

IPSec

Stephan Eckner
stephan@eckner.org

12. Dezember 2001

Überblick

- Verschlüsselung von Netzverkehr
 - Verschlüsselung auf Anwendungsebene
 - Verschlüsselung auf Linkebene
 - Verschlüsselung auf IP- Ebene
- IPSec im Einzelnen
 - Authentication Header (AH)
 - Encapsulating Security Payload (ESP)
 - Transport Mode
 - Tunnel Mode
- IPSec in action
 - Security Parameter Index (SPI)
 - Security Association (SA)/ SA Database (SAD)
 - Security Policy Database (SPD)
 - Inbound Processing
 - Outbound Processing

Überblick

- IKE
 - Phase I
 - Phase II
- Anwendungsszenarien
 - VPN (Virtuelle Private Netze)
 - „Road Warriors”
- Interoperabilität, Performanz, Troubleshooting
 - Interoperabilität
 - Performanz
 - Troubleshooting
- Links und Literatur

Verschlüsselung von Netzverkehr

- Verschlüsselung auf Anwendungsebene
 - TLS/SSL
 - SSH
 - PGP, S/MIME
- anwendungsspezifisch, insbesondere *nicht transparent*
- Vertrauensbeziehung zwischen User-Level Programmen

Verschlüsselung von Netzverkehr

- Verschlüsselung auf Linkebene
 - ISDN-Krypto-Router
 - PPTP (?)
- transparent
- kann nicht geroutet werden

Verschlüsselung von Netzverkehr

- Verschlüsselung auf IP-Ebene
 - IPSec
- transparent
- kann geroutet werden
- problemlose Koexistenz mit unverschlüsseltem IP-Traffic

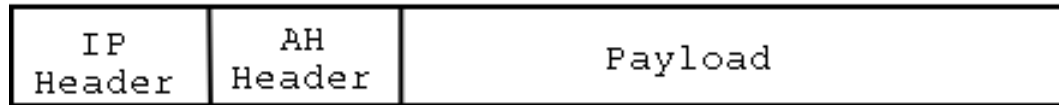
Überblick

- Verschlüsselung von Netzverkehr
- **IPSec im Einzelnen**
- IPSec in action
- IKE
- Anwendungsszenarien
- Interoperabilität, Performanz, Troubleshooting
- Links und Literatur

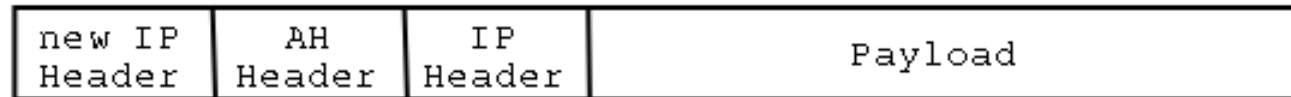
IPSec im Einzelnen

- AH (Authentication Header) – RFC 2402
 - Authentisierung von IP Paketen
- ESP (Encapsulating Security Payload) – RFC 2406
 - Authentisierung und Verschlüsselung von IP Paketen
- Transport Mode
 - AH bzw. ESP wird nur auf die Payload des IP Paketes angewendet
- Tunnel Mode
 - AH bzw. ESP wird auf das gesamte IP Paket angewendet

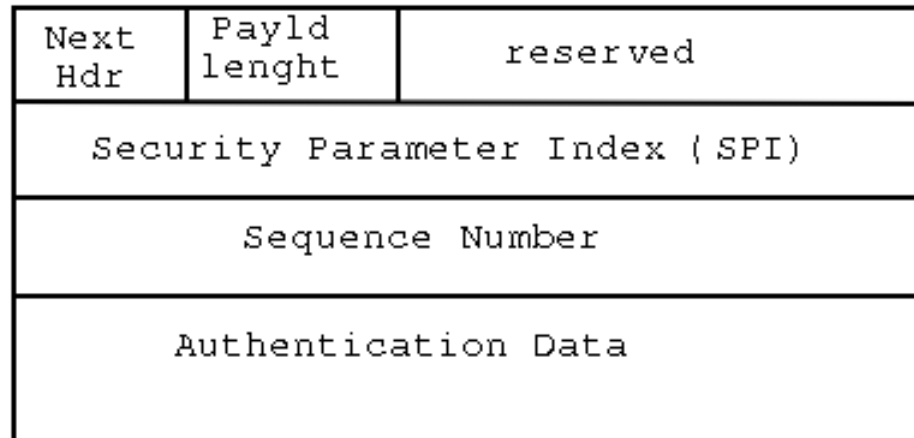
AH (Authentication Header)



