Netzsicherheit – Architekturen und Protokolle
IP Security (IPsec)

1. Bausteine der Datensicherung
2. IPsec
3. Bewertung

Netzsicherheit – Architekturen und Protokolle
IP Security (IPsec)

1. Bausteine der Datensicherung
2. IPsec
3. Bewertung

Entwurfsentscheidung:

In welcher Reihenfolge sollten MAC und Verschlüsselung angewendet werden?

Reihenfolge Sicherungsmechanismen

- Erst verschlüsseln, dann authentifizieren
  - schnelles Verwerfen von nicht authentischen Paketen
    - Ziel: DoS-Angriffe einschränken
    - Empfänger prüft erst die Authentizität
    - Entschlüsselung nur von authentischen Paketen
    - DoS-Angriff aber nur minimal erschwert
  - Entschlüsselung mit dem falschen Schlüssel nicht erkennbar
- Erst authentifizieren, dann verschlüsseln
  - nur der verschlüsselte MAC für Eve sichtbar
    - grundsätzlich: nur der äußere Sicherungsmechanismus direkt angreifbar
    - Schneier, Ferguson: „Authentizität wichtiger als Vertraulichkeit“
  - Horton-Prinzip
    - „You should authenticate what you mean, not what you say“
- Auch gleichzeitig möglich

Schnittstelle: Schlüsselaustausch

Entwurfsentscheidung:

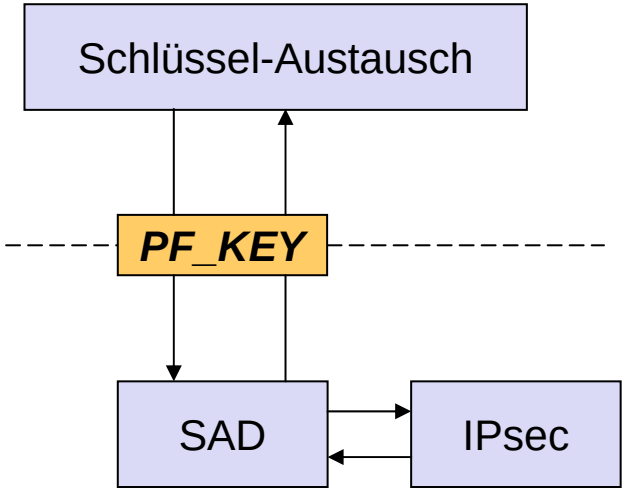
Wie entkoppelt man Schlüssel-austausch und Sicherung?

PF_KEY Key Management API

Key Management API

→ Generisches Management von Schlüsseln

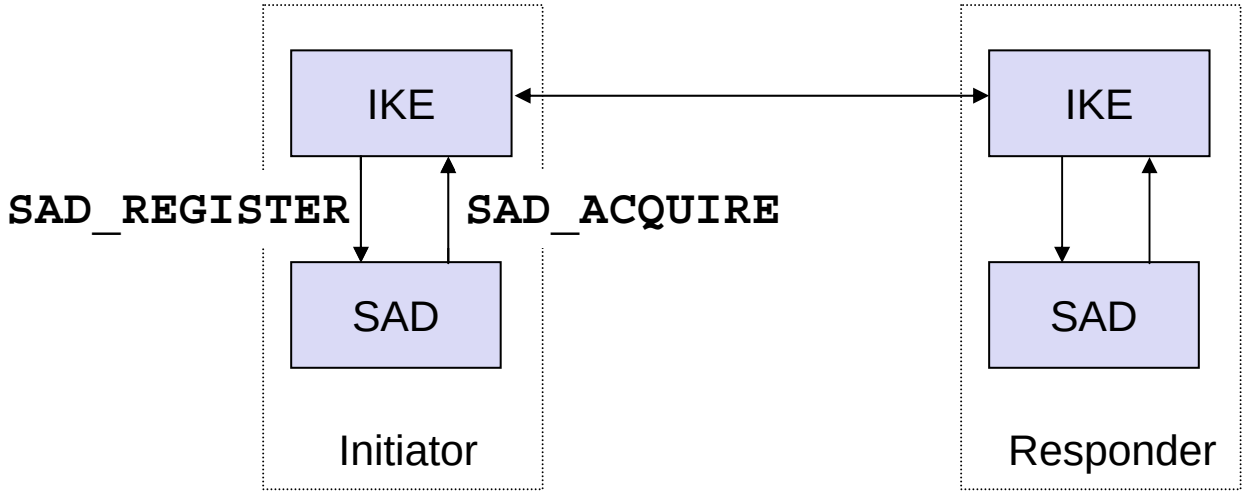
- Konfigurationsschnittstelle SAD
  - **S**ecurity **A**ssociation **D**atabase
  - IPsec-Funktionalität im Kern, im Netzwerk-Treiber oder in Hardware
  - SA aus User-Space Programm (manuell oder automatisch)
  - Nachrichten-basierte Kommunikation



