IPSec

Michael Gschwandtner, Alois Hofstätter,
Roland Likar, Horst Stadler

Jänner 2003

Einleitung (1)

- **Ziele des Datenverkehrs**
  - ⋆ Geschwindigkeit
  - ⋆ Verlässlichkeit
  - ⋆ Sicherheit
- **Begriff: Sicherheit**
  - ⋆ Authentizität
  - ⋆ Integrität
  - ⋆ Vertraulichkeit

Einleitung (2)

- **IPSec**
  - ⋆ konzipiert von: IPSec Working Group der IETF
  - ⋆ seit 1992 in der Entwicklung
  - ⋆ Definition besteht aus Arbeitspapieren und RFC's
  - ⋆ Ziele der Arbeitsgruppe:
    - ∗ Implementierungen für Hardware und Software
    - ∗ Pflege des Standards
  - ⋆ Packet von Protokollen
  - ⋆ Aufgabe: Schutz vor Ausspähungen und Modifikationen
  - ⋆ fest in das Internet Protokoll integriert
  - ⋆ integraler Bestandteil von IPv6
  - ⋆ Wichtig: Nur der Transport von Daten wird gesichert

Symmetrische Verschlüsselungsarten (1)

- **One Time Pad**
- **DES**
- **3DES**
- **Blowfish**
- **IDEA**
- **RC4**

Symmetrische Verschlüsselungsarten (2)

- **RC5**
- **AES**
- **CAST**
- **Twofish**

Rechenbeispiel *One Time Pad*

verwendete Verschlüsselung: XOR-Verknüpfung

Klartext	01000001
Schlüssel	10101010
Geheimtext	11101011

Geheimtext	11101011
Schlüssel	10101010
Klartext	01000001

Asymmetrische Verschlüsselungsarten

- **RSA**
- **ElGamal**
- **DSS Digital Signature Standard**
- **Kryptographische Hashfunktionen**

Rechenbeispiel RSA

- **n = p * q**
- $\Phi(n) = \Phi(p) * \Phi(q)$
- $(e * d)\ mod\ \Phi(n) = 1$
- **public = e und n, private = d und n**
- $(m \leq n)$
- $c = m^e\ mod\ n,\ \ m = c^d\ mod\ n$

Schlüssellebenszeit

In RFC 2541 werden folgende Werte für die Schlüssellebenszeit vorgeschlagen:

- **Niemals länger als 4 Jahre**
- **Ein guter Wert ist 1 Jahr**
- **Online verfügbare Schlüssel nicht länger als einen Monat**
- **Auf keinen Fall weniger als 3 Minuten**

Schlüsselaustausch - Vorbereitung

Ausgetauscht wird jeweils nur der Public-Key

- **Manuell:**
  Die Administratoren tauschen über einen gesicherten / ungesicherten Kanal "ihre" Public-Keys aus

- **Automatisch:**
  IPSec verwendet eine Option von DNSSec und besorgt den "fremden" Public-Key vom zuständigen DNS-Server

DNS - Domain Name Service (1)

DNS ist in RFC 1034 und RFC 1035 vollständig definiert

- **Lookup:**
  www.cosy.sbg.ac.at $\longrightarrow$ 141.201.2.14

- **Reverse Lookup:**
  141.201.2.14 $\longrightarrow$ www.cosy.sbg.ac.at

DNS - Domain Name Service (2)

- **Config Files:**
  - ⋆ CNAME, A:
    www.cosy.sbg.ac.at. IN CNAME bulldogge.cosy.sbg.ac.at.
    bulldogge.cosy.sbg.ac.at. IN A 141.201.2.14
  - ⋆ MX:
    MX 10 spinx.cosy.sbg.ac.at
    MX 20 barracuda.cosy.sbg.ac.at
  - ⋆ HINFO
  - ⋆ PTR:
    14 PTR bulldogge.cosy.sbg.ac.at.

