Network Security

- IPsec -

- Firewalls -

Dr. John Keeney

3BA33

Background

Slides Sources: Henric Johnson, Charlie Kaufman, Wikipedia, Andre E. Bar'yudin, Lawrie Brown, Munehiro Fukuda, Sue Moon.

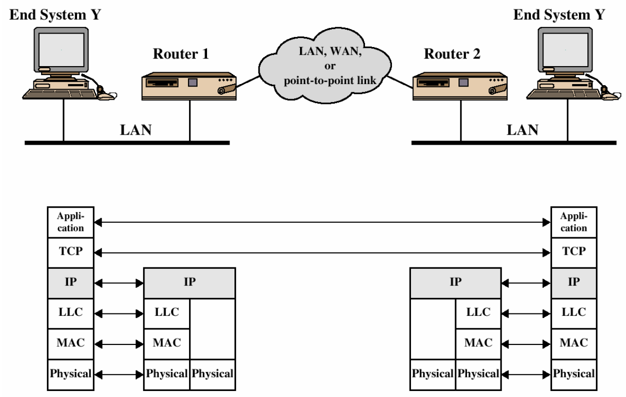
Recommended Reading:

- Stallings, W., Cryptography and Network Security: Principles and Practice, 2nd edition. Prentice Hall, 1999
- Pfleeger, C., Security in Computing. Prentice Hall, 1997.
- Kurose, J., Ross, K., Computer Networking: A Top Down Approach Featuring the Internet. Addison-Wesley, 2002.
- RFC4301-4309
- Chapman, D., and Zwicky, E. Building Internet Firewalls. O'Reilly, 1995
- Cheswick, W., and Bellovin, S. Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley, 2000
- Wikipedia

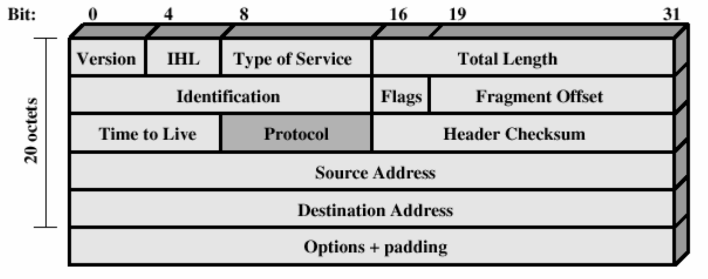
IP Security

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

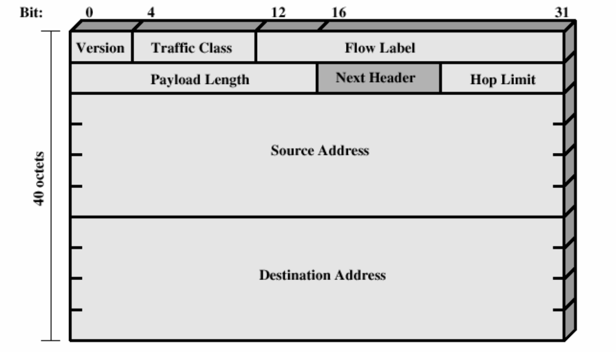
TCP/IP Example



IPv4 Header



IPv6 Header



IPsec: Network Layer Security

- Network-layer secrecy:
  - sending host encrypts the data in IP datagram
  - TCP and UDP segments; ICMP and SNMP messages.
- Network-layer authentication
  - destination host can authenticate source IP address
- Applicable to use over LANs, across public & private WANs, & for the Internet
- Optional in IPv4, Mandatory in IPv6
  - Designed for IPv6, back-ported to IPv4

IPsec: Network Layer Security

- Tunnel mode versus Transport mode
  - Transport Mode provides a secure connection between two endpoints as it encapsulates IP's **payload.** The IP header is neither modified nor encrypted. Requires IPSec support at each host.
  - Tunnel Mode encapsulates the **entire** IP packet to provide a virtual "secure hop" between two gateways. Encrypted Packet is encapsulated into a new IP packet. Requires IPSec support at end hosts.
- Two options: AH (authentication) and ESP (encapsulated security)
  - the two main wire-level protocols used by IPsec
  - Authenticate (AH) the data flowing over the connection.
  - Encrypt & Authenticate (ESP) the data flowing over the connection.
  - Typically used independently,
    - possible (but uncommon) to use them both together.

