Module 3 – Protection of Information Assets

IT304 Internet and Network Security

04/21/2010

Agenda

- Information Assurance Career
  - IA job types & skill set
  - Scholarships
  - Certifications
  - IA Courses
- CISA exam six areas
  - Six areas
  - Topics in area 5
- Firewalls
- Virtual Private Networks
- Intrusion Detection

IA Job Types

- By contract type:
  - Full-time/In-House: typically recruited/promoted from within the company
  - Hired Guns: outside security contractors/consultants
- By position levels:
  - Security Engineers/Technicians: security in wired & wireless networks, firewall, intrusion detection & prevention, host security, (web) application security
  - Security Analysts: perform security audits and regulatory compliance checks
  - Security Architects: management-level position for designing and managing security infrastructure

IA Skill Set Requirements

- Hard Skills
  - Confidentiality:
    - working (but not necessarily expert) knowledge of encryption and cryptography, access control/authentication
    - → involves protecting the data from disclosure while stored or in transit
  - Integrity:
    - networking, hashing, public key infrastructure (PKI)
    - → ensures data stored or in transit cannot be corrupted or modified by unauthorized personnel without detection
  - Availability:
    - physical and network security, expert knowledge in Ethernet, Wifi, TCP/IP, FW/IDS/IPS, DDOS, etc
    - → requires not just technical know-how, but also physical construction and environment protections
  - Highly Marketable "Advanced skills":
    - expertise in penetration testing and code reviews, etc. Can really set the candidate apart
- Soft Skills
  - Communications skills, including technical writing and presentation skills, general management skills

Scholarships

- Department of Defense
  - DoD IA scholarship provides stipend and tuition
  - Will be required to serve a period of obligated service in DoD as a civilian employee or a member of one of the armed forces
- National Science Foundation
  - Federal Cyber Service: Scholarship for Service (SFS)
  - 2 years full scholarship
  - Will be required to work within the Federal Executive Branch at a Federal Agency, Independent Agency, Government Corporation, Commission, or Quasi-Official Agency, or at a National Laboratory
- Pace summer projects
  - Potential projects from Pace faculty

Industry certifications

- Information Systems Audit and Control Association, ISACA
  - Certified Information Security Auditor (CISA)
    - for professionals possessing information security audit and controls
  - Certified Information Security Manager (CISM)
    - for the individual who manages, designs, oversees and/or assesses an enterprise's information security
- The International Information Systems Security Certification Consortium, (ISC)^2
  - Certified Information Systems Security Professionals (CISSP)
    - for mid- and senior-level managers who are working toward or have already attained positions as Chief Information Security Officers or Senior Security Engineers

IA classes that you can take (for UG)

- CIT251 Computer Security Overview (originally IT300)
  - This course is usually offered in Fall
  - Wednesday 6:00-8:45PM
- CIT352 Network and Internet Security (originally IT304)
  - This course is usually offered in Spring
  - Wednesday 6:00-8:45PM
- CIT354 Computer Forensics (originally IT308)
  - This course is usually offered in Spring

MSIS or MSIT with a concentration on IA

- Introduction to Computer Security
- Information Security Management
- Web Security
- Network Security
- Security Forensics

Agenda

- Information Assurance Career
  - IA job types & skill set
  - Scholarships
  - Certifications
  - IA Courses
- CISA exam six areas
  - Six areas
  - Topics in area 5

CISA exam

- 200 multiple-choice questions that cover the six job practice areas
- The IS Audit Process (10%)
- IT Governance (15%)
- Systems and Infrastructure Life Cycle Management (16%)
- IT Service Delivery and Support (14%)
- Protection of Information Assets (31%)
- Business Continuity and Disaster Recovery (14%)

Importance of Information Security Management

- Key elements
- ISM Roles & responsibilities
- Inventory and classification of information assets
- System access permission
- Access control
- Privacy management and the role of IS auditor
- External parties and risks
- Addressing security when dealing with customers & 3rd party
- Human Resource Security
- Computer crimes & exposures
- Security incidence handling and responses

Logical Access

- Exposures
- Social engineering
- Logical access entry points
- Logical access control software
- Identification and authentication
- Authorization & access control lists
- Storing, retrieving, transporting and disposing of confidential information

Network Infrastructure Security

- LAN security
- Client-server security
- Wireless security
- Internet threat & security
  - IDS; firewalls/VPN
- Encryption
- Viruses
- Voice-over IP
- Private branch exchange

Auditing Information Security Management Framework

- Reviewing policies, procedures, and standards
- Logical access security policies
- Formal security awareness and training
- Data ownership; Documented authorization
- Terminate employee access; Security baseline
- Access standard
- Auditing logical access
- Testing tools & techniques

Auditing Network Infrastructure Security

- Auditing remote access
- Network penetration tests
- Full network assessment review
- Development and authorization of network changes
- Unauthorized changes
- Computer forensics

Environmental Exposures and Controls

- Environmental issues & exposures
  - Computer failure; power surge, etc
- Controls
- Fire suppression systems
- Location of computer rooms
- Emergency evacuation plan
- Power management

Physical Access Exposures and Controls

- Physical exposures
  - Blackmail; damage of equipments and documents
- Possible perpetrators
- Controls
- Auditing physical access

Mobile Computing

- WiFi security
  - Authentication; encryption; etc
- Laptop physical security

Firewall technology

IT304 Network and Internet security

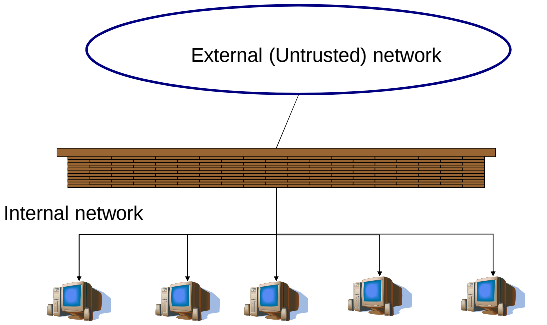
Li-Chiou Chen

03/12/2010

Firewall technology

- What is a firewall?
- Firewall technology
  - Packet filters
  - Inspection method
    - Non-stateful inspection
    - Stateful inspection
  - Proxy servers
  - Perimeter network (Demilitarized Zone, DMZ)
  - Network address translation (NAT)
- Firewall policy setting
- Using Firewalls with VPN

Firewall as a chock point between two networks



External (Untrusted) network

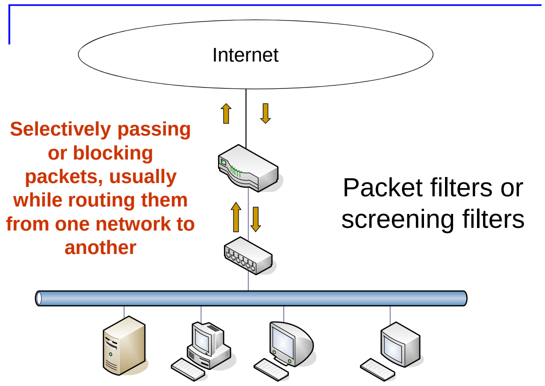
Internal network

What is a firewall

- Firewall is a component that restrict traffic between external and internal networks
- Can be any device, software or arrangement or equipment that limits network access
- Sometimes it is bundled with other devices, such as routers, modems, and IP switches
  - Usually with limited functionality, such as packet filtering
- Some OS is bundled with simple software packet filters, such as Windows XP, Linux

Firewall technology

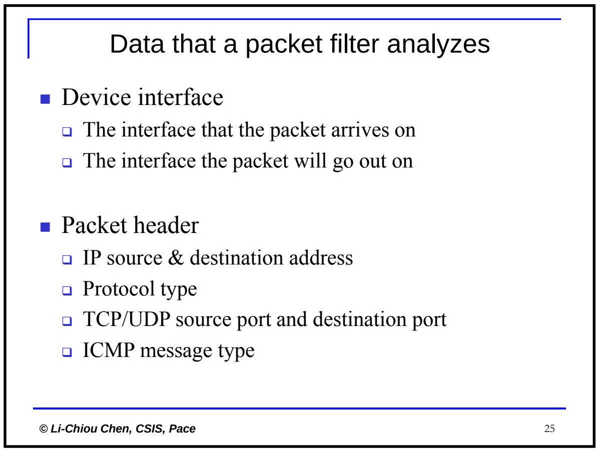
- What is a firewall?
- Firewall technology
  - Packet filters
  - Inspection method
    - Non-stateful inspection
    - Stateful inspection
  - Proxy servers
  - Perimeter network (Demilitarized Zone, DMZ)
  - Network address translation (NAT)
- Firewall policy setting
- Using Firewalls with VPN
- Blocking P2P applications on a firewall



