

CS549:
Cryptography and Network
Security

© by Xiang-Yang Li

Department of Computer Science,
IIT

Notice©

This lecture note (Cryptography and Network Security) is prepared by Xiang-Yang Li. This lecture note has benefited from numerous textbooks and online materials. Especially the "Cryptography and Network Security" 2nd edition by William Stallings and the "Cryptography: Theory and Practice" by Douglas Stinson.

You may not modify, publish, or sell, reproduce, create derivative works from, distribute, perform, display, or in any way exploit any of the content, in whole or in part, except as otherwise expressly permitted by the author.

The author has used his best efforts in preparing this lecture note. The author makes no warranty of any kind, expressed or implied, with regard to the programs, protocols contained in this lecture note. The author shall not be liable in any event for incidental or consequential damages in connection with, or arising out of, the furnishing, performance, or use of these.

Cryptography & Network Security

IPsec

XiangYang Li

IP Security

If a secret piece of news is divulged by a spy before the time is ripe, he must be put to death, together with the man to whom the secret was told.

– *The Art of War*, Sun Tzu

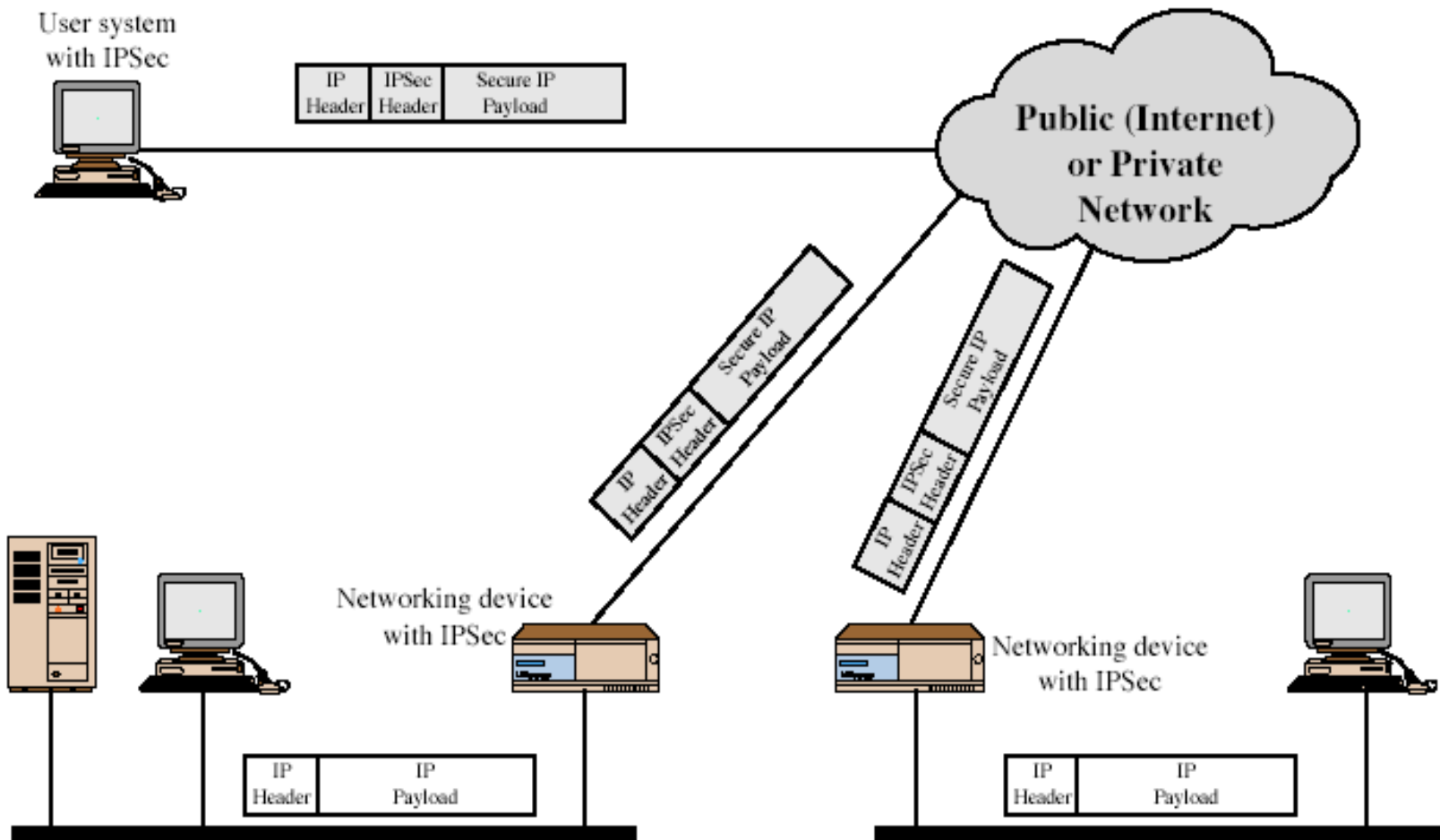
IP Security

- have considered some application specific security mechanisms
 - eg. S/MIME, PGP, Kerberos, SSL/HTTPS
- however there are security concerns that cut across protocol layers
- would like security implemented by the network for all applications

IPSec

- general IP Security mechanisms
- provides
 - authentication
 - confidentiality
 - key management
- applicable to use over LANs, across public & private WANs, & for the Internet

IPSec Uses



Benefits of IPSec

- in a firewall/router provides strong security to all traffic crossing the perimeter
- is resistant to bypass
- is below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users if desired

IP Security Architecture

- specification is quite complex
- defined in numerous RFC's
 - incl. RFC 2401/2402/2406/2408
 - many others, grouped by category
- mandatory in IPv6, optional in IPv4

IPSec Services

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
 - a form of partial sequence integrity
- Confidentiality (encryption)
- Limited traffic flow confidentiality

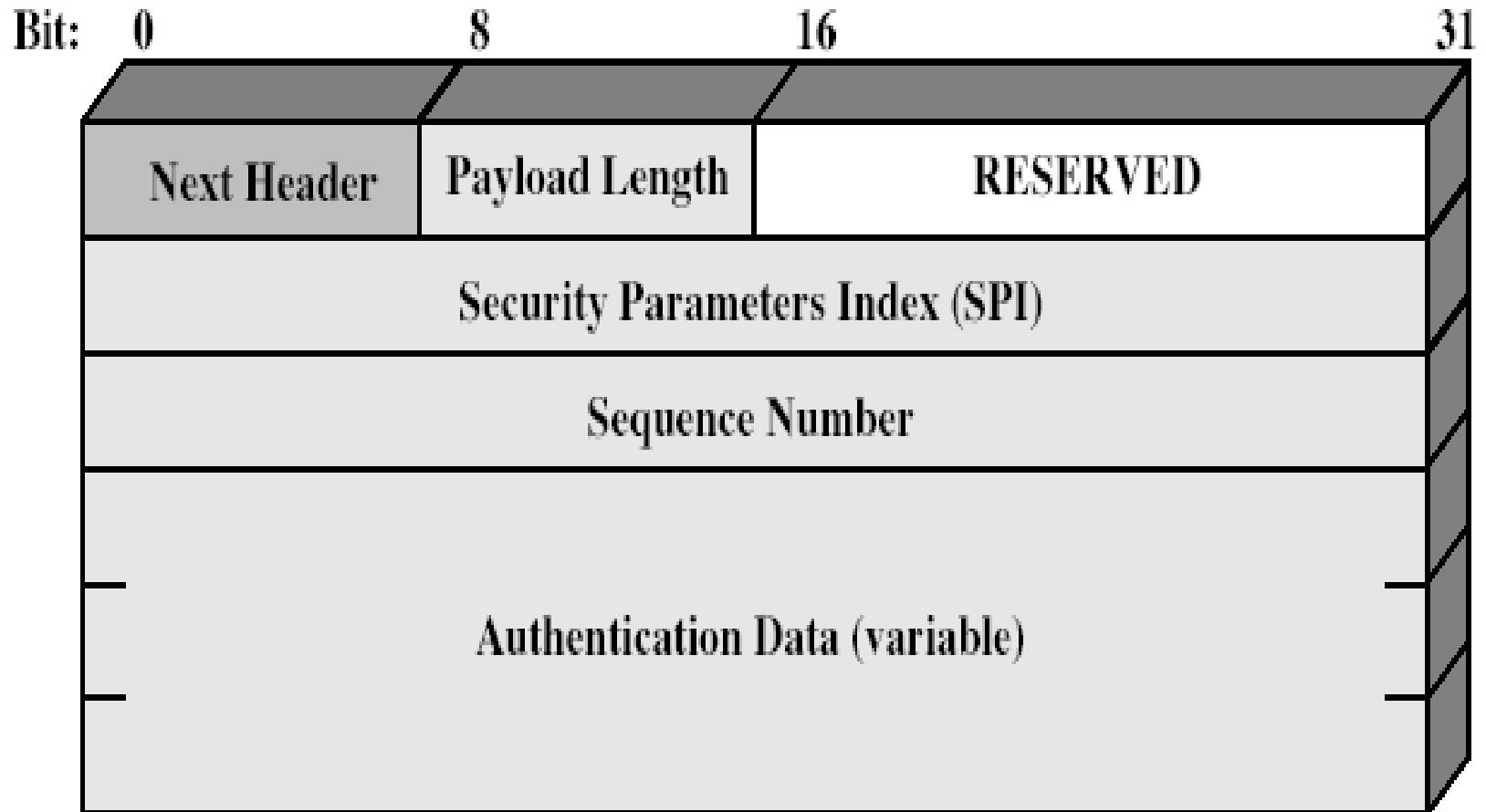
Security Associations

- a one-way relationship between sender & receiver that affords security for traffic flow
- defined by 3 parameters:
 - Security Parameters Index (SPI)
 - IP Destination Address
 - Security Protocol Identifier
- has a number of other parameters
 - seq no, AH & EH info, lifetime etc
- have a database of Security Associations