- Konzeptionelles Modell
  - neue SA erforderlich für ausgehendes IP-Paket
  - Anfordern der SA von Schlüsselaustausch-Programm
  - Setzen der SA bei Kommunikationspartnern (Initiator und Responder)

PF_KEY-API Nachrichten

- Anmeldung eines Schlüsselaustauschprogramms
  - **`SAD_REGISTER`**
  - eine Nachricht pro SA-Typ (AH, ESP, …)
  - Antwort enthält vollständige Liste aller im Kern unterstützten Algorithmen
- Anfordern von Sicherheitsparametern
  - **`SAD_ACQUIRE`**
  - mehrere ausstehende Anforderungen möglich



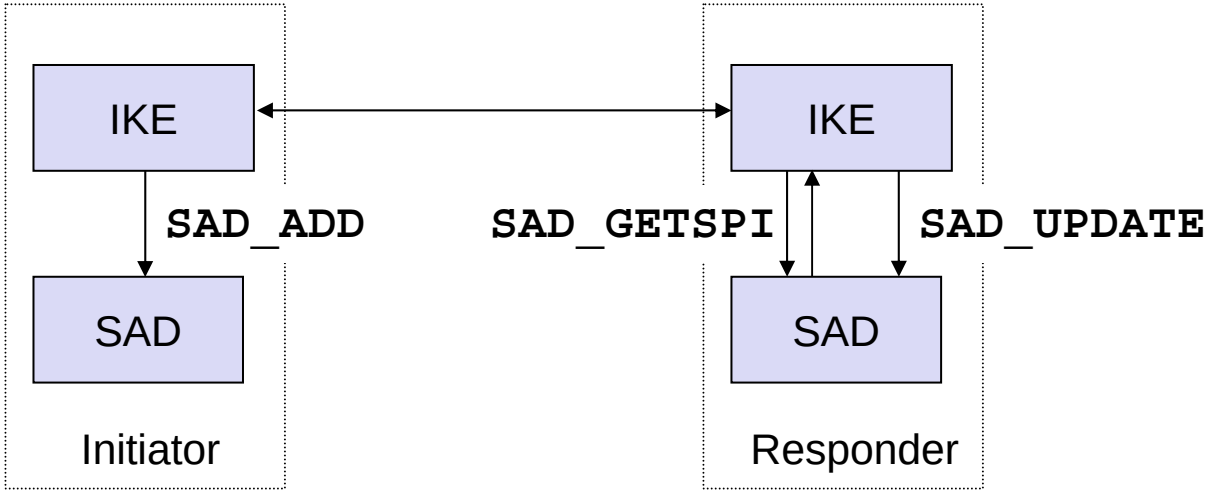
PF_KEY-API Nachrichten

Setzen der SA für den Responder (zwei Nachrichten)

- **`SAD_GETSPI`**: SAD des Responders legt SPI der SA fest, um Eindeutigkeit des SPI beim Responder zu garantieren. Anlegen einer Platzhalter-SA in SAD
- **`SAD_UPDATE`**: füllt die Platzhalter-SA mit Daten

Setzen der SA für den Initiator

- **`SAD_ADD`**



PF_KEY-API Nachrichten

Weitere Funktionen

SAD_EXPIRE	Aufforderung zur Neu-Aushandlung der SA zum Warnungs-Zeitpunkt
SAD_DELETE	Löschen einer SA aus der SAD
SAD_FLUSH	Löschen aller SAs eines Typs aus der SAD
SAD_GET	Auslesen der Sicherheits-Parameter durch eine Applikation
SAD_DUMP	Anzeigen aller SAs eines Typs (optional, für Debugging)

Baustein: Sequenznummern

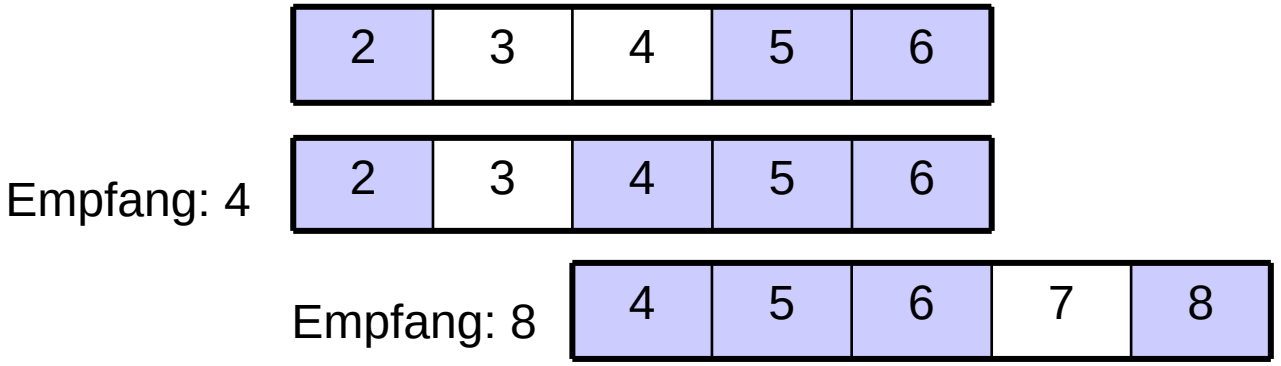
- Sequenznummern
  - eindeutig und monoton wachsend
  - Ende der sicheren Verbindung bei Zählerüberlauf
    - Neuaushandlung des Schlüsselmaterials
  - Aufgaben
    - Erkennung von Wiederholungsangriffen
    - mögliche Quelle für Initialisierungsvektor (IV)
      - für z.B. Counter-Modus
    - Anzeige von verloren gegangenen Paketen (nicht bei IPsec)
- Empfänger
  - Sequenznummer echt größer als letzte empfangene?
    - JA: Paket akzeptieren und Nummer speichern
    - NEIN: Paket verwerfen

