

Computer Security

Network Security 1

IP Security

- Application specific security mechanisms exist (eg., SSL, Kerberos, PGP)
- sometimes want security at a lower network layer
- want to be sure all traffic secure
- can put security at the level of IP

IP Security

- provides security even for applications with no security awareness
- three functional areas:
 - authentication
 - confidentiality
 - key management

History

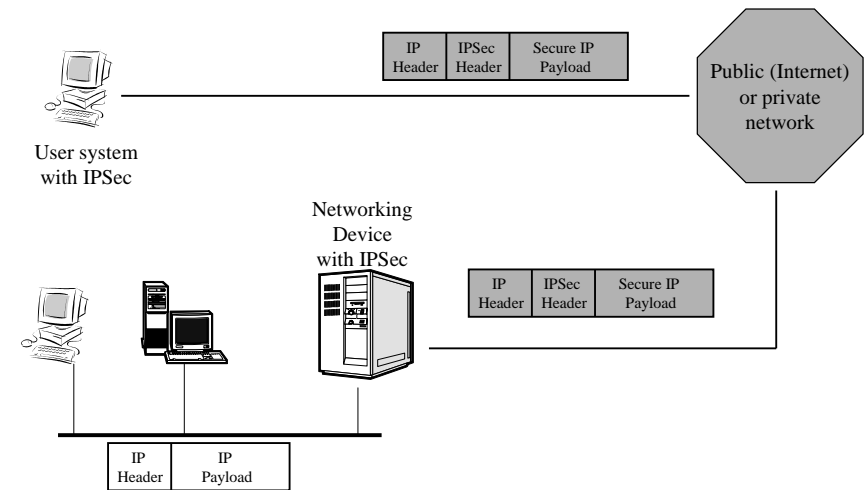
- development begun in 1994
- designed to be usable with IPv4 and IPv6

Applications

- secure communication across LANs and WANs, including the Internet
- examples
 - secure branch office connectivity
 - secure remote access
 - secure communication with other organisations
 - enhanced e-commerce security

5

Example



6

IPSec Benefits

- when implemented in firewall or router traffic across perimeter receives strong security with no overhead for traffic within perimeter
- IPSec in firewall resistant to bypass (assuming properly implemented firewall)
- IPSec below transport layer so transparent to applications & users
- can provide security for off-site users

7

Routing

- IPSec can contribute to routing architecture for Internetworking
- IPSec can assure
 - routing and neighbour advertisements come from authorised routers
 - redirect message comes from the router to which initial message was sent
 - routing updates are not forged

8

IPSec

- provides security at IP layer by allowing a system to select
 - security protocols
 - algorithms to be used
 - cryptographic keys

Protocols

- two protocols used to provide security
 - authentication protocol
 - combined encryption/authentication protocol
- first uses an Authentication Header (AH)
- second uses payload, Encapsulating Security Payload (ESP)

Services

Services

AH

ESP
(encryption only)ESP
(encryption/authentication)

Services	AH	ESP (encryption only)	ESP (encryption/authentication)
Access Control	Yes	Yes	Yes
Connectionless Integrity	Yes		Yes
Data Origin Authentication	Yes		Yes
Rejection of Replay	Yes	Yes	Yes
Confidentiality		Yes	Yes
Limited Traffic Flow Confidentiality		Yes	Yes

Security Association

- key concept for both authentication and confidentiality
- one way relationship between sender and receiver
- for two-way exchange need two SAs

Security Association

- identified by
 - Security Parameters Index (SPI)
 - IP Destination Address
 - Security Protocol Identifier

13

Security Parameters Index (SPI)

- bit string assigned to SA, local significance only
- SPI carried in AH and ESP headers
- allows receiver to select the SA under which packet processed

14

IP Destination Address

- endpoint of SA
- may be end user system or network system (router or firewall)

15

Security Protocol Identifier

- Is the SA for AH or ESP?

