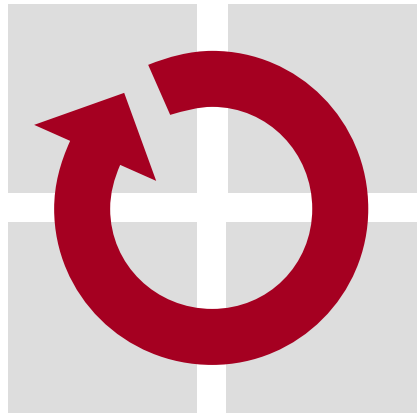
IPSec

Markus Weiten

markus@weiten.de



Lehrstuhl für Informatik 4
Verteilte Systeme und Betriebssysteme
Universität Erlangen-Nürnberg

Inhalt

- Motivation, Ansätze
- Bestandteile von IPsec (Kurzüberblick)
- IPsec Modi
- Bestandteile von IPsec – Übertragungsprotokolle
- Bestandteile von IPsec – Konfigurationsdatenbanken
- IPsec in Aktion

Das Internetprotokoll garantiert nicht:

- Dass eingehende IP-Pakete vom angegebenen Sender (Ursprungsadresse im IP-Header) stammen
- Dass die Daten unterwegs nicht böswillig verändert wurden
- Dass niemand anderes die Daten auf ihrem Weg eingesehen hat

Was ist zu tun ?

Es besteht Bedarf an:

- Integrität
- Authentizität
- Vertraulichkeit

Ansätze

- Sicherheit auf der Anwendungsschicht
  - SSL
  - SSH
  - PGP
- Anwendungsspezifisch, nicht transparent
- Implementierungsoverkill

Ansätze (2)

- Sicherheit auf der Transportschicht
  - Transport Layer Security (TLS)
- Keine Implementierung für UDP
- Teilweise immer noch Änderungen an den Anwendungen notwendig

Ansätze (3)

- Sicherheit auf der Datenübertragungsschicht
  - 802.1x
  - PAP
- transparent
- Erfordert dedizierte Verbindung

Ansätze (4)

- Sicherheit auf der IP-Schicht
  - IPsec
- Transparenz
- keine Anwendungen müssen angepasst werden
- Aufbau von VPNs möglich

Bestandteile von IPSec

- Übertragungsprotokolle
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)

Bestandteile von IPSec

- Übertragungsprotokolle
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- Konfigurationsdatenbanken
  - Datenbank für Sicherheitsassoziationen (SADB)
  - Datenbank für Sicherheitsstrategien (SPD)

Bestandteile von IPSec

- Übertragungsprotokolle
  - Authentification Header (AH)
  - Encapsulating Security Payload (ESP)
- Konfigurationsdatenbanken
  - Datenbank für Sicherheitsassoziationen (SADB)
  - Datenbank für Sicherheitsstrategien (SPD)
- Key Management Protokolle
  - IKE
  - ISAKMP
  - Photuris

IPsec Modi

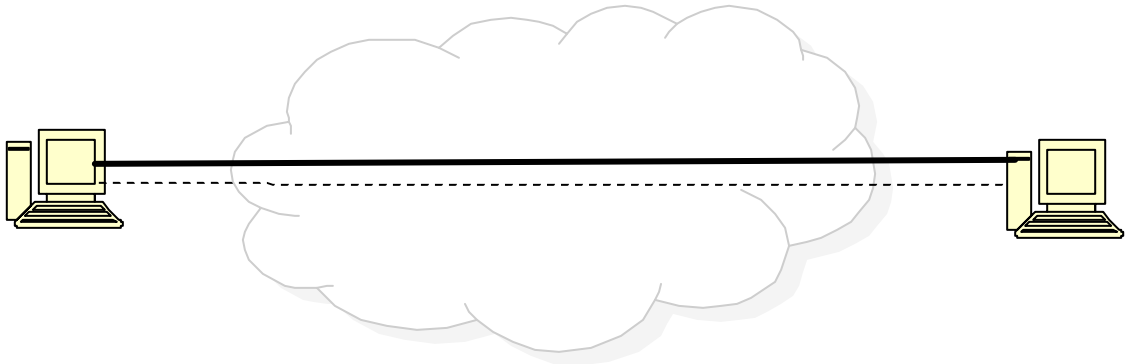
- Zwei verschiedene Modi: Transport- und Tunnelmodus
- Transportmodus: Zwischen IP-Header und restlichem Paket wird ein IPsec-Header eingefügt, der die sicherheitsrelevanten Informationen trägt:

IP Header	TCP/ UDP H.	Payload

IP Header	IPsec Header	TCP/ UDP H.	Payload

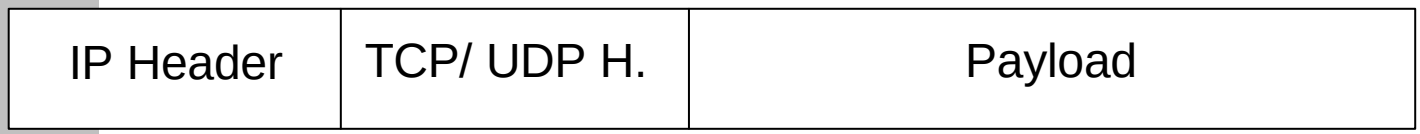
IPsec Modi (2)

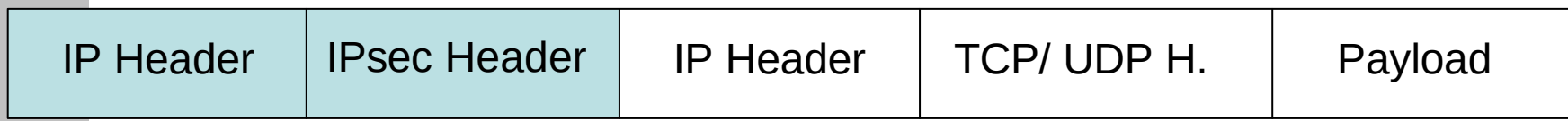
- im Transportmodus Peer-to-Peer Sicherung möglich:



IPsec Modi (3)

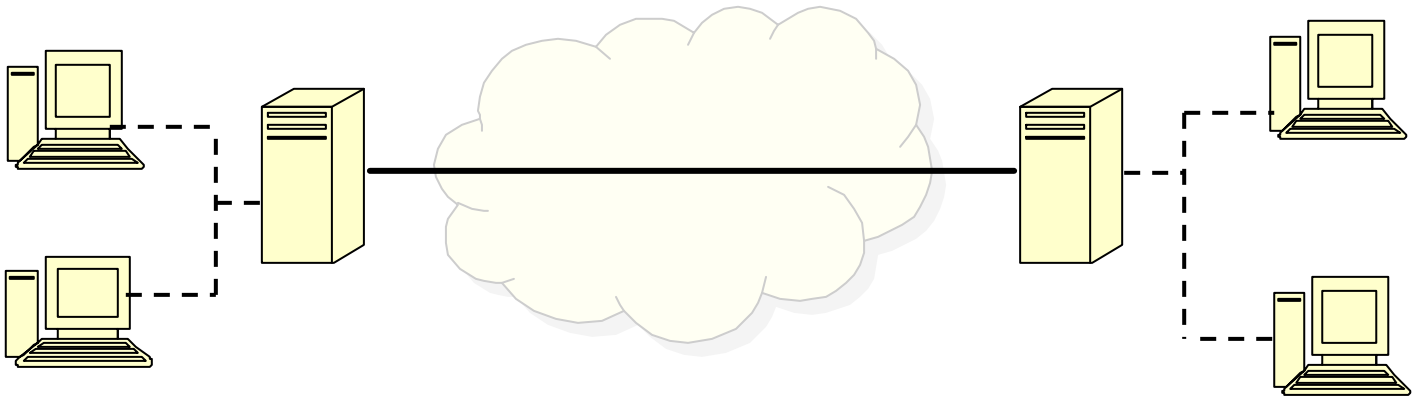
- Tunnelmodus: Datenpaket wird in ein komplett neues Datenpaket gekapselt





IPsec Modi (4)

