Proseminar Konzepte von Betriebssystem-Komponenten: Schwerpunkt Sicherheit

Sichere Kommunikation mit IPsec

Markus Weiten
markus@weiten.de

Inhalt

1 Motivation – Bedarf an Authentizität, Vetraulichkeit, Integrität

Das Internetprotokoll gewährleistet keinen sicheren Datentransfer. Weder die Authentizität des Absenders noch die Vertraulichkeit der übermittelten Daten wird garantiert. Auch ein Schutz der übertragenen Daten vor Veränderung auf dem Kommunikationsweg, also Integrität, ist nicht gegeben. Das „Abhören“ von Netzwerkverkehr in einem lokalen Netzwerk ist mit komfortablen Tools wie z.B. Ethereal ein Leichtes, durch die ansteigende Verbreitung von WLANs muss der Abhörer mittlerweile nicht einmal mehr Zugriff auf einen im Netz angeschlossenen Computer haben.
Firmen verzichten zunehmend auf teure private Mietleitungen, um Außenstellen oder Außendienstmitarbeitern den Zugriff auf das Firmennetzwerk zu ermöglichen und nutzen zu diesem Zweck das im Vergleich zu privaten Mietleitungen günstige Internet. Da das Internet ein öffentliches Netzwerk ist, besteht zunächst kein sicherer Übertragungsweg zwischen Firmennetzwerk und Außenstelle.

Es gibt etliche Ansätze, um Internet-Datenübertragung oder allgemein Datenübertragung mit der IP-Protokollfamilie sicher zu machen. Diese Ansätze werden auf unterschiedlichen Ebenen realisiert:

- Anwendungsschicht (z.B. SSL)
- Netzwerkschicht (z.B. IPsec)
- Datenübertragungsschicht (802.1x)

Die Implementierung in der Netzwerkschicht erzeugt die größtmögliche Transparenz für den Anwender und die Programmierer von Anwendungsprogrammen, da sie sich nicht mehr um Sicherheitsbelange kümmern müssen.

2 IPsec im Überblick

IPsec ist eine Protokollfamilie, die im wesentlichen in drei große Funktionsgruppen unterteilt werden kann: Die Übertragungsprotokolle, hierzu gehören Authentication Header (AH, RFC 2402) und Encapsulation Security Payload (ESP, 2406), und das Schlüsselmanagement, wozu das Internet Security Association and Key Management Protocol (ISAKMP, RFC 2408) und Internet Key Exchange (IKE, 2409) zählen. Ebenso wichtige Bestandteile sind die Datenbank für Sicherheitsassoziationen (Security Association Database SADB) und die Datenbank für Sicherheitsstrategien (Security Policy Database SPD).

3 IPsec Modi

IPsec kann grundsätzlich in zwei verschiedenen Übertragungsmodi betrieben werden: Dem Transport-Modus und dem Tunnel-Modus. Beide Modi unterscheiden sich (in der Regel) darin, wo der tatsächliche Kommunikationsendpunkt liegt und wo der krypotgraphische.

3a Der Transport-Modus

Der Transportmodus wird benutzt, um übergeordnete Protokollschichten zu schützen. Da Ipsec in der Netzwerkschicht implementiert ist, bedeutet dies, dass der nächste übergeordnete Header, also der TCP- oder der UDP-Header, der Application-Header und die Nutzdaten geschützt sind. Zu diesem Zweck wird der IPsec-Header, der die Sicherheitsinformation trägt, zwischen IP-Header und übergeordnetem Header eingefügt:

