



*SECURITY
ARCHITECTURE &
MODELS*



Computer Organization & Configuration

- **Open systems**
 - **Systems employing standard interfaces**
 - Shared by other vendors
 - Permits interoperability
 - **User provided with access to total system capability**
- **Closed systems**
 - **Systems without standard interfaces**
 - Lacks interoperability with other vendor systems
 - **User limited to single proprietary language**



Configuration (Cont.)

Multi-tasking

- **Concurrent performance/interleaved execution of 2 or more tasks**

Multiprogramming

- **Interleaved execution of 2 or more programs by a processor**

Multiprocessing

- **Simultaneous execution of 2 or more programs by a computer**
- **Parallel processing by 2 or more processors of a multiprocessor**

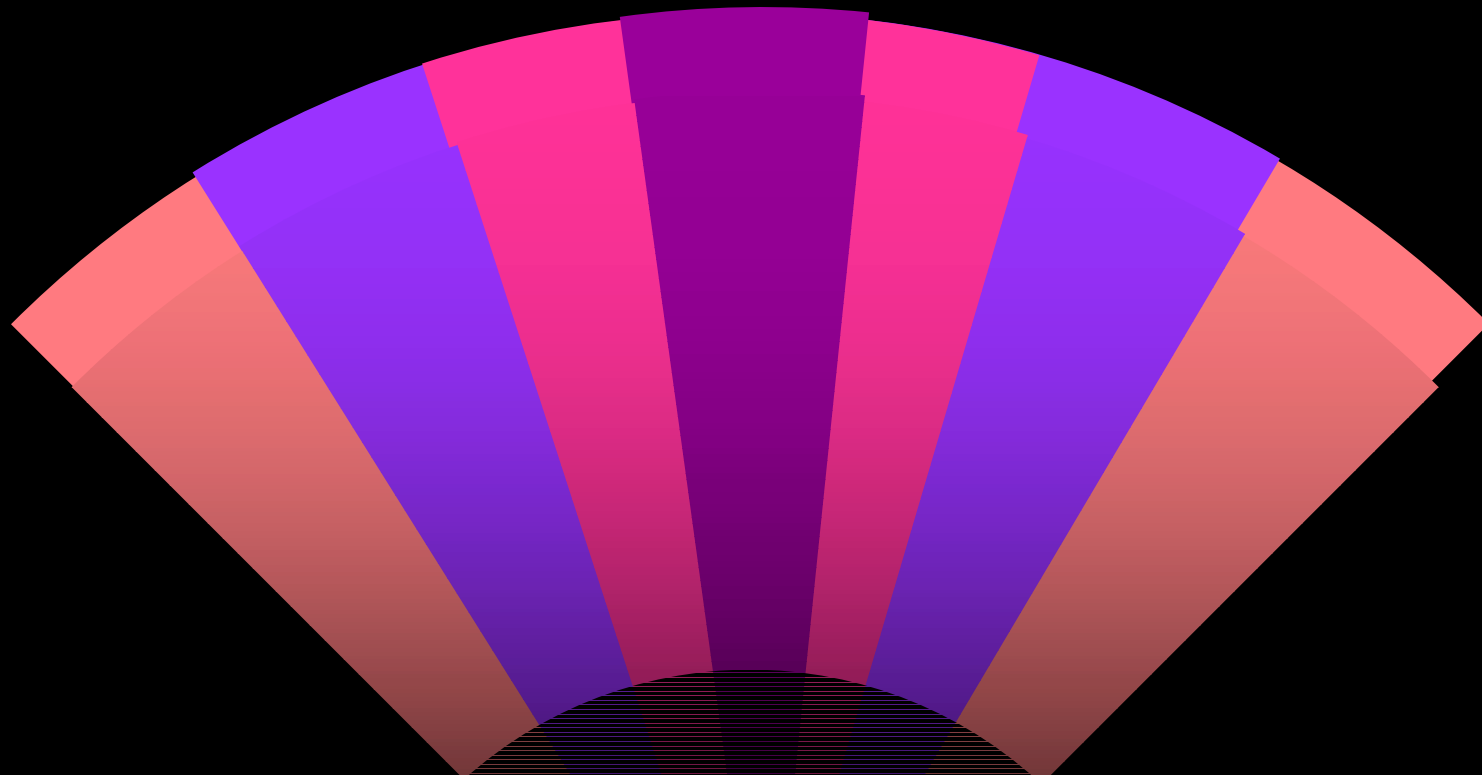
Multiprocessor

- **Computer with 2 or more processors having common access to main storage**



Configuration (Cont.)

- **Isolation/mediation**
 - **Hardware isolation**
 - TCB from untrusted parts of the system
 - **Software isolation**
 - Containment of subjects and objects
 - Separated from each other
 - Separated from protection controls of operating system
 - **Software mediation**
 - Control of subject access to system resources
- **State**
 - **Set of values of all entity attributes in a system**



Security & Control Concepts



Security Concepts

- Capability
 - Ticket/token conferring access rights to a resource
- Token value
 - Specific privilege/capability conferred
 - Read/write/execute/etc.
- Parameter
 - Value/option indicating action to be accomplished or object to be accessed
- Resource manager
 - Allocates CPU, main storage, auxiliary storage space, & I/O devices to user programs



Security Concepts (Cont.)

- Security perimeter
 - The security kernel as well as other security-related system functions, are within the (imaginary) boundary of the TCB, i.e., the security perimeter
 - System elements outside the security perimeter need not be trusted. For example, an entire computer system or a LAN, might be inside a security perimeter and connected to outside systems/networks via a trusted system called a gateway



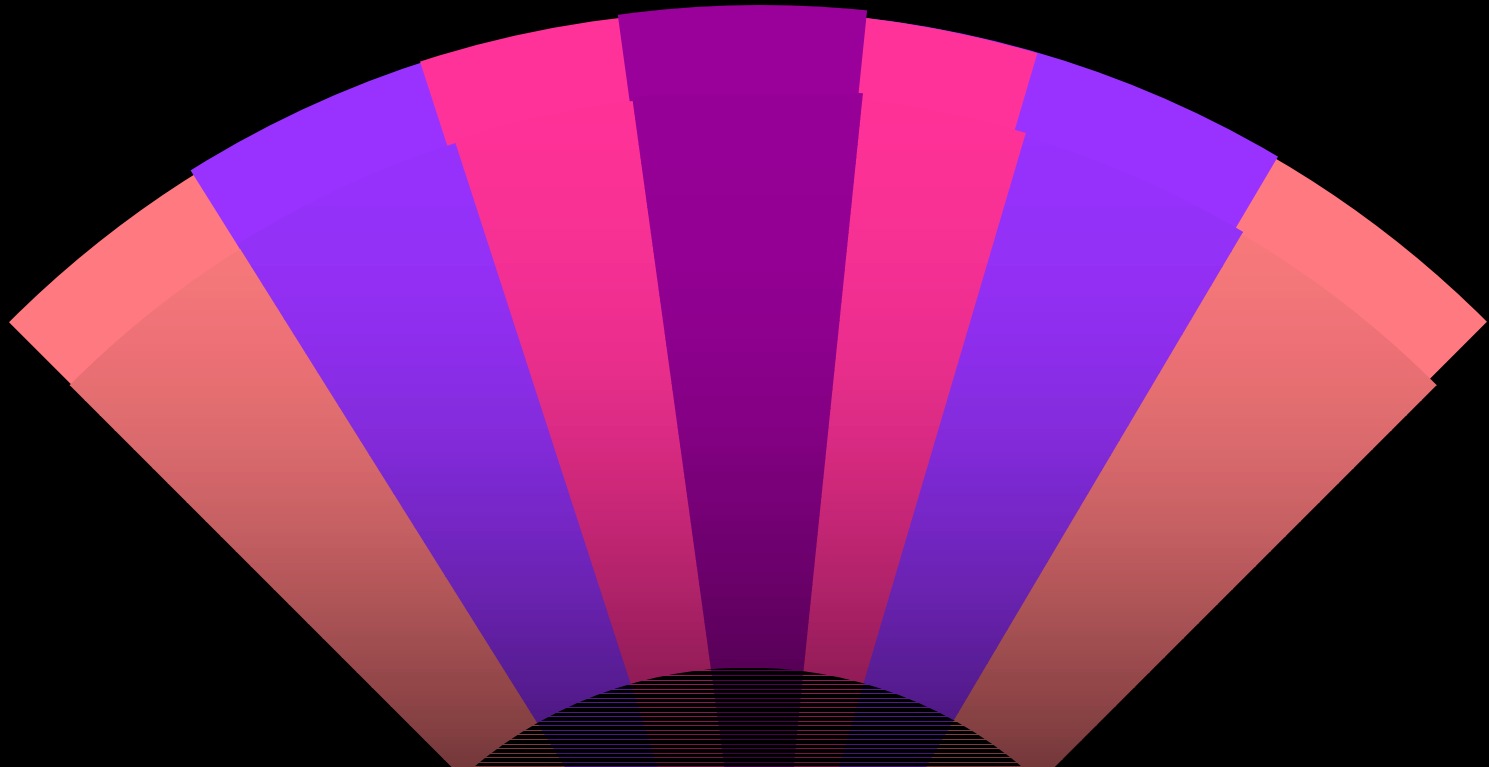
Security Concepts (Cont.)

- Reference monitor
 - Abstract machine which must mediate all access of subjects to objects
 - Must mediate all access, be protected from modification, be verifiable as correct, and is always invoked.
- Security kernel
 - The hardware, firmware, and software elements of a trusted computing base that implement the reference monitor concept.



Issues

- Hidden code
 - Undocumented program code
- Interrupts
 - Penetrator causes program/process interrupt to take advantage of privileged mode during interrupt processing
- Remote maintenance
- Logic bomb
 - Code covertly inserted to execute when logical event occurs
- Trap door
 - Code allowing access without authentication



Security Models



Models

- Bell-LaPadula
- Biba
- Clark & Wilson
- Non-interference
- State machine
- Access matrix
- Information flow



Classes of Trust

- Trusted Computer System Evaluation Criteria (TCSEC)
 - implementation of the Bell & LaPadula secrecy model
- Trusted systems - TCSEC classes
 - Div. D: minimal protection
 - Div. C: discretionary protection
 - Class (C1): discretionary security protection
 - Class (C2): controlled access protection
 - Div. B: mandatory protection
 - Class (B1): labeled security protection
 - Class (B2): structured protection
 - Class (B3): security domains
 - Div. A: verified protection
 - Class (A1): verified design



European Criteria

- Information Technology Security Evaluation Criteria (ITSEC)
 - Target of Evaluation (TOE): product or system
 - TCB = security enforcing + security relevant
 - Functionality classes, assurance classes, profiles
 - Security target
 - System security policy
 - Required security enforcing functions
 - Required security mechanisms (optional)
 - Claimed rating of minimum strength
 - Target evaluation level (F-xx,Ex)



Example ITSEC Functionality Classes

- F-IN (high integrity “TOE shall restrict access by users to explicitly designated objects”)
- F-AV (high availability “TOE shall recover from component failure such that the remaining functions continue to be available”)
- F-DI (high data integrity “TOE shall provide peer entity authentication, non-repudiation, error detection & correction during exchange”)
- F-DC (high data confidentiality “TOE shall have a facility to encrypt/decrypt”)
- F-DX (networks with high demands for confidentiality & integrity during exchange)



Common Criteria - Protection Profiles

- Specification of security product requirements
- Protection functions & assurances
- Design, implementation, & use



Client-Host Security Problems

- Access control (host)
 - Downloading
 - File protection
 - Uploading
 - Database corruption
 - Accidental/intentional
 - Dial-up
 - Unsupervised access
 - Hacker exposure
- Access control (PC)
 - Unsecured location
 - Limited access control software
 - Unprotected floppy disks (damage/theft)
 - Easy to move

