



---

# Vorlesung

## VPN: Drahtgebunden und drahtlos

Fachbereich Informatik (FB 20)

Lehrstuhl Prof. J. Buchmann

WS-05 / V2 - 20.205.1

In Zusammenarbeit mit dem CAST-Forum

Dr. Wolfgang Böhmer

Skript: <http://www.cdc.informatik.tu-darmstadt.de/~wboehmer/>

Email: [wboehmer@cdc.informatik.tu-darmstadt.de](mailto:wboehmer@cdc.informatik.tu-darmstadt.de)

---





# Vorlesungsinhalte

---

## 6. Layer-3-Techniken und der Sicherheitsstandard für das Internet (IPSec)

1. Das Ziel von IPSec
2. IPSec-Sicherheitsvereinbarungen (SA) / Initiierung und Kombination
3. IPSec-AH-Header
4. IPSec-ESP-Header
5. IPSec und Remote Access (siehe Exkurs WLAN)
6. Internet-Key-Exchange-Management (IKE) (Phase-1 /Phase-2)
7. ISAKMP/Oakley und Skip
8. Layer-2- und Layer-3-Vergleich

## 7. Layer-4-Techniken

1. Secure Socket Layer (SSL) und Transport Layer Sicherheit (TLS)
2. Vergleich IPSec und SSL/TLS

## 8. Layer-5-Techniken

1. Socks V.5





# Sicherheitsstandard für das Internet (IPSec)

- IETF (*IP Security Working Group*) gebildet
  - RFC-1825 bis RFC-1829 (1995)
  - RFC-2405 bis RFC-2412 und RFC-2451 (1998) und weitere siehe Lit.Liste
- Zwei neue Protokolle zur Erhöhung der Verkehrssicherheit
  - Authentication Header (AH)
    - Daten-Authentifizierung,
    - verbindungslose Integrität
    - Schutz von Wiedereinspielen (*Replay-attack*)
  - Encapsulation Security Payload (ESP)
    - Daten-Vertraulichkeit
    - begrenzte Vertraulichkeit des Verkehrsflusses
    - verbindungslose Integrität
    - Daten-Authentifizierung
    - Schutz von Wiedereinspielen (*Replay-attack*)





# IPSec: Kurzübersicht

---

- IPSec kennt zwei Betriebsmodi jeweils für AH und ESP
  - Transport Modus
  - Tunnelmodus
- Schlüsselmanagement IKE
  - ausgewählte Kryptographische Algorithmen für AH und ESP auszuhandeln
  - Erzeugung der notwendigen Schlüssel
- IPSec verwendet Protokolle die Algorithmus unabhängig sind
  - Wahl der Algorithmen obliegt in der Security Policy Database, SPD
  - hängt von der konkreten IPSec-Implementierung ab
  - Standard Satz zur Gewährleistung von Interoperabilität
  - IPSec gestattet Nutzer/Admin eines Systems Sicherheits-Dienste zu kontrollieren und Tiefe festzulegen.
  - IPSec verwendet Security Associations, SA





## IPSec: Sicherheitsvereinbarung

---

- Konzept der SA ist fundamental für IPSec
- AH und ESP arbeiten mit der Security Association, SA
- SA ist eine Vereinbarung zwischen Kommunikationspartnern
  - IPSec-Protokoll
  - Betriebsmodus (Tunnel / Transport)
  - kryptographischer Algorithmen
  - Lebensdauer und Gültigkeit der Schlüssel
  - Lebensdauer der SA
- Security Policy Database (SPD) Menge an grundsätzlichen Service
- Security Association Database (SAD) konkrete Parameter für ein unidirektionale SA