Internet

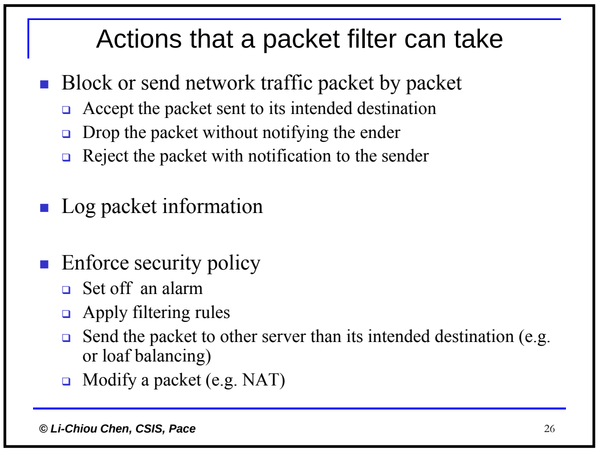
Selectively passing or blocking packets, usually while routing them from one network to another

Packet filters or screening filters



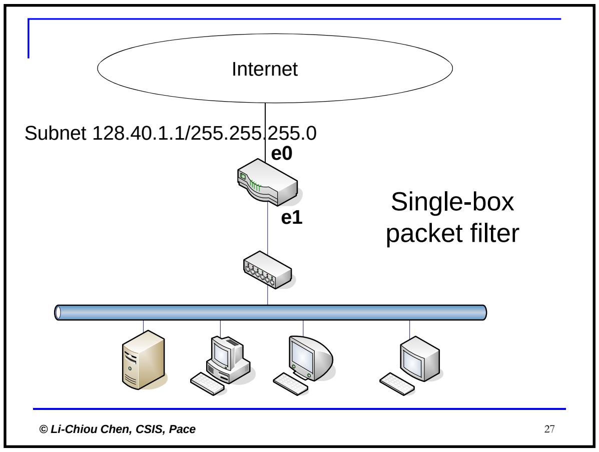
Data that a packet filter analyzes

- Device interface
  - The interface that the packet arrives on
  - The interface the packet will go out on
- Packet header
  - IP source & destination address
  - Protocol type
  - TCP/UDP source port and destination port
  - ICMP message type

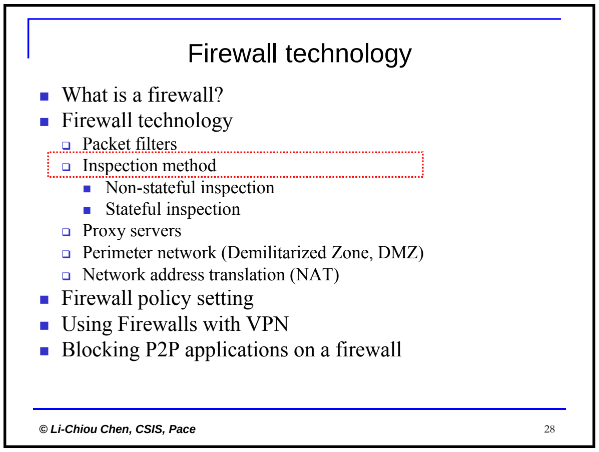


Actions that a packet filter can take

- Block or send network traffic packet by packet
  - Accept the packet sent to its intended destination
  - Drop the packet without notifying the ender
  - Reject the packet with notification to the sender
- Log packet information
- Enforce security policy
  - Set off an alarm
  - Apply filtering rules
  - Send the packet to other server than its intended destination (e.g. or loaf balancing)
  - Modify a packet (e.g. NAT)

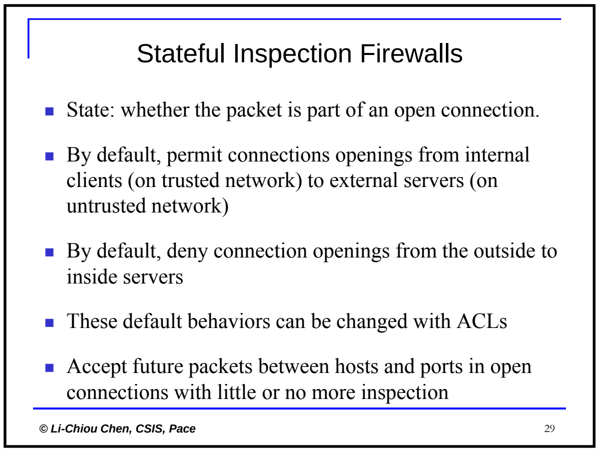


Single-box packet filter



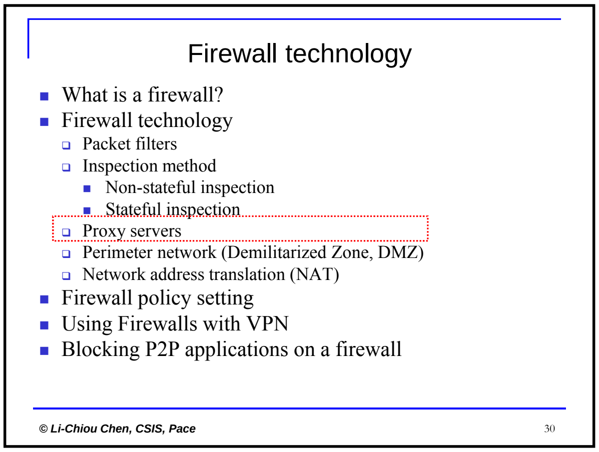
Firewall technology

- What is a firewall?
- Firewall technology
  - Packet filters
  - Inspection method
    - Non-stateful inspection
    - Stateful inspection
  - Proxy servers
  - Perimeter network (Demilitarized Zone, DMZ)
  - Network address translation (NAT)
- Firewall policy setting
- Using Firewalls with VPN
- Blocking P2P applications on a firewall



Stateful Inspection Firewalls

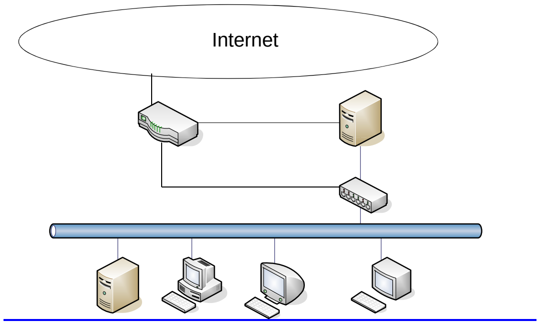
- State: whether the packet is part of an open connection.
- By default, permit connections openings from internal clients (on trusted network) to external servers (on untrusted network)
- By default, deny connection openings from the outside to inside servers
- These default behaviors can be changed with ACLs
- Accept future packets between hosts and ports in open connections with little or no more inspection



Firewall technology

- What is a firewall?
- Firewall technology
  - Packet filters
  - Inspection method
    - Non-stateful inspection
    - Stateful inspection
  - Proxy servers
  - Perimeter network (Demilitarized Zone, DMZ)
  - Network address translation (NAT)
- Firewall policy setting
- Using Firewalls with VPN
- Blocking P2P applications on a firewall

Proxy server



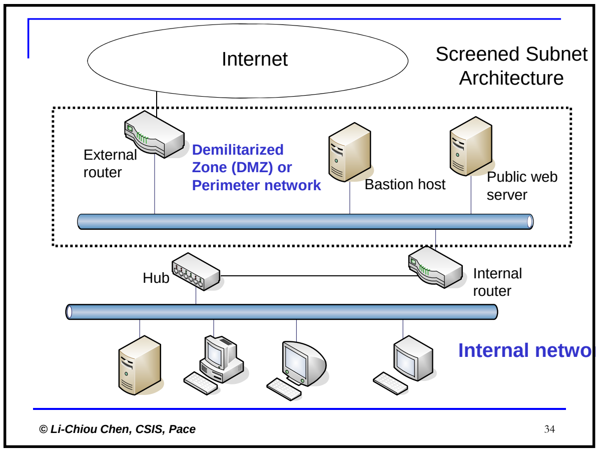
Proxy servers

- Specialized application or server programs that take users’ requests for Internet services, such as telnet or http
- Proxy servers forward users’ requests as appropriate according to the site’s security policy
- Also known as “application-level gateway”