Sequenznummernfenster

Fenstermechanismus für Sequenznummern auf Empfängerseite

- Erster Test der SA-Verarbeitung für schnelle Paket-Verwerfung
  - Verwerfen von Duplikaten
- Verfahren
  - Oberes Ende des Empfangs-Fenster ist höchste empfangene Sequenznummer
  - Unteres Ende ist um n kleiner als oberes Ende
    - IPsec: n=64 (Empfehlung)
  - Verwerfen von Paketen unterhalb des Fensters u. bereits erhaltene Pakete
  - Markieren von bereits empfangenen Sequenznummern

Beispiel für Fenstergröße 5 (weiß → noch nicht empfangen)



Netzsicherheit – Architekturen und Protokolle
IP Security (IPsec)

1. Bausteine der Datensicherung
2. IPsec
3. Bewertung

IP Security (IPsec)

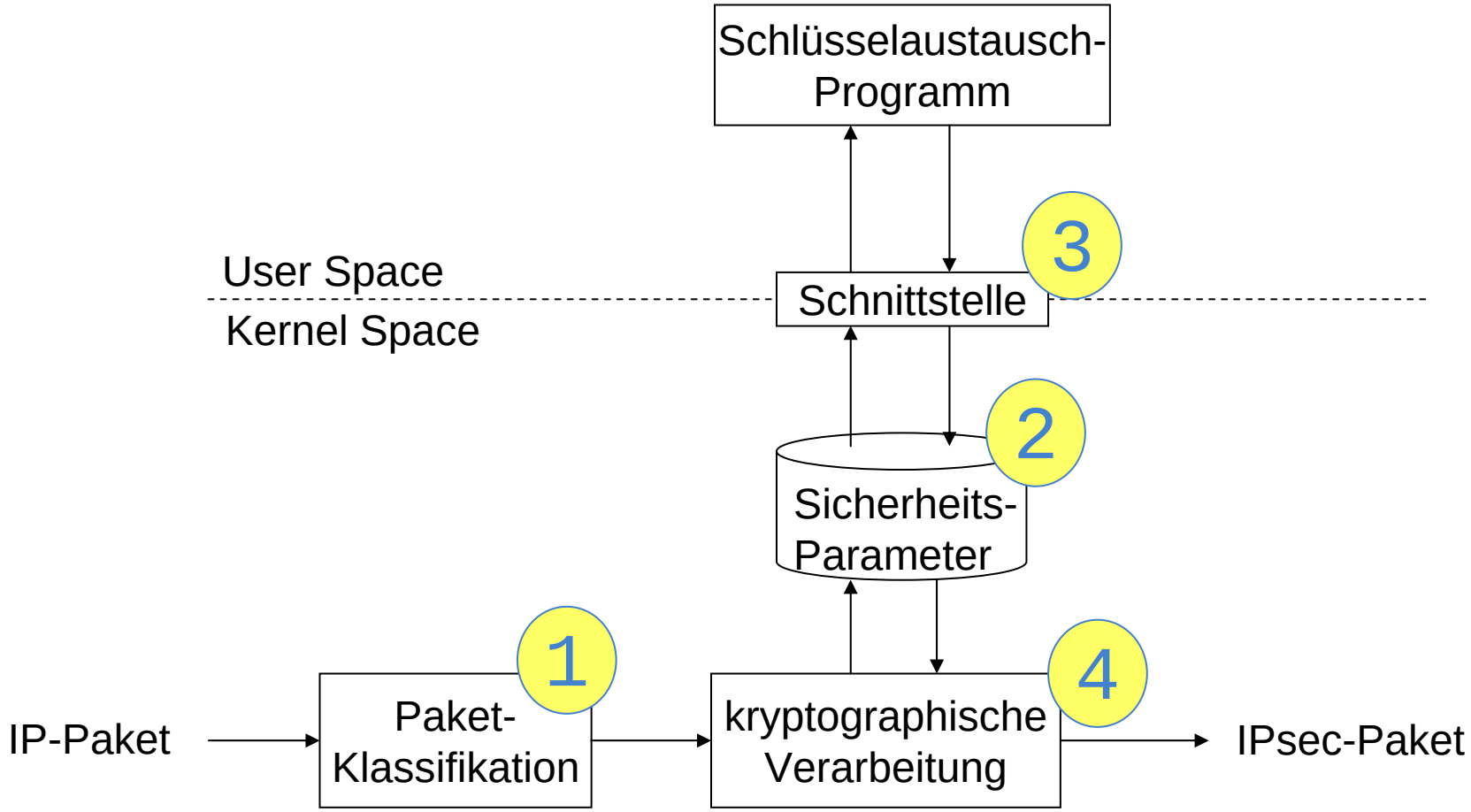
IPsec: Erweiterung des IP-Protokolls

- Zwei neue Protokolle (als Protokollköpfe bei IPv4, als Erweiterungsköpfe bei IPv6)
- Authentication Header (AH): Protokoll für Replay-Schutz sowie Daten- und Sender-Authentifizierung
- Encapsulating Security Payload (ESP): Protokoll zur Daten-Authentifizierung, Replay-Schutz und Vertraulichkeit

- IPsec definiert ausschließlich den gesicherten Datenkanal
  - Schlüsselaustausch durch IKE
  - Speicherung des Schlüsselmaterials in einer Datenbank
