1 IPsec Hintergrund

1.1 Überblick

IPv4 kannte ursprünglich keine Sicherheitsaspekte. Das Protokoll wurde unter den Aspekten Geschwindigkeit und Robustheit entwickelt. Bei IPv6 wurde bereits während der Standardisierungsphase auch die Sicherheit berücksichtigt. Diese Prinzipien wurden später auf IPv4 in Form des Protokolls IPsec übertragen. IPsec garantiert beim Einsatz von ESP[1] (s. Kapitel 1.5) die drei Hauptaspekte eines VPN:

- Vertraulichkeit
- Integrität
- Authentizität

Weiterhin kann über IPsec die **Zugangskontrolle** (Access Control) für Protokolle umgesetzt werden, sowie ein **Anti-Replay-Schutz**. Bei IPSec handelt es sich um ein sogenanntes Layer-3 Tunneling Protokoll. Andere Varianten von VPN-Protokollen werden in einem späteren Abschnitt diskutiert.

Die Basis der Übertragung bei IPsec bilden die beiden Unterprotokolle ESP und AH[2] (s. Kapitel 1.4). Genau genommen umfasst ESP auch den AH und bildet damit beides ab. IPsec setzt für die Verschlüsselung **symmetrische Schlüssel** ein, d.h. beide Kommunikationspartner nutzen den identischen Schlüssel (vgl. Kapitel 1.1.2).

Der Austausch der benutzten Schlüssel erfolgt entweder **manuell/statisch (Administrator)** oder **automatisch (IKE[3])**. Die manuelle Variante ist zwar in der Grundkonfiguration und beim Verbindungsaufbau einfacher, dafür aber auch anfälliger gegenüber Angriffen, sofern die Schlüssel nicht regelmäßig händisch aktualisiert werden.

Idealerweise werden die Schlüssel einer Verbindung automatisch ausgehandelt und wechseln während einer Session mehrmals. Dies kann per manueller Konfiguration nicht gewährleistet werden.

Bei IPsec wird der automatische Austausch der Sicherheitsparameter (s. Kapitel 1.1.4 sogenannte SAs) mittels IKE durchgeführt. IKE baut hierzu zunächst einen gesicherten Kanal auf und verhandelt darüber die eigentlichen Schlüssel. Die genaue Vorgehensweise wird in Kapitel 1.2 beschrieben.

IKE übernimmt dabei die Aufgaben:

- Authentifizierung der Kommunikationspartner
- Aushandlung der verwendeten Algorithmen
- Aushandlung der Verwaltungsinformationen
- Schlüsselaustausch mittels DH-Verfahren[4]

IKE existiert in zwei Versionen. IKEv1 ist problematisch beim Einsatz in IPv4-Umgebungen, daher wurde IKEv2 entwickelt, womit u.a. NAT- und DHCP-Probleme eliminiert werden können. IPsec wurde in Hinblick auf IPv6 entwickelt und lässt daher Aspekte wie NAT außen vor. In IKEv2 werden solche Verbindungen über UDP erneut gekapselt.

Die Authentifizierung wird über sogenannte Hash-Verfahren sichergestellt, die im nächsten Kapitel erläutert werden.

1.1.1 Hash-Algorithmen

Zur Sicherstellung der Integrität und Authentizität wird der Hash-Algorithmus HMAC[5] verwendet. HMAC wird u.a. in den Varianten **HMAC-MD5-96** und **HMAC-SHA-1-96** eingesetzt. Bei MD5 wird ein 128 Bit bei SHA-1 ein 160 Bit Schlüssel verwendet. Der Algorithmus errechnet bei SHA-1 aus dem Schlüssel und den Nutzdaten einen 160 Bit [6]langen Hash-Wert, von dem die 96 (daher der Name) höchstwertigsten Bits als HMAC verwendet werden.