Firewall technology

- What is a firewall?
- Firewall technology
  - Packet filters
  - Inspection method
    - Non-stateful inspection
    - Stateful inspection
  - Proxy servers
  - Perimeter network (Demilitarized Zone, DMZ)
  - Network address translation (NAT)
- Firewall policy setting
- Using Firewalls with VPN
- Blocking P2P applications on a firewall

Screened Subnet Architecture



Bastion host

- Main point of contact for incoming connections from external network
  - For FTP connections to the site’s anonymous FTP server
  - For DNS queries about the hosts in the site
  - For SMTP sessions to deliver emails
- Outbound connections handled as one of the two methods
  - Through routers that allows direct internal to external connections
  - Through proxy server that runs on bastion host
- Must be highly secure because it is usually exposed to the Internet

Perimeter network

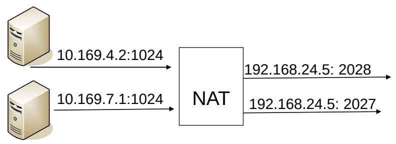
- A network added between an external network and an internal network in order to provide an additional layer of security
- Also called “demilitarized zone” (DMZ)
- No internal traffic is allowed
  - All traffic on the perimeter network should be to/from an external network or to/from bastion host

Firewall technology

- What is a firewall?
- Firewall technology
  - Packet filters
  - Inspection method
    - Non-stateful inspection
    - Stateful inspection
  - Proxy servers
  - Perimeter network (Demilitarized Zone, DMZ)
  - Network address translation (NAT)
- Firewall policy setting
- Using Firewalls with VPN
- Blocking P2P applications on a firewall

Network Address Translation (NAT)

- Also called IP-masquerading
- Dynamically allocate external address and port for each connection initiated by an internal host
- Mainly used to multiplex numerous IP addresses over a few
- Enforces a firewall over outbound connections
- Helps to conceal internal network configuration



IPv4 Private IP Addresses

Name	IP address range	number of IPs	*classful* description	largest CIDR block
24-bit block	10.0.0.0 – 10.255.255.255	16,777,215	single class A	10.0.0.0/8
20-bit block	172.16.0.0 – 172.31.255.255	1,048,576	16 contiguous class Bs	172.16.0.0/12
16-bit block	192.168.0.0 – 192.168.255.255	65,535	256 contiguous class Cs	192.168.0.0/16

Firewall technology

- What is a firewall?
- Firewall technology
  - Packet filters
  - Inspection method
    - Non-stateful inspection
    - Stateful inspection
  - Proxy servers
  - Perimeter network (Demilitarized Zone, DMZ)
  - Network address translation (NAT)
- Firewall policy setting
- Using Firewalls with VPN
- Blocking P2P applications on a firewall

Keep the Rule Base Simple

- Keep list of rules as short as possible
  - About 30 and 50 rules
  - Shorter the rule base, faster the firewall will perform
- Firewalls process rules in a particular order
  - Usually rules are numbered starting at 1 and displayed in a grid
  - Most important rules should be at the top of the list
  - Make the last rule a cleanup rule
    - A catch-all type of rule

Restrict Subnets, Ports, and Protocols

- Filtering by IP addresses
  - You can identify traffic by IP address range
  - Most firewalls start blocking all traffic
    - You need to identify “trusted” networks
    - Firewall should allow traffic from trusted sources

Control Internet Services

- Web services
  - Employees always want to surf the Internet
- DNS
  - Resolves fully qualified domain names (FQDNs) to their corresponding IP addresses
  - DNS uses UDP port 53 for name resolution
  - DNS uses TCP port 53 for zone transfers
- E-mail
  - POP3 and IMAP4
  - SMTP
  - LDAP and HTTP

Firewall technology

- What is a firewall?
- Firewall technology
  - Packet filters
  - Inspection method
    - Non-stateful inspection
    - Stateful inspection
  - Proxy servers
  - Perimeter network (Demilitarized Zone, DMZ)
  - Network address translation (NAT)
- Firewall policy setting
- Using Firewalls with VPN
- Blocking P2P applications on a firewall

Using VPNs with Firewalls

- VPNs do not reduce the need for a firewall
  - Always use a firewall as part of VPN security design
- Install VPN software on the firewall itself
  - Firewall allows outbound access to the Internet
  - Firewall prevents inbound access from the Internet
  - VPN service encrypts traffic to remote clients or networks

Install VPN software on the firewall itself

- Advantages
  - Control all network access security from one server
  - Fewer computers to manage
  - Use the same tools for VPN and firewall
- Disadvantages
  - Single point of failure
  - Must configure routes carefully
  - Internet access and VPN traffic compete for resources on the server

Set up VPN parallel to your firewall inside the DMZ

- Advantages
  - No need to modify firewall settings to support VPN traffic
  - Configuration scales more easily
  - Can deal with congested servers
- Disadvantages
  - VPN server is connected directly to the Internet
  - If VPN server becomes compromised, attacker will have direct access to your internal network
  - Cost of supporting a VPN increases with new servers

Set up VPN server behind the firewall connected to the internal network

- Advantages
  - VPN server is completely protected from the Internet
  - Firewall is the only device controlling access
  - VPN traffic restrictions are configured on VPN server
- Disadvantages
  - VPN traffic must travel through the firewall
  - Firewall must handle VPN traffic
  - Firewall might not know what to do with IP protocols other than ICMP, TCP, and UDP

PPTP Filters

- Might be only option when VPN connections pass through NAT
- PPTP uses two protocols
  - TCP
  - GRE

L2TP and IPSec Filters

- IKE uses protocol ID 171 and UDP on port 500
- ESP uses protocol ID 50
- AH uses protocol ID 51

Virtual Private Network

IT304 Internet and Network Security

Li-Chiou Chen

03/03/2010

Agenda

- VPN basics
  - Types of VPN
  - Encapsulation
  - Encryption in VPNs
  - Authentication in VPNs
  - Pros and Cons
- Configuration and Implementation
  - Design considerations
  - Configuration Options
  - Set up VPNs with firewalls
  - Guidelines for auditing VPNs and VPN policies
- Lab #7

What VPNs are

- A secure tunnel: enables computers to communicate securely over insecure channels such as the Internet
- Enables computers to exchange private encrypted messages that others cannot decipher
- Virtual network connection
- Extends an organization’s network perimeter

Business incentives driving VPN adoption

- VPNs are cost-effective
- VPNs provide secure connection for remote users
  - Contractors
  - Traveling employees
  - Partners and suppliers
  - ………

VPN Components

- VPN server or host
  - Configured to accept connections from clients
- VPN client or guest
  - Endpoints connecting to a VPN
- Tunnel
  - Connection through which data is sent
- VPN protocols
  - Sets of standardized communication settings
  - Used to encrypt data sent along the VPN

Types of VPNs

- In terms of VPN implementation
  - Hardware VPN
  - Software VPN
- In terms of end points
  - End-point solutions
    - Site-to-site VPN
      - Gateway-to-gateway VPN
    - Client-to-site VPN
      - Remote access VPN
  - Infrastructure solution: MPLS VPN

Hardware-based VPNs

- Connect one gateway to another
- Routers at each network gateway encrypt and decrypt packets
- VPN appliance
  - Designed to serve as VPN endpoint
  - Join multiple LANs
- Benefits
  - Scalable
  - Better security

Software-based VPNs

- Integrated with firewalls
- Appropriate when participating networks use different routers and firewalls
- Benefits
  - More cost-effective
  - Offer maximum flexibility

