FreeS/WAN – IPsec mit Linux

Hans-Jörg Höxer
<Hans-Joerg.Hoexer@yerbouti.franken.de>

25. November 2001

Überblick

- Die Sicherheitsarchitektur für das Internet – IPsec.
- IPsec für GNU/Linux – FreeS/WAN.
- Anwendungsmöglichkeiten.

Anforderungen an Kommunikation

- Geheimhaltung.
- Integrität.
- Authentifizierung.
- Wiederholungsschutz.

IPv4 entspricht nicht diesen Kriterien.

Die Sicherheitsarchitektur für das Internet – IPsec

Komponenten der Sicherheitsarchitektur:

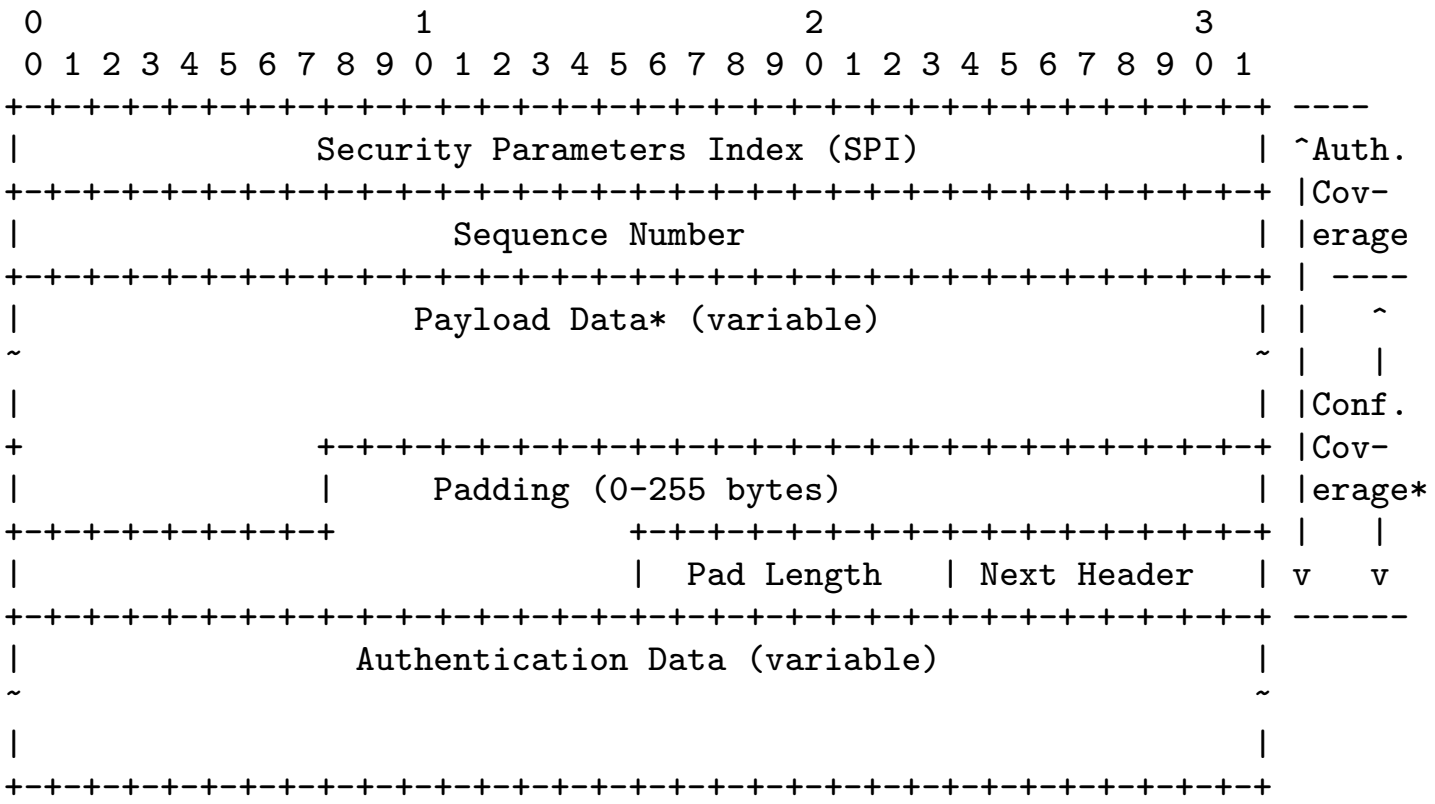
- Kryptographische Algorithmen.
- Sicherheitsprotokolle für IPv4 und IPv6 – ESP und AH.
- Sicherheitsassoziationen.
- Schlüssel- und Parameterverwaltung – ISAKMP/IKE oder Photuris.

