

# Konzeptionen von Betriebssystemskomponenten

## Schwerpunkt: Sicherheit

Lehrstuhl 4 Informatik - FAU Erlangen-Nürnberg



### Thema: IPsec, inkl. Schlüsselverwaltung (ISAKMP/IKE, Photuris)

Referent: Matthias D. Reinhardt

[Matthias.D.Reinhardt@informatik.stud.uni-erlangen.de](mailto:Matthias.D.Reinhardt@informatik.stud.uni-erlangen.de)

27. Mai 2002

#### 1) Bestandteile von IP-Sec

IP-Sec besteht aus verschiedenen Bestandteilen.

Zu diesen gehören:

AH	=	Authentication Header
ESP	=	Encapsulating Security Payload
SPI	=	Security Parameter Index
SA	=	Security Association
Schlüsselverwaltung		

#### 1.1) Sicherheitsanforderung an IP-Sec

- Authentisierung (Authentication)
  - Kommunikationspartners.
- Zugriffskontrolle (Access Control)
  - Rechte der User
- Vertraulichkeit (Confidentiality)
  - Unberechtigte Personen können Daten nicht einsehen
- Integrität (Integrity)
  - Die gesendete Nachricht ist unverändert.
- Verbindlichkeit
  - Unterschriftensatz
- Dienstgüte (Denial of Service)
  - Verfügbarkeit eines Dienstes

#### 1.2) IP-Sec ein Protokoll der Vermittlungsschicht

IP - Sec ist einzugliedern als Protokoll der Vermittlungsschicht. Um sich die Lage des Protokolls zu vergegenwärtigen sollte man sich das OSI und TCP/IP –Referenzmodell vor Augen führen.

#### Begriffe:

Schicht:	Bereitstellung von Diensten für die darüber liegende Schicht
Dienst:	bereitgestellte Gruppe von Operationen
Protokoll:	Regelgefüge, welches das Format und die Bedeutung der von den Partnereinheiten innerhalb einer Schicht ausgetauschten Rahmen, Pakete oder Nachrichten festlegt. Protokolle sind veränderbar, solange sie nicht ihre sichtbaren Dienste ändern (für User)

ISO/OSI-Referenzmodell <sup>1</sup>	TCP/IP – Protokoll <sup>2</sup>
1. Schicht: Bitübertragungsschicht	1. Schicht: Host-an-Netz: Ethernet – PPP – SLIP etc.
2. Schicht: Sicherungsschicht	2. Schicht: Internet <sup>3</sup> : IP
3. Schicht: Vermittlungsschicht <sup>4</sup>	3. Schicht: Transport: TCP bzw. UDP
4. Schicht: Transportschicht	4. Schicht: Verarbeitung: http, FTP, SSH-Protokoll etc.
5. Schicht: Sitzungsschicht	
6. Schicht: Darstellungsschicht	
7. Schicht: Anwendungsschicht	

<sup>1</sup> Darauf wird nicht näher eingegangen, da aus OTRs III als bekannt vorausgesetzt.

<sup>2</sup> Vgl. ISO/OSI-Referenzmodell

<sup>3</sup> hier ist das IP-Sec Protokoll anzuschließen: Aufgabe: Pakete in jedes beliebige Netz einzuschleusen und unabhängig an das Ziel zu befördern.

<sup>4</sup> hier ist das IP-Sec Protokoll anzuschließen: Aufgabe: Pakete vom Sender zum Empfänger transferieren

### 1.3) IP - Sec Internet Protocol Security

Ziel von IP-Sec ist eine sichere Internet-Kommunikation auf der Vermittlungsschicht. IP-Sec soll Schutz vor Verfälschung, unberechtigten Einblicken und Attacken durch externe Angreifer bei der TCP/IP - Kommunikation bieten. Mit IP-Sec können verschiedene Standorte ihren Datenverkehr sichern, wenn die Kommunikation über das öffentliche Internet stattfindet. IP-Sec erweitert das bestehende **IPv4** Internet Protokoll um den Schutz der Vertraulichkeit, der Integrität und der Authentifizierung von Datagrammen. Im **IPv6** Internet Protokoll ist IP-Sec standardmäßig enthalten.

### 1.4) IP Authentication Header (AH)

AH's gewährleisten mittels einer Prüfsumme die Datenintegrität und die Authentifizierung von statischen und dynamischen IP-Feldern. Ein zusätzliches Nummernschild schützt vor REPLAY-Angriffen.

