



Vorlesung

VPN: Drahtgebunden und drahtlos

Fachbereich Informatik (FB 20)

Lehrstuhl Prof. J. Buchmann

WS-05 / V2 - 20.205.1

In Zusammenarbeit mit dem CAST-Forum

Dr. Wolfgang Böhmer

Skript: <http://www.cdc.informatik.tu-darmstadt.de/~wboehmer/>

Email: wboehmer@cdc.informatik.tu-darmstadt.de





Vorlesungsinhalte

- Remote Access VPN (IPSec)
 - Probleme bei IPSec bzgl. RAS
 - IPSec und NAT Traversal
- Übersicht SSL/TLS
- Einordnung der SSL-Architektur im ISO/OSI-Referenzmodell
 - SSL-Connection / SSL-Session / SSL-Record Protocoll
- SSL-Handshake-Protokoll
 - Vier SSL-Phasen zum Aufbau einer Verbindung
- Vergleich zwischen IPSec und SSL /TLS
- Attacken auf SSL/TLS





Bekannte Fallstricke bei IPSec/Remote Access

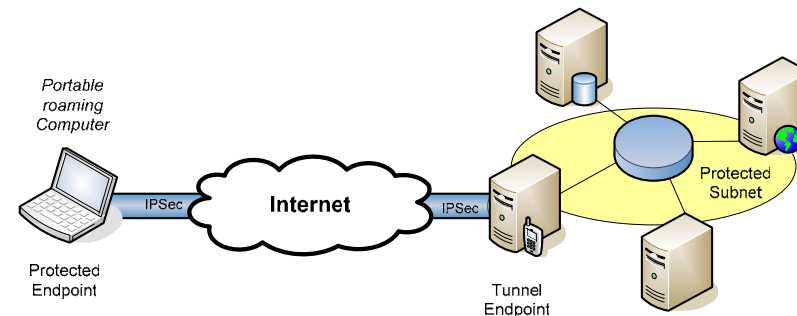
- Falls preshared Keys, Main Mode und dynamische IP-Adressen genutzt werden, müssen die preshared Keys für alle IPSec-Clients gleich sein.
- IPSec unterstützt nicht die traditionellen Authentifizierungsmethoden beim Fernzugriff wie Radius (PAP/CHAP), Secure-ID oder OTP.
- Es können offene Verbindungselemente verbleiben, wenn IPSec-Clients ihre PPP-Verbindung unterbrechen und ihre eigene SA löschen.
- Es darf zwischen IPSec-Client und VPN-Gateway kein IP-NAT-Verfahren eingesetzt werden. Hierzu gibt es inzwischen Verbesserungsvorschläge!!
- In umfangreichen Remote-Access-Installationen ist die Konfig. und Admin der SPD-Einträge auf Clientseite als auch im Zentralsystem sehr Zeit aufwendig





