IPsec basierte VPNs: Frei verfügbare Lösungen und aktuelle Weiterentwicklungen

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

23. November 2003

Überblick

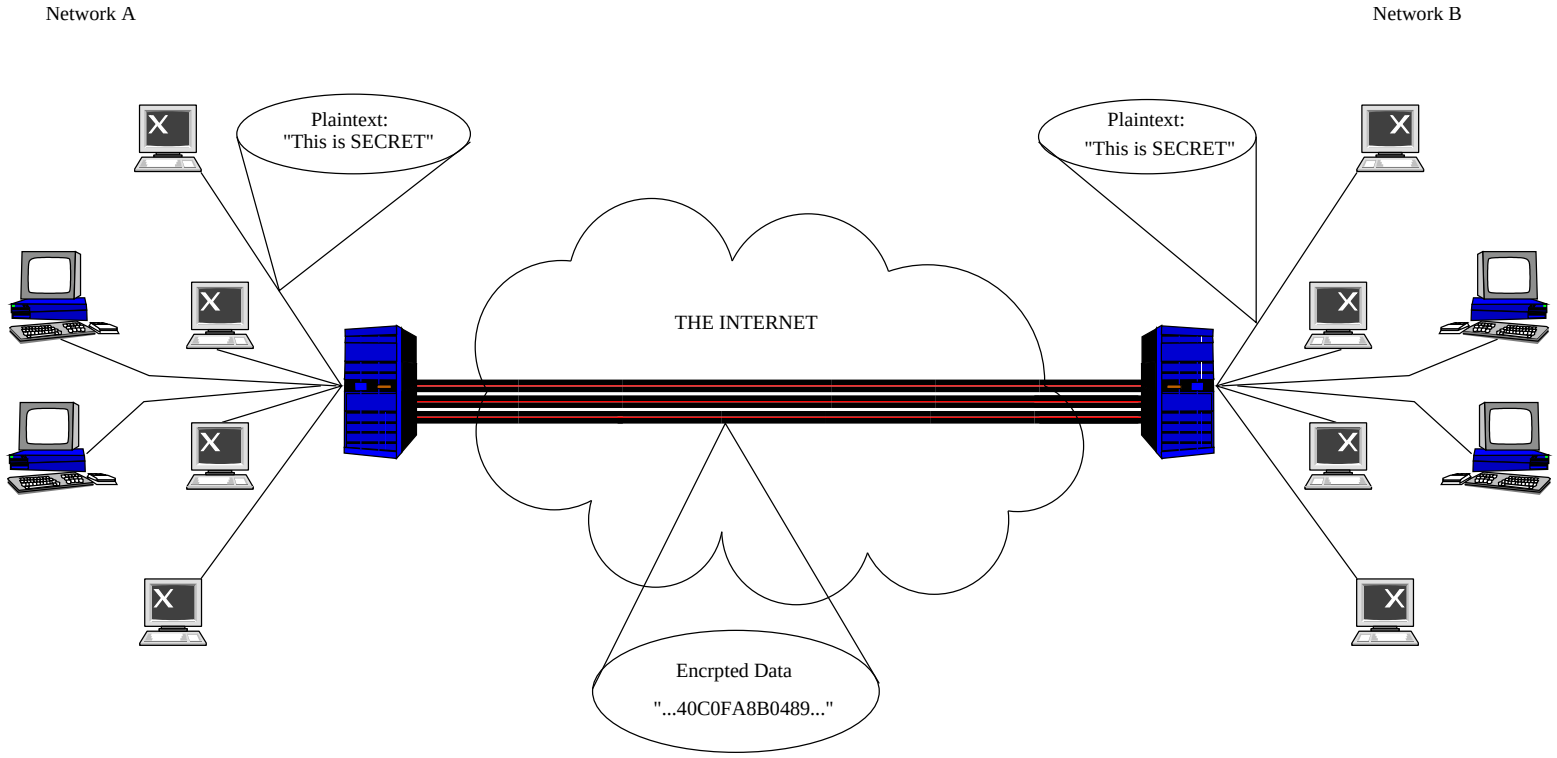
- VPN Grundlagen
- Einführung IPsec
- Verfügbare Implementierungen
- Alternativen zu IPsec
- Aktuelle Weiterentwicklungen

VPN Grundlagen – 1

“A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.”