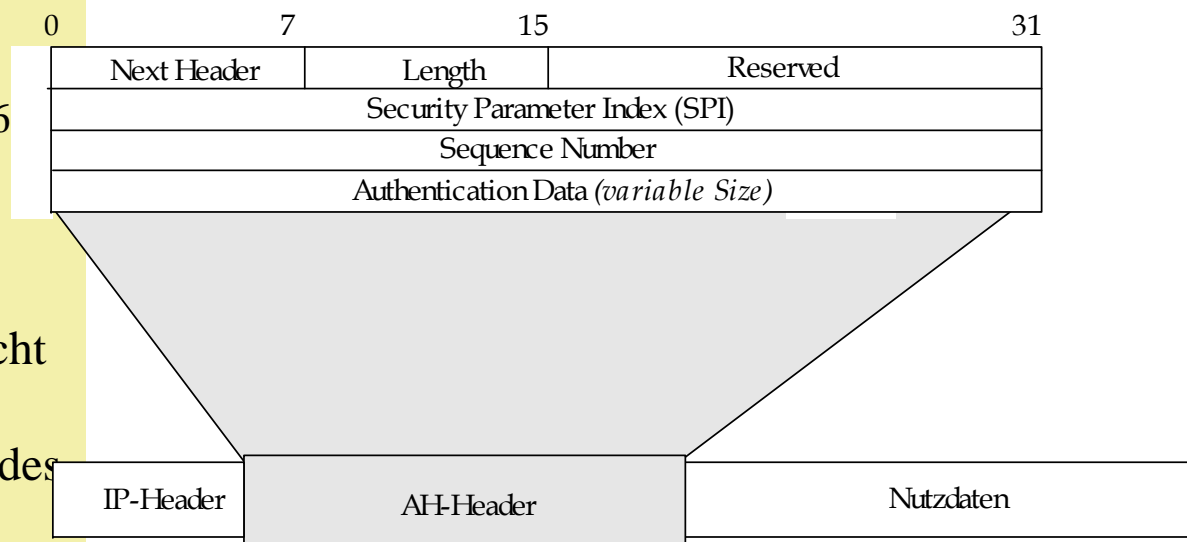
**SA = {Security Parameter Index, IP Destination Address, Security Protocol}**





## IPSec: AH-Header (*Authentifizierung*)

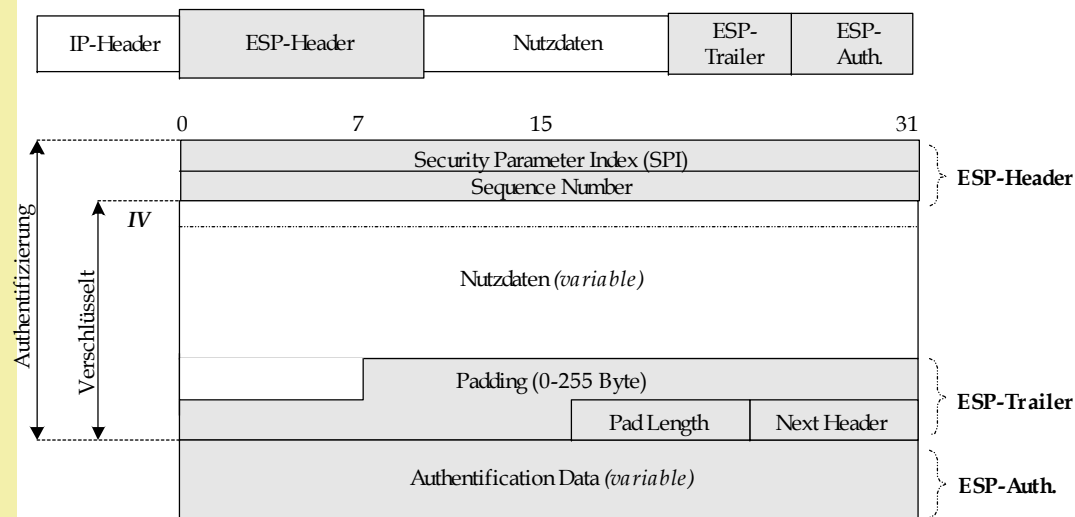
- AH-Header = 5 Felder
  - Next Header (TCP,UDP,ICMP)
  - Länge des AH-Header
  - SPI und Seq-Num
  - Authentifizierung mittels
    - HMAC-MD5-96
    - HMAC-SHA-1
    - Optional
      - DES-MAC
- IP-Datagramm wird nicht verschlüsselt
- 24 Byte Vergrößerung des IP-Paket