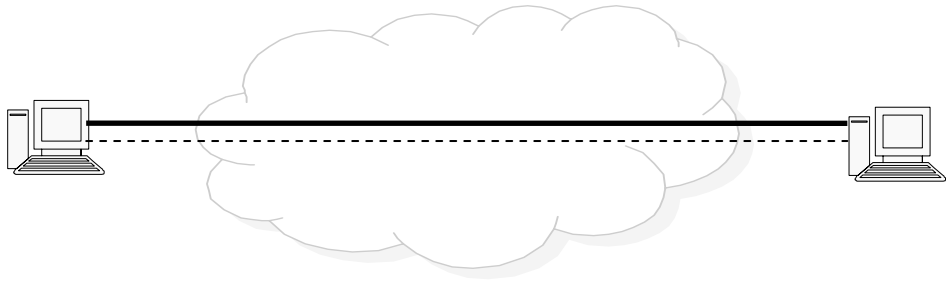
„Normales“ IP-Paket

IP-Header	TCP/UDP-Header	Nutzdaten

Geschütztes Paket im Transport-Modus

IP-Header	IPsec-Header	TCP/UDP-Header	Nutzdaten

Anhand des Aufbaus der Pakete ist erkennbar, dass der IPsec-Transportmodus nur zum Schutz von Verbindungen in Frage kommt, bei denen der kryptographische Kommunikationsendpunkt auch der tatsächliche Kommunikationsendpunkt ist.

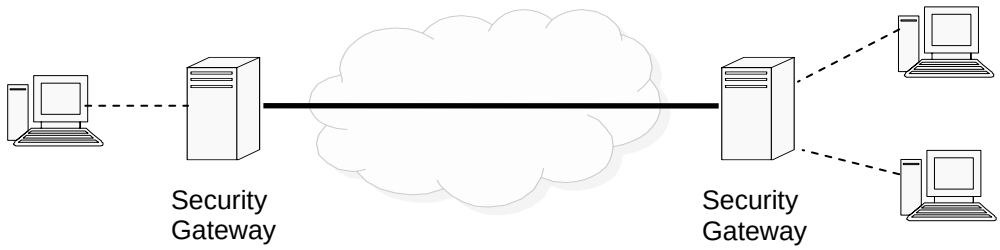


Zwei Hosts im Transportmodus. Die Sicherung findet ab der Transportschicht statt.

Legende: Die gestrichelte Linie steht für eine logische Kommunikationsverbindung, die fette Linie steht für eine gesicherte Verbindung.

3b Der Tunnel-Modus

Der Tunnel-Modus kann genauso wie der Transportmodus zum Zwecke einer sicheren Ende- zu Ende- Verbindung eingesetzt werden, seine herausragende Fähigkeit ist es aber, z.B. in sogenannten „Sicherheitsgateways“, Sicherheitsdienste für komplette Netzwerke anzubieten. Das bedeutet, dass der Tunnelmodus die Möglichkeit bietet, komplette IP-Datengramme zu schützen.



Zwei Netzwerke im Tunnelmodus. Datengramme, die zwischen den Hosts ausgetauscht werden, werden von den Security Gateways komplett gekapselt und gesichert. Dies geschieht für die Hosts transparent. Es handelt sich um ein virtuelles privates Netzwerk.

Im Tunnelmodus werden an ein IP-Datengramm ein kompletter neuer IP-Header und IPsec-Informationen angefügt. Die originalen IP-Quell- und Zieladressen bleiben im inneren, gekapselten Header erhalten.

„Normales“ IP-Datengramm:

IP-Header	TCP/UDP Header	Nutzdaten

Getunneltes IP-Datengramm (ungesichert, d.h. ohne IPsec):

IP-Header(neu)	IP-Header (alt)	TCP/UDP Header	Nutzdaten

Getunneltes, geschütztes IP-Datengramm.

