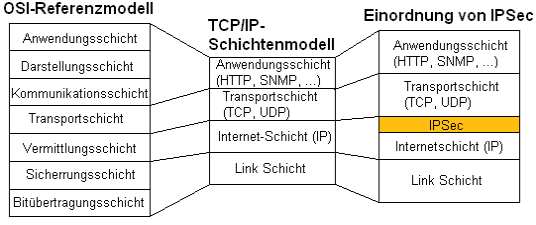
8. Kommunikationssverschlüsselung

Prof. Dr. Christoph Skornia
christoph.skornia@oth-regensburg.de

- **Sicherheitsmängel von IP** (Wiederholung)
  - keine Vertraulichkeit(Abhören möglich)
  - keine Authentifizierung
  - kein Fälschungssicherheit
  - kein Schutz vor Replays

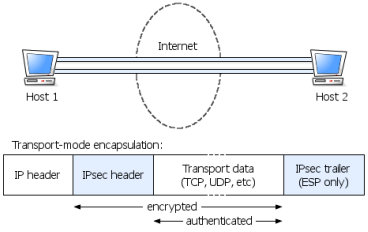
- **Konsequenz: Sicheres IP entwickeln**
  - **Ziel**
    IP-Sicherheitskonzepte, die in IPv4 und IPv6 integriert werden können
  - **Entwicklung**
    RFC 1636 "Security *in the Internet Architecture*", 1994
    - Notwendigkeit von Sicherheitsmaßnahmen in der Internet- Architektur
    - Initiierung der IPsec-Entwicklung (optional IPv4, verpflichtend IPv6)
    - Initiierung eines Sicherheitsprotokolls für die Transportschicht TLS/SSL

- **Ergebnis der Entwicklung: IPSec**
- **IPSec** stellt Mittel für eine sichere Übertragung von IP-Paketen über LAN, private und öffentliche WAN sowie das Internet bereit. Es kann den gesamten IP-Datenverkehr verschlüsseln und/oder authentifizieren. Des Weiteren können Sicherheitsrichtlinien (Security *Policies)* umgesetzt werden.
- **IPsec-Protokolle**
  - Die IPsec-Protokolle werden als Header-Erweiterungen realisiert, die wie folgt in die beiden IP-Protokollversionen integriert werden.
    - **IPv4**
      zwischen IP-Header und Payload
    - **IPv6**
      als Header-Erweiterung



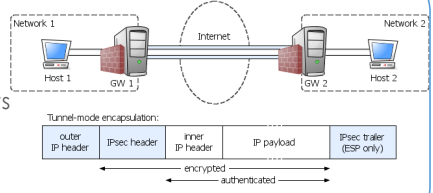
- Transport-Mode

  „Sichere“ Kommunikation direkt zwischen Quelle und Ziel



- Tunnel-Mode

  Kommunikation zwischen Quelle und Ziel aber „Sicherung“ nur zwischen 2 Gateways



- **Security Association (SA)**
  - In der **SAs** werden die Sicherheitsvorgaben (Verschlüsselungsverfahren, Schlüssel, Authentifizierungsverfahren) für eine Kommunikationsbeziehung zwischen den Partnern festgelegt.
  - SAs sind unidirektional: Falls eine 2-Wege-Sicherung erforderlich sind 2 getrennte SAs nötig
  - Eine Sicherheitsrelation ist eindeutig durch drei Parameter bestimmt:
    - **Security Parameter Index (SPI):**
      Identifikation der *SA*
    - **Destination Address:**
      Zieladresse (nur Unicast Adressen erlaubt)
    - **Security Protocol Identifier:**
      nur Authentifizierung oder auch Verschlüsselung

• Parameter von Sicherheitsassoziationen

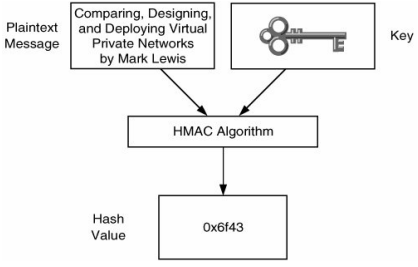
- **Sequence Number Counter** (32 *Bit):*
  dient der Generierung der Sequenznummer in den Headern
- **Sequence Counter Overflow:**
  Flag um anzuzeigen, wenn Sequenznummernbereich erschöpft
  - Generierung einer Audit-Nachricht
  - keine weitere Übertragung für Pakete mit dieser SA
- **Anti-Replay Window:** Sliding Window für erlaubte Wiederholungen von Paketen
- **Authentifizierungsinformation:**
  Authentifikationsalgorithmus, Schlüssel, Schlüssellebenszeiten und zugehörige Parameter, die für die Authentifizierung genutzt werden
- **Verschlüsselungsinformation:**
  Verschlüsselungs- und Authentifikationsalgorithmen, Schlüssel, Initialwerte, Schlüssellebensdauern und zugehörige Parameter, die für ESP genutzt werden
- **Lifetime of this SA**
- **IPSec Protocol Mode**
- **Path MTU:** maximale Übertragungseinheit der Verbindung