DNSSec - DNS Security Extensions

Die DNS Security Extensions sind in RFC 2535 spezifiziert

- **Wir verwenden nur den neue Eintrag $IN\ KEY$**
- **BIND Version 9.2.1 (01. Mai 2002) und FreeS/WAN Version 1.99 (04. Nov 2002) unterstützen DNSSec**
- **Config Eintrag von FreeS/WAN: leftrsasigkey=%dns**

Security Association (1)

- SA Felder
  - ⋆ AH Authentifizierungsalgorithmus + Schlüssel
  - ⋆ ESP Authentifizierungsalgorithmus + Schlüssel
  - ⋆ ESP Verschlüsselungsalgorithmus + Schlüssel
  - ⋆ Sequenznummernzähler
  - ⋆ Sequenzzähler Überlauf-Flag
  - ⋆ Anti Replay Fenster
  - ⋆ IPSec Protokollmodus
  - ⋆ Path Maximum Transmission Unit
  - ⋆ Lebensdauer der SA

Security Association Database

- enthält alle SAs
- indiziert durch
  - ⋆ *Quell Adresse*
  - ⋆ *Ziel Adresse*
  - ⋆ *IPSec Protokoll*

Security Policy Database (1)

Ein Eintrag in der SPD wir anhand folgender Selektoren ausgewählt

- SPD Felder
  - ⋆ Ziel Adresse
  - ⋆ Quell Adresse
  - ⋆ Transport Protokoll
  - ⋆ System Name
  - ⋆ User ID
- zusätzlich enthält der SPD Eintrag
  - ⋆ Verarbeitungsanweisung
  - ⋆ Verweis auf SA

Kryptographische Hash Funktionen und MAC

- die gängigsten Hash Funktionen sind
  - *MD5*
  - *SHA-I*
  - *RIPEMD-160*
  - *Tiger*
- Message Authentication Codes

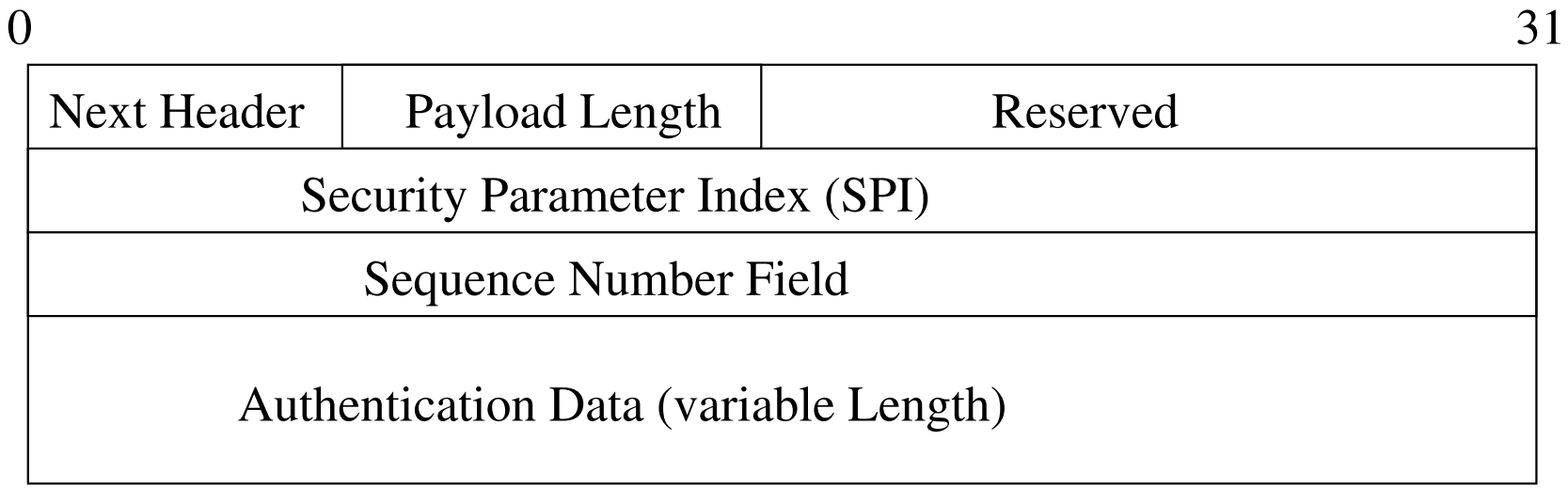
Authentication Header (1)