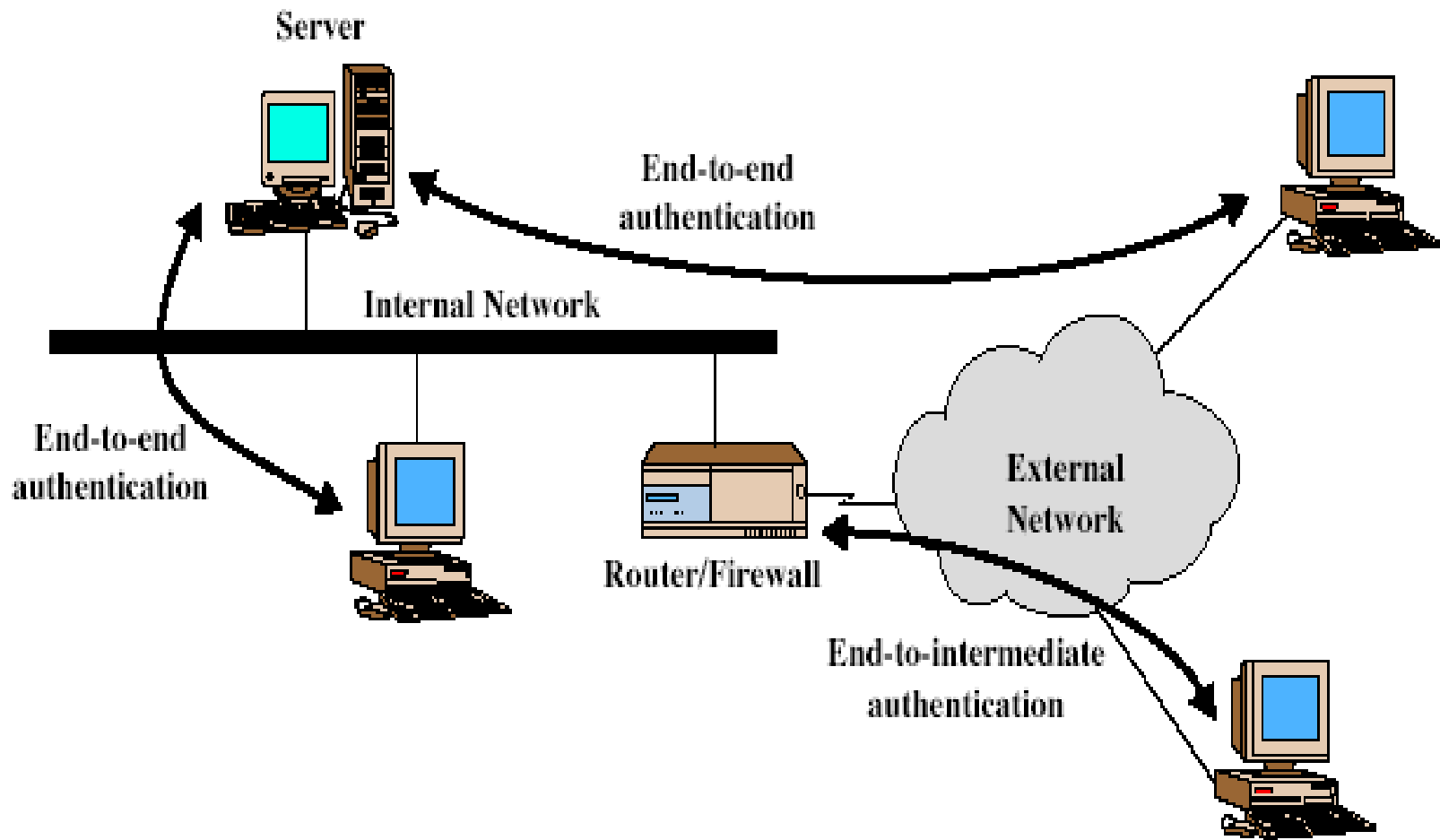
Authentication Header (AH)

- provides support for data integrity & authentication of IP packets
 - end system/router can authenticate user/app
 - prevents address spoofing attacks by tracking sequence numbers
- based on use of a *MAC*
 - HMAC-MD5-96 or HMAC-SHA-1-96
- parties must share a secret key

Authentication Header



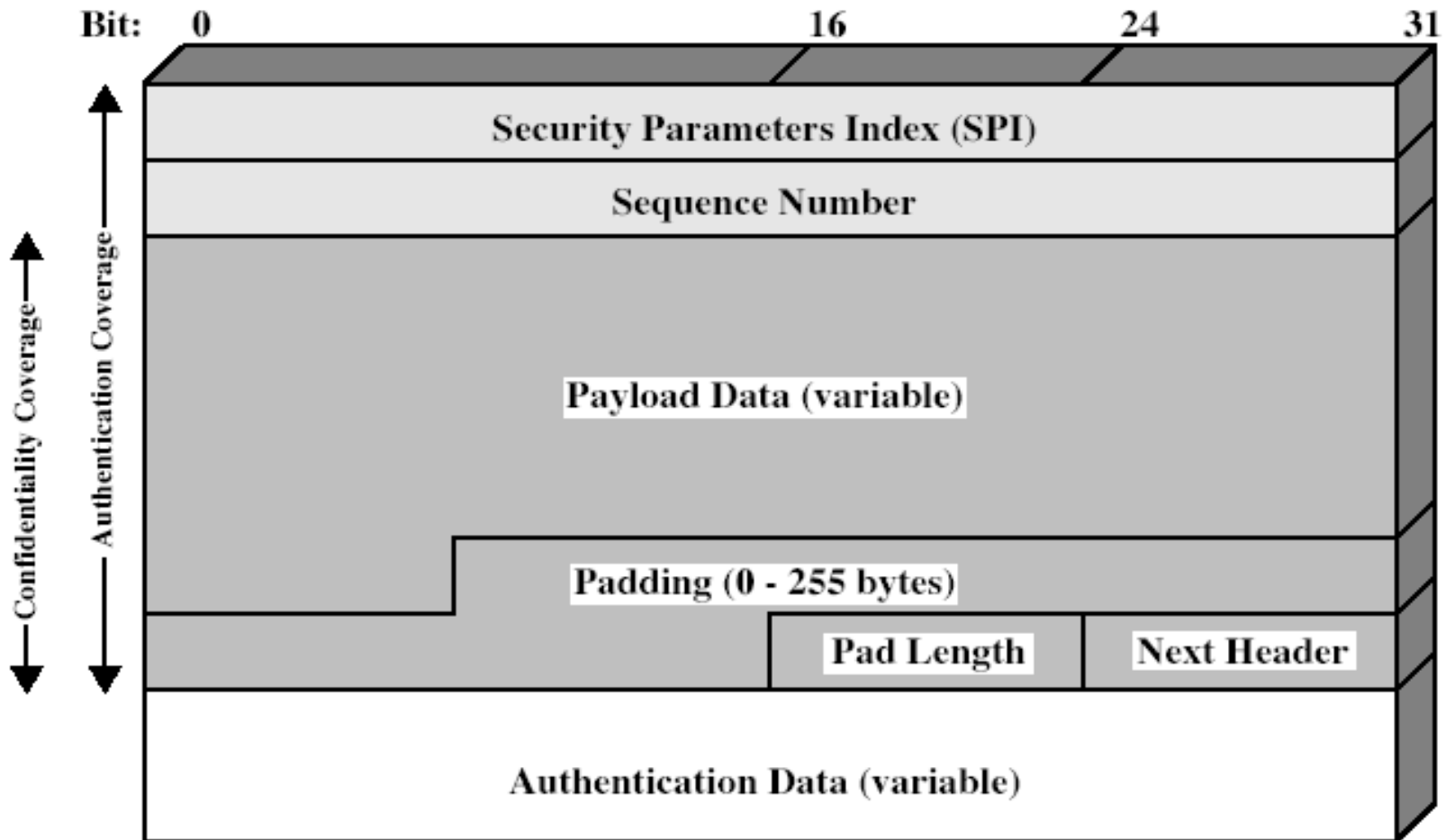
Transport & Tunnel Modes



Encapsulating Security Payload (ESP)

