

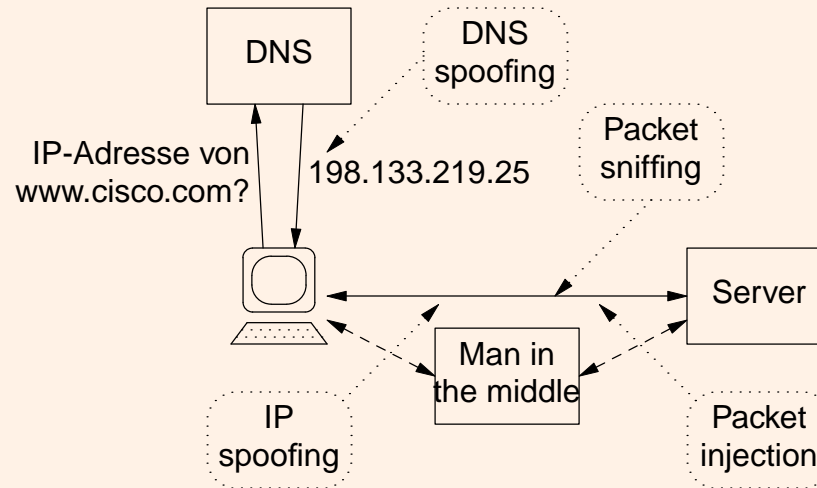
IPsec

Einführung in die Funktionsweise

Holger.Zuleger@hznet.de

IPsec Entwicklungshintergrund

Das Internet Protokoll (IPv4) ist unsicher:



- Keine Authentisierung der Kommunikationspartner (Client & Server).
- Keine Verschlüsselung der Kommunikation.
- Man in the middle Angriffe möglich.
- Lediglich IP-Address basierter Zugriffsschutz!

Lösungsansätze

ISO/OSI Layer		TCP/IP Layer	Applikation/Protokoll
7	Application		SSH, PGP, S/MIME Kerberos
6	Presentation		
5	Session	HTTPS, SMTP over TLS	SSL bzw. TLS
4	Transport	TCP/UDP	
3	Network	IP	IPSec, SKIP
2	Data Link	FR, Seriel, 802.11b	PPP, WEP
1	Physical		

- Häufig keine klare Trennung der Ebenen:
HTTPS und SSL bzw. IPSec mit XAUTH.
- Verschlüsselung (und Hostauthentisierung) auf der Netzwerkebene
- Benutzerauthentisierung auf der Sessionebene (z.B. IMAP)
Auch Klartextpassworte oder IP-Adressen (besser: Kerberos)
- End-To-End Verschlüsselung in der Anwendung (PGP, S/MIME).

IPsec Protokoll

- Arbeitet auf IP-Ebene (OSI-Layer 3, Network Control Layer).
- Seit 1995 (RFC 1825 ersetzt durch RFC 2401)
- Ist definiert für die Verwendung mit IPv4 **und** IPv6.
- Nur für IP-Traffic (TCP, UDP, ICMP, BGP, ...)!
Kein IPX, kein Appletalk, kein OSPF, Kein Multicasting.
- Kein NAT oder PAT (Cisco Hack: IPsec over UDP).

IPsec Protokoll (Aufbau)

Zwei Security Protokolle

- AH (Authentication Header)
- ESP (Encapsulating Security Payload)

Security Policy Database

Welche Kommunikation ist wie mit wem möglich?

Security Association Database

Realisierung einer Security Policy

Protokolle zum Schlüsselmanagement.

