Internet Protocol Security – IPSec

Prof. Dr.-Ing. habil. Andreas Mitschele-Thiel
Dipl.-Ing. Ali Diab
Outline

• Introduction
• Authentication Header (AH)
• Encapsulating Security Payload (ESP)
• Payload Compression Protocol (PCP)
• Key Management
• Conclusions
• Control Questions
• References
Introduction
Internet Protocol Security (IPSec)

- Security framework for IPv4 and IPv6
  - Provides security for transmission of sensitive information over unprotected networks such as the Internet
  - Provides network security services
    - Data origin authentication
    - Data integrity
    - Data confidentiality
    - Anti-Replay
  - Consists of a couple of separate protocols
Overview of IPSec Standardization

- **IPSec-Architecture**
  - RFC 2401

- **Authentication Header**
  - RFC 2402

- **Encapsulating Security Payload**
  - RFC 2406

  - DES-CBC
    - RFC 2405

  - CBC Mode Cipher Algorithms
    - RFC 2451

- **Key Management**

  - Photuris
    - RFC 2522

  - SKIP (expired Internet Draft)

  - ISAKMP
    - RFCs 2407, 2408

  - Internet Key Exchange
    - RFC 2409

  - Oakley Key Mgmt. Protocol
    - RFC 2412

- **Uses**

- **Consists of**
Authentication Header (AH) & Encapsulating Security Payload (ESP)
Authentication Header (AH)

**IPv4**

Before applying AH: IPv4 Header, Upper Protocol (e.g. TCP, UDP)

After applying AH: IPv4 Header, AH, Upper Protocol

**IPv6**


Authentication Header (Details)

- Identifies Security Association
- Against Replay Attack

<table>
<thead>
<tr>
<th>IPv4 header</th>
<th>protocol: 51</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Header</td>
<td>Payload Length</td>
</tr>
<tr>
<td></td>
<td>Security Parameters Index (SPI)</td>
</tr>
<tr>
<td></td>
<td>Sequence Number Field</td>
</tr>
<tr>
<td></td>
<td>Authentication …</td>
</tr>
<tr>
<td></td>
<td>… Data (variable)</td>
</tr>
<tr>
<td></td>
<td>Upper Protocol …</td>
</tr>
</tbody>
</table>

32 bit
AH Authentication

- Various authentication methods may be used
  - Used method is negotiated
  - Keyed MD5 (default)

- Authentication includes IP header (no variable IP options supported)
- No intermediate authentication when fragmented
- No encryption!

[Diagram showing the flow of data through an IPv4 header, AH, shared secret, and upper protocol.]
Encapsulating Security Payload (ESP)

- Encryption and authentication
- No authentication of IP header
Encapsulating Security Payload (Detail)

- **IPv4 header**: protocol: 50
- **Security Parameters Index (SPI)**
- **Sequence Number Field**
- **Upper Protocol (variable)**
- **Padding (0-255 bytes)**
- **Authentication Data**

- **32 bit**
Tunnel Mode (IPv4)

IPv4

Applying AH (authentication only)

Applying ESP (authentication and encryption)
Tunnel Mode (IPv6)

After applying AH (authentication only)
- New IP Header
- New ext. Headers
- AH
- IPv6 Header
- Hop-by-Hop /Routing
- Dest. opt.
- Upper Protocol

authenticated except for mutable fields

After applying ESP (authentication and encryption)
- New IP Header
- New ext. Headers
- ESP Hdr
- IPv6 Header
- Hop-by-Hop /Routing
- Dest. opt.
- Upper Protocol
- ESP Trailer
- ESP Auth

encrypted
authenticated
AH and ESP – Transport Mode

- **Transport mode** (protection of payload only)
- Application of ESP followed by AH

- **Transport mode** is used when the “cryptographic endpoints” are also the “communication endpoints” of the secured IP packets
  - Cryptographic endpoints: the entities that generate/process an IPSec header (AH or ESP)
  - Communication endpoints: source and destination of an IP packet
AH and ESP – Tunneling Hierarchies

- 2 different sequences for authentication and encryption
  - Authentication first, encryption second
  - Encryption first, authentication second
AH and ESP – Scenarios

- **Tunnel mode**
  - Used when at least one “cryptographic endpoint” is not a “communication endpoint” of the secured IP packets
  - Corporate user works outside corporate network
  - Connecting two sites to a corporate network
AH and ESP – Discussion

• AH causes smaller CPU overhead than bulk encryption

• Non-reputation not provided
  – Signing necessary

• ESP not always necessary
  – Sometimes only packet integrity is need
  – Strong authentication mechanisms are export restricted

• Minimum requirement for IPv6 is AH
Payload Compression Protocol (PCP)
Payload Compression Protocol (PCP)

• Problem: encrypted data cannot be compressed efficiently
  – Encryption introduces randomness

• PCP reduces IP data size before encryption
  – Hence must be a component of IPSec

• Increases the overall communication performance
Overview of Algorithms

- **AH**
  - MD5
  - SHA
  - ...