- provides message content confidentiality & limited traffic flow confidentiality
- can optionally provide the same authentication services as AH
- supports range of ciphers, modes, padding
 - incl. DES, Triple-DES, RC5, IDEA, CAST etc
 - CBC most common
 - pad to meet blocksize, for traffic flow

Encapsulating Security Payload



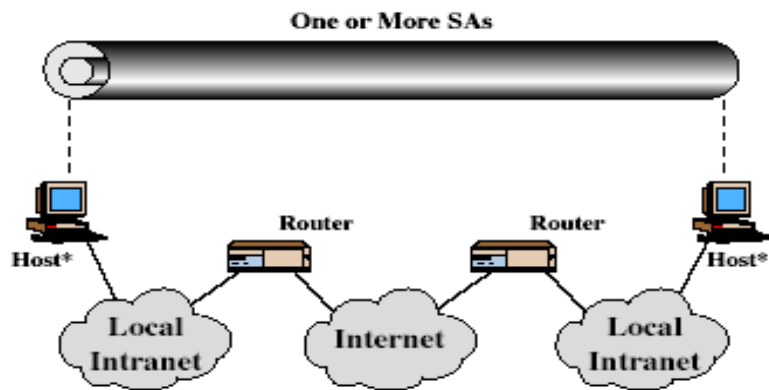
Transport vs Tunnel Mode ESP

- transport mode is used to encrypt & optionally authenticate IP data
 - data protected but header left in clear
 - can do traffic analysis but is efficient
 - good for ESP host to host traffic
- tunnel mode encrypts entire IP packet
 - add new header for next hop
 - good for VPNs, gateway to gateway security

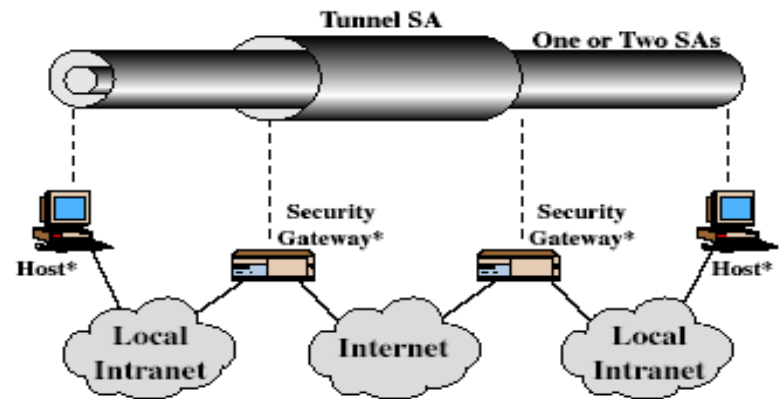
Combining Security Associations

- SA's can implement either AH or ESP
- to implement both need to combine SA's
 - form a security bundle
- have 4 cases (see next)

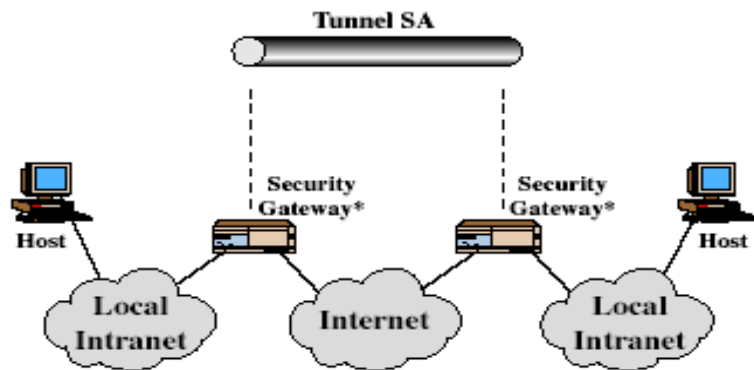
Combining Security Associations



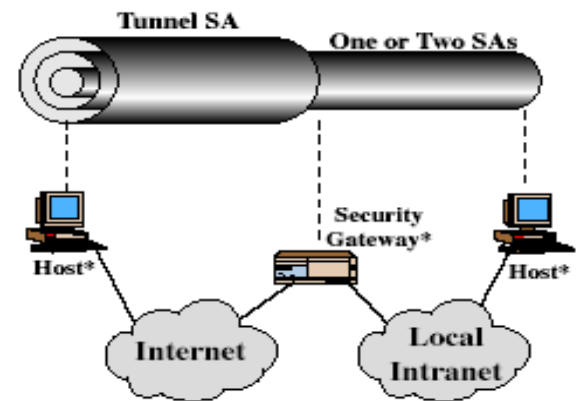
(a) Case 1



(c) Case 3



(b) Case 2



(d) Case 4

Key Management

- handles key generation & distribution
- typically need 2 pairs of keys
 - 2 per direction for AH & ESP
- manual key management
 - sysadmin manually configures every system
- automated key management
 - automated system for on demand creation of keys for SA's in large systems
 - has Oakley & ISAKMP elements

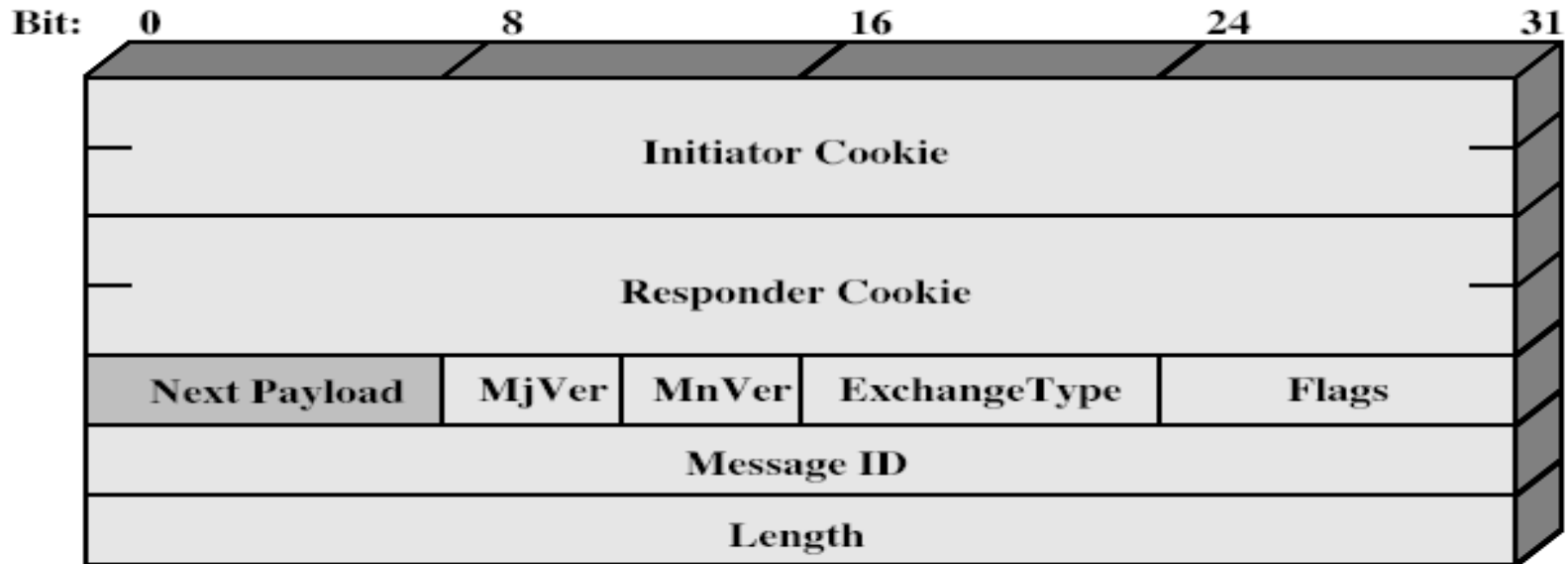
Oakley

- a key exchange protocol
- based on Diffie-Hellman key exchange
- adds features to address weaknesses
 - cookies, groups (global params), nonces, DH key exchange with authentication
- can use arithmetic in prime fields or elliptic curve fields