- IKE (Internet Key Exchange)
- Photuris

IPsec AH

- Authentication Header (RFC2402).
- IP-Protokoll Nummer 51 (vergl. UDP Nr. 17, TCP Nr. 6).
- Erlaubt eine authentifizierte Kommunikationsbeziehung zwischen zwei Partnern:
 - Absender Authentisierung.
 - Sicherung des Datenstroms gegen Manipulation (Integrität).
 - Sicherung gegen Replay Attacken (Optional).
- Schützt die Nutzdaten und Teile des IP-Headers durch eine Prüfsumme (HMAC).
- Minimale Anforderung laut RFC:
 - HMAC-MD5 (Hashlen = 16 Byte; Keylen > 128 Bit)
 - HMAC-SHA-1 (Hashlen = 20 Byte; Keylen > 160 Bit)

IPsec ESP

- Encapsulating Security Payload (RFC2406).
- IP-Protokoll Nummer 50.
- Erlaubt eine verschlüsselte **und/oder** authentifizierte Kommunikationsbeziehung zwischen zwei Partnern.
 - Verschlüsselung (Optional).
 - Absender Authentisierung (Optional).
 - Sicherung gegen Replay Attacken (Optional).
- Minimale Anforderung laut RFC:

Authentisierung

HMAC-MD5

HMAC-SHA-1

Null authentication

Verschlüsselung

DES in CBC-Mode

Null encryption

**NULL-Auth und NULL-Enc darf nicht gleichzeitig gewählt werden!
NULL-Auth setzt zusätzlich Authentication Header voraus
(AH+ESP)!**

Security Policy Database

Die Security Policy Database (SPD) bestimmt auf welchen Datenverkehr IPsec angewendet werden soll.

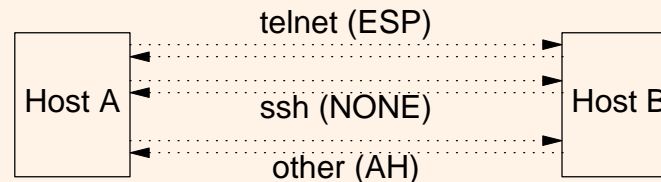
Auswahlkriterien (Selector):

- Source- oder Destination IP (IPv4/IPv6) auch mit Netzmaske.
- Transport Layer Protokoll (TCP/UDP) inklusive Source- oder Destination Port.
- Namen (im Zusammenhang mit Zertifikaten).
 1. User Id (Benutzerauthentisierung)
FQ Username (`zuleger@hznet.de`), X.500 DN (`C=DE, O=HZNET, CN=Holger Zuleger`)
 2. System Name (Host, Security Gateway)
FQDN (`ipsec-gw.example.com`), X.500 DN, X.500 general name.

!! Nicht alle Implementierungen unterstützen diese Vielzahl an Selektoren !!

Security Association

- Realisiert eine Security Policy.
- Eine SA stellt eine **einseitige, virtuelle** Kommunikationsbeziehung dar.
- Für eine funktionierende Kommunikation werden immer **zwei** SA's benötigt (Die Gegenseite muss entsprechend konfiguriert sein).
- Zu einem Kommunikationspartner können durchaus mehrere SA's bestehen.



- Die Einrichtung einer SA kann manuell erfolgen
In der Praxis kaum sinnvoll
- Der Aufbau einer SA sollte automatisch erfolgen
Über Key Management Protokoll

Schlüsselverwaltung

Manuelle Schlüsselverwaltung:

- + Große Interoperabilität.
- Keine dynamische Generierung von Session Keys.
- Kompliziert zu konfigurieren.

Key Management Protokolle:

- ISAKMP, Oakley, SKEME
- IKE
- Photuris
- + Dynamisches Re-Keying, Zeitbasiert oder Volumenabhängig.
- + Vergleichsweise geringer Konfigurationsaufwand.
- + SA Parameter Negotiation.
- Leistungsmerkmale der Implementierungen unterschiedlich.