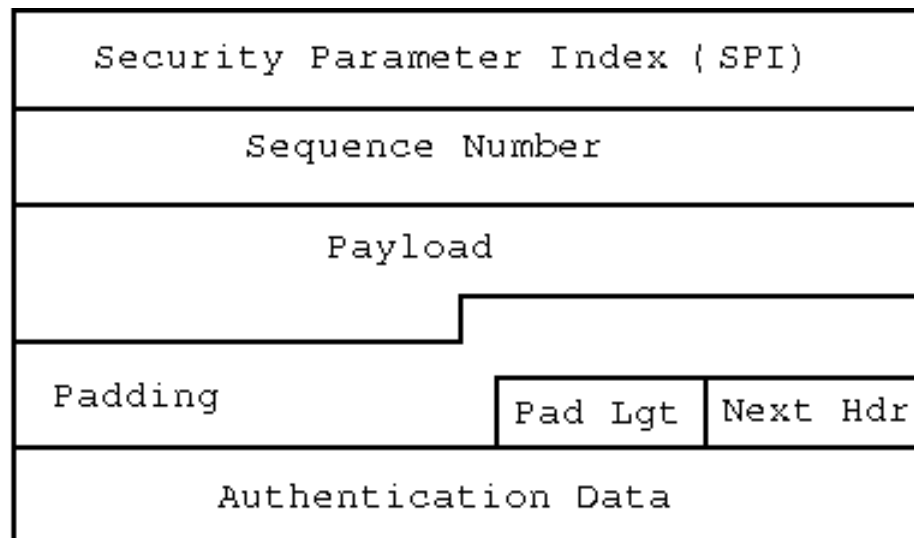
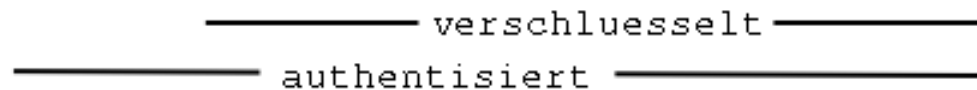
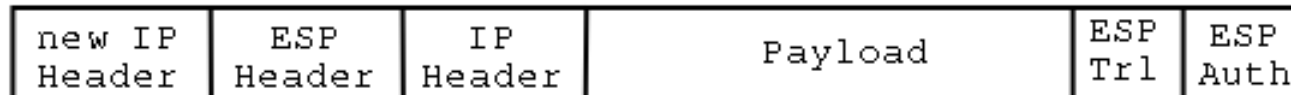
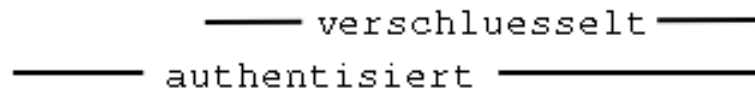
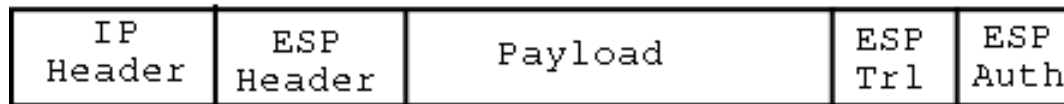
authentisiert



authentisiert



ESP (Encapsulating Security Payload)



IPSec im Einzelnen

- ESP Transport Mode versus ESP Tunnel Mode
 - Ursprüngliche Idee:
 - * Transport Mode für Peer-to-Peer Verschlüsselung
 - * Tunnel Mode für Netz-zu-Netz Verschlüsselung
 - IP-Header ist im Transport-Mode nicht authentisiert => AH Protokoll
 - Problem: zusätzliche Komplexität von AH, sowohl Konfiguration als auch Implementierung
 - daher: Tunnel Mode für Netz-zu-Netz *und* Peer-to-Peer
- Fazit: **Wenn IPSec, dann ESP im Tunnel Modus**

Überblick

- Verschlüsselung von Netzverkehr
- IPSec im Einzelnen
- **IPSec in action**
- IKE
- Anwendungsszenarien
- Interoperabilität, Performanz, Troubleshooting
- Links und Literatur

IPSec in action – SPD

- Die eigentliche (vom Admin definierbare) Konfiguration
- Mit welchen Peers kommuniziere ich verschlüsselt/unverschlüsselt/gar nicht?
- Wie authentisieren wir uns gegenseitig beim Verbindungsaufbau
 - PreShared Secret (PSK)
 - Digitale Signatur (DSS und RSA) (u.a. X.509 Zertifikate)
 - Public Key Encryption (RSA und revised RSA) (u.a. X.509 Zertifikate)
- Welche Algorithmen benutzen wir zur Verschlüsselung und Authentisierung der Pakete
- Welchen Traffic verschlüsseln wir (zB nur port 53 etc.)