IPSec provides

- Access Control
- Transparent to applications (below transport layer (TCP, UDP)
- Data origin authentication
- Rejection of replayed packets
- Confidentiality (encryption)
- Limited traffic flow confidentiallity
- Provide security for individual users
- IPSec can assure that:
  - A router or neighbour advertisement comes from an authorized router
  - A redirect message comes from the router to which the initial packet was sent
  - A routing update is not forged

Security Associations

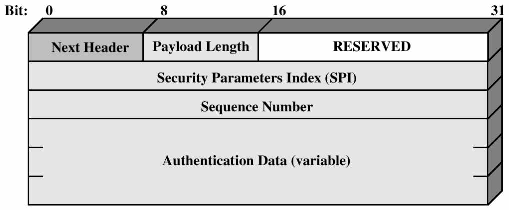
- For both AH and ESP, source/destination handshake creates a network-layer logical channel called a security association (SA
- a one-way relationship between sender & receiver that affords security for traffic flow
- Each SA unidirectional.
- A security association is simply the bundle of algorithms and parameters (such as keys) that is being used to encrypt a particular flow.
- The actual choice of algorithm is left up to the users.
- A security parameter index (SPI) is provided along with the destination address to allow the security association for a packet to be looked up in a database of SAs at the receiver.
- Before sender can use IPSec to communicate with a receiver, sender must know index value of a SA on receiver
  - Index values owned by destinations, not globally known!
  - SAs can have lifetimes by reusing index values

Authentication Header (AH)

- Authentication by adding a new Header
- provides support for data integrity & authentication of IP packets
  - end system/router can authenticate user/app
  - prevents address spoofing attacks by tracking sequence numbers
  - No encryption
- based on use of a MAC
  - MD5 or SHA-1
- parties must share a secret key
- protocol field: 51
- AH header inserted between IP header, data field.
  - intermediate routers process datagrams as usual

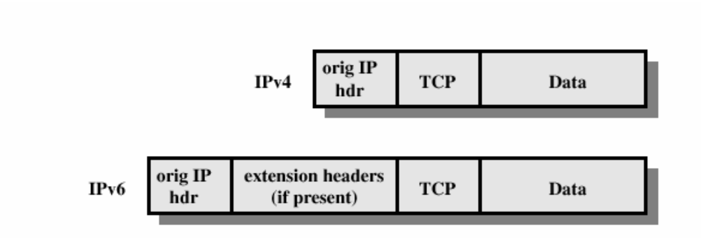
Authentication Header

- Provides support for data integrity and authentication (MAC code) of IP packets.
- Guards against replay attacks.
- Contains:
  - connection identifier
  - authentication data: source- signed message digest calculated over original IP datagram.
  - next header field: specifies type of data (e.g., TCP, UDP, ICMP)

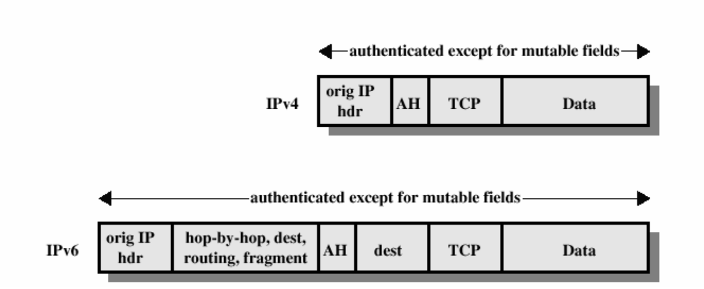

Bit: 0
8
16
31
Next Header
Payload Length
RESERVED
Security Parameters Index (SPI)
Sequence Number
Authentication Data (variable)

IP header	AH header	data (e.g., TCP, UDP segment)

