4.6 Internet Key Exchange
IKE

Prof. Dr. Andreas Steffen

Institute for Internet Technologies and Applications (ITA)
IPsec – Automatic Key Management
The Internet Key Exchange (IKE)

- **Security Association (SA)**
  - A Security Association is a contract established between two IPsec endpoints (hosts or security gateways).
  - Negotiation of parameters to be used for the IPsec connection.
  - ISAKMP SA (IKEv1) or IKE SA (IKEv2) protects the IKE negotiation.
  - Separate IPsec SA required for each subnet or single host.
  - Separate IPsec SA required for inbound and outbound connection.
  - IPsec SAs are assigned a unique Security Parameters Index (SPI) and are maintained in a database.

- **Negotiated Parameters**
  - Authentication Mechanism (IKEv1 only, pre-shared key or public key)
  - Encryption algorithm, Hash algorithm, PRF
  - Key exchange using Diffie-Hellman groups
  - Key lifetimes (IKEv1 only) for the ISAKMP and IPsec SAs.
Internet Key Exchange – IKEv1 Main Mode

Initiator

1. IKE Header
2. ISAKMP SA Proposal
3. IKE Header
4. DH Key Exchange
5. encrypted
6. IKE Header
   - ID_i
   - Cert_i
   - Sig_i

UDP/500

Responder

1. IKE Header
2. ISAKMP SA Response
3. IKE Header
4. DH Key Exchange
5. encrypted
6. IKE Header
   - ID_r
   - Cert_r
   - Sig_r

• IKEv1 Quick Mode – another three messages to negotiate traffic selectors
IKE Main Mode using Pre-Shared Keys

- Pre-shared key
  - is worked into Hash
  - is part of the IKE session key
IKE Aggressive Mode using PreShared Keys

Unencrypted IKE Aggressive Mode messages carrying cleartext IDs can be easily sniffed by a passive attacker.

Pre-Shared Key is worked into $\text{Hash}_r$, together with other known parameters, so that an off-line cracking attack becomes possible.
Man-in-the-Middle Attack possible with IKE Aggressive Mode and XAUTH

- With IKE Aggressive Mode, use One-Time Password scheme (e.g. SecureID).

VPN Client

Wireless LAN User

XAUTH
Username: bodo
Password: aznHu4Um

Attacker

Group Password

Man-in-the-Middle

WLAN Access Point

VPN Gateway

Group Password

bodo
azineHu4Um

With IKE Aggressive Mode, use One-Time Password scheme (e.g. SecureID).
ISAKMP and IPsec Security Associations

09:00  #1 ISAKMP SA  rightid=@gateway.kool.net
09:00  #2 IPsec SA  rightsubnet=10.1.1.0/22
09:10  #3 IPsec SA  rightsubnet=10.1.9.0/24
09:50  #4 IPsec SA  rightsubnet=10.1.1.0/22
10:05  #5 IPsec SA  rightsubnet=10.1.1.0/22  #6 IPsec SA  rightsubnet=10.1.9.0/24
11:00  ikelifetime=3h  keylife=1h
11:40  #7 IPsec SA
11:40  #8 ISAKMP SA
IKE Phase 2 – Quick Mode
Establish or Renew an IPsec SA

• Negotiation of IPsec Parameters
  • Phase 2 Quick Mode establishes an IPsec SA using the secure channel created by the phase 1 ISAKMP SA.
  • The specific configuration parameters for the IPsec connection are negotiated (AH, ESP, authentication / encryption methods and parameters).
  • Quick Mode can be used to renew IPSec SAs about to expire.

• ESP/AH Key Derivation
  • The ESP encryption and ESP/AH authentication keys for the IPsec SAs are derived from the Phase 1 Diffie-Hellman secret.

• Optional Perfect Forward Secrecy
  • If perfect forward secrecy is required, each consecutive Quick Mode will do a fresh Diffie-Hellmann key-exchange.
Motivation for a new IKE RFC

- IKEv1 is spread over three documents (RFCs 2407, 2408, and 2409)
- Too many messages (6 in Main Mode plus 3 in Quick Mode)
- Too many variants (AH/ESP, transport/tunnel, authentication modes)
- Too complex – therefore potentially insecure (Bruce Schneier)
- Cookies not required when not under DoS attack
- New features: NAT-T, Dead Peer Detection, etc.