IP-Header(neu)	IPsec-Header	IP-Header (alt)	TCP/UDP Header	Nutzdaten

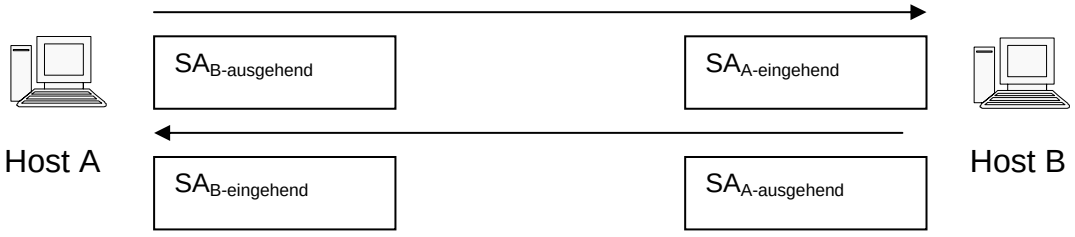
Zum Vergleich noch einmal das IPsec-geschützte Paket im Transportmodus:

IP-Header	IPsec-Header	TCP/UDP-Header	Nutzdaten

Im Tunnel-Modus sind die tatsächlichen Kommunikationsendpunkte diejenigen, die in den inneren Headern spezifiziert und die geschützt wurden. Die kryptographischen Endpunkte sind diejenigen, die in den äußeren Headern stehen. Ein Sicherheitsgateway würde bei einem eingehenden Paket im Zuge der IPsec Verarbeitung das innere Paket extrahieren und an den Kommunikationsendpunkt weiterleiten.

4 Sicherheitsstrategien und Sicherheitsassoziationen

Wichtige Bestandteile von IPsec sind die Datenbank für Sicherheitsstrategien (Security Policy Database, SPD) und die Datenbank für Sicherheitsassoziationen (Security Association Database, SADB). Die Datenbank für Sicherheitsstrategien definiert, wie ein aus- oder eingehendes Paket behandelt werden soll, d.h. ob Sicherheitsmechanismen angewandt werden sollen. Es besteht auch die Möglichkeit zu definieren, dass ein Paket verworfen werden soll. Der Zugriff auf einen Eintrag in dieser Datenbank erfolgt anhand sogenannter Selektoren, die aus dem ursprünglichen IP-Paket extrahiert werden: Ursprungsadressen, Zieladressen, Namen, übergeordnete Protokollschichten, Ports. Die SPD ist nicht zuletzt die Schnittstelle, die dem Administrator zur Konfiguration des IPsec-Systems zur Verfügung steht.
Die SPD arbeitet mit einer weiteren Datenbank zusammen, der Datenbank für Sicherheitsassoziationen. Diese Datenbank wird abgefragt, falls die Abfrage in der SPD ergeben hat, dass Sicherheit angewandt werden soll. In ihr werden die genauen Parameter der anzuwendenden Sicherheitsprotokolle spezifiziert, also ob AH oder ESP zum Einsatz kommen soll, welcher Verschlüsselungs- oder Authentifizierungsalgorithmus jeweils zum Einsatz kommen soll und notwendigerweise auch die Schlüssel. Jeder Eintrag in der SADB enthält auch einen sogenannten Sicherheitsparameter-Index(SPI). Dieser Index wird in jedem IPsec geschützten Paket mitgeführt und ermöglicht den Hosts bei eingehenden Paketen das Auffinden des passenden Eintrages in der SADB. Ein Eintrag in der SADB heißt Security Association. Security Associations werden in aller Regel vom Schlüsselmanagement erzeugt, können allerdings auch manuell erzeugt werden. Eine Security Association gilt unidirektional, was zur Folge hat dass eine bidirektionale Verbindung zwischen zwei Kommunikationspartnern auf bei jedem Kommunikationspartner zwei Security Associations erforderlich macht:



5 Die IPsec-Übertragungsprotokolle

Es gibt zwei IPsec Übertragungsprotokolle, Authentication Header (AH) und Encapsulating Security Payload (ESP), die sowohl einzeln als auch in Kombination angewandt werden können.