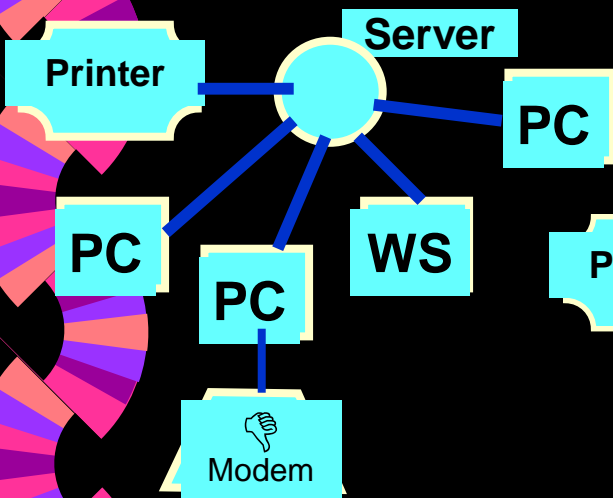


PC Security Issues

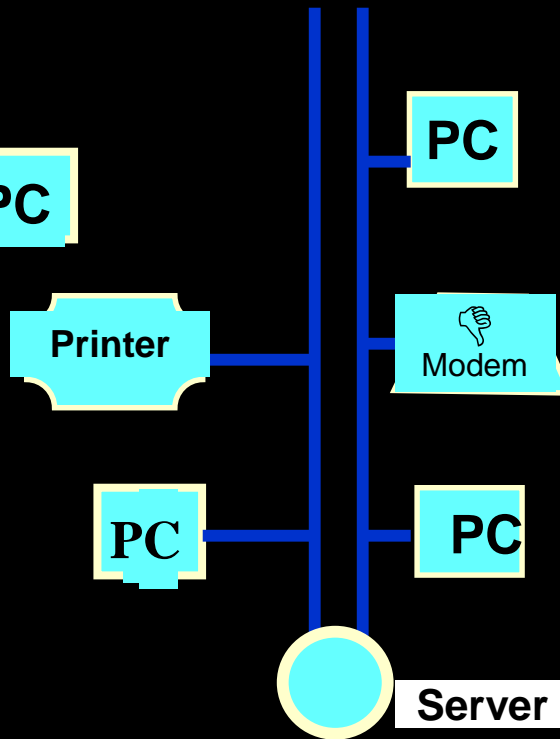
- Dialup entry control
- User training
- Internal control deficiencies
 - Separation of responsibilities
 - Audit trails
 - Automatic suspension of ID
 - Password criteria
- Need to limit access
 - Physical
 - Technical
- Remote access

LAN Topologies

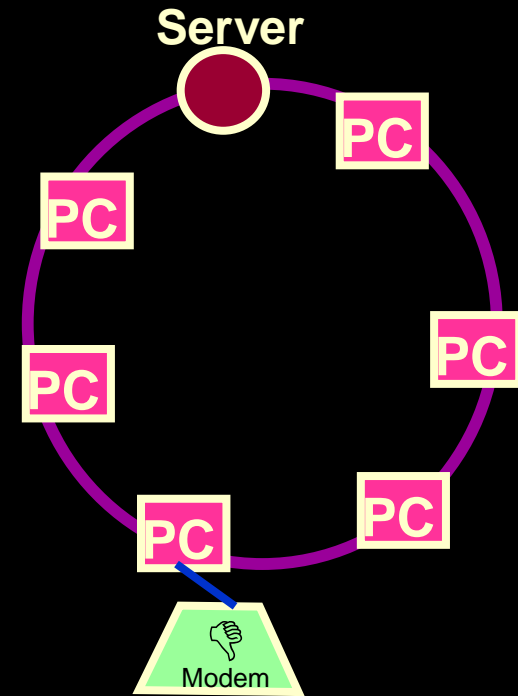
Star



Bus



Ring





Switches

- Network devices that select a path/circuit for sending data to its next destination, e.g., LAN switches & WAN/backbone switches (Note: May include router function)
- Switch is a simpler & faster mechanism than a router
- Located at:
 - Backbone & gateway levels of a network where one network connects to another
 - Subnetwork level where data is forwarded close to its destination/origin
- Switch not always required; LANs may be organized as rings or buses in which destinations inspect each message & read only those intended for that destination



Switches (Cont.)

- Circuit-Switching
 - Switch network path for exclusive use by 2 or more parties for certain duration then switch for use by another set of parties
 - Dedicated & continuously connected path for duration
 - Example: a phone connection generally uses circuit-switching



Switches (Cont.)

- Packet-Switching
 - Most data sent today uses digital signals over networks employing packet-switching
 - Users share same paths & data can be rerouted as conditions change
 - Message divided into packets, i.e., units of a certain number of bytes
 - Source & destination addresses added to the packet
 - Each network node or point examines each packet for routing



Switches (Cont.)

- Packet-Switching continued
 - Message packets may travel different paths & not arrive in same order as sent
 - At the destination, packets are collected & reassembled into the original message



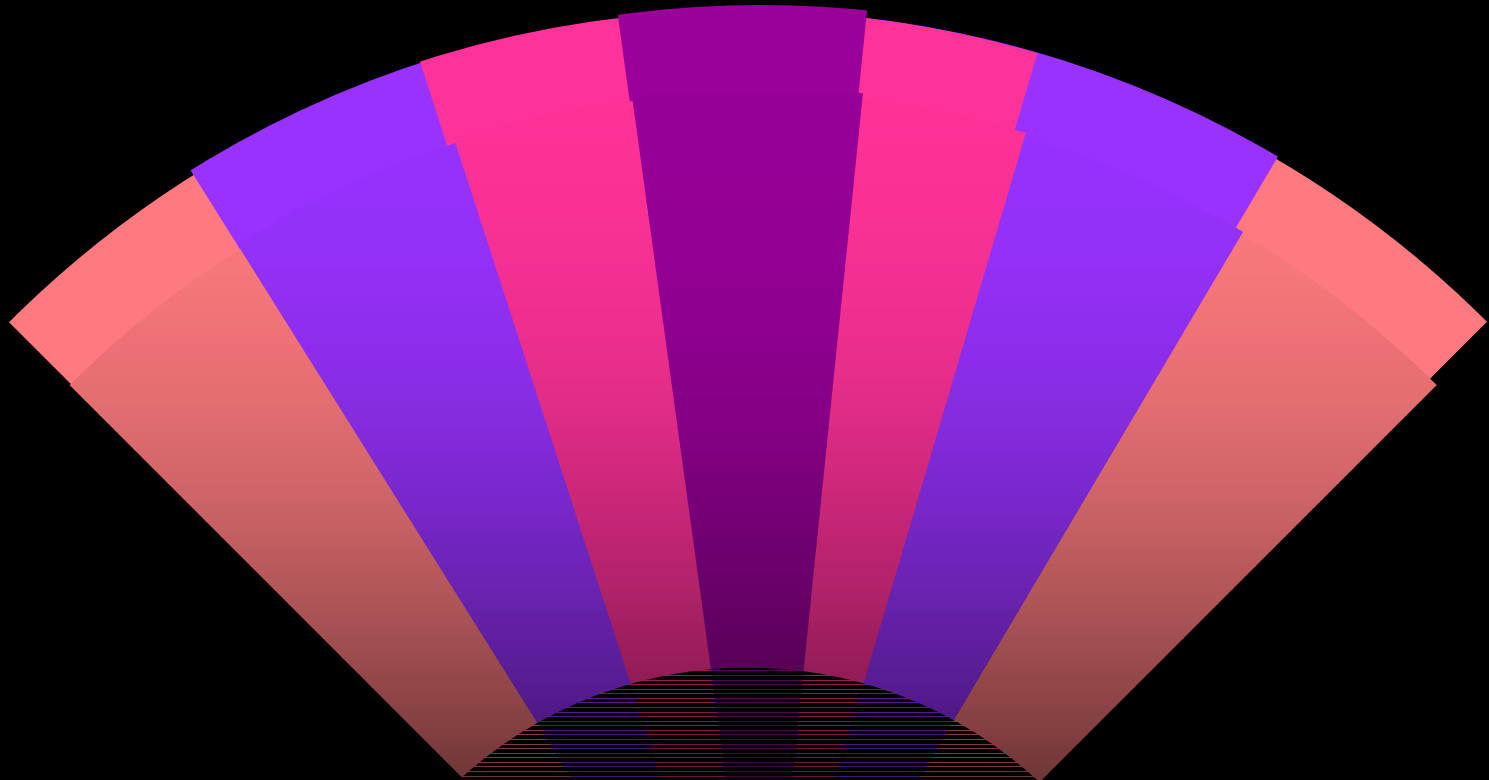
IETF IP Security Architecture (IPSec)

- Internet engineering task force request for comment
 - RFC 1825, (1995); updated, RFC 2401 (1998)
- Not an overall Internet security architecture
- Addresses security at the Internet Protocol (IP) layer
 - Host-host, gateway-gateway, host-gateway
 - Gateway = firewall or router implementing IPSec
- Critically dependent on environment
 - OS security
 - System management practices
 - Random number sources
 - System time variations



IETFIP Security Architecture (IPSec)(Cont.)

- IETF's IP security (IPSec) is designed to provide interoperable, high-quality, crypto-graphically-based security for IPv4 & IPv6
- The set of security services offered includes
 - access control
 - connectionless integrity
 - data origin authentication
 - protection against replays (a form of partial sequence integrity)
 - confidentiality (encryption)
 - limited traffic flow confidentiality
- Services are provided at the IP layer, offering protection for IP and/or upper layer protocols (TCP, UDP, ICMP, etc.)



SAMPLE QUESTIONS



Sample Question

- ▶ 1. A mechanism that enforces the authorized access relationships between subjects and objects is known as
 - a. the reference monitor.
 - b. discretionary access control.
 - c. trusted kernel.
 - d. mandatory access control.



Sample Question

- ▶ 2. What is the name of the first mathematical model of a multi-level security policy used to define the concept of a secure state, the modes of access, and rules for granting access?
 - a. Clark and Wilson Model
 - b. Harrison-Ruzzo-Ullman Model
 - c. Rivest and Shamir Model
 - d. Bell-LaPadula Model



Sample Question

- ▶ 3. Which of the following models does NOT include data integrity?
 - a. Biba
 - b. Clark-Wilson
 - c. Bell-LaPadula
 - d. Brewer-Nash



Sample Question

- ▶ 4. Which of the following describes a logical form of separation used by secure computing systems?
 - a. Processes use different levels of security for input and output devices.
 - b. Processes are constrained so that each cannot access objects outside its permitted domain.
 - c. Processes conceal data and computations to inhibit access by outside processes.
 - d. Processes are granted access based on granularity of controlled objects.



Sample Question

5. What security problem is most likely to exist if an operating system permits objects to be used sequentially by multiple users without forcing a refresh of the objects?
- a. Disclosure of residual data.
 - b. Unauthorized obtaining of a privileged execution state.
 - c. Denial of service through a deadly embrace.
 - d. Data leakage through covert channels.



*Access Control Systems &
Methodology*



Access Control

- Process of limiting access to system resources
 - Allowing only authorized users, programs, processes or other systems
- Controls
 - Policies (administrative)
 - Statements of intent regarding control over access to & dissemination of info
 - Software & hardware (logical)
 - Physical



Types of Controls

- Preventive
 - Avoid occurrence
- Detective
 - Identify occurrence
- Corrective
 - Remedy circumstances
 - Restore controls
- Deterrent
 - Discourage violations
- Recovery
 - Restore resources, capabilities, or losses
- Compensating
 - Alternative control (e.g., supervision)



Object Reuse (Residue) Issues

- Definition
 - Reassignment to a subject of a medium that contained one or more objects.
 - Page frame, disk sector, magnetic tape
- Secure reassignment
 - Media must contain no residual data
 - Format disks before copying
 - Write over or degauss tapes



Electronic Radiation (Emanations Security)

- Radiation threat
 - All electronic equipment
 - Listening devices
 - Detect emissions
 - Reproduce data streams/video screen images
 - Inexpensive Components
 - Wim van Eck experiments
 - Intercept & decipher signals from terminals in buildings



User Identification

- Asserts user identity
- Accountability
 - Enables activities to be traced to individuals
 - Individuals held responsible for actions
 - Log-on ID/userID/account/PIN
- Log-on ID characteristics
 - Unique
 - Nondescriptive of job function



User Authentication

- Verifying claimed identity
- Authentication factors
 - What a person knows
 - What a person has
 - What a person is



Onetime Passwords

- Changed after every use
 - Handheld password generators (tokens)
 - Synchronous/PIN-synchronous
 - Time synchronous
 - Event synchronous
 - Asynchronous/PIN-asynchronous
 - Integrated circuit chips, LCD display, keypad (if needed)



Smart Cards

- Smart cards
 - Processing capability
 - Reverse-engineer/tamper resistant
- Each user's card contains unique info
 - Identity, PIN, privileges, etc.
 - Card's micro performs secret, 1-way transformation of user's PIN
 - Stores unreadable PIN secretly in memory
 - User inserts card & enters PIN in reader



Biometric Authentication Devices

- Something a person is
 - Compares physiological/behavioral traits with that stored
 - Finger/hand print, retinal, voice, keystrokes
 - 2-factor authentication when used with PIN/password



Single Sign-On (SSO)

- Method for user to be identified & present credentials only once to a system
 - Information needed for future system to grant access to resources is forwarded by initial system
 - Grants access to workstation(s), server(s) and applications



Kerberos

- Trusted 3rd-party authentication service
 - MIT Project Athena
 - Kerberos is 3-headed dog that guards the entrance to the Underworld in Greek mythology
 - Assumptions - hosts, workstations, servers & network messages are vulnerable
 - A trusted Key Distribution Center (KDC) maintains secret keys of all principles
 - Kerberos database of clients & private keys
 - Network services requiring authentication
 - Clients desiring services



Remote Access Control Systems Standards

- Radius
 - Remote Authentication Dial-In User Service
 - Authentication server & dynamic passwords
 - Commercially available
 - Provides for password management
- TACACS
 - Terminal Access Controller Access Control System
 - Enables a network device to prompt for user name & static password
- TACACS +
 - TACACS with extended (2-factor) user authentication
 - Utilizes dynamic passwords through security tokens



System Protection

- Security domain
 - Domain of trust that shares a single security policy & single management
 - Access control parameters in which a program is operating
 - Set of objects a subject can access
 - Principle of separation protects resources
 - Resources encapsulated in distinct address spaces



System Protection (Cont.)