- **Verwaltung von Sicherheitsassoziationen**
- Für die Verwaltung und Festlegung von Sicherheitsassoziationen sind zwei Datenbanken erforderlich:
- **Association Database (SADB)**
  enthält die jeweils aktiven Sicherheitsassoziationen des Systems
- **Policy Database (SPD)**
  Abspeicherung der Richtlinien-Spezifikationen:
  Geben vor, für welche Datenströme Sicherheitsassoziationen mit welchen Parametern eingerichtet werden müssen

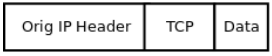
- Der **Authentication Header (AH)**

dient der Sicherung der Authentizität und der Integrität von (verbindungslos übertragenen) IP-Paketen.

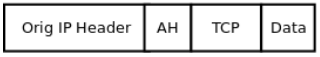
- Schutz gegen:
  - IP-Spoofing
  - Modifikation der Paketinhalte
  - *Replay-Attacken* (optional)
- HMAC für unveränderliche Teile des IP- und AH-Header sowie des IP-Datenteils



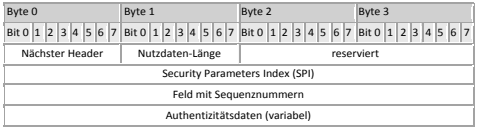
Normal Packet



Transport Mode After Applying AH



Tunnel Mode After Applying AH



- **Next Header** (8 *Bit):*

  Typ des nächsten Headers (IPv6)

- **Payload Length** (8 *Bit):*

  Länge *Authentication Data*

- **Reserved** (16 *Bit):* reserviert

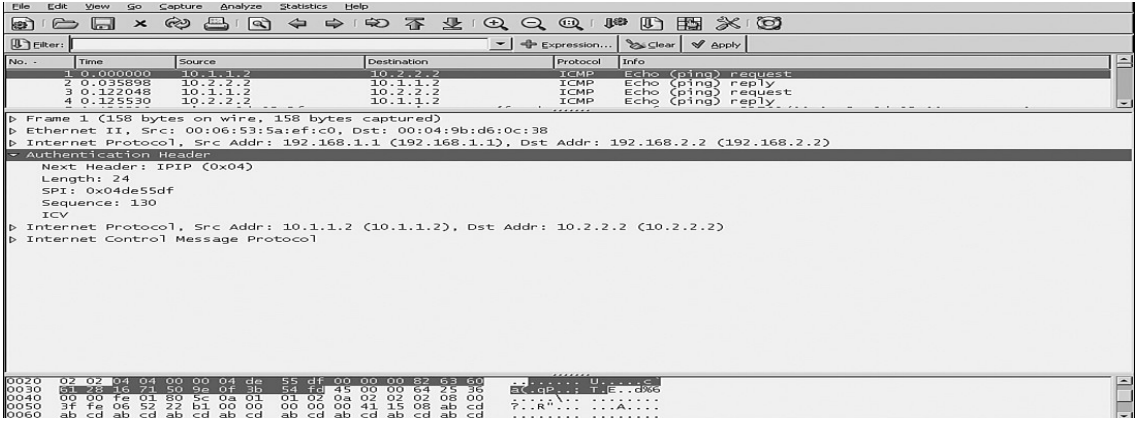
- **Security Parameters Index** (32 *Bit):*

  Identifikation der Sicherheits- Assoziation

- **Sequence Number** (32 *Bit):*

- **Authentication Data** (variabel):

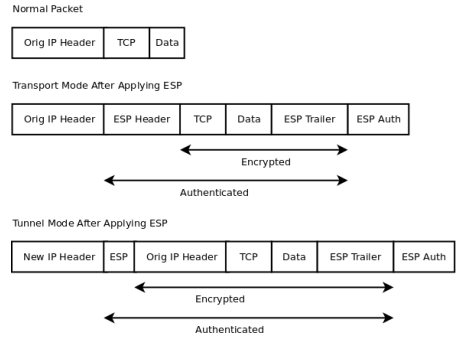
  enthält den MAC für unveränderliche Teile des IP-, AH-Header und IP- Datenteil z. B. *keyed* MD5