16

SA Parameters

- IPSec implementation includes database which defines parameters for each SA
- normal parameters
 - sequence number counter
 - sequence counter overflow
 - anti-replay window
 - AH information
 - ESP information
 - Lifetime of SA
 - IPSEC protocol mode
 - Path MTU (maximum transmission unit)

17

SA Selectors

- IPSec very flexible
- user can select which traffic gets IPSec protection
- SAs can be combined in a very fine grained manner

18

Modes

- AH and ESP support two modes
 - transport
 - tunnel

19

Transport Mode

- Primarily for protection of upper-layer protocols
- ie, payload of IP packet (TCP, UDP segments or ICMP packet)
- used for end-to-end communication between two hosts

20

Tunnel Mode

- Protects entire IP packet
- after AH or ESP fields are added to IP packet, entire packet plus security fields is treated as the payload of a new IP packet
- no routers can examine inner packet
- outer packet can have different source and destination

21

Tunnel Mode

- Used when one or both ends of an SA is a security gateway (firewall, router that implements IPSec)
- allows hosts behind firewall to engage in secure communications without implementing IPSec
- tunnelling happens at firewall

22

Combining Security Associations

- A single SA can use AH or ESP but not both
- if need both then need more than one SA
- may need a number of SAs - for
 - AH and ESP
 - two way communication
 - between hosts and firewalls
 - etc

23

Security Association Bundle

- Sequence of SAs
- traffic passes through them to provide desired security services
- SAs in bundle may terminate at the same or different endpoints
- SAs may may be bundled by
 - transport adjacency
 - iterated tunneling

24

Transport Adjacency

- More than one security protocol is applied to a packet, without tunneling
- AH and ESP are combined
- processing takes place at a single destination

25

Transport Adjacency

- ESP is applied to the IP payload, without authentication
- AH is then applied to resulting IP packet
- authentication covers more fields, such as IP source and destination, then are covered by ESP with authentication

26

Iterated Tunnelling

- may wish to do authentication before encryption
- makes altering authentication information harder and makes it easier to store authentication data with original message
- for example, apply authentication to IP header and payload
- then apply ESP to entire packet, giving tunnelling

27

IPSEC

- See text for more information on
 - iterated tunneling
 - AH
 - ESP
 - IPsec key management

28

Firewalls - need

- Internet connection is no longer an option for businesses
- their resources need protection from outside threat

29

Firewalls - rationale

- it is not practical to provide all machines of a large organisation with strong security
- updating and maintaining the security software on 100's or 1000's of machines is costly
- a firewall is a less expensive alternative

30

Characteristics

- all traffic to and from the Internet **must** pass through the firewall
- all other access must be blocked
- only authorised traffic is allowed to pass through the firewall
- the firewall must be secure

31

Firewalls

- define a single choke point for security protection
- provide a location for security monitoring
- can implement IPSec
- can implement non-security Internet functions (address translation, network management, logging)

32

Firewalls cannot

- protect against attacks that bypass them
- protect against internal threats
- protect against viruses

Techniques

- service control
- direction control
- user control
- behaviour control

Service Control

- firewall determines the type of Internet services that may be accessed
- may filter on port number or IP address
- may interpret each service request before passing it on
- may host server software itself, such as web or mail service

User Control

- allows/disallows access to a service based on user identity
- usually applied to users from inside the firewall
- may also be applied to incoming traffic, but this requires some authentication mechanism (such as IPSec)

Control

- Direction Control
 - firewall determines which direction service requests may come from and be allowed to flow
- Behaviour Control
 - controls how services are used (eliminate spam, limit access to information on local web server)

37

Types of Firewall

- packet filtering router
- application level gateway
- circuit level gateway

38

Packet Filtering Router

- filters IP packets
- filters packets going in both directions
- filtering based on rules
- rules based on fields in IP, TCP and UDP headers
 - IP source and destination address
 - IP protocol field
 - UDP or TCP port number

39

Rules

- all packets checked at firewall
- if rule matched rule is used to determine whether packet blocked or allowed to pass
- if no match, default action taken
- default is set as either forward or discard

40

Sample Rules

Class A	Source ADDR	Dest ADDR	Source Port	Dest Port	Action
tcp	*	123.4.5.6	>1023	23	permit
tcp	*	123.4.5.7	>1023	25	permit
tcp	*	123.4.5.8	>1023	25	permit
tcp	129.6.48.254	123.4.5.9	>1023	119	permit
udp	*	123.4.*.*	>1023	123	permit
*	*	*	*	*	deny

41

Advantages of Packet Filters

- simple
- fast
- transparent to users

42

Problems with Packet Filtering

- some packet filters only filter on IP address, not port number
- difficult to specify a complete and secure set of rules
- the rules sets can be very large and difficult to manage

