

Class One

- **Preliminaries & Logistics**
- **Basics of Computers and Networking**
- **Principals of Security**
- **Security Standards**
- **Ethics**
- **Professional Accreditation**

8/23/2007

Class 1

1

What's a Computer?

- Data in, Data out
- Hardware
- Software (programmable)
- Communications

Many common devices are computers...

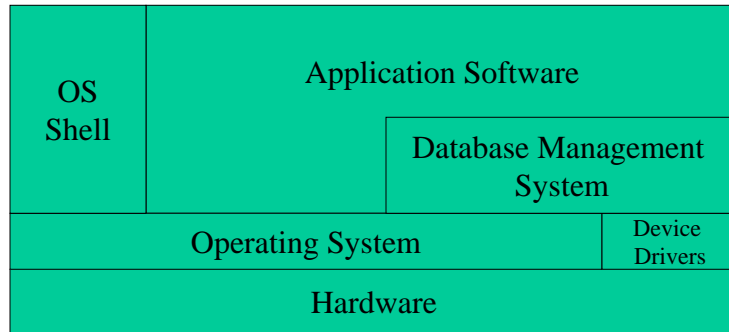
- Mainframes, servers
- Desktop systems
- Laptops, handheld
- Printers
- Phone systems
- Industrial control devices
- Retail Point of Sale devices

8/23/2007

Class 1

2

Layers of Computing

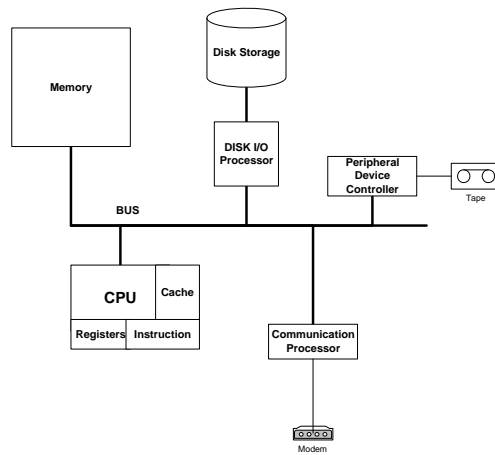


8/23/2007

Class 1

3

Hardware



8/23/2007

Class 1

4

Operating System

- Provides a command interface (a "shell") to the user
- Manages hardware resources:
 - Processor
 - Memory
 - Disk
 - Other devices
- Manages processes, tasks, and users
- Provides program interfaces (APIs) to permit application software to use hardware resources

How should an Operating System Protect Security:

- By protecting its own executable code from illicit modification
- By preventing modification or viewing of its own private memory areas
- By protecting users' private memory areas from other users
- By enforcing system security rules, and preventing the unauthorized bypassing of these rules

8/23/2007

Class 1

5

Database Management System

- Organizes information logically
- Allows applications to access data via standard interfaces
- Permits end users to generate ad-hoc reports
- Enforces data consistency

How should a DBMS Protect Security:

- By protecting its data from modification using non-DBMS utilities
- By maintaining data integrity through commit/rollback, referential integrity, etc.
- By assigning access rights consistent with the organization's policies
- By providing tamper-resistant audit logs of changes to critical data

8/23/2007

Class 1

6

Application Software

- Provides end user functionality
- Organizes and manages complex data objects (documents, ledgers, etc.)

How should Application Software Security:

- By supporting security functionality, such as identification and authentication of users, access controls, and audit logs.
- By maintaining reliability through high quality, well engineered design
- By assigning access rights to users consistent with the organization's policies
- By relying on (and not bypassing) DBMS and operating system security measures

8/23/2007

Class 1

7

Computer Networking

- **Scope:**
 - Local Area Network
 - Metropolitan Area Network
 - Wide Area Network
 - Common Carrier Network
- **Components:**
 - Computer (or other device input/output device)
 - Adapter/transceiver - Links device to LAN
 - Modem, CSU/DSU, PAD, FRAD - Links device to WAN
 - Transmission Media - How to get from here to there
 - Hub, Switch, Bridge, Router, Gateway - Devices to router and manage traffic between 2 end points

