

## IP Security Overview

- IP Packets have no inherent security
  - Relatively easy to
    - forge contents of IP packets
    - modify contents of IP packets
    - inspect the contents of IP packets in transit
- Therefore, there is no guarantee that IP datagrams received:
  - are from the claimed sender (source address in the IP header)
  - contain the original data that the sender placed in them
  - were not inspected by a third party while the packet was being sent from source to destination

*IPSec is a means to limit the spoofing of routers*



COMP 6370 – IPSec/VPNs – Lecture 14



## Virtual Private Networks

- A VPN is a way to simulate a private network over a public network, such as the Internet
  - “Virtual” because it depends on the use of virtual connections
  - temporary connections that have no real physical presence, but consist of packets routed over various machines on the Internet on an ad hoc basis
  - secure virtual connections are created between machines and networks as follows:
    - two machines
    - a machine and a network
    - two networks



COMP 6370 – IPSec/VPNs – Lecture 14



## Origins of VPNs

- WANs
  - T1/T3
  - ATM
  - Frame Relay
  - ISDN
  - X.25
- Forerunner of VPNs was the idea of a virtual circuit
  - A virtual circuit creates a logical path from the source to the destination



COMP 6370 – IPSec/VPNs – Lecture 14



## Virtual Circuits

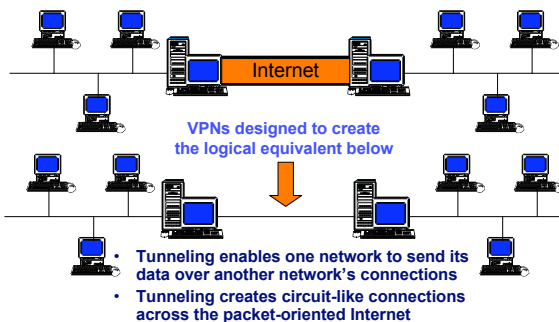
- In packet switched networks, the network makes dynamic decisions concerning the pathway each packet will take
- To improve reliability, a decision could be made prior to any data being sent
  - In this manner, a single static path could be set up between two communicating parties and used exclusively between them
  - This pathway is known as a virtual circuit
- When creating a virtual circuit, sender and receiver agree on which path will be used and on packet size.
  - During communications, acknowledgements are sent, including flow control info and error control info



COMP 6370 – IPSec/VPNs – Lecture 14



## Tunneling



COMP 6370 – IPSec/VPNs – Lecture 14



## VPNs versus long haul connections

- Long Haul connections
  - leased line
  - frame relay network
  - ISDN
  - .....
- For two remote offices, much cheaper to each get an ISP POP (point of presence)
  - Then deploy an VPN between the two routers at the two offices over the Internet



COMP 6370 – IPSec/VPNs – Lecture 14



## How VPNs Solve Internet Security Issues

- **Firewalls**
  - discussed next lecture
- **authentication**
  - multiple means including IPSec
  - Challenge Handshaking Authentication Protocol (CHAP)
  - RSA
- **encryption**
  - multiple means including IPSec
  - private key encryption
  - public key encryption



COMP 6370 – IPSec/VPNs – Lecture 14



## IP Spoofing

- **An attacker compromises the routing packets to redirect a file or transmission to a different destination**
  - most routing information is not encrypted
    - easy to modify source data or change destination
  - also used to mask attacker's identity
- **Best solutions**
  - screen packets at router and firewall, reject any that appear to come from an internal address
  - encryption to safeguard the payloads of the packets
  - authentication to verify sender



COMP 6370 – IPSec/VPNs – Lecture 14



## IPSec

- **IPSec is a method of protecting IP datagrams.**
- **This protection takes the form of**
  - data origin authentication
  - connectionless data integrity authentication
  - data content confidentiality
  - anti-replay protection
  - limited traffic flow confidentiality
- **Protection via Encapsulating Security Payload (ESP) or Authentication Header (AH)**
  - Ultimate security dependent upon the cryptographic algorithm applied
  - Symmetric key cryptography used – why?