ISAKMP

- Internet Security Association and Key Management Protocol
- provides framework for key management
- defines procedures and packet formats to establish, negotiate, modify, & delete SAs
- independent of key exchange protocol, encryption alg, & authentication method

ISAKMP



(a) ISAKMP Header



(b) Generic Payload Header

Summary

- have considered:
 - IPSec security framework
 - AH
 - ESP
 - key management & Oakley/ISAKMP

Cryptography & Network Security

Firewalls

XiangYang Li

Firewalls

The function of a strong position is to make the forces holding it practically unassailable
— **On War, Carl Von Clausewitz**

Introduction

- seen evolution of information systems
- now everyone want to be on the Internet
- and to interconnect networks
- has persistent security concerns
 - can't easily secure every system in org
- need "harm minimisation"
- a **Firewall** usually part of this

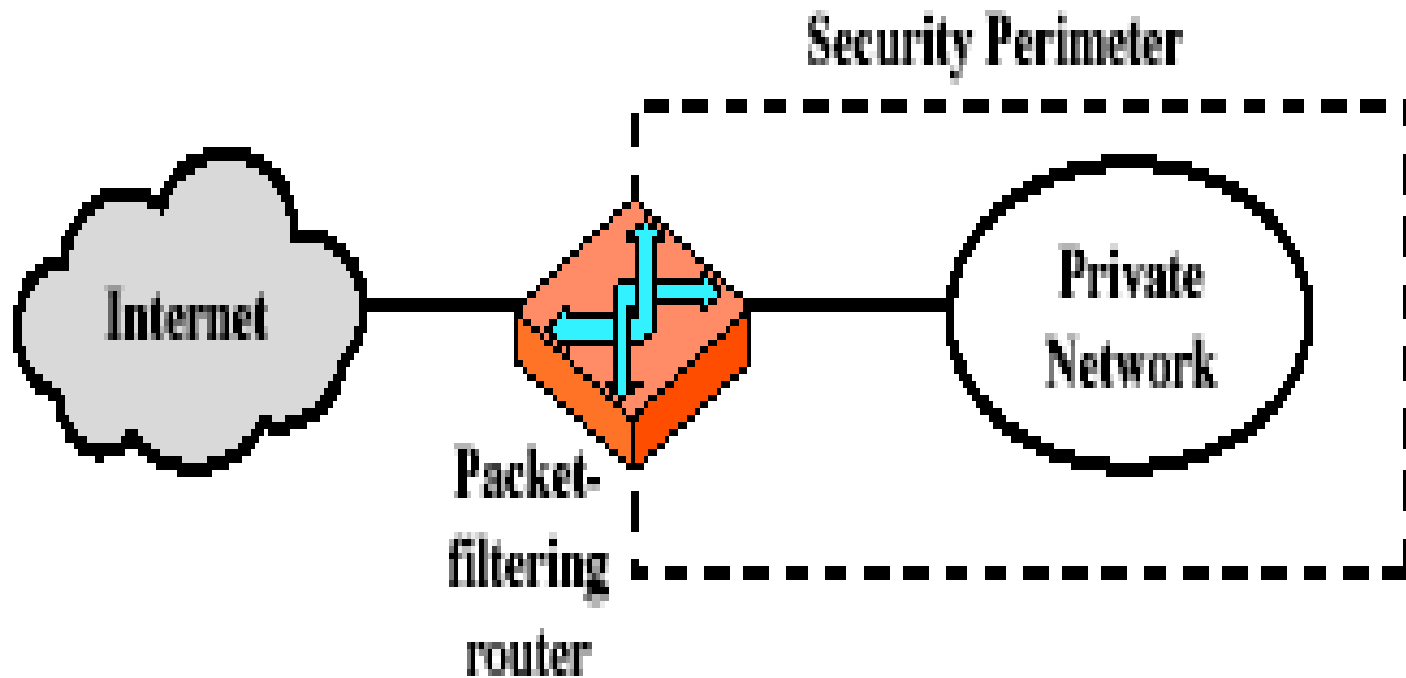
What is a Firewall?

- a **choke point** of control and monitoring
- interconnects networks with differing trust
- imposes restrictions on network services
 - only authorized traffic is allowed
- auditing and controlling access
 - can implement alarms for abnormal behavior
- is itself immune to penetration
- provides **perimeter defence**

Firewall Limitations

- cannot protect from attacks bypassing it
 - eg sneaker net, utility modems, trusted organisations, trusted services (eg SSL/SSH)
- cannot protect against internal threats
 - eg disgruntled employee
- cannot protect against transfer of all virus infected programs or files
 - because of huge range of O/S & file types

Firewalls - Packet Filters



(a) Packet-filtering router

Firewalls - Packet Filters

- simplest of components
- foundation of any firewall system
- examine each IP packet (no context) and permit or deny according to rules
- hence restrict access to services (ports)
- possible default policies
 - that not expressly permitted is prohibited
 - that not expressly prohibited is permitted

Firewalls - Packet Filters

Table 20.1 Packet-Filtering Examples

A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

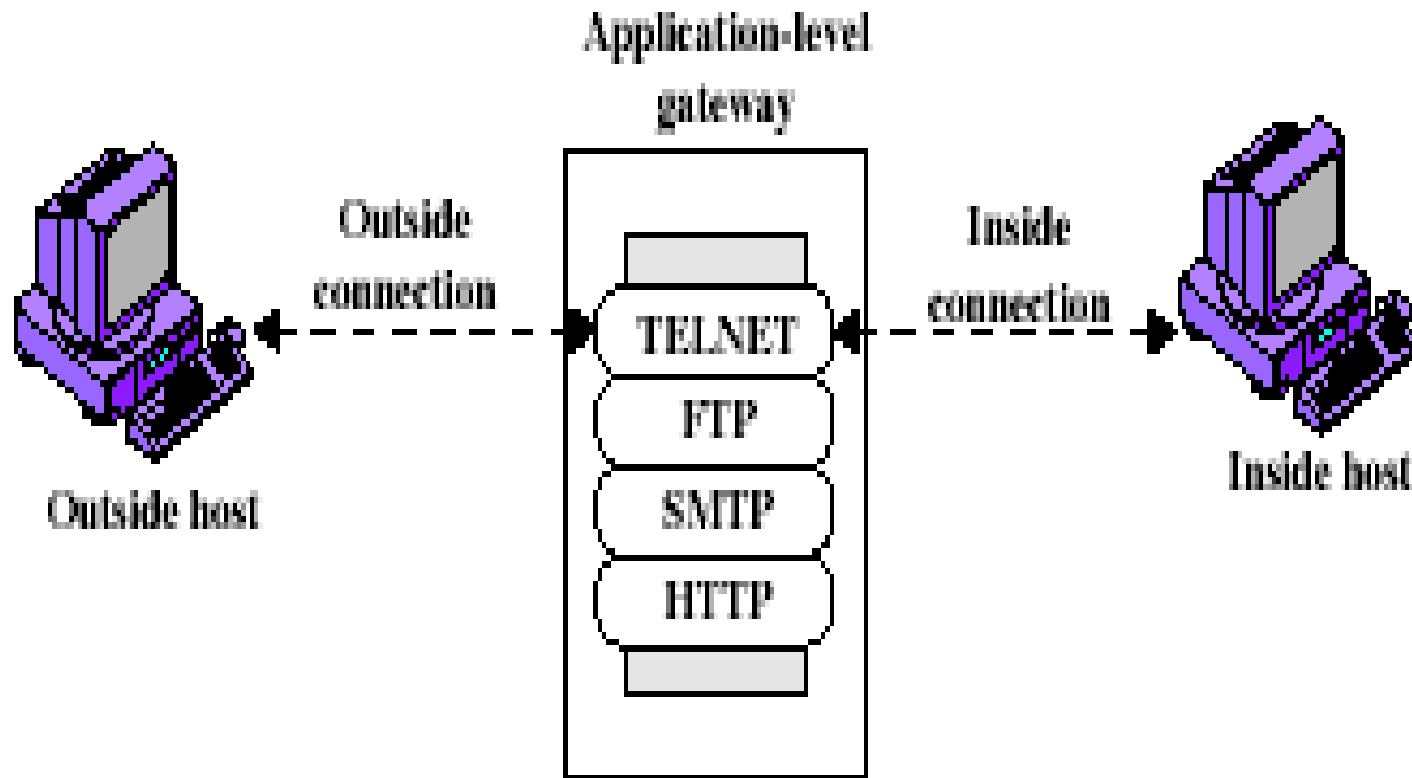
Attacks on Packet Filters

- **IP address spoofing**
 - fake source address to be trusted
 - add filters on router to block
- **source routing attacks**
 - attacker sets a route other than default
 - block source routed packets
- **tiny fragment attacks**
 - split header info over several tiny packets
 - either discard or reassemble before check