5a Authentication Header (AH)

Der Authentication Header bietet eine Authentifizierung der Datenquelle, um zu verhindern, dass jemand vortäuscht, jemand anderes zu sein, um an bestimmte Daten zu gelangen oder Zutritt zu einem System zu erlangen (Spoofing). Weiterhin sichert AH die Integrität der geschützten IP-Datengramme, was einen Schutz davor bietet, dass ein oder mehrere IP-Datenpakete unterwegs verändert werden. Ein weiteres Feature ist der Schutz vor dem wiederholten Senden von Paketen (Replay-Attacken) durch Hinzufügen einer Seriennummer.
Das Authentication Header Protokoll bietet keine Verschlüsselung und kann sowohl im Transport- als auch im Tunnelmodus eingesetzt werden.

Aufbau des Headers (jede Zeile ist ein 32-Bit Wort):

Next Header ID	Payload Length	Reserved
Security Parameter Index (SPI)		
Serial No		
Authentification Data		

Im Feld „next Header“ wird angegeben, welcher Header auf den AH-Header folgt. Dies ist vom verwendeten IPsec-Modus abhängig. Die Angabe ist eine Integer-Zahl, wie sie auch in den anderen IP-Headern verwendet wird (z.B. 5 für TCP). Wird IPsec im Transport-Modus verwendet, so folgt ein TCP- oder UDP- Header. Im Falle des Tunnelmodus folgt der IP-Header des geschützten und getunnelten Datengramms. Das Feld „payload Length“ gibt die Größe des Headers an. Der Sicherheitsparameter-Index ist eine 32-Bit Zahl, welche beim Erzeugen der Sicherheitsassoziation durch den Empfänger festgelegt wurde. Sie dient dem Empfänger des IP-Datengramms zum Auffinden der entsprechenden Security Association in seiner Security Association Database und somit zum Auswerten der Authentifizierungsinformationen. Bei eingehenden Paketen muss bereits eine Sicherheitsassoziation bestehen, sonst wird das Paket verworfen. Besteht bei ausgehenden Paketen noch keine Sicherheitsassoziation, so wird eine vom Schlüsselmanagement erzeugt und dann das Datenpaket versendet. Die Seriennummer ist ebenfalls eine Integerzahl. Sie bietet den oben angesprochenen Schutz vor abermaligen Senden eines IP-Paketes. Das Feld „Authentification Data“ enthält das Ergebnis des Authentifizierungsalgorithmus, welcher auf den Rest des Datengramms angewandt wurde. Da verschiedene Algorithmen zum Einsatz kommen können, handelt es sich um ein Feld variabler Länge.

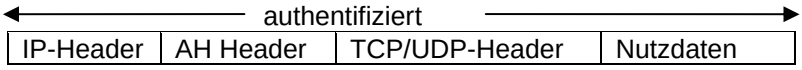
Algorithmen

Im IPsec Standard ist nicht vorgeschrieben, welche Authentifizierungsalgorithmen verwendet werden müssen. Es sind allerdings zwei Algorithmen vorgeschrieben, die in jeder Implementierung von IPsec vorhanden sein müssen: HMAC-MD5 und HMAC-SHA. Es handelt sich hierbei um verschlüsselte MACs (Message Authenitfication Code), also um verschlüsselte Hashfunktionen (keyed Hash). Bei dieser Art von Algorithmus wird eine Hashfunktion auf die zu hashenden Daten zusammen mit einem Schlüssel angewandt. Wie oben beschrieben, wird der Algorithmus auf das gesamte IP-Paket (ausgenommen veränderliche Felder des äußeren IP-Headers) angewandt und das Ergebnis in das Feld Authentification Data geschrieben. Der Empfänger kann nun, da er den richtigen Schlüssel besitzt und