IPSec/IKEv2 und NAT-Traversal

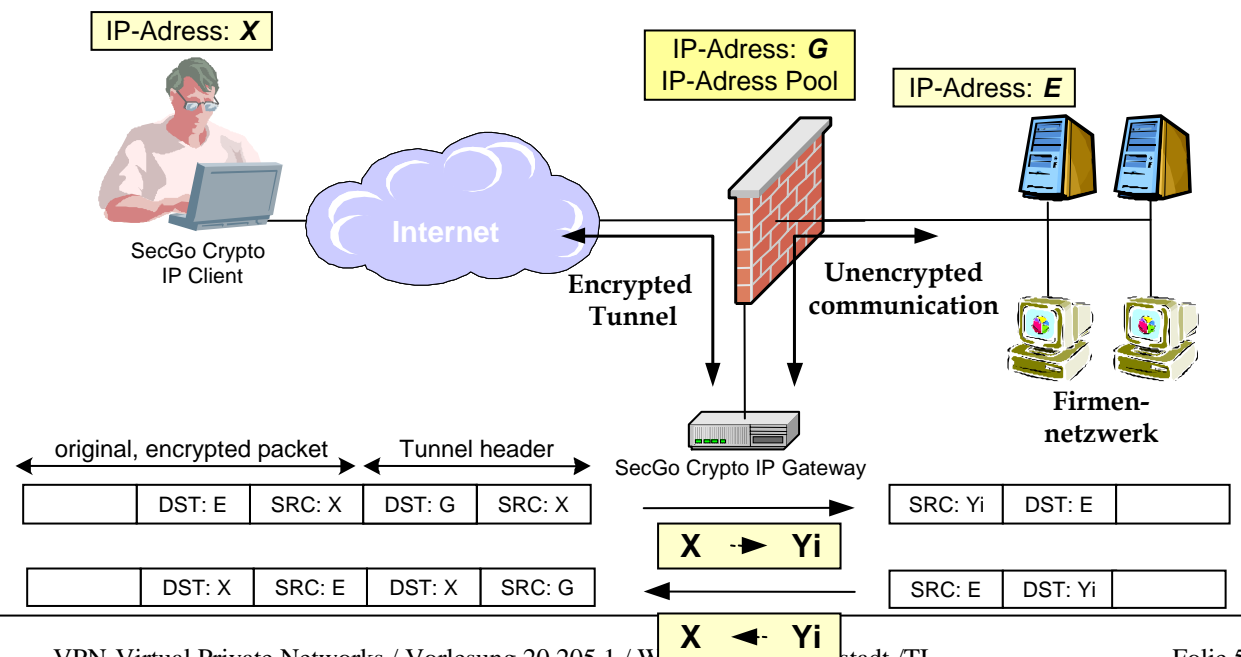
- Bei einem IPSec-Tunnelaufbau ist IKE die maßgebliche Komponente.
- Für einen mobilen User der IPSec im Tunnelmodus nutzen will, stößt an Grenzen.
- IKEv2 ist in der Lage eine IP-Adresse bei einem Client-request vom Tunnelendpoint an den protected Endpoint zu vermitteln um eine SA aufzubauen. (Änderung der Lifetime der SA ist erforderlich) -> IKE-Peers haben unabhängige Lifetimes für die SA. (IKEv2 nutzt UDP/4500 Port)
- Es wird ein Tunnel aufgebaut, indem die IP-Adresse des protected Endpoint als Outer IP-Header und die IP-Adresse des Security Gateway als Inner IP-Header genommen wird.





IPSec: Bekannte Probleme beim Remote Access

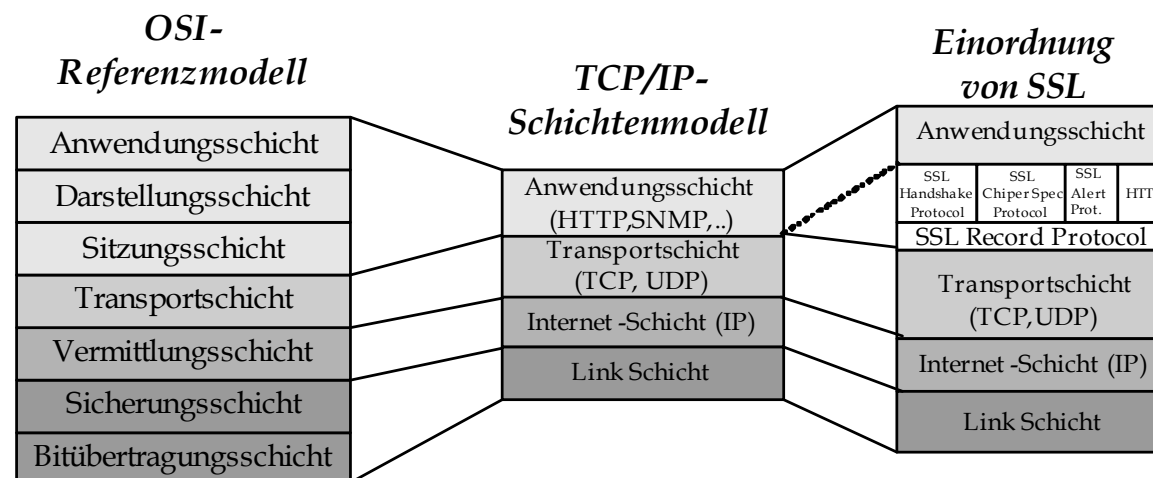
- Standard IPSec Technologie versagt bei dynamischer Port Vergabe und beim NAT.
- IP NAT-Traversal ist für eine point-to-point IPSec Verbindung die Problemlösung.
 - Es kann mit NAT Traversal eine sichere Verbindung aufgebaut werden, die durch Firewall-Systeme und anderen VPN-Devices hindurchgeht. Es wird dazu ein spezieller Client (SecGo Crypto IP-Client) und ein spezielles Gateway (SecGo Crypto IP-Gateway) erforderlich