Aufgaben von AH

- verbindungslose Integrität
- Datenursprungsauthentifizierung
- Replayschutz

Probleme mit NAT Gateways

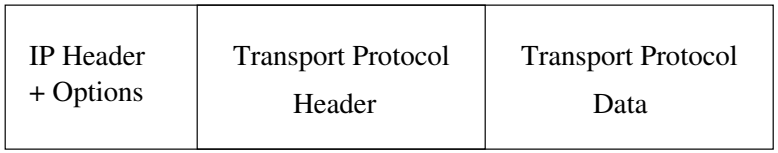
Authentication Header Format



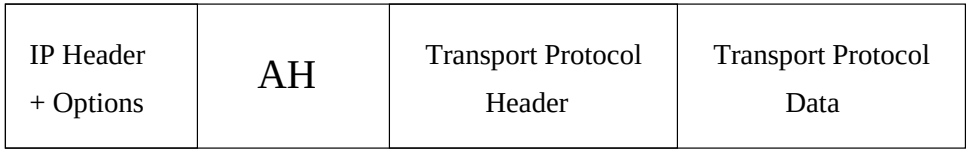
AH kann in zwei verschiedenen Modi betrieben werden:

- Transport Modus
- Tunnel Modus

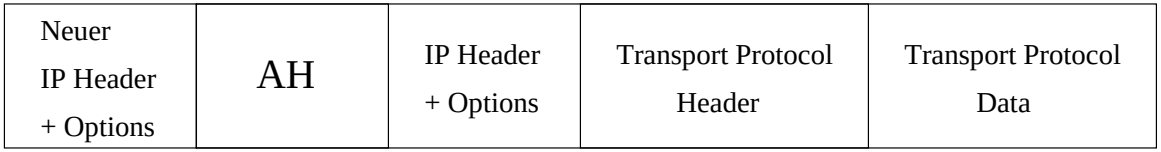
AH - Transport/Tunnel Modus



- Nach AH (Transport Mode)



- Nach AH (Tunnel Mode)