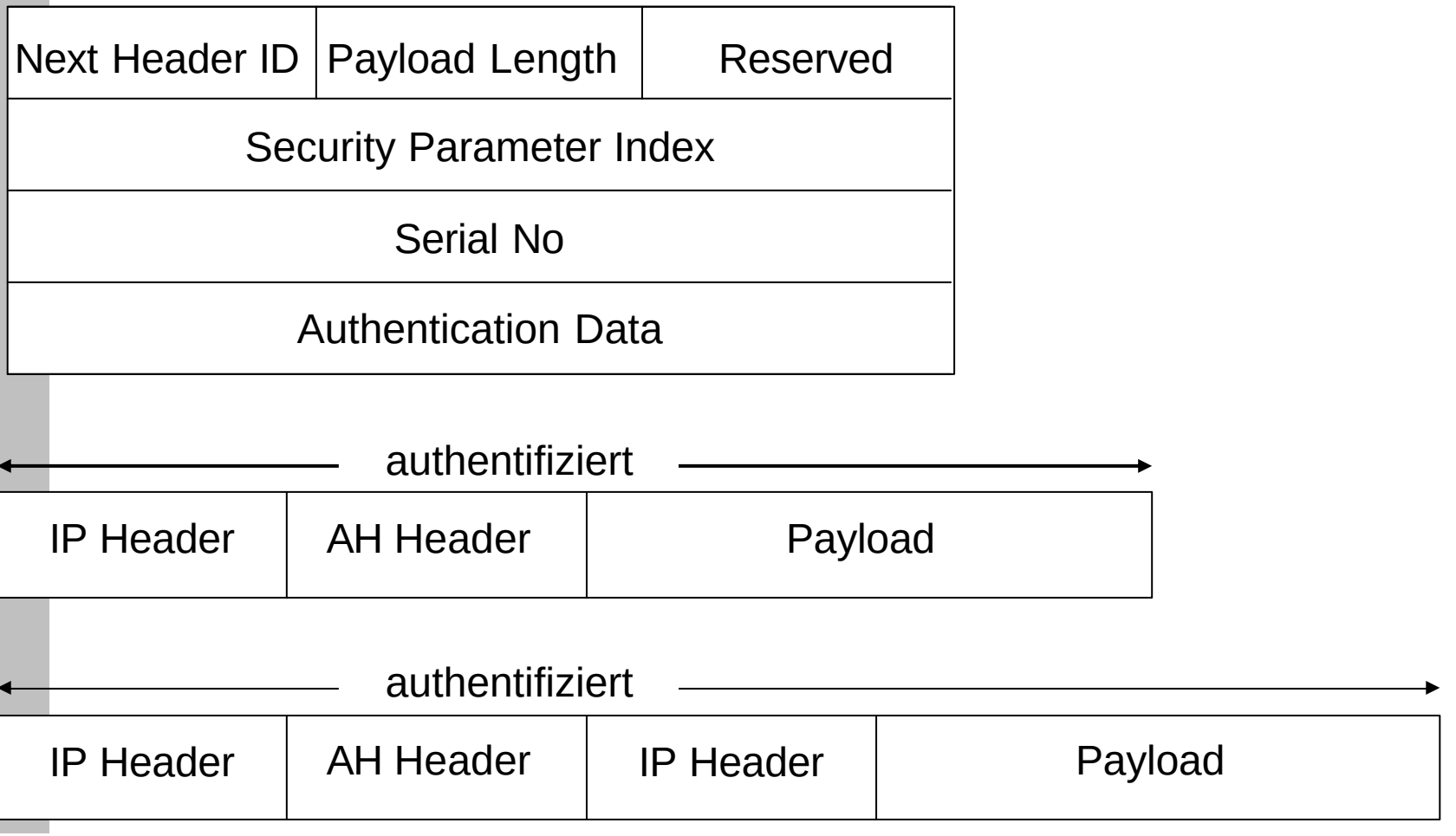
- im Tunnelmodus Netz-zu-Netz Sicherung möglich:



Authentication Header

- Zusätzlicher Header
- Bietet:
  - Authentizität des Absenders
  - Integrität der Daten
  - Schutz vor wiederholtem Senden von Paketen (Replay-Attacken)

