IPSec

Dr.Talal Alkharobi

IPsec (IP security)

- A suite of protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream.
- IPsec also includes protocols for cryptographic key establishment.
- IPsec is implemented by a set of cryptographic protocols for
  - (1) securing packet flows and
  - (2) internet key exchange.

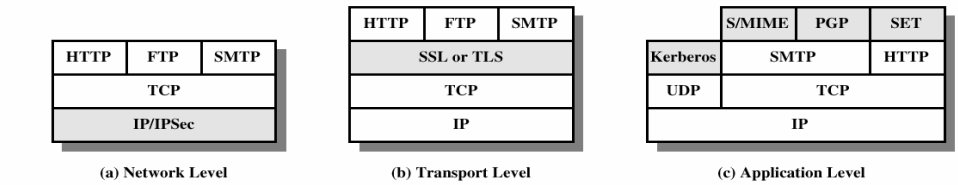
3

IPSec

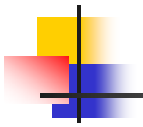
- IPsec protocols operate at the network layer, layer 3 of the OSI model.
- Other Internet security protocols in widespread use, such as SSL and TLS, operate from the transport layer up (OSI layers 4 - 7).
- This makes IPsec more flexible, as it can be used for protecting both TCP- and UDP-based protocols, but increases its complexity and processing overhead, as it cannot rely on TCP (OSI layer 4) to manage reliability and fragmentation.

4

Security facilities in the TCP/IP protocol stack



5



Design intent

- Since the Internet Protocol does not inherently provide any security capabilities, IPsec was introduced to provide security services such as:
  - Encrypting traffic
  - Integrity validation
  - Authenticating the peers
  - Anti-replay (protection against replay of the secure session)

6

IPsec Operations

- There are two modes of IPsec operation:
  - Transport mode
  - Tunnel mode
- The security implications are quite different between the two operational modes.
- IPsec can be used to create Virtual Private Networks (VPN) in either mode

IPsec Operations Transport mode

7

- End-to-end security of packet traffic in which the end-point computers do the security processing
- Only the payload (message) of the IP packet is encrypted.
- The routing is intact since the IP header is neither modified nor encrypted
- When the Authentication Header is used, the IP addresses cannot be translated, as this will invalidate the hash value.
- The transport and application layers are always secured by hash so they cannot be modified in any way (translating the port numbers)
- Transport mode is used for host-to-host communications

IPsec Operations Tunnel mode

8

- Portal-to-portal communications security in which security of packet traffic is provided to several machines (even to whole LANs) by a single node.
- In tunnel mode, the entire IP packet is encrypted.
- It must then be encapsulated into a new IP packet for routing to work.
- Tunnel mode is used for network-to-network communications (secure tunnels between routers) or host-to-network and host-to-host communications over the Internet.

9

Current status as a standard

- IPsec is a mandatory part of IPv6, and is optional for use with IPv4.
- While the standard is designed to be indifferent to IP versions, current widespread deployment and experience concerns IPv4 implementations.
- IPsec protocols were originally defined by RFCs 1825–1829, published in 1995.
- In 1998, these documents were obsoleted by RFCs 2401–2412.
- RFC 2401–2412 are not compatible with RFC 1825–1829, although they are conceptually identical.

10

Current status as a standard

- In December 2005, third-generation documents, RFCs 4301–4309, were produced.
- RFCs 4301–4309 are largely a superset of 2401–2412, but provide a second Internet Key Exchange standard.