1 ESP: **E**ncapusulation **S**ecurity **P**ayload
2 AH: **A**uthentication **H**eader
3 IKE: **I**nternet **K**ey **E**xchange; Protokoll zum Schlüsselaustausch
4 DH: **D**iffie **H**ellmann-Verfahren; Verfahren zum Austausch von symmetrischen Schlüsseln
5 HMAC: **H**ash **M**essage **A**uthentication **C**odes; Schlüsselbasiertes Hash-Verfahren
6 bei MD5 ist dieser Wert 128 Bit lang

1.1.2 Verschlüsselungsalgorithmen

Um die Vertraulichkeit sicherzustellen, werden bei IPsec die Nutzdaten so „verwürfelt", dass nur der Empfänger der im Besitz eines entsprechenden Schlüssels zum „entwürfeln" in der Lage ist die Nutzdaten wiederherzustellen. Zur Verschlüsselung der Daten wird bei IPsec u.a. **CBC-DES**[7] bzw. **CBC-3DES**, **AES**[8] eingesetzt. (vgl. Vertiefung Kryptografie). Dabei handelt es sich um sogenannte **symmetrische Verfahren**, die bei beiden Kommunikationspartner denselben Schlüssel voraussetzen. Dieser Schlüssel wird sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet.

Im Gegensatz dazu verwenden **asymmetrische Verfahren** zwei Schlüssel einen privaten (private key) und einen öffentlichen (public key) Schlüssel. Dabei wird der öffentliche Schlüssel zum Verschlüsseln verwendet und der private Schlüssel zum Entschlüsseln. Vorteil eines asymmetrischen Verfahrens ist es, dass nur die öffentlichen Schlüssel ausgetauscht werden müssen. Sollte also ein Angreifer an diesen Schlüssels gelangen, so kann er maximal Daten korrekt verschlüsseln. Die verschlüsselten Daten kann er damit jedoch nicht wiederherstellen.

1.1.3 Anti-Replay-Schutz

Um die Wiederholung von mitgeschnittenen Datenpaketen (z.B. für spätere Angriffszwecke) zu verhindern wird der Anti-Replay-Schutz eingesetzt. Dabei werden die Pakete sinngemäß durchnummeriert und nur Pakete, die innerhalb eines aktuell gültigen Nummernbereich liegen, werden weiterverarbeitet. Damit können „alte" Pakete direkt erkannt werden und bereits frühzeitig verworfen werden.

1.1.4 Die Security Association[9]

Mit der SA wird festgelegt, mit welchen Sicherheitsmechanismen die IP-Pakete geschützt werden sollen. Eine SA bezieht sich jeweils auf die Übertragung in EINE Richtung (unidirektional). Für eine bidirektionale Übertragung werden demnach zwei SAs benötigt. Ein VPN-Gateway hat für gewöhnlich viele Verbindungen (z.B. Mitarbeiter, die sich ins Firmennetz einwählen sollen), damit sind entsprechend viele SAs zu verwalten. Dies geschieht in der sogenannten SAD[10]

Eine SA enthält folgende Informationen:

`SA=[Source/Destination-IP-Address, SPI[11], Protocol, Auth-Algorithm]`

`Source/Destination-IP-Address` legt die Endpunkte bzw. Netze fest.

Der `SPI` ist ein Verweis auf die Security Policy, die für diese Verbindung angewendet werden soll. Diese Policies werden in einer eigenen Datenbank SPD[12] verwaltet. Eine Policy kann ähnlich einer Firewall-Regel verstanden werden. Mit einer Policy wird u.a. die Notwendigkeit der Verschlüsselung festgelegt.

Ein Eintrag in der SPD enthält darüber hinaus noch andere Informationen wie die Verschlüsselungsverfahren oder Schlüssel.

Mit `Protocol` wird die Art der Erweiterung des IP-Paketes dokumentiert. Es kann folgende Werte annehmen:

`Protocol = AH` oder `ESP`

Der letzte Parameter `Auth-Algorithm` legt fest, mit welchem Hash-Verfahren die Authentizität sicher gestellt wird. Hier kann beispielsweise HMAC-SHA-1 oder HMAC-MD5 eingesetzt werden.

Die SAs werden bei den jeweiligen Kommunikationspartnern hinterlegt.