Internet Key Exchange (IKE)

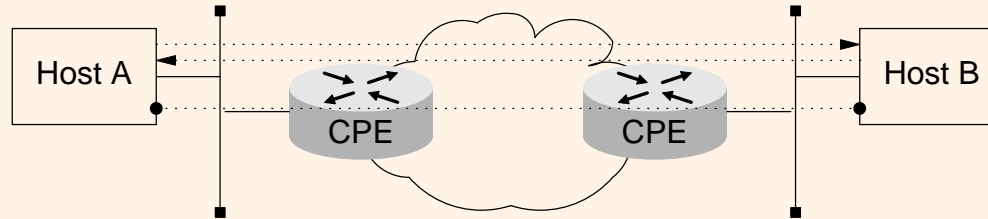
- Kombination aus ISAKMP, Oakley und SKEME(RFC 2409).
- Verwendet Port 500 UDP.
- Zwei Phasen Protokoll:
 1. Authentisierung des Partners (Main/Aggressive Mode).
 2. SA Negotiation und Austausch der Session Keys (Quick Mode).

Phase 1 findet nur einmal pro Kommunikationspartner statt, Phase 2 für jede SA separat.

- Unterschiedliche Authentisierungsverfahren:
 - Preshared Keys
 - Public Key Encryption
 - Public Key Signaturen (RSA|DSS), Zertifikate
- Erweiterungen für:
 - Dead Peer Detection (draft-ietf-ipsec-dpf-00.txt, Cisco)
 - Remote Config (draft-dukes-ike-mode-cfg-02.txt, Cisco)
 - Extended User Authentication (draft-beaulieu-ike-xauth-02.txt, Cisco)

IPsec Transport-Mode

Host to Host (Transport-Mode):



IP-Headerformate:

Original Paket: | IPHdr[6/17] | TCP/UDP-hdr | data |

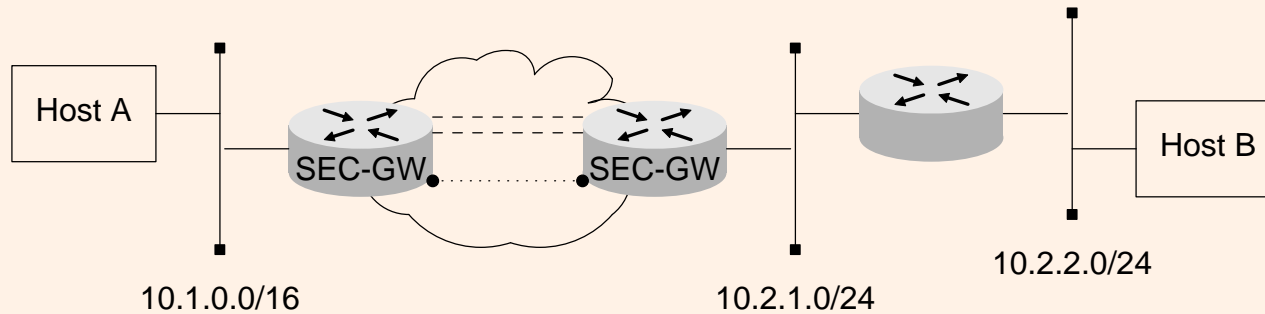
AH-Transport: | IPHdr[51] | AH-hdr[6/17] | TCP/UDP-hdr | data |

ESP-Transport: | IPHdr[50] | ESP-hdr[6/17] | TCP/UDP-hdr | data | ESP-Trailer | ESP-Auth |

IPsec Tunnel-Mode

- Eine IPsec-Box kann als Gateway für andere Hosts genutzt werden.
- IPsec Tunnel erlauben keine Weiterleitung von Multicast-Paketen.