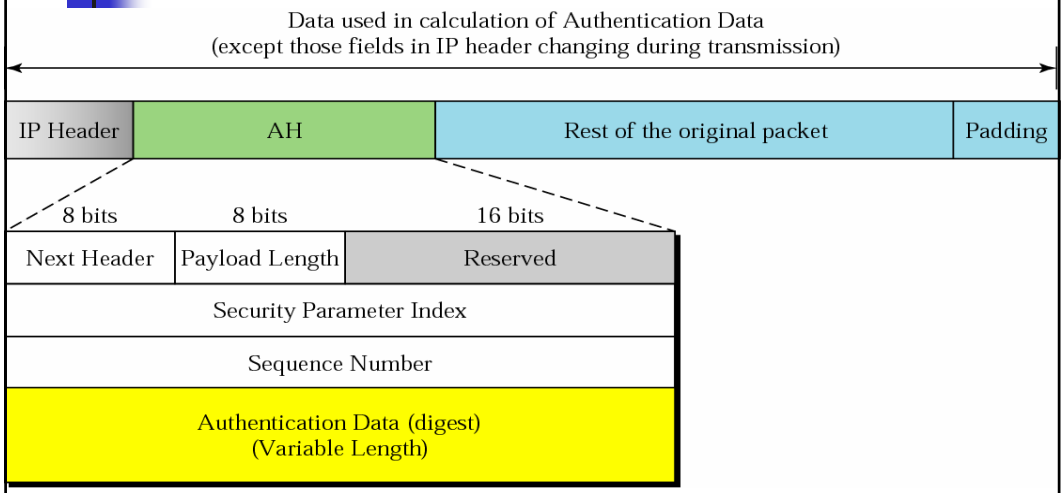
11

Authentication Header (AH)

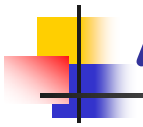
- Authentication Header (AH) protocol is designed to authenticate the source host and to ensure the integrity of the payload carried by the IP packet.
- The protocol calculates a message digest, using a hashing function and a symmetric key, and inserts the digest in the authentication header.
- The AH protocol provides source authentication and data integrity,but not privacy.

12

Authentication Header (AH)



13



Authentication header

- When an IP datagram carries an authentication header, the original value in the protocol field of the IP header is replaced by the value 51.
- A field inside the authentication header (next header field) defines the original value of the protocol field (the type of payload being carried by the IP datagram).

14

Authentication header

- Steps for authentication header:
  - AH is added to the payload with the authentication data field set to zero.
  - Padding may be added to make the total length even for a particular hashing algorithm
  - Hashing is based on total packet. For message digest, only those fields of IP header that don't change during transmission are considered.
  - Authentication data are included in the authentication header
  - IP header is added after changing the value of protocol field to 51.

15

Authentication header

- Payload length: Length of AH in 4-byte multiples.
- SPI: plays the role of VCI
- Sequence number: for anti replay

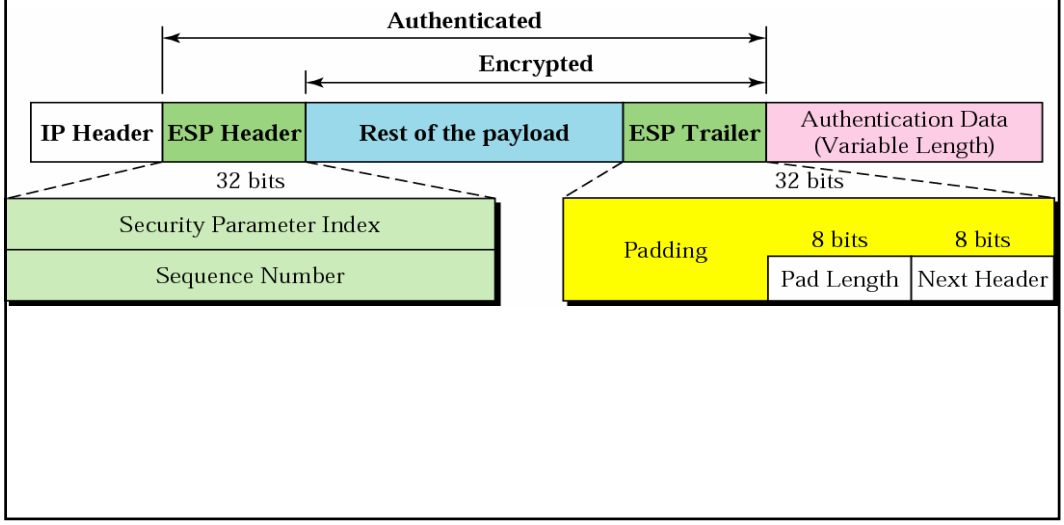
16

Encapsulation Security Payload (ESP)

- Encapsulation Security Payload (ESP) provides source authentication, privacy and integrity.
- Value of IP protocol field is 50.
- Field inside the ESP trailer (next header field) holds the original value of the protocol field of IP header.

Encapsulation Security Payload (ESP)

17



Encapsulation Security Payload (ESP)

18

- Steps
  - ESP trailer is added to the payload
  - Payload and trailer or encrypted
  - ESP header is added
  - ESP header, payload and ESP trailer are used to create authenticated data.
  - Authenticated data are added at the end of ESP trailer.
  - IP header is added after changing the protocol value to 50.

