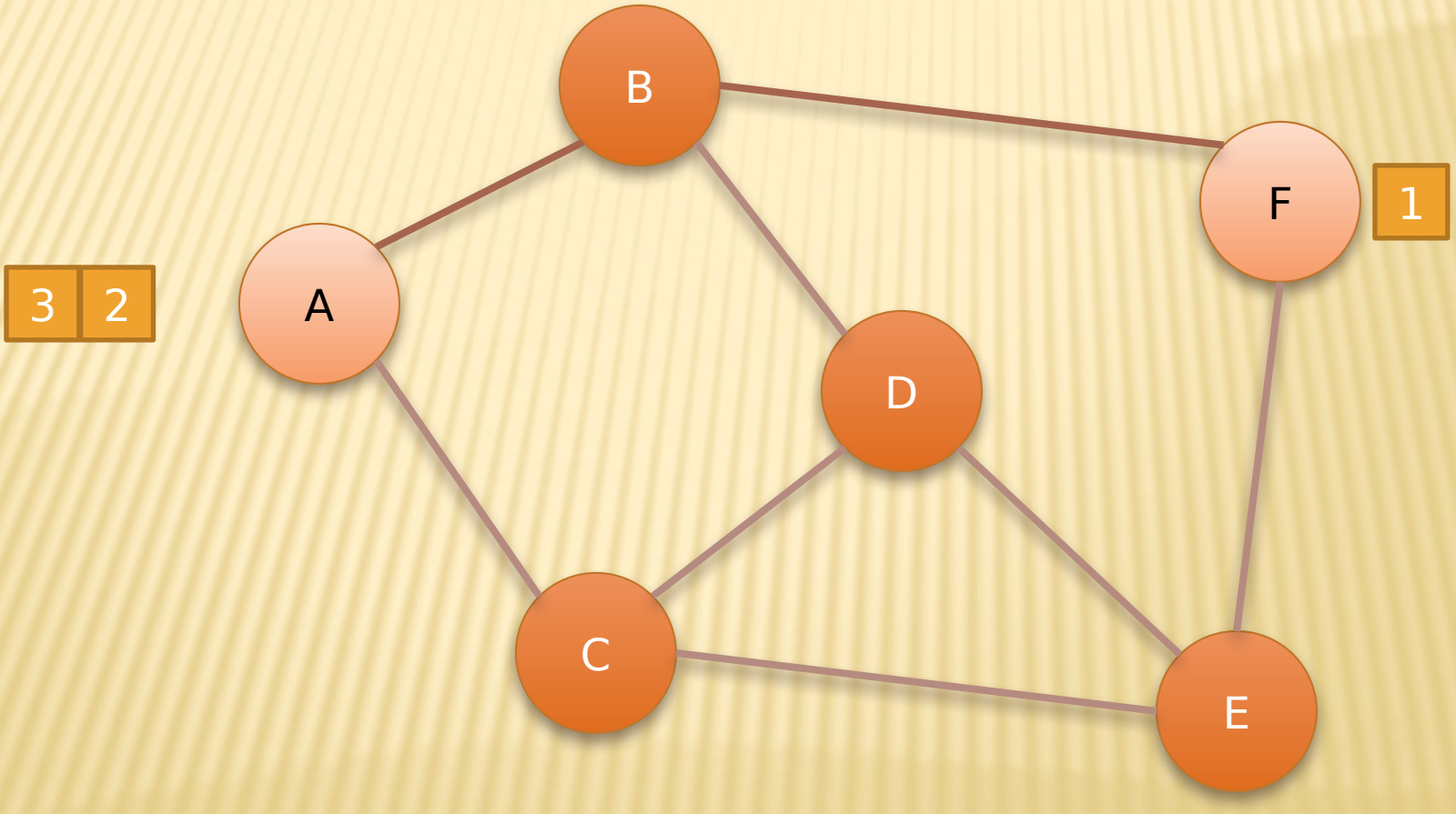
COMPUTER NETWORKS

- Circuit switching
  - Legacy phone network
  - Single route through sequence of hardware devices established when two nodes start communication
  - Data sent along route
  - Route maintained until communication ends
- Packet switching
  - Internet
  - Data split into packets
  - Packets transported independently through network
  - Each packet handled on a best efforts basis
  - Packets may follow different routes

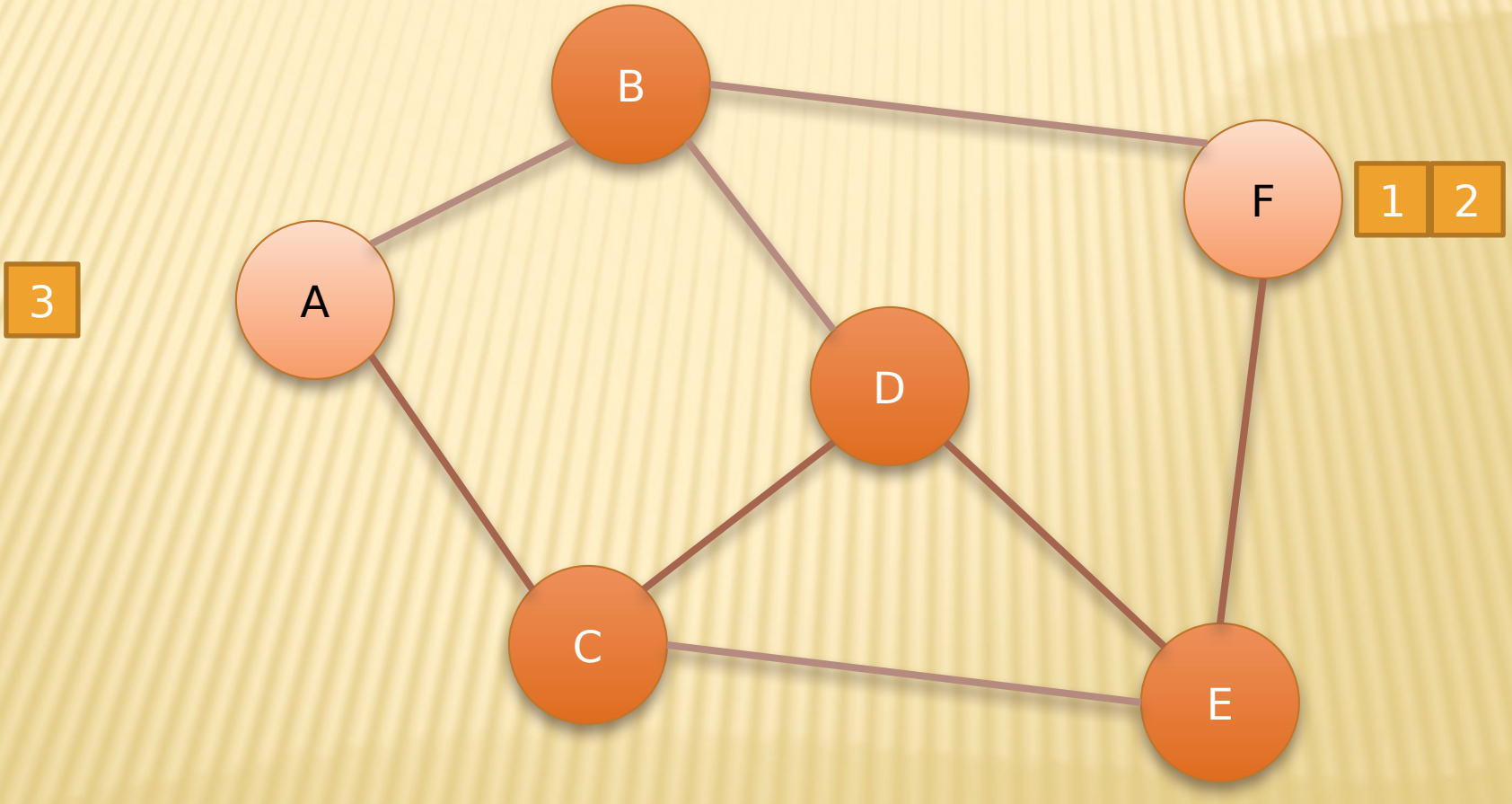
PACKET SWITCHING



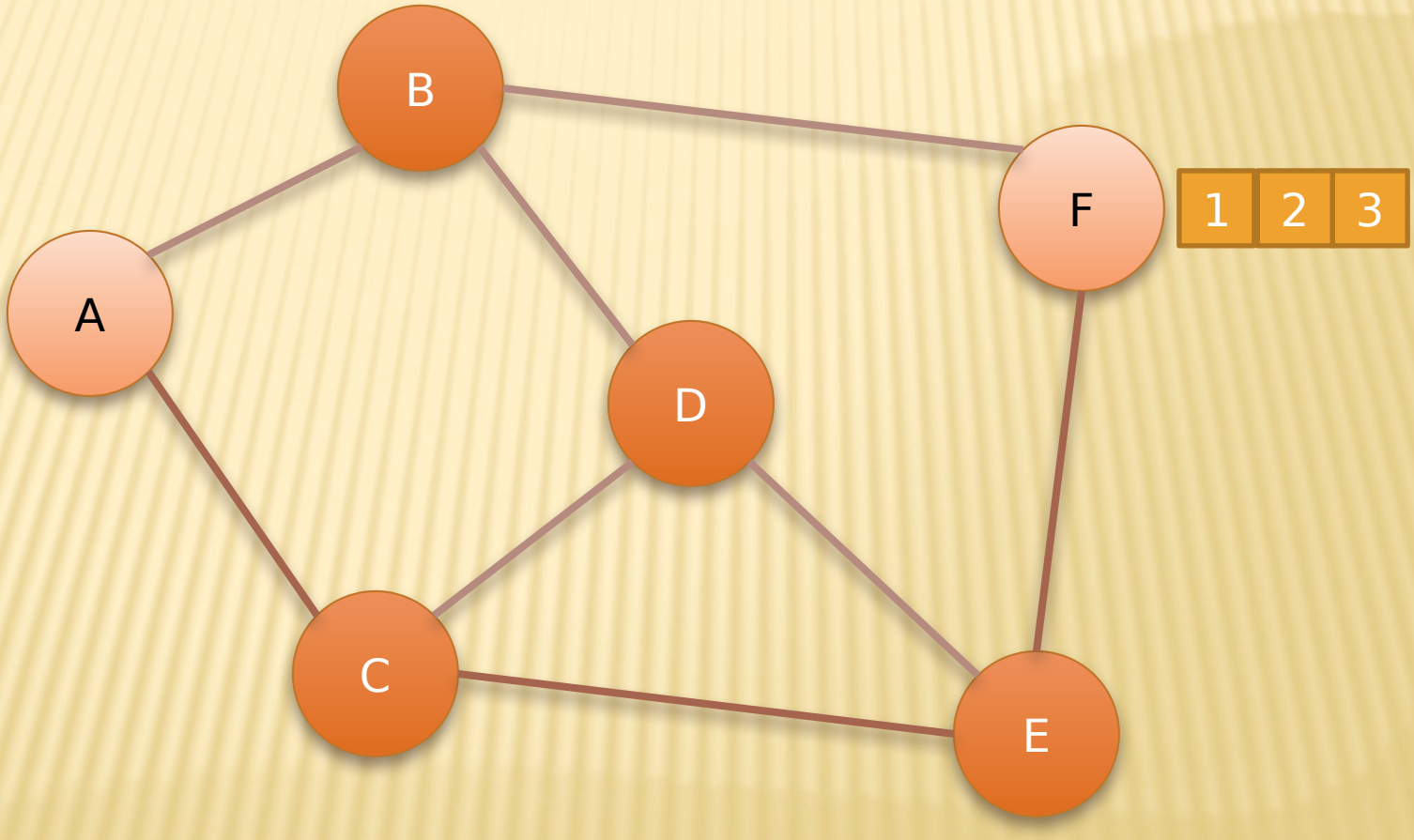
PACKET SWITCHING



PACKET SWITCHING



PACKET SWITCHING

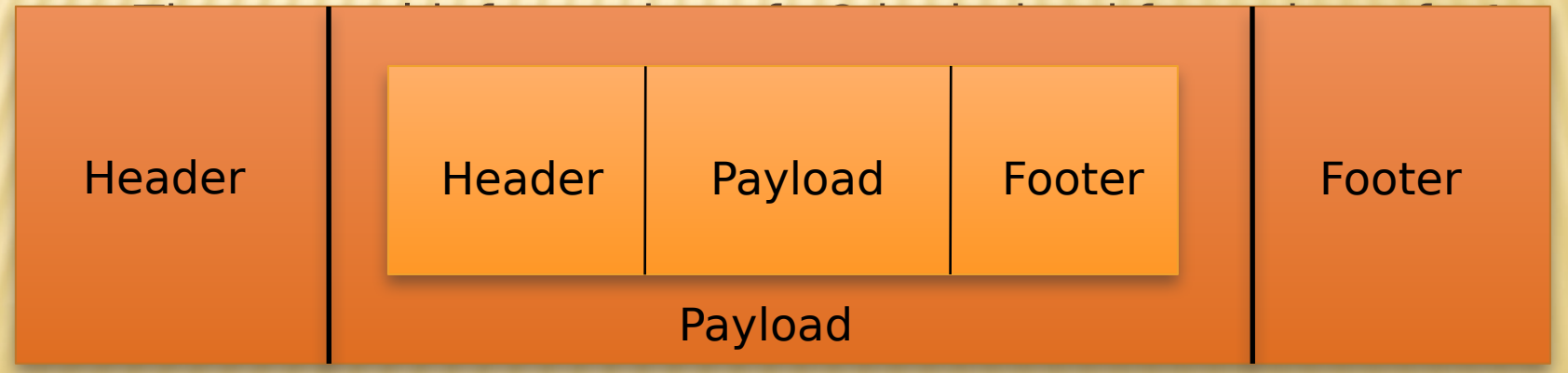


PROTOCOLS

- A protocol defines the rules for communication between computers
- Protocols are broadly classified as connectionless and connection oriented
- Connectionless protocol
  - Sends data out as soon as there is enough data to be transmitted
  - E.g., user datagram protocol (UDP)
- Connection-oriented protocol
  - Provides a reliable connection stream between two nodes
  - Consists of set up, transmission, and tear down phases
  - Creates virtual circuit-switched network
  - E.g., transmission control protocol (TCP)

ENCAPSULATION

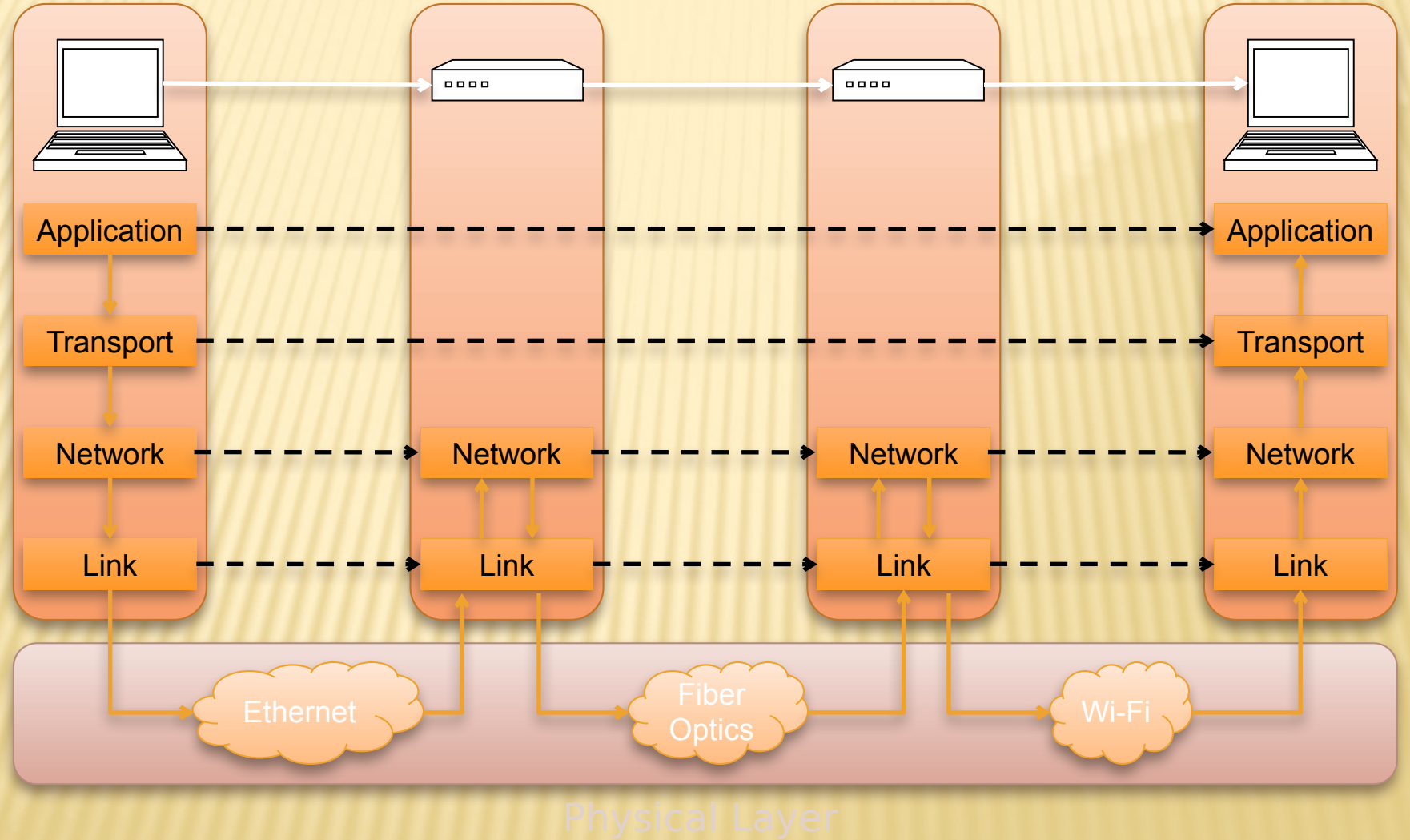
- A packet typically consists of
  - Control information for addressing the packet: header and footer
  - Data: payload
- A network protocol N1 can use the services of another network protocol N2
  - A packet p1 of N1 is encapsulated into a packet p2 of N2
  - The payload of p2 is p1



NETWORK LAYERS

- Network models typically use a stack of layers
  - Higher layers use the services of lower layers via encapsulation
  - A layer can be implemented in hardware or software
  - The bottommost layer must be in hardware
- A network device may implement several layers
- A communication channel between two nodes is established for each layer
  - Actual channel at the bottom layer
  - Virtual channel at higher layers