Firewalls - Stateful Packet Filters

- examine each IP packet in context
 - keeps tracks of client-server sessions
 - checks each packet validly belongs to one
- better able to detect bogus packets out of context

Firewalls - Application Level Gateway (or Proxy)

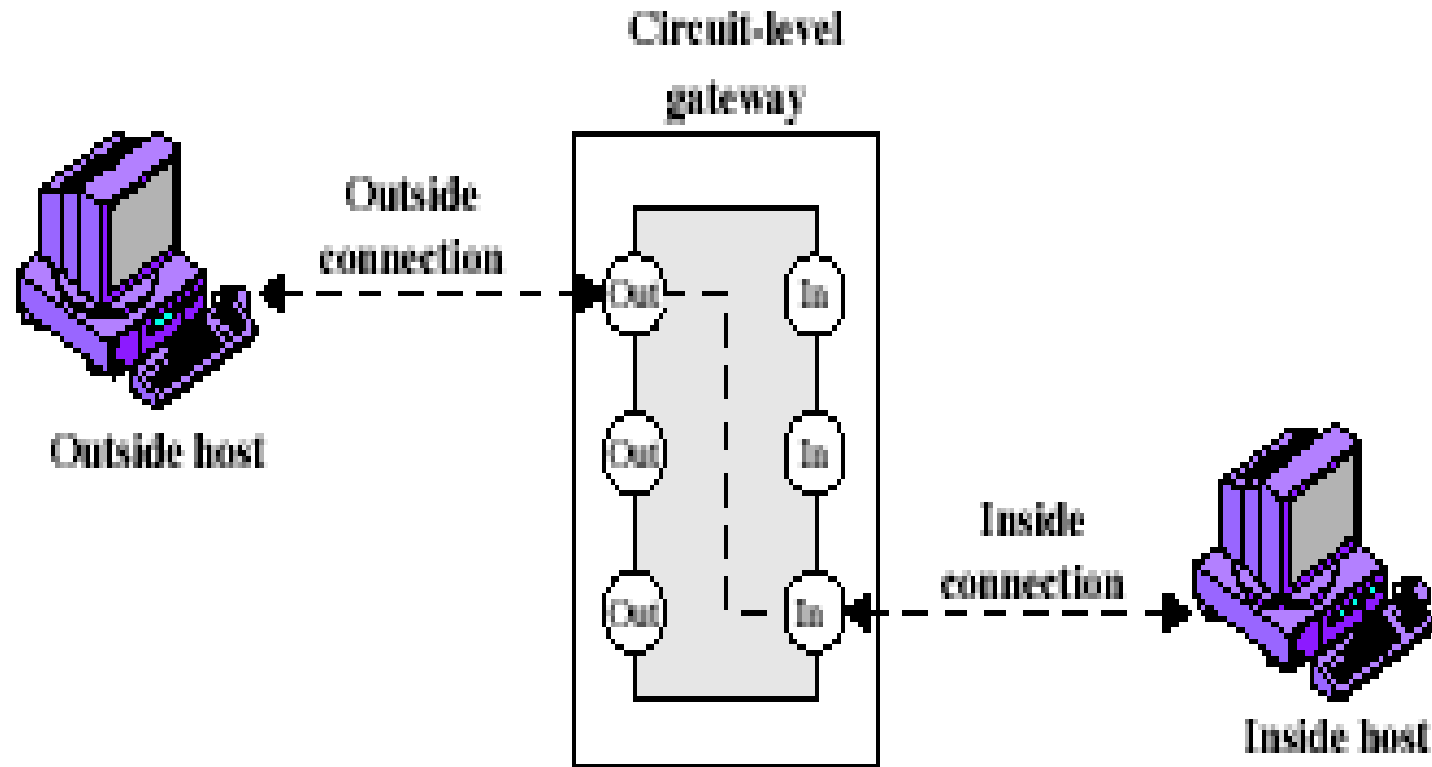


(b) Application-level gateway

Firewalls - Application Level Gateway (or Proxy)

- use an application specific gateway / proxy
- has full access to protocol
 - user requests service from proxy
 - proxy validates request as legal
 - then actions request and returns result to user
- need separate proxies for each service
 - some services naturally support proxying
 - others are more problematic
 - custom services generally not supported

Firewalls - Circuit Level Gateway



(c) Circuit-level gateway

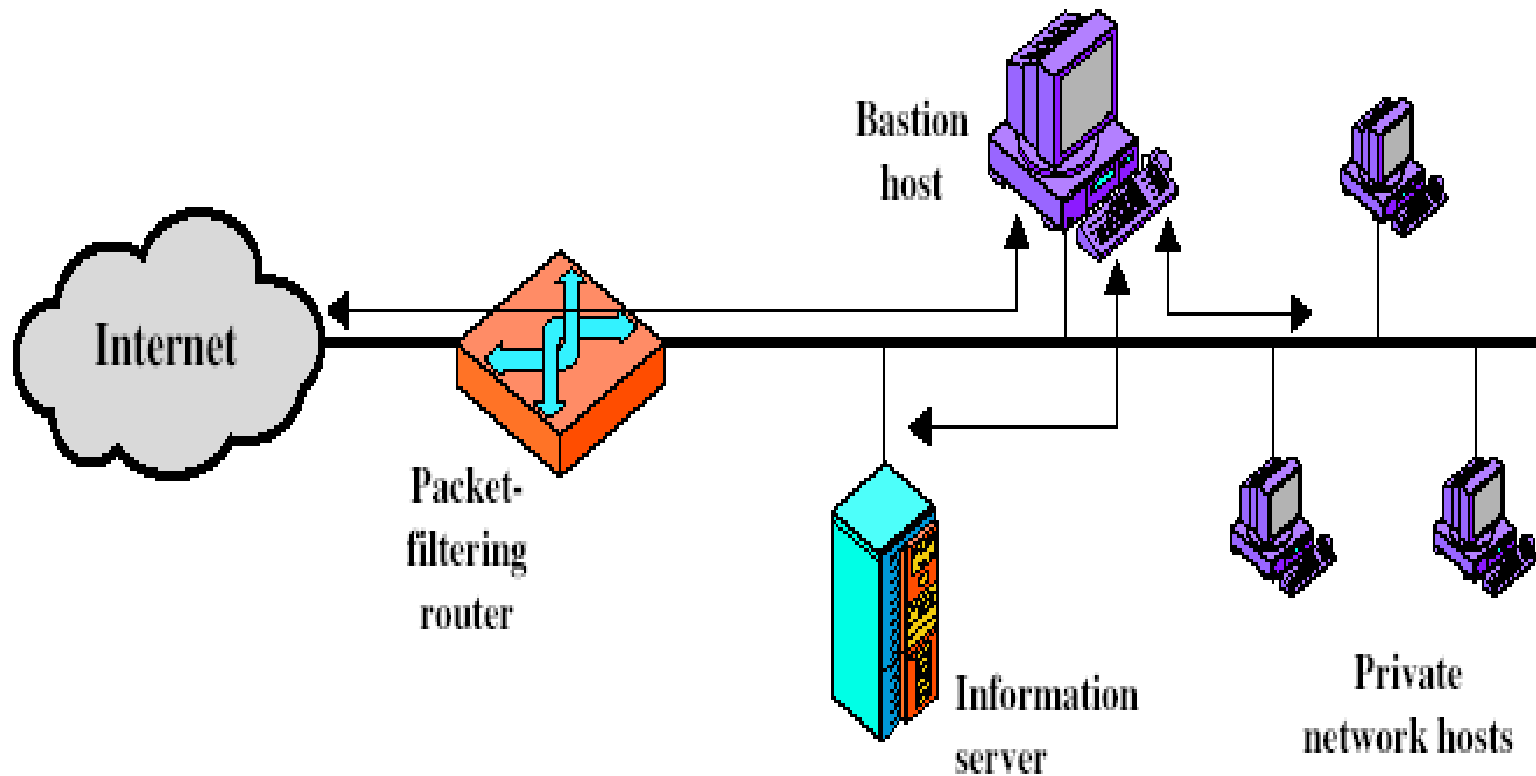
Firewalls - Circuit Level Gateway

- relays two TCP connections
- imposes security by limiting which such connections are allowed
- once created usually relays traffic without examining contents
- typically used when trust internal users by allowing general outbound connections
- SOCKS commonly used for this