“Encapsulating Security Payload” – ESP (50)

Dieses Sicherheitsprotokoll (RFC 2406) bietet:

- Verschlüsselung für Nutzlast: DES, 3DES und NULL.
- Authentifizierung für Nutzlast und ESP Präambel: HMAC mit MD5 oder SHA1.
- Wiederholungsschutz (“Replay Protection”).

ESP



Schlüsselgrössen für ESP im CBC-Modus

Algorithmus	Key Size (bits)	Popular Sizes	Default
CAST-128	40 to 128	40, 64, 80, 128	128
RC5	40 to 2048	40, 128, 160	128
IDEA	128	128	128
Blowfish	40 to 448	128	128
3DES	192	192	192
DES	64	64	64

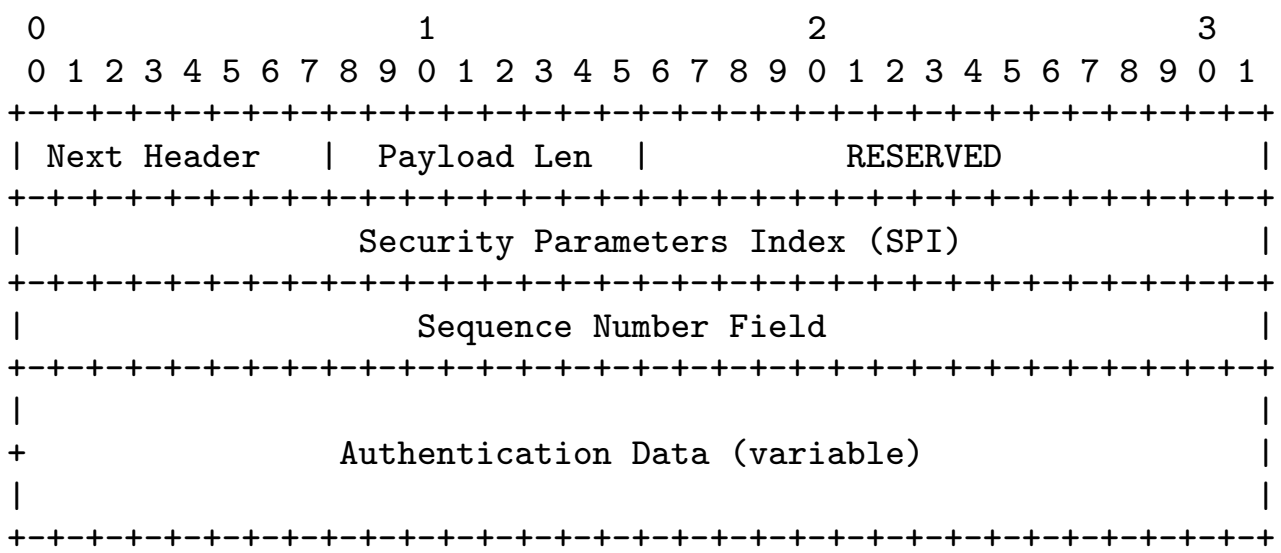
“Authentication Header” – AH (51)

Dieses Sicherheitsprotokoll (RFC 2402) bietet:

- Authentifizierung für Nutzlast, AH Präambel und *Teile der IP Präambel*: HMAC mit MD5 oder SHA1.