IPSec in action – SA/SAD

- Security Association (SA) = Menge aller momentan benötigten Krypto-Parameter
 - SA's sind unidirektional
 - Je zwei SA's pro Verbindung
- SAD = interne Datenbank (im Kernel) von SA's
- Tripel <SPI, dest, protocol> legt Eintrag eindeutig fest
- Krypto-Parameter
 - werden bei Verbindungsaufbau mittels IKE automatisch erzeugt, oder
 - können manuell festgelegt werden (nicht empfehlenswert)
- via IKE erzeugte SA's haben endliche Lebensdauer
 - IKE führt vor Ablauf automatisch neuen Key-Exchange durch

IPSec in action – SPI

- 32 Bit Wert
- SPI wird im Klartext mit jedem Paket übermittelt
- Index, anhand dessen die Peers auf ihre internen Krypto-Parameter zugreifen
- Wird beim Verbindungsaufbau vereinbart

IPSec in action – Inbound Processing

Ein IP Paket wird empfangen:

1. Konsultiere SPD anhand Source-Address
 - (a) Paket wird gedropt
 - (b) Paket wird direkt dem IP-Stack übergeben
 - (c) Paket wird IPSec-Processing übergeben
2. Falls (c), lese SPI und suche in SAD nach den entsprechenden Krypto Parametern
3. Existiert ein SAD Eintrag, entschlüssele Paket
4. Existiert kein Eintrag \Rightarrow Paket wird gedropt

IPSec in action – Outbound Processing

Ein IP Paket wird gesendet:

1. Konsultiere SPD anhand Destination-Address
 - (a) Paket wird direkt dem IP-Stack übergeben
 - (b) Paket wird IPSec-Processing übergeben
2. Falls (b), lese SPI und suche in SAD nach den entsprechenden Krypto Parametern
3. Existiert ein SAD Eintrag, verschlüssele Paket
4. Existiert kein Eintrag \Rightarrow Internet Key Exchange wird gestartet

Überblick

- Verschlüsselung von Netzverkehr
- IPSec im Einzelnen
- IPSec in action
- **IKE**
- Anwendungsszenarien
- Interoperabilität, Performanz, Troubleshooting
- Links und Literatur

IKE – Überblick

- ISAKMP (Internet Security Association and Key Management Protocol) – RFC 2408
 - allgemeines Protokoll zur Aushandlung/Modifizierung/Löschung von Security Parametern
- Oakley Key Determination Protocol – RFC 2412
 - Protokoll zum Austausch von kryptographischen Schlüsseln über ungeschützte Netze
- IKE (Internet Key Exchange) – RFC 2409
 - Protokoll zum Austausch von Schlüsseln und Aushandlung von Security Parametern – bunte Mischung aus ISAKMP und Oakley

IKE – Überblick

- IKE besteht aus 2 Phasen
- Phase I:
 - 'Main Mode' oder 'Aggressive Mode'
 - Peers erzeugen verschlüsselten und authentisierten Tunnel
 - via Diffie-Hellman Protokoll wird gemeinsamer geheimer Schlüssel (Master Secret) erzeugt
 - Beide Peers authentisieren sich gegenseitig
- Phase II:
 - 'Quick Mode'
 - Aushandlung von Security Associations (i.e. Krypto Parameter) für die IPSec Verbindung
- Die in Phase I ausgehandelten Kryptoparameter schützen die Phase II Exchange (auch mehrere)