- Verbindung von Subnetzen über das Internet
- Jedes Subnetz besitzt ein Gateway
- Gateways sind untereinander mit “Tunnels” verbunden
- Tunnels verschlüsseln und authentisieren Datenübertragung

VPN Grundlagen – 2



VPN Grundlagen – 3

Typische Anwendungen von VPNs:

- Verbindung von Netzwerken an verschiedenen Standorten
- “Roadwarrior”: Mobiler- bzw. Dial-Up-User verbindet sich zu Heimatnetz
- Absichern von WLAN-Netzen
- “Extruded subnets”: Tunneln statischer Adressen zu dynamischen

VPN Grundlagen – 4

Tunnel von IP-Paketen: IP-Pakete werden in andere Pakete gekapselt (“encapsulation”).

- IP-ENCAP (4), IPIP (94)
- TCP (6), UDP (17), ESP (50)
- PPP über SSH
- aber auch: DNS, HTTP, etc.

Probleme: MTU sinkt, Fragmentierung

Einführung IPsec – 1

Anforderungen an Kommunikation:

- Geheimhaltung
- Integrität
- Authentifizierung
- Wiederholungsschutz

IPv4 entspricht nicht diesen Kriterien.

Einführung IPsec – 2

Komponenten:

- Kryptographische Algorithmen
- Sicherheitsprotokolle für IPv4 und IPv6 – ESP und AH.
- Sicherheitsassoziationen
- Schlüssel- und Parameterverwaltung – automatisch mit ISAKMP/IKE oder manuell
- Kommunikation Kern/Userspace über `PF_KEY`-Socket