## IPSec: ESP (*Vertraulichkeit*)

- ESP = 6 Felder
  - Nutzdaten liegen zwischen ESP-Header und ESP-Trailer eingebettet
  - SPI und Seq-Num
  - ESP-Authentication data
  - Verschlüsselung
    1. DES-CBC
    2. Null (RFC-2410) !
    3. Optional
      - CAST, RC5, IDEA, AES Blowfish, 3DES
  - HASH-Algorithmen
    1. HMAC-MD5
    2. HMAC-SHA-1
    3. Optional
      - DES-MAC





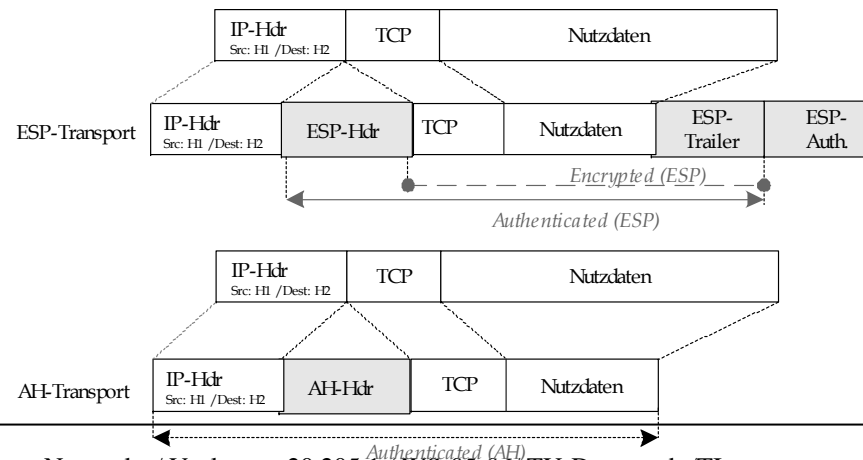
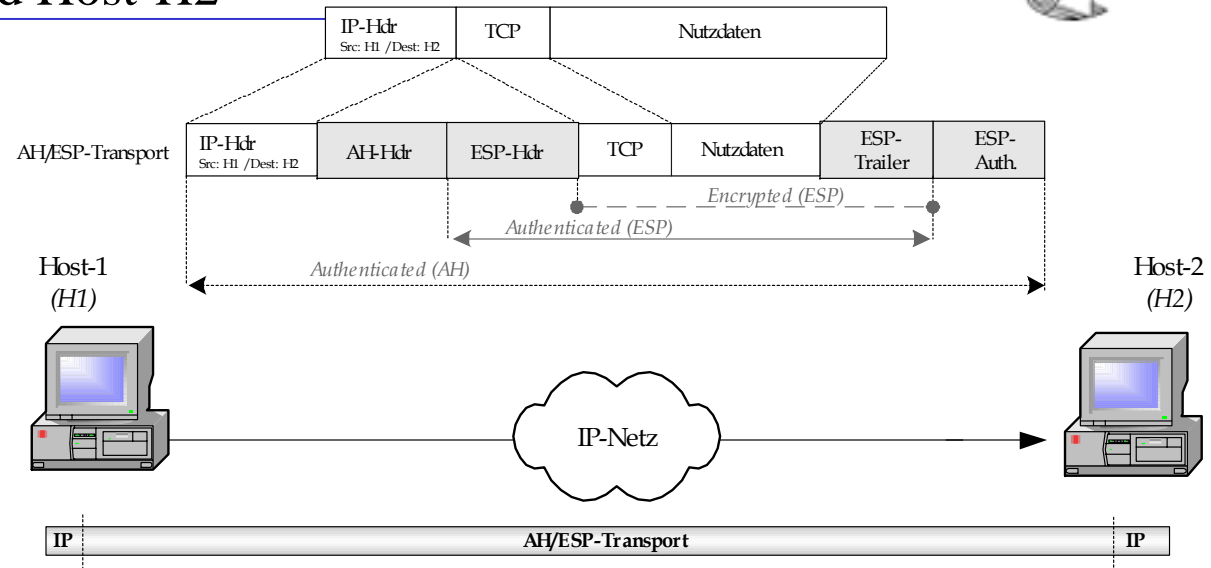
# IPSec: Transport Modus