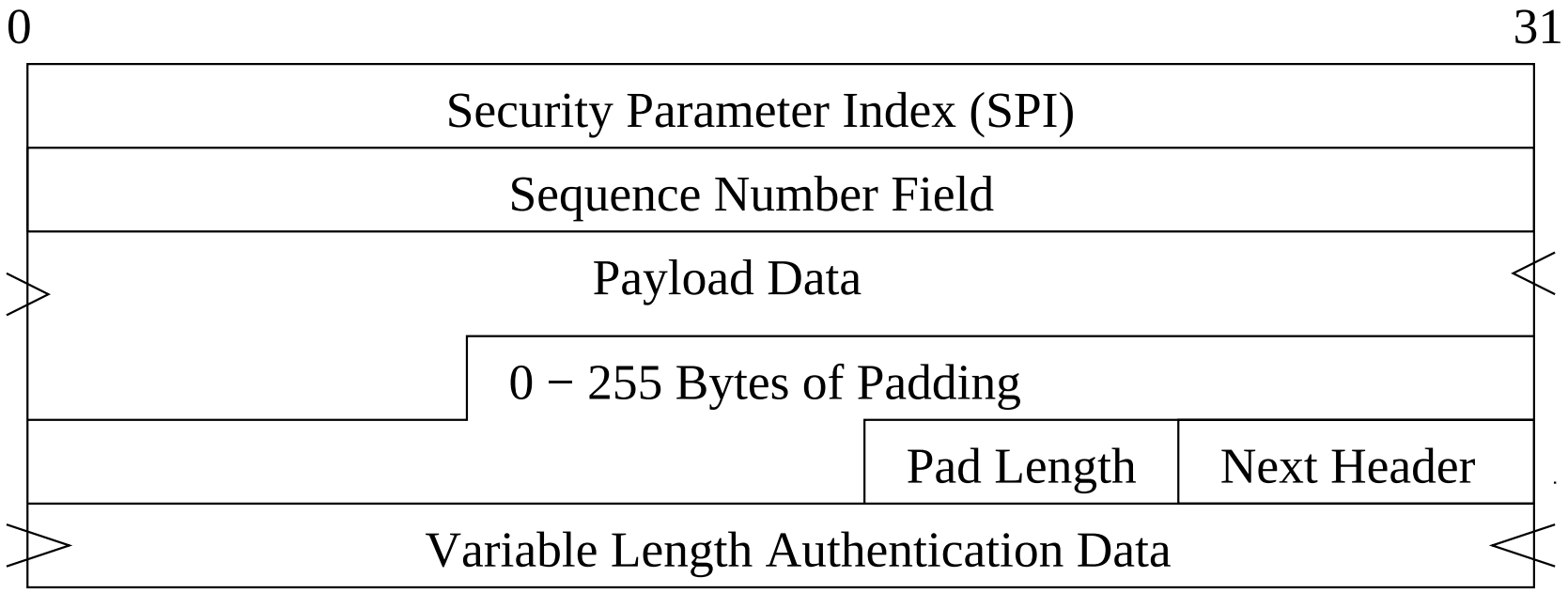


Integritätswertberechnung

Vor der ICV Berechnung werden die veränderlichen Felder des IP Headers auf 0 gesetzt

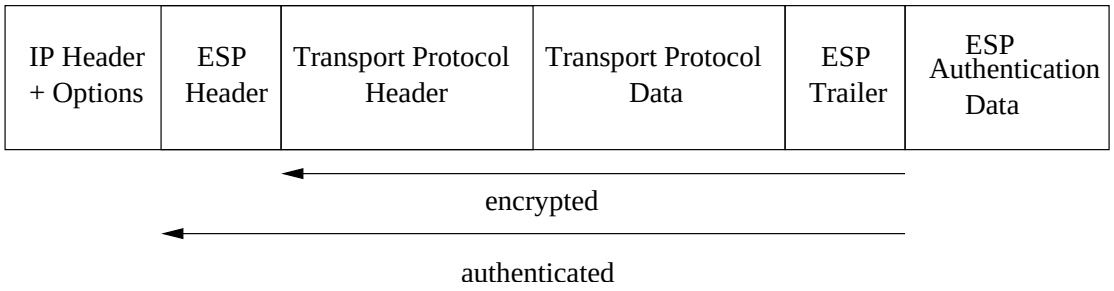
- Type of Service
- Flags
- Fragment Offset
- TTL
- Header Checksum
- Options

Encapsulating Security Payload Header Format

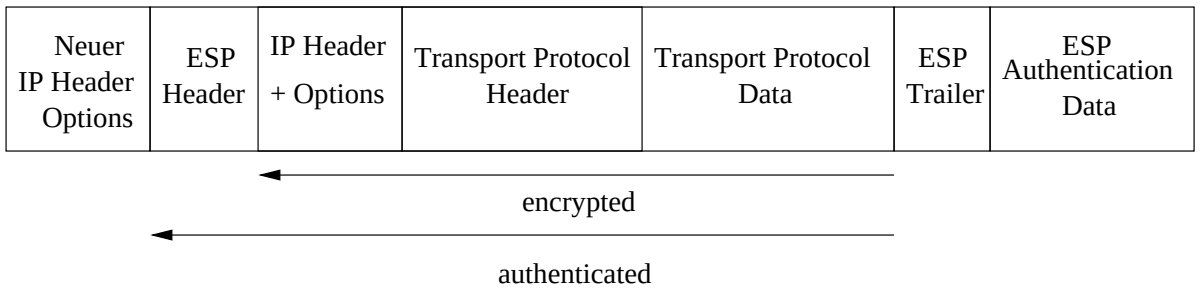


ESP - Transport/Tunnel Modus

- Nach ESP (Transport Mode)