IKE – Diffie-Hellman Algorithmus

- 'erster' Public-Key-Algorithmus
- Ermöglicht Erzeugung eines gemeinsamen geheimen Schlüssels trotz Kommunikation über unsichere Kanäle
- Hintergrund: Sei $x = c^a \bmod n$, dann kann aus x und c nicht a errechnet werden
- Algorithmus:
 - A und B einigen sich auf Modulus n und Basis c
 - A wählt Exponent a und berechnet $x = c^a \bmod n$
 - B wählt Exponent b und berechnet $y = c^b \bmod n$
 - A und B übermitteln x und y (aus denen ein Angreifer nicht a oder b berechnen kann, s.o.)
 - A berechnet $y^a = (c^b)^a \bmod n = e$
 - B berechnet $x^b = (c^a)^b \bmod n = e$
 - e ist das gemeinsame Geheimnis von A und B

IKE – Phase I, Main Mode

- Message 1: A schlägt B mehrere Diffie-Hellman Parameter, Verschlüsselungs- und Authentisierungsalgorithmen vor und sendet Initiator-Cookie
- Message 2: B wählt einen Verschlüsselungs- und einen Authentisierungsalgorithmus aus und sendet Responder-Cookie
- Message 3: A sendet c^a und Authentisierungsmaterial (Pseudo-Zufallszahl N_A (Nonce))
- Message 4: B sendet c^b und Authentisierungsmaterial (N_B)
- A und B erzeugen gemeinsamen geheimen Schlüssel aus $e = (c^a)^b$, N_A , und N_B

IKE – Phase I, Main Mode

- Message 5 und 6: A und B authentisieren sich gegenseitig
 - Messages 5 und 6 sind verschlüsselt
 - Authentisierung mittels:
 - PreShared Secret (PSK)
 - Digitale Signatur – RSA oder DSA
 - Public Key Verschlüsselung – RSA oder DSA

IKE – Phase I, Aggressive Mode

- Nur 3 Messages statt 6 im Main Mode
- A sendet c^a gleich in Message 1
- Krypto Parameter können nicht ausgehandelt werden
- Funktioniert nur, wenn vor der Verbindung hinreichende Informationen über den jeweils anderen Peer vorhanden ist
- Einzige Möglichkeit für 'Road Warriors' und PreShared Secret

IKE – Phase II, Quick Mode

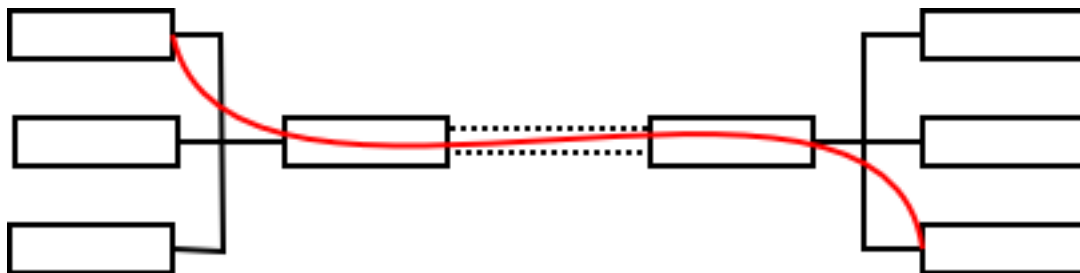
- 3 Messages
- Aushandlung der IPSec Security Associations
- Messages sind verschlüsselt mit dem in Phase I ausgehandelten Schlüssel
- Das Schlüsselmaterial für die IPSec Verschlüsselung wird aus dem in Phase I erzeugten abgeleitet, es sei denn, man benutzt ...
- Perfect Forward Security (PFS)
 - im PFS-Modus werden die IPSec Schlüssel durch einen weiteren Diffie-Hellman Exchange neu erzeugt

Überblick

- Verschlüsselung von Netzverkehr
- IPSec im Einzelnen
- IPSec in action
- IKE
- **Anwendungsszenarien**
- Interoperabilität, Performanz, Troubleshooting
- Links und Literatur

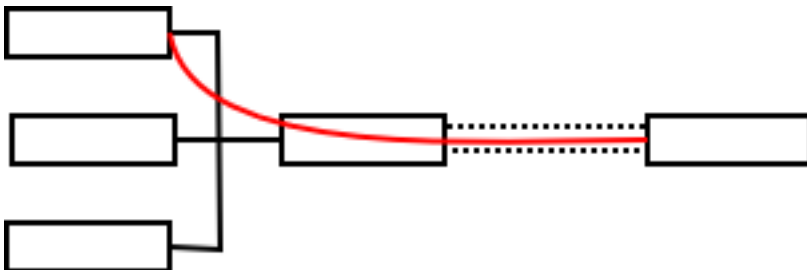
Anwendungsszenarien – VPN

- Verbindung von verschiedenen LAN's
- Transport von nicht routebaren IP-Paketeten über das Internet
- ESP (+ event. AH) im Tunnel Modus