- Wiederholungsschutz (“Replay Protection”).

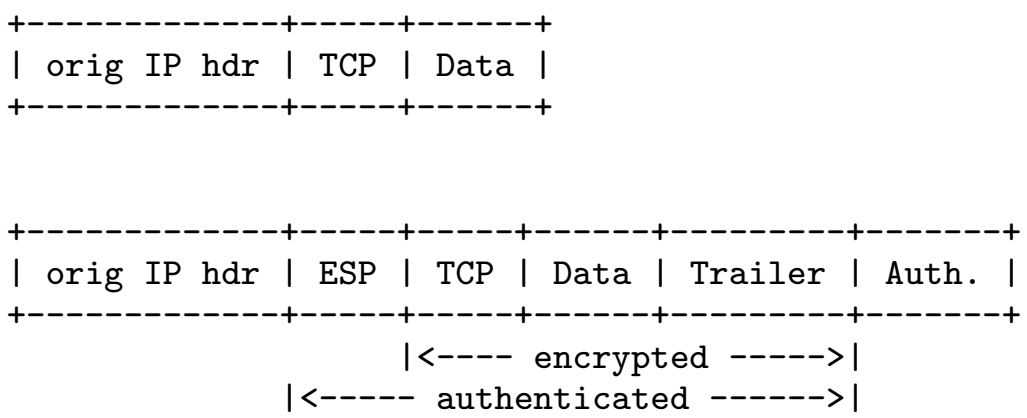
AH



Tunnelmodus versus Transportmodus 1

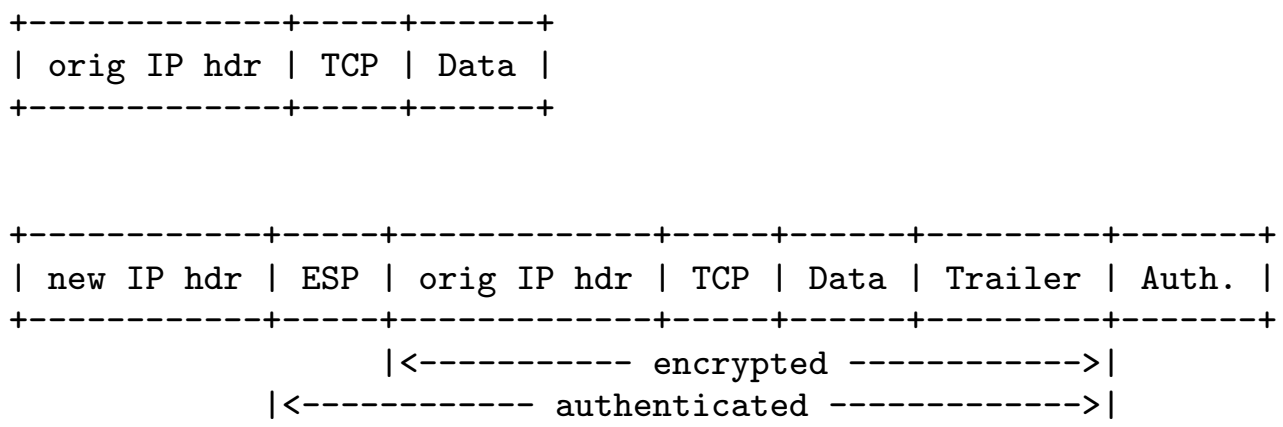
IPsec Protokolle können in zwei verschiedenen Modi genutzt werden:

- Transportmodus:



Tunnelmodus versus Transportmodus 2

- Tunnelmodus:



ISAKMP/IKE

Ablauf in zwei Phasen:

- Aushandeln einer SA für IKE – Main Mode.
  → Authentifizierung über preshared secrets oder public keys.

- Aushandeln von IPsec SAs – Quick Mode.
  → Erzeugen symmetrischer session keys.

