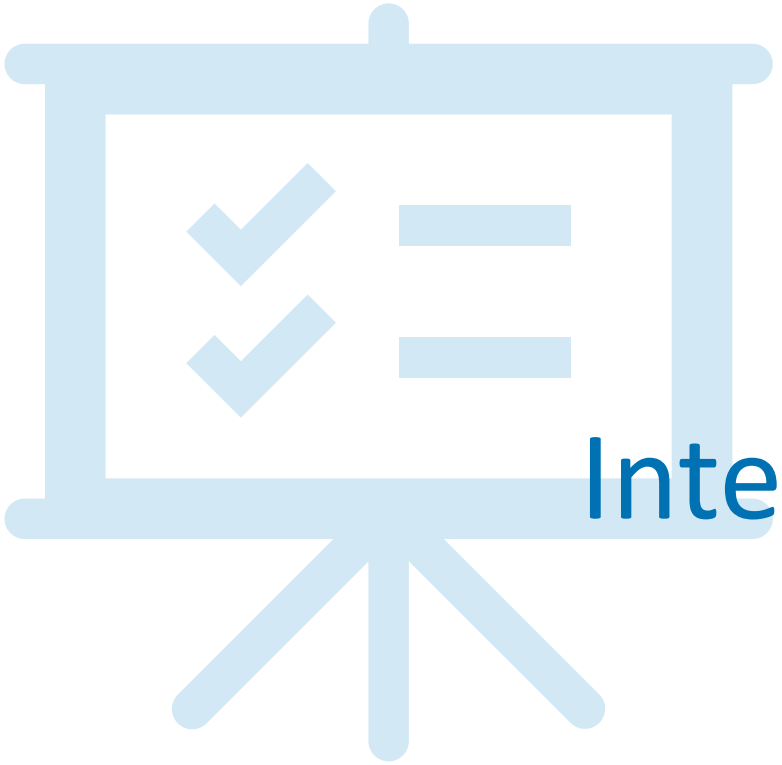


Netzwerke und Internettechnologien 2

IPsec (Internet Protocol Security)

Netzwerke und Internettechnologien 2

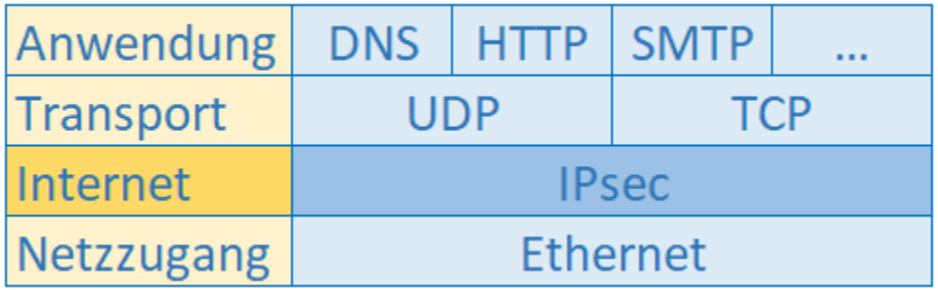
Lernziele

1. IPsec Grundlagen

2. IPsec Modi

IPsec (Internet Protocol Security

- Die Aufgabe von IPsec (Internet Protocol Security) ist es, eine gesicherte Kommunikation über potentiell unsichere IP-Netze, wie das Internet, zu ermöglichen.
- IPsec arbeitet direkt auf der Internetschicht (Internet Layer) des TCP/IP-Models und ist eine Weiterentwicklung der IP-Protokolle.



- Das Ziel ist es, die Schutzziele Vertraulichkeit (durch Verschlüsselung), Authentizität und Integrität zu erfüllen.

IPsec (Internet Protocol Security

Transportmodus

- Dieser wird verwendet, um übergeordnete Protokollschichten zu schützen
- IPsec ist in der Netzwerkschicht implementiert, deswegen sind der nächste übergeordnete Header, also der TCP- oder der UDP-Header, der Application-Header und die Nutzdaten geschützt
- Der IPsec-Header, der die Sicherheitsinformation trägt, wird zwischen IP-Header und übergeordnetem Header eingefügt
- Kommt bei Host-to-Host oder Host-to-Gateway-Verbindungen zum Einsatz.