IKEv2 Protocol

- IPsec SA can be established with 2 request/response pairs
- Additional Child SAs require one request/response pair, each
- EAP authentication modes supported (e.g. One-Time-Passwords), replaces proprietary XAUTH
- New IKE configuration payload replaces proprietary Mode Config

IKEv2 is not backwards compatible with IKEv1 !!!
IKEv2 – Authentication and first Child SA

IKE/Header: SA1ᵢ, KEᵢ, Nᵢ

1. IKE_SA_INIT exchange pair
2. IKE_AUTH exchange pair

Initiator

IKE/Header: IDᵢ, Certᵢ, IDᵢ

UDP/500

Responder

IKE/Header: SA1ᵣ, KEᵣ, Nᵣ

encrypted

IKE/Header: IDᵢ, Certᵢ, Authᵢ

encrypted

Responder

IKE/Header: IDᵣ, Certᵣ, TSᵣ
Cookie Mechanism against DoS Attacks

# strongswan.conf
charon {
    dos_protection = yes
    cookie_threshold = 10
    block_threshold = 5
}
IKEv2 – Additional Child SAs

- CREATE_CHILD_SA exchange pair

- Rekeying IKE_SA: \{ SA_i, Ni, KE_i \}
- Rekeying CHILD_SA: \{ N(REKEY_SA), SA_i, Ni, [KE_i], TSi, TSr \}
- Reauthentication: Start with IKE_SA from scratch
IKEv2 Remote Access Scenario

#ipsec.secrets for roadwarrior carol
: RSA carolKey.pem "nH5ZQEtu0RJEZ6"

#ipsec.conf for roadwarrior carol
conn home
  keyexchange=ikev2
  left=%any
  leftsourceip=%config
  leftcert=carolCert.pem
  leftid=carol@strongswan.org
  leftfirewall=yes
  right=192.168.0.1
  rightid=@moon.strongswan.org
  rightsubnet=10.1.0.0/16
  auto=start

#ipsec.secrets for gateway moon
: RSA moonKey.pem

#ipsec.conf for gateway moon
conn rw
  keyexchange=ikev2
  left=%any
  leftsubnet=10.1.0.0/24
  leftcert=moonCert.pem
  leftid=@moon.strongswan.org
  leftfirewall=yes
  right=%any
  rightsourceip=10.3.0.0/24
  auto=add
4.7 VPN Applications
Virtual Private Networks
• Road Warrior sign on to their home network via IKE with varying IP addresses assigned dynamically by the local ISP.

• Authentication is usually based on RSA public keys and X.509 certificates issued by the home network.

• Virtual IP assigned statically or dynamically by the home network. Remote hosts thus become part of an **extruded net**.
Windows 7 Agile VPN Client

- Gateway certificate must contain host name [or IP address] and the **serverAuth** extendedKeyUsage flag.
strongSwan Applet for the Linux Desktop

- D-Bus based communication between NetworkManager and strongSwan daemon.
- If a CA root certificate is specified then the hostname [or IP address] of the VPN gateway must be contained as a subjectAltName in the received gateway certificate.
strongSwan in a Mixed VPN Environment

Windows Active Directory Server

Campus Network

Linux FreeRadius Server

High-Availability strongSwan VPN Gateway

Internet

strongswan.hsr.ch

Windows 7/8 Agile VPN Client

strongSwan Linux Client

Andreas Steffen, 1.10.2013, 4.6-IKE.pptx 19
4.8 VPN Features
Extended Authentication

- **IKEv1** - XAUTH (eXtended AUTHentication)
  - Proprietary extension used by many vendors (Cisco, Checkpoint, etc.)
  - Based on expired draft-beaulieu-ike-xauth-02.txt

- **IKEv2** - EAP (Extensible Authentication Protocol)
  - EAP-AKA, EAP-SIM, EAP-MSCHAPv2, EAP-MD5, EAP-GTC, EAP-TLS, etc.
  - VPN client triggers EAP by omitting AUTH payload
  - VPN gateway **must** send public key AUTH payload first!