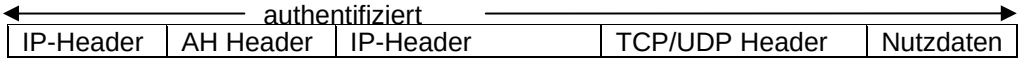
durch die Security Association Kenntnis vom verwendeten Algorithmus und Schlüssel hat, seinerseits den Algorithmus auf die empfangene Nachricht anwenden und die Ergebnisse miteinander vergleichen. Sind die Ergebnisse identisch, ist das empfangene Paket authentifiziert. Warum keyed Hash? Eine normale Hashfunktion würde keine Datenintegrität gewährleisten, da das Paket unterwegs manipuliert werden kann und der Hash-Algorithmus einfach abermals auf die manipulierten Daten angewandt werden kann. Bei keyed Hash ist es nicht möglich, ohne den nötigen Schlüssel einen Hash zu berechnen, der die Nachricht authentifiziert

Wie bereits bemerkt, kann AH im Tunnel- und im Transportmodus zum Einsatz kommen. In beiden Modi ist jeweils das gesamte resultierende IP-Datengramm (bis auf veränderliche Felder des äußeren IP-Headers) authentifiziert:

Datagramm AH im Transportmodus



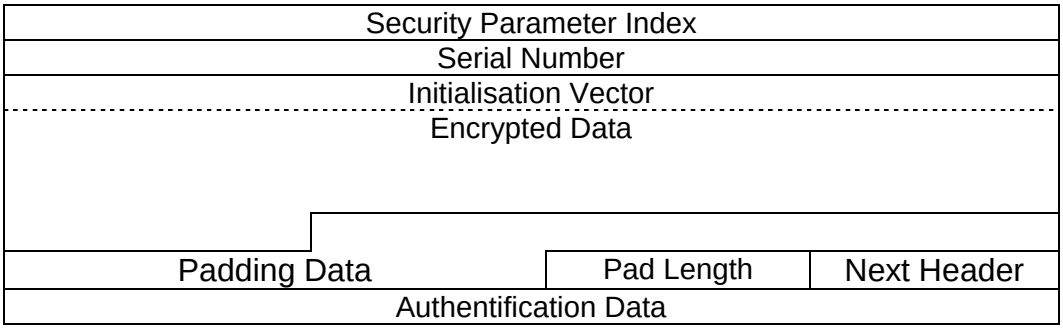
Datagramm AH im Tunnelmodus



5b Encapsulating Security Payload (ESP)

Das Encapsulating Security Payload Protocol bietet neben der auch von AH unterstützten Integrität und Authentifizierung der Datenquelle auch Vertraulichkeit, d.h. die übertragenen Daten werden verschlüsselt. Dies ermöglicht einen sicheren Schutz vor dem „Abhören“ der Pakete. Genau wie AH bietet ESP auch Schutz vor wiederholtem Senden eines Datengramms mittels einer Seriennummer.

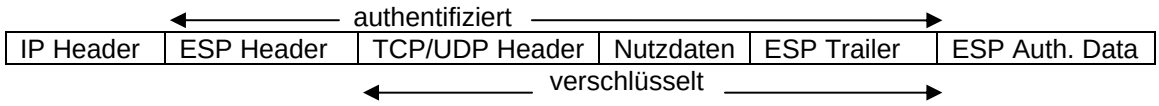
Aufbau des Headers (jede Zeile ist ein 32-Bit Wort):



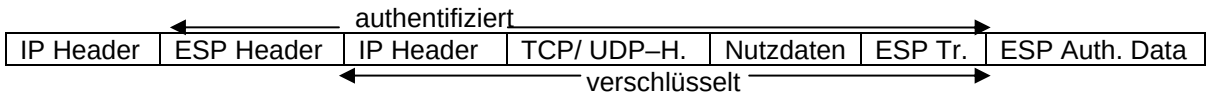
Wie der Authentification Header auch, enthält der ESP-Header ein Security Parameter Index Feld, um dem Empfänger des IP-Paketes die Zuordnung zu einer Security Association zu ermöglichen. Die Seriennummer zum Schutz vor wiederholtem Senden entspricht ebenfalls der im AH verwendeten. Nach der Seriennummer beginnen die verschlüsselten Nutzdaten. Hier ist erkennbar, dass der ESP-Header sich in einen Header und einen Trailer aufspaltet , da er das gesamte