Anwendungsszenarien – Road Warriors

- Anbindung von einzelnen Rechnern an das lokale Netz
- IP-Adresse des Peers nicht bekannt
- ESP (+ event. AH) im Tunnel Modus
- Falls Authentisierung via PreShared Secret \Rightarrow IKE Aggressive Mode Exchange



Anwendungsszenarien – Road Warriors

- Ende-zu-Ende Verschlüsselung
- Problem: Key Management
 - DNSSEC + Weltweite PKI
 - Problem: s. Microsoft Security Bulletin MS01-017 vom 22.03.01
- Problem: Masquerading und Firewalls

Überblick

- Verschlüsselung von Netzverkehr
- IPSec im Einzelnen
- IPSec in action
- IKE
- Anwendungsszenarien
- **Interoperabilität, Performanz, Troubleshooting**
- Links und Literatur

Interoperabilität

- Getestet:
 - Linux – Win2k (GPI)
 - Linux – Cisco (ULU)
 - Linux – OpenBSD (SEC)
- <http://www.vpnc.org/conformance.html>
 - testet 'Konformität' von proprietären VPN Produkten
 - Unter 'Konformität' wird Interoperabilität mit KAME Implementierung unter OpenBSD und OpenBSD's isakmpd verstanden

Performanz

- Hardware: AMD K6 3D, 500 MHz, 64 MB RAM, Intel Etherpro 100
- Freeswan 1.8, Kernel 2.2.18, 3DES-MD5:
 - 10 MBit/s
 - Belastungstest (57 GB übertragen) 9 MBit/s
- OpenBSD 2.8 3DES-MD5:
 - 6 MBit/s
- OpenBSD 2.8 Blowfish-MD5:
 - 9 MBit/s

Troubleshooting

- Firewall-Konfiguration:
 - udp Source und Destination Port 500 für IKE
 - IP Protokoll 50 für ESP
 - IP Protokoll 51 für AH
- Probleme mit Fragmentierung
- MTU Path-Recovery nicht möglich

Überblick

- Verschlüsselung von Netzverkehr
- IPSec im Einzelnen
- IPSec in action
- IKE
- Anwendungsszenarien
- Interoperabilität, Performanz, Troubleshooting
- **Links und Literatur**

Links und Literatur – RFC's

- RFC 2401 – Security Architecture for the Internet Protocol
- RFC 2402 – IP 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 – IP Encapsulating Security Payload (ESP)
- RFC 2407 – The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 – Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 – The 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

Links und Literatur – Bücher

- „IPSec – The New Security Standard for the Internet, Intranets and VPN's” *Naganand Doraswamy, Dan Harkins*, Prentice Hall, Aug. 1999
 - Beides RFC-Autoren ⇒ Das Buch ist genauso schlecht geschrieben wie die RFC's
- „A Guide to Virtual Private Networks” *Murhammer, Bourne et al.*, Prentice Hall, 1998
 - IBM Redbook, gefällt mir recht gut
- „Implementing IPsec” *Elizabeth Kaufman, Andrew Newman*, Wiley, Sept. 1999
 - Hab ich nur kurz überflogen, machte guten Eindruck
- „A technical Guide to IPSec VPN's” *James S. Tiller, Jim S. Tiller*, Auerbach Pulications, Dez. 2000
 - Kenn ich nicht, hat das höchste Rating bei amazon

Links und Literatur – FreeSWAN, OpenBSD

- http://www.freeswan.org/freeswan_trees/freeswan-1.8/doc/index.html
 - aktuelle FreeSWAN Dokumentation
- <http://www.openbsd.org/faq/faq13.html>
 - IPsec Kapitel des OpenBSD FAQ's
- <http://www.secureops.com/vpn/ipsecvpn.html>
 - Guter Überblick über Sinn und Einsatzszenarien von IPsec VPN's
- <http://www.secureops.com/vpn/vpn.html>
 - Gute Einführung in die Realisierung eines IPsec VPN's unter OpenBSD
- <http://www.counterpane.com/ipsec/>
 - His Masters Voice – Bruce Schneiers Kryptographische Analyse der IPsec Protokolle
- <http://www.eckner.org/>