- **ESP Encryption**
  - NULL
  - DES
  - 3DES
  - AES
  - ...

- **ESP Auth.**
  - MD5
  - SHA
  - ...

- **PCP**
  - PCP-LZS
Key Management
Security Associations (SA)

- Fundamentals of IPSec
  - A contract established between two IPSec endpoints
  - Automatic negotiation of parameters
  - Separate SA required for each subnet or single host
  - Separate SA required for inbound and outbound connections
  - Assigned a unique Security Parameters Index (SPI)

- SA include
  - Key establishment method
  - Authentication
  - Symmetry
  - Perfect forward secrecy (long-term key is compromised)
  - Back traffic protection (current session key is compromised)
Different Key Management Techniques

• **Internet Security Association and Key Management Protocol (ISAKMP)**
  – Utilizing security concepts needed for establishing Security Associations (SAs) and cryptographic keys between two or more hosts in a network
  – Combines the security concepts of authentication, key management, and SAs to establish the required security on the Internet

• **Internet Key Exchange (IKE)**
  – Purpose: obtain keying material and other security associations, such as Authentication Header, and Encapsulated Security Payload for IPSEC
  – IKE is based partly on ISAKMP

• **Photuris**
  – Based on zero knowledge exchanges, followed by authentication of the exchanging parties
  – Originated as NSA’s key exchange protocol for STU-III secure phones

• **Simple Key Management for IP (SKIP)**
  – Proposed by Sun Microsystems
Internet Security Association and Key Management Protocol (ISAKMP)

- **Features**
  - Defines procedures and packet formats to establish, negotiate, modify or delete SAs
  - Provides a framework for authentication and key exchange (but does not define them)
  - Based on Diffie-Hellmann key exchange algorithm to agree on a secret key over an insecure communication channel
  - Digital signature algorithm is used within this protocol

- **Two negotiation phases**
  - First phase: agreement on how to protect further negotiation traffic between two entities
    => ISAKMP SA is established
  - Second phase: security associations for other protocols such as IPSEC are established
Domain of Interpretation (DOI) is used to group related protocols using ISAKMP to negotiate security associations.
ISAKMP – Discussion

• By extending ISAKMP to use public key cryptography and the certificates, it is possible to reduce the number of transmissions for the key exchange, detect masquerades faster and perform all transmissions encrypted from the beginning.

• ISAKMP does not guarantee correct correspondence between the host and the public key used in the key exchange.
Internet Key Exchange (IKE) – Cookie Exchange

• A cookie is the result of hashing a unique identifier of the peer (peer’s IP address, port and protocol), a secret known only to the generator of the cookie, and a time stamp

• The initiator generates a cookie, sets the responder cookie to zero and sends to the responder

• The responder generates a responder cookie, copies the initiator cookie to the message and sends it to the initiator

• The initiator can easily check that the initiator cookie is to one it generated and that the peer’s addresses match

• Only if the cookie matches, check of signatures etc. are made
Internet Key Exchange (IKE) – Phase One

• **Normal mode**
  - Using preshared key authentication
  - Using public key exchanges
    - $\text{SKEYID} = \text{PRF(}\text{preshared key, Ni|Nr}\text{)}$
    - $\text{SKEYID} = \text{PRF(}\text{Ni|Nr, g}^x\text{y}\text{)}$
    - $\text{SKEYID} = \text{PRF(}\text{hash(}\text{Ni|Nr}\text{), CKY-i|CKY-r}\text{)}$
  - Policy negotiation
    - After IKE SA is agreed, IKE will negotiate the policy
    - Example of policy: authenticate everything and if possible encrypt it, and if possible also compress it
    - For each operation there may be several algorithms
    - SA payload may contain several proposals for protocols and exact algorithms (transforms)
    - Negotiating of compression is also included in IKE since it is not good to try to compress encrypted data, therefore link layer compression like in PPP will not work with IPsec
Phase one, normal mode
Using preshared key authentication

Initiator → Responder
Header, SA ← Header, SA

Header, KE, Nonce ← Header, KE, Nonce

Header, IDi, Hash ← Header, IDi, Hash

The normal mode has an exchange of six messages, several versions of the phase one normal mode exist. SA=Security Association, KE=Key Exchange, Nonce=random number, IDi=identity of the peer
**Internet Key Exchange (IKE) – Phase One**

**Phase one of normal mode**

Using public key exchanges:

<table>
<thead>
<tr>
<th>Initiator</th>
<th>Responder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header, SA</td>
<td>Header, SA</td>
</tr>
<tr>
<td>Header, KE, Ni [,Cert_Req ]</td>
<td>Header, KE, Ni [,Cert_Req ]</td>
</tr>
<tr>
<td>Header, IDi, [Cert,] Signature</td>
<td>Header, IDi, [Cert,] Signature</td>
</tr>
</tbody>
</table>