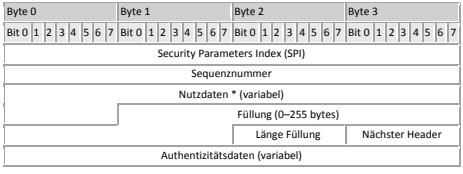

File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
1 0.000000 10.1.1.2 10.2.2.2 ICMP Echo (ping) request
2 0.035898 10.2.2.2 10.1.1.2 ICMP Echo (ping) reply
3 0.122048 10.1.1.2 10.2.2.2 ICMP Echo (ping) request
4 0.125530 10.2.2.2 10.1.1.2 ICMP Echo (ping) reply
Frame 1 (158 bytes on wire, 158 bytes captured)
Ethernet II, Src: 00:06:53:5a:ef:c0, Dst: 00:04:9b:d6:0c:38
Internet Protocol, Src Addr: 192.168.1.1 (192.168.1.1), Dst Addr: 192.168.2.2 (192.168.2.2)
Authentication Header
Next Header: IPIP (0x04)
Length: 24
SPI: 0x04de55df
Sequence: 130
ICV
Internet Protocol, Src Addr: 10.1.1.2 (10.1.1.2), Dst Addr: 10.2.2.2 (10.2.2.2)
Internet Control Message Protocol
0020 02 02 04 04 00 00 04 de 55 df 00 00 00 82 63 60
0030 81 28 16 71 50 9e 0f 3b 54 fd 45 00 00 64 25 36
0040 00 00 fe 01 80 5c 0a 01 01 02 0a 02 02 02 08 00
0050 3f fe 06 52 22 b1 00 00 00 00 00 41 15 08 ab cd
0060 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd

Encapsulating Security Payload (ESP)

- gewährleistet die Vertraulichkeit der Übertragung der IP-Pakete und eine Authentizitätsprüfung.
- Verschlüsselung (optional)
  - symmetrische Verschlüsselung
  - erforderliche Algoritmen AES-CBC, AES-GCM, ChaCha20 + Poly1305 (RFC 8221)
- Authentifizierung (optional)
  - Implementierung muss HMAC-SHA2 unterstützen (RFC 8221)
  - HMAC-Berechnung bezieht sich nur auf ESP-Header, IP-Datenteil und verschlüsselten Teil des ESP-Trailers

IPSEC



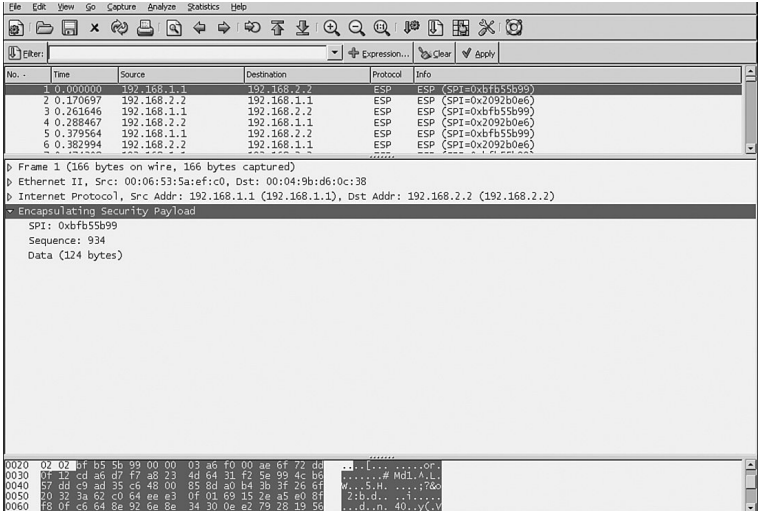


- **Security Parameters Index** (32 *Bit):*

  Identifikation der Sicherheits- Assoziation
- **Sequence Number** (32 *Bit):*
- **Payload Data** (variabel): verschlüsselte Daten
- **Padding** (0 - *255 Bytes):*

  Auffüllbytes, falls Verschlüsselungsalgorithmus ein Vielfaches einer bestimmten Zahl von Oktetts verlangt
- **Pad Length** (8 *Bit):*

  Zahl der benutzten Padding-Bytes
- **Next Header** (8 *Bit):* Verweis auf nächsten Headers
- **Authentication Data** (variable): *MAC* für ESP-Header, IP-Datenteil und verschlüsselten Teil des ESP-Trailers