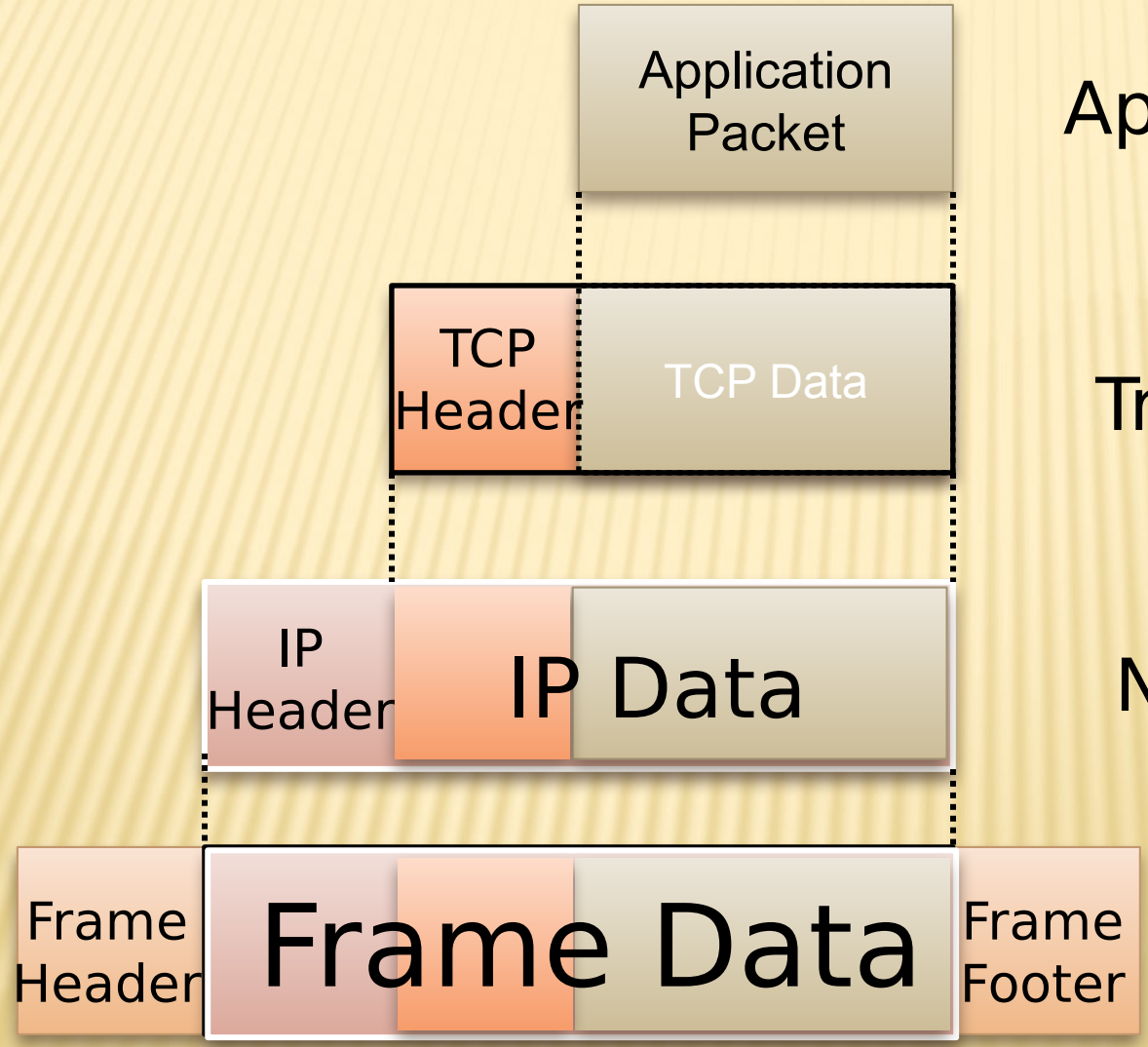
INTERNET LAYERS



INTERMEDIATE LAYERS

- Link layer
  - Local area network: Ethernet, WiFi, optical fiber
  - 48-bit media access control (MAC) addresses
  - Packets called frames
- Network layer
  - Internet-wide communication
  - Best efforts
  - 32-bit internet protocol (IP) addresses in IPv4
  - 128-bit IP addresses in IPv6
- Transport layer
  - 16-bit addresses (ports) for classes of applications
  - Connection-oriented transmission layer protocol (TCP)
  - Connectionless user datagram protocol (UDP)

INTERNET PACKET ENCAPSULATION



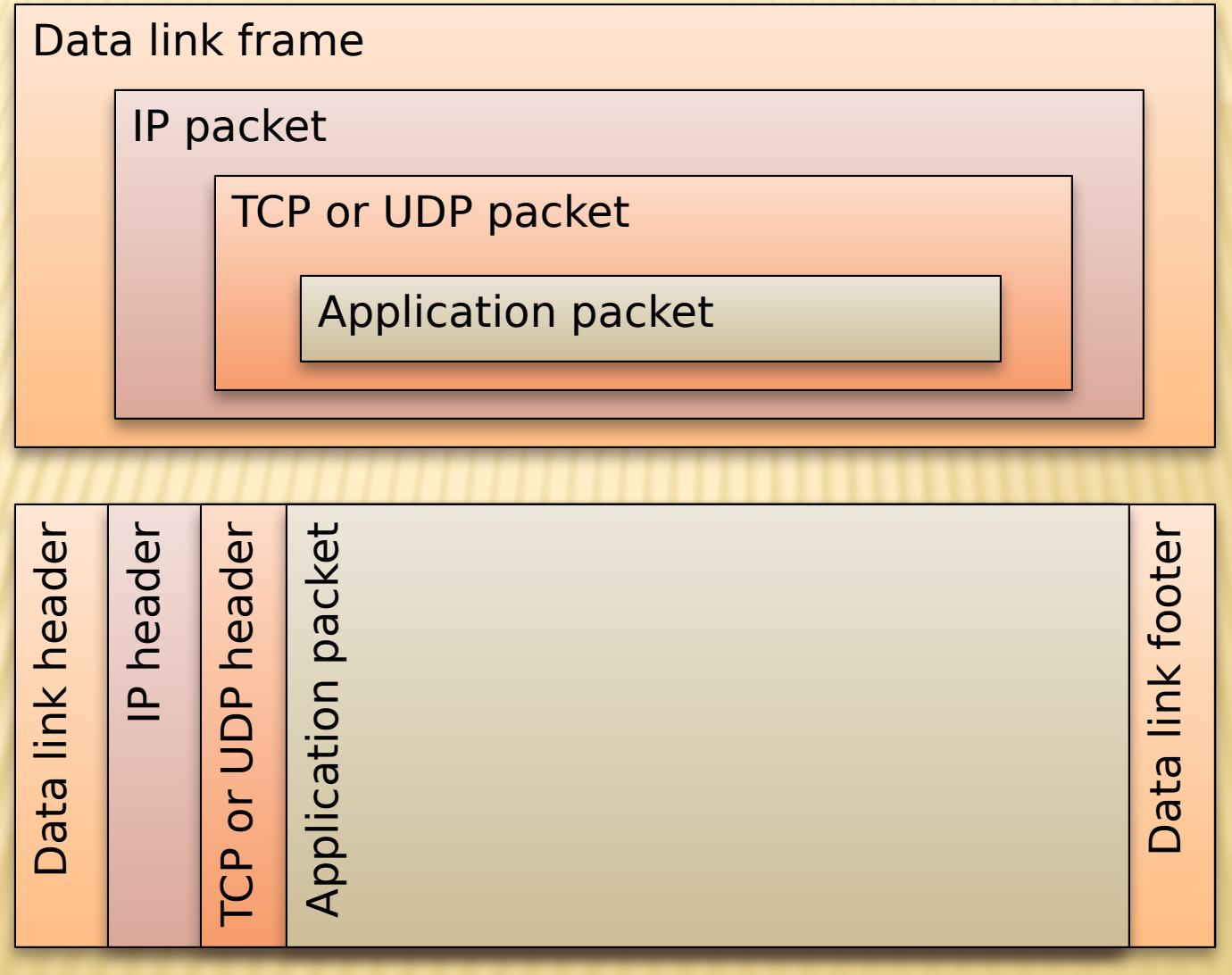
Application Layer

Transport Layer

Network Layer

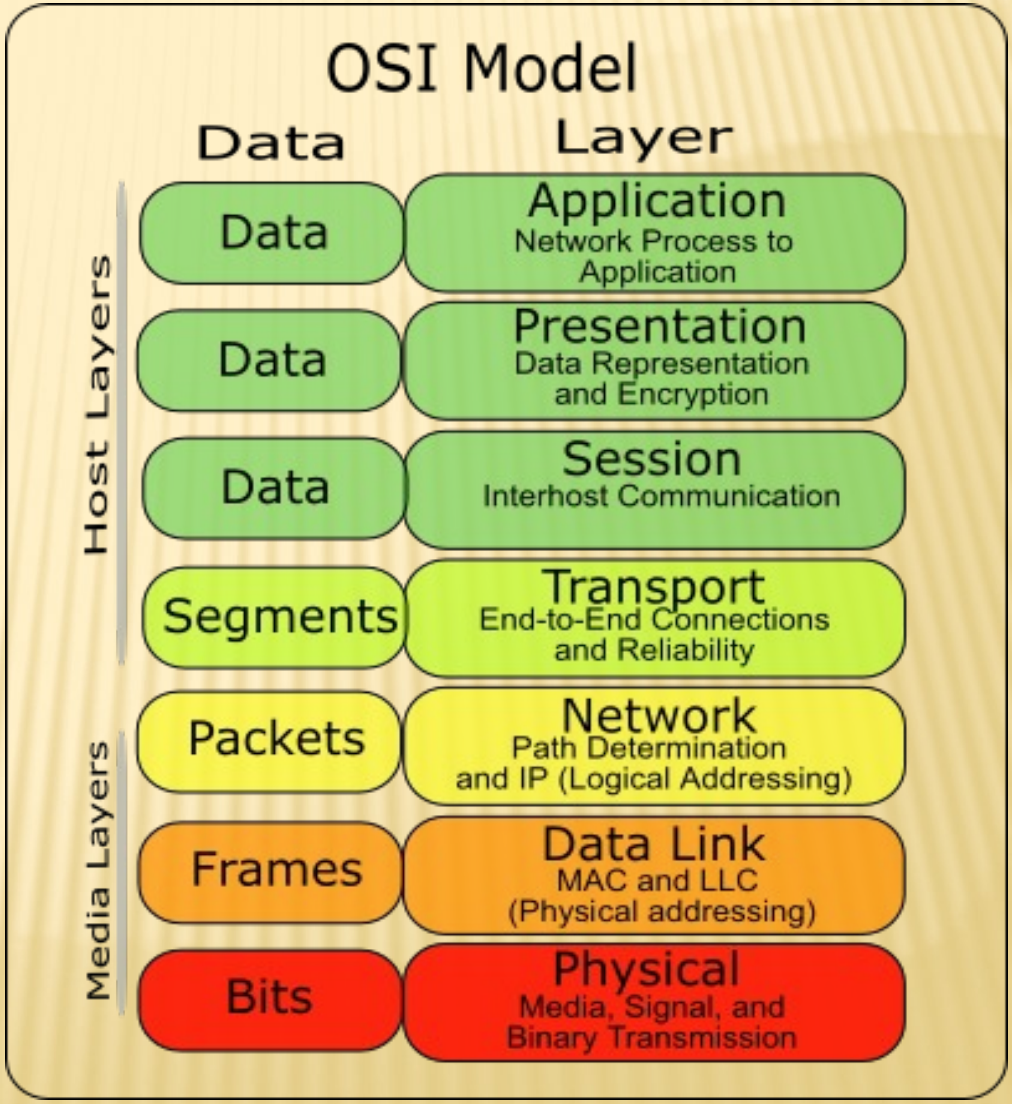
Link Layer

INTERNET PACKET ENCAPSULATION



THE OSI MODEL

- The OSI (Open System Interconnect) Reference Model is a network model consisting of seven layers
- Created in 1983, OSI is promoted by the International Standard Organization (ISO)



NETWORK INTERFACES

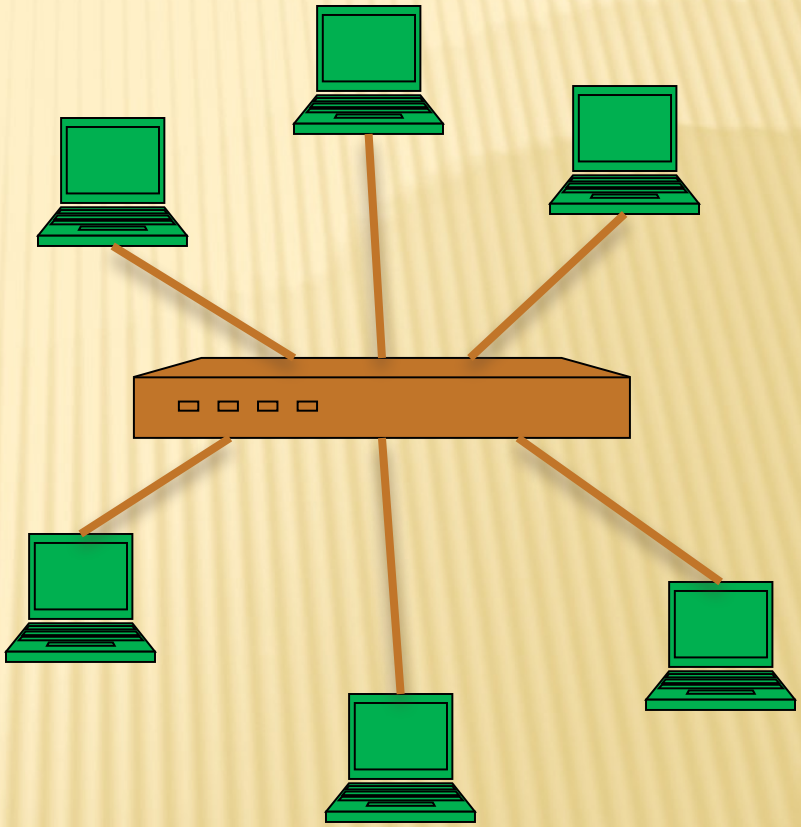
- Network interface: device connecting a computer to a network
  - Ethernet card
  - WiFi adapter
- A computer may have multiple network interfaces
- Packets transmitted between network interfaces
- Most local area networks, (including Ethernet and WiFi) broadcast frames
- In regular mode, each network interface gets the frames intended for it
- Traffic sniffing can be accomplished by configuring the network interface to read all frames (promiscuous mode)

MAC ADDRESSES

- Most network interfaces come with a predefined MAC address
- A MAC address is a 48-bit number usually represented in hex
  - E.g., 00-1A-92-D4-BF-86
- The first three octets of any MAC address are IEEE-assigned Organizationally Unique Identifiers
  - E.g., Cisco 00-1A-A1, D-Link 00-1B-11, ASUSTek 00-1A-92
- The next three can be assigned by organizations as they please, with uniqueness being the only constraint
- Organizations can utilize MAC addresses to identify computers on their network
- MAC address can be reconfigured by network interface driver software

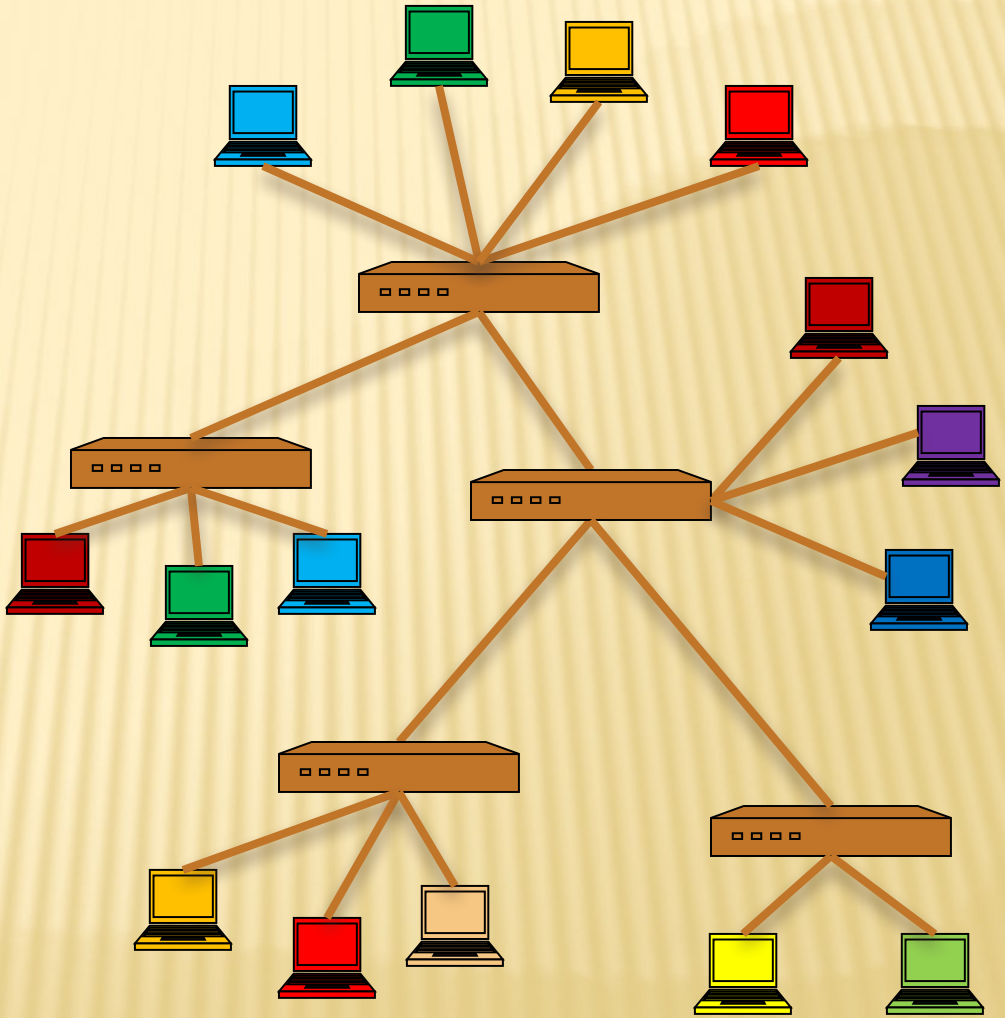
SWITCH

- A switch is a common network device
  - Operates at the link layer
  - Has multiple ports, each connected to a computer
- Operation of a switch
  - Learn the MAC address of each computer connected to it
  - Forward frames only to the destination computer



COMBINING SWITCHES

- Switches can be arranged into a tree
- Each port learns the MAC addresses of the machines in the segment (subtree) connected to it
- Fragments to unknown MAC addresses are broadcast
- Frames to MAC addresses in the same segment as the sender are ignored



MAC ADDRESS FILTERING

- A switch can be configured to provide service only to machines with specific MAC addresses
- Allowed MAC addresses need to be registered with a network administrator
- A MAC spoofing attack impersonates another machine
  - Find out MAC address of target machine
  - Reconfigure MAC address of rogue machine
  - Turn off or unplug target machine
- Countermeasures
  - Block port of switch when machine is turned off or unplugged
  - Disable duplicate MAC addresses

VIEWING AND CHANGING MAC ADDRESSES

- Viewing the MAC addresses of the interfaces of a machine
  - Linux: ifconfig
  - Windows: ipconfig /all
- Changing a MAC address in Linux
  - Stop the networking service: /etc/init.d/network stop
  - Change the MAC address: ifconfig eth0 hw ether <MAC-address>
  - Start the networking service: /etc/init.d/network start
- Changing a MAC address in Windows
  - Open the Network Connections applet
  - Access the properties for the network interface
  - Click “Configure …”
  - In the advanced tab, change the network address to the desired value
- Changing a MAC address requires administrator privileges

ARP

- The address resolution protocol (ARP) connects the network layer to the data layer by converting IP addresses to MAC addresses
- ARP works by broadcasting requests and caching responses for future use
- The protocol begins with a computer broadcasting a message of the form

  who has <IP address1> tell <IP address2>

- When the machine with <IP address1> or an ARP server receives this message, its broadcasts the response

  <IP address1> is <MAC address>

- The requestor's IP address <IP address2> is contained in the link header
- The Linux and Windows command arp - a displays the ARP table

```
Internet Address      Physical Address      Type
128.148.31.1          00-00-0c-07-ac-00     dynamic
128.148.31.15         00-0c-76-b2-d7-1d     dynamic
128.148.31.71         00-0c-76-b2-d0-d2     dynamic
128.148.31.75         00-0c-76-b2-d7-1d     dynamic
128.148.31.102        00-22-0c-a3-e4-00     dynamic
128.148.31.137        00-1d-92-b6-f1-a9     dynamic
```

ARP SPOOFING

- The ARP table is updated whenever an ARP response is received
- Requests are not tracked
- ARP announcements are not authenticated
- Machines trust each other
- A rogue machine can spoof other machines

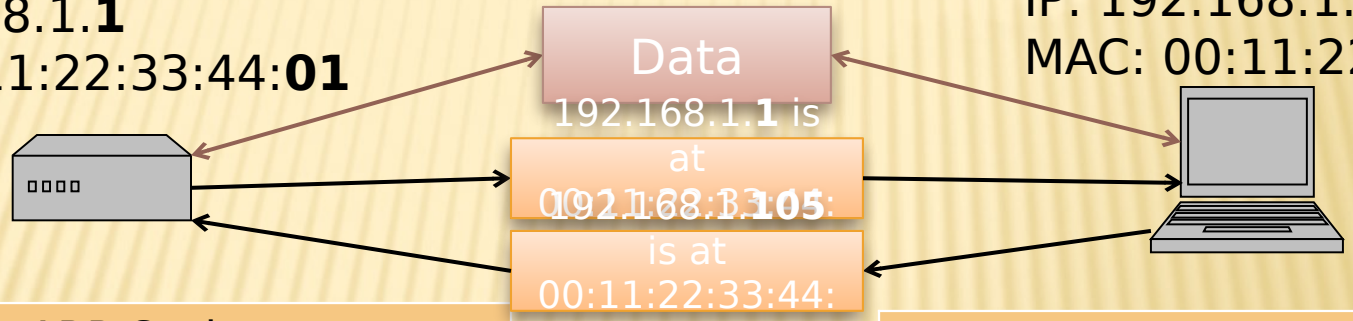
ARP POISONING (ARP SPOOFING)

- According to the standard, almost all ARP implementations are stateless
- An arp cache updates every time that it receives an arp reply… even if it did not send any arp request!
- It is possible to “poison” an arp cache by sending gratuitous arp replies
- Using static entries solves the problem but it is almost impossible to manage!