Bastion Host

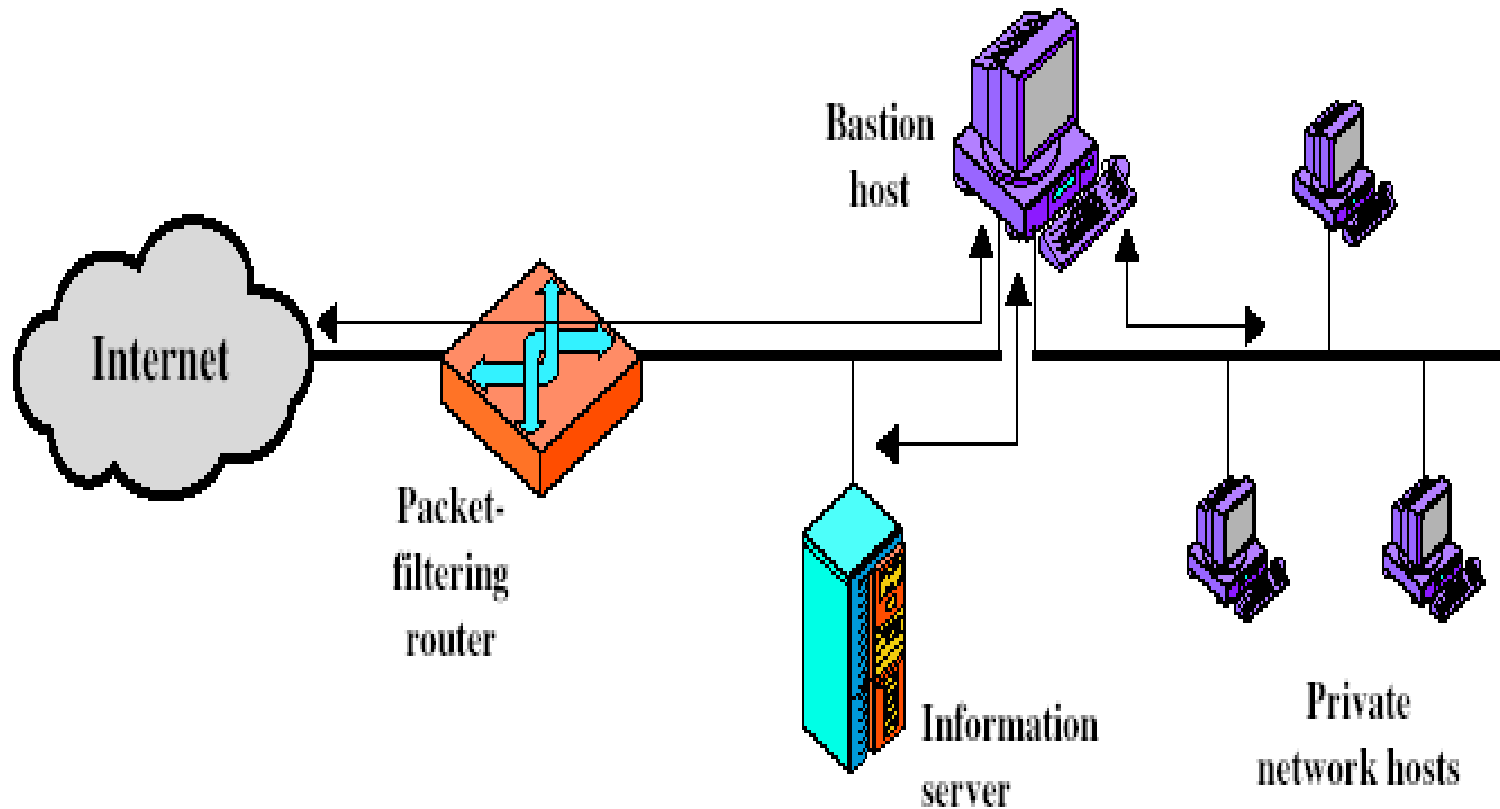
- highly secure host system
- potentially exposed to "hostile" elements
- hence is secured to withstand this
- may support 2 or more net connections
- may be trusted to enforce trusted separation between network connections
- runs circuit / application level gateways
- or provides externally accessible services

Firewall Configurations



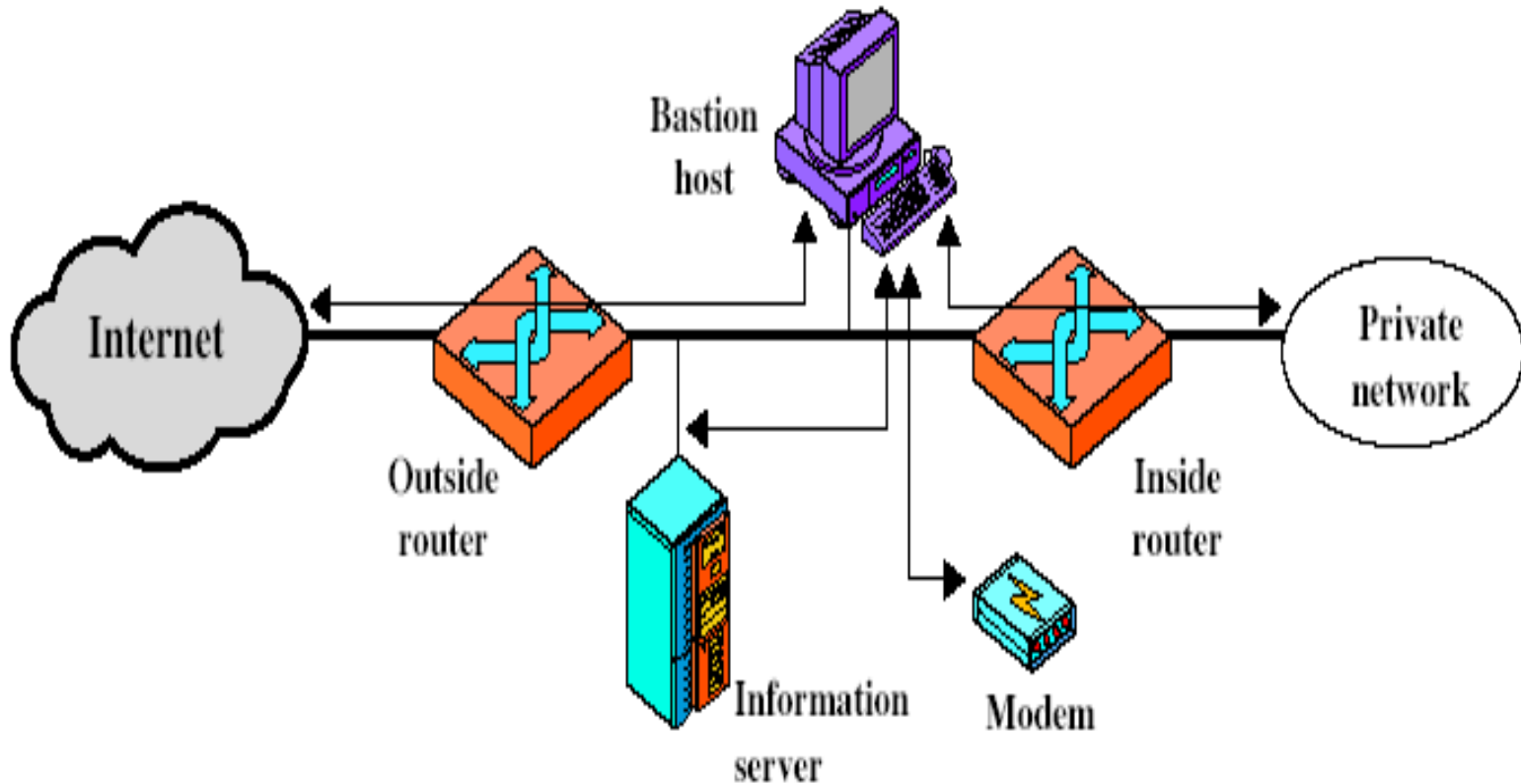
(a) Screened host firewall system (single-homed bastion host)

Firewall Configurations



(b) Screened host firewall system (dual-homed bastion host)

Firewall Configurations



(c) Screened-subnet firewall system

Access Control

- given system has identified a user
- determine what resources they can access
- general model is that of access matrix with
 - **subject** - active entity (user, process)
 - **object** - passive entity (file or resource)
 - **access right** – way object can be accessed
- can decompose by
 - columns as access control lists
 - rows as capability tickets

Access Control Matrix

	Program1	...	SegmentA	SegmentB
Process1	Read Execute		Read Write	
Process2				Read
•				
•				
•				