COMP 6370 – IPSec/VPNs – Lecture 14



## What is Tunneling?

- **Tunneling encloses one type of data packet into the packet of another protocol**
  - Protocol of the encapsulating packet is understood by the network and by the network entry and exit points
- **Before encapsulation takes place, packets are encrypted so that they payloads are unreadable during transit**
- **Tunneling involves three different protocols**
  - **Carrier protocol** – used by the network that the information is traveling over – usually TCP/IP
  - **Encapsulation protocol** – protocol that the original data is packaged in such as GRE, IPSec, L2F, PPTP or L2TP
  - **Passenger protocol** – original or native data that is being carried from the network where the originating host resides such as IPX, AppleTalk, IP



COMP 6370 – IPSec/VPNs – Lecture 14



## Tunneling Protocols

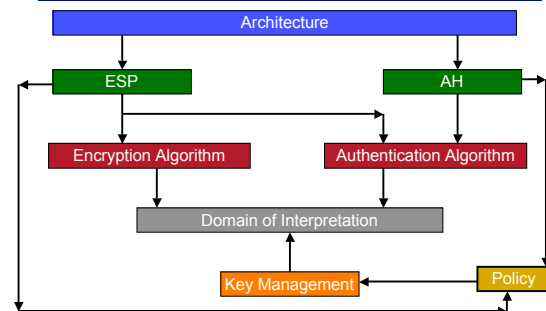
- **Layer 2 tunneling protocols**
  - Layer 2 protocols correspond to the Data Link layer and use frames as their unit of exchange. PPTP, L2TP and L2F are Layer 2 tunneling protocols. These protocols encapsulate the data in a Point-to-point Protocol (PPP) frame to send across an **internetwork\***
  - \*an internet with a lower case i, is any collection of networks that are networked or connected together over a common infrastructure.
- **Layer 3 tunneling protocols**
  - Layer 3 protocols correspond to the network layer and use packets. IP over IP and IPSec Tunnel Mode are examples of Layer 3 tunneling protocols. These protocols encapsulate IP packets in an additional IP header before sending them across an IP internetwork.



COMP 6370 – IPSec/VPNs – Lecture 14



## IPSec Overview



IPSec Roadmap, Doraswamy and Harkins

COMP 6370 – IPSec/VPNs – Lecture 14



## IPSec Architecture Revisited

- Defined by RFC 2401
- Mandatory in IPv6
- Internet Key Exchange (IKE)
  - Symmetric key cryptography is used for efficiency
  - To exchange keys securely, a negotiation protocol is used that allows users to agree on authentication methods, encryption methods and the keys to use.
  - It also specifies how long keys can be used before changing and how to accomplish key exchange
- The IPSec protocols, AH and ESP can be used to protect an entire IP payload or the upper layer protocols of an IP payload.
  - AH used for authentication
  - ESP used for encryption
- Two different modes of IPSec
  - Transport mode to protect upper-layer protocols
  - Tunnel mode to protect entire IP datagrams



COMP 6370 – IPSec/VPNs – Lecture 14



13

## Internet Key Exchange (IKE)

- Compliant IKEs require adherence to three documents
  - ISAKMP specification (RFC 2408) (Internet Security Association and Key Management Protocol)
  - Domain of Interpretation for (DOI) for for IPSec (RFC 2407)
  - IKE specification (RFC 2409)
- Security Associations (SAs) are used with IPSec to define the processing done on a specific IP packet.
- IKEs establish shared security parameters and authenticated keys – SAs- between IPSec peers
- IKE is a generic protocol with application beyond IPSec
  - ex. RIPv2 or OSPF



COMP 6370 – IPSec/VPNs – Lecture 14



14

## Transforms

- Transformation applied to the data to secure it.
  - includes algorithm, key sizes, derivations
  - specific information required in order for different implementations to interoperate
- IKE – Internet Key Exchange
  - establishes shared security parameters and authenticated keys
    - i.e. security associations (SAs) between IPSec peers
  - Actual negotiated parameters come up in the Domain of Interpretation (DOI)
- Policy
  - Necessary but not sufficient for interoperability
  - Determines transforms, representations and implementation