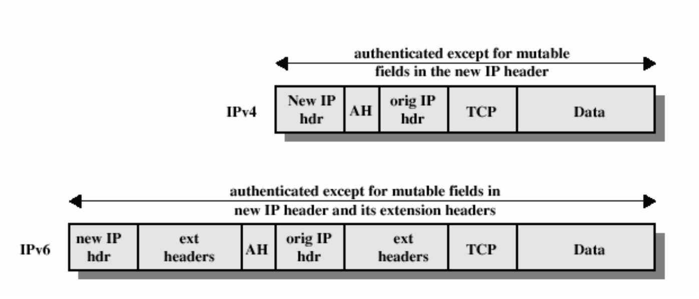
Before applying AH



Transport Mode AH Authentication

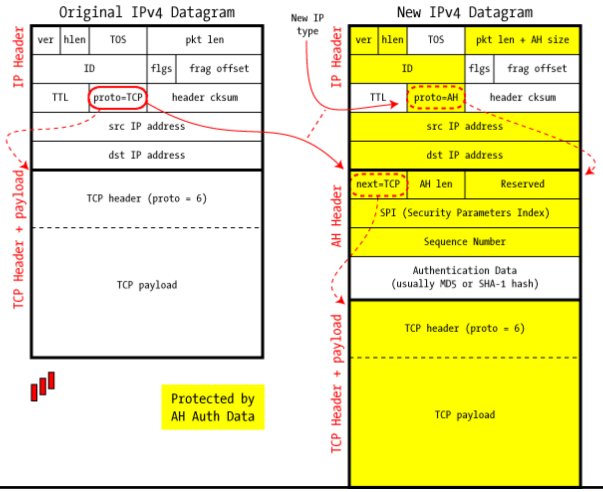

authenticated except for mutable fields
IPv4
orig IP hdr
AH
TCP
Data
authenticated except for mutable fields
IPv6
orig IP hdr
hop-by-hop, dest, routing, fragment
AH
dest
TCP
Data

Tunnel Mode AH Authentication

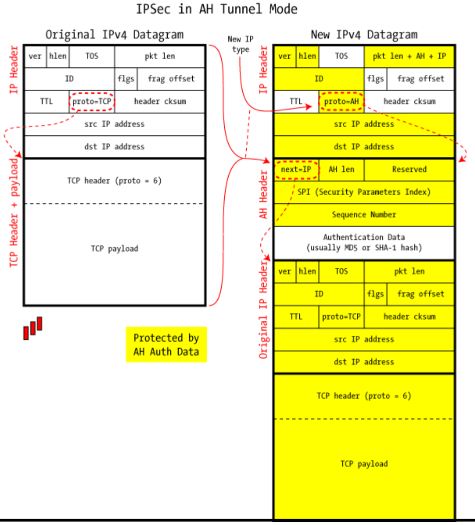

authenticated except for mutable fields in the new IP header
IPv4
New IP hdr
AH
orig IP hdr
TCP
Data
authenticated except for mutable fields in new IP header and its extension headers
IPv6
new IP hdr
ext headers
AH
orig IP hdr
ext headers
TCP
Data

AH in Transport Mode

IPSec in AH Transport Mode

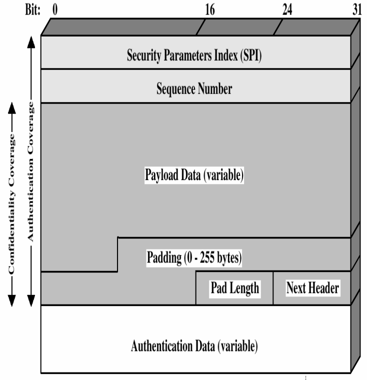


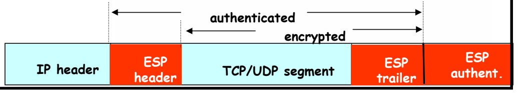
AH in Tunnel Mode



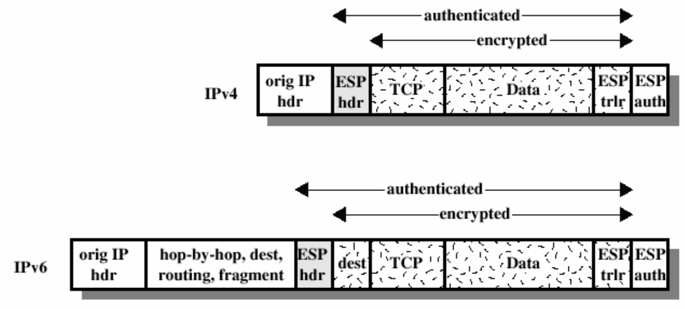
Encapsulating Security Payload: ESP

- Authentication and Encryption by encrypting and encapsuling the datagram rather than adding a header
- ESP provides confidentiality services
- can optionally provide the same authentication services as AH
- Data & ESP trailer encrypted.
- Next header field is in ESP trailer.
- ESP authentication field is similar to AH authentication field.
- Protocol = 50.
- Encryption
  - 3DES, RC5, IDEA, 3IDEA, CAST, Blowfish
- Authentication:
  - MD5, SHA-1