1.1.5 Die Security Policy

Die SAs legen fest wie die Daten behandelt werden. Erst eine Security Policy legt fest **welches** Paket **wann mittels IPsec** verarbeitet werden muss oder unverändert einfach dem normalen Routing zugeführt wird. Alle SPs werden in einer SPD gespeichert. Eine Policy kann als Satz von Eigenschaften verstanden werden. Treffen diese Eigenschaften zu, dann wird eine der drei möglichen Aktionen ausgeführt:

`DISCARD` (verwerfen), **`PASS`** (unverändert) oder **`APPLY`** (IPsec-SA anwenden)

7 DES, 3DES: **D**ata **E**ncryption **S**tandard (**Triple** DES); Verschlüsselungsverfahren
8 AES: **A**dvanced **E**ncryption **S**tandard; Verschlüsselungsverfahren nach Rijndael-Algorithmus
9 SA: **S**ecurity **A**ssociation
10 SAD: **S**ecurity **A**ssociation **D**atabase; Verwaltung der SAs
11 SPI: **S**ecurity **P**arameter **I**ndex; Verweis auf einen Eintrag in der SPD
12 SPD: **S**ecurity **P**olicy **D**atabase

Eine SP enthält folgende Informationen:

```
SP=[Source-Range Destination-Range Direction Action Policy]
```

`Source-Range/Destination-range`: Quell-/Ziel-IP-Bereich für den die Policy gelten soll
`Direction`: Eingehende oder ausgehende Richtung der Pakete
`Action`: ipsec, discard, none wie soll mit dem Paket verfahren werden
`Policy`:

- protocol IPsec Protokoll [ah|esp]
- mode Modus für Tunnel [transport|tunnel]
- src_dst Quell-/Ziel-Netz; kann entfallen, wenn genauso wie SA
- level Verschlüsselungslevel [use|require] Verschlüsselung erwünscht / zwingend

1.2 IKE und ISAKMP[13]

Bei IKE wird mittels ISAKMP der Schlüsselaustausch in einer gesicherten Umgebung vorgenommen (Lösung des Henne-Ei-Problems). IKE existiert in zwei Versionen. Version 2 wurde hauptsächlich zur Vereinfachung (IKEv1 gilt als komplex) und zur Lösung der NAT-Problematik entwickelt. IKEv1 wird in zwei Phasen betrieben, die sich grob in eine erste Aufbauphase[14] (Sicherer Verwaltungskanal wird generiert) und eine zweite Übermittlungsphase, in der die Parameter (SAs) für die eigentliche Nutzdatenverbindung ausgehandelt werden, aufteilen. Die folgenden Abbildung zeigt den Nachrichtenfluss im sogenannten Main Mode mit RSA-Authentifizierung.