- Relational database controls
 - Basic entity is a relation
 - Relationships represent data
 - Data in 2-dimensional tables
 - Columns contain attributes
 - Rows contain records
 - Relation scheme = names of attributes & their permissible values
 - Relational instance: tuples of a relation at a given instance
 - Set of permissible values = attribute's domain
 - Values can be character strings or integers
 - Tables related by common column
- Table must include primary key (attribute) for every row



Access Control Technologies

- Discretionary access control
 - Owner determines who has access & what privileges they have
- Mandatory access control
 - Owner & system determine who has access
 - System decision based on privilege (clearance) of subject (user) & sensitivity (classification) of object (file)
 - Requires labeling
 - Based on the organization's security policy
 - Puts limitations on authorizers



Rule-Based Access Control

- Rules created or authorized by system owners specify the privileges granted to users
 - Read, write, execute, allocate
- Mediation
 - Part of access control mechanism
 - Decides if access is allowed or denied



Role-Based Access Control

- Groups of users need similar or identical privileges
 - Generally associated with discretionary access control
 - Privileges appropriate to functional roles are assigned
 - Individual users are enrolled in appropriate roles
 - Privileges are inherited



Access Control Lists

- Lists of subjects authorized access to some object
 - Users/groups with specific permissions
 - Flexible discretionary access control
- Preferred for need to know access control



Constrained User Interfaces

- Restrict users' access to specific functions by not allowing them to request it
 - Three major types
 - Menus
 - Database views
 - Physically constrained user interfaces - Limited number of buttons to select options



Capability Tables

- Tables of protected identifiers
 - Identifies the object
 - Specifies access rights allowed a subject possessing the capability
- Capability-based system
 - Access to protected objects granted if accessor possesses a capability (ticket) for the object



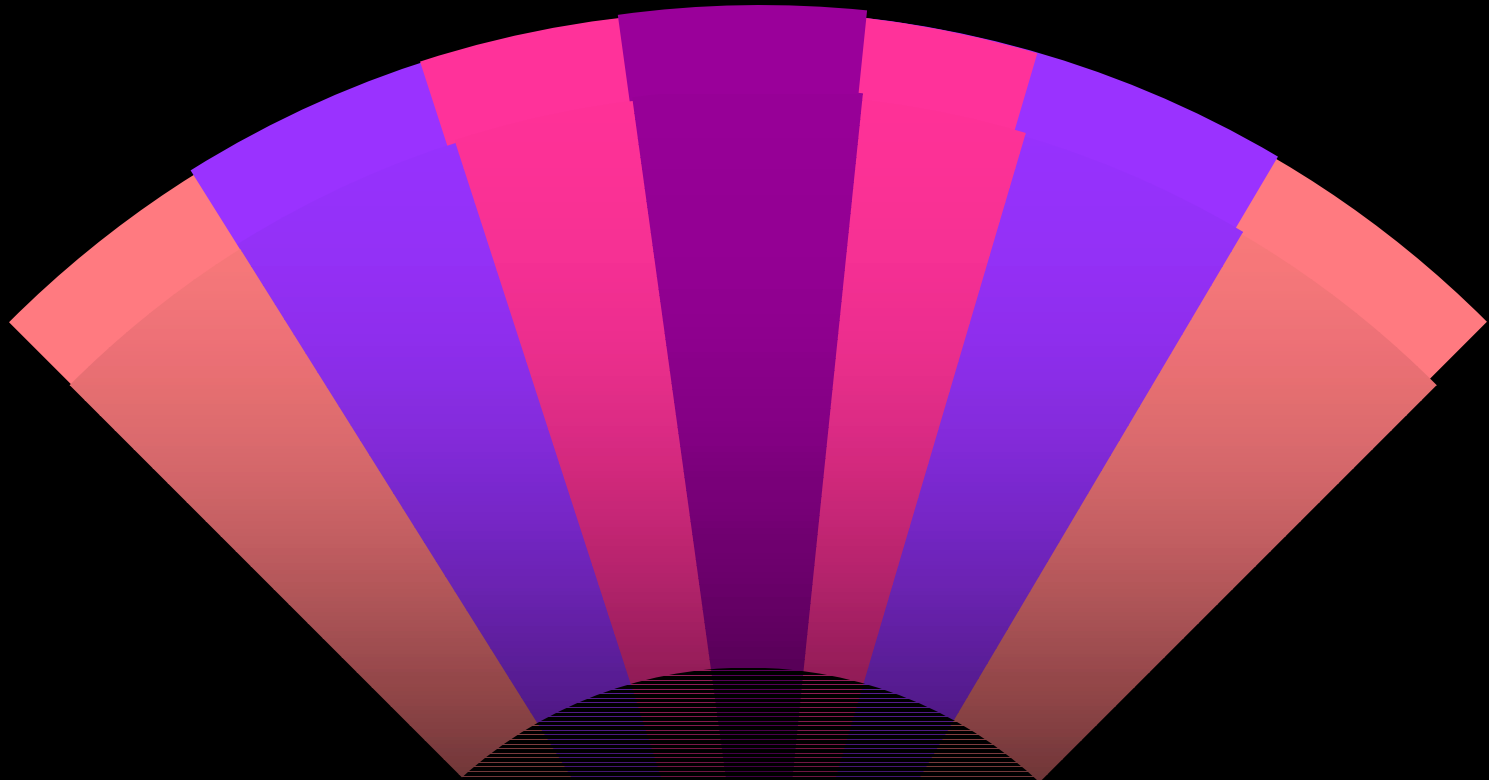
Content-Dependent Access Control

- Utilizes information in object being accessed
- Especially applicable to data base systems since data are structured
- Provides more access control granularity
- Content of record
- Form of question
- Arbiter program controls access



Intrusion Detection

- Techniques which attempt to detect computer/network attacks by observing traffic logs or other audit data
- Automated intrusion detection examines current audit records & compares user activity with profiles of expected activity to infer in real-time if an intrusion is occurring
- Previously, automated intrusion detection systems were R&D products but currently, commercial systems are available
 - Usually based on “expert system” technology



SAMPLE QUESTIONS



Sample Question

- 1. What is the PRIMARY use of a password?
 - a. Allow access to files.
 - b. Identify the user.
 - c. Authenticate the user.
 - d. Segregate various user's accesses.



Sample Question

- ▶ 2. The three classic ways of authenticating yourself to the computer security software are: something you know, something you have, and something
 - a. you need.
 - b. you read.
 - c. you are.
 - d. you do.



Sample Question

- ▶ 3. A timely review of system access audit records would be an example of which basic security function?
 - a. Avoidance
 - b. Deterrence
 - c. Prevention
 - d. Detection



Sample Question

- 4. An access system that grants users only those rights necessary for them to perform their work is operating on which security principle?
 - a. Discretionary Access
 - b. Least Privilege
 - c. Mandatory Access
 - d. Separation of Duties



Sample Question

- ▶ 5. Tokens, smart cards, and biometric devices used for identification and authentication provide robust authentication of the individual by practicing which of the following principles?
 - a. Multi-party authentication
 - b. Two-factor authentication
 - c. Mandatory authentication
 - d. Discretionary authentication



CRYPTOGRAPHY



Encryption Definitions

- Plaintext
 - Data in unscrambled form
- Ciphertext
 - Scrambled data
- Encipher
 - Act of scrambling
- Decipher
 - Descrambling with secret key
- Cryptanalysis
 - Descrambling without secret key
 - **Art of breaking ciphers**



Definitions (Cont.)

- **Key**
 - Secret sequence governing en/deciphering
- **Key clustering**
 - Two different keys generate same cipher text from same plain text
- **Work factor**
 - An estimate of the effort/time needed to overcome a protective measure by a penetrator with specified expertise & resources
- **Algorithm**
 - Set of rules by which enciphering & deciphering is done



Methods of Encryption

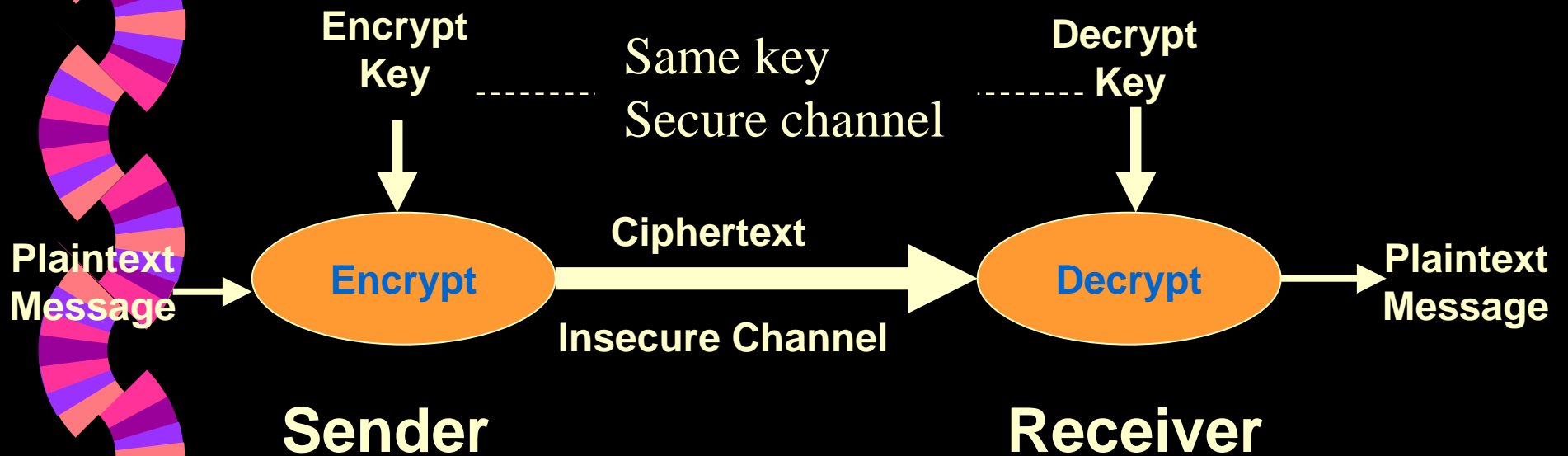
- Stream ciphers
 - Operate on continuous streams of plain text (as 1's & 0's)
 - Usually implemented in hardware
- Block ciphers
 - Operate on fixed size blocks of plain text
 - More suitably implemented in software to execute on general-purpose computer
- Overlap when block operated as stream



Basic Technologies

- Symmetric key cryptography
 - AKA: private key/single key/secret key
 - Key shared by originator & receiver
 - Computational efficiency advantage
 - 10-100 million bits/sec.
 - Algorithms:
 - Data Encryption Standard (DES)
 - Triple DES (3DES)
 - Blowfish
 - IDEA
 - RC4
 - SAFER