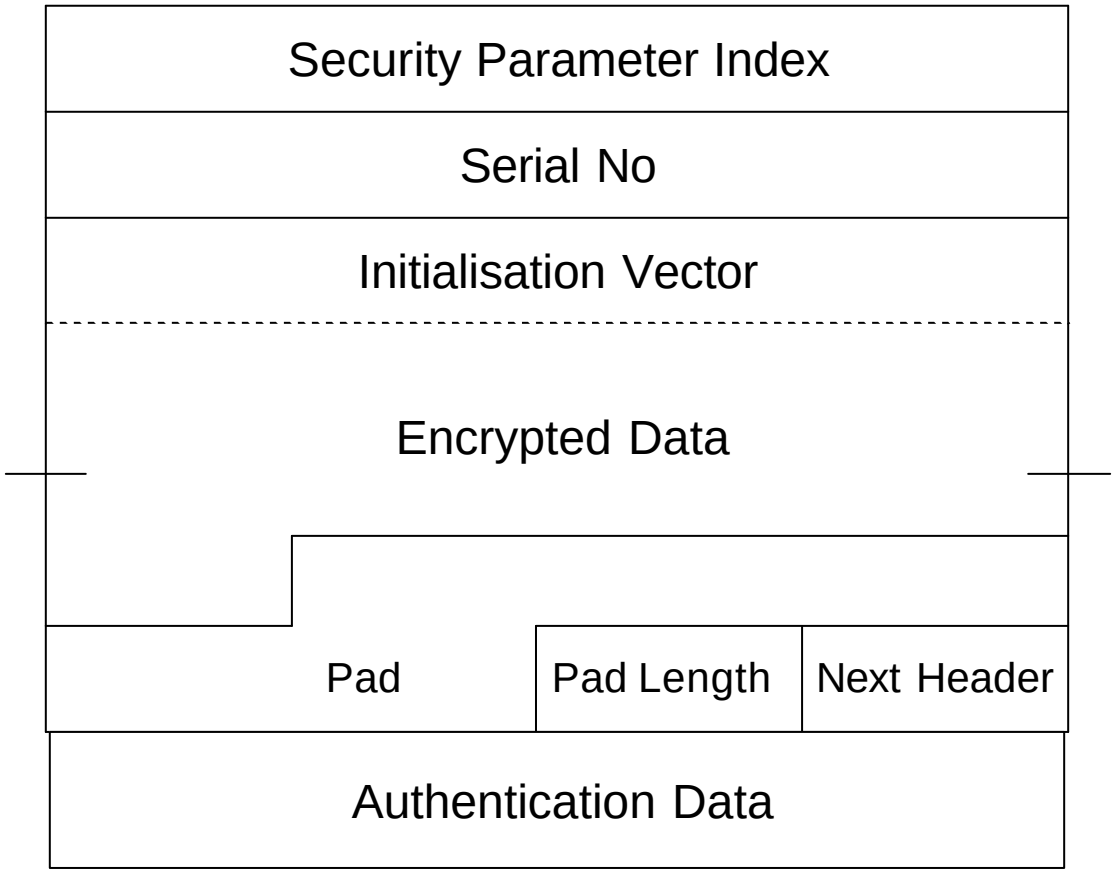
Authentication Header graphisch



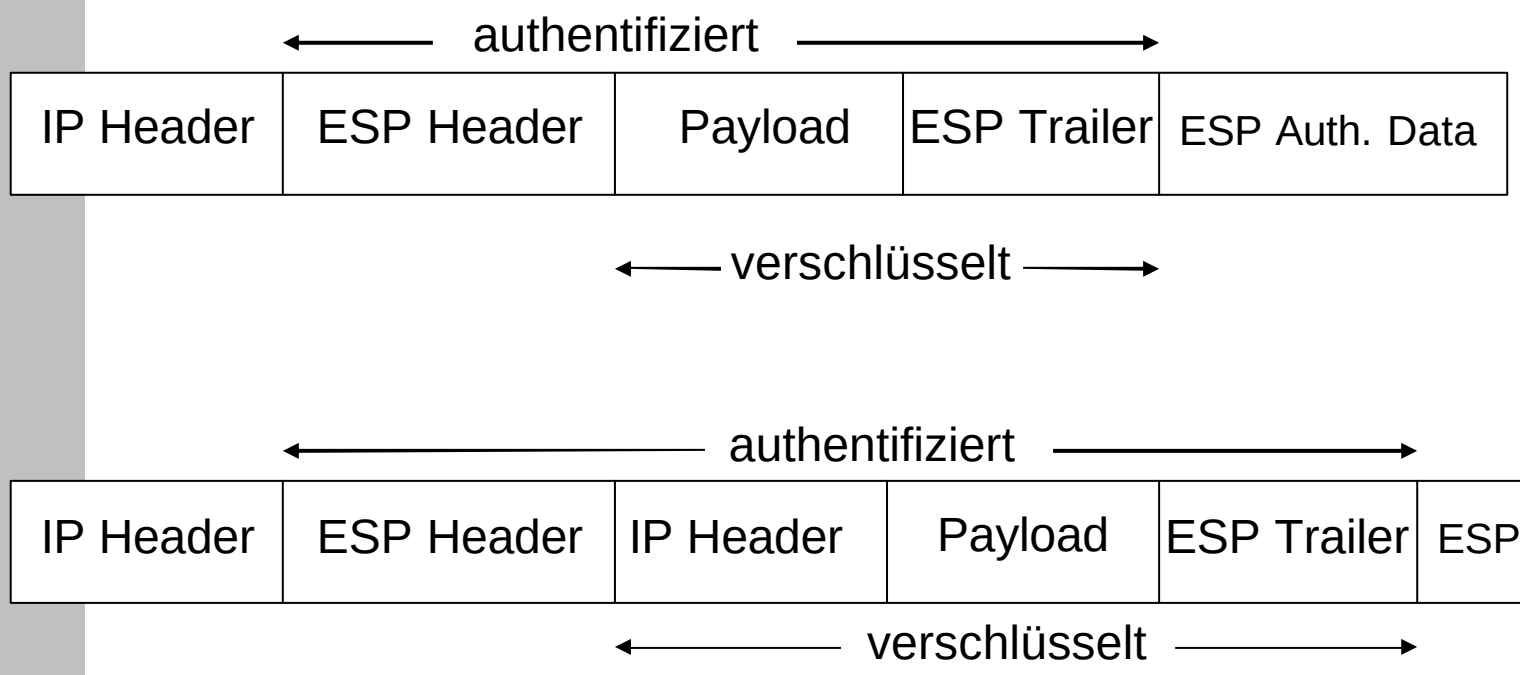
Encapsulating Security Payload (ESP)

- Zusätzlicher Header + Trailer
- Bietet:
  - Authentizität des Absenders
  - Integrität der Daten
  - Schutz vor wiederholtem Senden von Paketen (Replay-Attacken)
  - Vetraulichkeit

ESP graphisch



ESP graphisch (2)



Datenbank für Sicherheitsstrategien

- Wie wird eingehendes/ausgehendes Paket behandelt?
- 3 Aktionen:
  - Keine Sicherheit wird angewandt (bypass)
  - Sicherheit wird angewandt (apply)
  - Paket wird verworfen (discard)
- Zugriff anhand von Selektoren
- Die vom Admin definierbare Konfiguration

Datenbank für Sicherheitsstrategien

- Selektoren:
  - Ursprungsadresse
  - Zieladresse
  - Protokoll (TCP oder UDP)
  - ULP (upper layer ports)

SADB

- Datenbank von Sicherheitsassoziationen
- Eine Sicherheitsassoziation beschreibt, wie man mit anderem Host kommuniziert (Krypto-Parameter)
  - Gilt in eine Richtung
  - Jeweils für eingehenden/ausgehenden Verkehr
  - => pro Host zwei SAs für eine Verbindung
- Tripel <SPI, destination address, protocol> legt Eintrag eindeutig fest
- Security Associations werden automatisch vom Key Management erzeugt
- Manuelle Erzeugung möglich

SADB (2)

- Parameter:
- Generische Parameter (von beiden Protokollen benutzt)
  - Seriennummer
  - Seriennummerüberlauf
  - Fenster gegen wiederholtes Senden
  - Lebensdauer
  - Modus
  - Tunnel-Zielort
  - PMTU-Parameter

SADB (3)