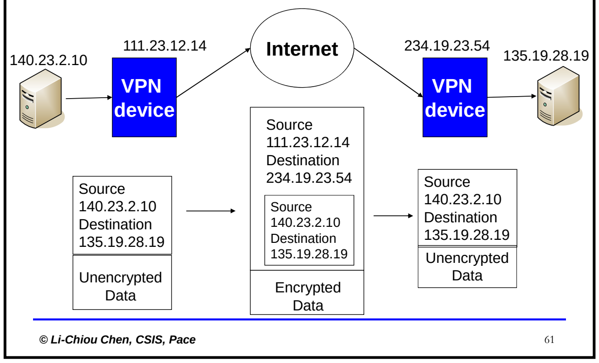
End point solutions

- Use tunneling protocols to encrypt and encapsulate IP packets
- Encrypted route through the Internet
  - Routes may be asymmetric as regular Internet routing
- Need VPN compliant routers
- Do not need to subscribe specific services from ISPs

Agenda

- VPN basics
  - Types of VPN
  - Encapsulation
  - Encryption in VPNs
  - Authentication in VPNs
  - Pros and Cons
- Configuration and Implementation
  - Design considerations
  - Configuration Options
  - Set up VPNs with firewalls
  - Guidelines for auditing VPNs and VPN policies
- Lab #7

Encapsulation encloses a packet within another and assigns a different IP source and destination

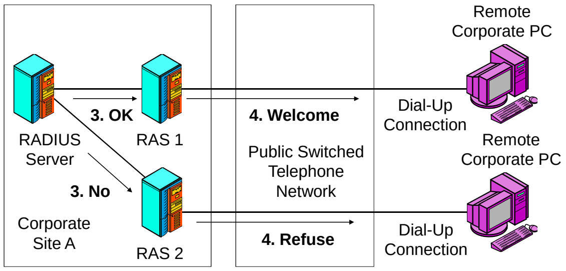


140.23.2.10
111.23.12.14
VPN device
Internet
234.19.23.54
VPN device
135.19.28.19
Source 140.23.2.10 Destination 135.19.28.19
Unencrypted Data
Source 111.23.12.14 Destination 234.19.23.54
Source 140.23.2.10 Destination 135.19.28.19
Encrypted Data
Source 140.23.2.10 Destination 135.19.28.19
Unencrypted Data

Tunneling protocols

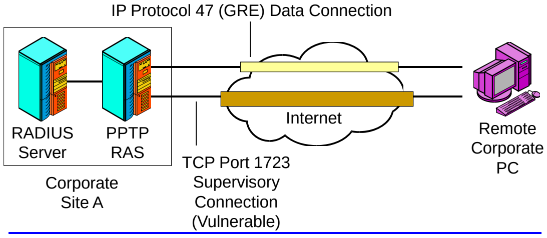
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Both PPTP and L2TP operates at the data link layer

Point-to-Point Protocol (PPP) and RADIUS for Dial-Up Remote Access



Point-to-Point Tunneling Protocol (PPTP)

Direct connection between PC and RAS



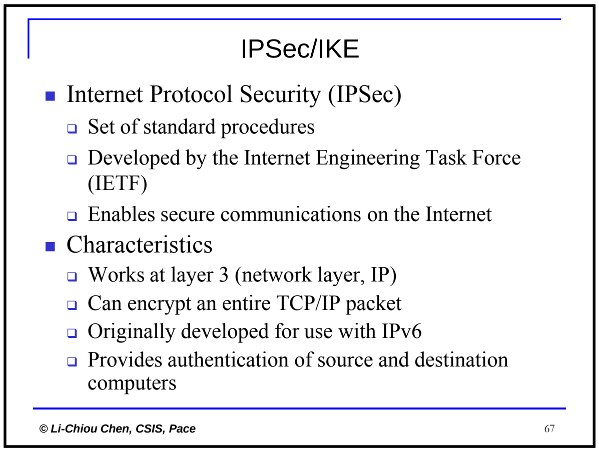
IP Protocol 47 (GRE) Data Connection
RADIUS Server
PPTP RAS
Internet
Remote Corporate PC
Corporate Site A
TCP Port 1723 Supervisory Connection (Vulnerable)

Point-to-Point Tunneling Protocol (PPTP)

- Encapsulates PPP data frames within IP packets for Internet
- Allow corporations that used PPP dialup systems to transform to VPN for remote access
- Header contains only information needed to route data from the VPN client to the server
- Uses Microsoft Point-to-Point Encryption (MPPE)
  - Encrypt data that passes between the remote computer and the remote access server

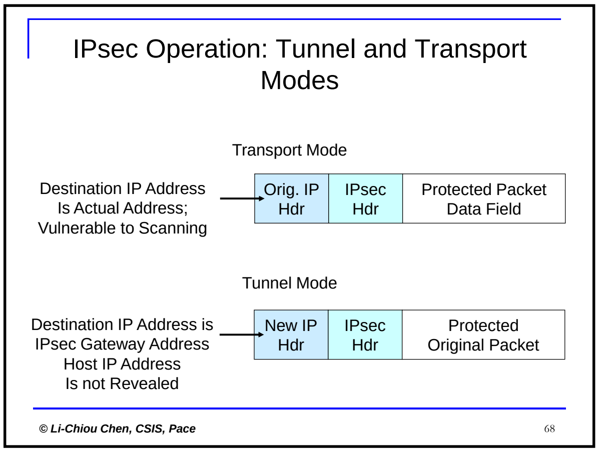
Layer 2 Tunneling Protocol (L2TP)

- Provides better security through IPSec
- IPSec encryption is more secure and widely supported
- IPSec enables L2TP to perform
  - Authentication
  - Encapsulation
  - Encryption



IPSec/IKE

- Internet Protocol Security (IPSec)
  - Set of standard procedures
  - Developed by the Internet Engineering Task Force (IETF)
  - Enables secure communications on the Internet
- Characteristics
  - Works at layer 3 (network layer, IP)
  - Can encrypt an entire TCP/IP packet
  - Originally developed for use with IPv6
  - Provides authentication of source and destination computers



IPsec Operation: Tunnel and Transport Modes

Transport Mode

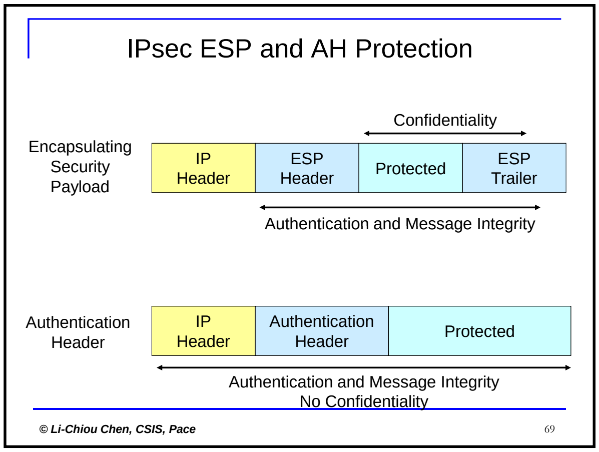
Destination IP Address Is Actual Address; Vulnerable to Scanning

Orig. IP Hdr	IPsec Hdr	Protected Packet Data Field

Tunnel Mode

Destination IP Address is IPsec Gateway Address Host IP Address Is not Revealed

New IP Hdr	IPsec Hdr	Protected Original Packet



IPsec ESP and AH Protection

Encapsulating Security Payload

Confidentiality

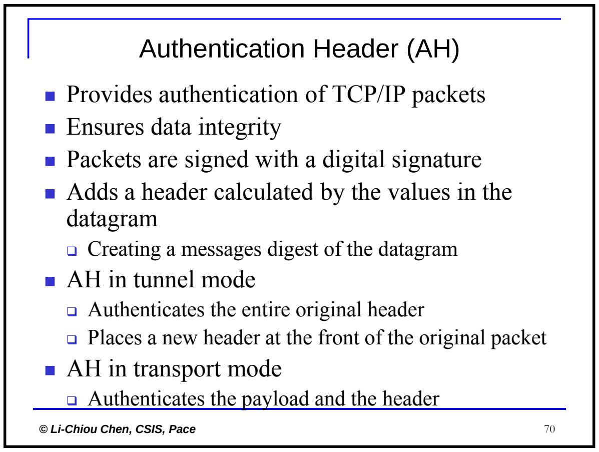
IP Header	ESP Header	Protected	ESP Trailer