geschützte IP-Paket umschließt. Da ESP symmetrische Verschlüsselungsverfahren im „Cipher Block Chaining“ Modus vorschreibt, wird im Nutzdatenfeld ein Initialisierungsvektor mitgeführt, um dem Empfänger die Entschlüsselung zu ermöglichen. Der Initialisierungsvektor wird nicht verschlüsselt. Danach folgen die eigentlichen verschlüsselten Nutzdaten. Da symmetrische Chiffren benutzt werden, sind eventuell Fülldaten notwendig, um auf die Blockgröße des Schlüssels zu kommen (Pad). Das Feld Pad Length enthält die Anzahl der Fülldaten, die hinzugefügt wurden, damit vom Empfänger die tatsächliche Nutzdatenlänge ermittelt werden kann. Next Header gibt wieder, wie auch bei AH, die Art des nächsten Headers innerhalb der geschützten Daten an (4 für IP, also Tunnelmodus, 6 für TCP, Transportmodus). Im Authentification Data-Feld steht das Ergebnis des Authentifizierungsalgorithmus, ähnlich wie bei AH.

Datagramm ESP im Transportmodus



Datagramm ESP im Tunnelmodus



ESP Pakete im Transport-und Tunnelmodus. Der ESP Trailer wurde aufgeteilt in den Teil mit Pad Length und Next Header Feld (ESP Trailer) und die ESP Authentifizierungsdaten. Man sieht, dass sich die AH- und die ESP Authentifizierung unterscheiden, da ESP nicht die äußeren IP Header authentifiziert.

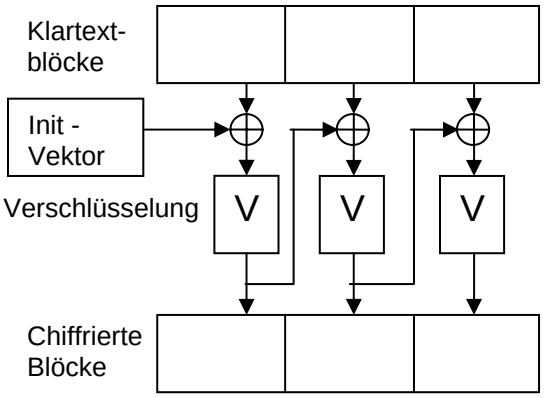
Algorithmen

Wie bei AH auch, sind keine speziellen Algorithmen für ESP vorgeschrieben, genauso müssen aber bestimmte Algorithmen in jeder Implementierung von IPsec vorhanden sein. Bei der Authentifizierung sind es die selben Algorithmen wie auch bei AH, die oben kurz beschriebenen keyed Hashes HMAC-MD5 und HMAC-SHA. Bei der Verschlüsselung sind aus Performancegründen im Cipher Block Chaining (CBC)-Modus arbeitende symmetrische Algorithmen zugelassen. Implementiert sein muss in jeder Implementierung von IPsec DES-CBC.