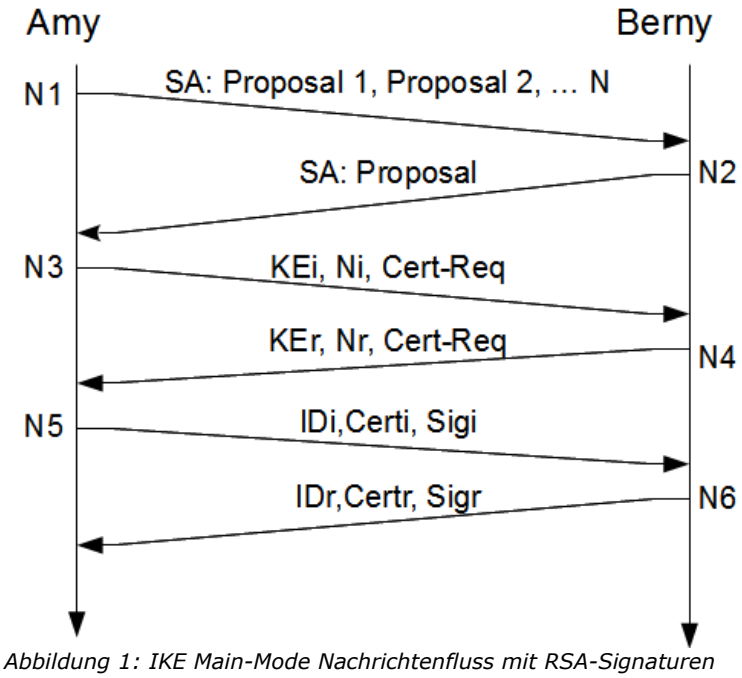

Abbildung 1: IKE Main-Mode Nachrichtenfluss mit RSA-Signaturen

Nachrichten	Bemerkung	Phase
N1, N2	Angebot (Proposal) von Parametersätzen für die ISAKMP-SA und Einigung auf eine gemeinsame SA.	1
N3, N4	Austausch der öffentlichen DH-Berechnung (KEi[15], KEr, Ni[16] und Nr)	2
N5, N6	Abschließend werden mittels der symmetrischen Schlüssel, die aus dem DH-Verfahren ermittelt wurden, eine Identität (IDi, IDr), die Zertifikate (Certi, Certr) und eine Signatur (Sigi, Sigr) verschlüsselt ausgetauscht.	2

Tabelle 1: Erklärung der ISAKMP-Nachrichten

13 ISAKMP: **I**nternet **S**ecurity **A**ssoziation **K**ey **M**essage **P**rotocol
14 Hierfür wird eine eigene SA, die ISAKMP-SA definiert.
15 KEi, KEr: **K**ey **E**xchange **I**nitiator bzw. **R**esponder
16 Ni, Nr: **N**once **I**nitiator bzw. **R**esponder zufälliger Wert für die Berechnung der Signatur

Im Main-Mode gibt es folgende Varianten zur Authentifizierung:

- mit RSA-Signaturen (s.o.)
- mit Public-Key-Verschlüsselung
- mit revidierter Public-Key-Verschlüsselung
- mit Preshared Keys (PSK)

Alle Varianten unterscheiden sich nur in Phase 2 in der die SAs für die eigentliche Datenverbindung ausgehandelt werden.

Die folgende Abbildung zeigt die auch in der Laborübung verwendete Variante mit PSK.

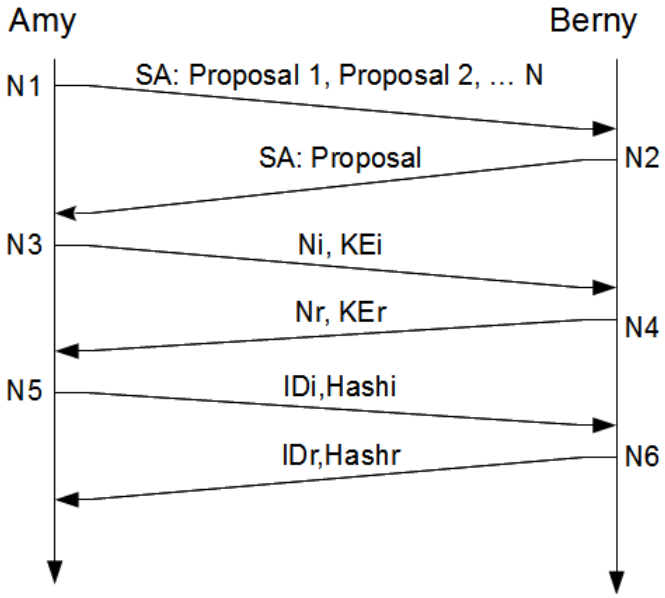

Abbildung 2: IKE Main-Mode Nachrichtenfluss mit Preshared Keys (PSK)

Wesentlicher Unterschied ist das vor dem eigentlichen Verbindungsaufbau der PSK ausgetauscht wurde (konfiguriert) und dieser für die Erzeugung der verwendeten Schlüssel eingesetzt wird. Die so generierten Schlüssel werden in N3 und N4 ausgetauscht. In N5 und N6 werden wieder die verschlüsselten Identität (IDi, IDr) und ein Hash ausgetauscht. Über den Hash kann der Empfänger die Gegenstelle authentifizieren.