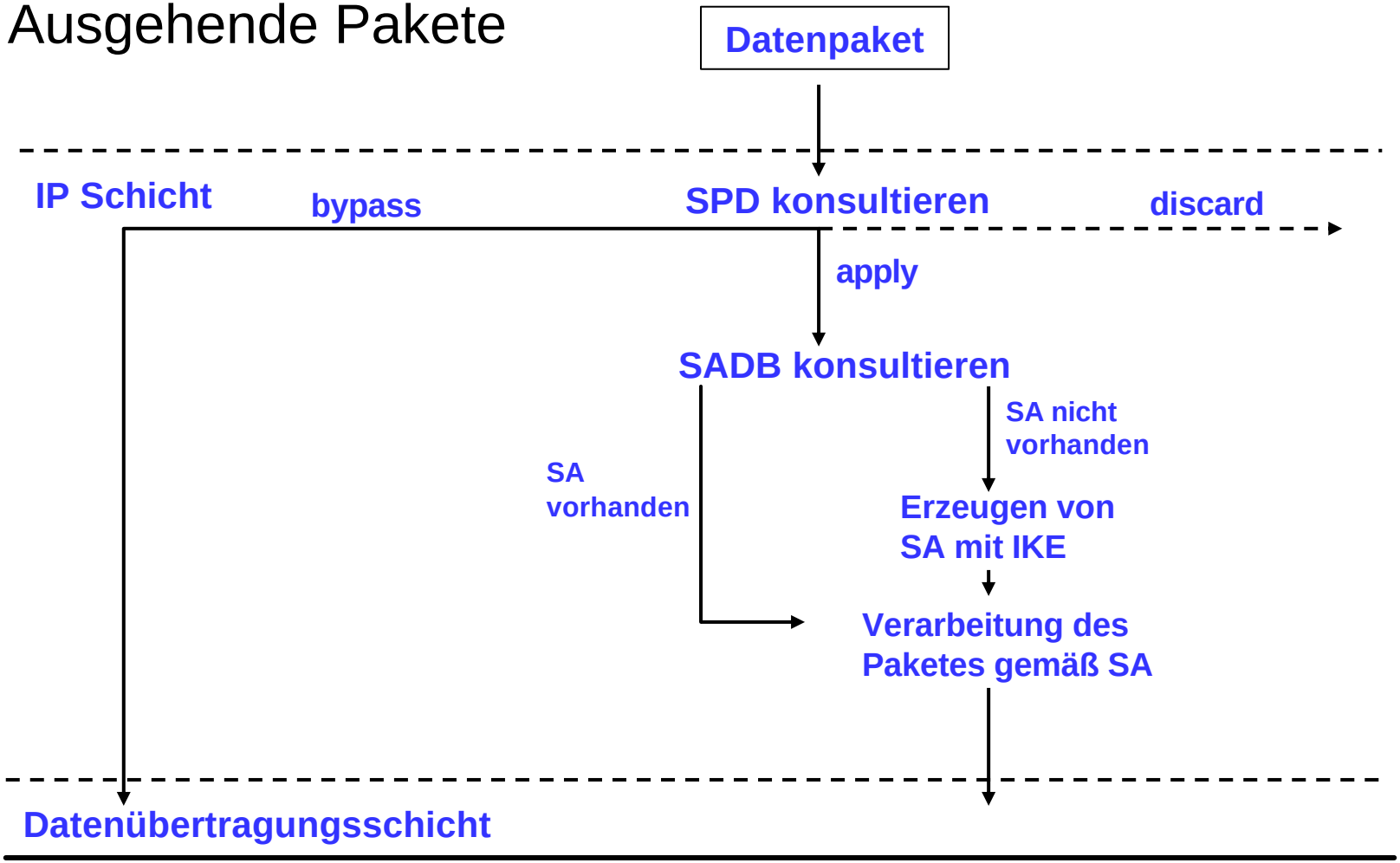
- Protokollspezifische Parameter
  - Schlüssel
  - Authentifikationsalgorithmus
  - Verschlüsselungsalgorithmus

Security Parameter Index (SPI)