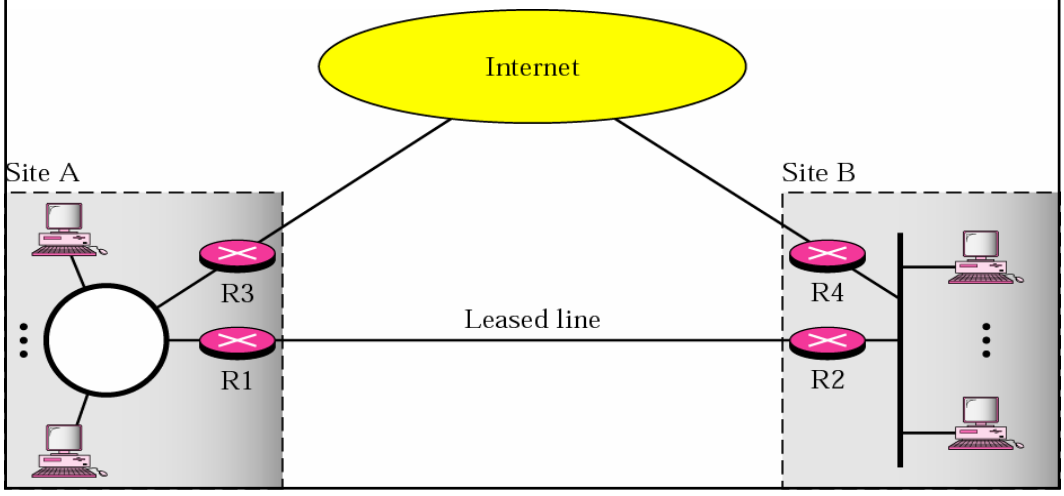
19

VPN

- Privacy within intra-organization but still connected to global Internet.
- Intra-organization data are routed through the private internet; inter-organization data are routed through the global Internet.

20

VPN



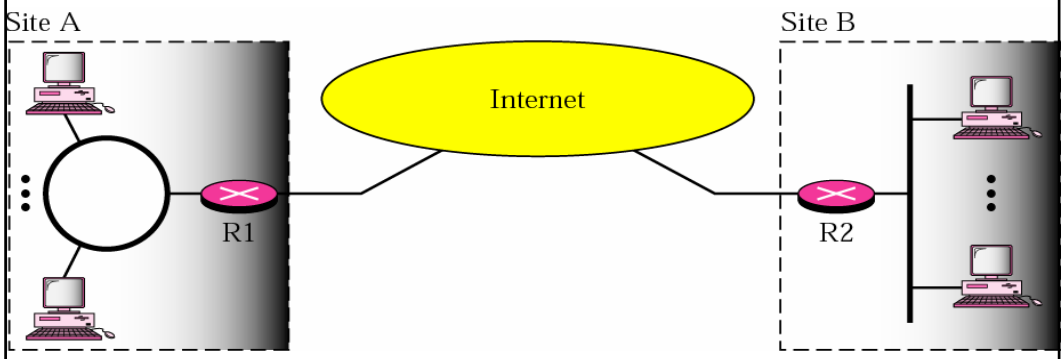
21

VPN

- Private and hybrid networks are costlier.
- Best solution is to use global Internet for both private and public communications.
- VPN creates a network that is private but virtual. It is private but it guarantees privacy inside the organization. It is virtual because it does not use real private WANs; the network is physically public but virtually private.
- VPN uses IPSec in tunnel mode to provide authentication, integrity and privacy.