ARP CACHES

IP: 192.168.1.**1**
MAC: 00:11:22:33:44:**01**

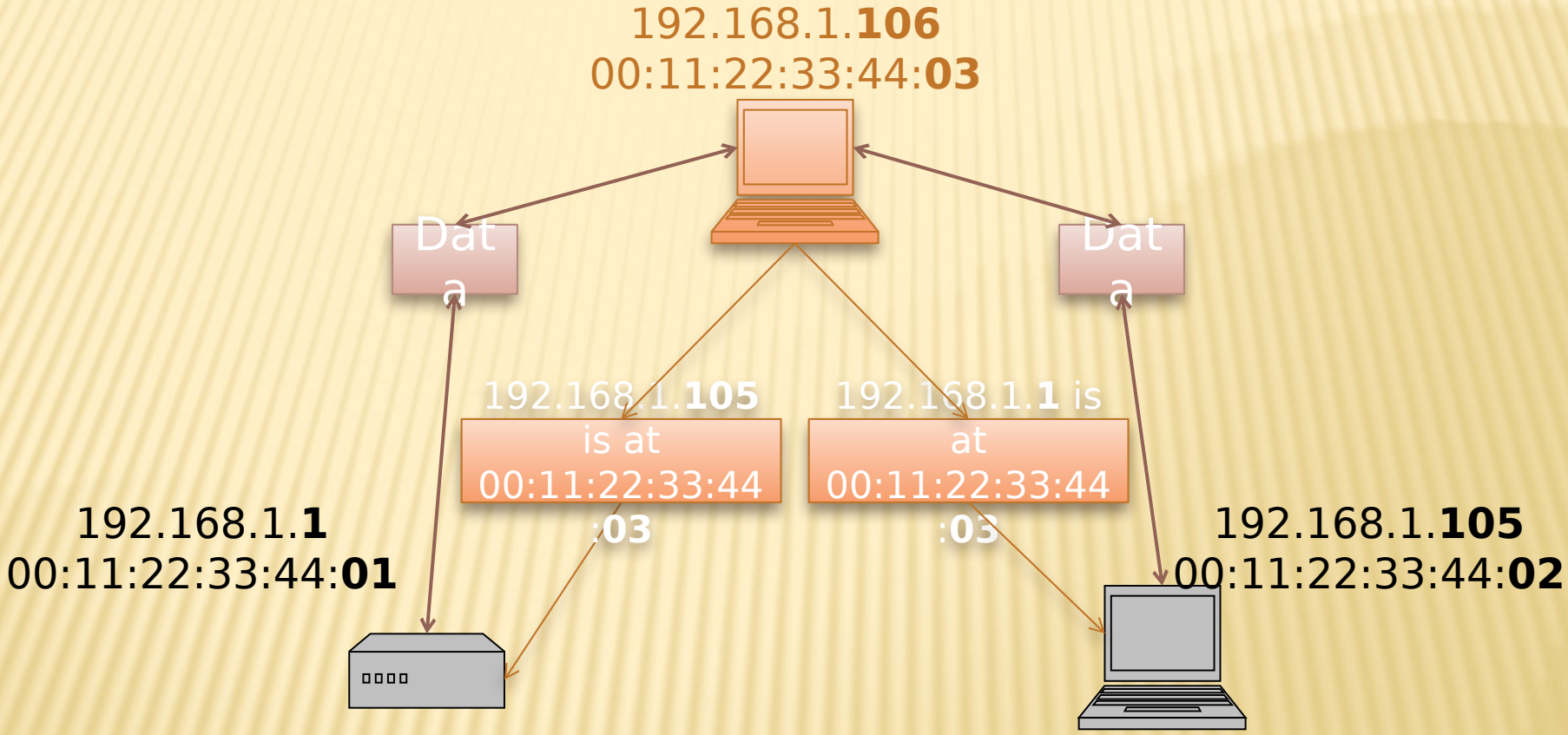
IP: 192.168.1.**105**
MAC: 00:11:22:33:44:**02**



ARP Cache	
192.168.1.**1** **05**	00:11:22:33:44:**0** **2**

ARP Cache	
192.168.1.**1**	00:11:22:33:44:**0** **1**

POISONED ARP CACHES



Poisoned ARP Cache	
192.168.1.**1** **05**	00:11:22:33:44:**0** **3**

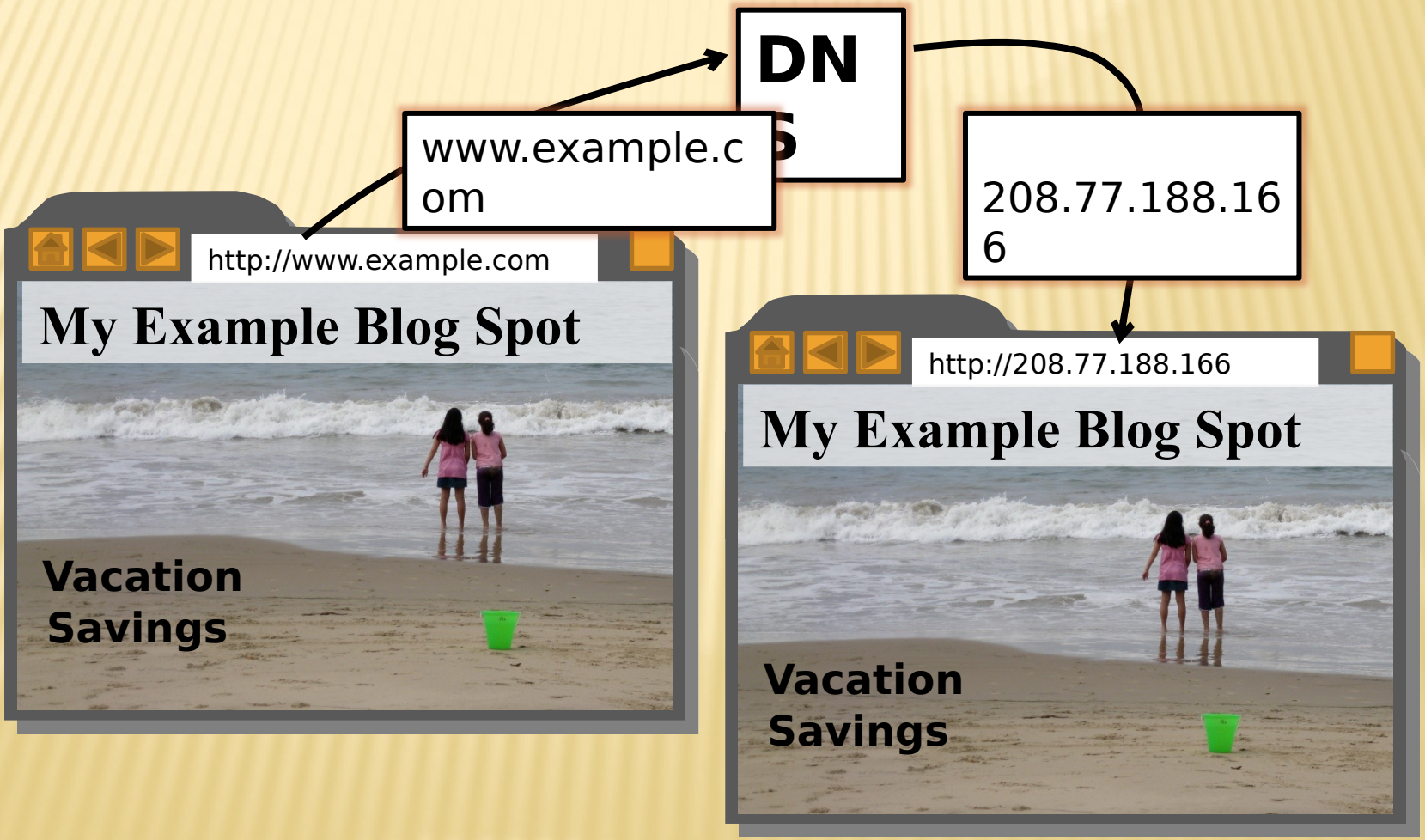
Poisoned ARP Cache	
192.168.1.**1**	00:11:22:33:44: **03**

ROOT CAUSE AND DEFENSE

- The ARP spoofing is derived from the lack of identity verification in the Internet's underlying mechanisms.
- Defense:
  - Checking for multiple occurrences of the same MAC address on the LAN.
  - Manually specify a router's ARP cache to assign certain MAC addresses to specify IP addresses. Requires to adjust the cache are ignored.

Domain Name System

- The domain name system (DNS) is an application-layer protocol for mapping domain names to IP addresses



Domain Name System

- DNS provides a distributed database over the internet that stores various resource records, including:
  - Address (A) record: IP address associated with a host name
  - Mail exchange(MX) record: mail server of a domain
  - Name server (NS) record: authoritative server for a domain

For example, if example.com wishes to sub-delegate "john.example.com." to John who works at Example, inc., lines like this can be added to the example.com zone file:

```
john.example.com. NS ns1.john.example.com.
john.example.com. NS ns2.john.example.com.
# It's important to provide "glue"; in other words, let the world know
# the IPs for these name servers.
ns1.john.example.com. 10.9.8.7
ns2.john.example.com. 10.5.77.65
```

John, who is running is own nameservers with the IPs 10.9.8.7 and 10.5.77.65 then has a zone file for john.example.com. that looks something like this:

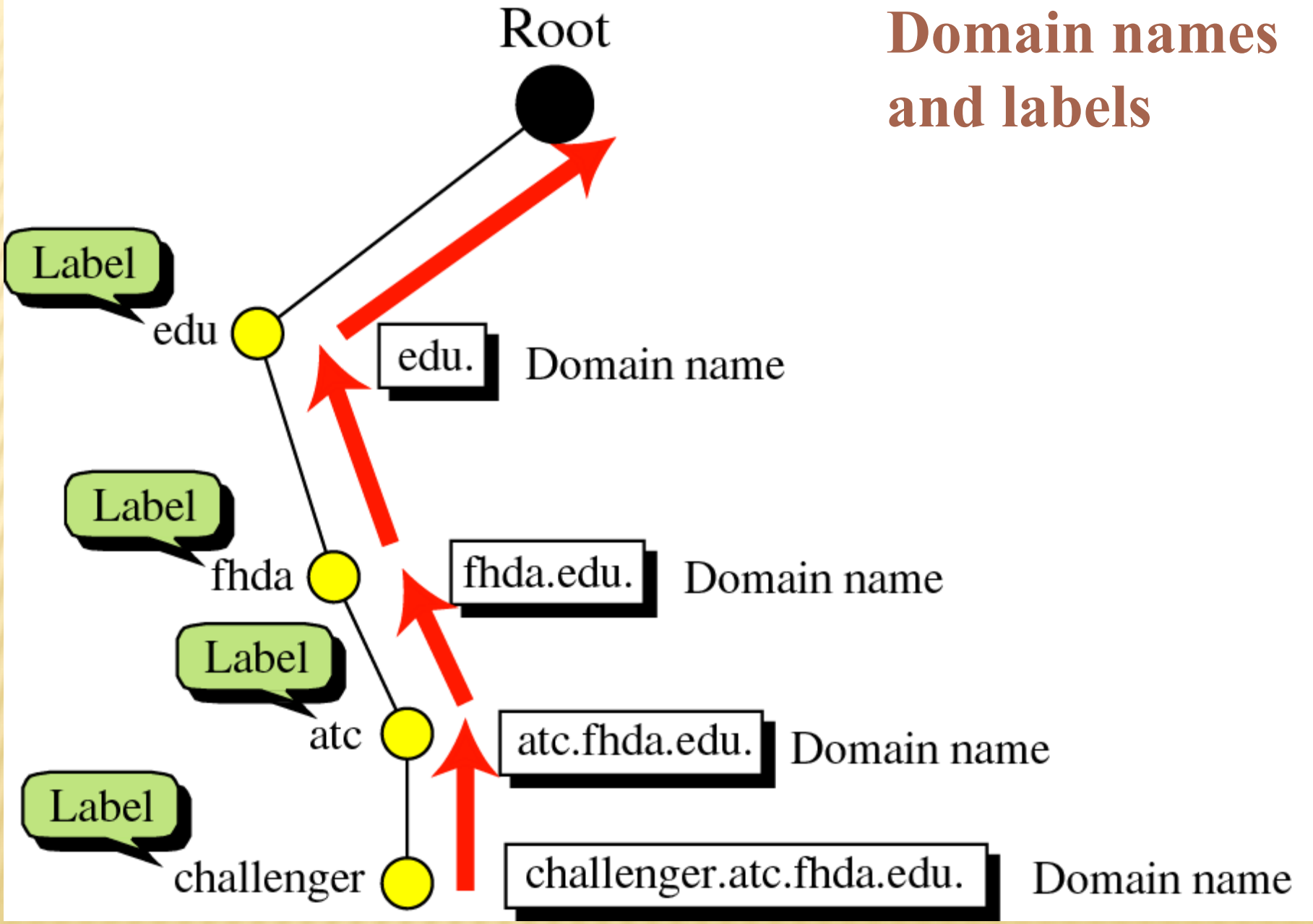
```
# It is best if the NS records for a subzone agree with the delegation
# records above
john.example.com. NS ns1.john.example.com.
john.example.com. NS ns2.john.example.com.

ns1.john.example.com. 10.9.8.7
ns2.john.example.com. 10.5.77.65

# Now that that is out of the way, here is the rest of the zone
john.example.com. 10.9.8.7
www.john.example.com. 10.5.77.65
john.example.com. MX 10 mail.john.example.com.
mail.john.example.com. 10.9.8.7
```

Example DNS entries from http://www.maradns.org/tutorial/recordtypes.html

Name Servers

- Domain names:
  - Two or more labels, separated by dots (e.g., cs166.net)
  - Rightmost label is the top-level domain (TLD)
- Hierarchy of authoritative name servers
  - Information about root domain
  - Information about its subdomains (A records) or references to other name servers (NS records)
- The authoritative name server hierarchy matches the domain hierarchy: root servers point to DNS servers for TLDs, etc.
- Root servers, and servers for TLDs change infrequently
- DNS servers refer to other DNS servers by name, not by IP: sometimes must bootstrap by providing an IP along with a name, called a glue record

Domain names and labels



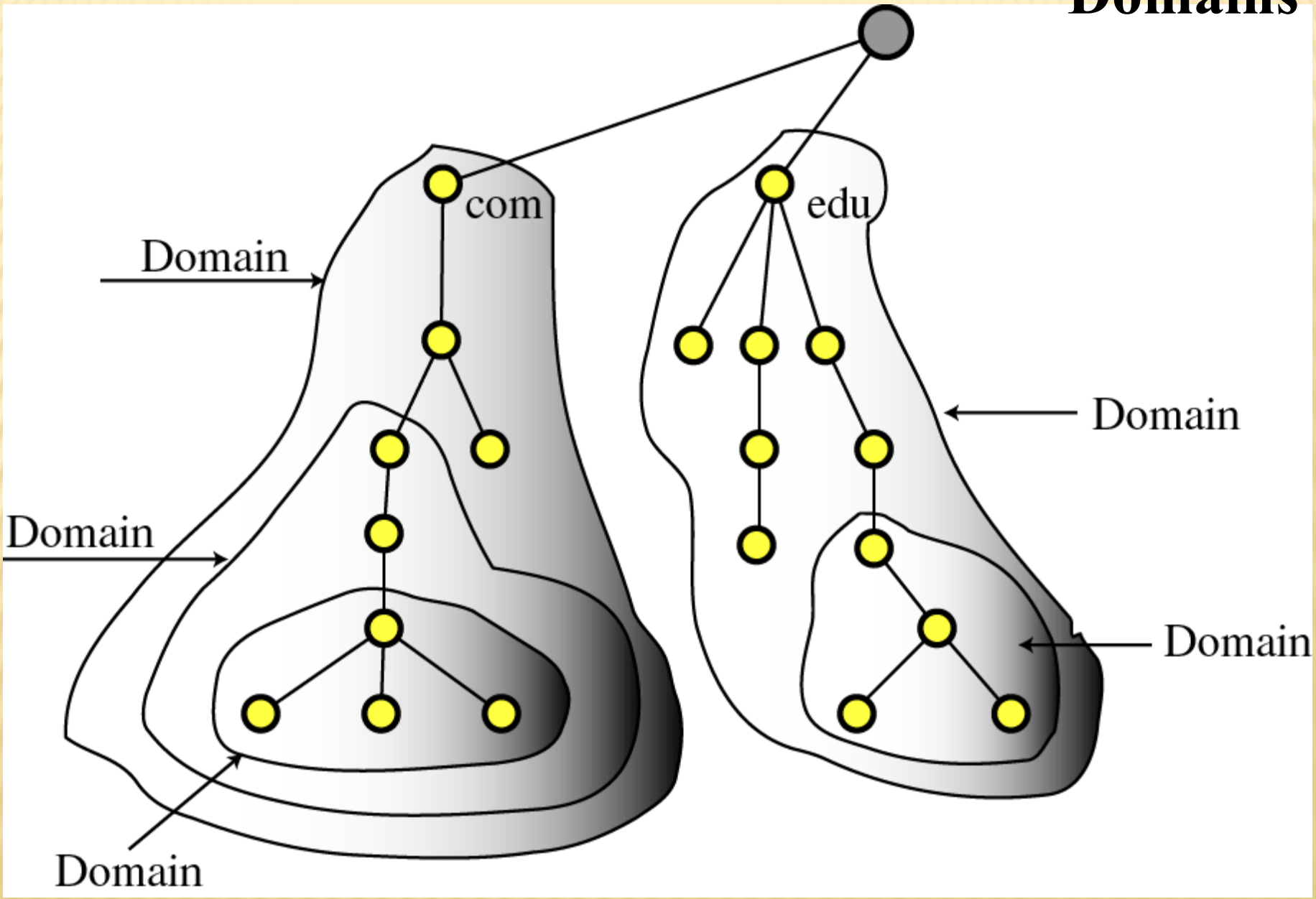
Namespace Management

- ICANN: Internet Corporation for Assigned Names and Numbers
- ICANN has the overall responsibility for managing DNS. It controls the root domain, delegating control over each top-level domain to a domain name registry
- Along with a small set of general TLDs, every country has its own TLD -- (cTLDS) – controlled by the government.
- ICANN is the governing body for all general TLDs
- Until 1999 all .com, .net and .org registries were handled by Network Solutions Incorporated.
- After November, 1999, ICANN and NSI had to allow for a shared registration system and there are currently over 500 registrars in the market
- Also since 1999, ICANN has created additional gTLDs including some which are sponsored by consortiums or groups of companies.