8/23/2007

Class 1

8

The OSI 7 Layer Model

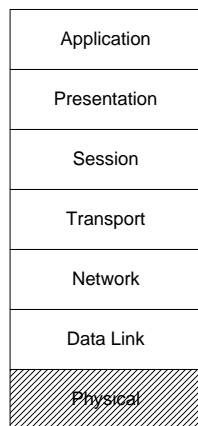
Application	Applications which use network services - e-mail, file transfer, etc.
Presentation	Data formatting (e.g., ASCII, EBCDIC, etc.)
Session	Adds additional end-to-end functions to the transport layer
Transport	Establishes reliable end-to-end communication by buffering packets, ensuring they are in the correct sequence, et.
Network	Determines how to send a packet across an entire network to the proper destination. Determines routing logic.
Data Link	Delivers information frames from one point to the adjacent point.
Physical	Defines transmission media, modulation, signal characteristics

8/23/2007

Class 1

9

OSI Layer 1 - Physical layer



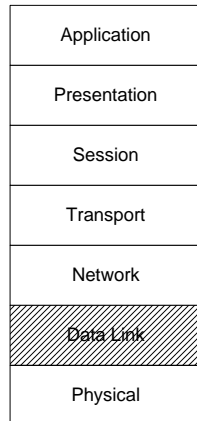
- Signal Characteristics
 - Frequency
 - Phase
 - Amplitude
- Transmission Media
- Encoding

8/23/2007

Class 1

10

OSI Layer 2 - Data Link Layer



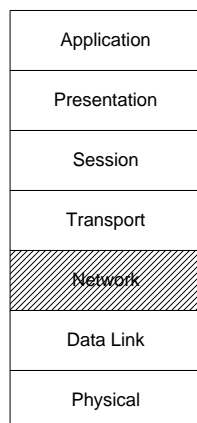
- Link-to-Link communication
- Basic unit is the “frame”. Adds point-to-point addressing to the packet
- Flow Control
- Error Control
- Synchronous vs. Asynchronous
- Split into 2 sublayers for LANs
 - Media Access Control (MAC)
 - Logical Link Control
- Examples: SDLC, X.25, Token Ring, Ethernet

8/23/2007

Class 1

11

OSI Layer 3 - Network Layer



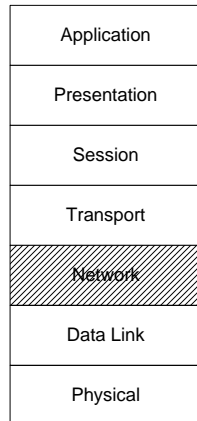
- How to follow a sequence of links to the ultimate destination
- Basic unit is the “packet”
- Adds routing information to the session information
- Examples:
 - IP
 - APPN (IBM’s SNA)
 - IPX (Novell)
- Includes protocols for updating routes (e.g., RIP, OSPF, BGP, etc.)

8/23/2007

Class 1

12

OSI Layer 3 - Network Layer



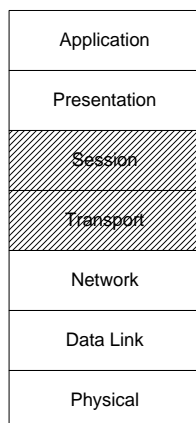
- Routing Protocols
 - How other routing devices learn the network's "map"
 - Not directly the concern of network end users
- Routed Protocols
 - The "package" delivered from source to destination
 - The routers must be able to forward package, based on the destination address

8/23/2007

Class 1

13

OSI Layers 4 & 5 - Transport and Session Layers



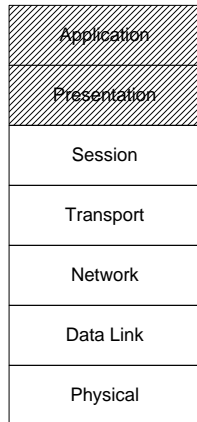
- How the client & server establish "state" across a network
- Most practical protocols combine Transport & Session features into one layer
- Adds session information to the basic application information
- Examples:
 - TCP
 - APPC (IBM's SNA)
 - SPX (Novell)
- Includes Application Programming Interfaces (APIs) for application use