22

VPN



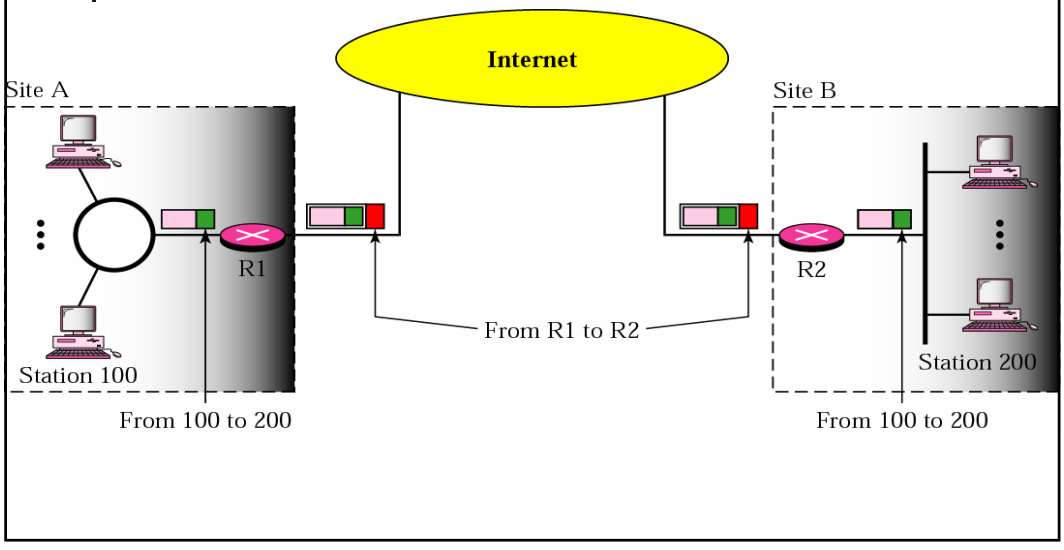
23

VPN

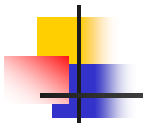
- Each IP datagram destined for private use in the organization is encapsulated in another datagram.
- To use IPSec in the tunneling mode, the VPNs need to use two sets of addressing.
- The public network (Internet) is responsible for carrying the packet from R1 to R2. Outsiders cannot decipher the contents of the packet or the source and destination addresses. Deciphering takes place at R2, which finds the destination address of the packet and delivers it.

24

VPN



25



IP Security Architecture

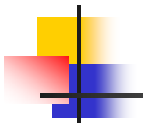
- The IP security architecture uses the concept of a security association (SA) as the basis for building security functions
- SA is simply the bundle of algorithms and parameters (such as keys) that is being used to encrypt a particular flow.
- The actual choice of algorithm is left up to the users.
- A security parameter index (SPI) is provided along with the destination address to allow the security association for a packet to be looked up.
- For multicast therefore, a security association is provided for the group, and is duplicated across all authorised receivers of the group.

26

IP Security Architecture

- There may be more than one security association for a group, using different SPIs, so allowing multiple levels and sets of security within a group.
- Indeed, each sender can have multiple security associations, allowing authentication, since a receiver can only know that someone knowing the keys sent the data.
- Note that the standard doesn't describe how the association is chosen and duplicated across the group; it is assumed that a responsible party will make the choice.

27



IP Security Architecture

- Two headers have been designed to provide security for both IPv4 and IPv6:
  - The IP Authentication Header provides integrity and authentication and non-repudiation, if the appropriate choice of cryptographic algorithms is made.
  - The IP Encapsulating Payload provides confidentiality, along with authentication and integrity.

28

IPSec Implementation

- IPsec support is usually implemented in the kernel with key management and ISAKMP/IKE negotiation carried out from user-space.
- Existing IPsec implementations tend to include both of these functionalities.
- However, as there is a standard interface for key management, it is possible to control one kernel IPsec stack using key management tools from a different implementation.
- Because of this, there is confusion as to the origins of the IPsec implementation that is in the Linux kernel.

29

IPSec Implementation

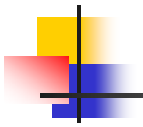
- The FreeS/WAN project made the first complete and open source implementation of IPsec for Linux.
- It consists of a kernel IPsec stack (KLIPS), as well as a key management daemon (pluto) and many shell scripts.
- The FreeS/WAN project was disbanded in March 2004.
- Openswan and strongSwan are continuations of FreeS/WAN.
- The KAME project also implemented complete IPsec support for NetBSD, FreeBSD.
- Its key management daemon is called racoon.

30

IPSec Implementation

- OpenBSD made its own ISAKMP/IKE daemon, simply named isakmpd (that was also ported to other systems, including Linux).
- However, none of these kernel IPsec stacks were integrated into the Linux kernel.
- Alexey Kuznetsov and David S. Miller wrote a kernel IPsec implementation from scratch for the Linux kernel around the end of 2002.
- This stack was subsequently released as part of Linux 2.6, and is referred variously as "native" or "NETKEY".
- Therefore, contrary to popular belief, the Linux IPsec stack did not originate from the KAME project.