  - Multiplexen mehrerer IP-Ströme auf einen Kanal

IPsec im Überblick

Schema der IPsec-Verarbeitungsschritte eines ausgehenden IP-Pakets



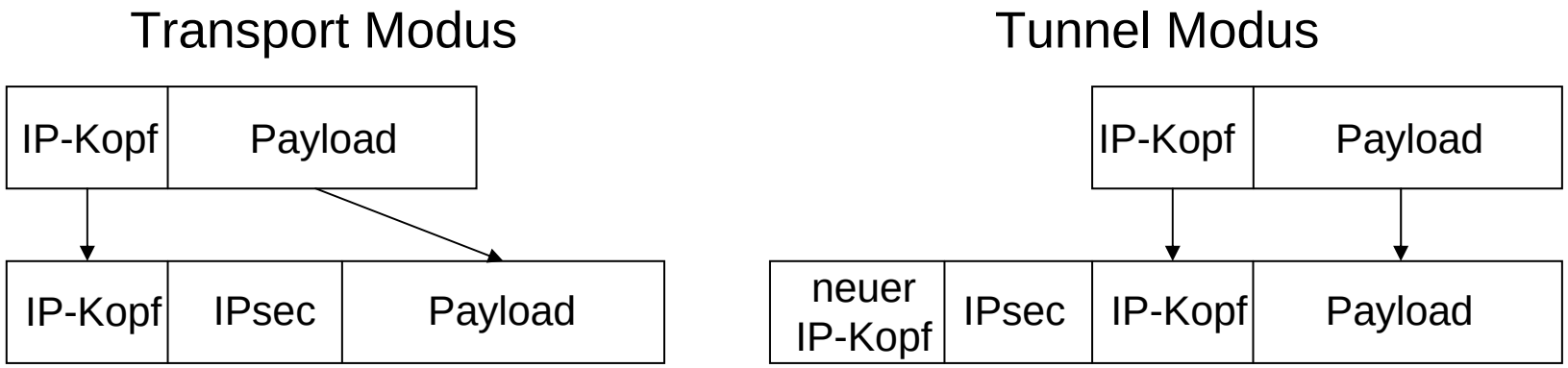
Sicherheitsparameter

- Sicherheitsbeziehung (Security Association – SA)
  - zwischen zwei IP-Instanzen
  - unidirektional
  - ermöglicht Vertraulichkeit und/oder Authentizität der Daten

- SA-Parameter
  - IPsec-Protokoll: AH oder ESP
    - Authentifizierungsalgorithmus mit Schlüssel, usw.
    - Verschlüsselungsalgorithmus mit Schlüssel, usw.
  - IPsec-Übertragungs-Modus: Tunnel oder Transport
  - Lebenszeit der SA
    - in Bytes oder Zeiteinheiten gemessen
    - Soft-Lifetime (Warnung), Hard-Lifetime (SA deaktiviert)
  - Sequenznummernzähler
  - Anti-Replay-Empfangsfenster beim Empfänger
  - Path Maximum Transfer Unit (Path MTU)
    - für Fragmentierung notwendig

IPsec Übertragungsmodi

- Transport-Modus
  - Einfügen von Sicherheitsinformationen in das IP-Paket selbst
- Tunnel-Modus
  - IP-in-IP Kapselung
  - Anhängen der Sicherheitsinformationen an äußeren IP-Paketkopf
  - Anwendung
    - Security Gateway als Stellvertreter für Endsysteme eines Netzes
    - Nutzung von privaten IP-Adressen (RFC1918, z.B. 192.168.0.1)