8/23/2007

Class 1

14

OSI Layers 6 & 7 - Presentation & Application Layers



- How the “real work” gets done
- Most practical protocols combine into one layer
- The “data” portion of the packet/frame
- Examples:
 - Telnet, FTP, SMTP (TCP/IP)
 - DDM, SNADS (IBM’s SNA)
 - NDS, SAP (Novell)
- Client/Server logic resides at these layers

8/23/2007

Class 1

15

Security Economics

Protection of Value

Value comes from:

- ✓ Effort required to create or compile data
- ✓ Integrity of data
- ✓ Ability to use data to make something of value
- ✓ Ability to control use of data
- ✓ Ability to sell the data

8/23/2007

Class 1

16

Risk Analysis - How Much Security is Enough?

- Risk Analysis attempts to:
 - Place an economic value on data
 - Quantify loss if security breached
 - Estimate value of protection
 - Provide economically optimal level of protection

8/23/2007

Class 1

17

Risk Analysis - How Much Security is Enough?

- Risk Analysis general approach:
 - **Threat** - human and natural forces that threaten data
 - **Exposure** - Threats relevant to the data at hand
 - **Vulnerability** - inherent weaknesses in current protection of data
 - **Risk** - Probability of loss actually occurring, due to realization of a threat
 - **Protection** - Measures to reduce risk, by reducing the probability of a threat being realized, reducing the loss if a threat is realized, or both

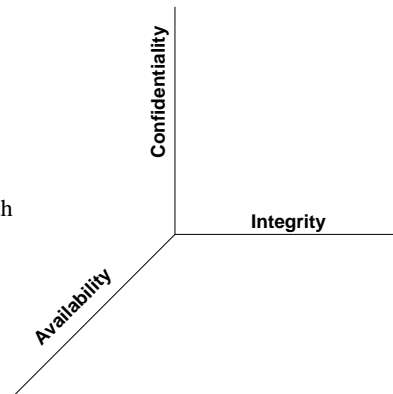
8/23/2007

Class 1

18

The Big Three - CIA

- **Confidentiality**
 - Keeping sensitive information secret
 - “Sensitivity”
- **Integrity**
 - Information is trustworthy
 - Internally consistent and consistent with reality
- **Availability**
 - Information is there, when you need it
 - “Criticality”

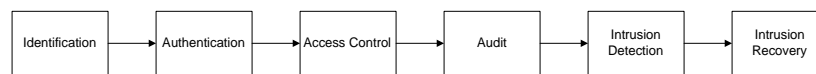


8/23/2007

Class 1

19

Security Transaction Life Cycle



Who am I?

Can I prove who I am?

What can I do?
What shouldn't I do?

What did I do?

Did I attempt to violate security policy?

How do we restore our data, if it is lost or security compromised

8/23/2007

Class 1

20

Identification and Authentication

- The “siamese twins” of security
- Identification is the assertion of an identity
 - Person
 - Organization
 - Role
 - System
 - Network
- Authentication is the proof of that identity
 - What information do I need to provide to prove who I am?



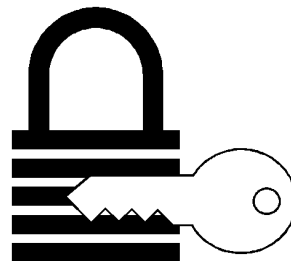
8/23/2007

Class 1

21

Access Control

- Once I have proven my identity, what may I access?
 - On which networks may I search for servers?
 - Which server applications may I execute?
 - Which files may I read/write/delete
 - Which applications may I execute



8/23/2007

Class 1

22

Audit

- Now that I have access:
 - How am I held accountable for my actions?
 - How can responsibility for activities be determined?
 - How can the history of activity affecting a valuable data resource be reconstructed
 - How can patterns of unusual or possibly illicit access be uncovered?