43

Problems with Packet Filtering

- some services, such as Remote Procedure Call (RPC) are difficult to filter as their ports are randomly assigned
- for all its problems packet filtering is an important tool

44

Attacks on Packet Filters

- IP Spoofing
- Source Routing attacks
- Tiny Fragment Attacks

45

IP Spoofing

- IP source address altered to appear to come from inside network, not outside
- can bypass simple minded application of rules
- can be countered by discarding packets with inside source address that arrive from outside

46

Source Routing Attack

- source station specifies route
- attacker hopes to use this to bypass checking
- firewall should discard packets which use this option

47

Tiny Fragment Attack

- uses small IP packets to put TCP header in separate packets
- designed to circumvent filtering on TCP header
- can be defeated by discarding small packets or retaining TCP information to check subsequent packets

48

Application Level Gateway

- also called a proxy server
- relays application level traffic (eg., ftp, http, telnet, smtp)
- user contacts gateway, specifying name of remote host to be contacted
- firewall contacts host
- in effect, two connections, spliced at firewall

49

Application Level Gateway

- user must authenticate
- firewall provides service if service implemented and allowed to user
- gateway can be configured to support only some features of an application

50

Application Level Gateway

- more secure than packet filters
- does not need to manage numerous rules, only a limited number of application settings
- easy to do logging
- disadvantage is overhead of managing two connections

51

Circuit Level Gateway

- does not permit end to end TCP connections
- sets up two TCP connections, one for inside and one for outside, as for application-level gateway
- Can be stand alone system or specialised function of an application-level gateway

52

Circuit Level Gateway

- relays TCP segments from one connection to another without examining them
- security lies in which connections are allowed
- often used when internal users trusted
- supports application level service for inbound connections
- circuit level functions for outbound

53

Bastion Host

- critical host for system security
- common example is platform for application-level or circuit-level gateway

54

Common Characteristics

- runs secure version of operating system
- only essential applications installed (such as proxy servers for telnet, ftp, smtp, etc)
- may require additional authentication before allowing use of proxy servers
- proxies may only support limited functionality

55

Common Characteristics

- proxies may only be accessible from certain local hosts
- maintains detailed auditing information
- proxies are small and designed for security
- proxies independent of each other
- proxies perform limited disk access
- proxies run in non-privileged mode

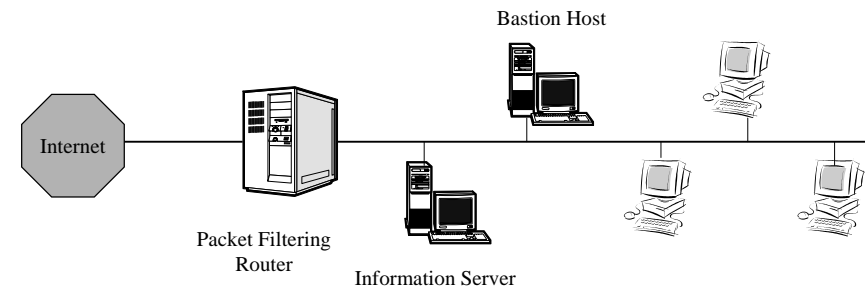
56

Firewall Configurations

- may be more complicated than simply a single gateway host
- common configurations
 - screened host firewall, single-homed bastion
 - screened host firewall, dual-homed bastion
 - screened subnet firewall

57

Single Homed Bastion Host



58

Screened host firewall, single-homed bastion

- firewall consists of two systems
 - packet filtering router
 - bastion host
- router allows only
 - IP traffic from Internet addressed to bastion
 - outward IP traffic from bastion
- bastion performs authentication and proxy functions

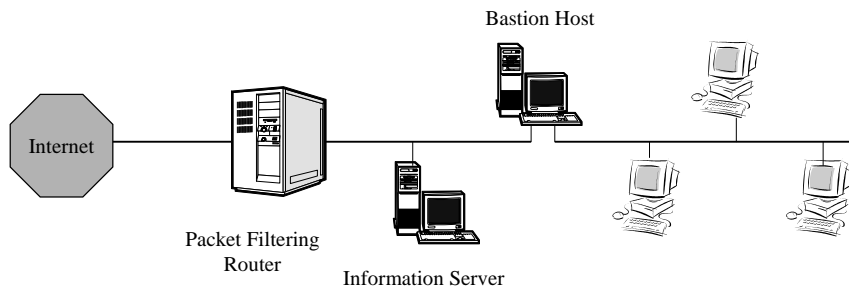
59

Comparison

- more secure than just a gateway
- implements both application and packet level filtering
- provides flexible Internet access, router can be configured to allow direct connection to specified network nodes, such as web server