Authentication and Message Integrity

Authentication Header

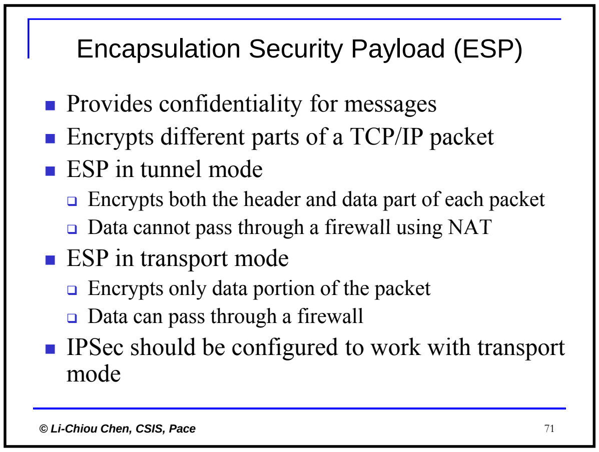
IP Header	Authentication Header	Protected

Authentication and Message Integrity
No Confidentiality



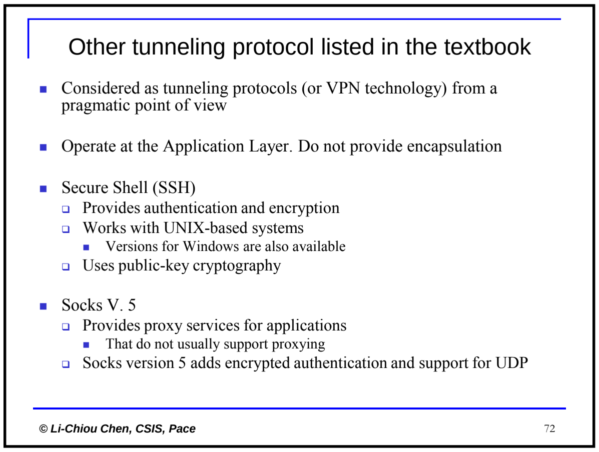
Authentication Header (AH)

- Provides authentication of TCP/IP packets
- Ensures data integrity
- Packets are signed with a digital signature
- Adds a header calculated by the values in the datagram
  - Creating a messages digest of the datagram
- AH in tunnel mode
  - Authenticates the entire original header
  - Places a new header at the front of the original packet
- AH in transport mode
  - Authenticates the payload and the header



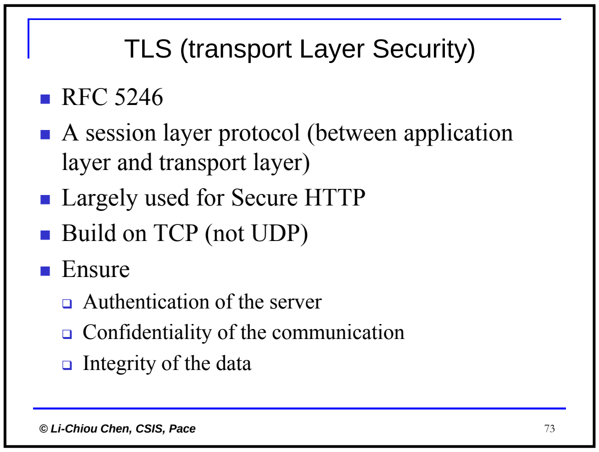
Encapsulation Security Payload (ESP)

- Provides confidentiality for messages
- Encrypts different parts of a TCP/IP packet
- ESP in tunnel mode
  - Encrypts both the header and data part of each packet
  - Data cannot pass through a firewall using NAT
- ESP in transport mode
  - Encrypts only data portion of the packet
  - Data can pass through a firewall
- IPSec should be configured to work with transport mode



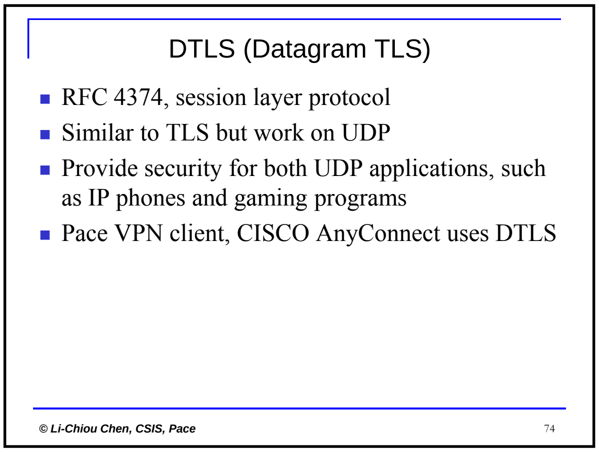
Other tunneling protocol listed in the textbook

- Considered as tunneling protocols (or VPN technology) from a pragmatic point of view
- Operate at the Application Layer. Do not provide encapsulation
- Secure Shell (SSH)
  - Provides authentication and encryption
  - Works with UNIX-based systems
    - Versions for Windows are also available
  - Uses public-key cryptography
- Socks V. 5
  - Provides proxy services for applications
    - That do not usually support proxying
  - Socks version 5 adds encrypted authentication and support for UDP



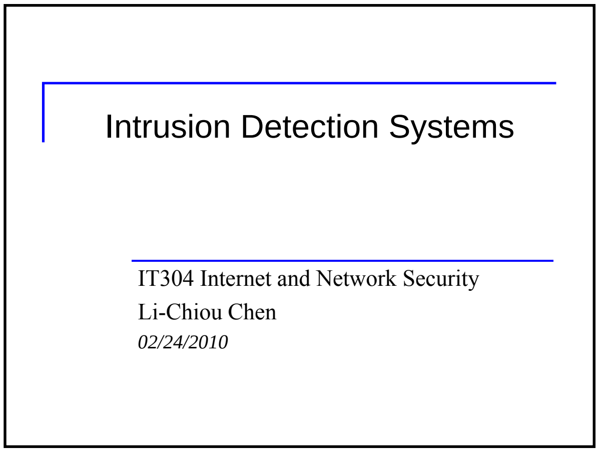
TLS (transport Layer Security)

- RFC 5246
- A session layer protocol (between application layer and transport layer)
- Largely used for Secure HTTP
- Build on TCP (not UDP)
- Ensure
  - Authentication of the server
  - Confidentiality of the communication
  - Integrity of the data



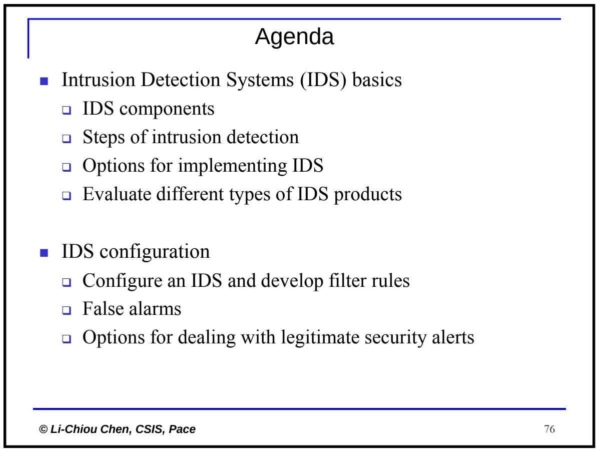
DTLS (Datagram TLS)

- RFC 4374, session layer protocol
- Similar to TLS but work on UDP
- Provide security for both UDP applications, such as IP phones and gaming programs
- Pace VPN client, CISCO AnyConnect uses DTLS