8/23/2007

Class 1

23

Intrusion Detection/Intrusion Response

- How do I find out if something has happened to my systems or data
- How do I recover?
- How do I handle the immediate cri



8/23/2007

Class 1

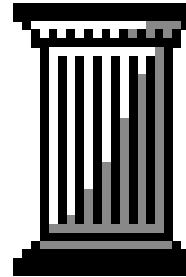
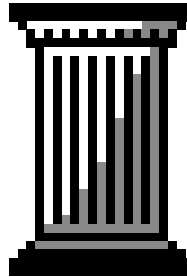
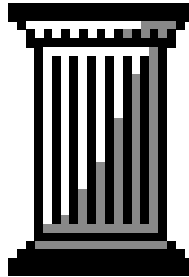
24

The Pillars of Security

Classification

Need to Know

Separation of Duties



8/23/2007

Class 1

25

Classification

- When is **more** security required?
- Applied typically (almost always!) to **confidentiality**
- Hierarchical
 - Systems and data are ordered by their confidentiality needs
 - Users and processes are ordered by their trustworthiness
 - A user or process must meet minimum trustworthiness standards to access data of a given sensitivity

8/23/2007

Class 1

26

Need to Know

- What may a user, process, or system access?
- Organized horizontally, by function, role, or department
- What does a system user require to do their jobs?
- Reduce possibility of information misuse by providing information to the minimum useful subset of staff
- Example:
 - Sales prospect lists restricted to sales department
 - Attorney/Client confidential documents restricted to legal
 - Technical network topology restricted to network support staff

8/23/2007

Class 1

27

Separation of Duties

- Some activities offer the opportunity for conflict of interest
- Fraud, theft, and just plain stupidity are reduced when areas which present conflicts are split into two or more separate individual responsibilities
- Honest people, when faced with inherently conflicting job duties, will choose the easiest path, even when that is not in an organization's best interest
- Examples:
 - Separate disbursements and bank reconciliation functions
 - Separate order taking and payment intake (e.g., in big ticket retail)
 - Separate programming and operations
 - Separate Internal Audit from everything else

8/23/2007

Class 1

28

Security is a Quality Issue

- *Reliability*
- *Trust*
- *Accountability*

- Most security problems represent inadvertent errors and omissions
- Security designed to thwart crooks can often help prevent well-intended errors
- Audit trails can be just as useful in tracking errors as in catching crooks

8/23/2007

Class 1

29

Security Standards

- Public Accounting
 - Requirement to rely on veracity of automated accounting systems
 - Financial transactions must be properly recorded and reflect the actual state of the enterprise
 - AICPA Standard Audit Statements (SAS) esp. SAS3
- HIPAA – Health care information privacy
- Sarbanes Oxley – Publicly traded companies
- CISP – VISA online merchant accounts
- Financial Sector
 - FFIEC examination criteria
 - Gramm Leach Bliley – Personal financial information privacy

8/23/2007

Class 1

30

Security Standards

- **Common Criteria** – Designed for component “certification” meaning evaluation
- **BS7799** - British Standard for security policies and practices. Has become an ISO standard (ISO 17799)
- **CobIT** - Control Objective for Information and Technology

8/23/2007

Class 1

31

The Common Criteria

- Component-level security evaluation
- Evaluates both functionality and assurance
 - Functionality - What security features does the component support
 - Assurance - How reliable are these security features? How well engineered are they?
- Functionality is described in “bundles” called Protection Profiles
- The specific product being evaluated is the Target of Evaluation (TOE)
- The application of a protection profile to the TOE is the Security Target

8/23/2007

Class 1

32

BS7799/ISO17799/ISO27000

- Criteria for the management and administration of security
- Applied to an organization, rather than a component
- Covers the following sections:
 - Security Policy
 - Security Organization
 - Assets Classification and control
 - Personnel security
 - Physical and environmental security
 - Computer and network security
 - System access control
 - Systems development and maintenance
 - Business continuity planning
 - Compliance
- ISO 27000 additionally covers risk management and metrics