60

Dual-homed Bastion



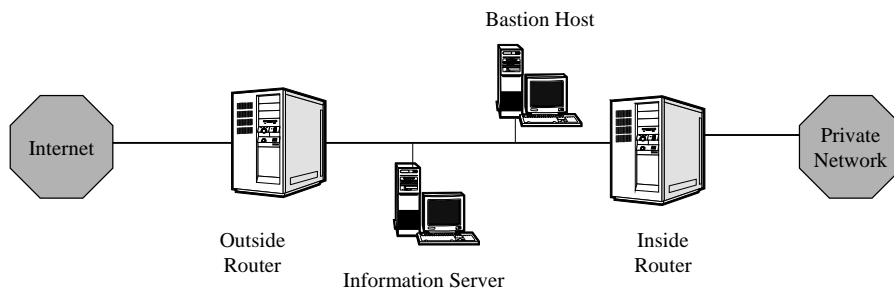
61

Screened host firewall, Dual-homed bastion

- in single homed configuration, compromise of packet filter allows direct traffic flow between Internet and internal hosts
- in this configuration all traffic must pass through bastion as well as packet filter
- means both must be subverted to allow free access to Internet

62

Screened Subnet Firewall



63

Screened Subnet Firewall

- two packet filtering routers are used
- bastion host is between them
- isolated subnet which includes bastion host may also have information servers and modems
- only isolated subnet visible to Internet - remainder of local system is not

64

Intrusion Detection

- Even the best intrusion prevention systems may fail
- If an intruder will enter a system then the next best thing is detecting the intrusion
- also may be cheaper to prevent some attacks and detect others
- these attacks handled by administrators

65

Uses of Intrusion Detection

- The intruder can be forced out of the system
- Intrusion detection can serve as a deterrent
- Intrusion detection can collect information to improve intrusion prevention

66

Intruder Behaviour

- Intrusion detection based on the theory that
 - intruder behaviour differs from legitimate users
 - This difference can be quantified
- However, the difference will not be total – there will be some overlap

67

False Positives

- This overlap can cause problems in intrusion detection
- Loose interpretation of intruder behaviour leads to legitimate users being classified as intruders – **false positives**

68

False Negatives

- A too tight definition of intruder behaviour leads to the reverse
- Intruders are classified as legitimate users – **false negatives**

69

Identifying Intruders

- Patterns of legitimate use identified by observation
- Significant deviations can then be detected (at least in theory)
- However an outsider will probably be more easily detected than an insider gone rogue

70

Audit Records

- Very important for intrusion detection
- Used as input to intrusion detection system
- Two main types
 - Native audit records
 - Detection-specific audit records

71

Native Audit Records

- Operating systems own accounting facilities
- no additional auditing tools used/needed
- may not collect exactly the information the intrusion detection system requires

72

Detection-specific Audit Records

- Collection facility purpose designed for intrusion detection system
- collects exactly the information required
- does involve extra overhead as additional to operating systems accounting software

73

Example Detection-Specific Audit Record

- Contains
 - Subject
 - Action
 - Object
 - Exception condition raised (if any)
 - Resource usage
 - Time stamp

74

Audit Record

- User actions broken down into elementary operations
- So one user action may result in a number of audit actions
- This has a number of advantages, at the cost of more information to be collected and stored

75

Advantages

- All behaviour affecting all objects is audited
- The format of the information kept is simplified
- Information easy to collect, as based directly on actions

76

Approaches to Intrusion Detection

- Statistical Anomaly Detection
- Rule-based Detection

Statistical Anomaly Detection

- Data relating to legitimate user behaviour collected over time
- Statistical tests applied to observed behaviour to determine whether that behaviour is legitimate or not
- Can only give an answer that is within a level of certainty, not definite

Threshold Detection

- Thresholds are defined, independent of the user
- These define frequency of occurrence of various events
- If threshold surpassed, may be an intruder