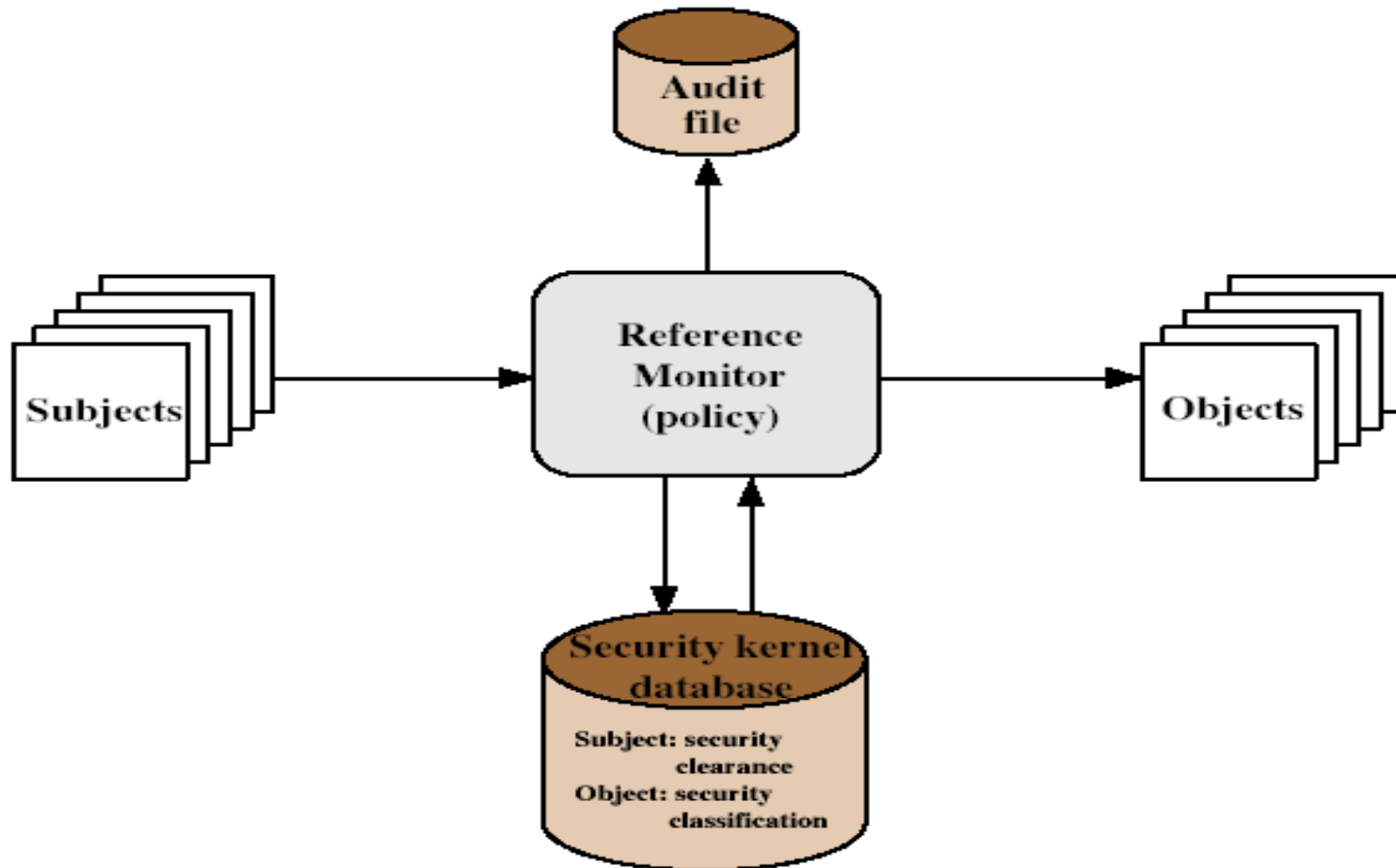
Trusted Computer Systems

- information security is increasingly important
- have varying degrees of sensitivity of information
 - cf military info classifications: confidential, secret etc
- subjects (people or programs) have varying rights of access to objects (information)
- want to consider ways of increasing confidence in systems to enforce these rights
- known as multilevel security
 - subjects have **maximum** & **current** security level
 - objects have a fixed security level **classification**

Bell LaPadula (BLP) Model

- one of the most famous security models
- implemented as mandatory policies on system
- has two key policies:
- **no read up (simple security property)**
 - a subject can only read/write an object if the current security level of the subject dominates (\geq) the classification of the object
- **no write down (*-property)**
 - a subject can only append/write to an object if the current security level of the subject is dominated by (\leq) the classification of the object

Reference Monitor



Evaluated Computer Systems

- governments can evaluate IT systems
- against a range of standards:
 - TCSEC, IPSEC and now Common Criteria
- define a number of "levels" of evaluation with increasingly stringent checking
- have published lists of evaluated products
 - though aimed at government/defense use
 - can be useful in industry also

Summary

- have considered:
 - firewalls
 - types of firewalls
 - configurations
 - access control
 - trusted systems

Cryptography and Network Security

Third Edition
by William Stallings

Lecture slides by Lawrie Brown

Intruders

They agreed that Graham should set the test for Charles Mabledene. It was neither more nor less than that Dragon should get Stern's code. If he had the 'in' at Utting which he claimed to have this should be possible, only loyalty to Moscow Centre would prevent it. If he got the key to the code he would prove his loyalty to London Central beyond a doubt.

— Talking to Strange Men, Ruth Rendell

Intruders

- significant issue for networked systems is hostile or unwanted access
- either via network or local
- can identify classes of intruders:
 - masquerader
 - misfeasor
 - clandestine user
- varying levels of competence

Intruders

- clearly a growing publicized problem
 - from “Wily Hacker” in 1986/87
 - to clearly escalating CERT stats
- may seem benign, but still cost resources
- may use compromised system to launch other attacks

Intrusion Techniques

- aim to increase privileges on system
- basic attack methodology
 - target acquisition and information gathering
 - initial access
 - privilege escalation
 - covering tracks
- key goal often is to acquire passwords
- so then exercise access rights of owner

Password Guessing

- one of the most common attacks
- attacker knows a login (from email/web page etc)
- then attempts to guess password for it
 - try default passwords shipped with systems
 - try all short passwords
 - then try by searching dictionaries of common words
 - intelligent searches try passwords associated with the user (variations on names, birthday, phone, common words/interests)
 - before exhaustively searching all possible passwords
- check by login attempt or against stolen password file
- success depends on password chosen by user
- surveys show many users choose poorly

Password Capture

- **another attack involves password capture**
 - watching over shoulder as password is entered
 - using a trojan horse program to collect
 - monitoring an insecure network login (eg. telnet, FTP, web, email)
 - extracting recorded info after successful login (web history/cache, last number dialed etc)
- **using valid login/password can impersonate user**
- **users need to be educated to use suitable precautions/countermeasures**

Intrusion Detection

- inevitably will have security failures
- so need also to detect intrusions so can
 - block if detected quickly
 - act as deterrent
 - collect info to improve security
- assume intruder will behave differently to a legitimate user
 - but will have imperfect distinction between

Approaches to Intrusion Detection

- statistical anomaly detection
 - threshold
 - profile based
- rule-based detection
 - anomaly
 - penetration identification

Audit Records

- fundamental tool for intrusion detection
- native audit records
 - part of all common multi-user O/S
 - already present for use
 - may not have info wanted in desired form
- detection-specific audit records
 - created specifically to collect wanted info
 - at cost of additional overhead on system

Statistical Anomaly Detection

- **threshold detection**
 - count occurrences of specific event over time
 - if exceed reasonable value assume intrusion
 - alone is a crude & ineffective detector
- **profile based**
 - characterize past behavior of users
 - detect significant deviations from this
 - profile usually multi-parameter

Audit Record Analysis

- foundation of statistical approaches
- analyze records to get metrics over time
 - counter, gauge, interval timer, resource use
- use various tests on these to determine if current behavior is acceptable
 - mean & standard deviation, multivariate, markov process, time series, operational
- key advantage is no prior knowledge used

Rule-Based Intrusion Detection

- observe events on system & apply rules to decide if activity is suspicious or not
- rule-based anomaly detection
 - analyze historical audit records to identify usage patterns & auto-generate rules for them
 - then observe current behavior & match against rules to see if conforms
 - like statistical anomaly detection does not require prior knowledge of security flaws

Rule-Based Intrusion Detection

- rule-based penetration identification
 - uses expert systems technology
 - with rules identifying known penetration, weakness patterns, or suspicious behavior
 - rules usually machine & O/S specific
 - rules are generated by experts who interview & codify knowledge of security admins
 - quality depends on how well this is done
 - compare audit records or states against rules