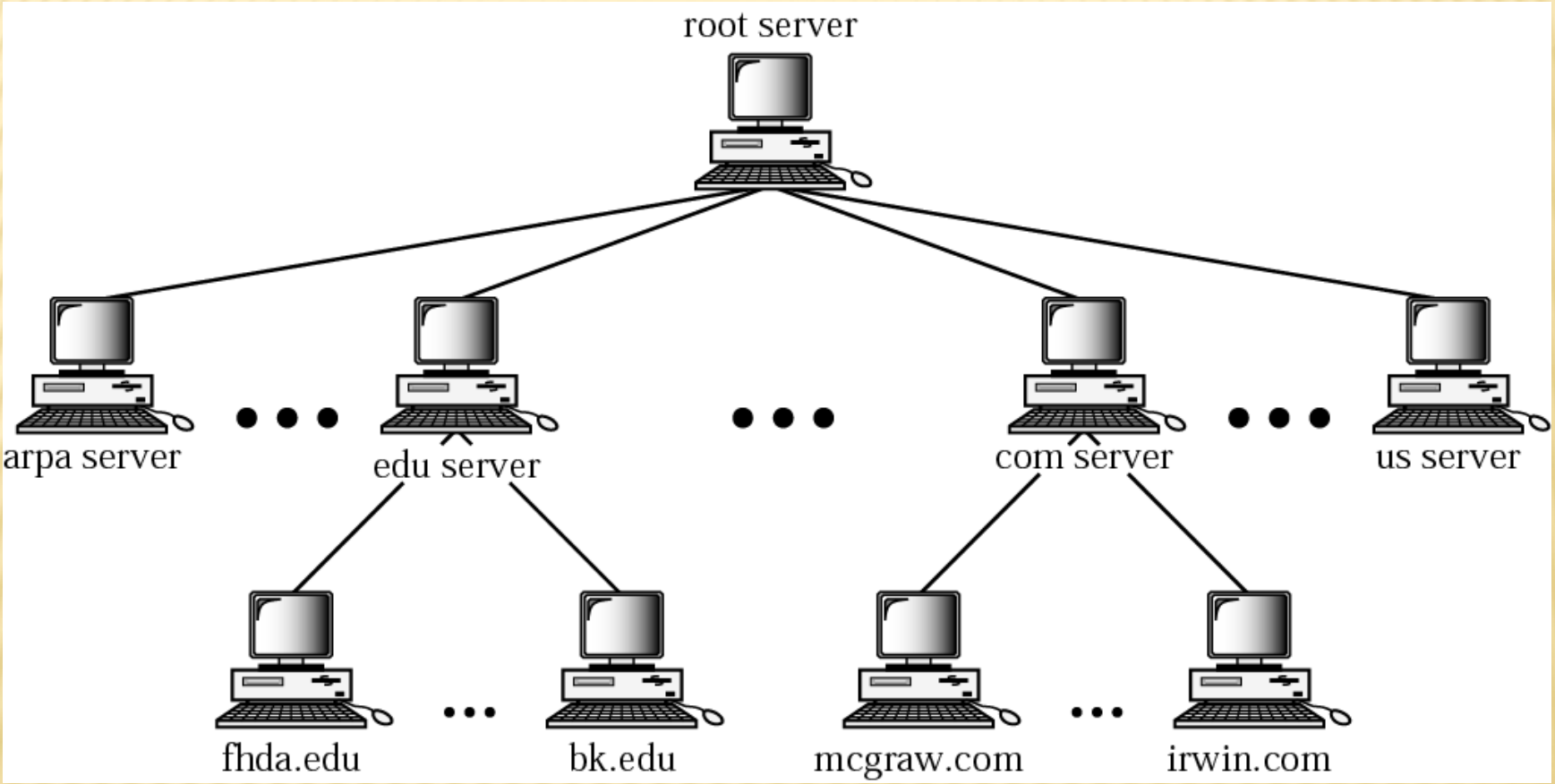
TOP LEVEL DOMAINS

- Started in 1984
- Originally supposed to be named by function
  - .com for commercial websites, .mil for military
- Eventually agreed upon unrestricted TLDs for .com, .net, .org, .info
- In 1994 started allowing country TLDs such as .it, .us
- Tried to move back to hierarchy of purpose in 2000 with creation of .aero, .museum, etc

Domains

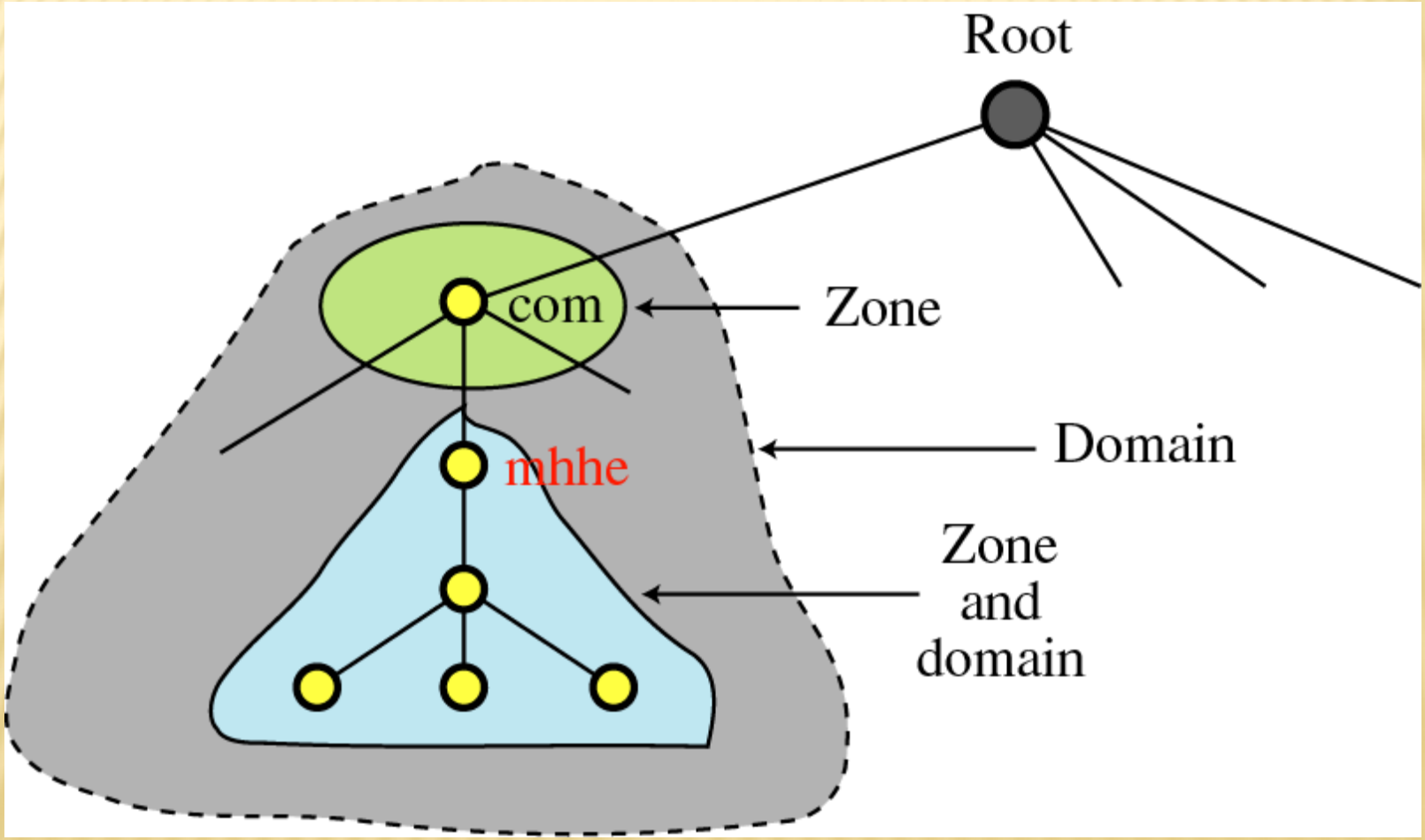


Hierarchy of name servers



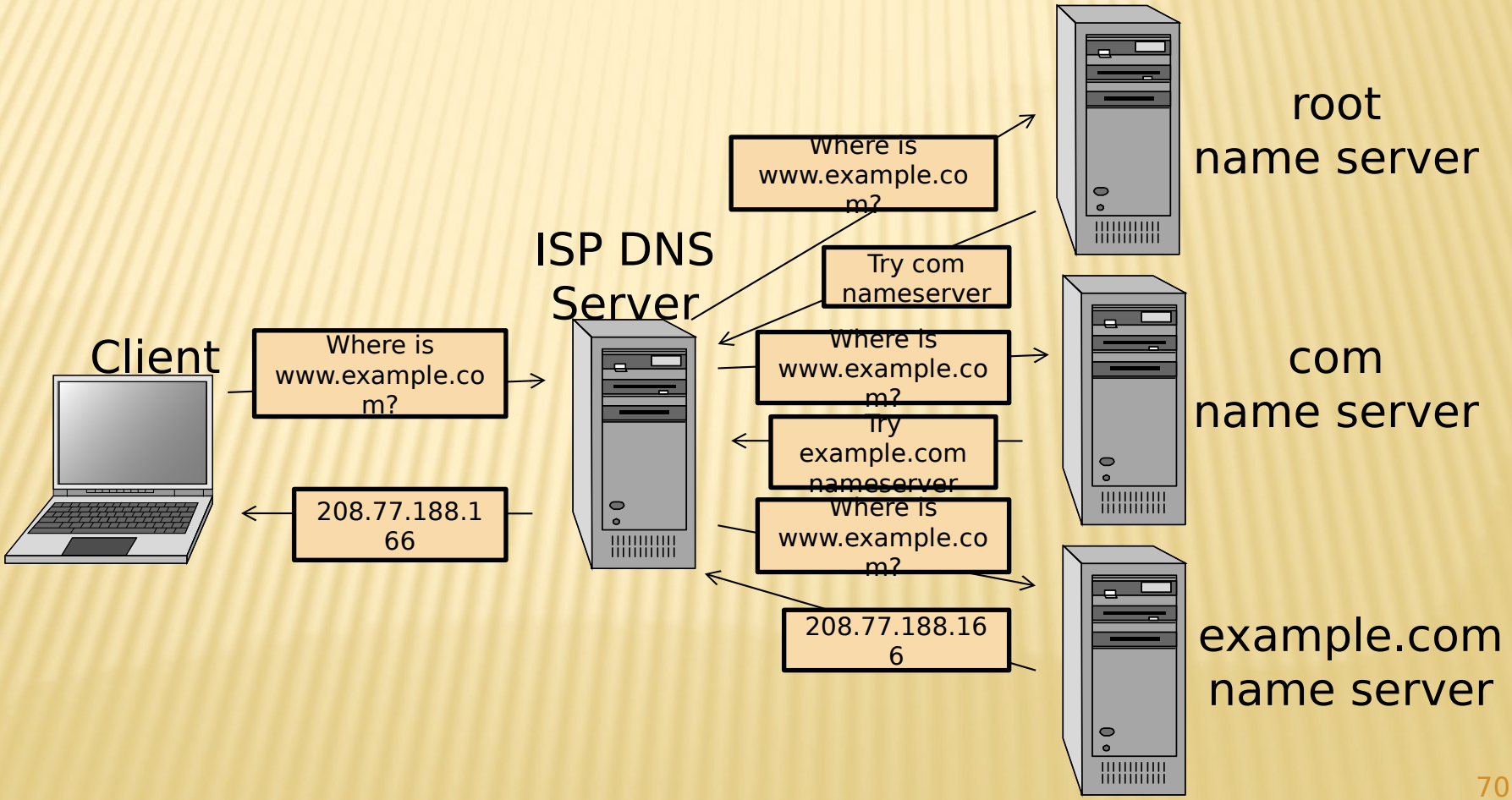
Zones and domains

- Zone: collection of connected nodes with the same authoritative DNS server

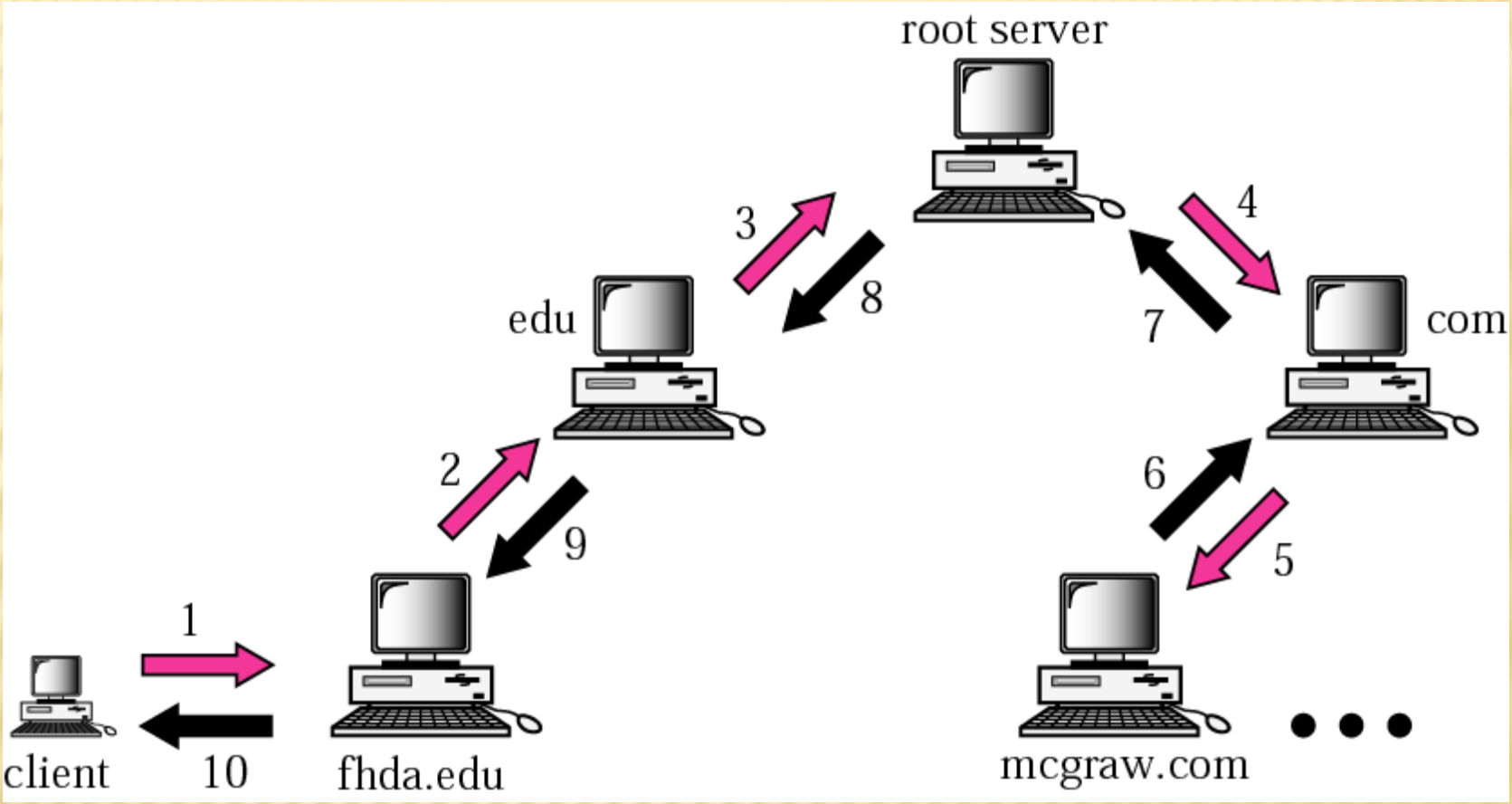


Name Resolution

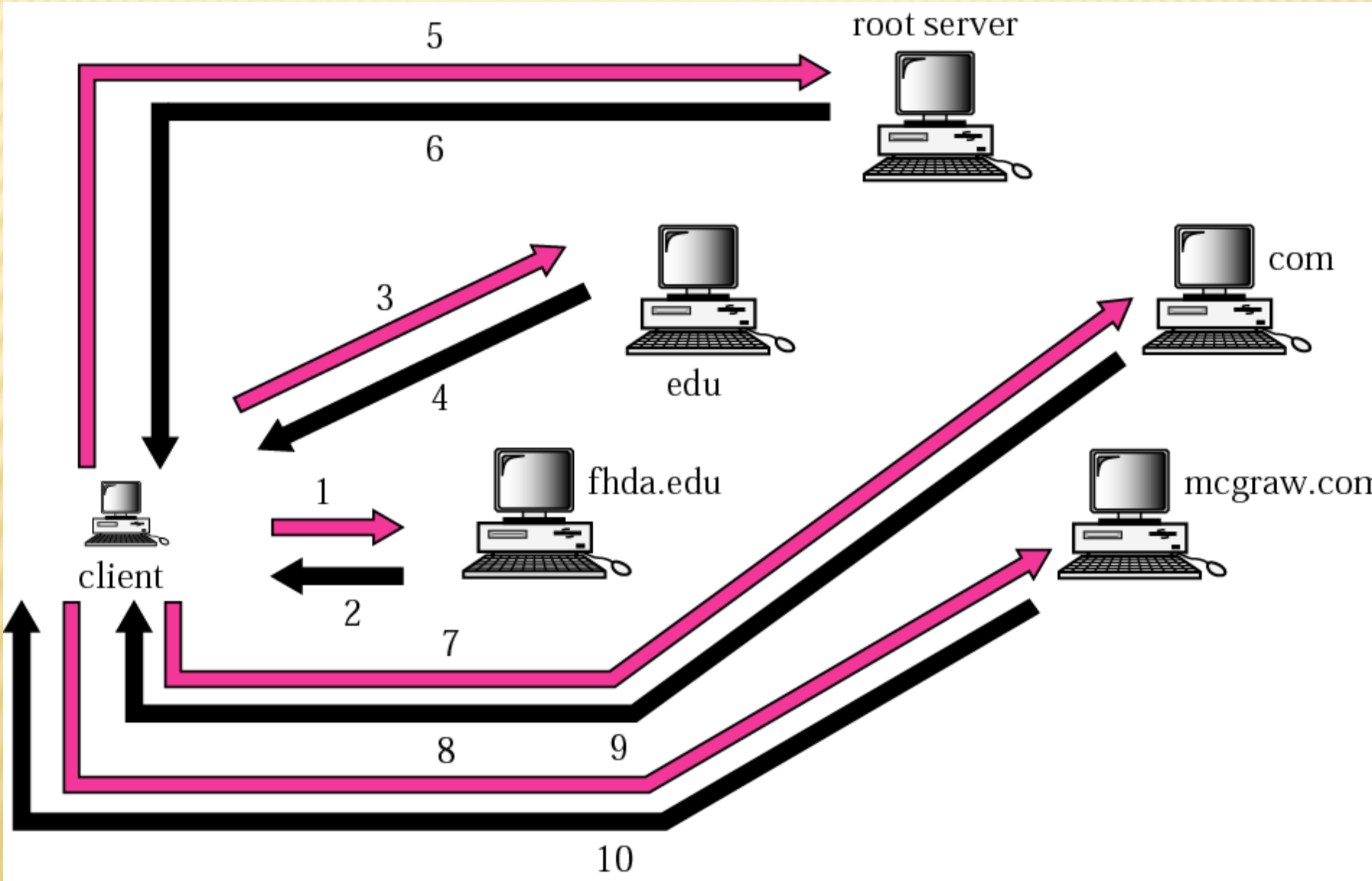
- Resolution method when answer not in cache:



Recursive resolution



Iterative resolution



AUTHORITATIVE NAME SERVERS

- Control distributed among authoritative name servers (ANSs)
  - Responsible for specific domains
  - Can designate other ANS for subdomains
- ANS can be master or slave
  - Master contains original zone table
  - Slaves are replicas, automatically updating
- Makes DNS fault tolerant, automatically distributes load
- ANS must be installed as a NS in parents' zone

DYNAMIC RESOLUTION

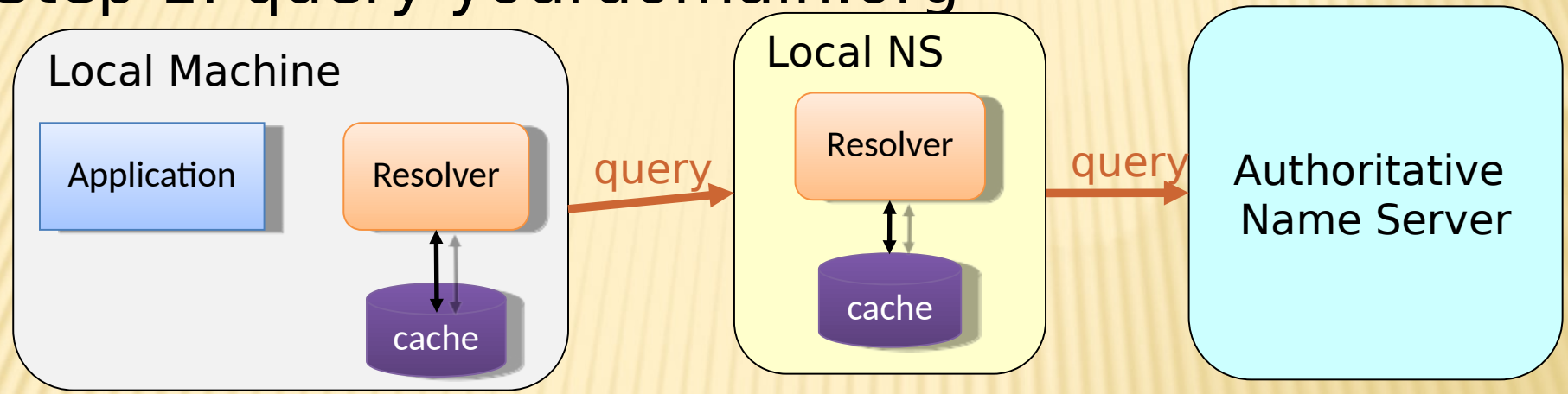
- Many large providers have more than one authoritative name server for a domain
- Problem: need to locate the instance of domain geographically closest to user
- Proposed solution: include first 3 octets of requester's IP in recursive requests to allow better service
- Content distribution networks

DNS Caching

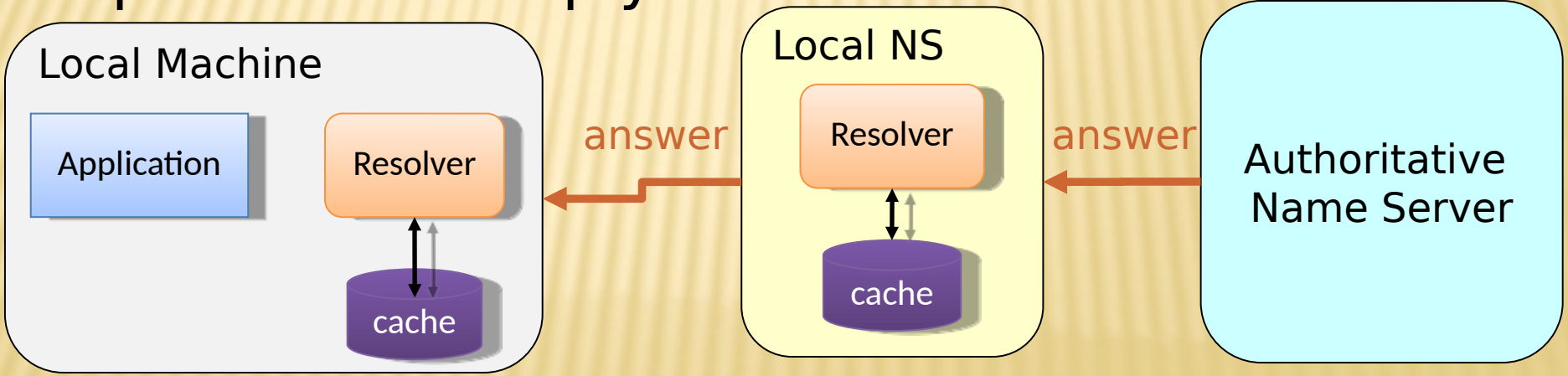
- There would be too much network traffic if a path in the DNS tree would be traversed for each query
  - Root zone would be rapidly overloaded
- DNS servers cache results for a specified amount of time
  - Specified by ANS **reply's time-to-live field**
- Operating systems and browsers also maintain resolvers and DNS caches
  - View in Windows with command ipconfig /displaydns
  - Associated privacy issues
- DNS queries are typically issued over UDP on port 53
  - 16-bit request identifier in payload

DNS CACHING

Step 1: query yourdomain.org

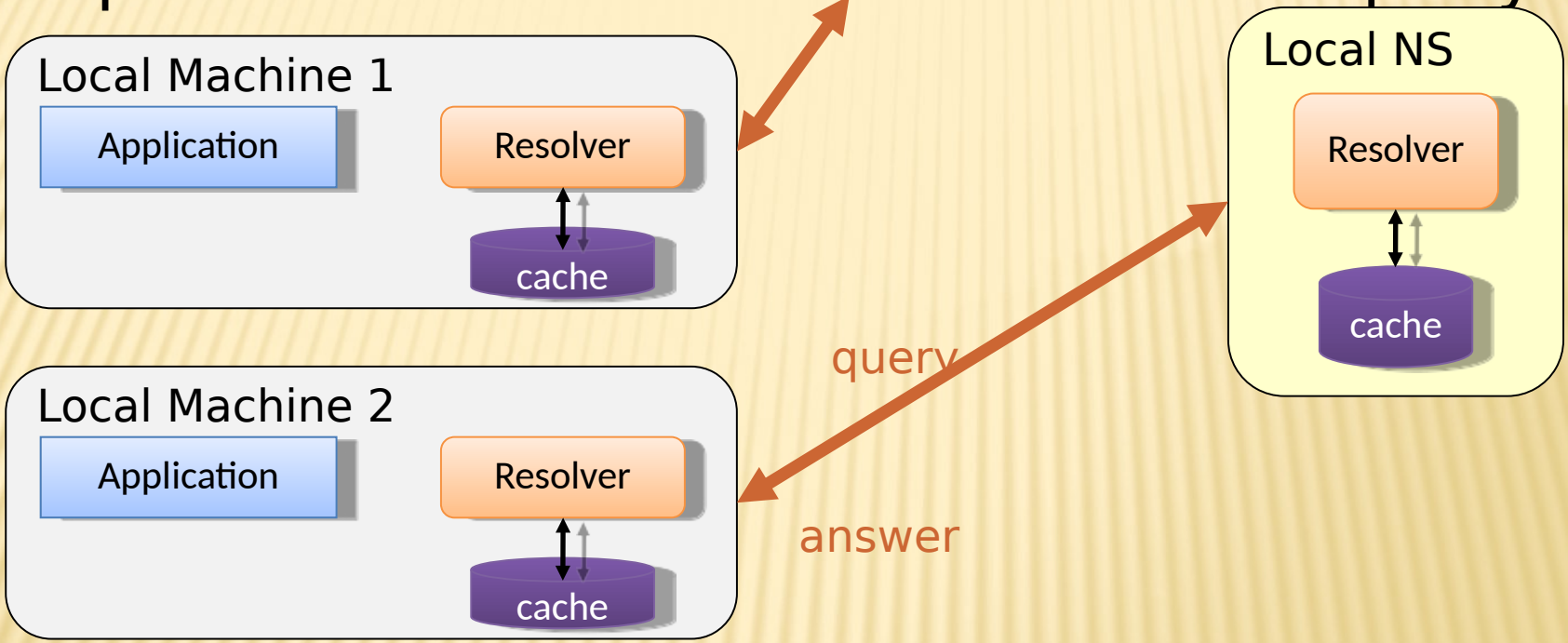


Step 2: receive reply and cache at local NS and h



DNS CACHING (CON'D)

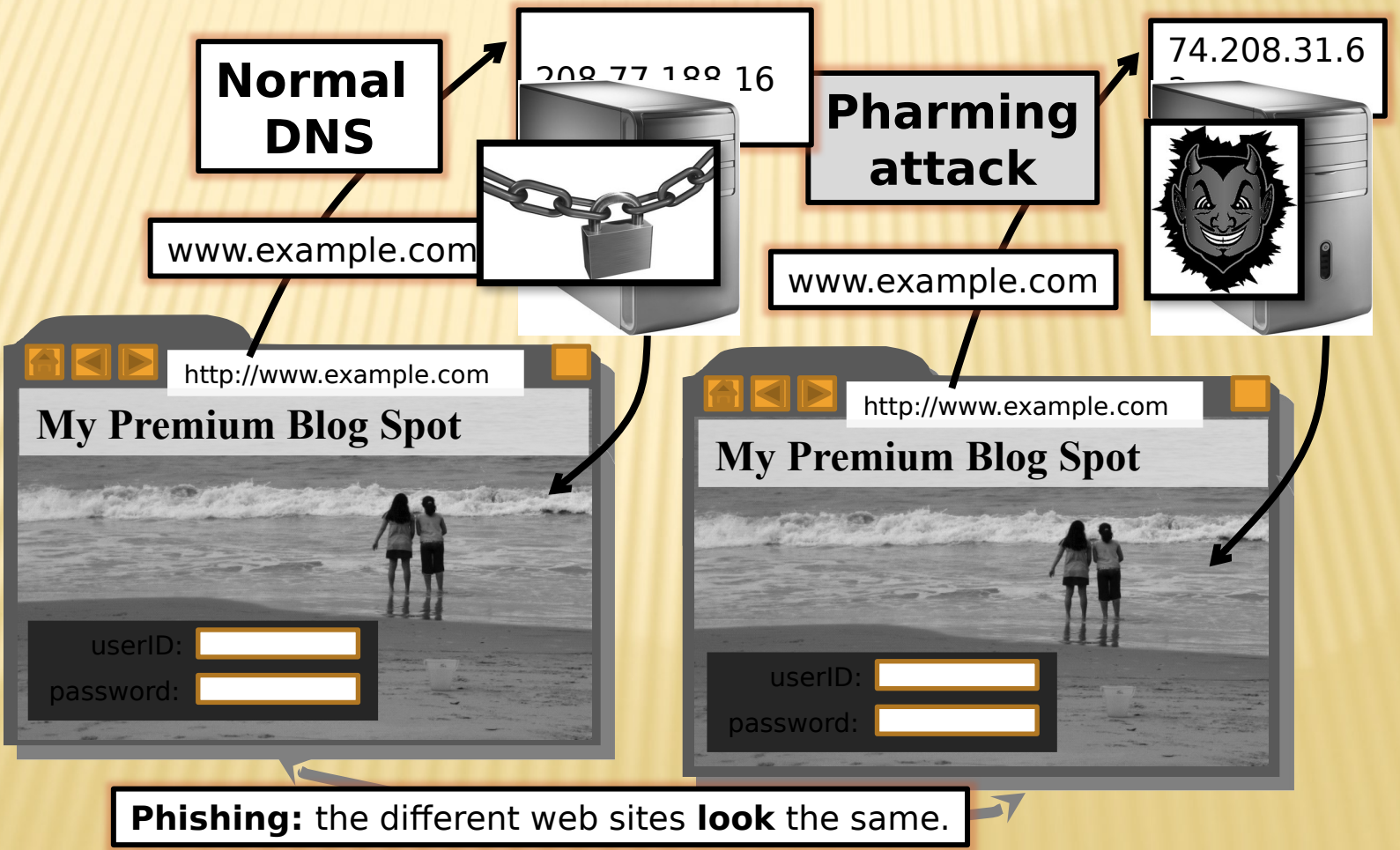
Step 3: use cached results rather than querying th



Step 4: Evict cache entries upon ttl expiration

PHARMING: DNS HIJACKING

- Changing IP associated with a server maliciously:



DNS Cache Poisoning

- Basic idea: give DNS servers false records and get it cached
- DNS uses a 16-bit request identifier to pair queries with answers
- Cache may be poisoned when a name server:
  - Disregards identifiers
  - Has predictable ids
  - Accepts unsolicited DNS records

DNS Cache Poisoning Prevention

- Use random identifiers for queries
- Always check identifiers
- Port randomization for DNS requests
- Deploy DNSSEC
  - Challenging because it is still being deployed and requires reciprocity

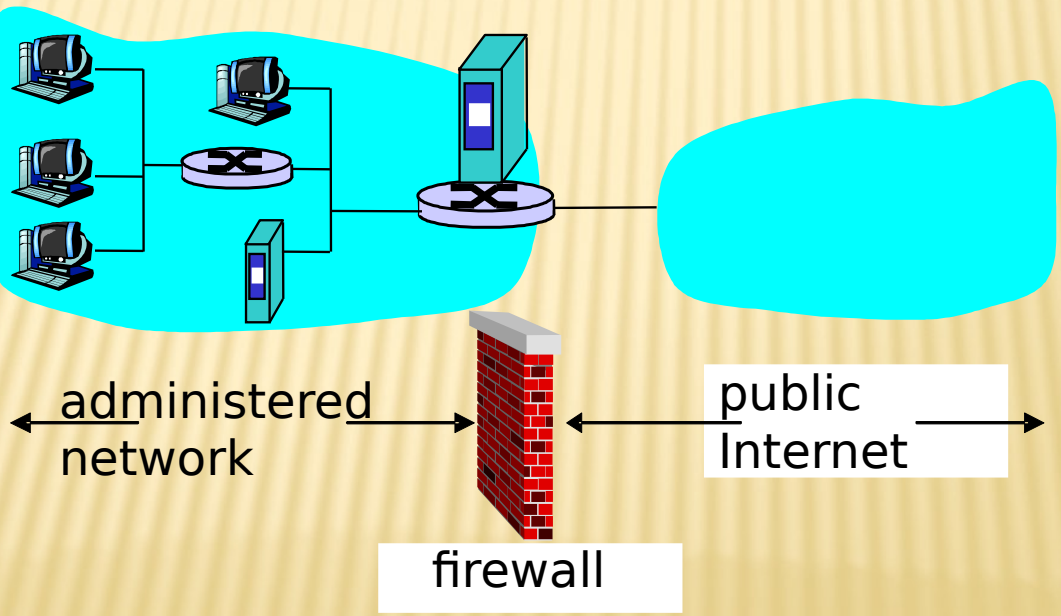
DNSSEC

- Guarantees:
  - Authenticity of DNS answer origin
  - Integrity of reply
  - Authenticity of denial of existence
- Accomplishes this by signing DNS replies at each step of the way
- Uses public-key cryptography to sign responses
- Typically use trust anchors, entries in the OS to bootstrap the process

FIREWALLS

firewall

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.



FIREWALLS: WHY

prevent denial of service attacks:

- SYN flooding: attacker establishes many bogus TCP connections, no resources left for “real” connections

prevent illegal modification/access of internal data.