COMP 6370 – IPSec/VPNs – Lecture 14



15

## Overview of ISAKMP

- AH Transform Identifiers
  - AH\_MD5
  - AH\_SHA
  - AH\_DES
  - AH\_SHA2-256 (256 bit message digest)
  - AH\_SHA2-384
  - AH\_SHA2-512
  - AH\_RIPEMD
- Certificate Types
  - PGP certificates
  - DNS signed key
  - x.509 cert – signature
  - x.509 cert – key exchange
  - Kerberos tokens
  - CRL (Cert Revocation List)
  - ARL (Auth Revocation List)
  - SPKI cewrt
  - x.509 cert - Attribute
- ESP Transform Identifiers
  - ESP\_DES\_IV64 (DES in CBC mode with a 64 bit IV)
  - ESP\_DES (DES in CBC mode)
  - ESP\_3DES
  - ESP\_RC5
  - ESP\_IDEA
  - ESP\_CAST
  - ESP\_Blowfish
  - ESP\_3IDEA
  - ESP\_DES\_IV32 (DES in CBC mode with a 32-bit IV)
  - ESP\_RC4
  - ESP\_NULL (NONE)
  - ESP\_AES



COMP 6370 – IPSec/VPNs – Lecture 14



16

## Security Associations

- SAs form the basis for IPSec
  - contract between two communicating entities
  - determine the protocols used for securing packets
- SAs are one-way, i.e. simplex
  - If two hosts are communicating, host A will have an SAout and an SAin
- SAs are protocol specific
  - Each host builds a separate SA for AH and ESP
- Security policy database
  - Works in conjunction with the security association database
- Security Parameter Index
  - 32-bit entity that is used to uniquely identify an SA at the receiver
  - SPI passed to AH and ESP headers using a tuple <spi,dst,protocol>

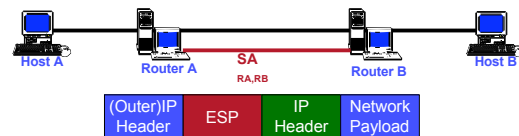


COMP 6370 – IPSec/VPNs – Lecture 14



17

## IPSec in Tunnel Mode



IPSec tunneled mode packet format

- An IPSec tunnel mode packet has two headers – inner and outer
  - Inner header constructed by the host
  - Outer header is added by the device providing security services



COMP 6370 – IPSec/VPNs – Lecture 14



18

### Nested Tunnels

**Nested Packet Format**

IP Header	ESP	IP Header	AH	IP Header	Data
SRC = 2.2.2.1 Dest = 2.3.2.2		SRC = 1.1.1.1 Dest = 2.3.2.2		SRC = 1.1.1.1 Dest = 3.3.3.2	

- IPSec defines tunnel mode for both ESP and AH
- In the nested tunnel example above, host A is sending a packet to host B.
  - Policy requires authentication to router B
  - VPN between the two networks bounded by router A and router B

COMP 6370 – IPSec/VPNs – Lecture 14

### Valid and Invalid Nested Tunnels

- The requirement for the tunnel is that the inner header must be completely encompassed by the outer header.

COMP 6370 – IPSec/VPNs – Lecture 14

### Authentication Header

1<sup>st</sup> 96 bits of second hash becomes Integrity Check Value (ICV)

- 96 bits is selected to maintain compatibility with original IPSec spec
- Replay protection is provided by using the Sequence Number field within the AH header whose value is covered by the authentication procedure

COMP 6370 – IPSec/VPNs – Lecture 14

### Mutable IPv4 fields that cannot be protected by AH

- Mutable IPv4 fields that cannot be protected by AH
  - Type of Service (TOS)
  - Flags
  - Fragment Offset
  - Time to Live (TTL)
  - Header Checksum
- When protection of these fields is required, tunneling should be used
- Payloads of an IP packet are considered immutable and therefore always protected by AH
- An IP packet with AH applied can be fragmented BUT AH cannot be applied to a fragmented packet

COMP 6370 – IPSec/VPNs – Lecture 14

### AH Transport and Tunnel Modes

- In transport mode, the original datagram's IP header is the outermost IP header
- In tunnel mode, a new IP header is generated for use as the outer IP header of the resulting datagram
  - Source and destination address of the new header will generally differ – i.e. the destination address of the new IP header may be a corporate firewall.