FreeS/WAN – IPsec für Linux

- Patch für den Linuxkern.
- KLIPS – Kernel IP Security.
- Pluto – IKE Dämon.
- Zahlreiche Skripten zur Administration.
- Photuris als sichere Alternative zu ISAKMP/IKE (experimentell).

Unterstützte Algorithmen

- 3DES.
- *kein* DES und NULL.
- MD5-HMAC und SHA1-HMAC.
- Kompression.

Konfiguration

- Beschreibung des Verbindungen: `/etc/ipsec.conf`
- Shared secrets und RSA keys: `/etc/ipsec.secrets`
- X509 Zertifikate (optional): `/etc/ipsec.d/<certs>`

Anwendungen – VPN

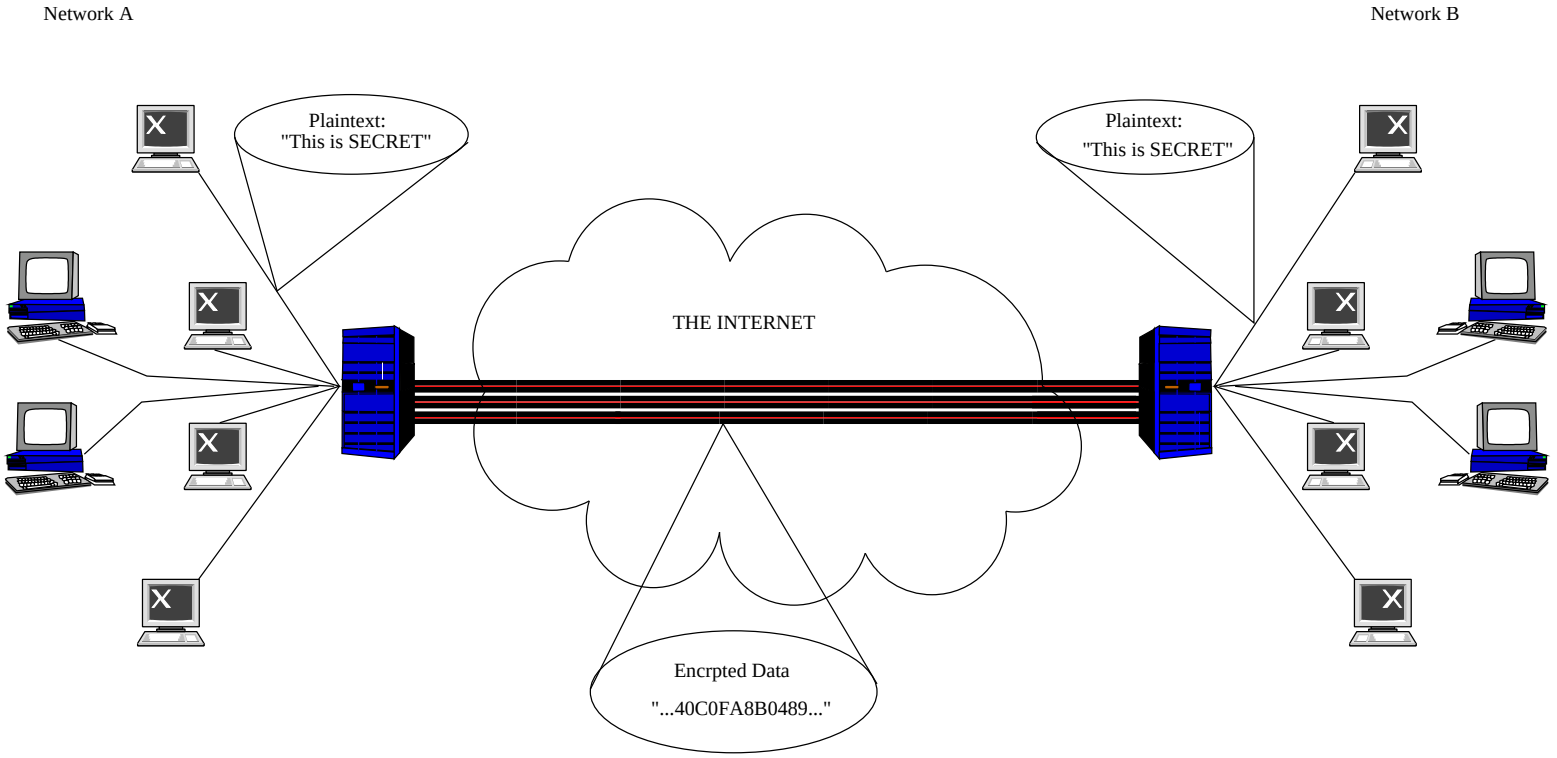
Virtual Private Network:

- Kommunikation zwischen zwei Netzwerken über ein unsicheres drittes.
- Datenfluß zwischen Gateways ist verschlüsselt und authentifiziert – IPsec Tunnel.
- Zwei Netzwerke erscheinen als ein Netzwerk.

ipsec.conf

```
conn VPN
     auto=start
     type=tunnel
     left=131.188.31.48
     leftsubnet=192.168.2.0/24
     right=131.188.31.39
     rightsubnet=192.168.3.0/24
     keyexchange=ike
     ikelifetime=1h
     keylife=10m
     rekeymargin=1m
     rekeyfuzz=25%
```

Ein VPN

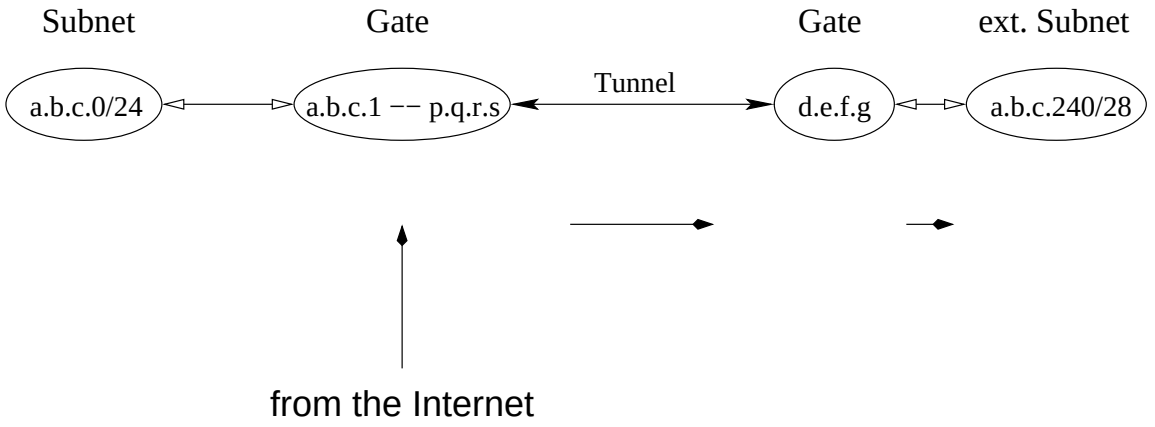


Anwendungen – “Road Warrior”

- Maschine mit dynamischer IP – “Road Warrior”.
- Heimat Gateway mit fester IP.
- IPsec Tunnel zwischen beiden Maschinen.
- Authentifizierung mittels Public–Key–Verfahren.

Anwendungen – “Extruded Subnet”

- Ausgliederung eines Subnetzes.
- Statische IP trotz dynamischer Verbingung möglich (DSL).