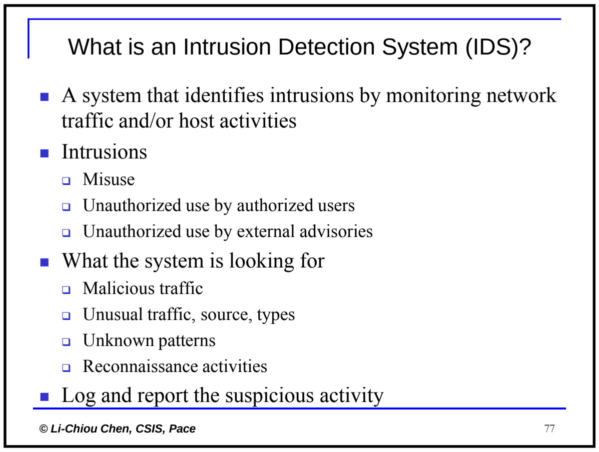
Intrusion Detection Systems

IT304 Internet and Network Security
Li-Chiou Chen
02/24/2010



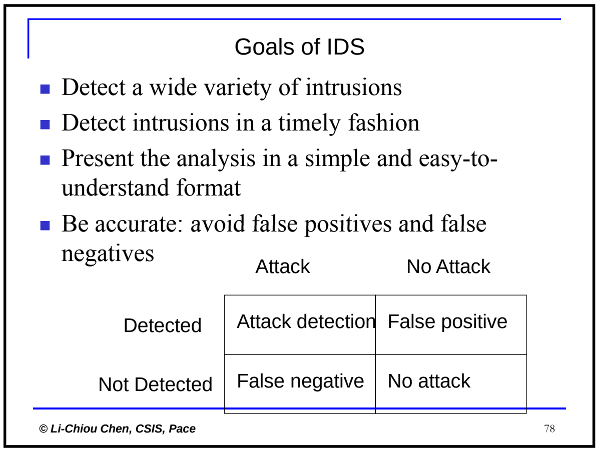
Agenda

- Intrusion Detection Systems (IDS) basics
  - IDS components
  - Steps of intrusion detection
  - Options for implementing IDS
  - Evaluate different types of IDS products
- IDS configuration
  - Configure an IDS and develop filter rules
  - False alarms
  - Options for dealing with legitimate security alerts



What is an Intrusion Detection System (IDS)?

- A system that identifies intrusions by monitoring network traffic and/or host activities
- Intrusions
  - Misuse
  - Unauthorized use by authorized users
  - Unauthorized use by external advisories
- What the system is looking for
  - Malicious traffic
  - Unusual traffic, source, types
  - Unknown patterns
  - Reconnaissance activities
- Log and report the suspicious activity



Goals of IDS

- Detect a wide variety of intrusions
- Detect intrusions in a timely fashion
- Present the analysis in a simple and easy-to-understand format
- Be accurate: avoid false positives and false negatives

	Attack	No Attack
Detected	Attack detection	False positive
Not Detected	False negative	No attack

Intrusion Detection System Components

- Network sensors
- Alert systems
- Command console
- Response system
- Database of attack signatures or behaviors

Network Sensors

- Electronic “eyes” of an IDS
- Hardware or software that monitors traffic in your network and triggers alarms
- Sensors should be placed at common-entry points
  - Internet gateways
  - Connections between one LAN and another
  - Remote access server that receives dial-up connections from remote users
  - Virtual private network (VPN) devices
  - Sensors could be positioned at either side of the firewall
    - Behind the firewall is a more secure location
- Management program controls sensors

Alert Systems

- Trigger
  - Circumstances that cause an alert message to be sent
- Types of triggers
  - Detection of an anomaly
  - Detection of misuse

Command Console

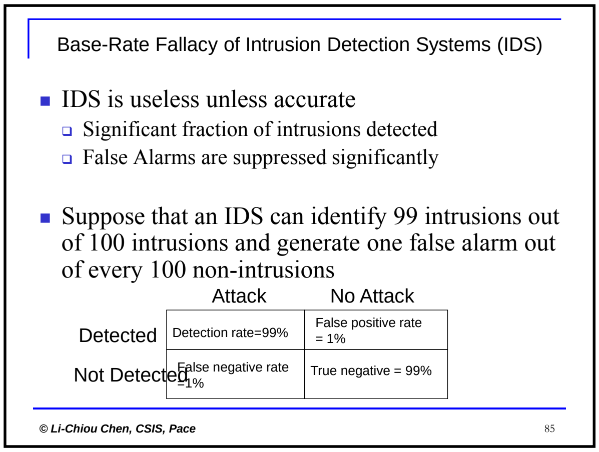
- Provides a graphical front-end interface to an IDS
  - Enables administrators to receive and analyze alert messages and manage log files
- IDS can collect information from security devices throughout a network
- Command console should run on a computer dedicated solely to the IDS
  - To maximize the speed of response

Response System

- IDS can be setup to take some countermeasures
- Response systems do not substitute network administrators
  - Administrators can use their judgment to distinguish a false positive
  - Administrators can determine whether a response should be escalated
    - Increased to a higher level

Database of Attack Signatures or Behaviors

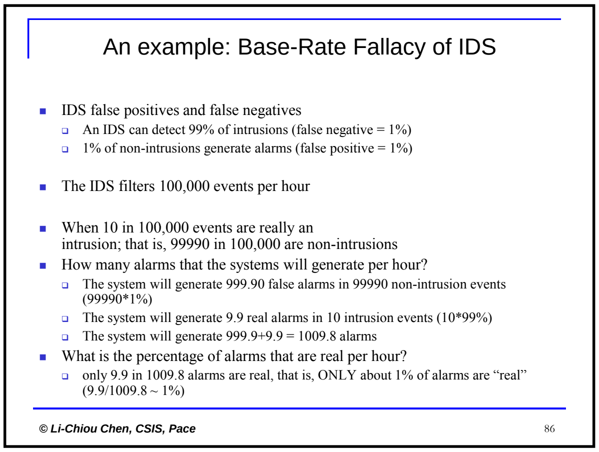
- IDSs don’t have the capability to use judgment
  - Can make use of a source of information for comparing the traffic they monitor
- Misuse detection
  - References a database of known attack signatures
  - If traffic matches a signature, it sends an alert
  - Keep database updated
  - Passive detection mode
- Anomaly-based IDS
  - Store information about users in a database



Base-Rate Fallacy of Intrusion Detection Systems (IDS)

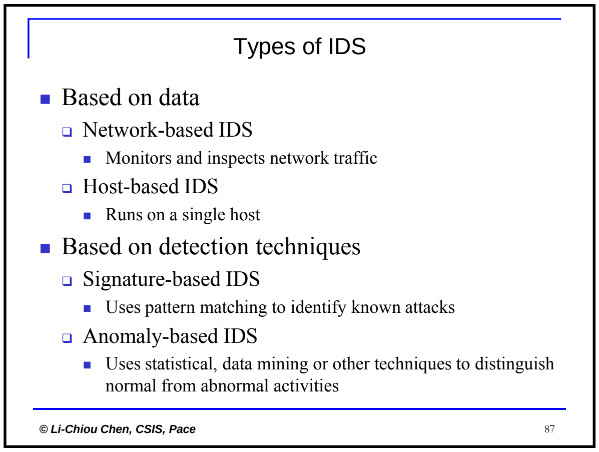
- IDS is useless unless accurate
  - Significant fraction of intrusions detected
  - False Alarms are suppressed significantly
- Suppose that an IDS can identify 99 intrusions out of 100 intrusions and generate one false alarm out of every 100 non-intrusions

	Attack	No Attack
Detected	Detection rate=99%	False positive rate = 1%
Not Detected	False negative rate =1%	True negative = 99%



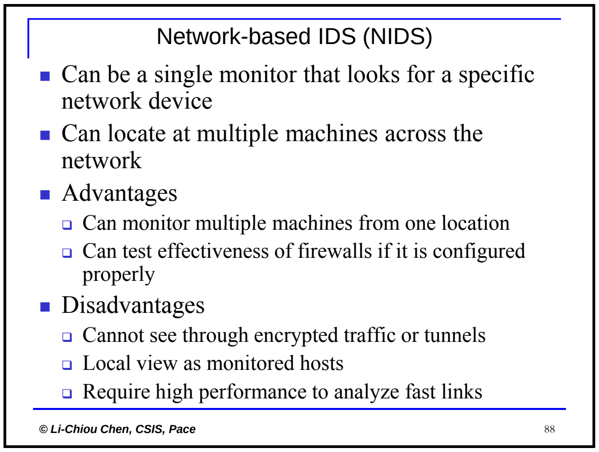
An example: Base-Rate Fallacy of IDS

- IDS false positives and false negatives
  - An IDS can detect 99% of intrusions (false negative = 1%)
  - 1% of non-intrusions generate alarms (false positive = 1%)
- The IDS filters 100,000 events per hour
- When 10 in 100,000 events are really an intrusion; that is, 99990 in 100,000 are non-intrusions
- How many alarms that the systems will generate per hour?
  - The system will generate 999.90 false alarms in 99990 non-intrusion events (99990*1%)
  - The system will generate 9.9 real alarms in 10 intrusion events (10*99%)
  - The system will generate 999.9+9.9 = 1009.8 alarms
- What is the percentage of alarms that are real per hour?
  - only 9.9 in 1009.8 alarms are real, that is, ONLY about 1% of alarms are “real” (9.9/1009.8 ~ 1%)