1.2.1 Weitere IKE Modi

Neben dem Main Mode gibt noch den sogenannten **Aggressive Mode** und den **Quick Mode**. Der aggressive-Mode stellt eine beschleunigte Variante da, in der bereits drei Nachrichten alle relevanten Daten verschlüsselt übertragen werden. Die ist allerdings auch gleichzeitig die potentielle Schwachstelle des Aggressive Mode, da die Verschlüsselung grundsätzlich mehr Rechenleistung erfordert als ein Klartextnachrichtenaustausch. Schickt ein Angreifer viele Verbindungsaufbaunachrichten, so kann die zu einem DoS führen, da der Empfänger alle Nachrichten zunächst entschlüsseln muss, bevor sie als ungültig verworfen werden können.

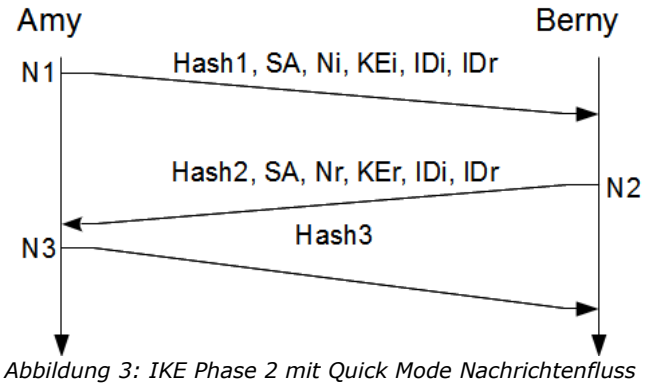

Abbildung 3: IKE Phase 2 mit Quick Mode Nachrichtenfluss

Der Quick-Mode setzt in Phase 2 ein, d.h. Phase 1 wird wie im Main Mode durchlaufen. Mit Hilfe der bereits in Phase 1 ausgetauschten ISAKMP-SAs können die für die eigentliche Verbindung benötigten SAs erzeugt und ausgetauscht werden.