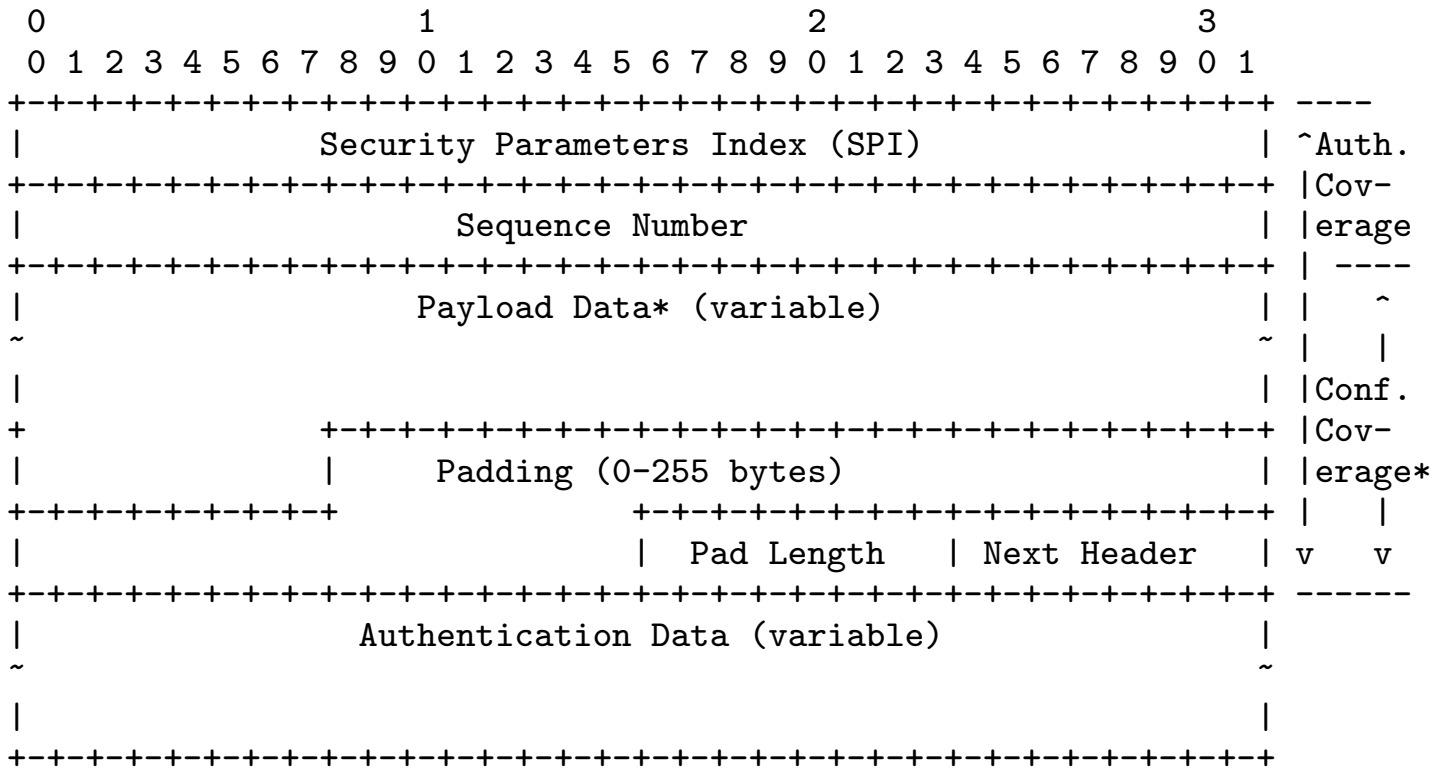
Einführung IPsec – 3

“Encapsulating Security Payload” – ESP (50):

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

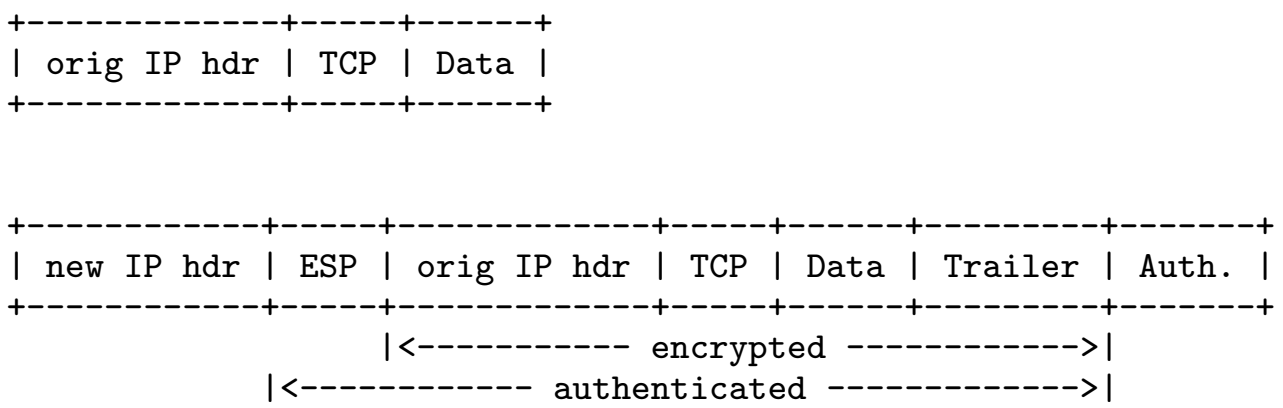
Einführung IPsec – 4

ESP Paketformat:



Einführung IPsec – 5

- Tunnelmodus:



- Overhead (ca.): 20 Byte + 8 Byte + 20 Byte = 48 Byte

Verfügbare freie Implementierungen

Für alle gängigen Betriebssyteme ist IPsec verfügbar:

- Linux: FreeS/WAN (ab Kern 2.2), USAGI und nativ (ab Kern 2.5.x)
- OpenBSD: nativ
- NetBSD/FreeBSD: KAME Stack
- MacOS X: native bzw. KAME Stack (?)
- Windows 95, 98 und Me: PGPNet (PGP-Freeware)

Linux FreeS/WAN – 1

Ziel des Projekts:

John Gilmore: “My project for 1996 was to secure 5% of the Internet traffic against passive wiretapping. It didn’t happen in 1996, so I’m still working on it in 1999! If we get 5% in 1999 or 2000, we can secure 20% the next year, against both active and passive attacks; and 80% the following year.”