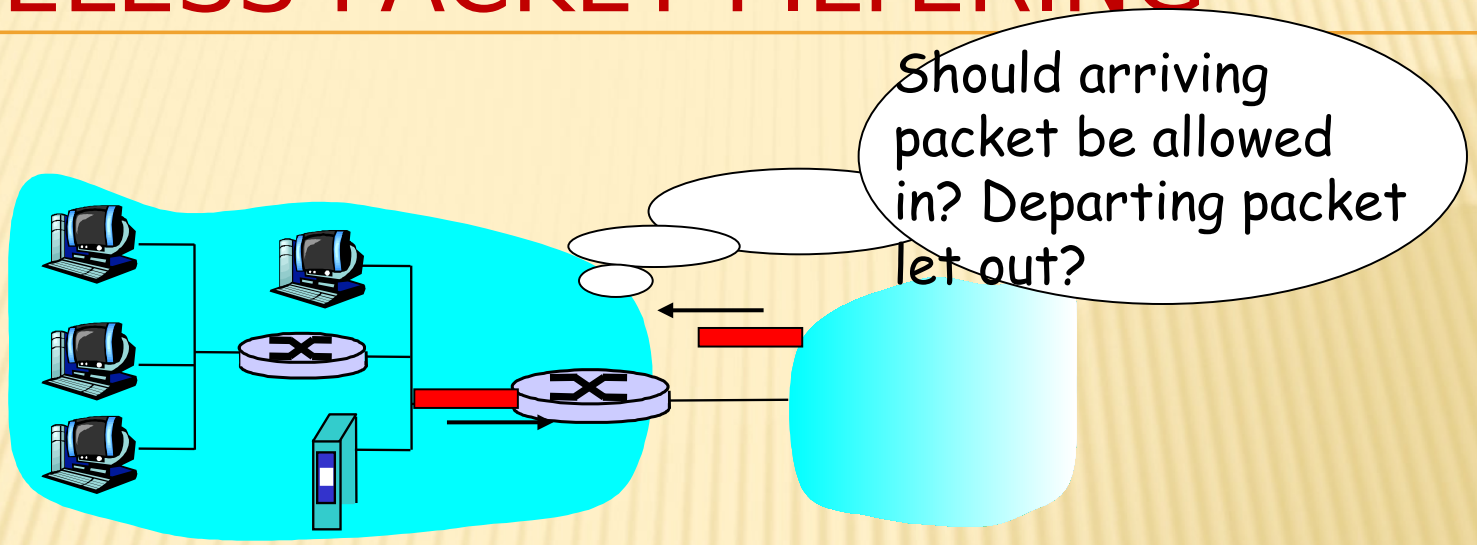
- e.g., attacker replaces CIA’s homepage with something else

allow only authorized access to inside network (set of authenticated users/hosts)

three types of firewalls:

- stateless packet filters
- stateful packet filters
- application gateways

STATELESS PACKET FILTERING



- internal network connected to Internet via router firewall
- router filters packet-by-packet, decision to forward/drop packet based on:
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type
  - TCP SYN and ACK bits

STATELESS PACKET FILTERING: EXAMPLE

- example 1: block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23.
  - all incoming, outgoing UDP flows and telnet connections are blocked.
- example 2: Block inbound TCP segments with ACK=0.
  - prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

STATELESS PACKET FILTERING: MORE EXAMPLES

Policy	Firewall Setting
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for institution's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets - except DNS and router broadcasts.
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP packets going to a "broadcast" address (eg 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

ACCESS CONTROL LISTS

- *ACL:* table of rules, applied top to bottom to incoming packets: (action, condition) pairs

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80 (web)	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53 (DNS)	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

STATEFUL PACKET FILTERING

- stateless packet filter: heavy handed tool
  - admits packets that "make no sense," e.g., dest port = 80, ACK bit set, even though no TCP connection established:

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

- *stateful packet filter:* track status of every TCP connection
  - track connection setup (SYN), teardown (FIN): can determine whether incoming, outgoing packets "makes sense"
  - timeout inactive connections at firewall: no

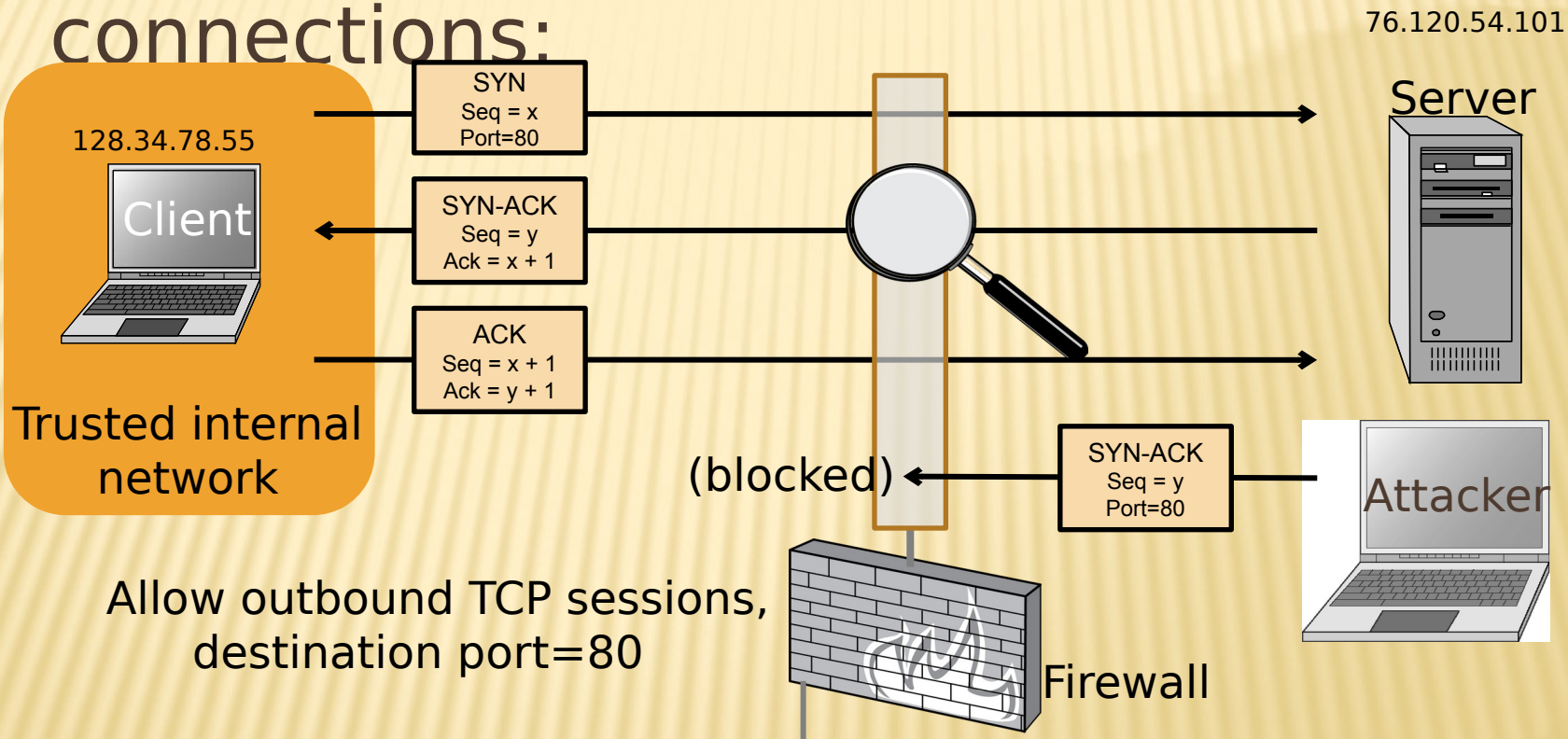
STATEFUL PACKET FILTERING

- ACL augmented to indicate need to check connection state table before admitting packet

action	source address	dest address	proto	source port	dest port	flag bit	check conxion
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

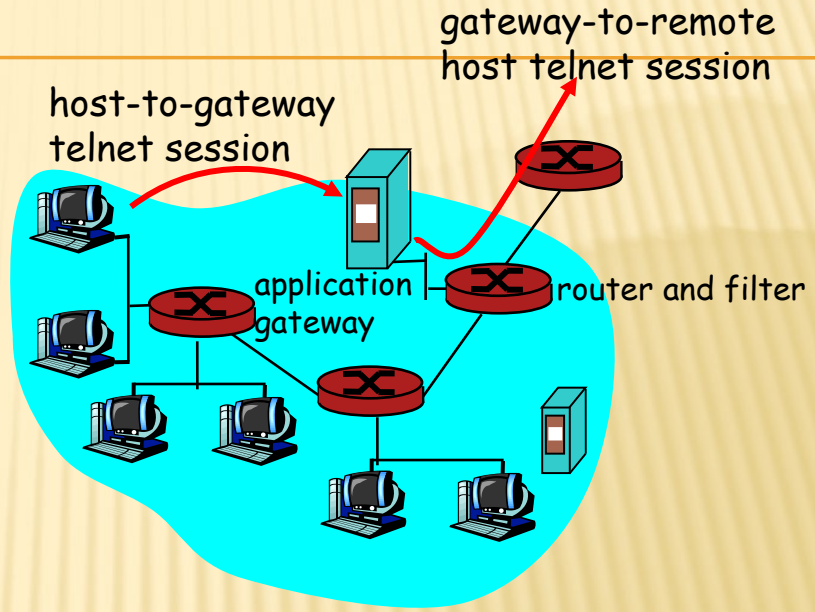
STATEFULL FIREWALL EXAMPLE

- Allow only requested TCP connections:



APPLICATION GATEWAYS

- filters packets on application data as well as on IP/TCP/UDP fields.
- example: allow select internal users to telnet outside.



1. require all telnet users to telnet through gateway.
2. for authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
3. router filter blocks all telnet connections not originating from gateway.

LIMITATIONS OF FIREWALLS AND GATEWAYS

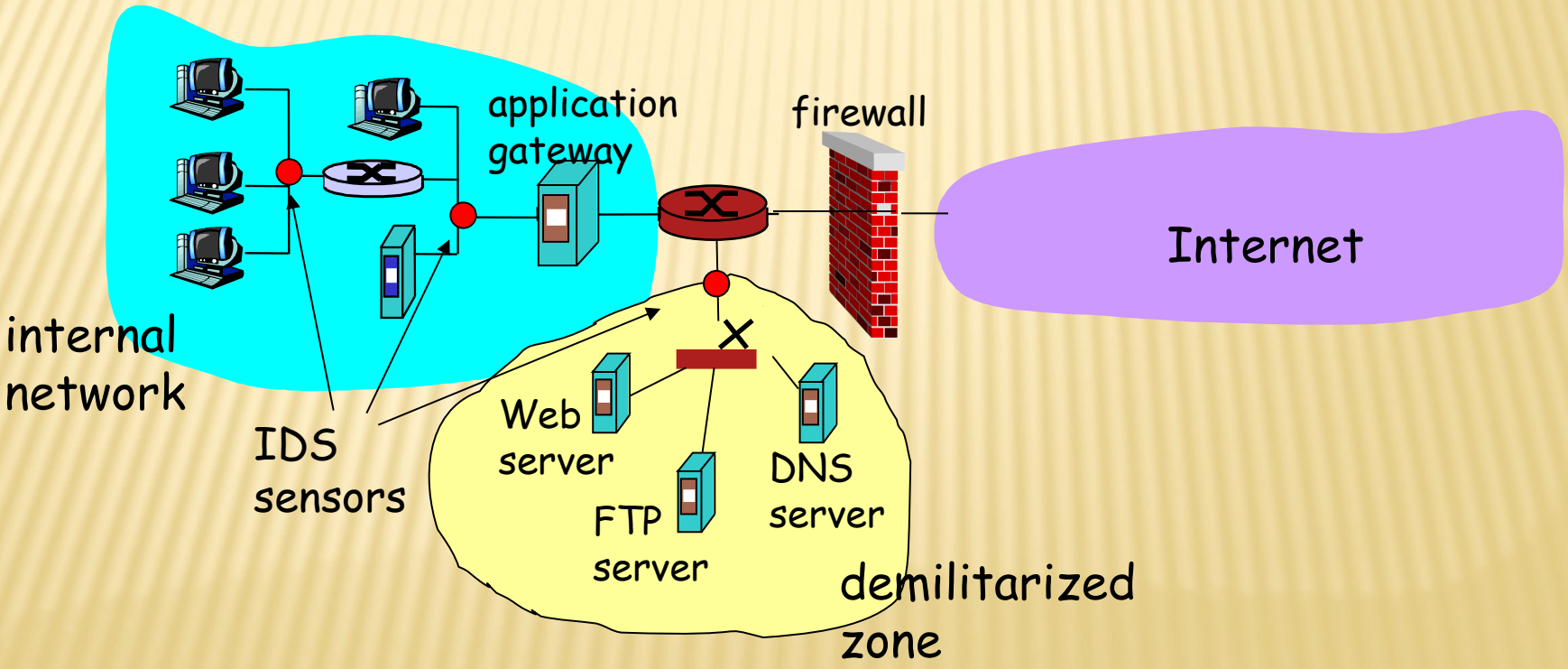
- IP spoofing: router can't know if data "really" comes from claimed source
- if multiple app's. need special treatment, each has own app. gateway.
- client software must know how to contact gateway.
  - e.g., must set IP address of proxy in Web browser
- filters often use all or nothing policy for UDP.
- tradeoff: degree of communication with outside world, level of security
- many highly protected sites still suffer from attacks.

INTRUSION DETECTION SYSTEMS

- packet filtering:
  - operates on TCP/IP headers only
  - no correlation check among sessions
- *IDS: intrusion detection system*
  - *deep packet inspection:* look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)
  - examine correlation among multiple packets
    - port scanning
    - network mapping
    - DoS attack

INTRUSION DETECTION SYSTEMS

- multiple IDSs: different types of checking at different locations



IP SECURITY (IPSEC)

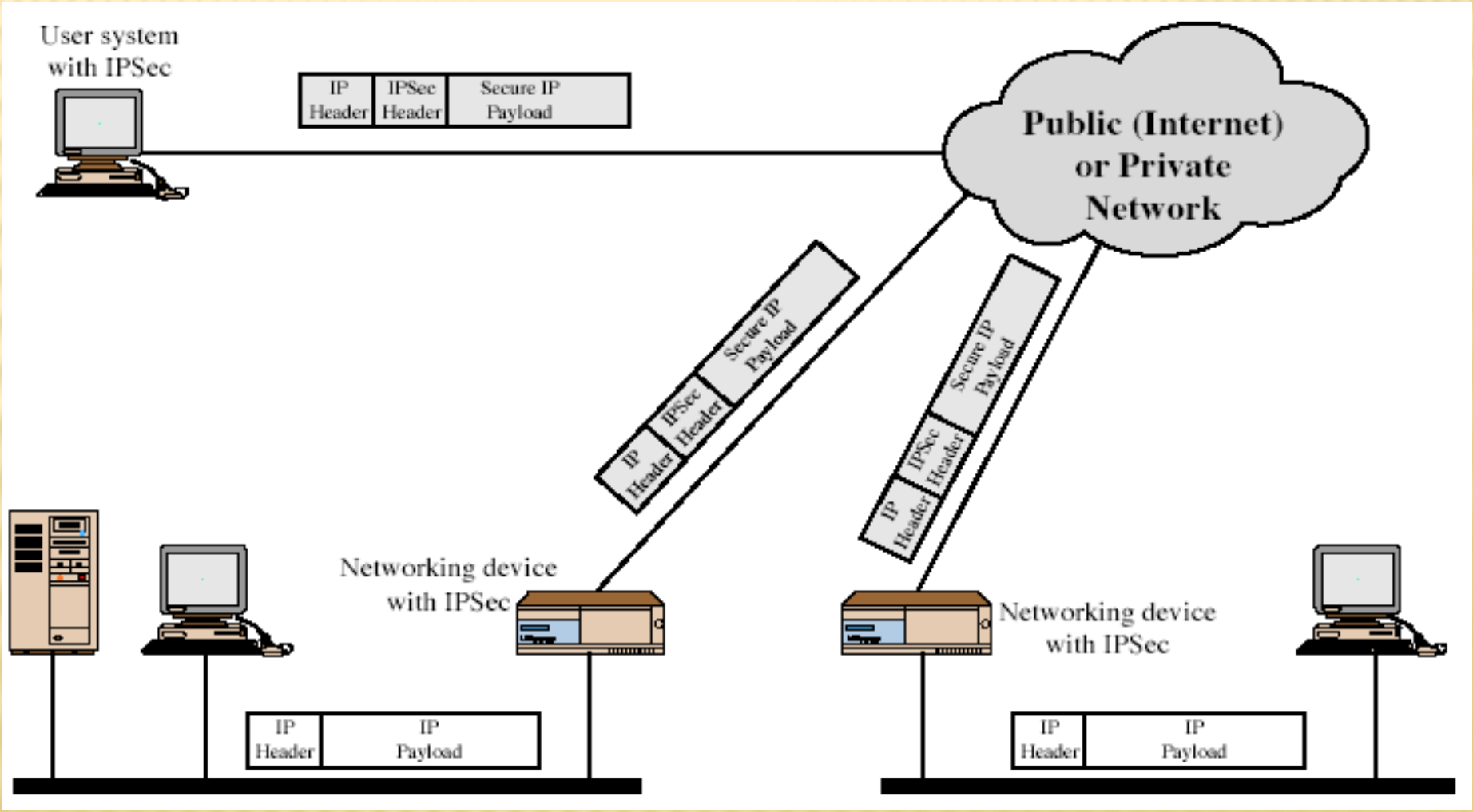
- Suite of protocols from Internet Engineering Task Force (IETF) providing encryption and authentication at the IP layer
  - Arose from needs identified in RFC 1636
  - Specifications in:
    - RFC 2401: Security architecture
    - RFC 2402: Authentication
    - RFC 2406: Encryption
    - RFC 2408: Key management
- Objective is to encrypt and/or authenticate **all** traffic at the IP level.

IP SECURITY ISSUES

- Eavesdropping
- Modification of packets in transit
- Identity spoofing (forged source IP addresses)
- Denial of service

- Many solutions are application-specific
  - TLS for Web, S/MIME for email, SSH for remote login
- IPSec aims to provide a framework of open standards for secure communications over IP
  - Protect every protocol running on top of IPv4 and IPv6

TYPICAL USAGE



IPSEC SERVICES

- Data origin authentication
- Confidentiality
- Connectionless and partial sequence integrity
  - Connectionless = integrity for a single IP packet
  - Partial sequence integrity = prevent packet replay
- Limited traffic flow confidentiality
  - Eavesdropper cannot determine who is talking
- These services are transparent to applications above transport (TCP/UDP) layer

Major IPSec Components

- Security Association (SA) Database
  - Each SA refers to all the security parameters of one communication direction
  - For two-way communications, at least two SAs are needed.
- Two Protocols
  - AH – Authentication Header
  - ESP – Encapsulating Security Payload
    1. Encryption only
    2. Encryption with authentication
- Two Encapsulation modes
    1. Transport mode
    2. Tunnel mode

USES OF IPSEC

- **Virtual Private Network (VPN) establishment**
  - For connecting remote offices and users using public Internet
- **Low-cost remote access**
  - e.g. teleworker gains secure access to company network via local call to ISP
- **Extranet connectivity**
  - Secure communication with partners, suppliers, etc.

