
# Softwareprojekt 2019

## Verschleierung von IPsec in HTTPS-Verbindungen

### Szenario

Mit Hilfe der Protokollfamilie IPsec können virtuelle Tunnel zwischen zwei Hosts aufgebaut werden, um (unter anderem) die Vertraulichkeit und Datenintegrität von beliebigen Verbindungen im Internet zu schützen. Durch ein Overlay aus mehreren Tunneln können zudem virtuelle private Netzwerke (VPNs) realisiert werden. Neben der reinen Sicherung der Kommunikation haben sich VPNs auch zu einem beliebten Mittel entwickelt, um eine Zensur (Blockierung von unerwünschten Verbindungen) zu umgehen. Allerdings ist die Verwendung von IPsec effizient erkennbar, so dass ein Angreifer einfach sämtliche IPsec-Tunnel detektieren und anschließend blockieren kann. Dadurch wird auch der herkömmliche Einsatz von IPsec (etwa zur Absicherung zwischen Firmenstandorten) eingeschränkt bzw. unmöglich.

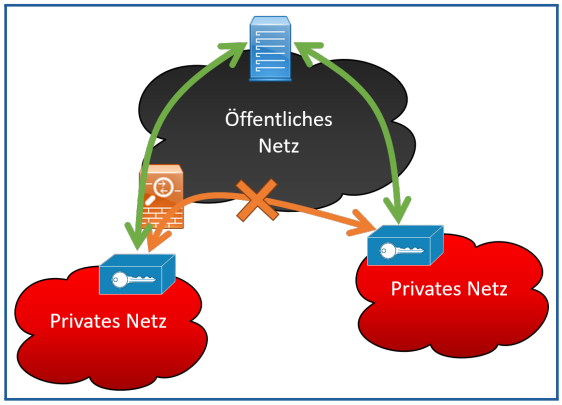
### Aufgabe

Im Rahmen des Softwareprojekts soll ein Ansatz entwickelt werden, welcher IPsec-Tunnel verschleiern kann, um so eine Blockierung zu verhindern. Als erster Ansatz soll dabei verfolgt werden, IPsec über HTTPS zu tunneln. Während HTTPS (bzw. das dafür eingesetzte Protokoll TLS) ähnliche Ziele verfolgt wie IPsec, macht der allgegenwärtige Einsatz von HTTPS im „World Wide Web“ eine pauschale Blockierung unwahrscheinlich, da sonst weite Teile des Internets nicht mehr erreichbar wären.

Insgesamt sollen dafür folgende Themengebiete bearbeitet werden:

- Entwicklung einer Server-Komponente, welche die HTTPS-Tunnel terminiert und ankommende IP-Pakete weiterleitet. Für Unbeteiligte soll sich der Server wie ein normaler Webserver verhalten (d. h. plausible Inhalte ausliefern), um eine Erkennung durch „active probing“ des Angreifers zu vermeiden.
- Die Client-Software soll beliebige IP-Pakete entgegennehmen können, um sie über die HTTPS-Verbindung zum Server zu tunneln. Paketgröße und Paket-Timing des HTTPS-Tunnels sollen plausible Charakteristika aufweisen.
- Je nach Gruppengröße ist auch ein Eingriff in das TCP-Protokoll (z. B. geschickte Veränderung der Staukontrolle) denkbar. Dies soll den Nachteil eines Tunnels über TCP im Hinblick auf die Performance der durch IPsec geschützten Kommunikation abschwächen.

Das gesamte Framework soll dabei möglichst flexibel und erweiterbar gestaltet sein, um in Zukunft einfach alternative Tunnel (zu HTTPS) integrieren zu können.




## Lernziele

Neben den Kernzielen des Software-Projektes, wie dem Erlernen von effektiver Gruppenarbeit, der strukturierten Analyse von Problemen und natürlich der Schulung praktischer Fähigkeiten, wird in diesem Projekt Wissen zu moderner Netzwerkprogrammierung und IT-Security vermittelt.

## Kontakt

M. Sc. David Schatz, Fachgebiet Telematik/Rechnernetze
Email: david[dot]schatz[at]tu-ilmenau[dot]de, Telefon: +49 3677 69 4546

Dr.-Ing. Michael Roßberg, Fachgebiet Telematik/Rechnernetze
Email: michael[dot]rossberg[at]tu-ilmenau[dot]de, Telefon: +49 3677 69 4553

Web: `https://www.tu-ilmenau.de/telematik`