1.3 Tunnel- und Transport-Modus

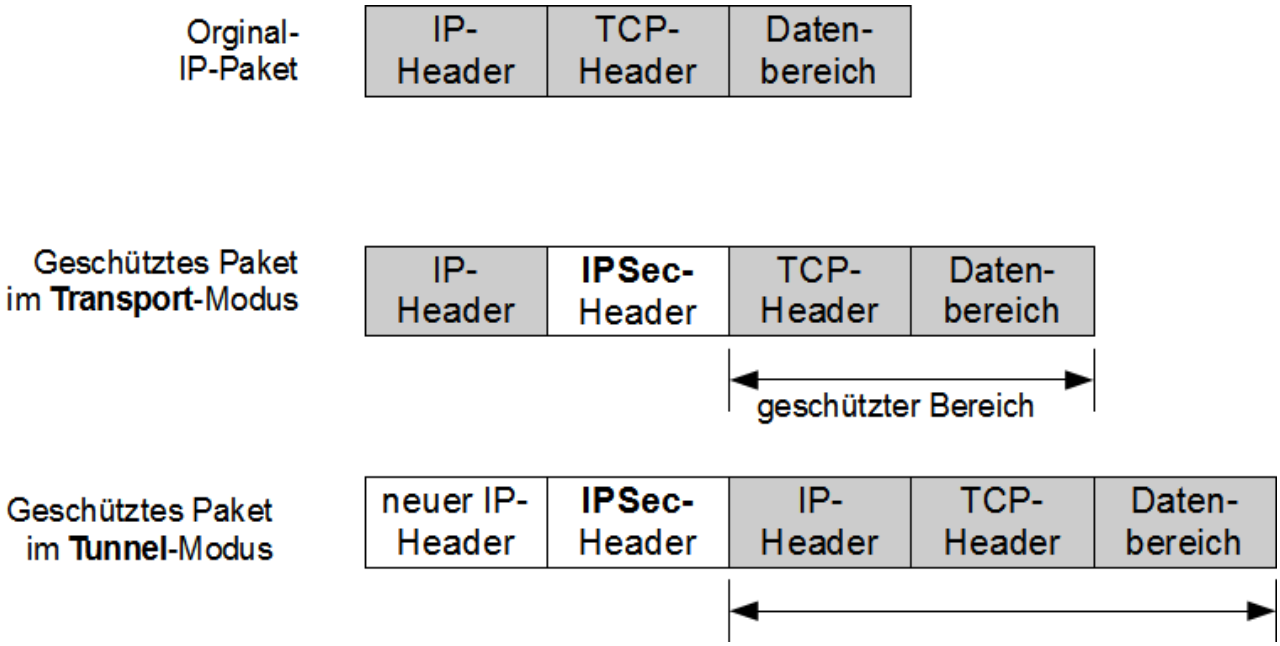

Abbildung 4: Tunnel- und Transport-Modus

Der Transport-Modus ist streng genommen kein VPN, da er das Kriterium „Vertraulichkeit" nicht erfüllt. Die Daten werden zwar gegen Manipulationen geschützt, nicht jedoch gegen das Einsehen, da keine Verschlüsselung eingesetzt wird.

Erst der Tunnel-Modus garantiert auch die Vertraulichkeit (durch Verschlüsselung) und bietet damit eine echte VPN-Verbindung.

1.4 AH[17]

Der AH ist für die folgenden Sicherheitskriterien zuständig:

- Authentifizierung der Datenquelle
  Ist der Absender, der korrekte Absender. Echtheit des Absenders!
- Datenintegrität
  Schutz gegen gezielte Verfälschung der Daten.
- Anti-Replay Schutz
  Schutz gegen Ausspähen des Zielrechners mittels abgefangener Daten.

WICHTIG: Die Vertraulichkeit wird aufgrund der fehlenden Verschlüsselung nicht gewährleistet. Erst mit dem ESP[18] wird diese hergestellt. Das heißt, die Daten sind zwar gegen Manipulationen geschützt, können aber mitgeschnitten werden.

17 AH: **A**uthentication **H**eader
18 ESP: **E**ncapsulation **S**ecurity **P**ayload

1.4.1 Aufbau des AH

Die nächste Abbildung zeigt den Aufbau des AH im Einzelnen.

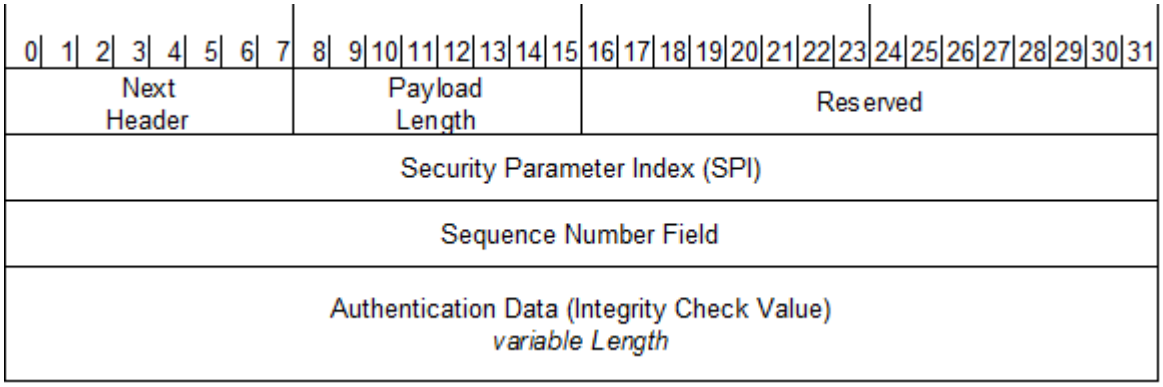

Abbildung 5: Aufbau des AH

Next Header: Header des nachfolgenden Protokolls, welches nach dem AH im IP-Paket folgt.