8/23/2007

Class 1

33

CoBit

- Goal: To be an authoritative, up-to-date, international set of generally accepted information technology control objectives
- Concerned with IT governance – linking technology management to enterprise goals.
- Identifies 34 information technology processes:
 - An overall approach to control over these processes
 - Detailed control objectives for each process
 - Audit guidelines for each process
- Management guidelines
 - Maturity Models: Benchmarking, a standard for comparison with accepted practices)
 - Key Goal Indicators: Has the IT process achieved its business requirements?
 - Key Performance Indicators: Measures how well IT process is supporting goal
 - Critical Success Factors: Most significant issues or actions for enhancing control of IT processes

8/23/2007

Class 1

34

Security Profession Standards

- (ISC)2 Common Body of Knowledge (CBK)
 - Attempt to define a common body of knowledge for information security practitioners
 - Ten domains defined (Access Control, Communication Security, Risk Management & Continuity Planning, Policy and Standards, Computer Architecture, Law, Application Program Security, Cryptography, Operations Security, Physical Security)
 - Basis of CISSP

8/23/2007

Class 1

35

Security Profession Standards

- Generally Accepted Information Security Principles (GAISP)
 - Response to 1992 publication of "Computers at Risk" by US Government
 - Formerly "Generally Accepted System Security Principles (GASSP)"
 - Intended to promote good security practice, and to provide an authoritative point of reference for information security principles, practices and opinions
 - Supports both professional certification and product validation
 - Linked to Common Criteria, the CISSP CBK, and now ISO17799
 - Attempts to build on existing methodologies and standards
 - Version 1.0 of Pervasive Principles released July 1997
 - Dormant for many years
 - Now being actively developed by the ISSA

8/23/2007

Class 1

36

Professional Accreditation

- Certified Information Systems Security Professional (CISSP)
- Certified Information System Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified Protection Professional (CPP)
- Certified Fraud Examiner (CFE)
- Certified Internal Auditor (CIA)
- Cisco Certified Security Professional (CCSP)
- SANS GIAC
- CompTIA Security+
- Certified Ethical Hacker (CEH)
- Vendor-specific certifications

8/23/2007

Class 1

37

SANS GIAC Certifications

- Security Essentials Certification (GSEC)
- Certified Firewall Analyst (GCFW)
- Certified Intrusion Analyst (GCIA)
- Certified Incident Handler (GCIH)
- Certified Windows Security Administrator (GCWN)
- Certified UNIX Security Administrator (GCUX)
- Information Security Officer (GISO)
- Systems and Network Auditor (GSNA)
- Certified Forensic Analyst (GCFA)
- IT Security Audit Essentials (GSAE)

For information on certificate programs, please visit <http://www.giac.org/certificates.php>

8/23/2007

Class 1

38

Appendix – Acronyms and Definitions

(Taken from Wikipedia and other sources)

CSU/DSU - Channel Service Unit/Data Service Unit. The CSU is a device that connects a terminal to a digital line

FRAD - Frame Relay Assembler/Disassembler, a communications device that breaks a data stream into frames for transmission over a Frame Relay network and recreates a data stream from incoming frames

SDLC - Acronym for synchronous data link control, a protocol used in IBM's SNA networks. SDLC is similar to HDLC, an ISO standard.

HDLC - The HDLC protocol embeds information in a data frame that allows devices to control data flow and correct errors. HDLC is an ISO standard developed from the Synchronous Data Link Control (SDLC) standard proposed by IBM in the 1970's.

For any HDLC communications session, one station is designated primary and the other secondary

8/23/2007

Class 1

39

Appendix – Acronyms and Definitions

(Taken from Wikipedia and other sources)

Synchronous – continuous, governed by a clock signal

Asynchronous - irregular in timing, uses start and stop commands to regulate data flow

X.25 - A popular standard for packet-switching networks. The X.25 standard was approved by the CCITT (now the ITU) in 1976.