- 32 Bit Zahl
- Wird in jedem Paket im Klartext mitgeführt
- Ermöglicht den Hosts Zuordnung von Datenpaketen zu Security Associations
- Wird vom Schlüsselmanagement beim Verbindungsaufbau vom Empfänger vereinbart

IPsec in Aktion

- Ausgehende Pakete



IPsec in Aktion

- ausgehende Verarbeitung bei AH

Next Header ID	Payload Length	Reserved
Security Parameter Index		
Serial No		
Authentication Data		

Seriennummer = ++Seriennummer der SA;

SPI = SPI der SA;

Payload Length = # 32-Bit Worte - 2;

Authentication Data = 0;

Next Header ID = Protocol (IP-Header);

Veränderliche Felder des IP-Headers = 0;

Ver.	IHL	TOS	Total Length
Identification		Flags	Fragment Offset
TTL	Protocol	Header Checksum	
Source Address			
Destination Address			

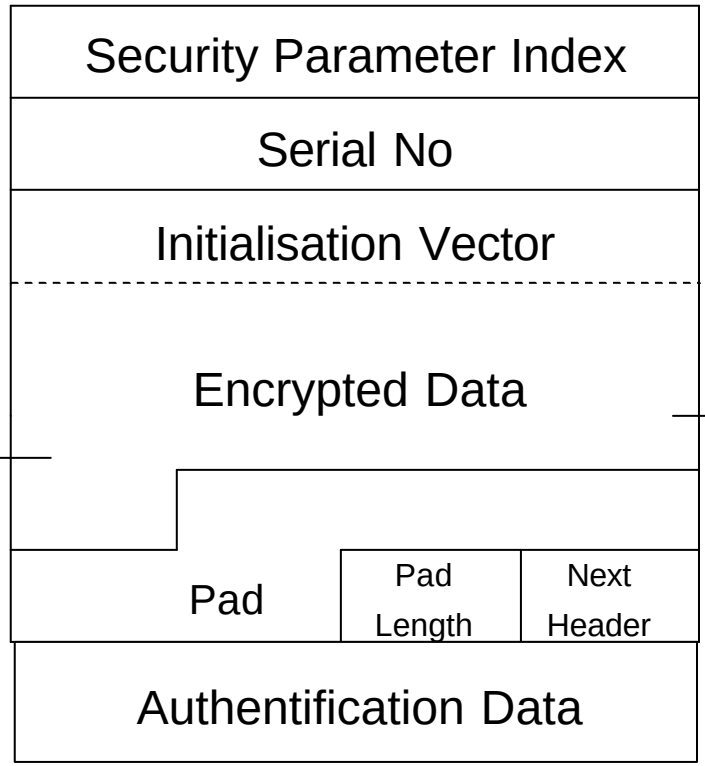
Komplettes Paket (incl. Payload) wird zusammen mit dem Schlüssel aus der SA dem Authentifizierungsalgorithmus übergeben;

Authentication Data = Ergebnis des Algorithmus;

Übergabe an Datenübertragungsschicht;

