Protecting Data with IPSec (1)

• IPSec
  - Stands for Internet Protocol Security
  - Provides authentication and encryption of data
  - A security framework that allows secure communication between two entities using appropriate algorithms
  - Manages and secures authentication, confidentiality, integrity, and packet anti-replay
Protecting Data with IPSec (2)

• IPSec in OSI Reference Model (left) vs. TCP/IP Model (right)

Introduce software into destination computer
so that software to packets and use packets to
attacking applications: attackers add own
– Modifying data
– Compromising data
– Spoofing: IP @, packet sequence numbers,
– Compromising keys: shared key
– Captured data

Protecting Data with IPSec (2)
Protecting Data with IPSec

- Digitally signing and encrypting data before transmission
- IPSec encrypts the information in IP datagrams by encapsulating Security Payload
- Security protocols: Authentication Header & Encapsulating Security Payload
- Security services for IP traffic
- Intermediate systems, such as routers, treat the encrypted part of the packets purely as payload
- Protocols besides IPSec, such as SSL or TLS, encrypt the payload, but intermediate systems, such as routers, treat the encryption differently
- IPSec provides end-to-end encryption
- Specific types of traffic (Web, application-layer protocols) can be encrypted by using protocols like SSL or TLS
- Key Management Service
- Security Services
- Security Architecture

IPSec Services
IPSec Services (2)

• Authentication Header (AH)
  – Establishes identity of the message sender and ensures that the transmitted data has not been tampered with

  – Encapsulating Security Payload (ESP)
    • Same as AH + defines data encryption methods
    • Establishes identity of the message sender
    • Authenticates Header (AH)

IPSec Services (3)

• Security Association
  – Contract or negotiation between 2 communicating entities defining security parameters to use during IPSec communication
  – Ciphering algorithms & IPSec protocols
  – Keys & key validity
IPSec Services (4)

• Key Management Service
  – Usually Internet Key Exchange (IKE)
  – Keys can also be passed manually

  IPSec Architecture

IPSec Application

- Used for LANs, WANs, Internet
  - Used to build secure tunnel over open network such as Virtual Private Network (VPNs)
  - Branch office connectivity
  - Remote access
  - Connectivity with partners: Intranet
- Usually in border routers and/or firewalls
  - Connectivity with partners: Internet
  - Remote access
  - Branch office connectivity
    (VPNs)
  - Used to build secure tunnel over open network such as Virtual Private Network
  - Used for LANs, WANs, Internet

IPSec Functions (1)

- Key generation
  - Diffie-Hellman algorithm
    - 2 C both must access to shared encryption key
  - HMAC in combination with Secure Hash Algorithm-1 (SHA1)
- Cryptographic checksums
  - HMAC in combination with Message Digest 5 (MD5) and SHA1
- Authentication
  - Hash Algorithm 1 (SHA1)
IPSec Functions (2)

- Mutual authentication
  - C authenticate e/o to establish a trust relationship
  - Kerberos in Windows, digital certificates, or pre-shared key

- Replay prevention
  - Replay even when data in packets is encrypted
  - IPSec prevents replay by assigning a sequence number to each packet: anti-replay services
  - Prevents reply even when data in packets is encrypted

IPSec Protocols (1)

- Two protocols that provide different types of security for network communications
- IP Authentication Header (AH)
- IP Encapsulating Security Payload (ESP)

IPSec Functions (2)

- Prevents DoS attacks: port, @, protocol
- IPSec includes its own packet filtering mechanism:
  - Packet filtering
  - Number to each packet: anti-replay services
  - IPSec prevents reply by assigning a sequence number even when data in packets is encrypted
  - Shared key
  - Kerberos in Windows, digital certificates, or pre-shared
  - C authenticates e/o to establish a trust relationship
  - Mutual authentication
Detail of AH and ESP Protocols (2)

IP Authentication Header (AH)