→ Gute Idee!

Linux FreeS/WAN – 2

FreeS/WAN war erste IPsec Implementation für Linux:

- GPL
- KLIPS Kernel Patch
- ISAKMP/IKE-Dämon `pluto`
- Keine Unterstützung von X509-Zertifikaten (Patch existiert)
- Besonderheit: “Opportunistic Encryption”

Linux FreeS/WAN – 3

Probleme:

- Entwicklerteam ist zu pragmatisch (bzw. einfach stur)
- Schlechte Kooperation mit Kernelentwicklern
- Schlechte Kooperation mit anderen Entwicklern
- Teils unschöner Code
- Für sinnvolle Anwendungen sind Patches nötig (Super-FreeS/WAN)

→ Keine Übernahme von FreeS/WAN in den Linux-Kern

USAGI-Projekt – 1

USAGI (UniverSAl playGround for Ipv6):

- Fokus ist IPv6 für Linux basierte Systeme
- IPv6 und IPsec (IPv6 und IPv4) für den Linux-Kern
- Volle IPv6-Unterstützung für das User-Land
- Kooperation mit den KAME, WIDE und TAHI Projekten

USAGI-Problem – 2

Probleme:

- Nur langsame Integration von USAGI-Patches in den Linux-Kern
- Keine Kompatibilität mit FreeS/WAN

Vorteile:

- Portierung der KAME IPsec-Utilities
- `racoon` ISAKMP/IKE-Dämon
- `setkey` für manuelles Keying

IPsec für Linux 2.6 – 1

Der Linux-Kern 2.6 hat (endlich) eigene IPsec Implementierung:

- “from scratch” neu geschrieben
- Für IPv4 und IPv6
- Bietet Standardschnittstelle `PF_KEY` und zusätzlich eine eigene Schnittstelle
- Noch “Baustelle”, aber schon funktionsfähig!

IPsec für Linux 2.6 – 2

Utilities und Dämon anderer Systeme wurden portiert:

- `pluto` – FreeS/WAN unterstützt auch Linux 2.6
- `racoon` – KAME/USAGI
- `isakmpd` – OpenBSD
- `setkey`-Utility

→ IPsec für linux 2.6 ist vielversprechend!

KAME IPsec und IPv6 für Net-/FreeBSD

KAME-Protokollstack:

- IPv6 für *BSD
- IPsec für IPv4 und IPv6
- KAME-Stack ist in Net-/FreeBSD fest integriert
- `racoon` als ISAKMP/IKE-Dämon
- `setkey` für manuelle Verwaltung

IPsec bei OpenBSD

OpenBSD besitzt eigene vollständige IPsec-Implementierung:

- `ipsecadm` für manuelle Verwaltung
- `isakmpd` als ISAKMP/IKE-Dämon
- `isakmpd` läuft auch auf zahlreichen anderen Systemen
- Dient VPNC als Referenz-Implementierung
- Abgleich mit KAME (Entwickler arbeiten teils an beiden Projekten)

MacOS X

Keine persönlichen Erfahrungen `:-(`

- KAME-Implementierung seit MacOS X 10.2 (Codename Jaguar) integriert
- `isakmpd` und `racoon` laufen
- Es sollte also alles gehen `:-)`

Windows 95, 98 und ME

Nur Third-Party-Implementierungen; kostenloser Client PGPNet:

- PGPNet ist in PGP-Freeware enthalten
- nur beschränkt einsetzbar (nur Host-to-Host)
- Unterstützung von X509-Zertifikaten
- Hinreichend für Roadwarrior-Szenarien
- Kostenpflichtige Vollversion “PGP Desktop Security”

(Windows XP und 2000 verfügen nativ über IPsec)

Freie Implementierungen – Interoperabilität

- IPsec ist IETF-Standard
- Anfänglich Interoperabilitätsprobleme (meist IKE) behoben
- Ich habe erfolgreich getestet: Linux (FreeS/WAN, 2.6), {Free,Net,Open}BSD, Windows {98,Me} mit PGPNet (und Windows 2000/XP)