Payload Length: Länge des AH (minus 2 in 32 bit-Worten)

SPI: Zeiger auf die Stelle in der SPD Datenbank des Zielrechners

Sequence Number: Zur „Durchnummerierung" der IP-Pakete (Anti-Replay-Schutz)

Authentication Data: kryptographische Prüfsumme, die mit geheimen Schlüsseln berechnet wird

1.4.2 AH im Transport-Modus und Tunnel-Modus

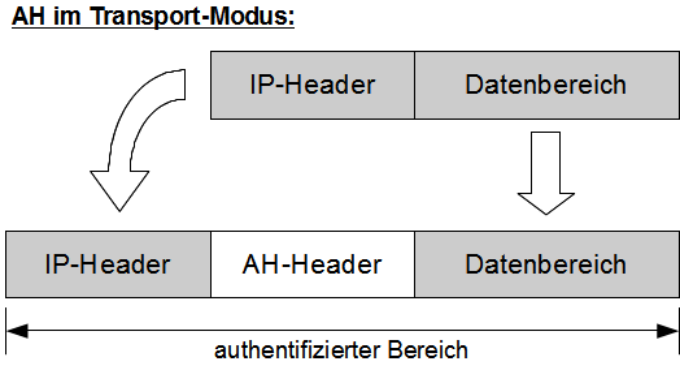

Abbildung 6: AH Header im Transportmodus

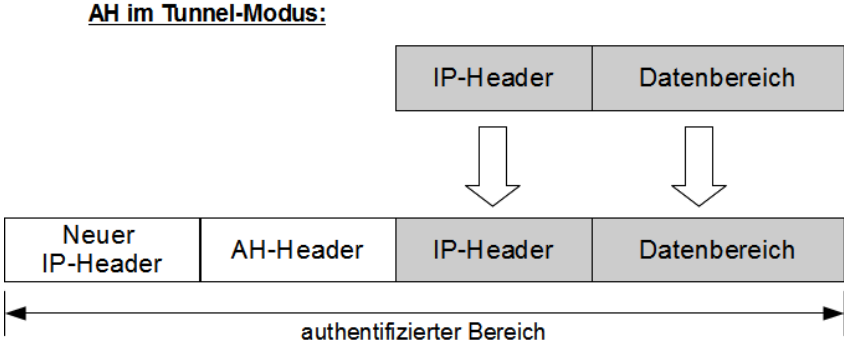

Abbildung 7: AH-Header im Tunnel-Modus

1.5 ESP[19]

Der ESP besteht aus zwei Komponenten. Einem Header und einem Trailer (Anhang). Über den ESP werden die folgenden Sicherheitskriterien realisiert:

- **Vertraulichkeit**
- Authentifizierung
- Datenintegrität
- Anti-Replay-Schutz

1.5.1 Aufbau des ESP

Die nächste Abbildung zeigt den Aufbau des AH im Einzelnen.

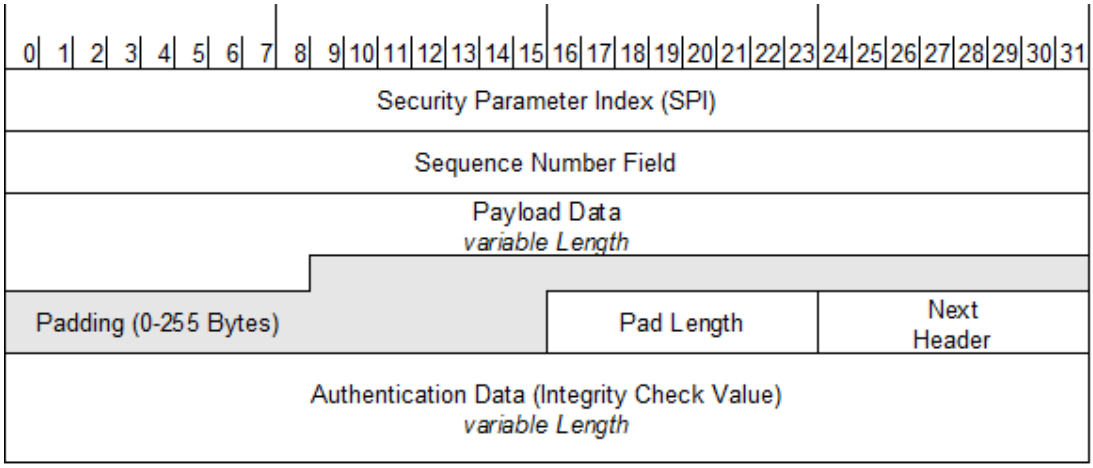

Abbildung 8: Aufbau des ESP-Headers

Payload Data: im Transport-Modus: Inhalt des eingebetteten IP-Paketes (ohne IP-Header)
im Tunnel-Modus: das ganze IP-Paket