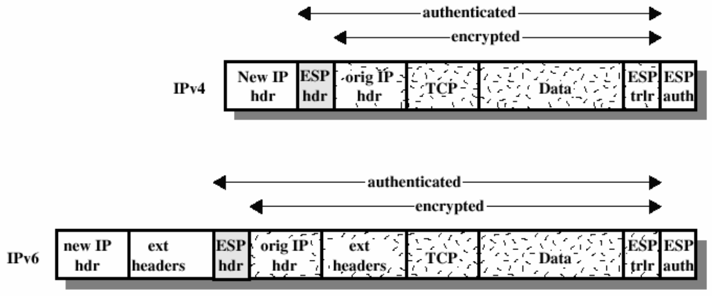


ESP Encryption and Authentication



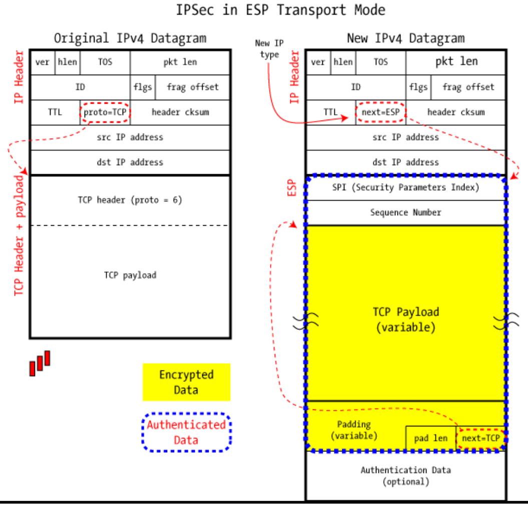
(a) Transport Mode

ESP Encryption and Authentication

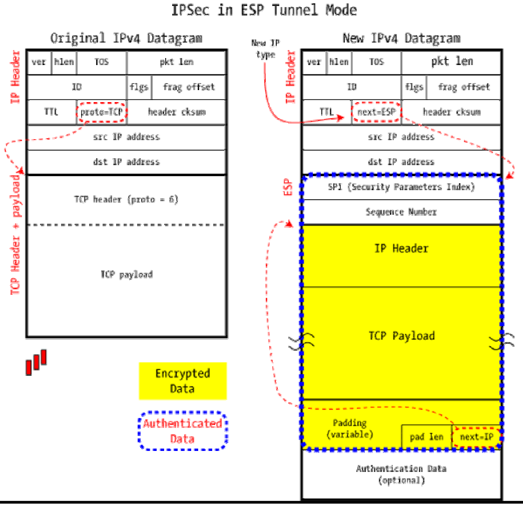


(b) Tunnel Mode

ESP in Transport Mode



ESP in Tunnel Mode



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

Summary

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers	Authenticates entire inner IP packet plus selected portions of outer IP header
ESP	Encrypts IP payload and any IPv6 extension header	Encrypts inner IP packet
ESP with authentication	Encrypts IP payload and any IPv6 extension header. Authenticates IP payload but not IP header	Encrypts inner IP packet. Authenticates inner IP packet.

Key management

- ESP and AH use *session keys*
- Sessions are called *Security Associations*
  - Indexed by protocol, IP address, SPI
- Two types:
  - Manual
    - Can manually config AH/ESP keys
    - sysadmin manually configures every system
  - Automated
    - for on demand creation of keys for SA's in large systems
    - Oakley Key Determination Protocol
      - based on Diffie-Hellman key exchange
      - address weaknesses of DH, e.g man-in-the-middle, DoS etc
    - Internet Security Association and Key Management Protocol (ISAKMP)
      - defines procedures and packet formats to establish, negotiate, modify, & delete SAs
      - independent of key exchange protocol, encryption alg, & authentication method

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

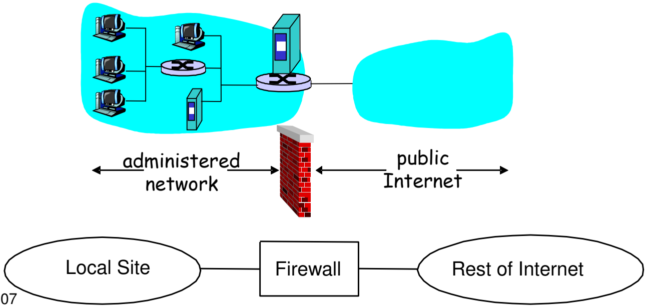
IPsec redux

- Deployment of IPsec limited
  - Global PKI infrastructure hard to set up
  - Wrong layer for security
    - Session/Application-layer, rather than Network layer
  - Fixes a "solved" problem
    - SSL & SSH work well
- IPsec success: VPNs
  - Use tunnel mode of IPsec

Firewalls

firewall

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.



administered network

public Internet

Local Site

Firewall

Rest of Internet

What is a Firewall?