→ IPsec als allgemeine Basis für VPNs geeignet

Alternativen zu IPsec – 1

IPsec hat Schwächen:

- Komplexität (zahlreiche RFCs)
- “Kann zu viel!”
- (vermeidbar) Sicherheitsprobleme – Aggressive Mode, DoS
- schwache Kryptographie (DES) verpflichtend
- Problem mit NAT

Alternativen zu IPsec – 2

Es existieren zahlreiche alternative VPN-Lösungen:

- CIPE
- vtun
- OpenVPN
- …

Diese sind oft benutzerfreundlicher oder weniger komplex als IPsec!

Alternativen zu IPsec?

Peter Gutmanns Analyse verschiedener VPN-Lösungen (CIPE, vtun, tinc):

- Zahlreiche Schwächen kryptographischer Natur entdeckt
- Diese Schwächen existieren teilweise seit Jahren!

Fazit:

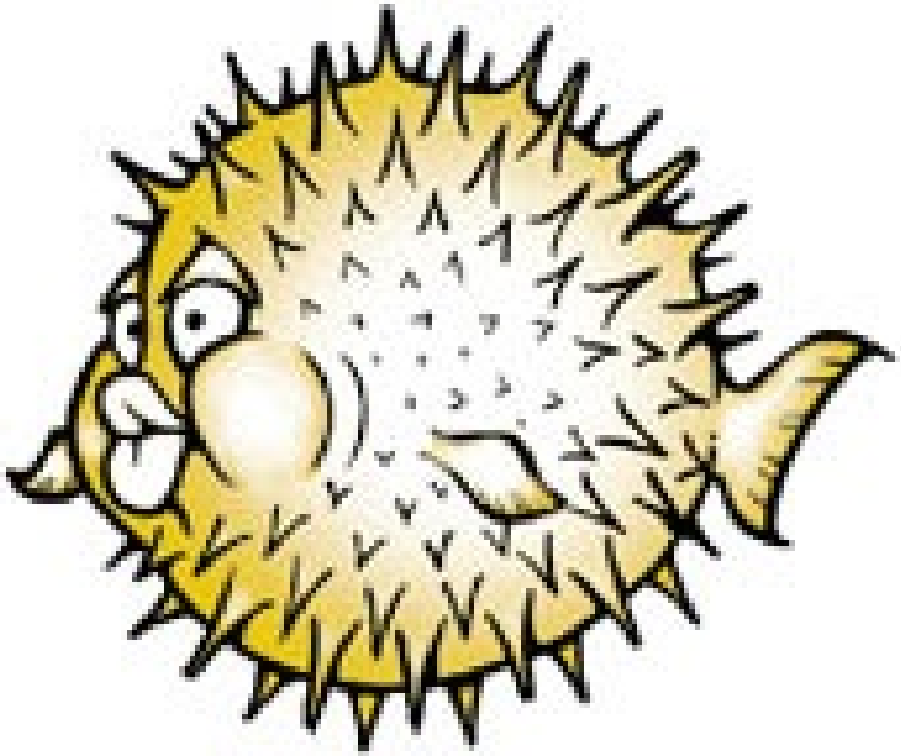
- Richtige Anwendung von Kryptographie ist sehr schwierig!
- Es gibt derzeit kaum Alternativen zu SSL, SSH oder IPsec
- Diese sind gut untersucht und verstanden

Aktuelle Weiterentwicklungen

- stärkere kryptographische Verfahren: AES, SHA2-{256,384,512}
- NAT-Traversal: Kapseln von IPsec in UDP ($\rightarrow$ Patente?!)
- Ersetzen von IKE mit IKEv2: Vereinfachtes(!) Protokoll, bessere Fehlerbehandlung, Robustheit gegen DoS

Zusammenfassung

- IPsec ist bei gängigen Betriebssystem frei verfügbar
- Aufbau von VPNs in heterogener Umgebung möglich
- Durch fortschreitende Standardisierung wohl “zukunftssicher” :-)



So long, and thanks
for all the passwords

Fragen?