MAC - The Media Access Control Layer is one of two sublayers that make up the Data Link Layer of the OSI model. The MAC layer is responsible for moving data packets to and from one Network Interface Card (NIC) to another across a shared channel.

LLC - Logical Link Control (LLC) is the upper portion of the data link layer of a local area network, as defined in IEEE 802.2. The LLC sublayer presents a uniform interface to the user of the data link service, usually the network layer. Beneath the LLC sublayer is the Media Access Control (MAC) sublayer. Defines type of connection provided to upper layers

8/23/2007

Class 1

40

Appendix – Acronyms and Definitions

(Taken from Wikipedia and other sources)

RIP - an interior gateway protocol defined by RFC 1058 that specifies how routers exchange routing table information. With RIP, routers periodically exchange entire tables. A *distance vector* routing protocol.

OSPF - Open Shortest Path First, an interior gateway routing protocol developed for IP networks based on the shortest path first or *link-state algorithm*. Routers use link-state algorithms to send routing information to all nodes in an internetwork by calculating the shortest path to each node based on a topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations) that describes the state of its own links, and it also sends the complete routing structure (topography).

BGP - Border Gateway Protocol, an exterior gateway routing protocol that enables groups of routers (called autonomous systems) to share routing information so that efficient, loop-free routes can be established. BGP is commonly used within and between Internet Service Providers (ISPs). The protocol is defined in RFC 1771.

8/23/2007

Class 1

41

Appendix – Acronyms and Definitions

(Taken from Wikipedia and other sources)

NDS – Novell Directory Services, the directory services for Novell Netware networks. NDS complies with the X.500 standard and provides a logical tree-structure view of all resources on the network so that users can access them without knowing where they're physically located.

SAP - Service Advertising Protocol, a NetWare protocol used to identify the services and addresses of servers attached to the network. The responses are used to update a table in the router known as the Server Information Table.

8/23/2007

Class 1

42

Appendix – Acronyms and Definitions

(Taken from Wikipedia and other sources)

HIPAA - Health Insurance Portability and Accountability Act, HIPAA provides national standards to protect the privacy of personal health information

CISP - Cardholder Information Security Program. Effective since June 2001, CISP compliance has been required of all entities that store, process, or transmit Visa cardholder data. Financial institutions offering VISA cards must comply with CISP and are responsible for ensuring the compliance of their merchants and service providers for all payment channels, including retail, mail/telephone-order and ecommerce.

FFIEC - Federal Financial Institutions Examination Council. A formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS) and to make recommendations to promote uniformity in the supervision of financial institutions.

8/23/2007

Class 1

43

Appendix – Acronyms and Definitions

(Taken from Wikipedia and other sources)

CobIT - Control Objectives for Information and related Technology. COBIT has been developed as a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners.

8/23/2007

Class 1

44

Appendix – Acronyms and Definitions

(Taken from Wikipedia and other sources)

MATURITY MODELS for control over IT processes consist of developing a method of scoring so that an organisation can grade itself from non-existent to optimised (from 0 to 5). This approach has been derived from the Maturity Model that the Software Engineering Institute defined for the maturity of the software development capability².
CMM - a method for evaluating and measuring the maturity of the software development process of organizations on a scale of 1 to 5.
1 - Initial processes are usually ad hoc and chaotic.
2 - Repeatable Software development successes are repeatable. The organization may use some basic project management to track cost and schedule.
3 - Defined processes are well characterized and understood, and are described in standards, procedures, tools, and methods.
4 - Managed Using precise measurements, management can effectively control the software development effort.
5 - Optimizing focuses on continually improving process performance through both incremental and innovative technological improvements..

8/23/2007

Class 1

45

Appendix – Acronyms and Definitions

(Taken from Wikipedia and other sources)

(ISC)² - International Information Systems Security Certification Consortium
CISSP - Certified Information Systems Security Professional
ISSA - Information Systems Security Association

8/23/2007

Class 1

46