IP-Datagramm im Transportmodus

IPsec (Internet Protocol Security

Tunnelmodus

- Wird, wie der Transportmodus, für einer sicheren Ende- zu Ende- Verbindung eingesetzt.
- Der Tunnelmodus bietet die Möglichkeit komplette IP-Datengramme zu schützen.
- Dafür werden ein kompletter neuer IP-Header und die IPsec-Informationen an ein IP-Datengramm angefügt.
- Die originalen IP-Quell- und Zieladressen bleiben im inneren, gekapselten Header erhalten.

IP-Datagramm im Tunnelmodus

IPsec (Internet Protocol Security

Tunnelmodus

- Die tatsächlichen Kommunikationsendpunkte sind diejenigen, die in den inneren Headern spezifiziert und die geschützt sind.
- Die kryptographischen Endpunkte sind diejenigen, die in den äußeren Headern stehen
- Ein Sicherheitsgateway (z.B. VPN-Gateway) extrahiert im Zuge der IPsec Verarbeitung das gekapselte Paket und leitet es an den Kommunikationsendpunkt weiter.
- Der Tunnelmodus kommt vorzugsweise bei Gateway-zu-Gateway- oder auch Host-zu-Gateway-Verbindungen zum Einsatz. Möglich sind aber auch Host-to-Host oder Host-to-Gateway-Verbindungen.

IPsec (Internet Protocol Security)

IP-Datagramme

IP-Datagramm

getunneltes, ungeschütztes IP-Datagramm

IP-Datagramm im Transportmodus

IP-Datagramm im Tunnelmodus

IPsec (Internet Protocol Security

Authentication Header (AH)

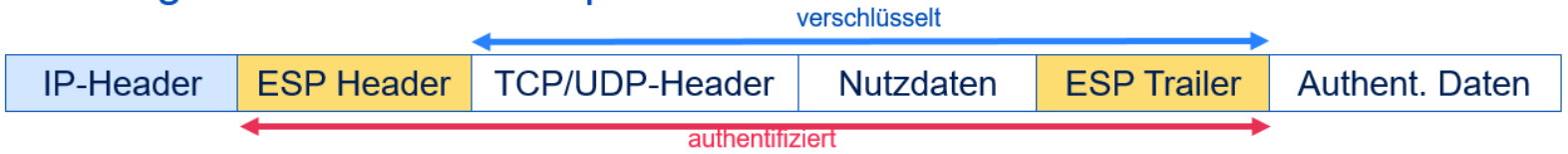
- AH soll die Authentizität und Integrität der übertragenen Pakete sicherstellen und den Sender authentifizieren.
- AH schützt die invarianten Teile eines IP-Datagramms. IP-Header-Felder, die beim Transport durch Router verändert werden, z.B. das TTL-Feld, werden nicht geschützt.
- Das IP-Adressfeld wird geschützt, dadurch ist AH mit NAT inkompatibel.
- Durch AH ist auch ein Schutz gegen Replay-Angriffe gegeben.
- Die Nutzdaten werden von AH nicht verschlüsselt.

IPsec (Internet Protocol Security

Encapsulating Security Payload (ESP)

- ESP bietet neben Integrität und Authentifizierung der Datenquelle auch Vertraulichkeit, überträgt die Nutzdaten also verschlüsselt.
- Im Unterschied zum AH wird der Kopf des IP-Paketes vom Integritätscheck nicht berücksichtigt.
- ESP-Feld ist in Header und Trailer aufgespalten.

IP-Datagramm ESP im Transportmodus



IP-Datagramm ESP im Tunnelmodus

Quellen

Buchquelle

Kersken, Sascha (2017): IT-Handbuch für Fachinformatiker. Der Ausbildungsbegleiter. 8. Auflage, revidierte Ausgabe. Bonn: Rheinwerk Verlag; Rheinwerk Computing.

Schreiner, Rüdiger (2014): Computernetzwerke. Von den Grundlagen zur Funktion und Anwendung. 5., erw. Aufl. München: Hanser.

Weiten, Markus: Sichere Kommunikation mit IPsec. Online verfügbar unter https://www4.informatik.uni-erlangen.de/DE/Lehre/SS03/PS_KVBK/talks/ipsec.pdf, zuletzt geprüft am 16.06.2021.

IPsec - Security Architecture for IP (VPN) (2021). Online verfügbar unter https://www.elektronik-kompendium.de/sites/net/0906191.htm, zuletzt aktualisiert am 16.06.2021, zuletzt geprüft am 16.06.2021.

VIELEN DANK!