Symmetric Key Cryptography

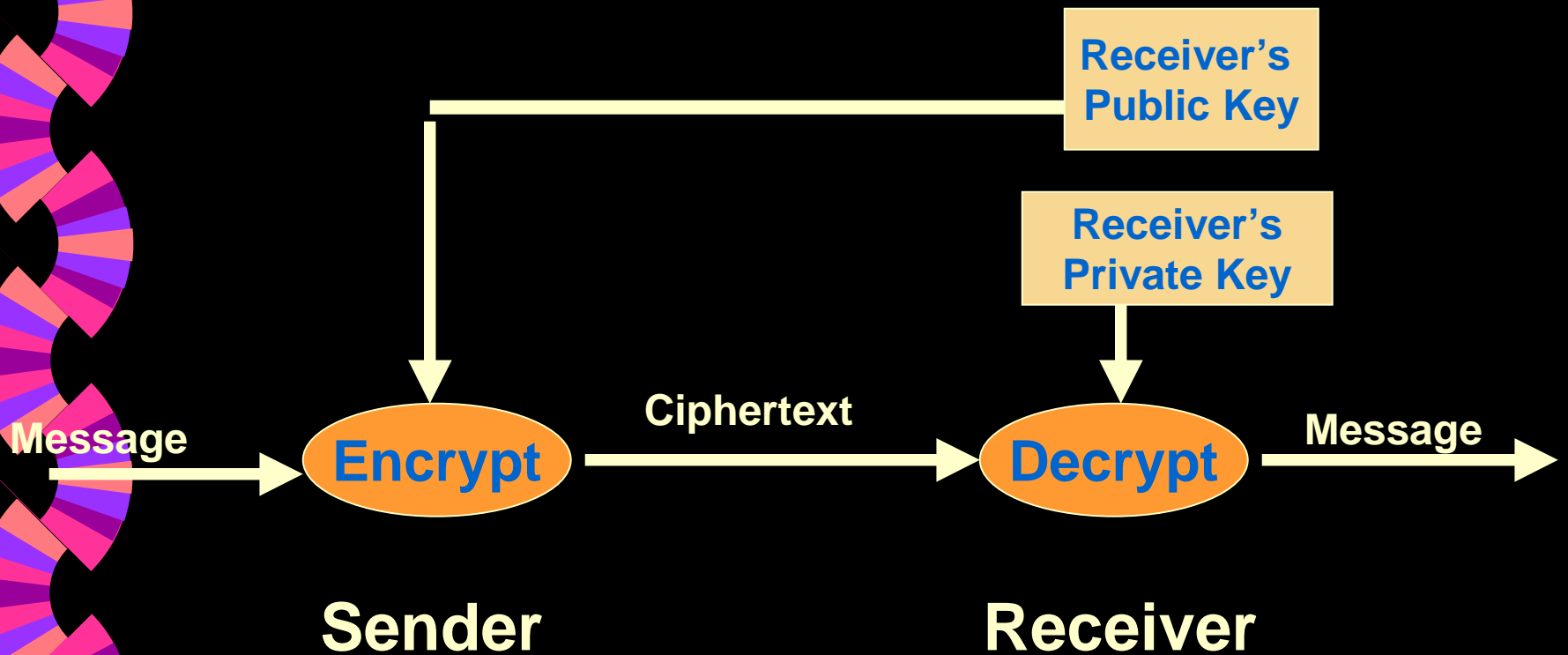




Basic Technology (Cont.)

- Asymmetric key cryptography
 - AKA: public key
 - Uses 2 asymmetric keys
 - One to encrypt, the other to decrypt
 - Computationally slow
 - Few thousand bits/sec. (early versions)
 - Related to known mathematical problem
 - Difficulty factoring product of 2 large prime numbers
 - Rivest-Shamir-Adleman (RSA) algorithm
 - Discrete logarithms in a finite field
 - Diffie-Hellman
 - ECC (Elliptic Curve)
 - DSS (Digital Signature Standard)
 - El Gamal
 - LUC

Public-Key Cryptosystem





Steganography

- Art of hiding communications
 - Deny message exists
 - Data hidden in picture files, sound files, slack space on floppies
 - i.e., least significant bits of bitmap image can be used to hide messages, usually without material change to original file



One-Time Pad

- Unbreakable by exhaustive search (brute force)
- Random key same length as message
 - Only used once
- Digital system key & message both bit streams
 - 8 bits per character
 - Each key bit XORed with corresponding message bit
 - Produces ciphertext bit
 - Key bits XORed with ciphertext to decrypt



DES Algorithm

- Description
 - 64-bit plain & cipher text block size
 - 56-bit true key plus 8 parity bits
 - Seventy quadrillion possible keys
 - 16 rounds of simple operations to encrypt
 - Transposition & substitution
 - Reverse to decrypt



Double/Triple DES

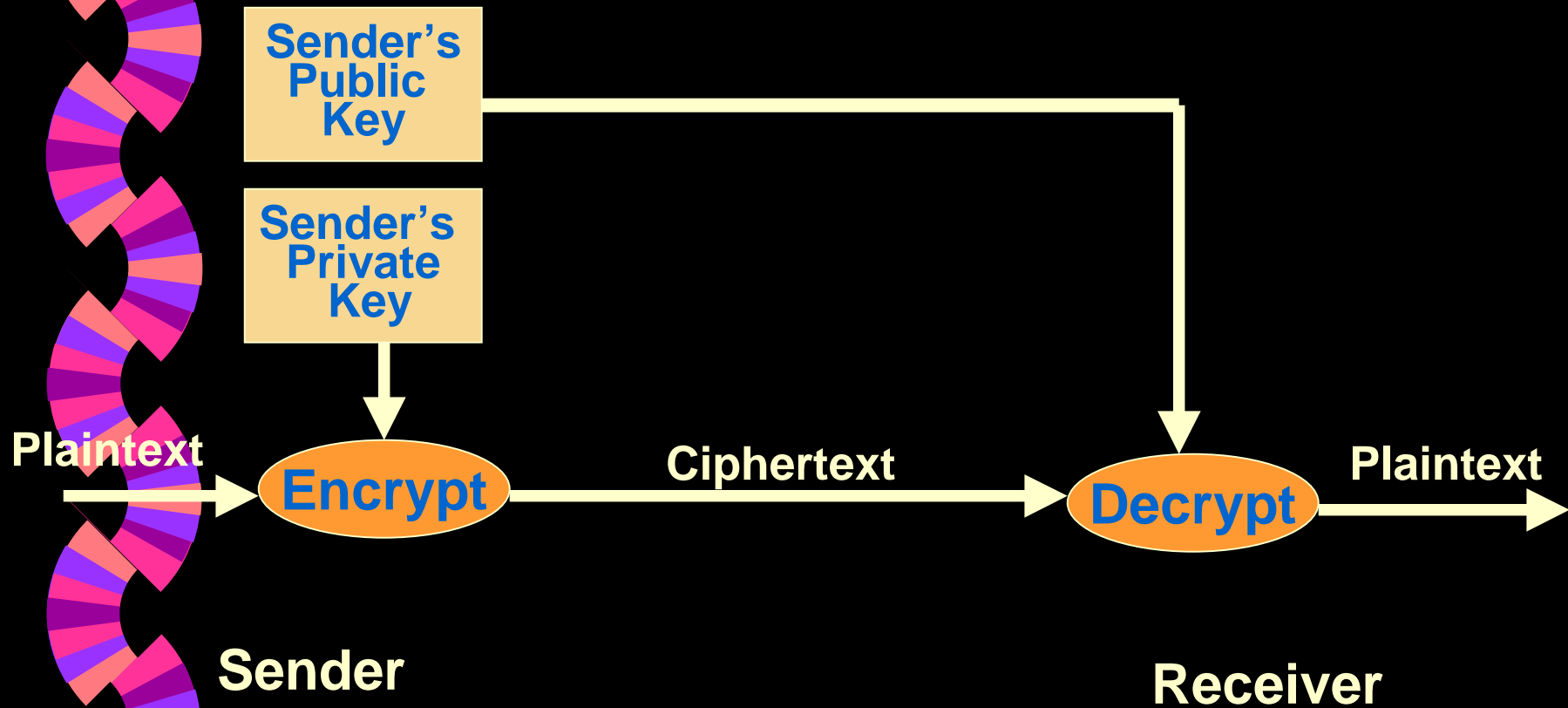
- Double DES
 - Effective key length 112 bits
 - Work factor about same as single DES
 - No more secure
- Triple DES
 - Different modes
 - DES-EEE3: 3 DES encryptions with 3 different keys
 - DES-EDE3: 3DES operations (encrypt-decrypt-encrypt) with 3 different keys
 - DES-EEE2, DES-EDE2: same as previous, except 1st & 3rd operations use same key
- No successful attacks reported



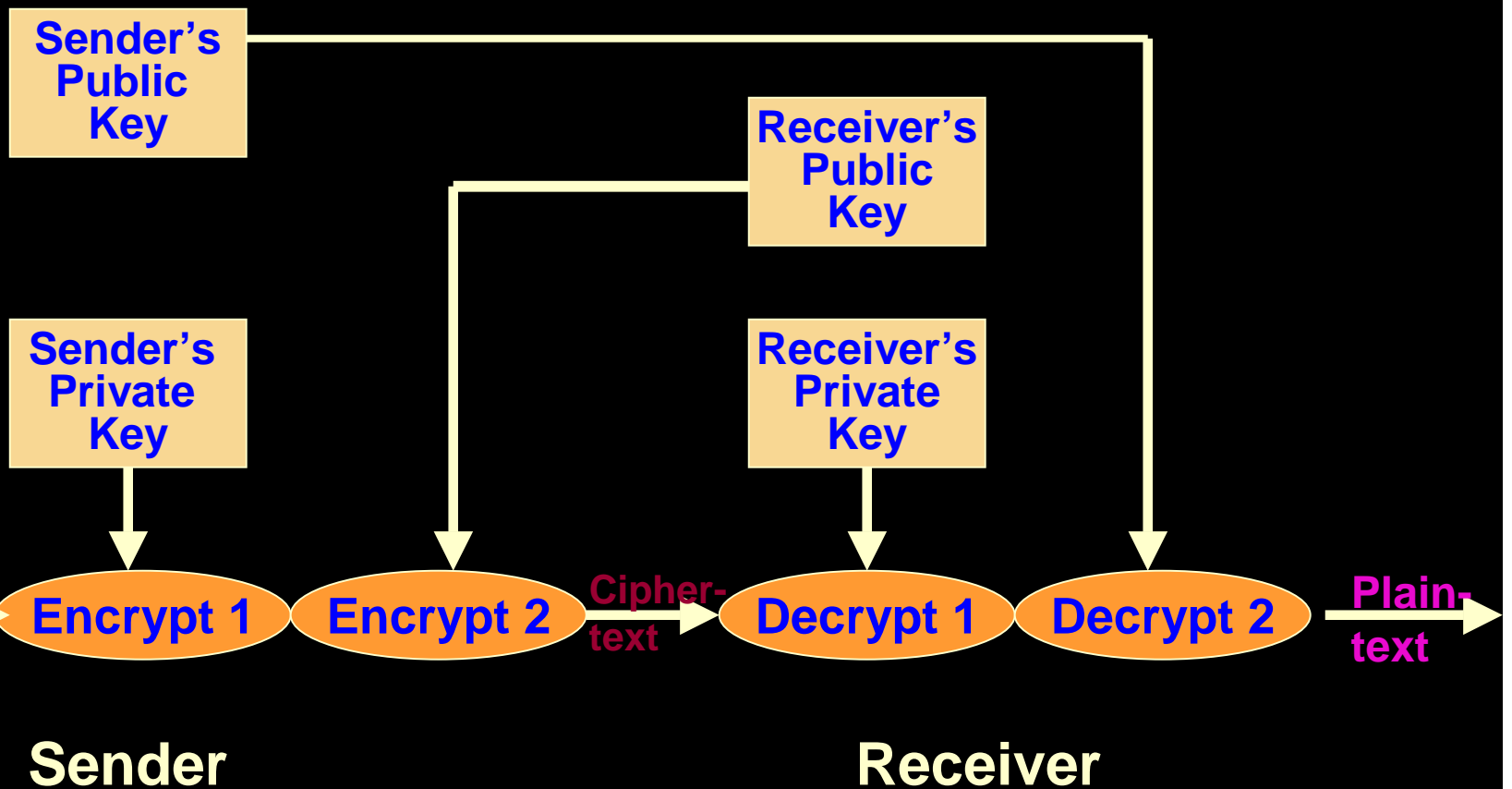
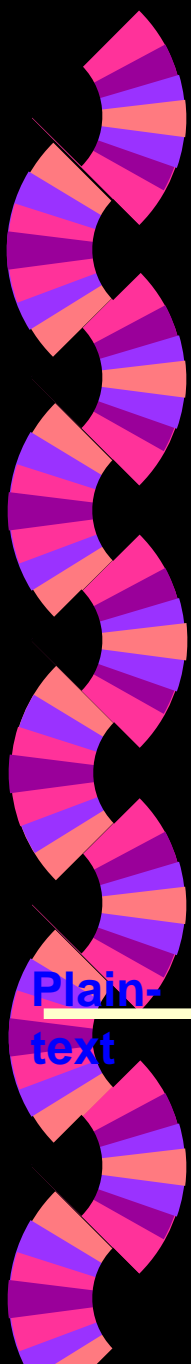
Public-Key Crypto

- Open message
 - Receiver decodes with sender's public key
 - Sender encodes message with own private key
- Secure & signed message
 - Sender encodes message with own private key
 - Sender re-encodes message with receiver's public key
 - Receiver decodes message with own private key
 - Receiver decodes message with sender's public key