Threshold Detection

- Count based on event type occurrence over specified time interval
- Threshold and time interval need to be determined
- Crude and not effective against even moderately sophisticated attack

Threshold Detection

- Activities of users vary
- This will lead to either a large number of false negatives or false positives, depending on threshold chosen
- Still useful when combined with other techniques

81

Profile Based

- A profile of each user's activity developed
- Used to detect changes in behaviour of individual accounts
- A profile may consist of a set of parameters
- Deviation on a single parameter may not be enough to signal an alert

82

Profile Based

- Fundamental to this approach is analysis of audit records
- Designer must decide which quantitative metrics are used to measure user behaviour
- User behaviour examined over time to ascertain normal behaviour
- Current audit records can then be used to detect intruders

83

Example Metrics

- Counter : a count of an event type
 - #logins/hour, times command executed, password failures
- Gauge: a measure of activity
 - #connections, #outgoing messages
- Interval timer: time between events
 - Time between successive logins
- Resource utilisation: resources consumed
 - #pages printed, total time of program execution

84

Tests on Metrics

- Various statistical test can be applied
 - Mean and standard deviation
 - Multivariate
 - Markov process
 - Time series
 - Operational
- Need to define acceptable limits

85

Statistical Profiles

- Prior knowledge of security flaws not required
- Detector program learns what is “normal”
- Then looks for deviations

86

Statistical Profiles

- Does assume learning process not corrupted by attackers (false negatives)
- Problems with users changing to new, but still legitimate, behaviour (false positives)

87

Rule-Based Detection

- A set of rules defined
- used to decide that a given behaviour is that of an intruder
- Anomaly detection – rules to detect deviation from previous usage patterns
- Penetration identification – an expert system approach that searches for suspicious behaviour

88

Anomaly Detection

- Similar to statistical anomaly detection
- Historical audit records analysed
- Usage patterns identified and rules which describe those patterns automatically generated
- Current behaviour matched against rules to determine if it conforms to historically observed patterns

Anomaly Detection

- As with statistical anomaly detection assumes future behaviour will be like the past
- Requires a large database of rules
- Can run to 1000's or even 100,000's of rules

Penetration Identification

- Different to intrusion detection
- Based on expert systems
- Uses rules for identifying known penetrations or penetrations that would exploit known weaknesses
- Rules can also identify suspicious behaviour (even if that is within established usage patterns)

Penetration Identification

- Rules generated by experts
- Often based on interviews of sys admin, security experts, etc
- Strength of system depends on knowledge of interviewees

Heuristics

- Simple example using heuristics
 - Users should not read files in other users' directories
 - User must not write to other user's files
 - Users should not simultaneously be logged in more than once
 - Users who log in after hours should do the same things they do during working hours
 - etc

93

Heuristics

- Audit records examined as generated
- If a match found to a rule user's *suspicion rating* increased
- If enough rules matched a threshold is passed and a report made to operators

94

High vs. Low Level Actions

- It may be difficult to express all possible intrusions in detailed low level rules
- Can use higher level actions and state transition approach
- See text

95

Statistics vs. Rules

- Statistical approaches attempt to define normal, or expected behaviour
- Rules based approaches attempt to define "proper" behaviour
- Statistical better against masqueraders, rule based better against misfeasors
- A system will probably need both

96

Distributed Intrusion Detection

- Can base defence on individual machines
- more effective if there is coordination across the network
- major issues
 - audit record formats
 - information transmission
 - architecture
- see text for example system (p.302-3)

Audit Record Formats

- Different machine/systems in the network may use different formats
- any cooperation between them, or any central system, will need to allow for this

Information Transmission

- data sent may be raw or summary
- Some systems may serve as central collection/analysis points
- Any audit information sent be confidentiality/integrity protected

Architecture

- Centralised or decentralised
- single central point simplifies correlation of information
- also creates bottleneck and single point of failure
- decentralised systems need to exchange information and coordinate activities

Problems with Intrusion Detection

- Intrusion detection isn't easy
 - Explaining the systems in court
 - high level of “junk” packets on internet
 - very few attacks mean high ratio of false positives and admin fatigue
 - huge variety of possible attacks
 - no organisational commitment
 - encrypted traffic
- most systems detect at best 60-80% of attacks in laboratory conditions