Der ESP-Trailer besteht aus:

Padding: Fülldaten

Pad Length: Länge des Padding Feldes

Die restlichen Felder entsprechen denen des AHs.

19 ESP: **E**ncapsulation **S**ecurity **P**ayload

1.5.2 ESP im Transport-Modus und Tunnel-Modus

ESP im Transport-Modus:

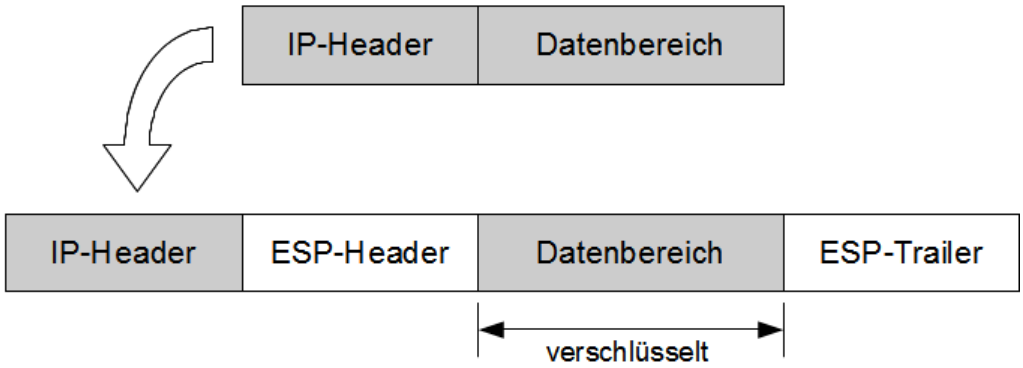

Abbildung 9: ESP-Header im Transport-Modus

ESP im Tunnel-Modus:

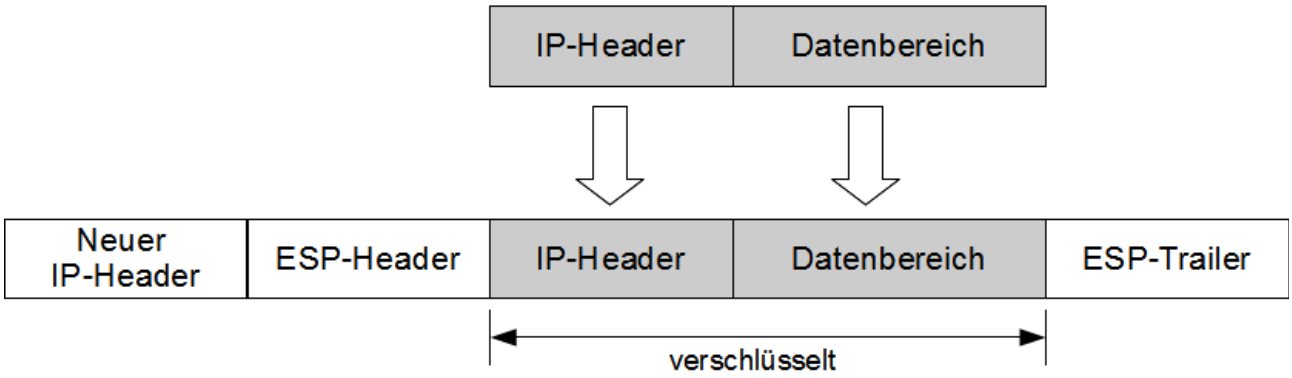

Abbildung 10: ESP-Header im Tunnel-Modusq

Quellen für dieses Arbeitsblatt: A. Badach, Technik der IP-Netze sowie R. Spenneberg, VPN mit Linux