Open Message



Secure & Signed Message



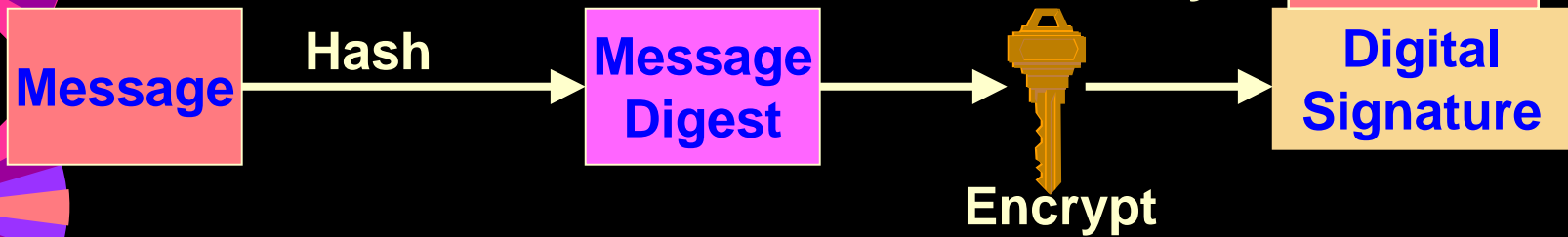


Digital Signatures

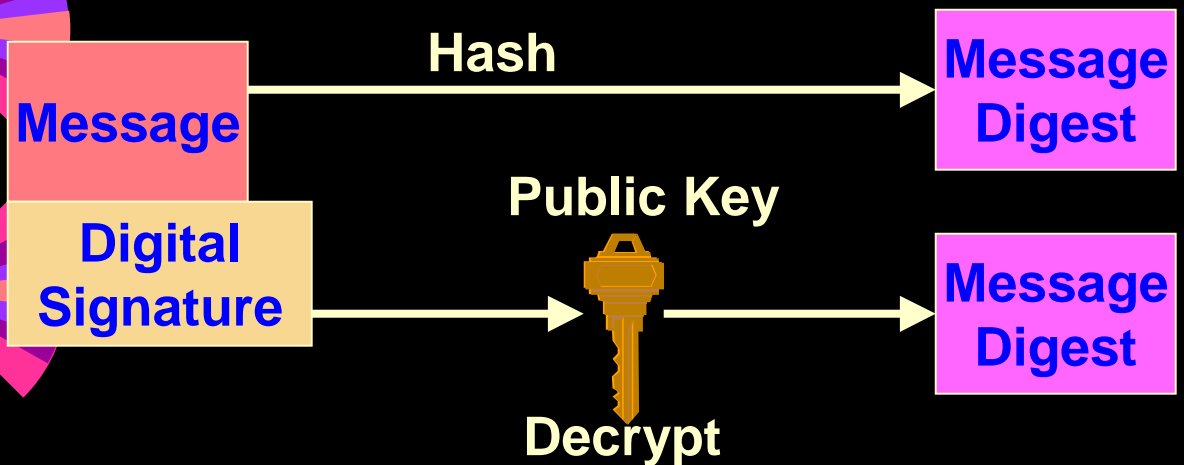
- Authentication tool to verify a message origin & sender identity
 - Resolve authentication issues
 - Block of data attached to message (document, file, record, etc.)
 - Binds message to individual whose signature can be verified
 - By receiver or third party
 - Can't be forged
 - Each user has public-private key pair
 - Private key signs (creates) signature, public key verifies it

Digital Signature Graphically

Sender



Receiver





MD5 Algorithm

- Rivest upgrade of MD4
 - 1-way hash function producing 128-bit hash (message digest) of input message
 - Message undergoes 4 rounds of transformation
 - Specified as an Internet standard (RFC1312)



Certification

- Binds individuals to their public keys
- Certification authority's digital signature
 - Attests binding
 - Certification authority certification
 - User identification, public key, date
 - X.509 certification standards
- NIST National Digital Signature Certification Authority study



Key Management Activities

- Key generation
- Key change
- Key disposition
- Key recovery
- Control of crypto keys



Symmetric Key Management Techniques

- Link encryption
- End-to-end encryption
 - Key Distribution Center (KDC)
 - User unique key distributed
 - Changed infrequently
 - A calls B
 - Calling protocol contacts KDC
 - KDC generates random session key (k)
 - KDC encrypts k using A's unique key & sends it to A
 - KDC encrypts k using B's unique key & sends it to B
 - A & B use k for session



PKI

- For electronic business transactions provides
 - Confidentiality
 - Data must be protected from unauthorized access when being stored and when being transmitted
 - Access Control
 - Data can only be accessed by the parties for whom it was intended
 - Integrity
 - Data being stored or transmitted is protected from unauthorized modification
 - Authentication
 - The identity of the originator can be validated
 - Non-repudiation services
 - The originator cannot deny participation in the transaction



PKI (Cont.)

- Manages generation and distribution of public/private key pairs
- Publishes public keys as ‘certificates’
- Provides high degree of confidence that
 - Private keys can be kept secure
 - Specific public keys are truly linked to specific private keys
 - Parties holding private/public key pairs are who they say they are



PKI (Cont.)

- A PKI is defined as
 - Certification Authority (CA)
 - Certificate Repository
 - Certificate Revocation System
 - Key Backup and Recovery System
 - Support for Non-repudiation
 - Automatic Key Update
 - Management of Key Histories
 - Cross-certification
 - Timestamping
 - Client side software interacting with all of the above in a consistent, trustworthy manner



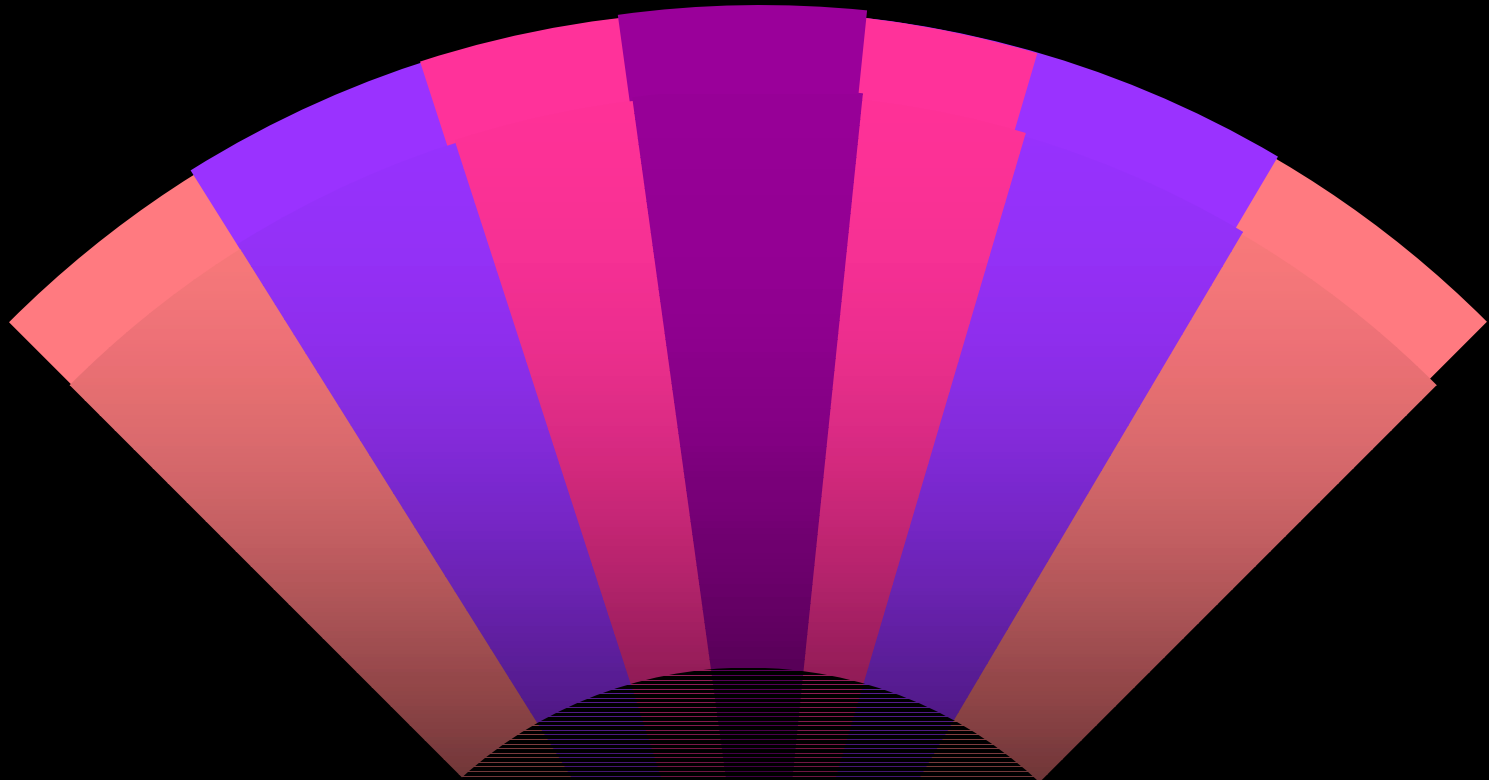
Brute Force Attack

- Trying all keys
 - Cost
 - Time
- Moore's Law (Gordon Moore, Intel founder)
 - Processing speed doubles every 18 months
- MIPS per Year (MY)
 - Number of instructions a million-instruction-per-second computer can execute in one year



Other Attacks

- Analytic
 - Using algorithm & algebraic manipulation weakness to reduce complexity
 - RSA factoring attack
 - Double DES attack
- Statistical
 - Using statistical weakness in design
 - More 1's than 0's in the keystream
- Implementation
 - Using the specific implementation of the encryption protocol
 - '95 attack of Netscape key
 - Deficient key randomization
 - String algorithm + 128-bit key



SAMPLE QUESTIONS



Sample Question

- ▶ 1. Which of the following statements is true about data encryption as a method of protecting data?
 - a. It verifies the accuracy of the data.
 - b. It is usually easily administered.
 - c. It requires careful key management.
 - d. It makes few demands on system resources.



Sample Question

- ▶ 2. In what way does the Rivest-Shamir-Adleman algorithm differ from the Data Encryption Standard?
 - a. It is based on a symmetric algorithm.
 - b. It uses a public key for encryption.
 - c. It eliminates the need for a key-distribution center.
 - d. It cannot produce a digital signature.



Sample Question

3. Which of the following is NOT a property of a one-way hash function?
- a. It converts a message of a fixed length into a message digest of arbitrary length.
 - b. It is computationally infeasible to construct two different messages with the same digest.
 - c. It converts a message of arbitrary length into a message digest of a fixed length.
 - d. Given a digest value, it is computationally infeasible to find the corresponding message.



Sample Question

- ▶ 4. The Data Encryption Algorithm performs how many rounds of substitution and permutation?
 - a. 4
 - b. 16
 - c. 54
 - d. 64



Sample Question

5. Which of the following statements is most accurate of digital signature?

- a. It is a method used to encrypt confidential data.
- b. It is the art of transferring handwritten signature to electronic media.
- c. It allows the recipient of data to prove the source and integrity of data.
- d. It can be used as a signature system and cryptosystem. a