---

- Nur die Nutzlast des IP-Paket wird verschlüsselt
- Original IP-Kopf bleibt erhalten
  - IETF-Empfehlung zur Absicherung zweier Host ohne Gateway
    - Nur Verwendung des Transport Modus in der Kombination AH/ESP-Transport
  - Probleme beim Einsatz von AH im Transport Modus bei NAT-Gateways
    - Lösung: Das Gateway müsste die Authentifizierung durchführen
  - Probleme beim Einsatz von AH im Transport Modus bei Proxys
- Einschränkungen gelten für IPv4 und IPv6
- Einschränkungen gelten nicht für ESP im Transport Modus
  - Es können ohne Probleme NAT-Gateways und Proxys eingesetzt werden
  - Außer ESP-Header kann jedes IP-Header-Feld verändert werden, falls die Header-Prüfsumme neu berechnet wird und die SA nur die ESP-Authentifizierung nutzt
  - Authentifizierung des ESP-Transport Modus bietet weniger Schutz als AH-Transport Modus



# IPSec-Verbindung im Transport Modus zwischen Host-H1 und Host-H2





# IPSec-VPN Fallstudie (1)

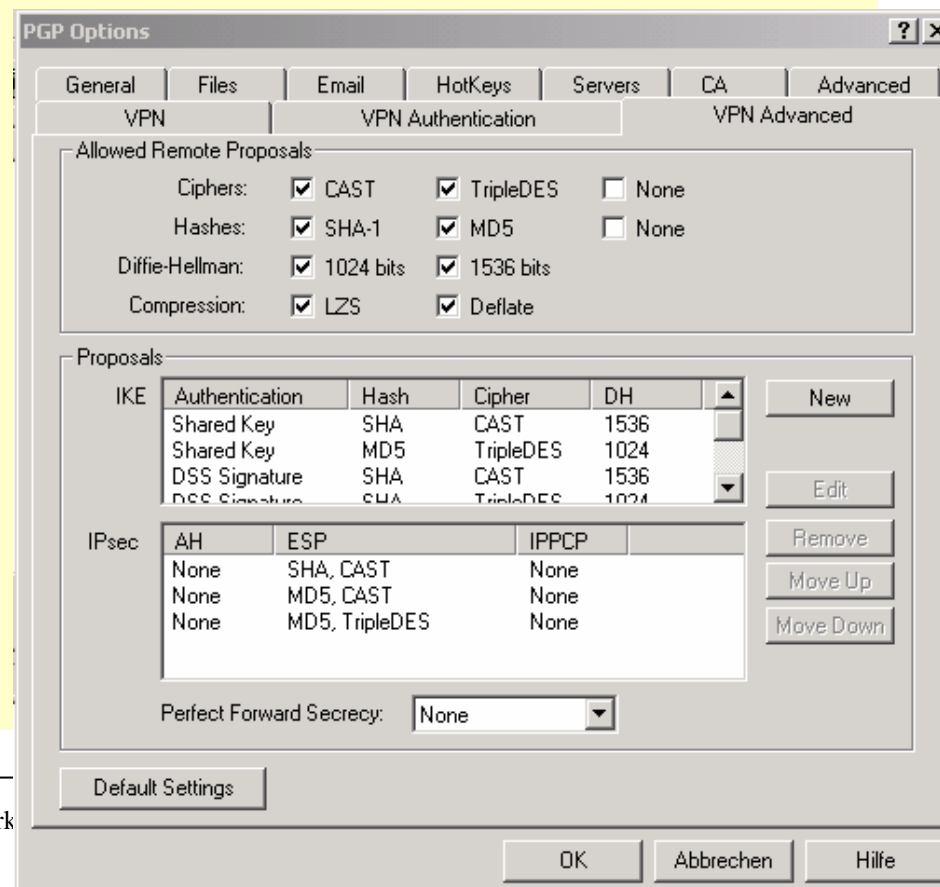
- Konfiguration des PKI-Servers (NetTools PKI Xcert-PKI-Appl. Fa. NAI)
  1. Eingeben genereller Konfigurationsinformationen
  2. Erstellen der ROOT Certificate Authority (CA)-Zertifikate
  3. Generieren der Administrativen CA-Zertifikate
  4. Erzeugung der Beitritts- und Administrations-Web-Server-Zertifikate
  5. Erstellen eines administrativen Client-Zertifikates
- Konfiguration des VPN-Gateways (Gauntlet Firewall)
  1. Erstellen der PKI-Komponenten
  2. Download der CA-Zertifikate
  3. Erstellung eines Requests für ein Firewall-Zertifikat
  4. Wiederlangung des Firewall-Zertifikates vom PKI-Server während der Verarbeitung und der Aktivierung
  5. Konfiguration des VPN-Links
  6. Konfigurieren der Link-Einstellungen
- Konfiguration des VPN-Clients (PGP-VPN-Client)