Kryptographische Verarbeitung

- Authentication Header (AH)
  - Authentifizierung des Senders
  - Authentizität der Daten
  - Anti-Replay Protection
- Encapsulating Security Payload (ESP)
  - Authentizität der Daten
  - Anti-Replay Protection
  - Vertraulichkeit der Daten
  - Schutz vor Verkehrsanalyse (nur Tunnel-Modus)

Aufbau einer AH-Dateneinheit

Next Header	Payload Length	Reserved
Security Parameter Index (SPI)		
Sequence Number (Anti-Replay)		
Integrity Check Value (abhängig vom Verfahren)		

- Next-Header-Feld
- Security Parameter Index (SPI)
- Anti-Replay-Sequenznummer
- Authentication Data
  - Integrity Check Value (ICV)

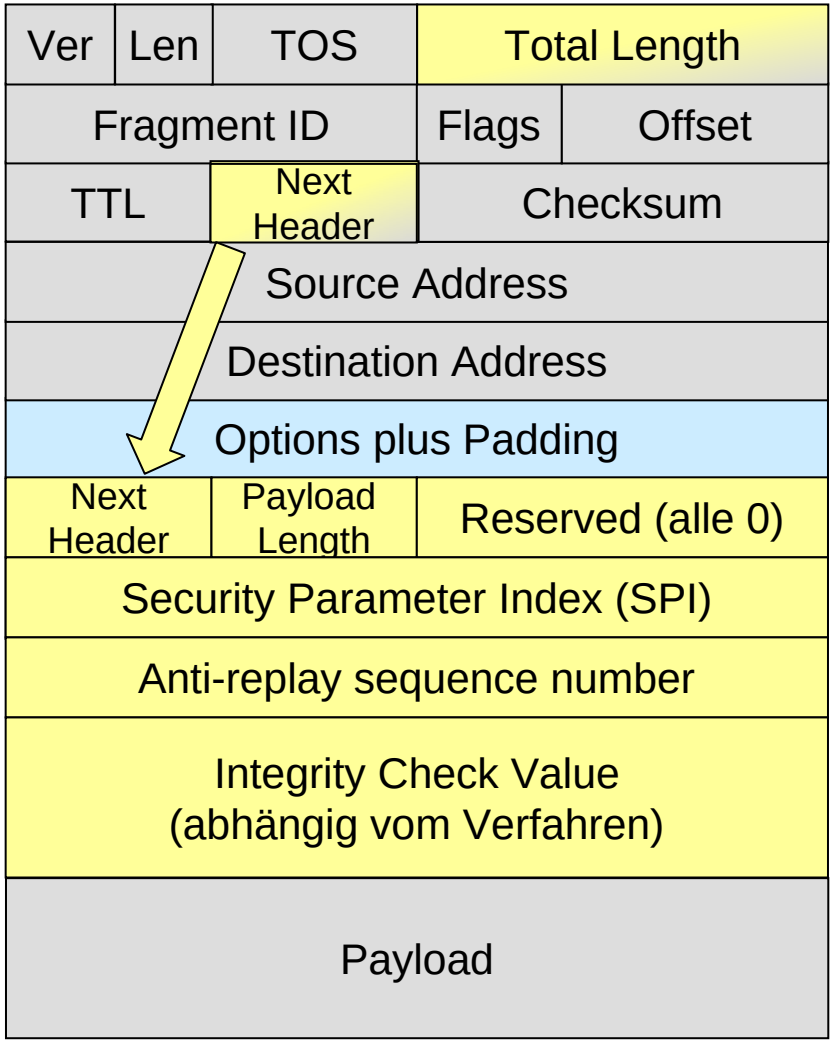
Bearbeitungsschritte des Authentication Header

- Beispiel für IPv4-AH-Transport Mode

Ver	Len	TOS	Total Length	
Fragment ID			Flags	Offset
TTL		Next Header	Checksum	
Source Address				
Destination Address				
Options plus Padding (optional)				
Payload				