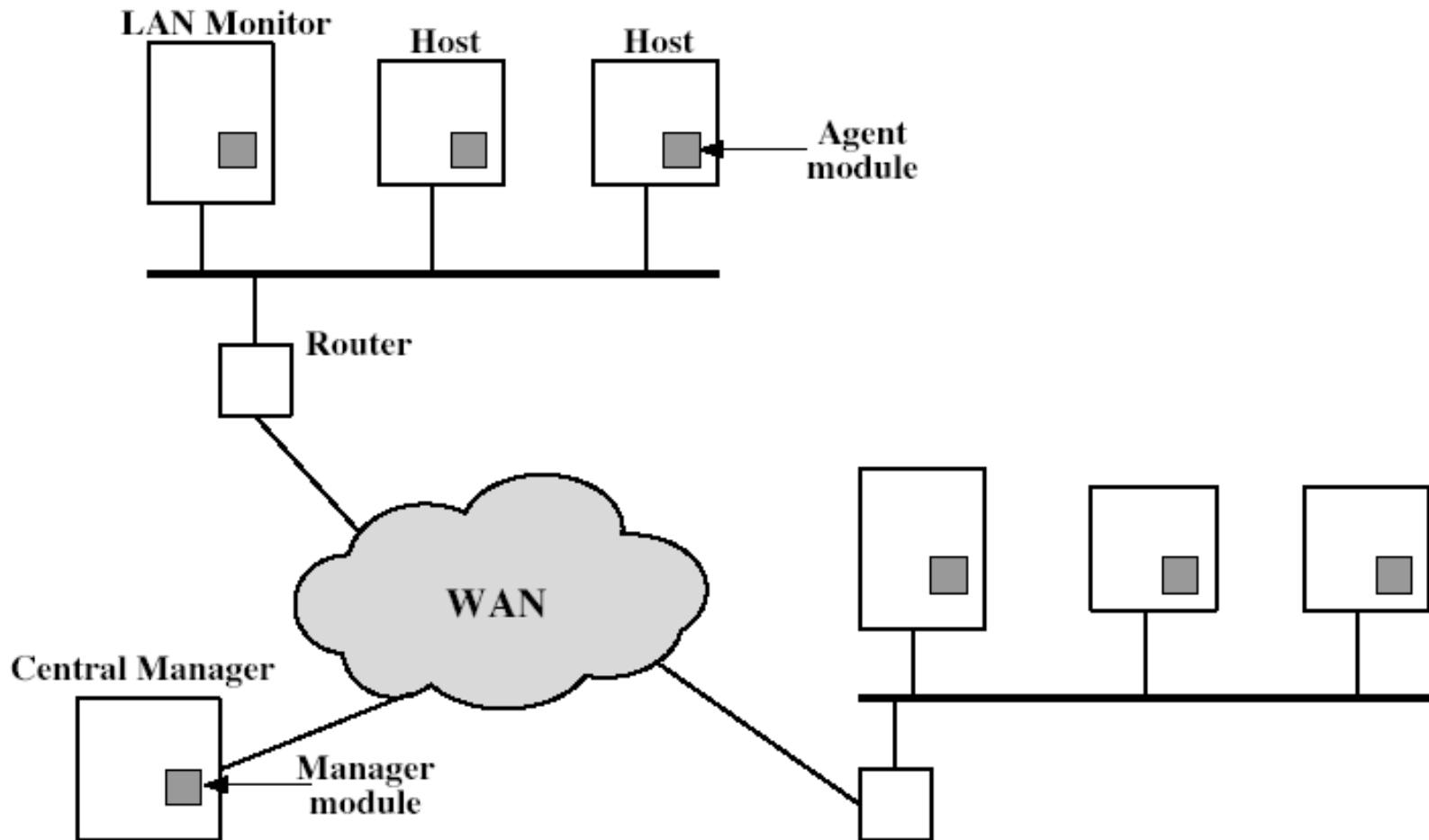
Base-Rate Fallacy

- practically an intrusion detection system needs to detect a substantial percentage of intrusions with few false alarms
 - if too few intrusions detected -> false security
 - if too many false alarms -> ignore / waste time
- this is very hard to do
- existing systems seem not to have a good record

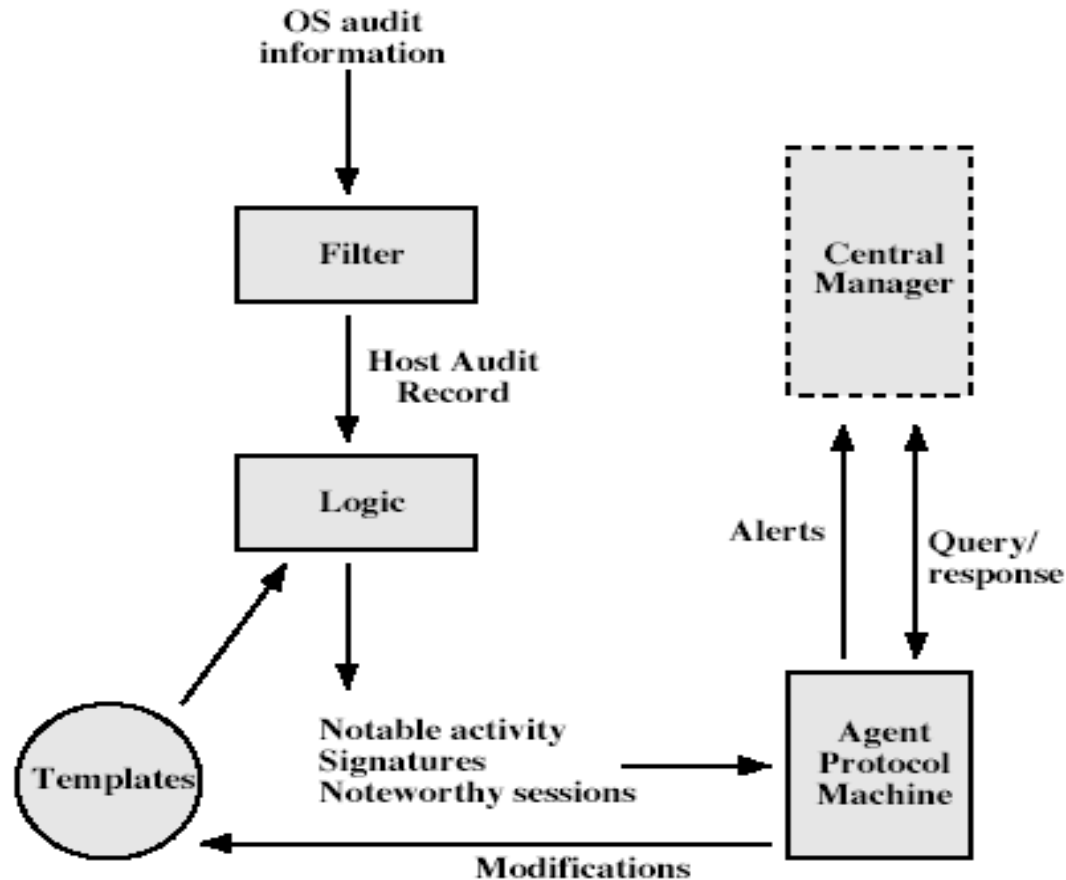
Distributed Intrusion Detection

- traditional focus is on single systems
- but typically have networked systems
- more effective defense has these working together to detect intrusions
- **issues**
 - dealing with varying audit record formats
 - integrity & confidentiality of networked data
 - centralized or decentralized architecture

Distributed Intrusion Detection - Architecture



Distributed Intrusion Detection - Agent Implementation



Honeypots

- decoy systems to lure attackers
 - away from accessing critical systems
 - to collect information of their activities
 - to encourage attacker to stay on system so administrator can respond
- are filled with fabricated information
- instrumented to collect detailed information on attackers activities
- may be single or multiple networked systems

Password Management

- front-line defense against intruders
- users supply both:
 - login – determines privileges of that user
 - password – to identify them
- passwords often stored encrypted
 - Unix uses multiple DES (variant with salt)
 - more recent systems use crypto hash function

Managing Passwords

- need policies and good user education
- ensure **every** account has a default password
- ensure users change the default passwords to something they can remember
- protect password file from general access
- set technical policies to enforce good passwords
 - minimum length (>6)
 - require a mix of upper & lower case letters, numbers, punctuation
 - block known dictionary words

Managing Passwords

- may reactively run password guessing tools
 - note that good dictionaries exist for almost any language/interest group
- may enforce periodic changing of passwords
- have system monitor failed login attempts, & lockout account if see too many in a short period
- do need to educate users and get support
- balance requirements with user acceptance
- be aware of **social engineering** attacks

Proactive Password Checking

- most promising approach to improving password security
- allow users to select own password
- but have system verify it is acceptable
 - simple rule enforcement (see previous slide)
 - compare against dictionary of bad passwords
 - use algorithmic (markov model or bloom filter) to detect poor choices

Summary

- have considered:
 - problem of intrusion
 - intrusion detection (statistical & rule-based)
 - password management