Datenintegrität:	Checksumme generiert durch einen Message Authentication Code (z.B. MD-5)
Datenauthentizität:	durch einen in den Daten enthaltenen secret shared key
Schutz vor REPLAY - Attacken:	durch eine Sequenznummer

AH schützt Inhalte eines IP - Datagrammes bis auf die veränderlichen Felder (mutable fields), die sich während dem Transport verändern (z.B. TimeToLive - Feld). Die mutable fields werden bei der Berechnung als Null-wertige Felder angesehen. Der Wert des Integritätschecks wird im AH Header mitgeführt.

**Es gibt zwei Modi für AH's:**

#### AH Transport Mode

Beim AH Transport Mode bleibt der Original IP - Header erhalten. Danach folgt der AH - Header und die Nutzdaten des Original - Datagrammes. Es können alle Veränderungen der Originaldaten und des AH-Headers festgestellt werden. Der AH Transport Modus bietet keinen Schutz der Vertraulichkeit, da alle Informationen im Datagramm in Klartext sind.

#### AH Tunnel Mode

Beim AH Tunnel Mode wird ein neuer IP - Header generiert, wobei sich in der Regel die Herkunft- und die Zieladresse im IP - Header von dem Original IP - Header unterscheidet. Auf den neuen IP - Header folgt der AH-Header und dann das Original Datagramm (IP - Header mit Nutzdaten). Dabei können am neuen IP - Header, am AH-Header sowie am Original IP - Header und den Nutzdaten Änderungen festgestellt werden. Auch hier sind alle Informationen in Klartext!

#### Bemerkung:

AH kann alleine, in Kombination mit ESP (wird nachfolgend vorgestellt), oder verschachtelt eingesetzt werden. Durch diese Kombinationsmöglichkeiten kann z.B. eine Authentification zwischen zwei Hosts, zwischen zwei Firewalls bzw. einer Firewall und einem Host realisiert werden.

### 1.5) Encapsulating Security Payload (ESP)

ESP sorgt mittels Verschlüsselung für die **Vertraulichkeit** des Datenverkehrs.

Wie bei AH kann ESP zur **Authentifizierung** dienen und besitzt auch geeignete Maßnahmen gegen **Replay-Angriffe**.

- **Schutz vor unberechtigtem Lesen:**
  - durch Verschlüsselung der Daten. Die Daten können nur von Personen gelesen werden, die den Schlüssel besitzen
- **Originalzustand der Pakete:**
  - durch die Verschlüsselung der Pakete, wobei jede kleinste Änderung erkannt wird. Die Pakete können demnach nicht unbemerkt verändert werden
- **Datenauthentizität:**
  - durch den HMAC-Algorithmus (s. AH - Authentication Header).
  - Der Sender kann hier eindeutig Authentifiziert werden
- **Schutz vor Replay Attacken**
  - durch Sequenznummern

ESP setzt einen **Symmetric Shared Key** ein. Diesen Schlüssel benutzen beide Parteien zum Ver- und Entschlüsseln der Daten

**Die beiden Modi des ESP:**

#### ESP Transport Mode

Beim ESP Transport Mode werden nur die Nutzdaten des original IP - Datagrammes und des ESP-Trailer verschlüsselt. Der IP - Header ist weder authentifizierbar noch verschlüsselt!

Die ESP Authentifikationsfunktion schützt nur die Original Nutzdaten aber nicht den Original IP - Header.

!!! AH schützt hier beides !!!

## **ESP Tunnel Mode**

Beim ESP Tunnel Mode wird ein neuer IP-Header erzeugt. Das Original - Datagramm (IP-Header und Nutzdaten) und der ESP - Trailer werden verschlüsselt. Somit kann ein Angreifer also keine Informationen aus dem Original IP - Header gewinnen.

Die ESP Authentifikationsfunktion schützt den Original IP - Header und die IP - Nutzdaten, jedoch nicht den neuen IP - Header. !!! AH schützt hier beides !!!

### **Bemerkung:**

ESP kann alleine, in Kombination mit AH oder verschachtelt eingesetzt werden. Auch hier kann zum Beispiel eine Authentifikation zwischen zwei Hosts, zwei Firewalls bzw. einer Firewall und einem Host realisiert werden.

## **1.6) Einsatzort des Transport-Modus (AH und ESP)**

Der Transport Modus wird normalerweise zwischen den Endpunkten einer Verbindung eingesetzt. Dies bedeutet eine sichere Kommunikation über den gesamten Verbindungspfad hinweg. Die Protokolle authentifizieren das gesamte Paket bis auf veränderliche Einträge des IP - Kopfes. Die Verschlüsselungsmechanismen greifen nur für die höheren Protokollebenen und den Datenbereich des Paketes. Der ursprüngliche IP-Header bleibt erhalten.