- Does not encrypt the data in IP packets, but it does provide authentication, anti-replay, and integrity services
- AH by itself or in combination with ESP
- AH alone provides basic security services, with relatively low overhead

Detail of AH and ESP Protocols (3)

IP Authentication Header

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Header</td>
<td>Security Parameters Indices</td>
</tr>
<tr>
<td>Payload Length</td>
<td>Sequence Number</td>
</tr>
<tr>
<td>Reserved</td>
<td>Authentication Data</td>
</tr>
</tbody>
</table>
Detail of AH and ESP Protocols

• Next Header
  – code specifying the protocol that generated header immediately following the AH header.
  – codes specified by the Internet Assigned Numbers Authority (IANA).
  – IPSec is using AH alone, this field contains the code for the protocol that generated the header immediately following the AH header.

• Payload Length

• Reserved Unused

• Security Parameters Index
  – defines the datagram’s security association = a list of security measures negotiated by the communicating Cs.

• Sequence Number
  – increments by 1 in every subsequent packet using the same security association.
  – form 1 in first packet using a particular security association, and the same sequence numbers are discarded.

• Authentication Data
  – integrity check value (ICV) that the sending computer calculates, based on selected IP header fields, the AH header, and the datagram’s payload.

• ESP Encapsulating Security Payload (ESP)
  – actually encrypts the data in an IP datagram.
  – ESP also provides authentication, integrity, and anti-replay services.
  – inserts header and trailer, surrounds the data in an IP datagram.

IP Encapsulating Security Payload (ESP)

Payload
  – on selected IP header fields, the AH header, and the datagram’s payload.

Authentication Data
  – integrity check value (ICV) that the sending computer calculates, based on selected IP header fields, the AH header, and the datagram’s payload.

Sequence Number
  – increments by 1 in every subsequent packet using the same security association.

Reserved Unused

Payload Length
  – specifies the length of the AH header.

Security Parameters Index

Next Header
Detail of AH and ESP Protocols (7)

IP Encapsulating Security Payload

By itself or in combination with AH
- Maximum possible security for a data transmission
- By itself or in combination with AH
  - ICV, it calculates the value only on the information between the ESP header and trailer; no IP header fields
- Maximum possible security for a data transmission
Transport Mode

- All of AH and ESP protocols applies to

- Not

- Intermediate systems (such as routers) need

- Two end systems must support IPsec but

between computers on NW

Transport Mode: Protect communications
The tunnel mode communications process proceeds as follows:

1. On one of PN transmit data using standard, unprotected IP datagrams.
2. Packets reach router that provides access to WAN, encapsulates using IPSec, encrypting and hashing data.
3. Router transmits encapsulated packets to destination router at end of the WAN connection.
4. Destination router verifies packets by calculating and comparing ICVs, and decrypts if necessary.
5. Destination router repackages information in packet into standard, unprotected IP datagrams and transmits to destination(s) on PN.

Transport Mode:

- Tunnel mode designed provide security for WAN connections, particularly Virtual Private Network (VPN) connections, via the Internet as a communications medium.
- But routers at both ends of the WAN connection do not support and implement the IPSec protocols.
- Tunnel mode connection, end systems do not support and implement IKE, IPSec, encapsulating packets by calculating and comparing ICVs, and decrypting if necessary.

Taken from: https://technet.microsoft.com/en-us/library/BB726946.aspx#ECAA
Tunnel Mode (2)

- IPSec uses a different packet structure in tunnel mode
- Create entirely new datagram and use it to encapsulate the existing datagram.
- Original datagram, inside new datagram.
- Original datagram from one router to the other.