***TELECOMMUNICATIONS AND
NETWORK SECURITY***



Telecommunications Security Definition

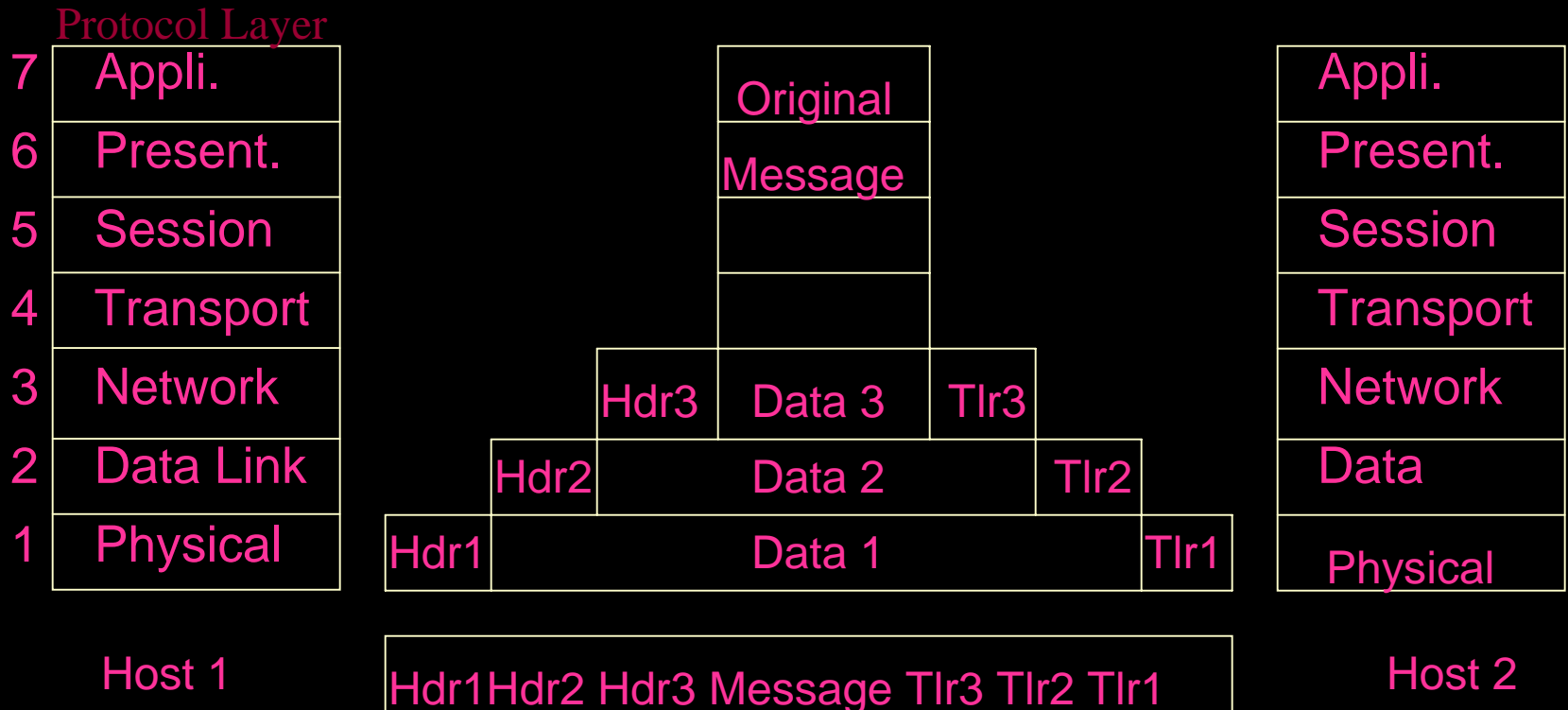
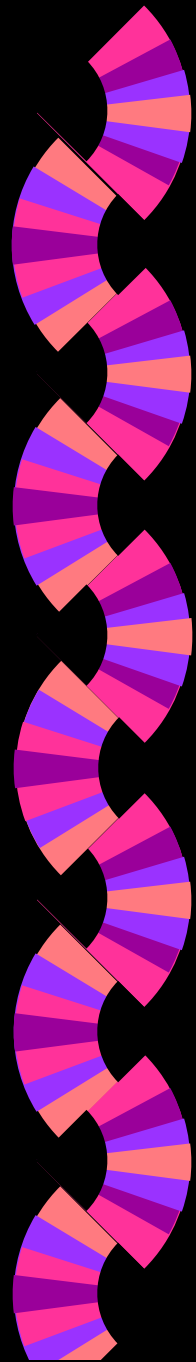
- Domain of information security concerned with protecting data, voice and video communications and ensuring:
 - Availability
 - Integrity
 - Confidentiality
 - Prevention/Detection of misuse/abuse
- Management and administrative functions
 - Information
 - E-mail
 - Network security management
 - Remote access
 - Voice/facsimile/video



Network Communications Protocols

- Open system interconnect (OSI) model
 - Network architecture
 - 7 layers in the communication process
 - ISO introduced (adopted 1984)
 - Communication & interoperability between systems
 - Regardless of hardware or networking characteristics
- TCP/IP
 - Transmission control protocol/internet protocol
 - Allows systems on different networks to communicate
 - Most popular
 - The Language of the Internet

Open System Interconnect (OSI)



Protocol Layer - Receive & transmit data from layer above

A Message passed across interface to lower layer with control info

A Header Info: Destination / source / security / label / etc.

A Trailer Info - checksum



Network Access Controls

- Virtual private networks (VPNs)
 - Concept of dynamically establishing a secure network link between two specific network nodes using a secret encapsulation method
 - Secret encapsulation (tunneling) enabled by:
 - VPN agent (hardware/software) at remote client and on server at network gateway or within the private network
 - User and/or node authentication
 - Secure session handshake and key exchange
 - Establishing a dynamic encrypted link or tunnel through an external or internal network
 - Popular VPN techniques include:
 - Point-to-Point Tunneling Protocol (PPTP)
 - Layer 2 Forwarding (L2F)
 - Layer 2 Tunneling Protocol (L2TP)



Data Network Structure

- Local area network (LAN)

- Data communications network that:
 - Lies within a limited spatial area
 - Has a specific user group and specific topology
 - Not a public switched network but may be connected to one
- Comprised of network components and media (cable) that provide network services such as file services, mail services, print services, terminal emulation and communications.
- Interconnection of LANs:
 - Campus area network - within a limited geographic area/complex
 - Metropolitan area network - over a city-wide area
 - Wide area network - over a large area such as nation-wide

Media Types

- Twisted Pair
 - Cheapest, limited in distance & bandwidth
 - Used within buildings or small areas
 - Easily tapped
- Coaxial cable
 - More expensive & resistant to electromagnetic interference
 - Greater bandwidth & distance
 - Baseband - single channel
 - Broadband - many channels (video, voice, data)



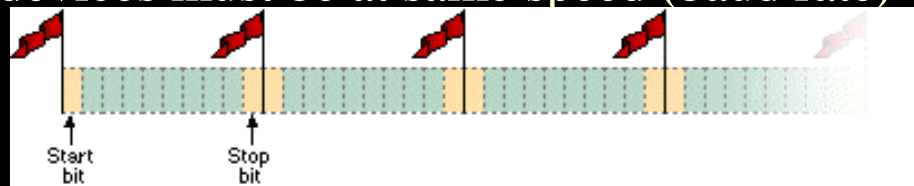
Media (Cont.)

- Fiber optics
 - Carries signals as light waves
 - Higher speed, longer distance, many channels
 - Difficult to tap, resistant to interference
 - Most expensive
- Leased line networks
 - Dedicated (private) analog facilities
 - Routing & transmission quality engineered
 - Conditioning yields lower error rate
- Dedicated line
 - Private or leased line

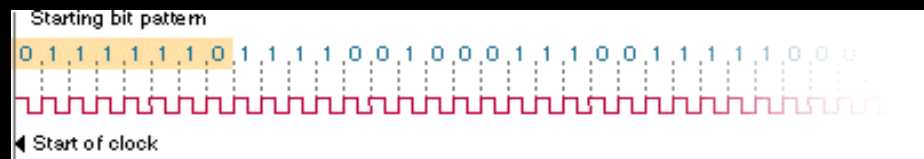


Network Technologies

- Asynchronous communications
 - Transfer of data by sending bits sequentially
 - Start bit & stop bit marks beginning & end
 - Communications devices must be at same speed (baud rate)



- Synchronous communications
 - Very high speed
 - Transfer of data synchronized by electronic clock signals



Network Technologies (Cont.)

- Analog / Digital technologies
 - Analog - continuous signal varied by amplification



- Digital - passes info encoded as discrete, on-off pulses





Remote Access Security Standards

- Password Authentication Protocol (PAP)
 - Provides automated identification and authentication of remote entity
 - Authentication accomplished with “static” replayable password
 - Supported by most network devices; e.g., routers, communication servers
 - Decreasing use due to weakness of authentication process
 - PAP database is encrypted, but PAP does not encrypt user id or password on the transmission line



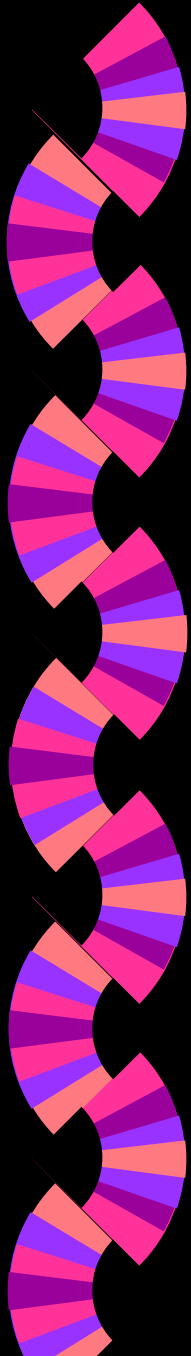
Remote Access Security Standards (Cont.)

- Challenge Handshake Authentication Protocol (CHAP)
 - Similar use and function as PAP but uses stronger authentication process
 - Authentication process uses non-replayable, challenge/response dialog to verify the identification of the remote entity
 - Commonly used by routers and communication servers to authenticate connecting entity before linking two or more networks together
 - Commonly used by remote access servers and remote ISDN/cable modems



Remote Access Security Administration Systems

- Terminal Access Controller Access Control System (TACACS)
 - TACACS enables a network device to prompt for username and static password; network device then queries a TACACS server to verify password
 - Extended TACACS mode (TACACS+) provides:
 - Enables use of two-factor (dynamic) passwords
 - Allows user to change static passwords/resynch security token
 - Enables communications between network device and TACACS+ server and update audit trail



Remote Access Security Administration Systems (Cont.)

- Remote Authentication Dial-in User Service (RADIUS)
 - RADIUS adopted as standard protocol by Internet Engineering Task Force
 - Provides similar user authentication (including use of dynamic password) and password management as TACACS+
 - Provides similar communications with network devices and audit trail
 - Provides CHAP authentication of remote node
 - Provides extended user profile (network access control list)
 - Bundled in network operating system of network devices
 - **Robust RADIUS Systems commercially available**



Definition

- Web Security refers to:
 - Hypertext Transfer Protocol (HTTP) including:
 - HTTP services transmitted on the Internet, extranet and intranet
 - Protecting private networks from inherent security risks associated with Web-based technology including:
 - Web-based mobile code; e.g., Java applets and scripts, ActiveX, Visual Basic scripts, HTTP Cookies and Plug-ins
 - Vulnerabilities in web server and browser client software
 - Some Web security mechanisms and standards
 - Web content inspection engines
 - Secure Socket Layer (SSL)
 - Secure Hypertext Transfer Protocol (S-HTTP)



Firewall Architectures

- Types of firewalls
 - Packet-filtering router
 - Most common firewall mechanism
 - Packet-filtering router between private network and the “untrusted” network or network segment; i.e., a boundary router
 - May be used to manage access to DMZ network (extranet)
 - Security policy enforced through Access Control Lists (ACLs) that permit or deny connections based on protocol, Svc/Apl and IP address



Firewall Architectures (Cont.)

- Screened host firewall system
 - Employs both packet-filtering router and a bastion host (application-level gateway protected against attacks)
 - Provides higher level of security because it provides both network-layer (packet-filtering) and application-layer (proxy services)
 - Requires an intruder to penetrate two separate systems before private network is compromised



Firewall Mechanisms

- Proxy servers
 - Acts as transparent intermediary between client and information servers that provide information requested by the client
 - When connecting through a proxy server, the TCP/IP connection is broken at the server and there is less potential for network intrusion
 - Proxy servers are application specific
 - Most bastion host firewall systems provide proxy servers for:
 - telnet
 - FTP
 - Web-based services (HTTP, gopher and FTP)
 - Reverse proxy server: server works in reverse and allows a server, such as a Web server, to reside safely inside the firewall while the reverse proxy server acts as a Web server outside the firewall



Secure Sockets Layer (SSL)

- Provides transport (socket) layer security
 - Socket layer security protocol for TCP-based applications
 - Enables client/server applications to communicate securely, minimizing the risk of eavesdropping, tampering or message forgery
 - Widely used for securing web-based applications
 - SSL is a two-layered protocol: SSL Record Protocol (used to encapsulate higher level protocols) and SSL Handshake Protocol



Simple Key Management for Internet Protocols (SKIP)

- Provides services similar to SSL except requires no prior communication
- Enables TCP/IP host to send encrypted IP packet to another host without requiring a prior message Well suited for Internet, since both are stateless protocols
- Requires no prior communication in order to establish or exchange keys on a session-by-session basis
- SKIP does not continually generate new key values as SSH does
- Uses Diffie-Hellman to generate a shared secret, which in turn provides IP packet-based encryption and authentication



Application Layer Security Protocols

- Security-enhanced Application Protocols
 - Remote Terminal Access (TELNET)
 - Secure RPC Authentication (SRA)
 - Secure Telnet
 - Electronic Mail (SMTP)
 - PEM, SMIME, MOSS, PGP, etc.
 - WWW Transactions (HTTP)
 - Secure HTTP (S-HTTP)
 - Others
 - SNMP (Simple Network Management Protocol)
 - Electronic Payment Schemes
 - Ecash, NetCash, Mondex, CyberCash, SEPP, STT, SET