Der Transport Modus spart im Vergleich zum Tunnel Modus Rechenzeit und ist für Verbindungen innerhalb eines sicheren Netzwerkes vorgesehen. (Beim Transport Mode muß kein neuer IP-Header generiert werden, es müssen nur die Nutzdaten verschlüsselt werden, dafür wird bietet der Transport Mode jedoch weniger Schutz).

## **1.7) Einsatzort des Tunnel-Modus (AH und ESP)**

Der Tunnel Modus wird eingesetzt, falls zumindest ein Rechner keinen Endpunkt in der Verbindung darstellt. (Sichere Kommunikation zwischen Firewalls, oder entferntes Einwählen in ein Local Area Network (LAN) um eine sichere Verbindung bis zum Eingangs - Gateway zu erhalten).

Der Tunnel Modus bietet eine höhere Sicherheit, da das gesamte IP-Paket kodiert ist. Das Paket erhält einen neuen IP - Header gefolgt von einem AH- bzw. eine ESP - Header, die sowohl die Daten als auch die ursprünglichen Protokollköpfe sichern.

## **1.8) SPI – Security Parameter Index**

IPSec bietet für IP - Pakete Geheimhaltung, Fälschungssicherheit oder beides. Für jede dieser Funktionen gibt es einen eigenen optionalen Paket - Header. Dieser Paket - Header enthält einen numerischen Wert und zwar den Security Parameter Index. Anhand des SPI stellt der Rechner fest, welche Chiffrierschlüssel und Verfahren er verwenden muss.

## **1.9) SA – Security Association**

IP-Sec muss die beteiligten Rechner mit verschiedenen Schlüsseln und kryptographischen Verfahren assoziieren und deren Einsatz mit den IPSec - Headern koordinieren. Dazu müssen jeweils zwei Rechner eine Sicherheitsassoziation untereinander einrichten. Mithilfe dieser Beziehung wird dann das Verschlüsselungs- als auch das Authentifizierungsverfahren bestimmt. Eine Sicherheitsbeziehung enthält unter anderem folgende Werte:

- Zieladresse
- Verfahren zur Verschlüsselung oder Authentisierung
- den jeweiligen Modus (Transport- oder Tunnel-Modus)
- aktueller geheimer Schlüssel für diese Beziehung
- weitere Parameter speziell für dieses Verfahren
- Zeitangabe der Gültigkeit eines Schlüssels

Erreicht ein Paket mit einem IPSec-Header einen IP-Sec unterstützenden Rechner, so wird anhand des Security Parameter Index (SPI) und der IP - Adresse bestimmt, welche Security Association (SA) auf diesen IPSec - Header anzuwenden ist. Sicherheitsbeziehungen (SAs) zwischen zwei Rechnern werden mithilfe der eindeutigen IP-Adressen formuliert. Es wird eine Security Association (SA) pro Kommunikationsrichtung benötigt.

## **1.10) IP - Sec Schlüsselverwaltung**

Für Sicherheitsprotokolle sollte die Beziehung zwischen einzelnen berechtigten Einheiten sowie deren Chiffrierschlüsseln und Identifizierungscodes innerhalb der Nachrichten definierbar sein. Bei IP-Sec wird anhand des Security Parameter Indexes (SPI) die jeweils geltende Sicherheitsassoziation (SA) für den jeweiligen IPSec - Header ausgewählt. Benötigt wird noch eine Methode, um diese SAs einzurichten und ihnen SPIs zuzuordnen.

Die Verwaltung und Verteilung der Schlüssel wird nicht innerhalb von IP-Sec gelöst. Man geht davon aus, dass es ausreichend sichere Verfahren gibt. Es gibt vier Standardkonzepte zum IP-Sec - Schlüsselaustausch. Der Unterschied einzelner Konzepte besteht dabei in der Produktverfügbarkeit und Benutzerfreundlichkeit und weniger hinsichtlich Sicherheitsaspekte. Die manuelle Schlüsselverwaltung ist standardmäßig in jeder IPSec - kompatiblen Implementierung verfügbar.