In this variant optional payloads are bracketed. In the optional features a certificate can be requested (Cert_Req) and then it is returned in Cert. Ni=Nonce i
Internet Key Exchange (IKE) – Key Generation

- $SKEYID_d = PRF(SKEYID, g^{xy}|CKY-i|CKY-r|0)$
- $SKEYID_a = PRF(SKEYID, SKEYID_d|g^{xy}|CKY-i|CKY-r|1)$
- $SKEYID_e = PRF(SKEYID, SKEYID_a|g^{xy}|CKY-i|CKY-r|2)$

- $SKEYID_d$ is used for deriving keying data for IPSec
- $SKEYID_a$ is used for integrity and data source authentication
- $SKEYID_e$ is used to encrypt IKE messages
Internet Key Exchange (IKE) – Phase One

• **Aggressive mode**
  - Aggressive mode is more simple than the normal mode. In the aggressive mode there are only three messages exchanged
    - The initiator offers a list of protection suites, his Diffie-Hellman public key value, his nonce and his identity
    - The responder replies with a selected protection suite, his Diffie-Hellman public value, his nonce, his identity, and authentication payload, like a signature
    - The initiator responds with authentication payload
    - There is no chance to negotiate as much in this case as in the normal mode
    - The method suits well for connecting to own site from a remote site as then it is known in advance what kind of authentication the other side supports
Internet Key Exchange (IKE) – Phase Two

- **Quick mode**
  - Phase two of IKE creates IPsec SA. Since IKE can be used for other protocols than IPsec, like the routing protocols RIPv2 and OSPF, IKE SA is not directly IPsec SA
  - IKE SA protects the quick mode by encrypting messages and authenticating them. Authentication comes from use of PRF (the HMAC hash function)
  - The quick mode creates keys for IPsec association
  - Many quick modes can be made using the same IKE SA, therefore a message ID (M-ID) is used to identify the IPsec SA. Nonces are added to prevent replay of the same messages by an attacker
  - The quick mode has more details, but the following figure gives the general view of the protocol
Quick mode exchange

<table>
<thead>
<tr>
<th>Initiator</th>
<th>Responder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header, HASH1, SA, Ni [, KE][, IDci, IDcr]</td>
<td>Header, HASH2, SA, Nr [, KE][, IDci, IDcr]</td>
</tr>
</tbody>
</table>

Header, HASH3

HASH1=PRF(SKEYID_a, M-ID | SA | Ni [, KE] [, IDci | IDcr])
HASH2=PRF(SKEYID_a, M-ID | Ni | SA [, KE] [, IDci | IDcr])
HASH3=PRF(SKEYID_a, 0 | M-ID | Ni | Nr)
Internet Key Exchange (IKE)

- The IKE protocol sets up IPSec (ESP or AH) connections after negotiating appropriate parameters for them, which is done by exchanging packets on UDP port 500 between the two gateways.

- Both phases use the UDP protocol and port 500 for their negotiations. When both IKE phases are completed, IPSEC SAs carry the encrypted data. Then the ESP or AH protocols can be used. These protocols do not have ports; ports apply only to UDP or TCP.

- Automatically negotiates IPSec security associations (SAs) and enables IPSec secure communications without costly manual pre configuration.
IKE Summary

• **Benefits**
  – Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers
  – Allows you to specify a lifetime for the IPSec security association
  – Allows encryption keys to change during IPSec sessions
  – Allows IPSec to provide anti-replay services
  – Permits Certification Authority (CA) support for a manageable, scalable IPSec implementation
  – Allows dynamic authentication of peers

• **Functions**
  – Negotiation
  – Communication Parameters
  – Security Features
  – Authenticate Communicating Peer
  – Protect Identity
  – Generate, Exchange, and Establish Keys in a Secure Manner
  – Manage and Delete Security Associations
Conclusions

• Security architecture for the Internet Protocol

• Provides the following security services to IP packets:
  – Data origin authentication
  – Replay protection
  – Confidentiality

• Can be implemented in end systems or intermediate systems

• Two fundamental security protocols have been defined:
  – Authentication header (AH)
  – Encapsulating security payload (ESP)

• SA negotiation and key management is realized by
  – Internet security association key management protocol (ISAKMP)
  – Internet key exchange (IKE)
Control Questions

• What does IPSec provide?

• Compare between AH and ESP? Propose applications suitable for each?

• How can AH and ESP be used in tunnel mode? What are main differences between using each of them in this mode?

• When should transport mode and tunnel mode be used?

• Explain briefly the operation of ISAKMP? What are the main advantages when using public key cryptographic with ISAKMP?

• What are the tasks achieved in phase one of IKE? What is the purpose of phase two?

• What are the benefits of IKE?
References

Web Links for Security

• http://www.cs.auckland.ac.nz/~pgut001/tutorial/
• http://www.rsasecurity.com/rsalabs/faq/sections.html

IPSec

• http://encyclopedia.thefreedictionary.com/IPSec

Key Management