Bearbeitungsschritte des Authentication Header

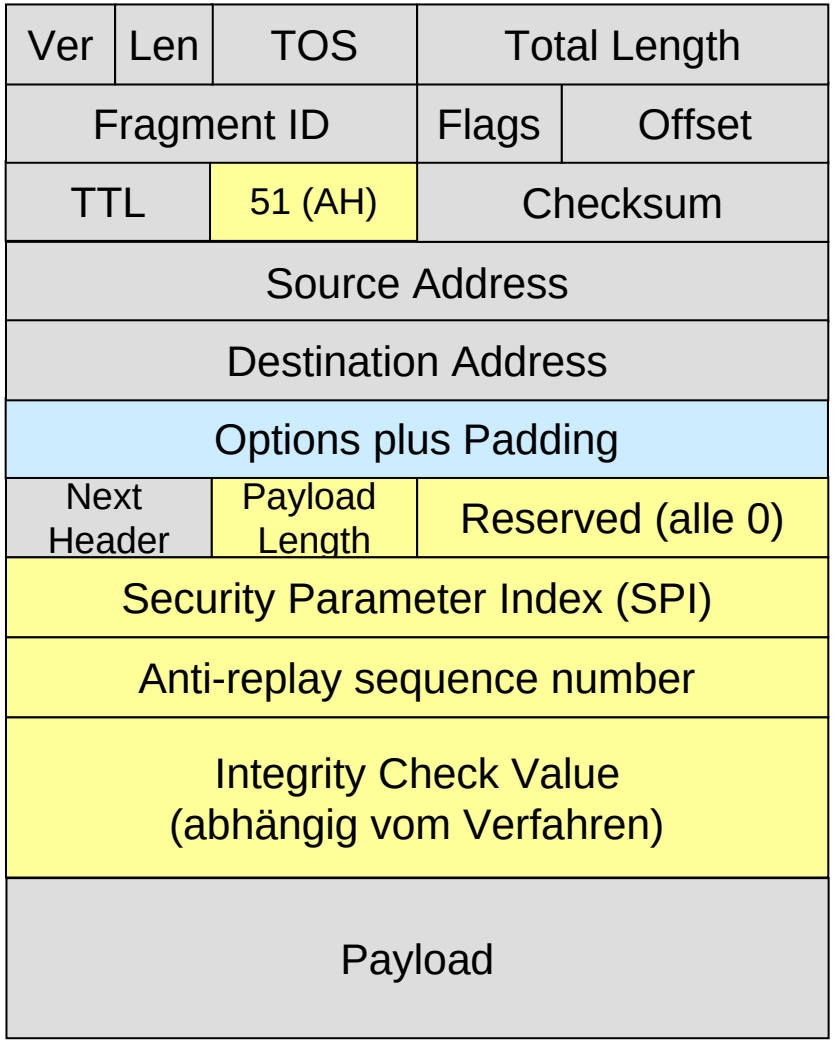
- IPv4-AH-Transport Mode
  1. Einfügen des AH-Templates
  2. Setzen des „Next Header“- und „Payload Length“-Felds
  3. Setzen des SPI für die ausgewählte SA
  4. Setzen der Anti-Replay Sequenznummer
  5. Ändern des IP „Next Header“-Felds im Transport Mode
  6. Berechnung der Authentifizierungs-Daten
  7. Fragmentieren des Pakets, wenn nötig