### 1.10.1) Manuelle Schlüsseleinrichtung

Sicherheitsassoziationen werden hier manuell konfiguriert. Hier werden die SPIs, kryptographische Verfahren und die Schlüssel sowie die Angabe eines Rechners, der diese Angaben verwendet definiert. Die Sicherheitsassoziationen werden in einer Textdatei mit einheitlichem Format definiert. Alle Zahlen werden dezimal dargestellt. Bei längeren Zahlen werden die einzelnen Bytes durch Punkte getrennt

### 1.10.2) Automatische Schlüsseleinrichtung

Der automatische Schlüsselaustausch erfolgt nach dem Internet-Key-Exchange Protokoll<sup>5</sup>

#### 1.11) SKIP - Simple Key Interchange Protocol

SKIP tauscht Schlüssel zwischen IP-Sec-Rechnern aus. Es wird ein spezieller Header vor den IP-Sec-Headern in die IP-Pakete eingetragen. Dabei beruht der Schlüsselaustausch auf einem gemeinsamen Geheimnis, oder es wird ein authentifizierter Schlüsselaustausch mit dem Diffie-Hellman-Algorithmus durchgeführt. Dabei tauschen die Kommunikationspartner ihre öffentlichen Schlüssel aus und können in Verbindung mit ihren privaten Schlüsseln ohne eine zusätzliche Verbindungsaufnahme einen gemeinsamen geheimen Wert erzeugen. SKIP verursacht dabei einen Overhead von 20 bis 30 Byte in jedem Paket.

SKIP wurde von Sun Microsystems entwickelt und im Produkt SunScreen zur Aushandlung von Schlüsseln in VPNs verwendet.

#### 1.12) IKE/ISAKMP

IKE ist ein Protokoll, das der Verwaltung von SA's innerhalb IP-Sec dient. Mit IKE ist der Protokollrahmen ISAKMP der IETF umgesetzt worden. IKE wird gebraucht, da IPSec die zur Verschlüsselung notwendigen Informationen (Algorithmus, Schlüssel, Gültigkeitsdauer etc.) nicht selbst überträgt, sondern sie aus einer lokalen SA bezieht.

Internet Key Exchange (IKE) ist ein in RFC 2410 beschriebenes Schlüsselaustauschverfahren, das speziell auf die Benutzung mit ISAKMP abgestimmt ist. In dem RFC befinden sich genaue Definitionen für das gesamte Verfahren des Schlüsselaustauschs.

Die dazu benötigten Schlüssel werden mittels des asymmetrischen Diffie-Hellman-Verfahrens ausgetauscht. Die wiederum dazu notwendigen öffentlichen Schlüssel müssen über den Verzeichnisdienst einer CA (PKI) bereitgestellt werden.

Das Internet Security Association and Key Management Protocol (=ISAKMP) ist ein Protokoll zur Verwaltung von Sicherheitsassoziationen als auch zum Schlüsselaustausch. Es bietet Funktionen für die Aushandlung, Einrichtung, Modifikation und Zurücknahme von SAs. ISAKMP gibt letztendlich nur den formalen und organisatorischen Rahmen für die Verwaltung von SAs vor. Die eigentliche Schlüsselgenerierung liegt in der Verantwortung anderer Protokolle (z.B. OAKLEY [rfc2412]). ISAKMP ist ein Protokoll der Anwendungsschicht und deshalb z.T. schlechter zu integrieren, belastet den Netzverkehr jedoch weniger, da keine Schlüsselverwaltungsdaten in jedem Paket übertragen werden. ISAKMP wird zur Automatisierung der Generierung und der Erneuerung kryptografischer Schlüssel eingesetzt.

##### 1.12.1) Automatisches Setzen von SA's

Automatisches Key Management ist vor allem bei großen Installationen anzuraten. Es muss darauf geachtet werden, dass die unterschiedlichen Sicherheitsrichtlinien (Security Policies) der miteinander kooperierenden Systeme angeglichen werden.

!!!Das System kann nur so sicher sein, wie sein schwächstes Glied!!!

Durch eine dynamische Adressvergabe der IP - Adressen lassen sich keine SAs auf Basis der IP - Adresse bilden. Dieses Problem kann in ISAKMP durch vorher ausgetauschte Schlüssel oder einer auf individuelle Benutzerzertifikate basierenden Authentifizierung gelöst werden. Man könnte so z.B. den Namen bzw. die Email-Adresse verwenden.

In Verbindung mit einem gültigen, von einer vertrauenswürdigen Instanz unterschriebenem X.509-Zertifikat ist die Identität des mobilen Mitarbeiters durch seine digitale Signatur sicher überprüfbar.