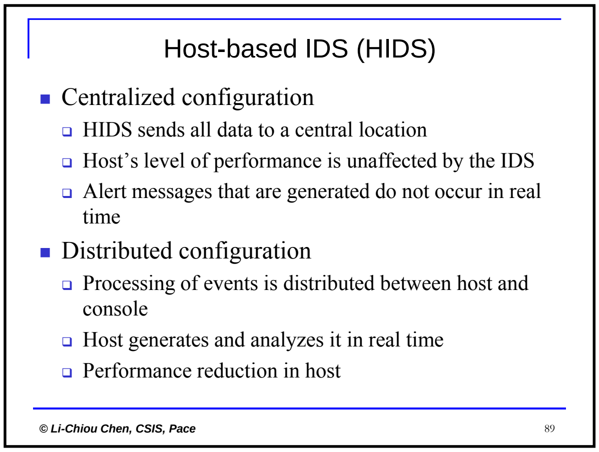
Types of IDS

- Based on data
  - Network-based IDS
    - Monitors and inspects network traffic
  - Host-based IDS
    - Runs on a single host
- Based on detection techniques
  - Signature-based IDS
    - Uses pattern matching to identify known attacks
  - Anomaly-based IDS
    - Uses statistical, data mining or other techniques to distinguish normal from abnormal activities



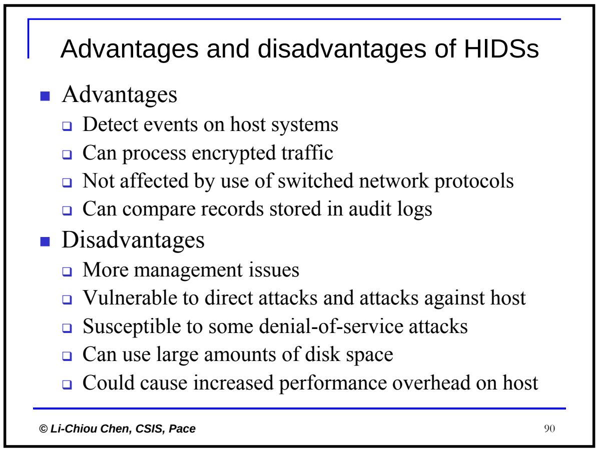
Network-based IDS (NIDS)

- Can be a single monitor that looks for a specific network device
- Can locate at multiple machines across the network
- Advantages
  - Can monitor multiple machines from one location
  - Can test effectiveness of firewalls if it is configured properly
- Disadvantages
  - Cannot see through encrypted traffic or tunnels
  - Local view as monitored hosts
  - Require high performance to analyze fast links



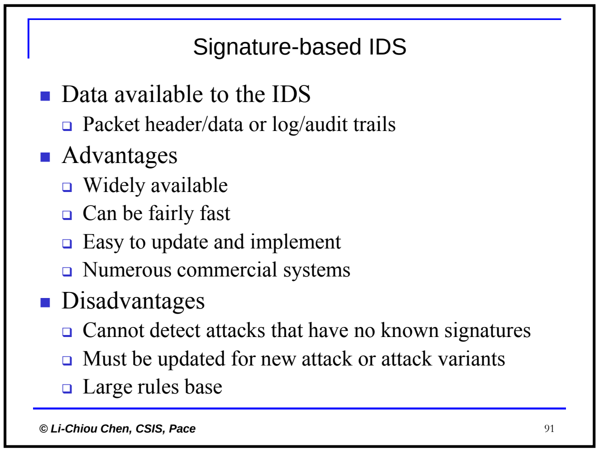
Host-based IDS (HIDS)

- Centralized configuration
  - HIDS sends all data to a central location
  - Host’s level of performance is unaffected by the IDS
  - Alert messages that are generated do not occur in real time
- Distributed configuration
  - Processing of events is distributed between host and console
  - Host generates and analyzes it in real time
  - Performance reduction in host



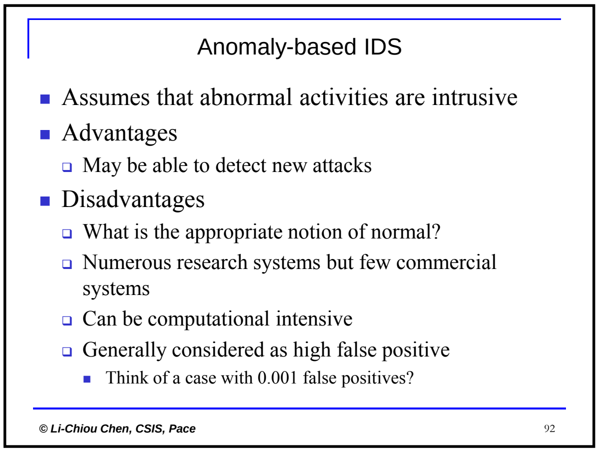
Advantages and disadvantages of HIDSs

- Advantages
  - Detect events on host systems
  - Can process encrypted traffic
  - Not affected by use of switched network protocols
  - Can compare records stored in audit logs
- Disadvantages
  - More management issues
  - Vulnerable to direct attacks and attacks against host
  - Susceptible to some denial-of-service attacks
  - Can use large amounts of disk space
  - Could cause increased performance overhead on host



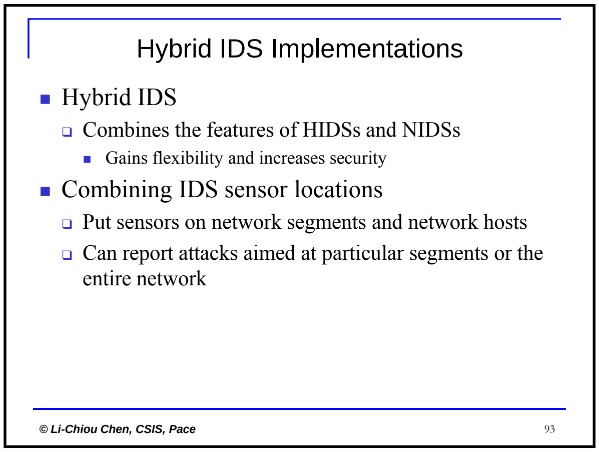
Signature-based IDS

- Data available to the IDS
  - Packet header/data or log/audit trails
- Advantages
  - Widely available
  - Can be fairly fast
  - Easy to update and implement
  - Numerous commercial systems
- Disadvantages
  - Cannot detect attacks that have no known signatures
  - Must be updated for new attack or attack variants
  - Large rules base



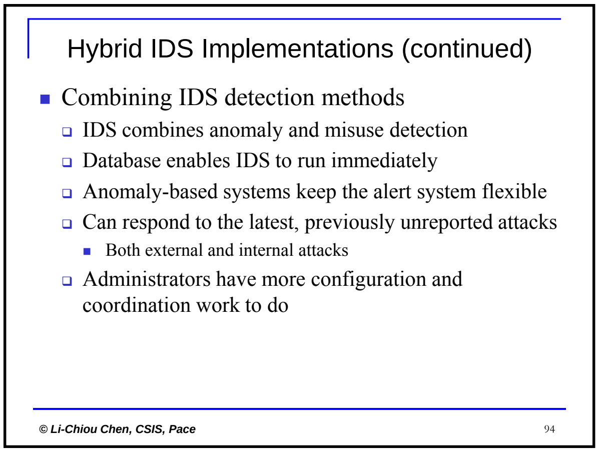
Anomaly-based IDS

- Assumes that abnormal activities are intrusive
- Advantages
  - May be able to detect new attacks
- Disadvantages
  - What is the appropriate notion of normal?
  - Numerous research systems but few commercial systems
  - Can be computational intensive
  - Generally considered as high false positive
    - Think of a case with 0.001 false positives?