Site to Site (Tunnel-Mode):



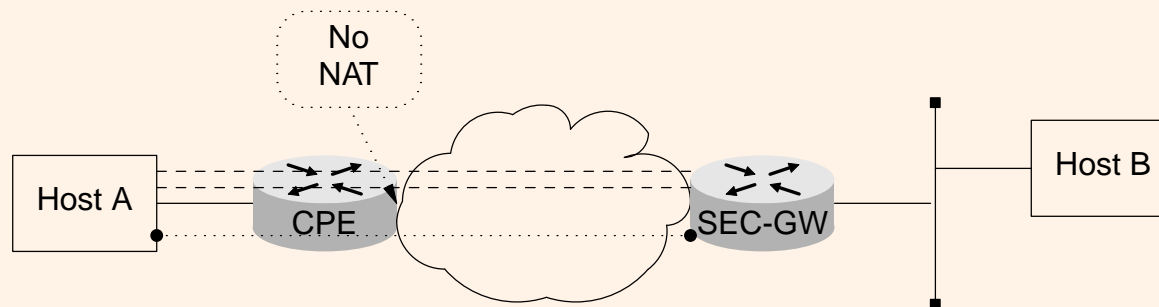
Original Paket: | IPhdr | TCP/UDP-hdr | data |

AH-Tunnel: | GW-IPhdr[51] | AH | IPhdr | TCP/UDP-hdr | data |

ESP-Tunnel: | GW-IPhdr[50] | ESP | IPhdr | TCP/UDP-hdr | data | ESP-Trailer | Auth |

IPsec Transport/Tunnel Mode

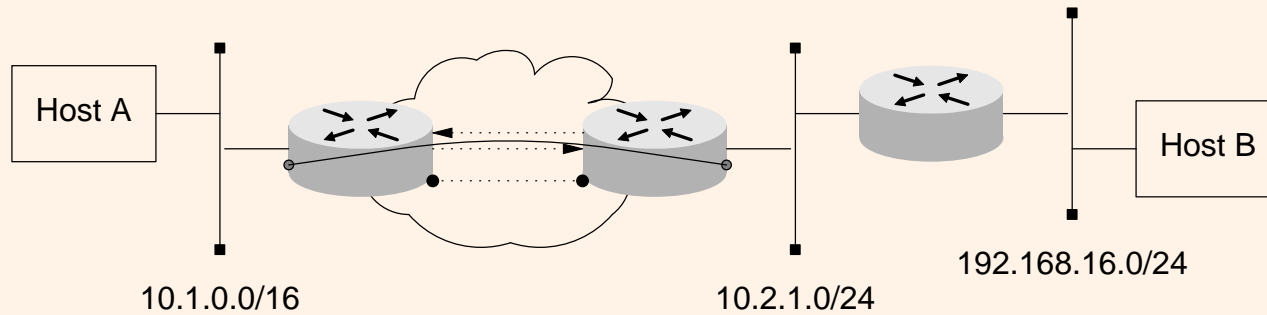
Host to Site (Tunnel-Mode)
Road Warrior:



- IP-Adresse des Hosts am Gateway nicht konfigurierbar.
- Verbindungsaufbau nur einseitig möglich (host \Rightarrow IPsec-GW)
- Hostauthentisierung in der Regel über Zertifikate.
- Evtl. Benutzerauthentisierung über XAUTH (Hybrid Mode).

IPsec Transport/Tunnel Mode (2)

Site to Site (IPsec Transport-Mode plus GRE-Tunnel):



- Erlaubt beliebige Transport-Protokolle, auch Multicasting.
- Erlaubt dynamisches Routing (einfachere Policy).
- Dynamisches Routing ermöglicht Redundanzkonzept.

IPsec Transport/Tunnel Mode (3)

Transport Mode wird im wesentlichen in Host Umgebungen verwendet.
Tunnel-Mode wird von Security Gateways verwendet.

	Transport-Mode	Tunnel-Mode
AH	schützt IP-Header + Upper-Layer-Protokoll	schützt Outer + Inner IP-Header + Upper-Layer-Protokoll
ESP	schützt Upper-Layer-Protocol verschl. Upper-Layer-Protokoll	schützt Inner IP-Header verschl. Inner IP-Header + Upper-Layer-Protokoll
AH+ESP	schützt IP-Header verschl. Upper-Layer-Protokoll	

IPsec stellt nicht die Erreichbarkeit der Gegenseite sicher.