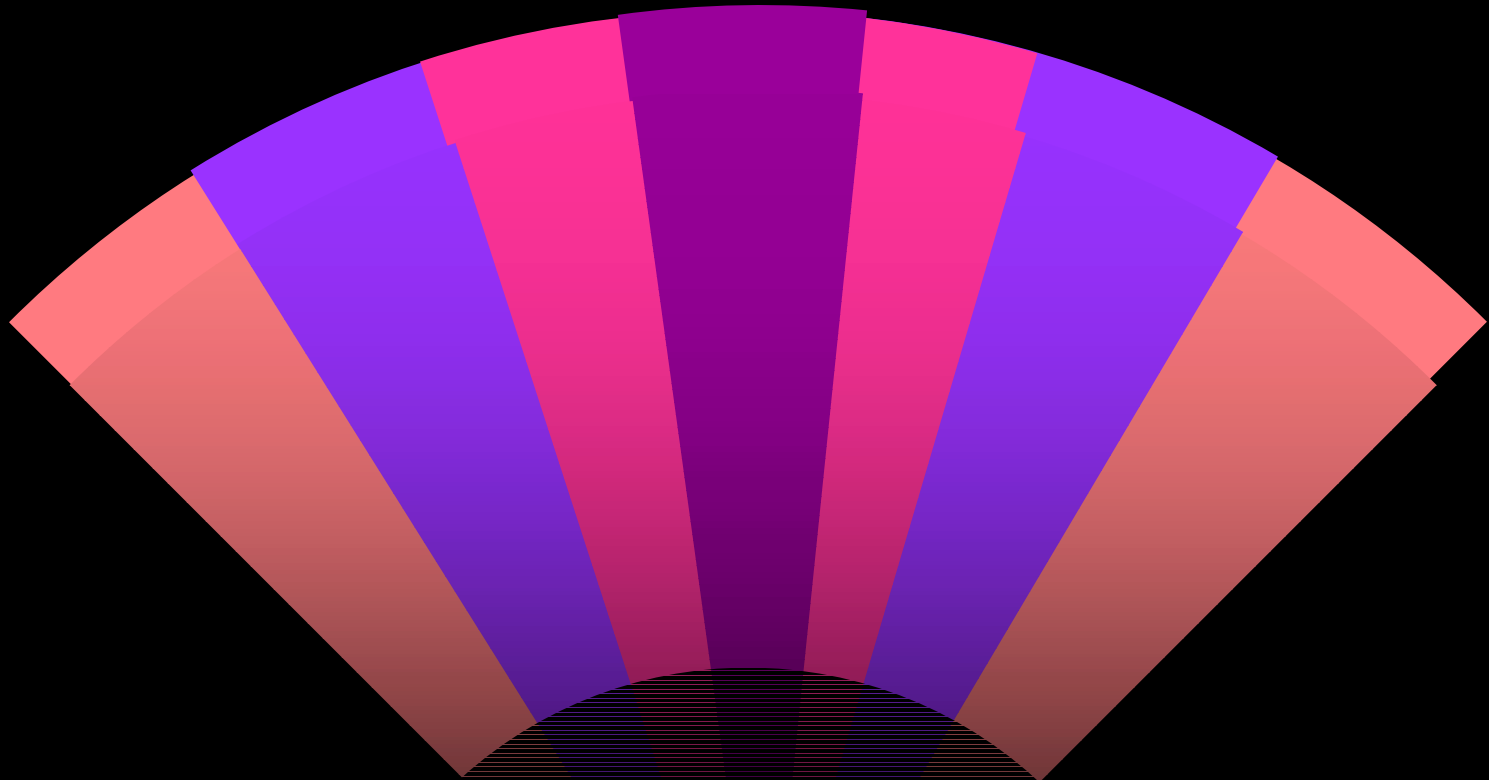
Application Layer Security Protocols

- Authentication and Key Distribution Systems
 - Kerberos
 - NetSP
 - SPX
 - TESS
 - SESAME
 - DCE



Well-Known Attack Methods

- Denial of Service Attack
 - Smurf
- Large Packet Ping Attack
- Buffer Overflow Attacks
- TCP SYN Flood Attacks
- IP Spoofing Attacks
- TCP Sequence Number Attacks
- IP Fragmentation Attacks
 - Tiny fragment attack
 - Overlapping fragment attack
 - Teardrop attack



SAMPLE QUESTIONS



Sample Question

- ▶ 1. Why does fiber optic communication technology have significant security advantage over other transmission technology?
 - a. Higher data rates can be transmitted.
 - b. Interception of data traffic is more difficult.
 - c. Traffic analysis is prevented by multiplexing.
 - d. Single and double-bit errors are correctable.



Sample Question

2. Layer 4 of the OSI stack is known as
- a. the data link layer
 - b. the transport layer
 - c. the network layer
 - d. the presentation layer



Sample Question

3. Another name for a VPN is a
- a. tunnel
 - b. one-time password
 - c. pipeline
 - d. bypass



Sample Question

- ▶ 4. Why is traffic across a packet switched network (e.g. frame relay, X.25) difficult to monitor?
 - a. Packets are link encrypted by the carrier
 - b. Government regulations forbid monitoring
 - c. Packets are transmitted on multiple paths
 - d. The network factor is too high



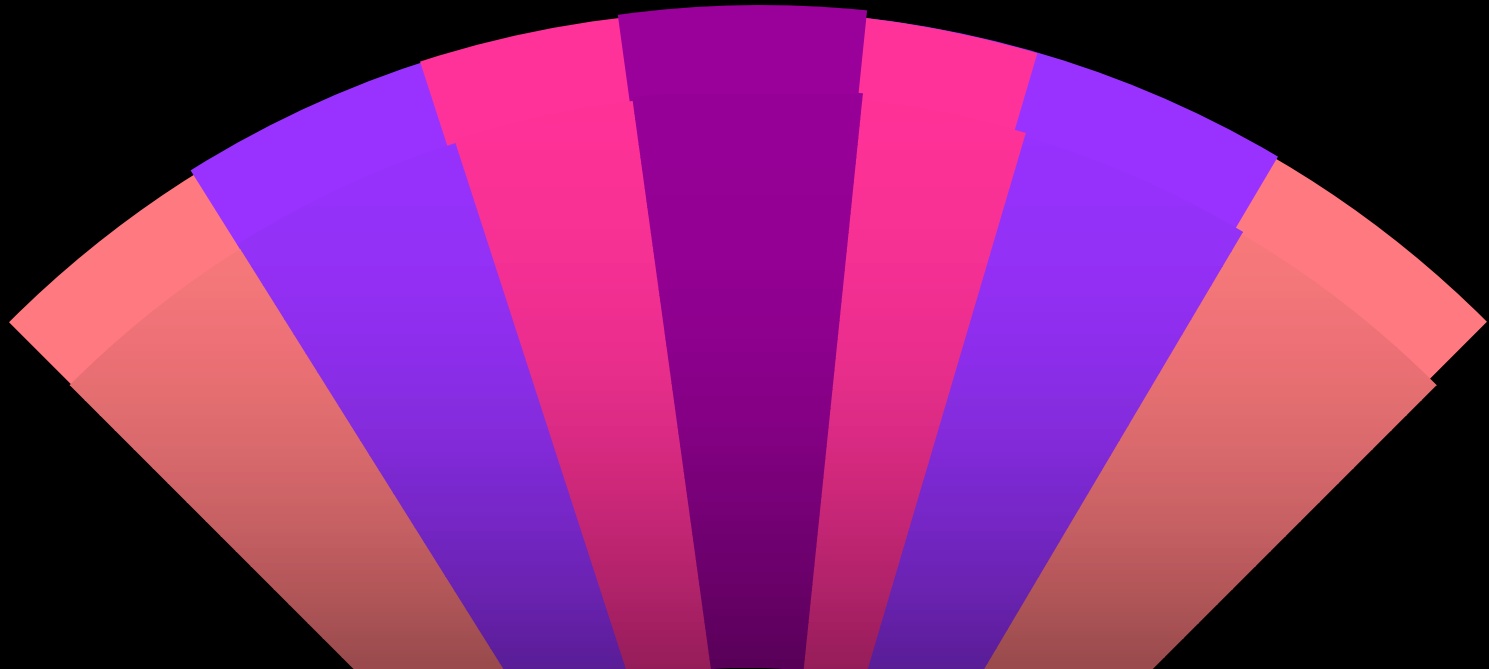
Sample Question

- ▶ 5. Which one of the following is used to provide authentication and confidentiality for e-mail messages?
 - a. Digital signature
 - b. PGP
 - c. IPSEC AH
 - d. MD4



Sample Question

6. What is a packet sniffer?
- a. It tracks network connections to off-site locations.
 - b. It monitors network traffic for illegal packets.
 - c. It scans network segments for cabling faults.
 - d. It captures network traffic for later analysis.



***APPLICATIONS & SYSTEMS
DEVELOPMENT SECURITY***



Definitions

- Acceptance
 - Technical performance/security requirements met
- ActiveX
 - Microsoft's answer to Java
 - Stripped down implementation of OLE
 - Designed to run over slow internet links
- Agent
 - In the client/server model
 - Performs information preparation & exchange for client or server



Definitions (Cont.)

- Aggregation (programming related)
 - Composition technique for building new object from 2 or more existing objects that support the new object's required interfaces
- Aggregation (security related)
 - Combining info from separate sources on same object
 - Combination sensitivity greater than individual parts
 - Higher classification/protection



Definitions (Cont.)

- Artificial Neural Network (ANN)
 - Network of many very simple processors (“units” or “neurons”), each with a small amount of local memory
 - Units connected by unidirectional communications channel
 - Units operate only on local data & inputs received via connections.
 - Training rule enables learning from examples & ability to do generalizations



Definitions (Cont.)

- Covert channel
 - Communication channel violating policy transferring info
- Covert storage channel
 - Writing to storage by one process & reading by another of lower security level
- Covert timing channel
 - One process signals to another by modulating own system use
 - Real response time observed by second process affected



Definitions (Cont.)

- Data mining
 - Analyzing databases using tools that look for trends or anomalies without knowledge of meaning of the data
- Design verification
 - Demonstrating mathematical correspondence between an abstract model & formal design spec.



Definitions (Cont.)

- Encapsulation
 - Object's protection of private data from outside access
 - No object should be able to access another object's internal data
 - Ability to have objects bundled (data & code)
- Expert system
 - Computer program containing a knowledge base & set of algorithms/rules that infer new facts from knowledge & incoming data
 - Artificial intelligence application using knowledge base of human experience to aid in solving problems



Definitions (Cont.)

- Granularity
 - Fineness or coarseness of security control mechanism
- Inference
 - Ability to derive information not explicitly available
 - Comparable problem to aggregation



Definitions (Cont.)

- Java
 - Object-oriented, distributed, interpreted architecture-neutral, multithreaded, general-purpose programming language
 - Developed by Sun Microsystems
 - Supports programming for the Internet with platform-independent Java "applets"
- Knowledge-base system (KBS)
 - Program for extending/querying a knowledge base (collection of knowledge expressed using a formal knowledge representation language)



Definitions (Cont.)

- Object-oriented programming (OOP)
 - Class of programming languages & techniques based on concept of “object,” a data structure (abstract data type) in a set of routines called “methods” which operate on the data
- Polyinstantiation
 - Iteratively producing a more defined version of an object by replacing variables with values (or other variables)
- Polymorphism
 - Different objects responding to the same command in different ways



Definitions (Cont.)

- Scalability
 - How well a problem solution will work when the size of the problem increases/decreases
- Trap door
 - Hidden mechanism to bypass protection measures
- Trojan Horse
 - Useful program containing hidden code exploiting the authorization of process to violate security



Definitions (Cont.)

- **Virus**
 - Program that searches out other programs and “infects” them by embedding a copy of itself
 - When program executes, embedded virus is executed, thereby propagating the “infection”
- **Work factor**
 - Effort or time needed to overcome protective measure
- **Worm**
 - Program that propagates itself over a network, reproducing itself enroute



System Life Cycle Phases

- Project initiation
 - Conceptual definition
 - Concept proposal & initial study
- Functional design analysis & planning
 - Functional requirements definition
 - System environment specification
- System design specification
 - System functional design review
 - Detailed planning of functional breakdown
 - Specification errors create system bugs
 - Preliminary design review
 - Code design review
- Software development
 - Programming & documentation



Life Cycle (Cont.)