- Nach ESP (Tunnel Mode)



Fazit

Der optimalste Schutz wird geboten wenn man eine Kombination aus AH und ESP benutzt, da dadurch das ganze Packet authentifiziert und die Daten verschlüsselt werden.

Schlüsselverwaltungs-Protokolle (1)
Übersicht

- **Aufgaben:**
  - ⋆ verhandeln, etablieren, modifizieren und löschen von Sicherheitseigenschaften und Sicherheitsattributen
  - ⋆ Schutz gegen Angriffe
- **Protokolle:**
  - ⋆ *SKEME*
  - ⋆ *OKDP*
  - ⋆ *ISAKMP*
  - ⋆ *IKE*

Schlüsselverwaltungs-Protokolle (2)
ISAKMP

- Favorit unter den Schlüsselverwaltungs-Protokollen für $IPSec$
- unabhängig von Schlüssel-Austausch-Protokollen, kryptographischen Algorithmen, Schlüssel-Erstellungs-Verfahren sowie Authentifizierungsmechanismen
- Zwei-Phasen-Verhandlung:
  - ⋆ Erste-Phase:
    Authentifikation und Einrichten eines verschlüsselten Kanals
  - ⋆ Zweite-Phase:
    übermitteln der Schlüssel z.B. für $IPSec$

Schlüsselverwaltungs-Protokolle (3)
IKE

- Hybrid-Protokoll ($ISAKMP$, $OKDP$, $SKEME$)
- ist $ISAKMP$ sehr ähnlich
  - ⋆ Zwei-Phasen-Verhandlung
  - ⋆ ähnliche Vermittlungstypen
  - ⋆ ähnliche Header
- wesentlicher Unterschied zu $ISAKMP$: definiert Schlüsselaustausch

Anwendungen / Implementierungen (1)

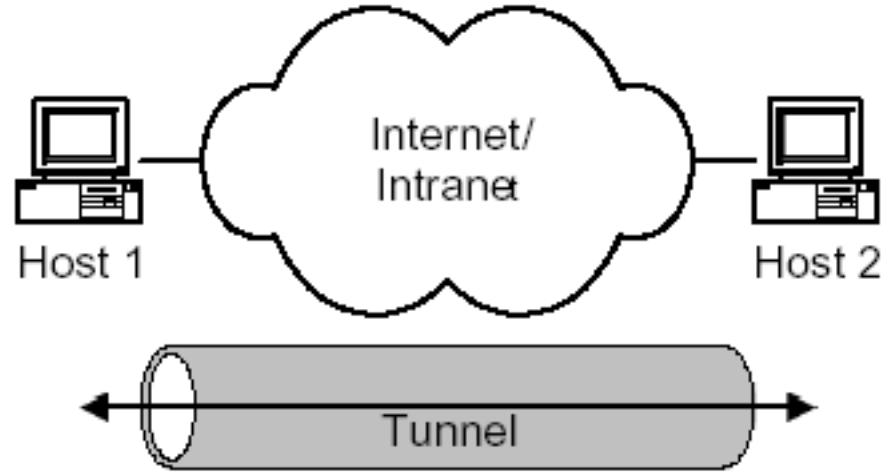
- **Implementierungen**
  - ⋆ FreeS/WAN Project (Linux)
  - ⋆ ipnsec (Linux)
  - ⋆ LIPsec-0.5 (Linux)
  - ⋆ OpenBSD hat IPSec in den Source-Tree übernommen
  - ⋆ SSH IPSEC Express; Toolkit für die Implementierung von IPSec bei Betriebssystemen, Routern und Firewalls
  - ⋆ SSH ISAKMP/Oaklay; Implementation von Key-Management Funktionen
  - ⋆ ...