ISAKMP automatisiert die Generierung und die Erneuerung der kryptografischen Schlüssel, dabei soll die manuelle Konfiguration soweit wie möglich ausgeschlossen werden. Der sichere Austausch der Schlüssel ist die kritischste Phase in Bezug auf die Sicherheit der Verbindung. Der ISAKMP Informationsaustausch muss verschlüsselt und mit einer geeigneten Authentifizierung ablaufen, damit niemand die Schlüsselinformationen lesen kann und der Austausch nur zwischen authentifizierten Partnern stattfindet.

Das ISAKMP-Protokoll beinhaltet die komplexesten und Prozessor-intensivsten Operationen im IP-Sec Protokoll. Folgende Punkte wurden beim Design beachtet:

- **Denial of Service:**
  - Die Nachrichten enthalten eindeutige "cookies" zur schnellen Identifizierung ohne intensive Berechnungen durchführen zu müssen.
- **Man-in-the-Middle:**
  - Schutz vor dem Löschen und Verändern, dem Umlenken und dem Reflektieren der Nachrichten sowie dem nochmaligen versenden alter Nachrichten.
- **Perfect Forward Secrecy:**
  - Unabhängige Schlüsselauswahl

---

<sup>5</sup> Auf welches hier nicht weiter eingegangen wird.

### 1.12.2) Die zwei Phasen von ISAKMP

#### Phase 1:

Hier kommt das „master secret“ zum Einsatz, das bei der gesamten Kommunikation zum Schutz verwendet wird. Diese Phase dient ausschließlich zum Schutz der ISAKMP Nachrichten. Die Phase 1 wird einmal (am Tag oder in der Woche) ausgehandelt, woraufhin die Phase 2 dann mehrmals (in einigen Minuten) abgehandelt werden kann.

#### Phase 2:

Hier werden die SA's und die Schlüssel ausgehandelt, welche die Nutzdaten schützen sollen. Die nötigen ISAKMP - Nachrichten werden durch die in der Phase 1 generierten SAs geschützt.

### 1.13) Photuris

Photuris konkurriert mit ISAKMP. Es dient zur Einrichtung von Sicherheitsassoziationen sowie zum Schlüsselaustausch und verwendet den Diffie-Hellman-Algorithmus. Dabei ist das Protokoll nicht so komplex aber auch nicht so flexibel wie ISAKMP. Es enthält keine Komponenten, mit denen ein einfacher und direkter Austausch von Sitzungsschlüsseln auf Basis geheimer Schlüssel möglich ist.

#### Vorteile Photuris vs. ISAKMP: (im Bezug auf DOS-Angriffe)

- Keine Verwendung Zeitstempeln bei COOKIE-Berechnung
- Nicht anfällig gegen Cookie-Race Attacke
- Preisgabe von Identifizierungsinformationen im aggressive mode

---

### 1.14) Literatur – Quellenangaben

- R. Atkinson, S. Kent: Security Architecture for the Internet Protocol, RFC 2401, Internet Engineering Taskforce (IETF), 1998
  - R. Atkinson, S. Kent: IP Authentication Header (AH), IETF, 1998
  - C. Madson, R. Glenn: The Use of HMAC-MD5-96 within ESP and AH, IETF, 1998
  - C. Madson, R. Glenn: The Use of HMAC-SHA-1-96 within ESP and AH, IETF, 1998
  - C. Madson, N. Doraswami: The ESP DES-CBC Cipher Algorithm With Explicit IV. IETF, 1998
  - R. Atkinson, S. Kent: IP Encapsulating Security Payload (ESP), IETF, 1998
  - D. Piper: The Internet IP-Security Domain of Interpretation for ISAKMP, IETF, 1998
  - D. Maughan, M. Schertler, M. Schneider, J. Turner: Internet Security Association and Key Management Protocol (ISAKMP), IETF, 1998
  - D. Harkins, D. Carrel: The Internet Key Exchange (IKE), IETF, 1998
  - Keromytis, N. Provos: The Use of HMAC-RIPEMD-160-96 within ESP and AH, IETF, 2000
  - Für sehr Lesefreudige empfiehlt sich die Lektüre diverser RFC's:
    - RFC 2401 – 2410, RFC2104, RFC 2451, RFC 2857, RFC 793 (um nur einige wesentliche zu nennen)
  - [www.google.de](http://www.google.de) → IPsec +ISAKMP +IKE +Photuris
  - TU Berlin
  - Universität München →
    - <http://www.mnmteam.informatik.uni-muenchen.de/Literatur/MNMPub/Fopras/fack00/HTML-Version>
  - Für RFCs: <http://www.rfc-editor.org/download.html>
-