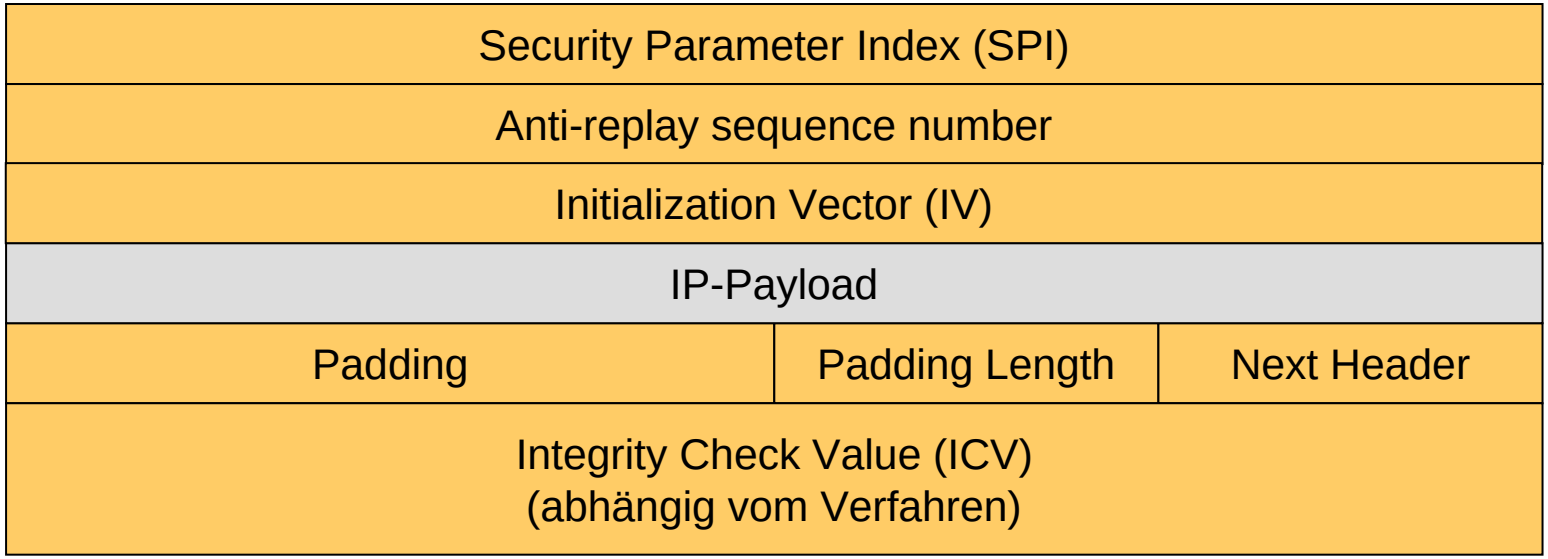
Prüfung beim Empfänger

→ **Wie prüft Empfänger die Authentizität des Pakets?**

→ **Welche Schwierigkeit tritt dabei auf?**



Aufbau einer ESP-Dateneinheit



- ESP-Kopf
  - Security Parameter Index (SPI)
  - Anti-Replay Sequenznummer
  - Initialisierungsvektor
- ESP-Anhang
  - Padding (0 – 255 Byte)
  - Padding Length
  - Next Header
- ESP-Authentication
  - wie AH-Authentication

Probleme

- IPsec und NAT
  - UDP-Encapsulation: Kapselung von IKE und IPsec in UDP
    - UDP-Port 4500 [RFC 3948]
  - AH authentisiert den IP-Kopf
    - Änderungen am äußeren IP-Protokollkopf machen Paket ungültig
    - IPsec muss Änderungen vorher in den ICV einberechnen
      - IKEv2 kann mittels NAT-Traversal die notwendigen Daten bestimmen
- IPsec-Köpfe vergrößern Paket
  - Fragmentierung notwendig
  - PMTU-Wert muss bestimmt werden!
    - wer tut dies? Sicherheit?
  - zuerst fragmentieren oder zuerst IPsec?
    - erster Fall: Kenntnis der PMTU notwendig / zweiter Fall: DoS möglich
- IPsec und Firewalls
  - häufiger Firewall Selektor: Portnummer
    - bei ESP ist jedoch die Schicht-4 Portnummer verschlüsselt
  - IPsec-fähige Endsysteme sind nicht sicherer als andere

Änderungen

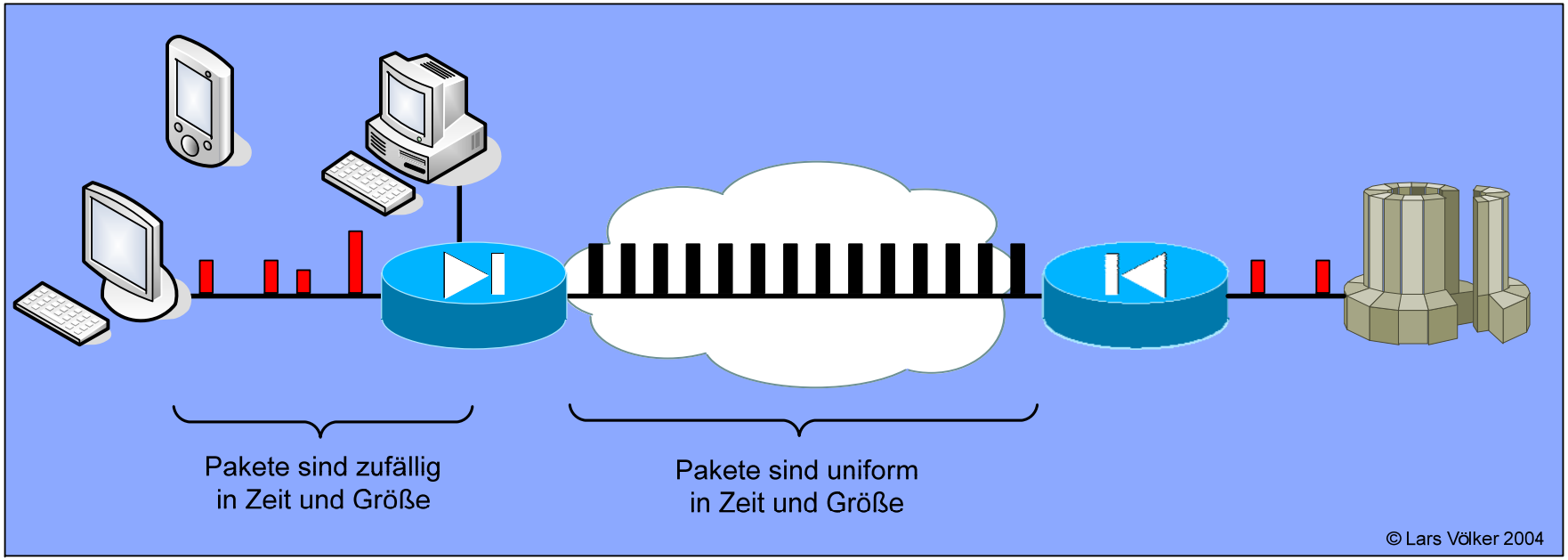
- Seit Dezember 2005 neu
  - IPsec (RFC 4301)
  - AH (RFC 4302)
  - ESP (RFC 4303)
- Im Folgenden erklärte Neuerungen
  - Erweiterte Sequenznummer mit 64 statt 32 Bit möglich
  - Traffic Flow Confidentiality (TFC) Padding
    - Dummy-Pakete einfügen
    - kurze Pakete verlängern