File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
1 0.000000 192.168.1.1 192.168.2.2 ESP ESP (SPI=0xbfb55b99)
2 0.170697 192.168.2.2 192.168.1.1 ESP ESP (SPI=0x2092b0e6)
3 0.261646 192.168.1.1 192.168.2.2 ESP ESP (SPI=0xbfb55b99)
4 0.288467 192.168.2.2 192.168.1.1 ESP ESP (SPI=0x2092b0e6)
5 0.379564 192.168.1.1 192.168.2.2 ESP ESP (SPI=0xbfb55b99)
6 0.382994 192.168.2.2 192.168.1.1 ESP ESP (SPI=0x2092b0e6)
Frame 1 (166 bytes on wire, 166 bytes captured)
Ethernet II, Src: 00:06:53:5a:ef:c0, Dst: 00:04:9b:d6:0c:38
Internet Protocol, Src Addr: 192.168.1.1 (192.168.1.1), Dst Addr: 192.168.2.2 (192.168.2.2)
Encapsulating Security Payload
SPI: 0xbfb55b99
Sequence: 934
Data (124 bytes)
0020 02 02 bf b5 5b 99 00 00 03 a6 f0 00 ae 6f 72 dd
0030 9f 12 cd a6 d7 f7 a8 23 4d 64 31 f2 5e 99 4c b6
0040 57 dd c9 ad 35 c6 48 00 85 8d a0 b4 3b 3f 26 6f
0050 20 32 3a 62 c0 64 ee e3 0f 01 69 15 2e a5 e0 8f
0060 f8 0f c6 64 8e 92 6e 8e 34 30 0e e2 79 28 19 56

IPSEC

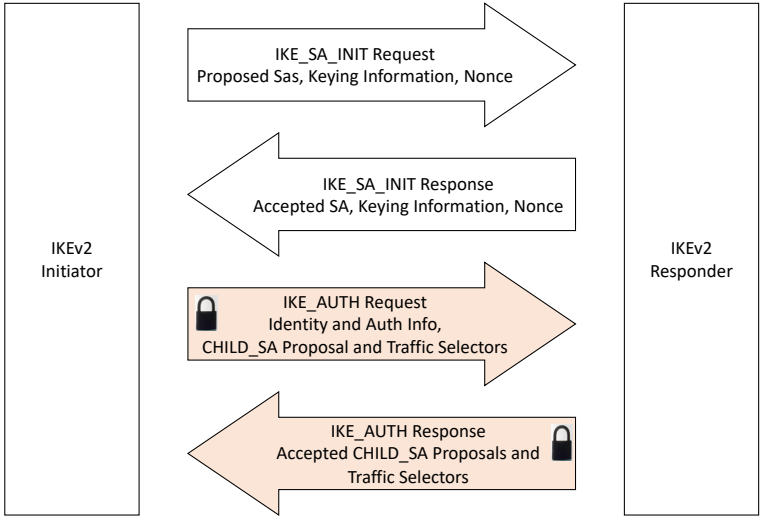
- **Schlüsselmanagement**
  - Das Schlüsselmanagement ist **nicht** Bestandteil von IPsec !!!
- **Herangehensweisen**
  - **manuell** manuelle Konfiguration auf der Basis der eigenen Schlüssel und der der Kommunikationspartner
    (nur praktikabel bei kleineren, statischen Systemen)
- **automatisch**

  On Demand-Generierung von Schlüsseln

  Default-Annahme: ISAKMP/IKE-Schlüsselaustauschprotokolle

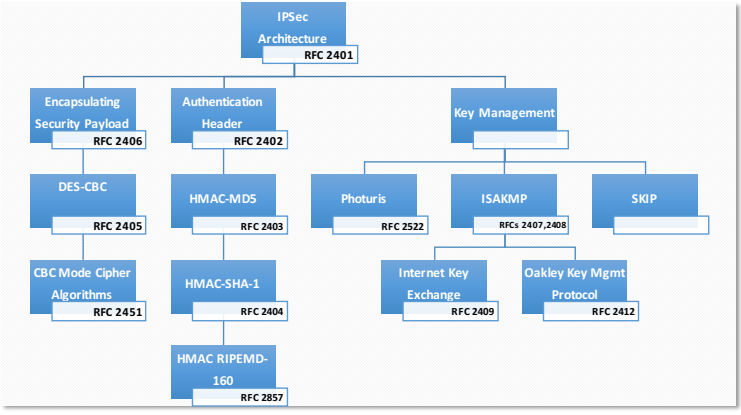
- **ISAKMP/IKE**
  - **Internet Security Association and Key Management Protocol** (ISAKMP)
    - Protokoll zur Aushandlung von Sicherheitsparametern
    - Instanzen-Authentifizierung
  - **Internet Key Exchange** (IKE)
    - Standard-Authentisierungs- und Schlüsselaustauschprotokoll auf der Basis von Diffie-Hellmann für IPsec
    - Aushandlung von Sicherheitsassoziationen
    - jetzt IKEv2
  - **anderes Protokoll:** Oakley Key Determination Protocol