Anwendungen / Implementierungen (2)

- **Anwendungsbereich**
  - ⋆ VPN
  - ⋆ WLAN
- VPN
  - ⋆ VPN = Virtual Private Network
  - ⋆ Kommunikation über öffentliches Netz
  - ⋆ Architekturen
    - ∗ End-to-End
    - ∗ Site-to-Site
    - ∗ End-to-Site

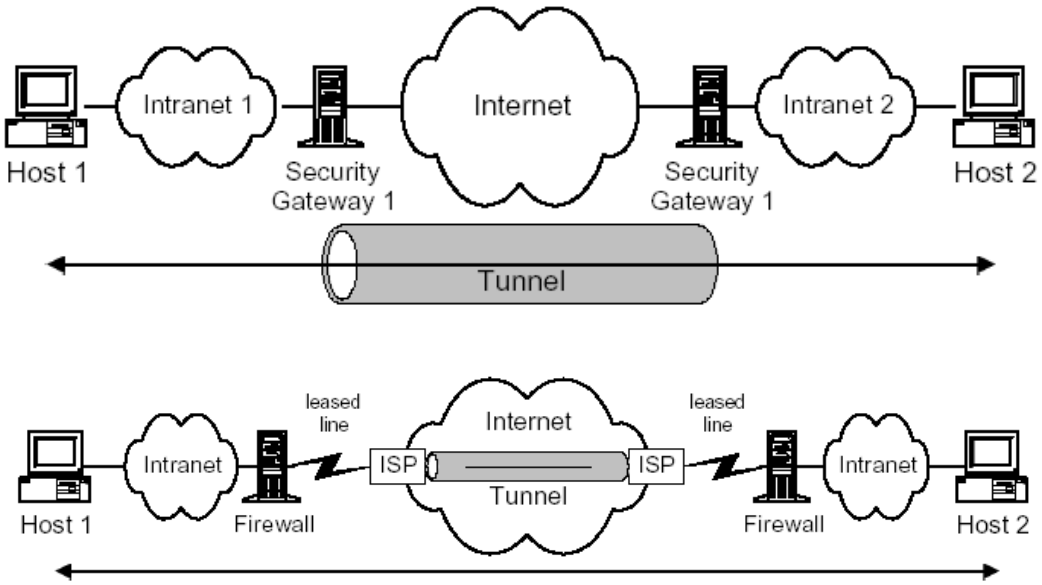
Anwendungen / Implementierungen (3)