- a **choke point** of control and monitoring
- interconnects networks with differing trust
- All traffic from in and out must pass through the firewall (physically blocking all access to the local network except via the firewall)
- imposes restrictions on network services
  - only authorised 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
- cannot protect against internal threats
  - E.g. disgruntled employee
- cannot protect against transfer of all virus infected programs or files
  - because of huge range of O/S & file types

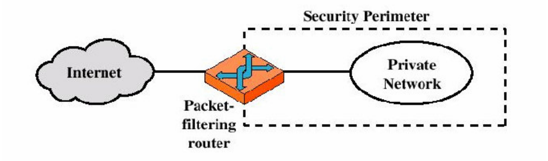
Firewall Characteristics

- Four general techniques:
  - Service control
    - Determines the types of Internet services that can be accessed, inbound or outbound
  - Direction control
    - Determines the direction in which particular service requests are allowed to flow
  - User control
    - Controls access to a service according to which user is attempting to access it
  - Behavior control
    - Controls how particular services are used (e.g. filter e-mail)

Types of Firewalls

- Three common types of Firewalls:
  - Packet-filtering routers
  - Application-level gateways
  - Circuit-level gateways

Firewalls – Packet Filters



Firewalls – Packet Filters

- simplest of components
- foundation of any firewall system
- Two default policies (discard or forward)
  - that not expressly permitted is prohibited
  - that not expressly prohibited is permitted
- Applies a set of rules to each incoming and outgoing IP packet (no context) and then forwards or discards the packet
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header

Packet Filters Example

- Example 1: block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23.
  - All incoming and outgoing UDP flows and telnet connections are blocked.
- Example 2: Block inbound TCP segments with ACK=0.
  - Prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

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

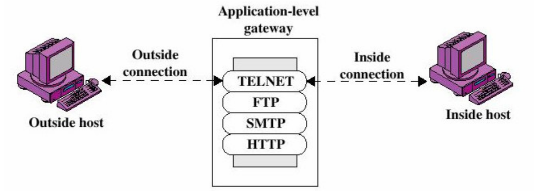
Firewalls – Stateful Packet Filters

- 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

Packet Filters

- Advantages:
  - Simplicity
  - Transparency to users
  - High speed
- Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of Authentication

Firewalls - Application Level Gateway (or Proxy)



Firewalls - Application Level Gateway (or Proxy)

- use an application specific gateway / proxy
  - acts as a relay of application-level traffic
- 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

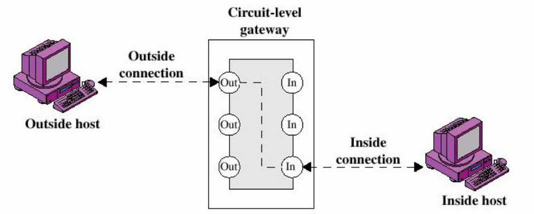
Application Level Gateway Example

- Example: allow select internal users to telnet outside.
  1. Require all telnet users to telnet through gateway.
  2. For authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
  3. Router filter blocks all telnet connections not originating from gateway.

Application Level Gateway (or Proxy)

- Advantages:
  - Higher security than packet filters
  - Only need to scrutinize a few allowable applications
  - Easy to log and audit all incoming traffic
- Disadvantages:
  - Additional processing overhead on each connection (gateway as splice point)
  - client software must know how to contact gateway.
    - e.g., must set IP address of proxy in Web browser

Firewalls - Circuit Level Gateway

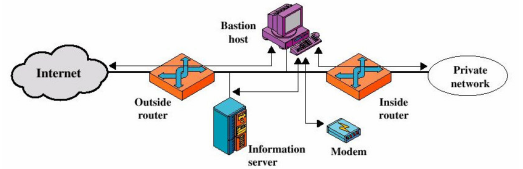


Firewalls - Circuit Level Gateway

- 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

Firewall Configuration example

- In addition to the use of simple configuration of a single system (single packet filtering router or single gateway), more complex configurations are possible
- e.g. Firewall consists of three systems:
  - An external packet-filtering router
  - A bastion host
    - A system identified by the firewall administrator as a critical strong point in the network´s security
    - The bastion host serves as a platform for an application-level or circuit-level gateway
  - An internal packet-filtering router



Firewall Configuration example

- Configuration for the packet-filtering router:
  - Only packets from and to the bastion host are allowed to pass through the router
- The bastion host performs authentication and proxy functions
- Greater security than single configurations because of two reasons:
  - This configuration implements both packet-level and application-level filtering (allowing for flexibility in defining security policy)
  - An intruder must generally penetrate two separate systems
- This configuration also affords flexibility in providing direct Internet access (public information server, e.g. Web server)