IKEv2


IKEv2
Initiator
IKE_SA_INIT Request
Proposed Sas, Keying Information, Nonce
IKE_SA_INIT Response
Accepted SA, Keying Information, Nonce
IKE_AUTH Request
Identity and Auth Info,
CHILD_SA Proposal and Traffic Selectors
IKE_AUTH Response
Accepted CHILD_SA Proposals and
Traffic Selectors
IKEv2
Responder

IPSEC

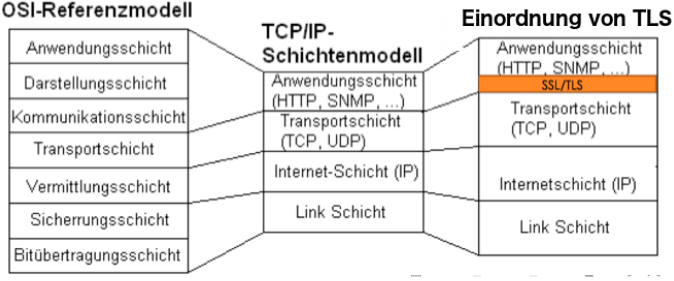
- Überblick über die IPsec Standardisierung

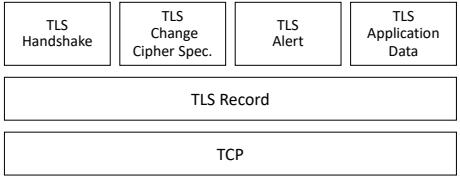


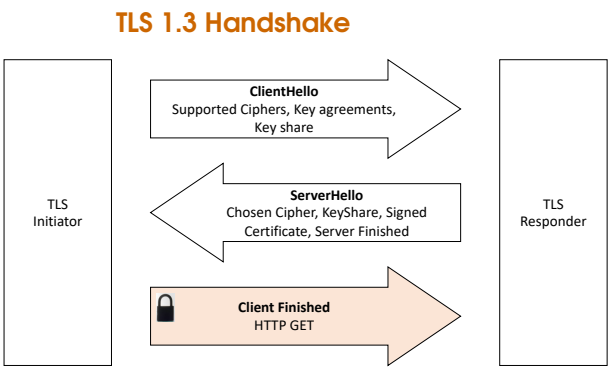
Transport Layer Security (TLS)

Idee von TLS:

- Vertraulichkeit und Authentizität
- Verwendung des Sitzungskonzepts
  - entstammt OSI-Konzept (Schicht 5)
  - längere Gültigkeitsdauer als eine Verbindung
  - kann mehrere Verbindungen enthalten
  - Kryptographische Verfahren und Hashfunktionen werden pro Verbindung ausgehandelt
  - Weiterentwicklung von SSL 3.1







Wichtige Teilprotokolle

- TLS Record
  - Berechnung eines MAC
  - Verschlüsselung der Daten und MAC
  - Fragmentierung und Komprimierung der zu übertragenden Daten
- TLS Handshake
  - Aushandlung von Sitzungsparametern
  - Sicherung der Konsistenz von Sitzungsinformationen

TLS Zusammenfassung

Vorteile

- Möglichkeit, jedes höhere Protokoll auf Basis von TLS zu implementieren.
- Unabhängigkeit von Applikationen und System gewährleistet
- wird von fast allen Browsern und Servern unterstützt

Nachteile

- Verbindungsaufbau auf Serverseite sehr rechenintensiv
- keine klare Trennung Authentifizierungs- und Schlüsselalgorithmen (Cipher Suiten implizieren bestimmte Kombinationen)
- keine Verhandlungsdynamik (einfacher Abgleich / Reduzierung der verwendeten Verfahren)

Sicherheitslage von TLS

- TLS 1.3 (und mit Abstrichen) TLS 1.2 gelten als sicher
- TLS 1.1 und ältere SSL-Versionen enthalten eine Reihe von Designschwächen und Sicherheitslücken
- Fallback auf ältere Protokollversionen und schwache CipherSuites wird regelmäßig für Angriffe genutzt

Danke für Ihr Interesse

Fortsetzung folgt