## IPSec-VPN Fallstudie (2)

- Konfiguration des VPN-Clients (PGP-VPN-Client)
  1. Erhalt eines digitalen Zertifikates sowie hinzufügen zum Key-Ring
  2. Auswahl des Zertifikates, das für die Authentifizierung am VPN-Gateway eingesetzt werden soll.
  3. Hinzufügen des VPN-Links
  4. Konfiguration der Security Policy Database (SPD)





## Verfügbare Implementierungen

- *KAME*-Projekt for FreeBSD, OpenBSD



<http://www.kame.net/>

- Free/SWAN in der Version 2.04 released am 13/11/2003 unterstützt den Linux Kernel 2.6



<http://www.freeswan.org/>



# Übungen

---



- Frage: Für welches Anwendungsszenario ist der Transport Modus bei IPSec ideal geeignet?
- Frage: Für welches Anwendungsszenario ist der Tunnel Modus bei IPSec ideal geeignet?
- Frage: Worauf sind die Interoperabilitätsprobleme bei IPSec zum großen Teil zurückzuführen?





# Literatur

---

- <http://www.tu-darmstadt.de/vv/20.205.1>.
- **Huston G.: Internet Performance Survival Guide, QoS Strategies for Multiservice Networks, ISBN 0-471-37808-9**
- **Comer, 1995: Internetworking with TCP/IP Vol. I., ISBN 0-13-216987-8**
- **Davis, C.R.: IPSec-Tunneling im Internet, mitp-Verlag, 1. Auflage 2002, ISBN 3-8266-0809-7.**
- **Aurand, A.: Sicherheit in Cisco- und Windows-2000-Netzwerken, Installation und Troubleshooting von IPSec in der Praxis, Addison-Wesley Verlag 2001, ISBN 3-8273-1930-7. (Teil 2- IPSec-Architektur)**
- **Schneier, B.: IPSec an critical description**
- **Liste der RFC die für IPSec geschrieben wurden (Stand 2003):**  
1191, 1321, 1421, 1422, 1423, 1424, 1701, 1827, 1728, 2093, 2094, 2104, 2246, 2311, 2312, 2315, 2394, 2395, 2401, 2403, 2404, 2405, 2408, 2409, 2410, 2411, 2412, 2437, 2451, 2507, 2510, 2511, 2522, 2523, 2535, 2549, 2559, 2560, 2585, 2627, 2631, 2633, 2660, 2661, 2828, 2845, 2857, 2888, 2898, 2931, 2944, 2945, 2985, 2986, 3007, 3008, 3039, 3051, 3526, 3554, 3566, 3602.