- VPN gateway relays authentication messages to and from AAA server (RADIUS, DIAMETER or LDAP)
Configuration Payload

- **IKEv1 – Mode Config Payload**
  - Proprietary extension used by many vendors (Cisco, Checkpoint, etc.)
  - Based on expired draft draft-dukes-ike-mode-cfg-02.txt

- **IKEv2 – Configuration Payload**
  - has official CP payload

- VPN gateway fetches configuration attributes from AAA server
  - Virtual IPv4 or IPv6 address
  - Internal DNS and WINS servers
  - Proprietary attributes (Cisco Unity, Microsoft, 3GPP, etc.)
IPsec Passthrough (Transparent IPsec Connection)

ADSL and Cable routers use Network Address Translation (NAT) to connect one or several hosts sitting behind the router access to the Internet.

IPsec passthrough forwards ESP and IKE packets to a preconfigured host behind the NAT router.

Drawback: Each router model is configured differently, causing exorbitant costs supporting individual users.

ESP and IKE from a single VPN client

10.3.0.2 UDP/500 ↔ 55.66.x.x UDP/500
10.3.0.2 ESP ↔ 55.66.x.x ESP
11.22.33.44 UDP/500
11.22.33.44 ESP
NAT-Traversal (UDP encapsulation of ESP packets)

10.3.0.2 UDP/4500 ←→ 55.66.x.x UDP/1025
11.22.33.44 UDP/4500

• NAT-Traversal is used if several VPN clients want to set up secure tunnels through a common router doing NAT.

• Typical Applications: WLAN hotspots, hotels, conferences, mobility via GSM/GPRS.

• NAT-Traversal facilitates remote access e.g. working at home.
ESP-in-UDP Encapsulation (RFC 3948)

- **UDP-Encapsulated ESP Header Format**

<table>
<thead>
<tr>
<th>Src Port (4500)</th>
<th>Dst Port (4500)</th>
<th>Length</th>
<th>Checksum</th>
<th>Security Parameters Index</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **IKE Header Format for Port 4500**

<table>
<thead>
<tr>
<th>Src Port (4500)</th>
<th>Dst Port (4500)</th>
<th>Length</th>
<th>Checksum</th>
<th>Security Parameters Index</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>0x00</td>
<td>0x00</td>
<td></td>
</tr>
</tbody>
</table>

- **NAT-Keepalive Packet Format**

<table>
<thead>
<tr>
<th>Src Port (4500)</th>
<th>Dst Port (4500)</th>
<th>Length</th>
<th>Checksum</th>
<th>Security Parameters Index</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>0xFF</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IKEv2 Dead Peer Detection

```
#ipsec.conf for roadwarrior carol
conn %default
dpdelay=60
dpdaction=restart
```

```
#ipsec.conf for gateway moon
conn %default
dpdelay=60
dpdaction=clear
```

```
Oct 24 11:45:10 13[IKE] CHILD_SA home{1} established with SPIs c50810d9_i c8485f4a_o
Oct 24 11:46:10 16[NET] received packet: from 192.168.0.1[500] to 192.168.0.100[500]
Oct 24 11:46:10 16[ENC] parsed INFORMATIONAL request 0 [ ]
Oct 24 11:46:10 16[ENC] generating INFORMATIONAL response 0 [ ]
Oct 24 11:47:09 09[IKE] sending DPD request
Oct 24 11:47:09 09[ENC] generating INFORMATIONAL request 2 [ ]
Oct 24 11:47:13 03[IKE] retransmit 1 of request with message ID 2
Oct 24 11:47:33 08[IKE] retransmit 3 of request with message ID 2
Oct 24 11:47:56 12[IKE] retransmit 4 of request with message ID 2
Oct 24 11:48:38 14[IKE] retransmit 5 of request with message ID 2
Oct 24 11:49:54 16[IKE] giving up after 5 retransmits
Oct 24 11:49:54 16[NET] restarting CHILD_SA home