Erweiterte Sequenznummer

- IPsec-Paket hat eine 32-Bit-Sequenznummer
  - das ergibt etwa 4 Milliarden Pakete
  - für schnelle Netze in Zukunft zu wenig
    - Paketrate für 10Gbit/s: 1 Million/Sekunde (1 KByte) ~ 1,12 h
- Extended Sequence Number (ESN): 64 Bit
  - Für Abwärtskompatibilität können allerdings nur 32 Bit im Nachrichtenkopf stehen
  - Lösung:
    - untere 32 Bit werden übertragen
    - obere 32 Bit nur in der SA geführt
    - die kompletten 64 Bit werden in den ICV eingerechnet und somit in den Schutz aufgenommen

Traffic Flow Confidentiality

- Idee: keine Informationen mittels Paketgröße und Frequenz verraten
  - Padding bis zu 64k Paketgröße
  - Dummy-Pakete einfügen (IP-Protokoll 59)



Netzsicherheit – Architekturen und Protokolle
IP Security (IPsec)

1. Bausteine der Datensicherung
2. IPsec
3. Bewertung

Bewertung

- Kritik von Bruce Schneier und Niels Ferguson

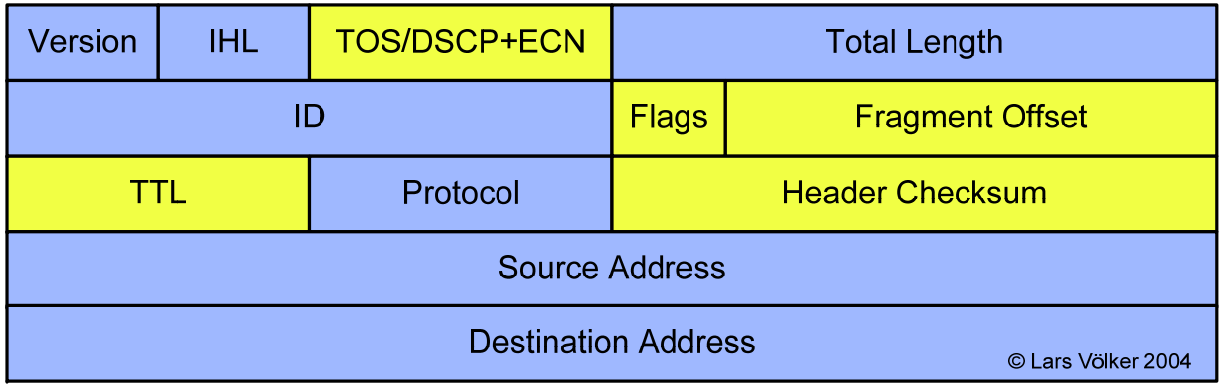
Kritikpunkte (basierend auf dem Stand Ende 1998)

- IPsec zu komplex
  - praktisch nicht möglich, IPsec ausreichend fehlerfrei zu programmieren
  - zu viele unterschiedliche Interessen berücksichtigt
- IPsec schlecht dokumentiert
  - Designziele werden in Dokumenten nicht ausreichend beschrieben. Leser weiß oft nicht, was die Funktionalitäten bedeuten
  - Varianten unterscheiden sich oft kaum
  - Vorschlag: auf AH und Transportmodus ganz verzichten

AH unnötig!?

- AH schützt alle blauen Felder
  - aber: Version, IHL, Protocol und Destination Address sind korrekt
    - sonst wäre das Paket nicht angekommen
  - Schutz der ID relativ wertlos, vor allem solange keine Fragmentierung
  - Schutz von Total Length wertlos, da sonst ICV falsch

- übrig: Source Address – aber was sagt die aus?



- gelb: veränderbar
- blau: geschützt

Literatur

Bücher (beziehen sich noch auf RFC240x-IPsec von 1998)

- S. Frankel; Demystifying the IPsec Puzzle; Artech House, 2001
  - sehr gutes IPsec-Buch
- C. Kaufmann, R. Perlman, M. Speciner; Network Security – Private Communication in a Public World; Prentice Hall; 2003
  - allgemeineres Buch

Standards und Papers

- RFC4301 – RFC4308 Dez. 2005 IPsec Standards, IETF
  - aktuelle Standards
- Furguson, N und Scheier, B.; A Cryptographic Evaluation of IPsec“, http://www.counterpane.com/ipsec.html, Feb. 1999
- Simpson, W.; IKE/ISAKMP Considered Dangerous; Draft; Jun. 1999
- RFC 2401 – RFC 2409 1998 IPsec Standards, IETF
  - veraltete Standards