SSL/TLS- Einordnung in die ISO/OSI-Schicht

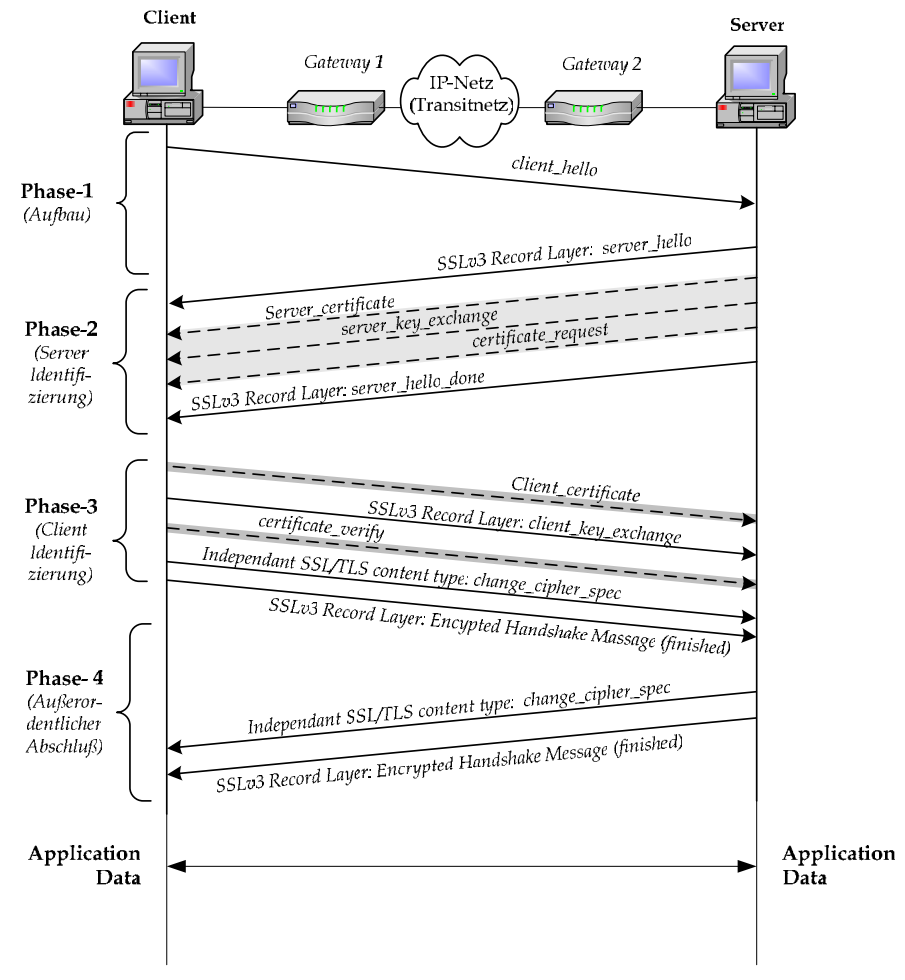
- SSL wurde im Jahr 1996 von Netscape entwickelt. (u.a. auch von Paul Kocher)
- SSL3.0 erlangte große Bedeutung. Die IETF setzte eine Arbeitsgruppe (TLS) ein.
- TLS-Protokoll 1.0 entstand 1999.
- SSL/TLS dient zu Absicherung (Vertraulichkeit, Integrität) der Transportschicht (TCP).
- Speziell zielte die Absicherung auf das HTTP ab.