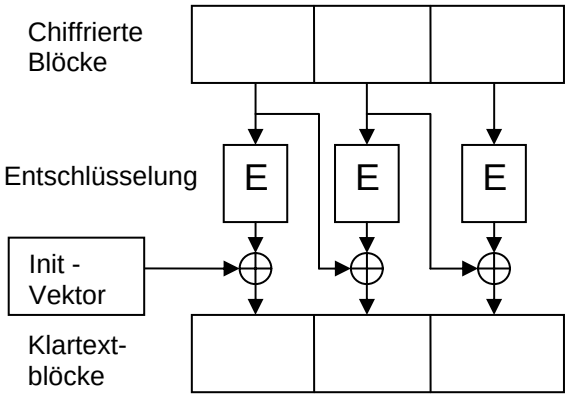
DES im Cipher Block Chaining Modus

Eine Methode, herkömmliche symmetrische Chiffren wie DES sicherer zu machen, ist die Verwendung des sogenannten Cipher Block Chaining Modus. Wie der Name schon sagt, findet eine Verkettung der einzelnen Chiffreblöcke statt.
Die Verkettung läuft folgendermaßen ab: Bevor der nächste Chiffrenblock verschlüsselt wird, wird er mit dem vorangegangenen Block XOR-verknüpft. Auf dieser Weise wird verhindert, dass identische Klartextblöcke identisch verschlüsselt werden. Der erste Block wird mit dem oben genannten Initialisierungsvektor verknüpft.

CBC-Verschlüsselung schematisch



CBC-Entschlüsselung schematisch



5c Authentification Header vs. Encapsulating Security Payload

Eine Frage, die sich nun stellt ist die, weshalb für IPsec überhaupt zwei verschiedene Protokolle existieren, von denen das eine, nämlich AH, scheinbar gerade mal einen Teilmenge dessen kann, was das umfangreichere ESP beherrscht. Zunächst fällt auf, dass AH keine Verschlüsselung bietet, sondern lediglich Authentizität und Integrität. Genauer betrachtet kann man sehen, dass sich die Authentifizierung von AH von der, die ESP bietet, unterscheidet. Anhand der oberen Abbildungen (ESP/AH im Transport/Tunnelmodus) wird klar, dass AH, im Gegensatz zu ESP, auch die äußeren IP Header authentifiziert. Man fragt sich, weshalb ESP diese Funktionalität nicht auch mitbringt. Eine Antwort ist die, dass eine Einbeziehung der äußeren IP Header in die Authentifizierung das Problem mit sich bringt, dass Network Adress Translation (NAT) nicht mehr funktionieren würde, da bei diesem Verfahren ja auch die Adressfelder im IP-Header modifiziert werden. Es ist möglich, dass aus diesem Grund die vollständige Authentifizierung in ein eigenes Protokoll ausgelagert wurde. Die einschlägige Literatur schweigt sich über diese Fragestellung aus. Um vollständige Authentifizierung auch beim Einsatz von ESP zu erreichen, besteht die Möglichkeit, beide Protokolle zu kombinieren, also das mit ESP verschlüsselte Paket durch die Verwendung von AH zu authentifizieren. Die IPsec RFC 2406 beschreibt Kombinationen, die jede IPsec Implementierung leisten muss:
Im Transportmodus müssen AH und ESP jeweils alleine, sowie AH nach ESP unterstützt werden.
Im Tunnelmodus müssen AH alleine und ESP alleine unterstützt werden.

6 Bewertung

IPsec ist ein vielseitiges und funktionelles Protokoll zur Sicherung von IP-Datenverkehr. Es bietet Vertraulichkeit, Integrität und Authentifizierung der Datenquelle, Schutz vor Replay-Attacken. Der wesentliche Vorteil gegenüber anderen Lösungsansätzen in anderen Protkollschichten ist die bereits zu Beginn erwähnte Transparenz, die IPsec für Anwendungsprogramme und deren Programmierer bietet. Jedoch können trotz aller Transparenz beim Einsatz von IPsec Probleme auftreten, die vorherzusehen und zu umgehen eines hohen Administrationsaufwandes und entsprechendes Fachwissen bedürfen. Dazu zählen

das oben beschriebene Problem mit der Network Adress Translation bzw. IP Masquerading. Weiterhin ist problematisch, dass einige anderen Ansätze zur Steigerung der Sicherheit und der Performance durch den Einsatz von IPsec ausgehebelt werden können, da solche Dienste oft „in“ das Paket sehen müssen, um herauszufinden, was übertragen wird. Fazit: IPsec bietet umfassende Sicherheit mit vielen Anpassungsmöglichekeiten, jedoch zum Preis eines hohen Konfigurations- und Administrationsaufwandes.

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