IPsec in Aktion

- ausgehende Verarbeitung bei ESP

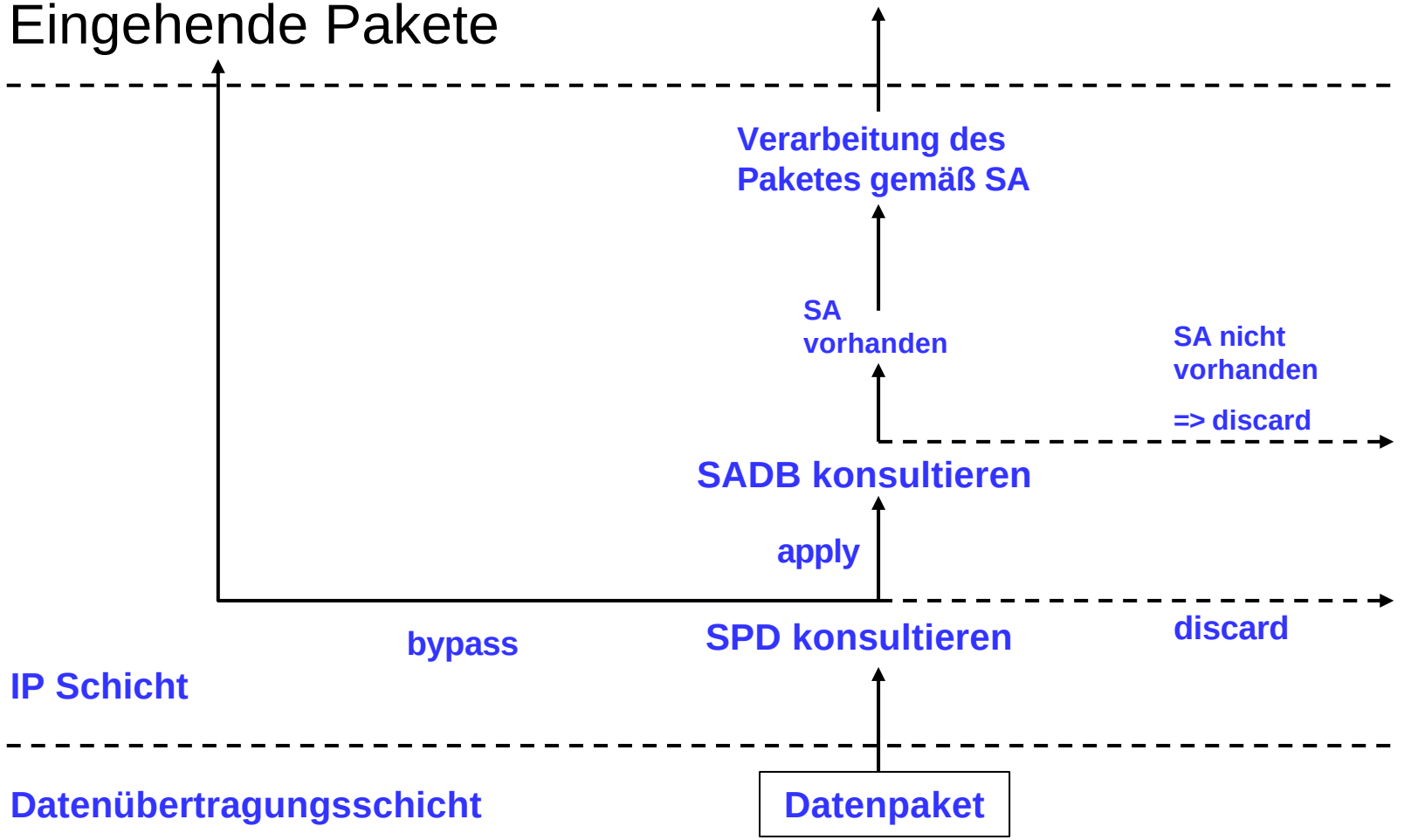


SPI = SPI der SA;
Seriennummer = ++Seriennummer der SA;
Berechnung der benötigten Fülldaten;
Anfügen der Fülldaten an die Payload;
Next Header ID = Protocol (IP-Header);
Verschlüsselung gemäß SA;
Init-Vektor entsprechend Algorithmus belegen;
Authentifizierung ähnlich AH;

Übergabe an Datenübertragungsschicht;

IPsec in Aktion

- Eingehende Pakete



Zusammenfassung

- IPsec bietet Vertraulichkeit, Authentizität, Integrität
- 2 Modi: Transportmodus für Host-zu-Host
  Tunnelmodus für Netz-zu-Netz Sicherheit
- Übertragungsprotokolle: AH und ESP
- Konfigurationsdatenbanken:
  - Security Policy Database
  - Security Association Database

Quellen

[1] IPsec
Naganand, Doraswamy, Harkins
Addison-Wesley, 2000

[2] Security im Überblick: Teil 4, Sicherheit auf der Netzwerkschicht
Axel Sikora
http://www.tecchannel.de/software/1168/index.html, 2003

[3] Angriffsmethoden und IPsec
Munich Network Management Team
http://wwwmnmteam.informatik.uni-muenchen.de/Literatur/MNMPub/Foprras/fack00/HTML-Version/node48.html

[4] Virtual Private Network – Mit sicherem Tunnel durchs Internet (Diplomarbeit)
Olivier Gärtner, Berkant Uneal
Zürcher Hochschule Winterthur, 1999