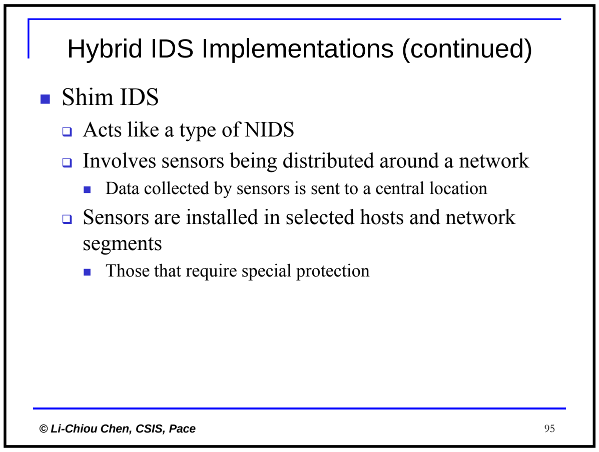
Hybrid IDS Implementations

- Hybrid IDS
  - Combines the features of HIDSs and NIDSs
    - Gains flexibility and increases security
- Combining IDS sensor locations
  - Put sensors on network segments and network hosts
  - Can report attacks aimed at particular segments or the entire network



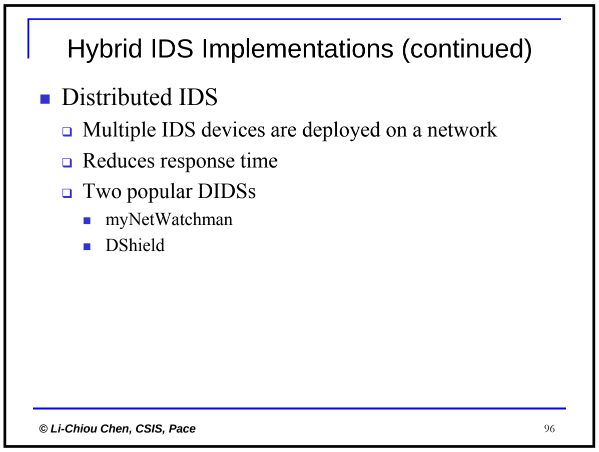
Hybrid IDS Implementations (continued)

- Combining IDS detection methods
  - IDS combines anomaly and misuse detection
  - Database enables IDS to run immediately
  - Anomaly-based systems keep the alert system flexible
  - Can respond to the latest, previously unreported attacks
    - Both external and internal attacks
  - Administrators have more configuration and coordination work to do



Hybrid IDS Implementations (continued)

- Shim IDS
  - Acts like a type of NIDS
  - Involves sensors being distributed around a network
    - Data collected by sensors is sent to a central location
  - Sensors are installed in selected hosts and network segments
    - Those that require special protection



Hybrid IDS Implementations (continued)

- Distributed IDS
  - Multiple IDS devices are deployed on a network
  - Reduces response time
  - Two popular DIDSs
    - myNetWatchman
    - DShield

Hybrid IDS Implementations (continued)

- Advantages
  - Combine aspects of NIDS and HIDS configurations
  - Can monitor network as a whole
  - Can monitor attacks that reach individual hosts
- Disadvantages
  - Need to get disparate systems to work in coordinate fashion
  - Data gathered by multiple systems can be difficult to absorb and analyze

Evaluating Intrusion Detection Systems

- Survey various options and match them to your needs
- Review topology of your network identifying
  - Number of entry points
  - Use of firewalls
  - Number of network segments
- Evaluating IDSs can be time consuming

IDS Hardware Appliances

- Can handle more network traffic
  - Have better scalability than software IDSs
- Plug-and-play capabilities
  - One of its major advantages
  - Do not need to be configured to work with a particular OS
- You should create a custom configuration
  - To reduce the number of false positives and false negatives
- Upgrade appliances periodically
  - Can be complicated and expensive
- Examples
  - iForce, Intrusion SecureNet, StealthWatch G1

Agenda

- Intrusion Detection Systems (IDS) basics
  - IDS components
  - Steps of intrusion detection
  - Options for implementing IDS
  - Evaluate different types of IDS products
- IDS configuration
  - Configure an IDS and develop filter rules
  - False alarms
  - Options for dealing with legitimate security alerts
- Lab #5

Developing IDS Filter Rules

- IDS effectiveness depends on its database
  - Database should be complete and up to date
- IDS can have its own set of rules
  - You can edit it in response to scans and attacks
- IDS can be used proactively
  - Block attacks
  - Move from intrusion detection to intrusion prevention

Rule Actions

- IDS has a passive and reactive nature
- Configure IDS to take actions
  - Other than simply triggering alarms
  - Provides another layer of network defense
- IDSs include documentation for writing rules
- Customized rules can increase false positives during the learning process
  - Test your rules before using them in a real system

Rule Data

- Specify the action you want Snort to perform
- Specify the rest of the data that applies to the rule
  - Protocol
  - Source and destination IP addresses
  - Port number
  - Direction

Filtering Alerts

- To reduce false alarms adjust rules used by
  - Firewalls
  - Packet filters
  - IDSs
- Exclude specific signature from connecting to a selected IP address
  - Both internal and external addresses
  - Can even exclude an entire subnet or network

Dealing with Legitimate Security Alerts

- Determine whether the attack is a false alarm
  - Look for indications such as
    - You notice system crashes
    - New user accounts suddenly appear on the network
    - Sporadic user accounts suddenly have heavy activity
    - New files appear, often with strange file names
    - A series of unsuccessful logon attempts occurs
- Respond calmly and follow established procedures
- Call law enforcement personnel if necessary
  - To handle the intrusion

Assessing the Impact

- Was any host on your network compromised
- Determine the extend of the damage
- Determine the scope and impact of the problem
- Determine if the firewall was compromised
  - If firewall was compromised, computers on network could be accessed
  - Reconstruct firewall from scratch

Developing an Action Plan

- Action plan might involve the following steps:
  - Assess seriousness of the attack
  - Notify team leader immediately
  - Begin to document all actions
  - Contain the threat
  - Determine the extend of the damage
  - Make a complete bit-stream backup of the media
    - If you plan to prosecute
  - Eradicate the problem
  - Restore the system
  - Record a summary of the incident

Handling Internal Versus External Incidents

- Intrusions and security breaches often originate from inside an organization
- Your response needs to be more measured
- Avoid notifying the entire staff
- Human Resources and Legal departments should be made aware of the problem
- Notify the entire staff only when they need to know something serious happened

Taking Corrective Measures to Prevent Reoccurrences

- Take steps to prevent intrusions from recurring
- Set up intrusion rules that send alarms when the same intrusions are detected
- Notify others on the Internet about your attack

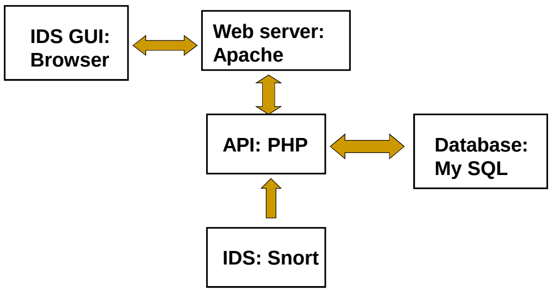
Gathering Data for Prosecution

- Rules to handle evidence
  - Make sure two people handle the data at all times
  - Write everything down
  - Lock it up!
- Chain of custody
  - Record of who handled an object to be used as evidence in court
  - Decide SIRT members that will handle the evidence
- Before an incident occurs, decide whether you will prosecute or not
  - Include this in your security policy

Steps for handling and examining hard disks and other computer data

- Secure the area
- Prepare the system
- Examine the system
- Shut down the system
- Secure the system
- Prepare the system for acquisition
- Examine the system
- Connect target media
- Secure evidence

BASE: a web GUI for Snort alerts



References

- Randy Weaver (2006). “Guide to Network Defense and Countermeasures,” Second Edition, Thomson Course Technology. ISBN: 1418836796.
- William Stallings and Lawrie Brown (2008). “Computer Security: Principles and Practice,” Prentice Hall. ISBN: 0106004245.
- Raymond R. Panko, Corporate Computer and Network Security, 2nd Edition, 2009, Pearson/Prentice Hall, ISBN: 0-13-185475-5.
- ISACA CISA Exam review Manual, ISACA