Ist die Gegenseite neu gestartet worden, kann es zu Situationen kommen, in denen der Datenverkehr im Tunnel "verschwindet" (black hole)!

IPsec Implementierungen

- Cisco 7100, VPN3000, VPN5000, PIX, IOS+3DES
IKE, Zertifikate **müssen** über SCEP geladen werden.
- Cosine
- Checkpoint Firewall-1/VPN-1
- Solaris Version 8 hat **kein** Keymanagement, Solaris 9 wird das IKE-Toolkit. von ssh.fi verwenden.
- Linux (FreeSwan)
nur 3DES, kein AH-only, IKE kann nur shared Keys und RSA-Sig, Zertifikate in Beta Stadium, rudimentäre SPD, erste KINK Implementierung(?).
- W2K
Vollständige IPsec-Integration inkl. Schlüsselmanagement (Kerberos) und Policymanagement (Active Directory).
- OpenBSD
Referenzimplementierung für IPsec-Testbed (www.VPNC.org).

Fazit

- IPsec deckt ein weites Anwendungsfeld ab:
Differenzierte Problembetrachtung notwendig.
 - Ideal für Host based Security:
Policy- und Schlüsselmanagement noch nicht gelöst.
 - Sehr gut für Road Warrior:
Lediglich Zertifikatsverwaltung muß sichergestellt werden.
 - VPN Gateway:
Redundanz- und Performanceprobleme bei grossen Implementierungen.
- IPsec stellt eine große Herausforderung dar:
 - Schlüsselmanagement ist nach wie vor schwierig.
 - Rechtliche Einschränkungen möglich.
 - Informationsdefizite müssen abgebaut werden (Schulungen).
- ABER: Definitiv keine Alternative verfügbar

☞ Wer Verschlüsselung auf IP Ebene benötigt kommt an IPsec nicht vorbei.

? ? ?

Anforderungen an Kryptoalgorithmen

Die Anlage vom 22. November 2001 zum Signaturgesetz legt die Kryptoalgorithmen fest, die bis Ende 2007 als geeignet für digitale Signaturen anzusehen sind.

Hashfunktionen

- RIPEMD-160
- SHA-1

Signaturalgorithmen

- RSA
- DSA
- DSA-Varianten basierend auf elliptischen Kurven
 - EC-DSA
 - EC-KDSA, EC-GDSA
 - Nyberg-Rueppel Signaturen

Anforderungen an Kryptoalgorithmen(2)

Algo.	minimale Bitlänge		
	bis Ende 2005	bis Ende 2006	bis Ende 2007
RSA			
n	1024	1024 (Minimum) 2048 (Empfohlen)	1280 (Minimum) 2048 (Empfohlen)
DSA			
p	1024	1024 (Minimum) 2048 (Empfohlen)	1280 (Minimum) 2048 (Empfohlen)
q	160	160	160
DSA-Varianten basierend auf elliptischen Kurven			
p	192	192	192
q	160	160	180
m	191	191	191
q	160	160	180

CONTENTS

IPsec Entwicklungshintergrund	2
Lösungsansätze	3
IPsec Protokoll	4
IPsec Protokoll (Aufbau)	5
IPsec AH	6
IPsec ESP	7
Security Policy Database	8
Security Association	9
Schlüsselverwaltung	10
Internet Key Exchange (IKE)	11
IPsec Transport-Mode	12
IPsec Tunnel-Mode	13
IPsec Transport/Tunnel Mode	14
IPsec Transport/Tunnel Mode (2)	15
IPsec Transport/Tunnel Mode (3)	16
IPsec Implementierungen	17
Fazit	18
.....	19
Anforderungen an Kryptoalgorithmen	20
Anforderungen an Kryptoalgorithmen(2)	21