Etablierung einer SSL/TLS-Verbindung



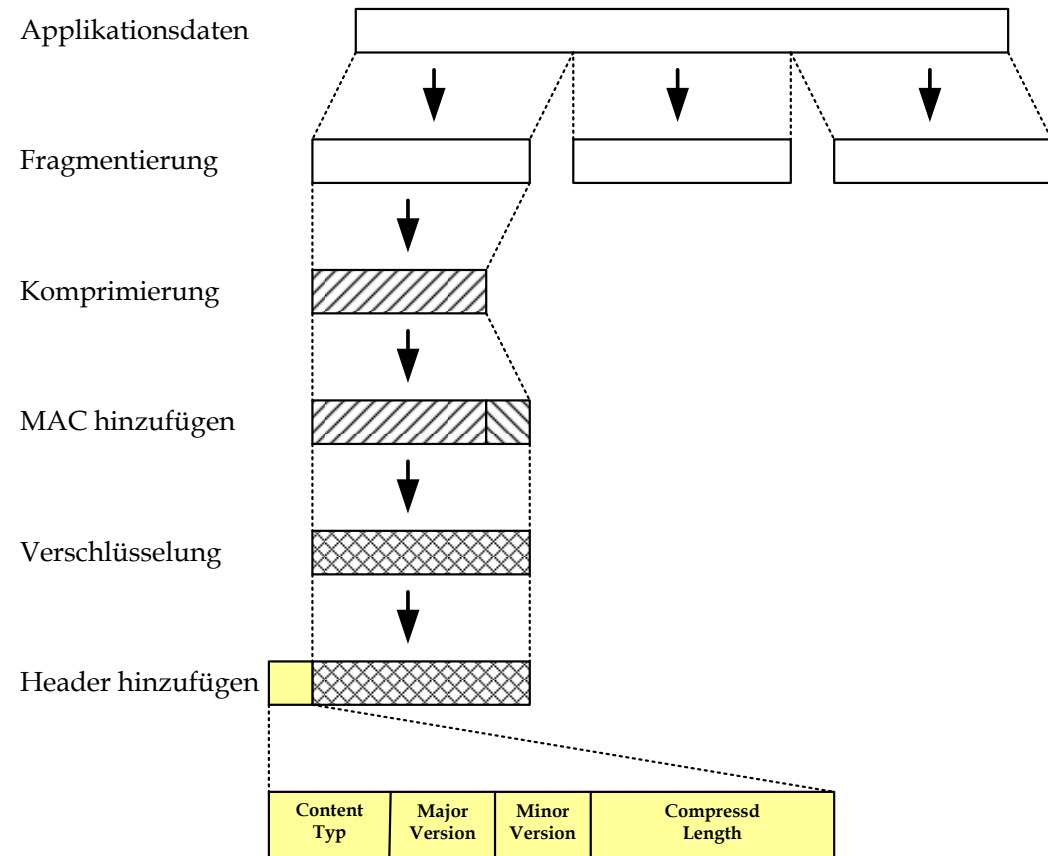
- Der Verbindungsaufbau geschieht in bis zu 4 Phasen. Innerhalb der Phasen gibt es optionale Parameter.
- Die durchgezogenen Linien sind ein (*must*). Die gestrichelten Linien sind optional und hängen von Client und Server ab.
- Die *change_cipher_spec* Message gehört nicht direkt zum Handshake.
- Nach Durchlaufen des Handshake werden die Applikationsdaten ausgetauscht.





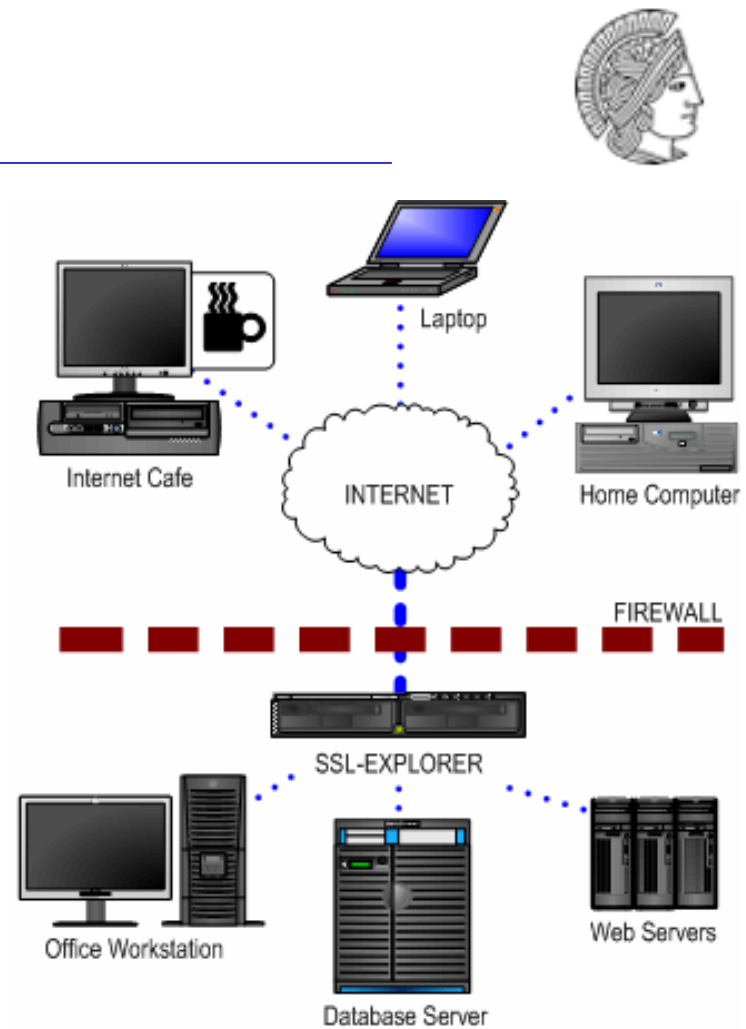
Funktionsweise des SSL/TLS-Record Protokoll