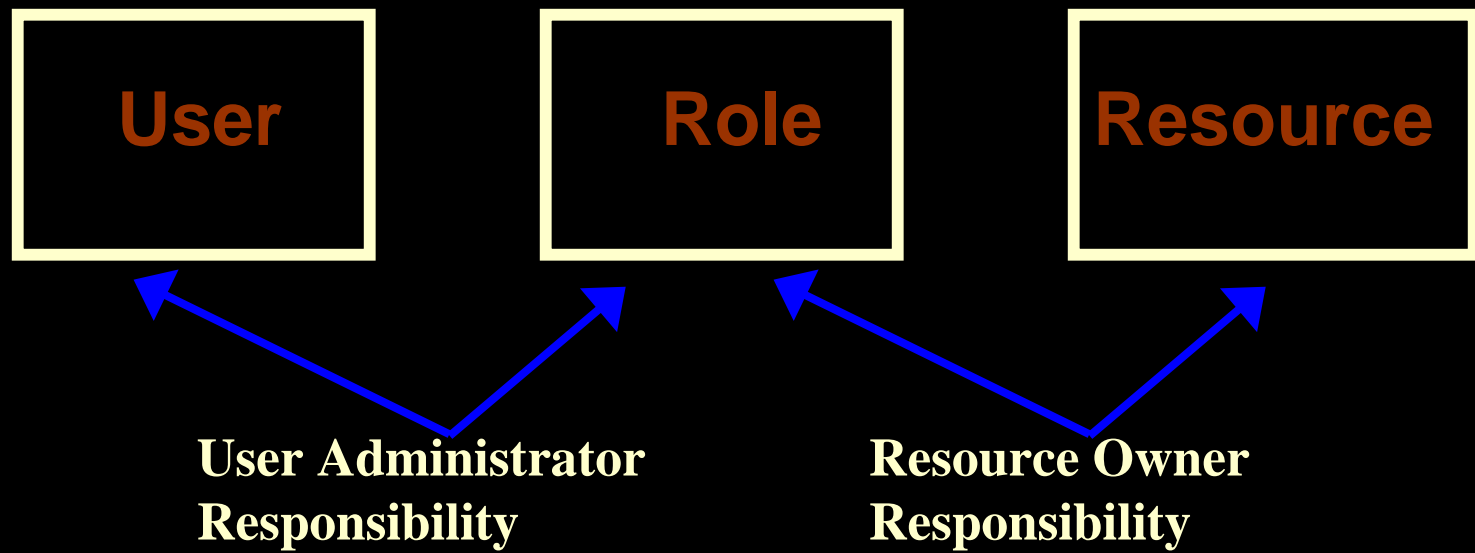
- Installation
 - Hardware installation/integration
 - Pre-implementation testing, installation & post-installation audit
 - Implementation must match spec. to avoid bugs
- Maintenance support
 - Program changes & minor modification
- Revisions & replacement
 - Major modification or replacement



Object-Oriented Technology

- Reuse components that work
- Class - software pattern for software object
 - May define relevant characteristics
 - Defined once
 - New objects created from it
 - Defines object's potential states, attributes, operations
 - Can limit ops & info to minimum for client to work
- Object – software entity that has state
 - Reusable
 - Contains data & methods or processes
 - State – some condition of its existence
 - Notion of state essential to modeling software objects

Role-Based Access Control

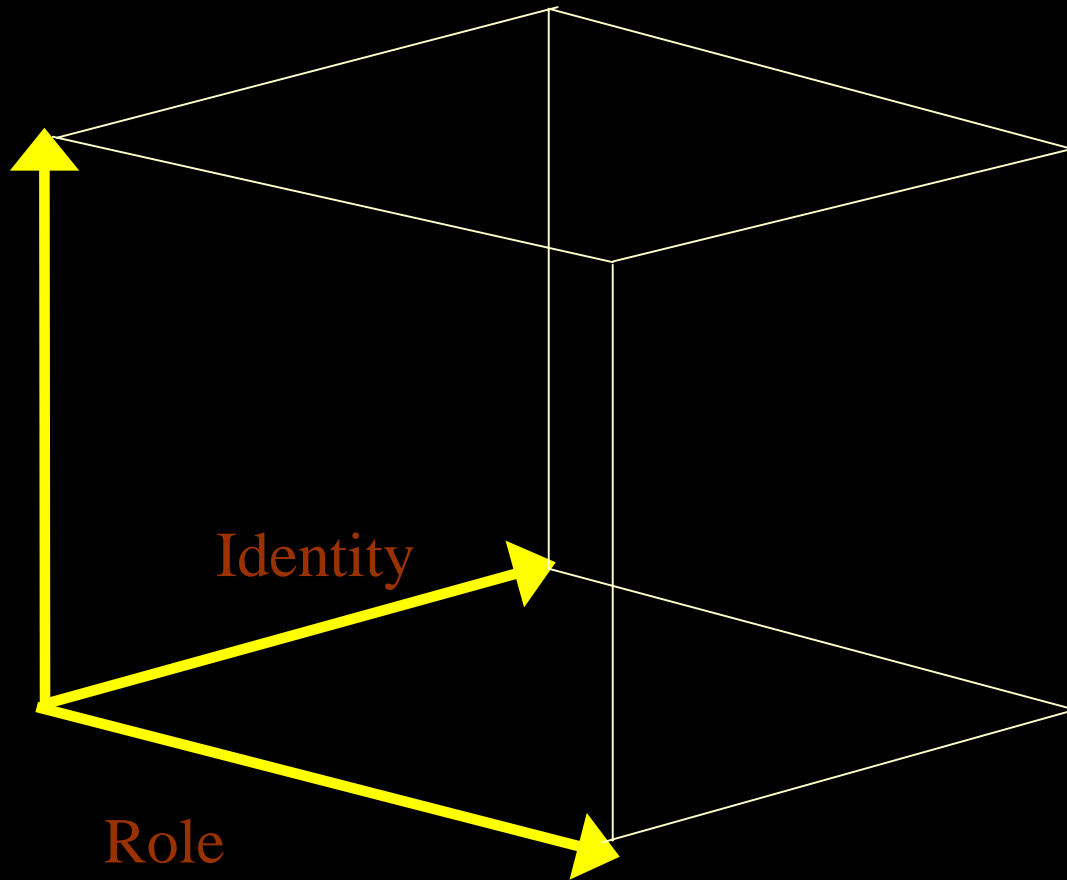


The Access Control Cube

Affinity

Identity

Role





Common Program Controls

- Edits
 - Syntax
 - Reasonableness
 - Range checks
 - Check digits
- Logs
 - Who, what, when
 - Time stamps
 - Before & after images



Common Controls (Cont.)

- Counts
 - Total transactions
 - Batch totals
 - Hash totals
 - Balances
- Internal checks
 - Parameter ranges & data types
 - Valid & legal address references
 - Completion codes
- Peer Review



On-Line Transaction Processing (OLTP)

- Enable applications to recover from errors more easily
- Monitoring system
 - Detects when individual processes abort
 - Can automatically restart them
 - Can back out transaction, if necessary
 - Allows distribution of multiple copies of application servers across machines
 - Monitor performs dynamic load balancing



Data Warehousing

- Combines data from multiple databases into a large database
- Attempts to find correlations between the various databases
- Develops MetaData from the Databases for analysis
- Very useful in making business decisions
- The Data Warehouse contains ALL of the companies data in one place
- Violation of the security perimeter would expose all data to an attacker

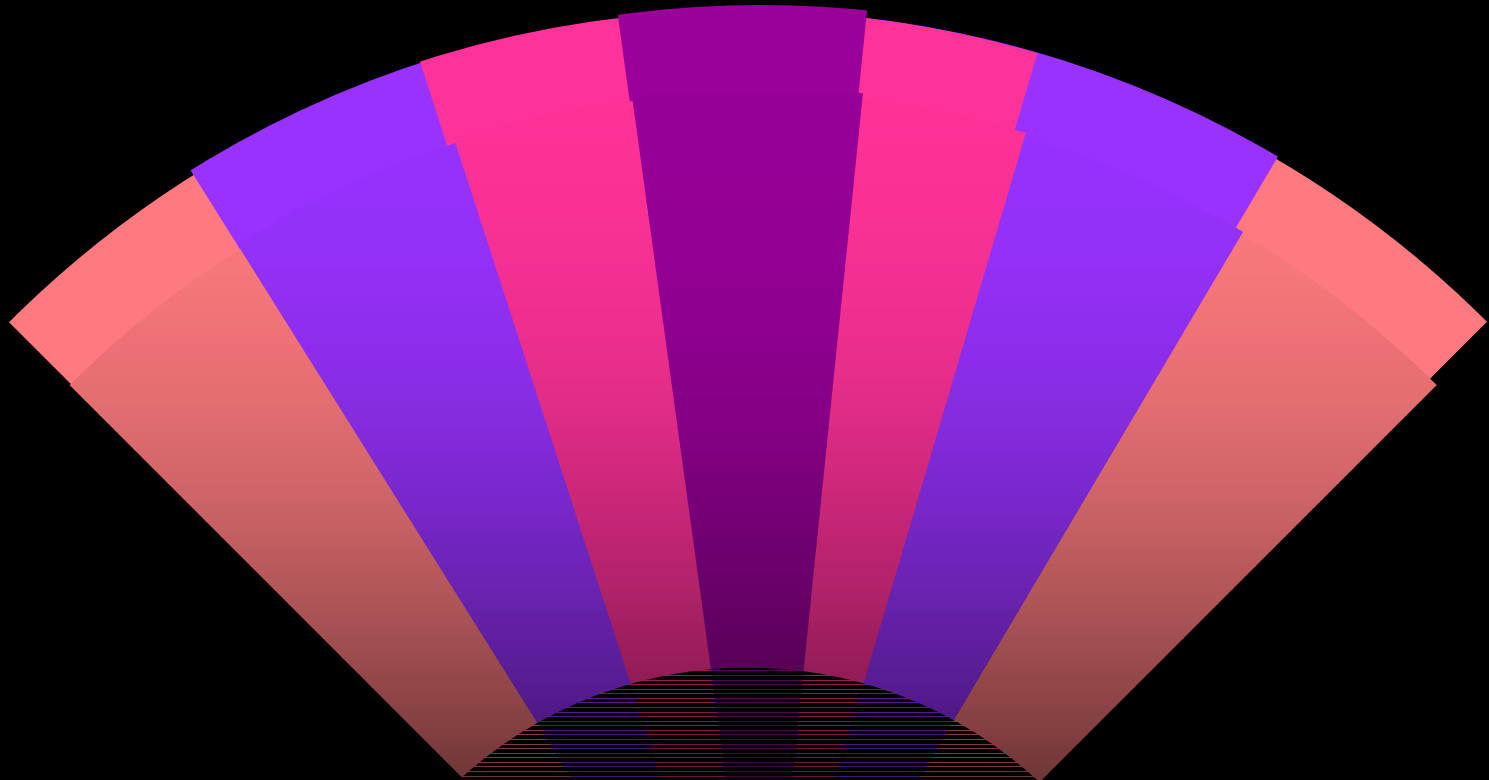


*Knowledge Base Systems, Expert
Systems & Neural Networks*



Relationship

- Knowledge Base
 - Contains all the data, or knowledge, on a particular matter
- Expert Systems use Knowledge Bases
 - Expert Systems use the data in the knowledge base to examine current events
 - They apply their rules, and then act
- Neural Nets
 - A “Learning System” or an “Adaptable Artificial Intelligence System”
 - Computer Systems which are taught



SAMPLE QUESTIONS



Sample Question

1. At what stage of the applications development process should the security department become involved?

- a. Prior to the implementation
- b. Prior to systems testing
- c. During unit testing
- d. During requirements development



Sample Question

2. What is one disadvantage of content-dependent protection of information?

- a. It increases processing overhead.
- b. It requires additional password entry.
- c. It exposes the system to data locking.
- d. It limits the user's individual address space.



Sample Question

3. In what way could Java applets pose a security threat?

- a. Their transport can interrupt the secure distribution of World Wide Web pages over the Internet by removing SSL and S-HTTP
- b. Java interpreters do not provide the ability to limit system access that an applet could have on a client system.
- c. Executables from the Internet may attempt an intentional attack when they are downloaded on a client system.
- d. Java does not check the bytecode at runtime or provide other safety mechanisms for program isolation from the client system.



Sample Question

4. Which of the following has the objective to control and manage data from a central location?

- a. Databases
- b. Data dictionaries
- c. Data access methods
- d. Data storage



Sample Question

5. A system file that has been patched numerous times becomes infected with a virus. The anti-virus software warns that disinfecting the file may damage it. What course of action should be taken?

- a. Replace the file with the original version from master media
- b. Proceed with automated disinfection
- c. Research the virus to see if it is benign
- d. Restore an uninfected version of the patched file from backup media