Tunnel Mode (3)

Taken from: http://technet.microsoft.com/enus/library/bb726946.aspx#ECAA
Virtual Private Network (1)

- VPN objectives
  - Security
    - End-to-end security (authentication and, optionally, privacy) for host connecting to a private network over untrusted public intermediate networks
    - Security for private network-to-network communication over untrusted intermediate networks
  - Connectivity: authorized sites, new users, mobile users
  - Simplicity and cost effective: transparency for user, simple for use
  - Quality: can provide QoS via SLAs

- VPN basic functions
  - Membership discovery (identity, authorization)
  - Establishment of secure tunnel (path) in network

Virtual Private Network (2)

- Tunnelling
  - Encapsulating data of one protocol inside the data field of another
  - Point-to-Point Tunneling Protocol (PPTP)
    - Layer 2 Tunneling Protocol (L2TP)
      - Merge PPP and Layer 2 Forwarding Protocol (L2F)
      - PPTP for tunnelling IP and non-IP packets
  - Layer 3 (routers for IP information): Portion of VPN connecting external sites (external)
  - Layer 2 (Ethernet): Portion of VPN connecting internal sites (internal)

- IP Security (IPsec)
  - IP and non-IP packets over IP network
  - IP and non-IP packets over IP network (L2F)
Different VPNs

- Two types
  - Remote-Access
  - Site-to-Site

Remote-Access
- Use the local dial-up infrastructures of Internet Service Providers. Allows mobile workers to take advantage of broadband connectivity and secure remote communication.
Different VPNs (3)

- Alternative to WAN infrastructure to connect branch offices, home offices, or business partners' sites to all or portions of a company's network

Remote-Access and Site-to-Site VPN (4)

- Public Internet or ISP networks — more cost-effectively and more flexible
- WAN requirements — multiple protocols, high reliability, and extensive scalability — but
- company's network partners' sites to all or portions of a business, home offices, or branch offices

Site-to-Site Different VPNs (3)
Advantages of VPN

- Inexpensive alternative to WAN over leased lines
- Provides security support (privacy over the Internet)
- Easy to use
- Resource consolidation
  - Mobile user should understand protocol -> transparent
  - Easy to use
  - Encrypt different insecure protocols: IP, 802.1
  - Provide security support
  - Inexpensive alternative to WAN over leased lines

Disadvantages of VPN

- Need time and expertise for setup
- Difficult to troubleshoot
- Small performance overhead
- VPN Interoperability
  - Encapsulation/decapsulation
Security provided by VPN

- Confidentiality, Integrity, Authenticity
- Encryption to secure communications

- IPSec
- SSH

Examples
- Both
- All software
- All hardware
- Hardware vs. Software

Design Choice

- Examples
  - Gateway to gateway
  - Software (end user) to gateway

Security depends on underlying protocols

- Other
- SSH
- IPSec

Encryption to secure communications

- Confidentiality, Integrity, Authenticity

Security provided by VPN
VPN Configuration: SSH over PPP

- Host Authentication + Certification
  - Secure Socket Layer (SSL)
  - Secure Shell

VPN Configuration: SSL over PPP

(2)

VPN Configuration: SSH over PPP

(1)
VPN Configuration: SSL over PPP

- Initial Handshake
  - “Hello”: SSL Version, Cipher choices, ...
- Session Key determined
- SSL Connection established
- Data transferred over PPP
- SSL Connection established
- Session Key determined
  - “Hello”: SSL Version, Cipher choices, ...
- Initial Handshake

VPN Configuration: Other (4)

• Via Concentrator
  - Accepts connections from VPN peer
  - Suppresses overhead in gateways
  - Concentrator

Layer 2 Tunneling Protocol (L2TP)

- Often combined with IPSec for highest security
- If supported by router
References

1. RFC 2401: Security Architecture for the Internet Protocol
   http://www.ietf.org/rfc/rfc2401.txt

2. RFC 2402: IP Authentication Header

3. RFC 2406: IP Encapsulating Security Payload (ESP)

4. RFC 2408: Internet Security Association and Key Management Protocol (ISAKMP)

5. RFC 2409: The Internet Key Exchange (IKE)