- Beim Verbindungsaufbau zwischen Client und WebServer werden die Daten erst nach Aufbereitung an die unteren Schichten weitergegeben.
- Es liefert die Eigenschaft: Vertraulichkeit und Integrität.
- Für die Vertraulichkeit können Block-Chiper als auch Strom-Chiper eingesetzt werden.
- Für die Integrität können SHA-1 bzw. MD5 eingesetzt werden.



SSL-Explorer VPN

- Beispiel für eine SSL-Architektur
- Hinter der FW steht ein SSL-Explorer, der eine Verschlüsselte Kommunikation aufbaut.





IPSec versus SSL/TLS

- Gemeinsamkeiten von IPSec und SSL/TLS
 - Beide bieten eine Client/Server –Authentifizierung
 - Beide bieten Datenintegrität und –authentifizierung und Vertraulichkeit, wenn auch auf unterschiedlichen OSI-Layern.
 - Es können bei beiden VPN-Techniken starke kryptographische Protokolle eingesetzt werden.
- Unterschiede zwischen IPSec und SSL/TLS
 - SSL/TLS arbeitet auf der Transportschicht, IPSec im Wesentlichen auf der Verbindungsschicht.
 - SSL/TLS schützt den IP-Protokollkopf (IP-Header) nicht. Damit ist ein Spoofing und Session Hijacking möglich.
 - SSL/TLS ist nur auf TCP ausgelegt und kann somit nicht UDP absichern. Dies stellt für IPSec kein Problem dar.
 - Bei SSL/TLS muss eine Modifikation auf Applikationsebene vorgenommen werden, bei IPSec nicht.
 - SSL/TLS ist problemlos mit NAT und Socks vereinbar. IPSec kann dies im Transport-Modus nicht. Nur der Tunnelmodus macht eine Überbrückung möglich.



Übungen



1. Frage: Wie ist die Arbeitsweise von IKEv2?
2. Wie funktioniert ein RAS-Zugang mit IPSec?
3. Frage: Worin liegen die wesentlichen Unterschiede zwischen IPSec und SSL/TLS
4. Welche Aufgabe kommt dem SSL-Alert-Protokoll zu?
5. Welche Anfälligkeiten hat SSL/TLS gegenüber Attacken?
6. Welche bekannten Attacken gibt es gegen SSL/TLS?





Literatur

- <http://www.tu-darmstadt.de/vv/20.205.1>.
- **Huston G.: Internet Performance Survival Guide, QoS Strategies for Multiservice Networks, ISBN 0-471-37808-9**
- **Comer, 1995: Internetworking with TCP/IP Vol. I., ISBN 0-13-216987-8**
- **Davis, C.R.: IPSec-Tunneling im Internet, mitp-Verlag, 1. Auflage 2002, ISBN 3-8266-0809-7.**
- **Aurand, A.: Sicherheit in Cisco- und Windows-2000-Netzwerken, Installation und Troubleshooting von IPSec in der Praxis, Addison-Wesley Verlag 2001, ISBN 3-8273-1930-7. (Teil 2- IPSec-Architektur)**
- **Schneier, B.: IPSec an critical description**
- **Secgo Crypt Manual für NAT-Traversal.**