“Opportunistic Encryption” mit FreeS/WAN

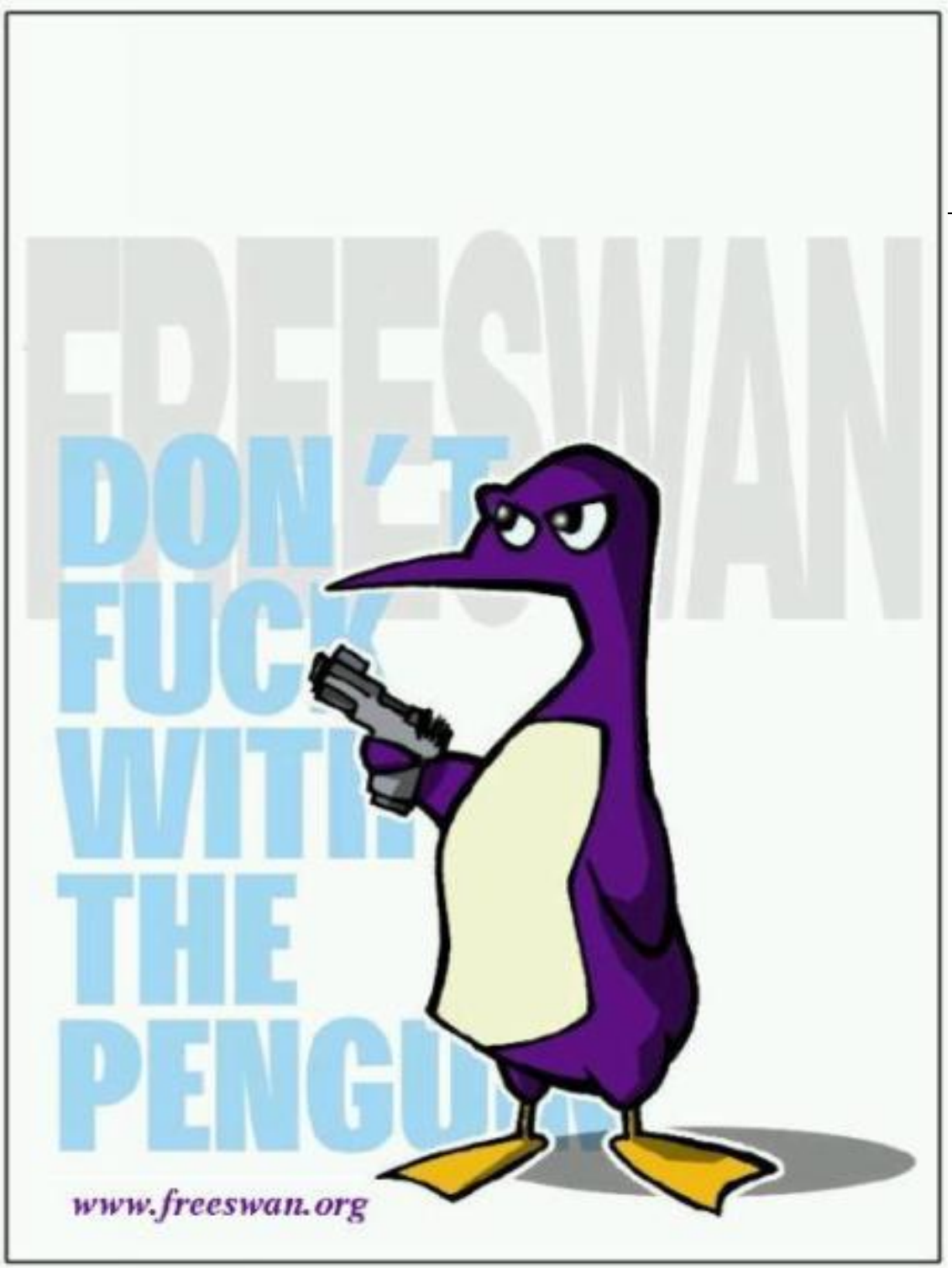
- Beliebige Maschinen können miteinander IPsec Verbindungen etablieren.
- Public–Keys werden über DNS verteilt:
  - TXT record.
  - DNSSEC.
- Problem: Verwendeter DNS Mechanismus ist *nicht* vollständig vertrauenswürdig.

Ausblick

- KLIPS Redesign: Netfilter vs. MAST-Device.
- X509 für Pluto.
- Integration von Photuris.
- Unterstützung von IPv6.
- AES/Rijndael.

URLs

- http://www.freeswan.org
- http://www.linux-ipv6.org
- http://wwwcip.informatik.uni-erlangen.de/~hshoexer



Fragen?