COMP 6370 – IPSec/VPNs – Lecture 14

### Encapsulating Security Payload (ESP)

- ESP adds approximately 24 bytes per packet
- For interoperability purposes, mandatory to implement algorithms has been defined for ESP
  - The must-implement cipher is DES-CBC with an explicit IV (RFC 2405)
  - The must-implement authenticators are HMAC-MD5-96 and HMAC-SHA-96 (RFCs 2403 AND 2404)
- Published prior to development of “deep crack”
- RFCs updated to indicate deprecated nature of DES and suggesting stronger cipher algorithms

COMP 6370 – IPSec/VPNs – Lecture 14

## Outbound ESP Processing

- Insert header (similar for both IPv4 and IPv6)
- Encrypt packet from beginning of the payload to the next header field in the trailer using appropriate cipher specified in the SA (policy check)
- Authenticate packet from ESP header through the ciphertext to the ESP trailer.
  - Insert result in the authentication data field of the ESP trailer
- Recompute checksum of the IP header the precedes the ESP header



COMP 6370 – IPSec/VPNs – Lecture 14



25

## Inbound ESP Processing

- SA determines what the incoming packet **should be**.
  - No way to tell until packet is decrypted
  - Makes unauthorized traffic analysis harder
  - If no valid SA exists – drop the packet
- Next, authenticate by checking the message digest
  - pass appropriate key to authentication algorithm from the SA
- Decrypt the packet -- from the beginning of the payload data to the next header field
  - decrypted using the key and cipher algorithm from the SA
  - check decryption by checking the padding
    - padding is completely deterministic
    - verifies whether packet was successfully decrypted.

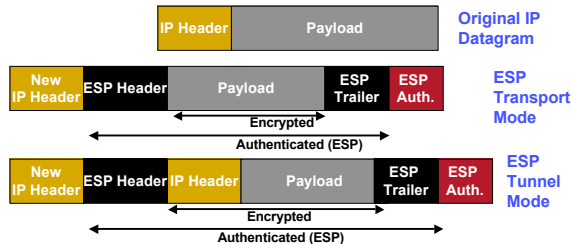


COMP 6370 – IPSec/VPNs – Lecture 14



26

## ESP Transport and Tunnel Modes



- ESP in transport mode provides neither authentication nor encryption for the IP header.
- In tunnel mode, the new IP header is not encrypted – everything else is



COMP 6370 – IPSec/VPNs – Lecture 14



27

## Transport Mode

- AH and ESP intercept the packets moving from the transport layer into the network layer.
  - When security is NOT enabled, TCP and UDP flow into IP which adds an IP header
  - When security is enabled, TCP / UDP flow into the IPSec component
  - When both AH and ESP are used, ESP is applied first – why?



Packet format with AH and ESP



COMP 6370 – IPSec/VPNs – Lecture 14



28

## Tunnel Mode

- IPSec in Tunnel mode is normally used when the ultimate destination of the packet is **different** from the security termination point.
  - ex. security termination point may be a router rather than a host.
  - also used when a router provides security services for packets it is forwarding
  - In the case of tunnel mode, IPSec encapsulates an IP packet with IPSec headers and adds an outer IP header



IPSec tunneled mode packet format



COMP 6370 – IPSec/VPNs – Lecture 14



29

## Conclusion: IPSec Implementation

- Can be implemented in end hosts, gateways / routers or both
- Advantages of OS-level integration
  - Efficiency: IPSec can use network services in the OS such as user context (sockets)
  - Ease of Implementation: Network connections, HTTP connections – all can be configured from the host
  - All IPSec modes are supported
- BUMP-in-the-Stack (BITS) network level integration
  - Supports multiple OSs
  - Duplicated functionality causing unnecessary complications
  - Allows firewall vendors to integrate with their products



COMP 6370 – IPSec/VPNs – Lecture 14



30