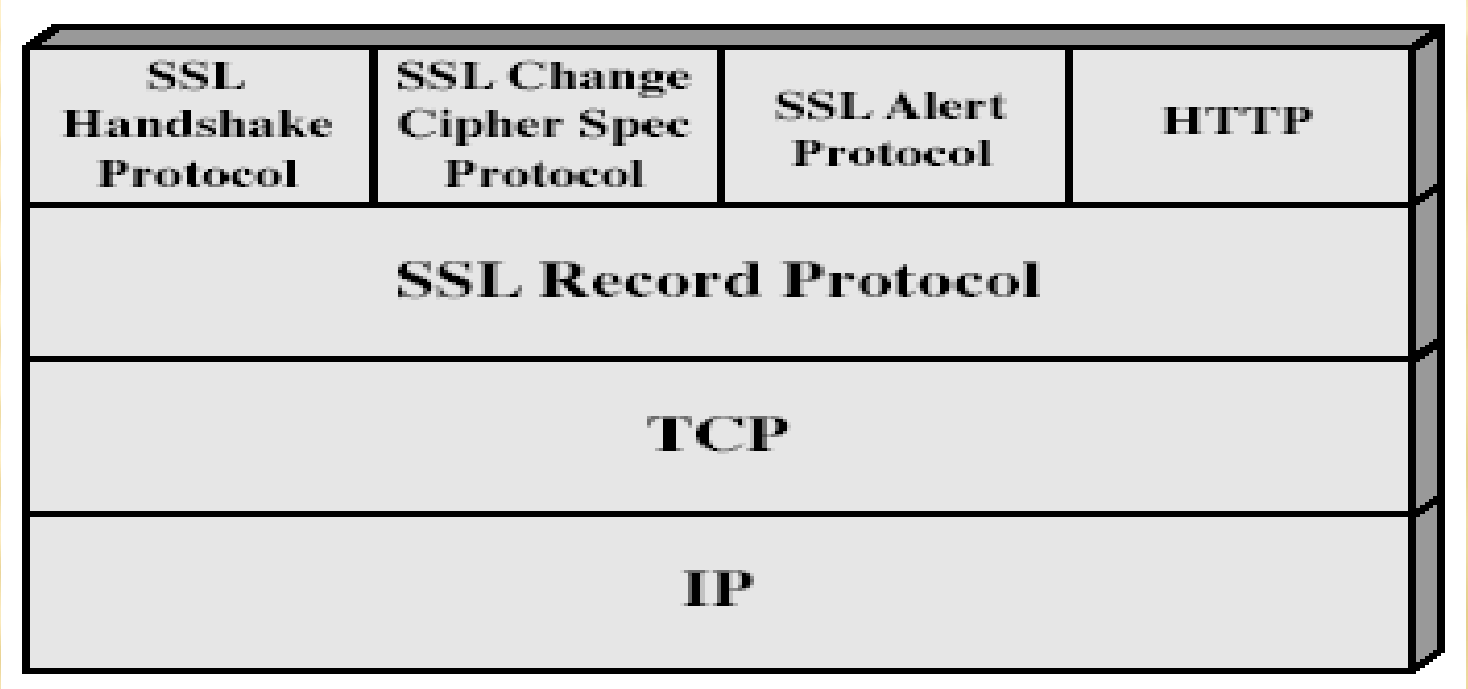
WEB SECURITY

- Web now widely used by business, government, individuals
- but Internet & Web are vulnerable
- have a variety of threats
  - integrity
  - confidentiality
  - denial of service
  - authentication
- need added security mechanisms

SSL (SECURE SOCKET LAYER)

- transport layer security service
- originally developed by Netscape
- version 3 designed with public input
- subsequently became Internet standard known as TLS (Transport Layer Security)
- uses TCP to provide a reliable end-to-end service
- SSL has two layers of protocols

SSL ARCHITECTURE



SSL ARCHITECTURE

- **SSL session**
  - an association between client & server
  - created by the Handshake Protocol
  - define a set of cryptographic parameters
  - may be shared by multiple SSL connections
- **SSL connection**
  - a transient, peer-to-peer, communications link
  - associated with 1 SSL session

SSL RECORD PROTOCOL

- **confidentiality**
  - using symmetric encryption with a shared secret key defined by Handshake Protocol
  - IDEA, RC2-40, DES-40, DES, 3DES, RC4-40, RC4-128
  - message is compressed before encryption
- **message integrity**
  - using a MAC with shared secret key
  - similar to HMAC but with different padding

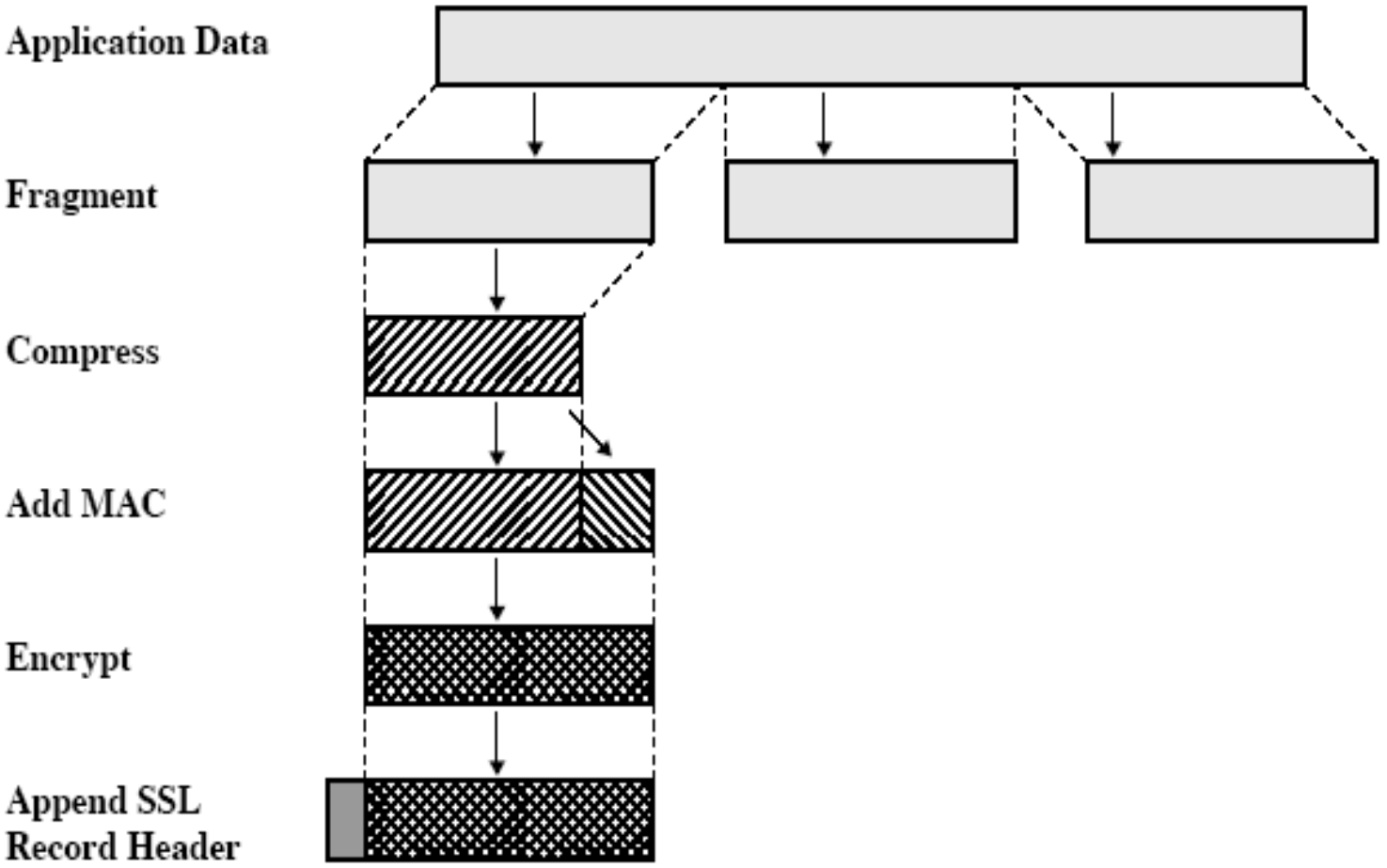


Figure 17.3 SSL Record Protocol Operation

SSL CHANGE CIPHER SPEC PROTOCOL

- one of 3 SSL specific protocols which use the SSL Record protocol
- a single message
- causes pending state to become current
- hence updating the cipher suite in use

TLS (TRANSPORT LAYER SECURITY)

- IETF standard RFC 2246 similar to SSLv3
- with minor differences
  - in record format version number
  - uses HMAC for MAC
  - a pseudo-random function expands secrets
  - has additional alert codes
  - some changes in supported ciphers
  - changes in certificate negotiations
  - changes in use of padding

IEEE 802.11 SECURITY

- *war-driving:* drive around Bay area, see what 802.11 networks available?
  - More than 9000 accessible from public roadways
  - 85% use no encryption/authentication
  - packet-sniffing and various attacks easy!
- securing 802.11
  - encryption, authentication
  - first attempt at 802.11 security: Wired Equivalent Privacy (WEP): a failure
  - current attempt: 802.11i

WIRED EQUIVALENT PRIVACY (WEP):

- authentication
  - host requests authentication from access point
  - access point sends 128 bit nonce
  - host encrypts nonce using shared symmetric key
  - access point decrypts nonce, authenticates host
- no key distribution mechanism
- authentication: knowing the shared key is enough

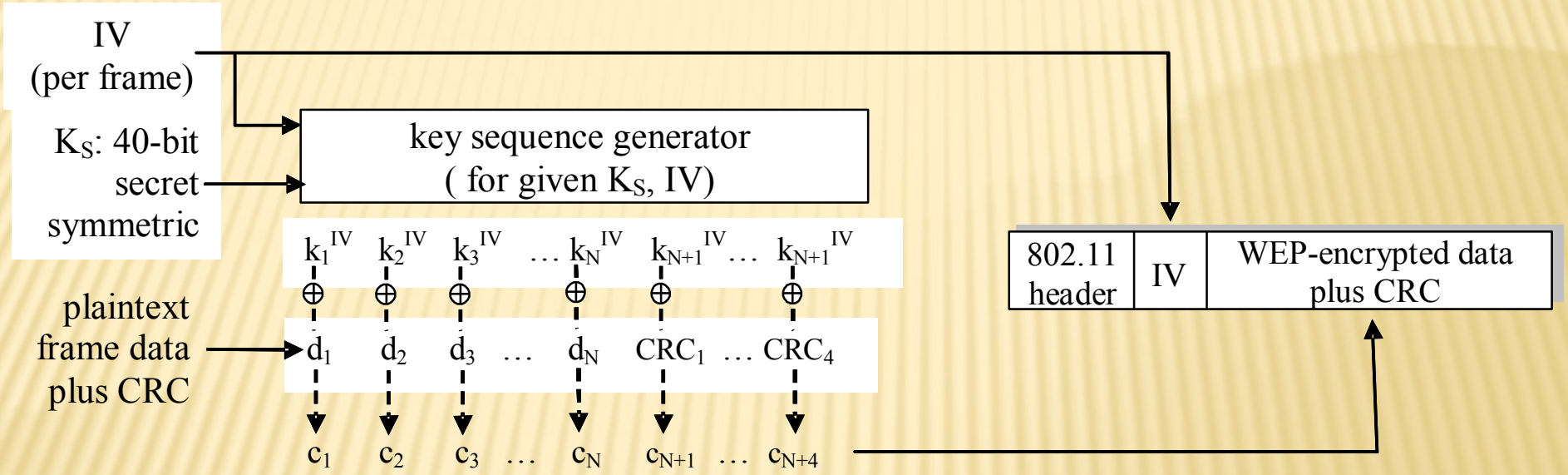
WEP DATA ENCRYPTION

- host/AP share 40 bit symmetric key (semi-permanent)
- host appends 24-bit initialization vector (IV) to create 64-bit key
- 64 bit key used to generate stream of keys, k_i^{IV}
- k_i^{IV} used to encrypt ith byte, d_i, in frame:

$$c_i = d_i \text{ XOR } k_i^{IV}$$

- IV and encrypted bytes, c_i sent in frame

802.11 WEP ENCRYPTION



Sender-side WEP encryption :ol

BREAKING 802.11 WEP ENCRYPTION

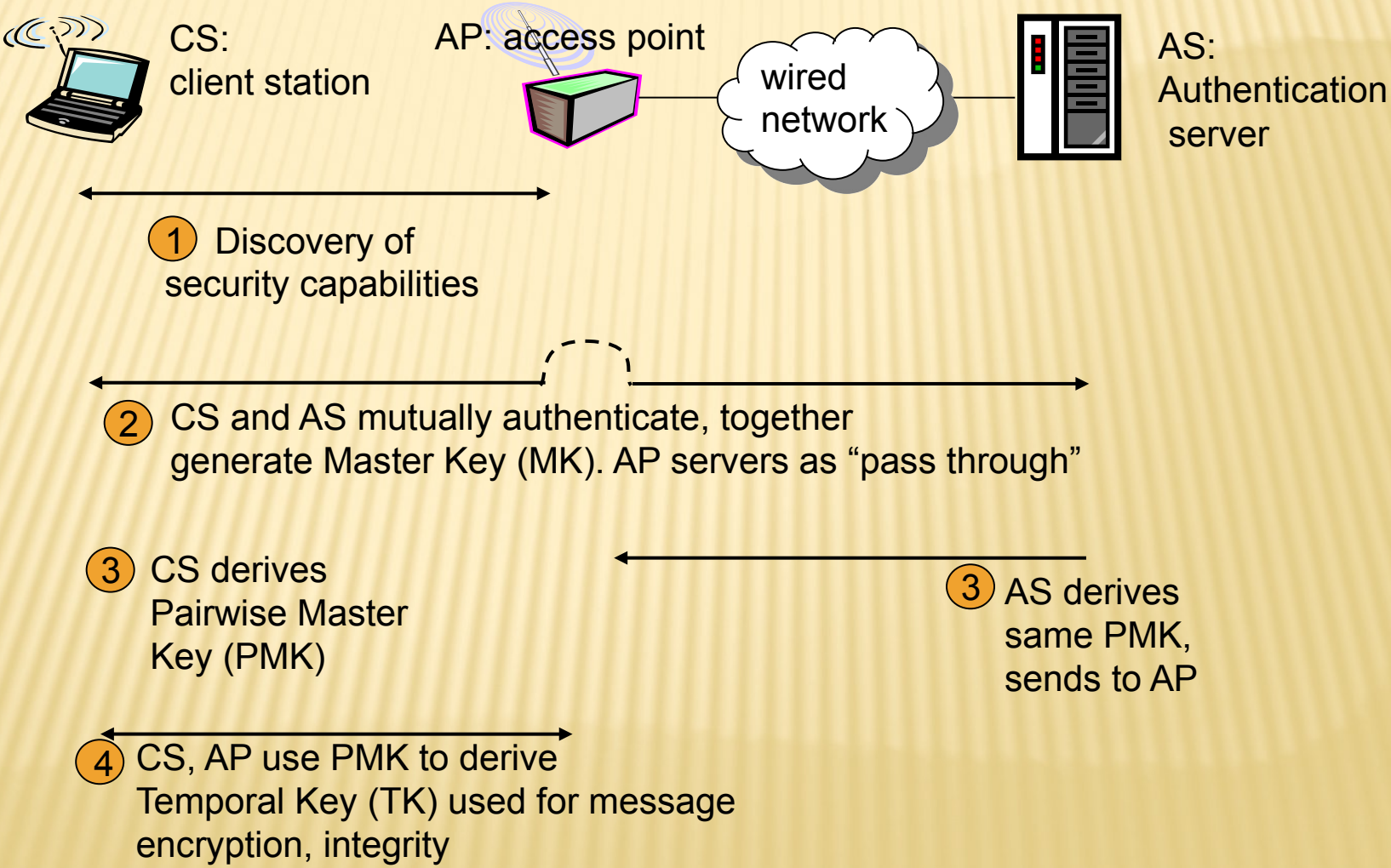
security hole:

- 24-bit IV, one IV per frame, -> IV's eventually reused
- IV transmitted in plaintext -> IV reuse detected
- attack:
  - Trudy causes Alice to encrypt known plaintext d_1 d_2 d_3 d_4 …
  - Trudy sees: $c_i = d_i$ XOR k_i^{IV}
  - Trudy knows c_i d_i, so can compute k_i^{IV}
  - Trudy knows encrypting key sequence k_1^{IV} k_2^{IV} k_3^{IV} …
  - Next time IV is used, Trudy can decrypt!

802.11I: IMPROVED SECURITY

- numerous (stronger) forms of encryption possible
- provides key distribution
- uses authentication server separate from access point

802.11I: FOUR PHASES OF OPERATION



VIRUSES, WORMS, TROJANS, ROOTKITS

- Malware can be classified into several categories, depending on propagation and concealment
- Propagation
  - Virus: human-assisted propagation (e.g., open email attachment)
  - Worm: automatic propagation without human assistance
- Concealment
  - Rootkit: modifies operating system to hide its existence
  - Trojan: provides desirable functionality but hides malicious operation
- Various types of payloads, ranging from annoyance to crime

INSIDER ATTACKS

- An **insider attack** is a security breach that is caused or facilitated by someone who is a part of the very organization that controls or builds the asset that should be protected.
- In the case of malware, an insider attack refers to a security hole that is created in a software system by one of its programmers.

DEFENSES AGAINST INSIDER ATTACKS

- Avoid single points of failure.
- Use code walk-throughs.
- Use archiving and reporting tools.
- Limit authority and permissions.
- Physically secure critical systems.
- Monitor employee behavior.
- Control software installations.

CSC459-ITC459-Security Engineering

System Security

Dr. Mehrdad Sharbaf

CSUDH-CSC

System Security (1 of 4)

Vital part of every computer system

System security concepts

CIA triangle: shows main elements used to develop a security policy

- Confidentiality
- Integrity
- Availability

System Security (2 of 4)

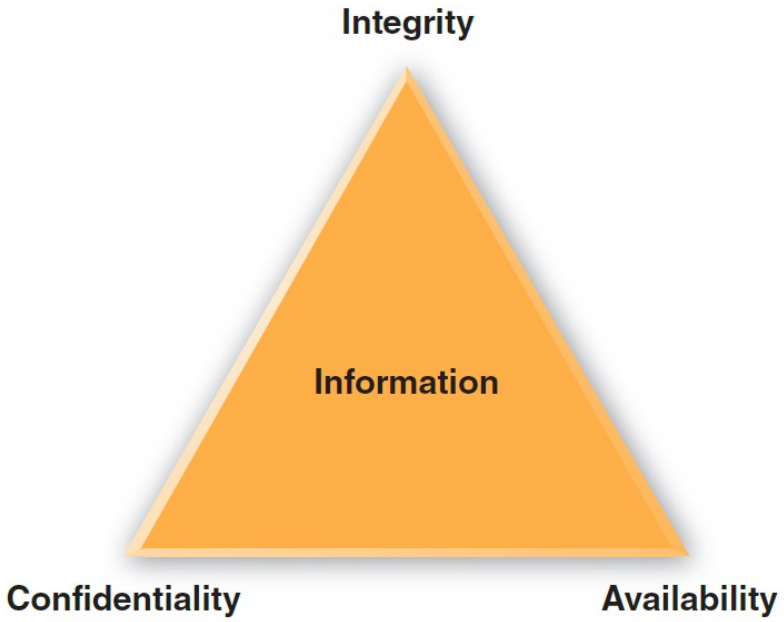


Figure 12-14 System security must provide information confidentiality, integrity, and availability (CIA).

System Security (3 of 4)

- Risk management
  - Risk identification
    - List and classify assets and analyze possible threats
    - Identify vulnerabilities and how they might be exploited
  - Risk assessment
    - Risks need to be calculated and prioritized
  - Risk control
    - Strategies: avoidance, mitigation, transference, and acceptance

System Security (4 of 4)

- **Figure 12-15** Risk management requires continuous risk identification, assessment, and control.

The slides are excerpted from Tilley 12 edition systems analysis and design book

Security Levels (1 of 12)

- System security involves six separated but interrelated levels

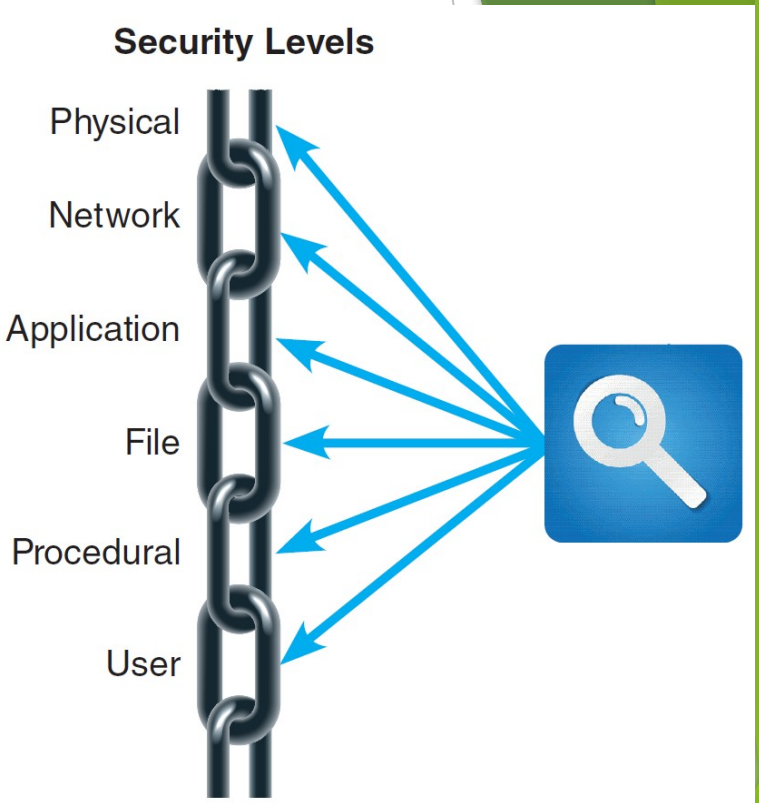


Figure 12-19 Each security link has a specific focus, and the overall chain is only as strong as the weakest link.