- End-to-End



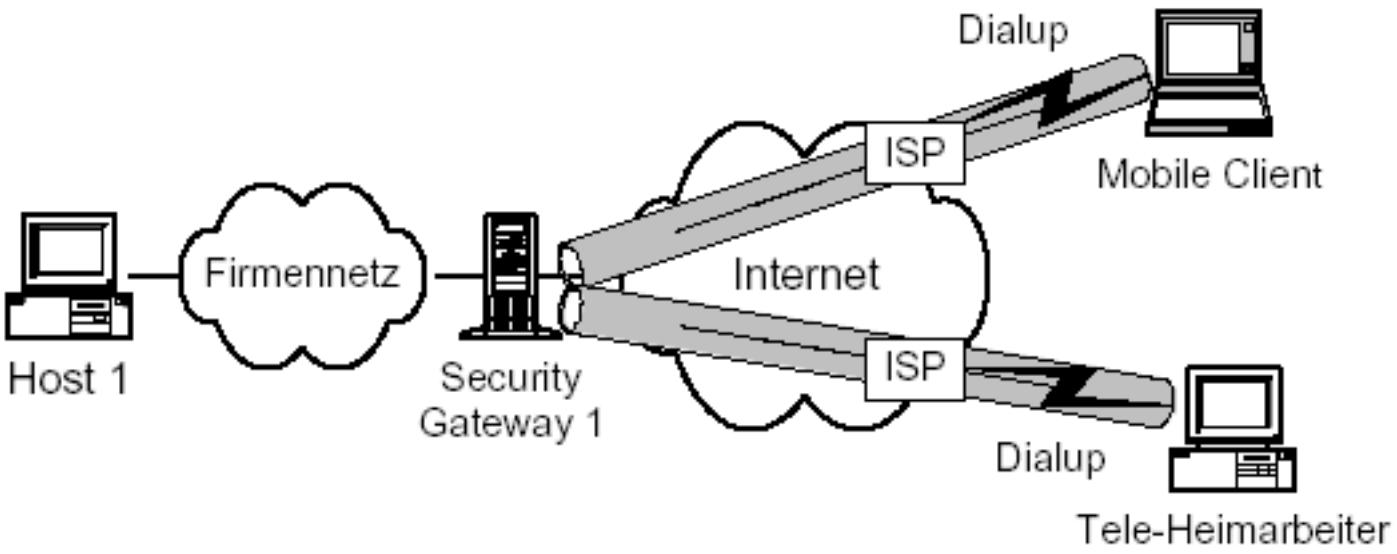
Anwendungen / Implementierungen (4)

- Site-to-Site



Anwendungen / Implementierungen (5)

- End-to-Site



Anwendungen / Implementierungen (6)

- Alternativen:
  - PPTP
  - L2F
  - L2TP
- WLAN
  - Standard IEEE 802.11
  - Transferraten von bis zu 11 Megabit
  - Frequenzband: 2,4 GHz
  - Sendeverfahren: FHSS, DSSS

Angriffsmöglichkeiten (1)
kryptographische Angriffe

- Brute-Force Attack
  - ⋆ alle möglichen Schlüssel durchprobieren
  - ⋆ Abhilfe: lange und kurzlebige Schlüssel
- known Plaintext Attack
  - ⋆ Teile des Datenstroms liegen unverschlüsselt vor
  - ⋆ Abhilfe: lange und kurzlebige Schlüssel

Angriffsmöglichkeiten (2)

- Man-in-the-Middle Attack
  - ⋆ Abhilfe: Authentifikation
- Cut-and-Paste Attack
  - ⋆ nur bei ESP mit hostbasierter Verschlüsselung ohne Integritätskontrolle
- Session Hijacking
  - ⋆ spezifischer Cut-and-Paste Angriff

Probleme / Schwächen

- kein Broadcast
- kein dynamisches Routing
- Verstoss gegen das OSI-Schichtenmodell
- Cut-and-Paste Attack
- warum gerade IPsec ?
- Komplexität

weitere Möglichkeiten (1)

- unterhalb der Netzwerkschicht:
  - ⋆ Kryptobox
- Netzwerkschicht:
  - ⋆ SKIP
- Transportschicht:
  - ⋆ TLS
  - ⋆ SSL

weitere Möglichkeiten (2)

- SSH
- Email-Sicherheit:
  - PGP
  - S/MIME
  - PEM

Quellen

IPSec - Tunneling im Internet, Carlton R. Davis, mitp-Verlag
RFCs: 2401, 2402, 2406, 2408, 2409
http://www.informatik.uni-bremen.de/grp/ag-sec/Seminar/WS00/ipsec.ps
http://mitglied.lycos.de/cthoeing/crypto/rsa.htm
http://www.cert.dfn.de/fwl/nsp/nsp-prod.html
http://www.repges.net/IPSec/ipsec.html
http://home.t-online.de/home/TschiTschi/ipsec.htm