31



IPSec Implementation

- As it supports the standard PF_KEY protocol (RFC 2367) and the native XFRM interface for key management, the Linux IPsec stack can be used in conjunction with either pluto from Openswan/strongSwan, isakmpd from OpenBSD project, racoon from the KAME project or without any ISAKMP/IKE daemon (using manual keying).
- The new architrectures of network processors, including multi-core processors with integrated encryption engines, change the way the IPsec stacks are designed.
- A dedicated Fast Path is used in order to offload the processing of the IPsec processing (SA, SP lookups, encryption, etc.).

32

IPSec Implementation

- These Fast Path stacks must be co-integrated on dedicated cores with Linux or RTOS running on other cores.
- These OS are the control plane that runs ISAKMP/IKE of the Fast Path IPsec stack.

33

IPsec and ISAKMP/IKE protocols

- 6WINDGate, Network processor MPU Fast Path IPsec stack
- NRL IPsec, one of the original sources of IPsec code
- OpenBSD, with its own code derived from NRL IPsec
- the KAME stack, that is included in Mac OS X, NetBSD and FreeBSD
- "IPsec" in Cisco IOS Software
- "IPsec" in Microsoft Windows, including Windows XP, Windows 2000, and Windows 2003
- SafeNet QuickSec toolkits

34

IPsec and ISAKMP/IKE protocols

- IPsec in Solaris
- IBM AIX operating system
- IBM z/OS
- IPsec and IKE in HP-UX (HP-UX IPSec)
- "IPsec and IKE" in VxWorks

35

Overview of IPsec-related RFCs

- RFC 2367: PF_KEY Interface
- RFC 2401: Security Architecture for the Internet Protocol
- RFC 2402: Authentication Header
- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405: The ESP DES-CBC Cipher Algorithm With Explicit IV
- RFC 2406: Encapsulating Security Payload
- RFC 2407: IPsec Domain of Interpretation for ISAKMP (IPsec DoI)

36

Overview of IPsec-related RFCs

- RFC 2407: IPsec Domain of Interpretation for ISAKMP (IPsec DoI)
- RFC 2408: Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409: Internet Key Exchange (IKE)
- RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec
- RFC 2411: IP Security Document Roadmap
- RFC 2412: The OAKLEY Key Determination Protocol
- RFC 2451: The ESP CBC-Mode Cipher Algorithms
- RFC 2857: The Use of HMAC-RIPEMD-160-96 within ESP and AH

37

Overview of IPsec-related RFCs

- RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3706: A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3715: IPsec-Network Address Translation (NAT) Compatibility Requirements
- RFC 3947: Negotiation of NAT-Traversal in the IKE
- RFC 3948: UDP Encapsulation of IPsec ESP Packets
- RFC 4106: The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)

38

Overview of IPsec-related RFCs

- RFC 4301: Security Architecture for the Internet Protocol
- RFC 4302: IP Authentication Header
- RFC 4303: IP Encapsulating Security Payload (ESP)
- RFC 4304: Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 4306: Internet Key Exchange (IKEv2) Protocol
- RFC 4307: Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 4308: Cryptographic Suites for IPsec

39

Overview of IPsec-related RFCs

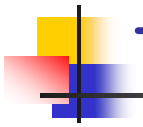
- RFC 4309: Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)
- RFC 4478 : Repeated Authentication in Internet Key Exchange (IKEv2) Protocol
- RFC 4543: The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH
- RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE)
- RFC 4621: Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol
- RFC 4806: Online Certificate Status Protocol (OCSP) Extensions to IKEv2

40

Overview of IPsec-related RFCs

- RFC 4809: Requirements for an IPsec Certificate Management Profile
- RFC 4835: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)

41



The five-layer TCP/IP model

5. Application layer: DHCP • DNS • FTP • Gopher • HTTP • IMAP4 • IRC • NNTP • XMPP • MIME • POP3 • SIP • SMTP • SNMP • SSH • TELNET • RPC • RTP • RTCP • TLS/SSL • SDP • SOAP •
4. Transport layer: TCP • UDP • DCCP • SCTP • RSVP • GTP • …
3. Internet layer: IP (IPv4 • IPv5 • IPv6) • IGMP • ICMP • BGP • RIP • OSPF • ISIS • IPsec • ARP • RARP • …
2. Data link layer: 802.11 • ATM • DTM • Ethernet • FDDI • Frame Relay • GPRS • EVDO • HSPA • HDLC • PPP • L2TP • PPTP • …
1. Physical layer : Ethernet physical layer • ISDN • Modems • PLC • SONET/SDH • G.709 • …