The slides are excerpted from Tilley 12 edition systems analysis and design book

Security Levels (2 of 12)

- Physical security
  - Operations center security
    - Each entrance must be equipped with a suitable security device
  - Servers and desktop computers
    - Install locks on server racks to avoid unauthorized placement of keystroke loggers
    - Tamper evident cases and BIOS-level passwords can be used

The slides are excerpted from Tilley 12 edition systems analysis and design book

Security Levels (3 of 12)

- Portable computers
  - Select an operating system with strong protection
  - Mark case with company name and address
  - Consider devices that have a built-in fingerprint reader, facial recognition, and use the Universal Security Slot (USS)
  - Back up all vital data before using the computer outside the office and link the system to a tracking software
  - Use location services
  - Be alert to high-risk situations while traveling
  - Establish stringent password protection policies

Security Levels (4 of 12)

- Network security
  - Encrypt network traffic: private key encryption and public key encryption
  - Wireless networks: WPA2 strengthens the level of wireless protection
  - Private networks can be used when speed is necessary
  - Virtual Private Networks (VPN) establish secure connections for a large number of computers

Security Levels (5 of 12)

Ports and services can be affected by port scans and denial of service (DOS) attacks

- A port routes incoming traffic to the correct application and a service monitors a particular port

Firewalls allow or block network traffic from each network interface based on preset rules

Network intrusion detection system (NDIS) alerts the administrator when it detects suspicious network traffic patterns

The slides are excerpted from Tilley 12 edition systems analysis and design book

Security Levels (6 of 12)

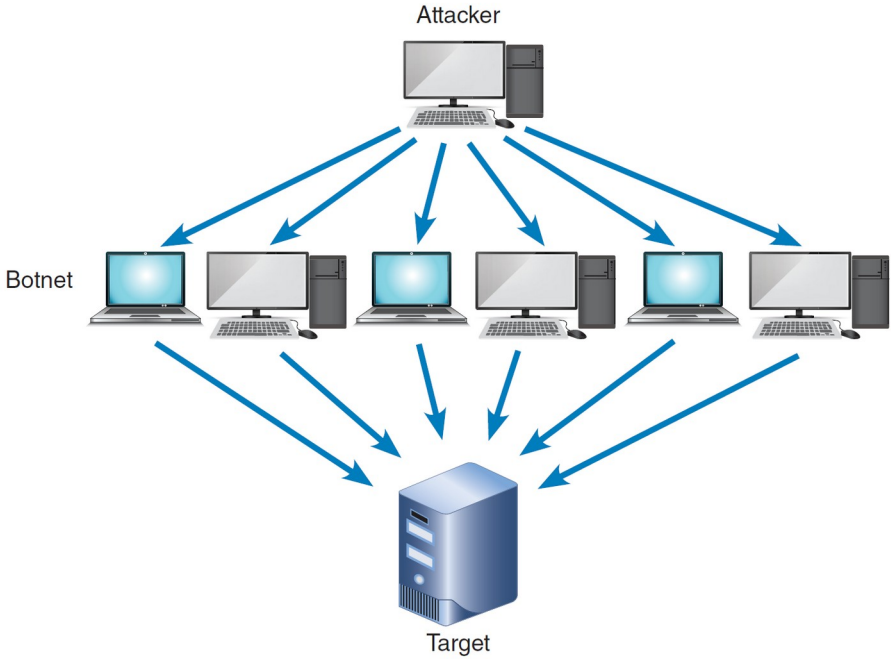
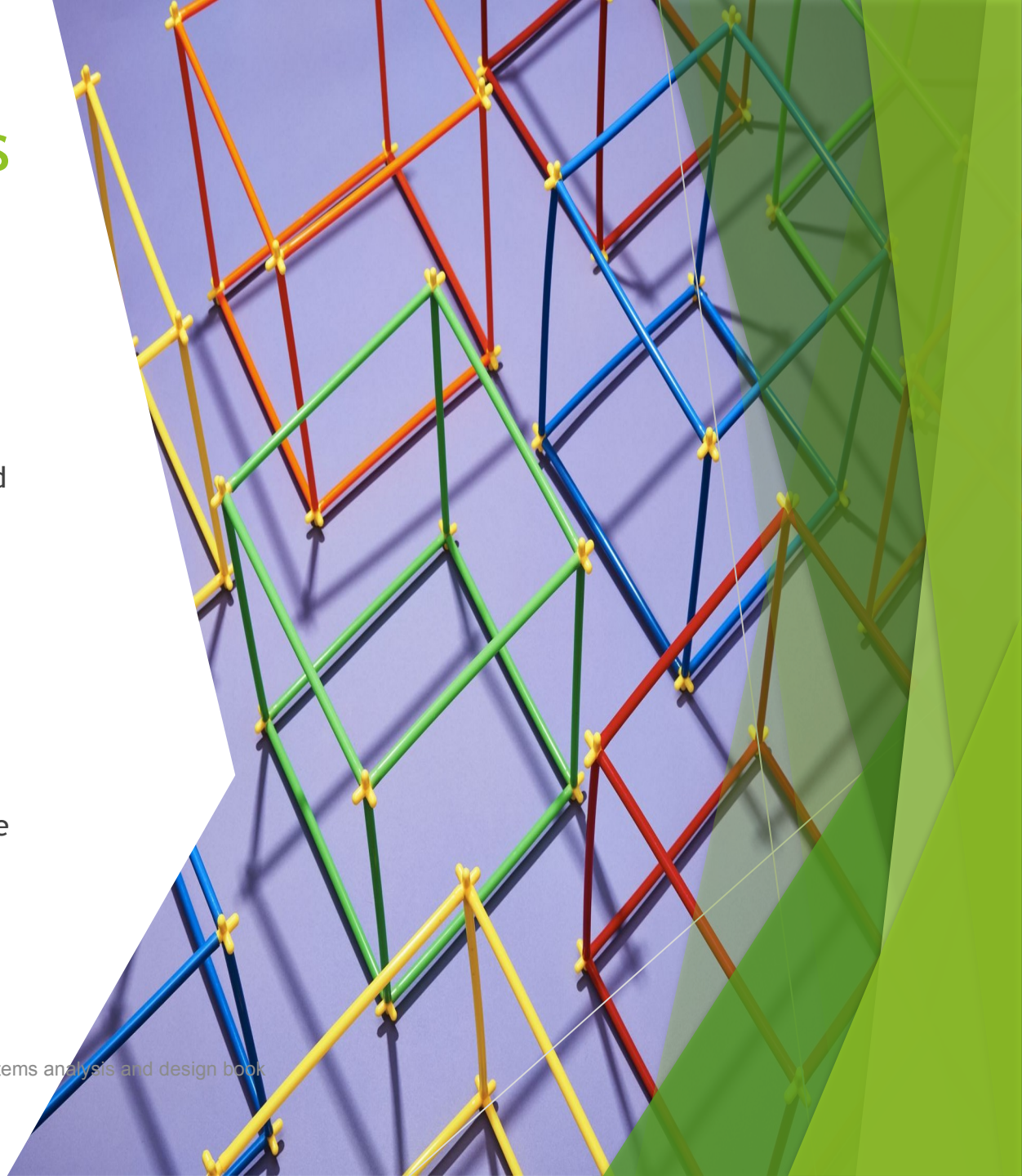


FIGURE 12-22: In a DoS attack, an attacker sends numerous authentication requests with false return addresses. The server tries unsuccessfully to send out authentication approval and is eventually disabled by the floor of requests. More sophisticated DoS attacks are distributed (DDoS), as shown in this figure. Instead of a single computer, the attacker uses an army of botnets (computers unknowingly infected with malware that are difficult to trace) to attack the target.

The slides are excerpted from Tilley 12 edition systems analysis and design book

Security Levels (7 of 12)



- Application security
  - Services that are not needed must be disabled
  - Unnecessary or improperly configured service could create a security hole
  - Hardening removes unnecessary accounts, services, and features
  - Application permissions: must be configured to be run by users who have specific rights
  - Input validation helps safeguard data integrity and security

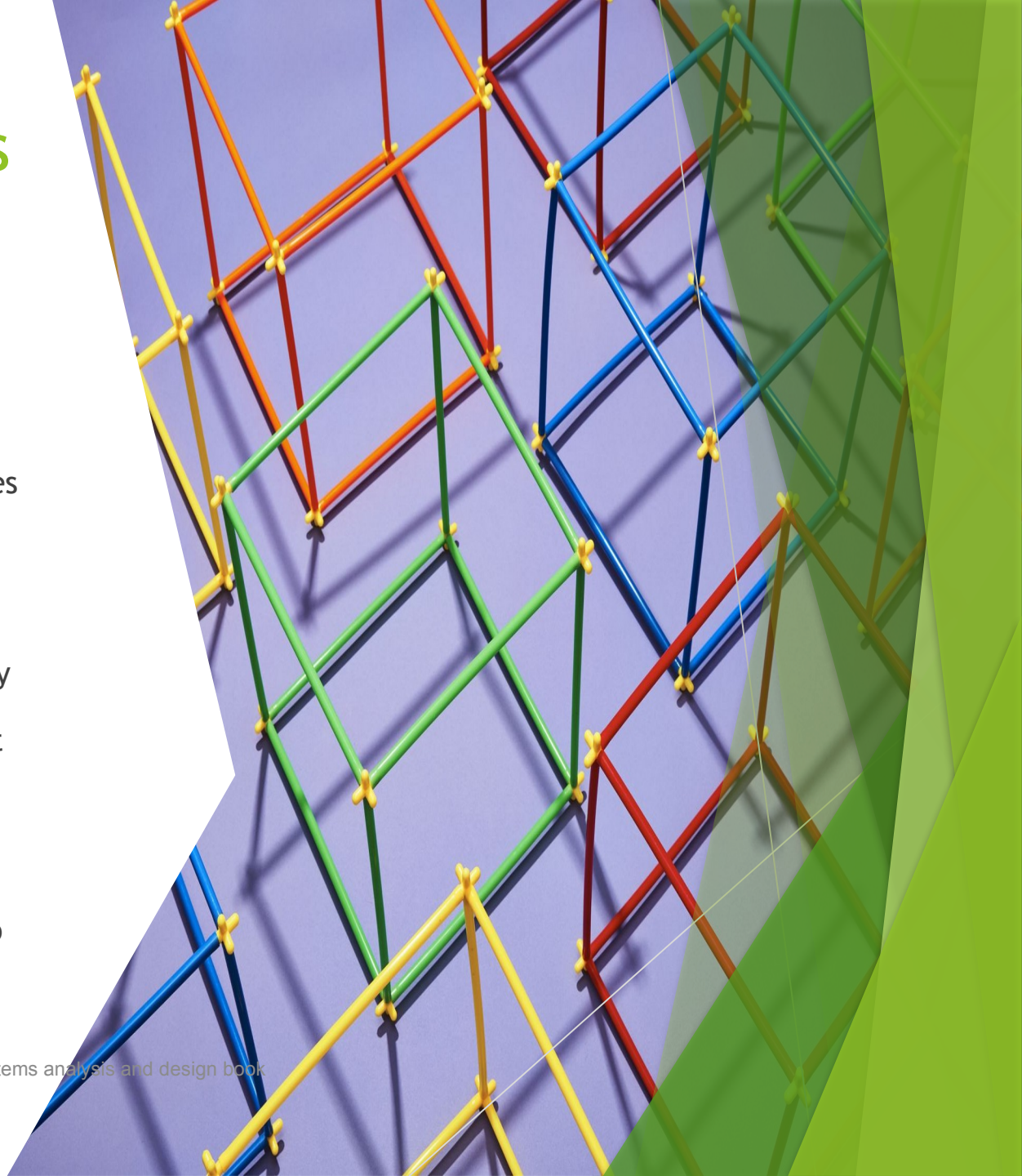
Security Levels (8 of 12)

- Patches and updates are used to repair security holes, reduce vulnerabilities, and update the system
- Software logs document all events and help understand past attacks and prevent future intrusions

Security Levels (9 of 12)

- File security
  - Encryption: scrambles the contents of a file or document to protect it from unauthorized access
  - Permissions: describe the rights a user has to a particular file or directory on a server
  - User groups: administrators can create user groups and assign file permissions

Security Levels (10 of 12)



- User security
  - Identity management: controls and procedures necessary to identify legitimate users and system components
  - Password protection: policies need to specify a set minimum length, complexity, and a limit on invalid attempts
  - Social engineering: intruder uses social interaction to gain unauthorized access to a computer system

Security Levels (11 of 12)

User resistance: users need to understand and be a part of the organization's commitment to security

New technologies can be used to enhance security and prevent unauthorized access

- Security token is a physical device that authenticates legitimate users

Security Levels (12 of 12)

- Procedural security (operational security)
  - Policies and controls that ensure secure operations
  - Defines how particular tasks are to be performed
  - Includes safeguarding procedures that would be valuable to an attacker
  - Organization must explain procedures and issue reminders that will make security issues a priority

The slides are excerpted from Tilley 12 edition systems analysis and design book

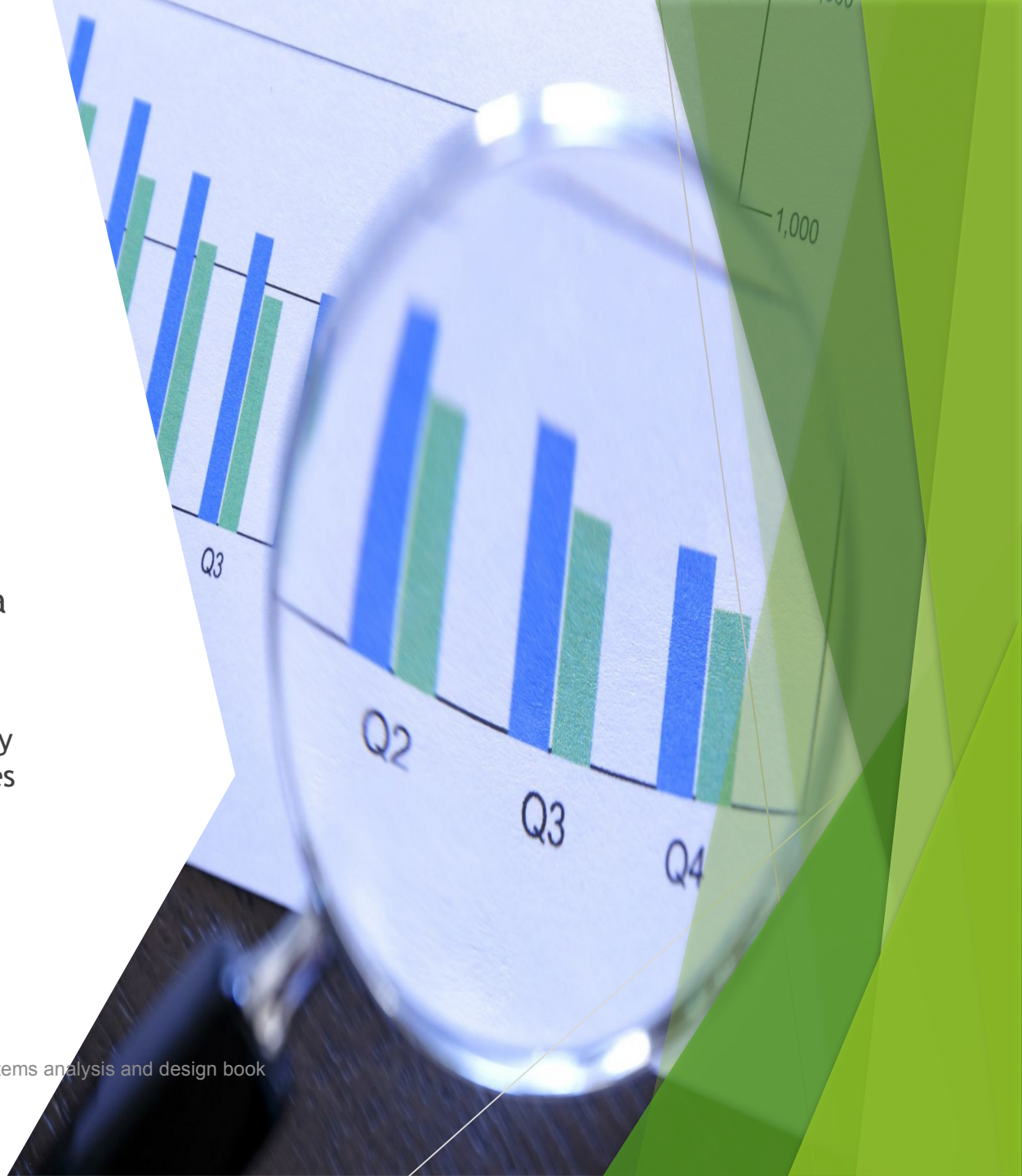
Backup and Recovery (1 of 2)

- Backup policies
  - Backup media: includes tape, hard drives optical and online storage
    - Offsiting: storing backup away from main location
    - Cloud-based storage is growing rapidly
  - Backup types: full, differential, incremental, and continuous
  - Retention periods: backups are stored for a specific time beyond which they are either destroyed or reused

The slides are excerpted from Tilley 12 edition systems analysis and design book

Backup and Recovery (2 of 2)

- Business continuity issues
  - A disaster recovery plan should be created along with a test plan
    - Often part of a business continuity plan (BCP): defines how critical business functions can continue during a major disruption



System Retirement

- Factors
  - Maintenance increasing steadily
  - Operational costs or times increasing rapidly
  - Software package provides the same or additional services more efficiently
  - New technology offers a way to perform the same or additional functions more efficiently
  - Maintenance changes or additions are difficult and expensive to perform
  - Users request significant new features

Future Challenges and Opportunities (1 of 3)

- Trends and predictions
  - Cybercrime will increase significantly
  - Smartphones and tablets will become the dominant computing platform
  - Software-as-a-Service will become the norm
  - Cloud computing will become the principal computing infrastructure
  - Insourcing will increase
  - Large enterprises may require suppliers to certify green credentials and sourcing policies

Future Challenges and Opportunities (2 of 3)

Strategic planning for IT professionals

System analysts should work backwards from goals to develop intermediate milestones

IT credentials and certification

Professional organizations and IT industry leaders offer continuing educational courses and credentialed certifications

Critical thinking skills

System analysts should possess soft skills and critical thinking skills

The slides are excerpted from Tilley 12 edition systems analysis and design book

Future Challenges and Opportunities (3 of 3)

- Cyberethics
  - As computers permeate more and more of our lives, the decisions made by IT professionals can have serious implications
  - Situations may arise involving ethical considerations that are not easy to resolve
  - Ethical, social, and legal aspects of IT are topics that today's systems analyst should be prepared to address

Summary (1 of 3)

Systems support and security	Types of system maintenance	Maintenance team
• Implementation of an information system until the system no longer is used	• Corrective, adaptive, perfective and preventative	• Systems analysts and programmers

Summary (2 of 3)

Configuration management and system performance measurements

- Necessities of maintenance management

Security is a vital part of every computer system

- Risk management identifies, analyzes, anticipates and reduces risk to an acceptable level
- Data backup and recovery plans are essential

Summary (3 of 3)

All information systems eventually become obsolete

Intense competition is predicted in the future

IT professionals should have a strategic career plan

Long-term goals

Intermediate milestones

The slides are excerpted from Tilley 12 edition systems analysis and design book