

IT-Security Tutorübung 10

Dorian Zedler

7. Januar 2024

Technische Universität München

Aufgabe 1

Aufgabe 2

- Firewalls
- TLS

Aufgabe 1

Aufgabe 1a - Paketfilter vs DPI vs ALG

- a) Grenzen Sie die Konzepte Paketfilter-Firewall, Deep Packet Inspection (DPI) Firewall und Application Layer Gateway (ALG) voneinander ab!
- **Paketfilter:** ACCEPT oder DROP pro Paket, basierend auf IP-Header
 - **DPI:** Paketfilter + Analyse des Paketinhalts, meist mit Signaturdatenbank
 - **ALG:** Zugeschnitten auf bestimmte Protokolle, z.B. HTTP, SMTP, FTP. Arbeitet als Man-in-the-Middle und kann Paketinhalte verändern

Aufgabe 1b - DPI und ALG im Einsatz

- b) Vergleichen Sie jeweils welche Angriffe mit einer DPI Firewall und welche mit einer ALG Firewall verhindert bzw. erkannt werden!

Angriff	DPI	ALG
Malware	Ja, sofern Signatur der Malware in Datenbank	Nein
XSS, SQL-Injection	Nein	Ja
Phishing	Nein	Ja, z.B. Proxmox mail Gateway
Buffer-Overflow	Nein	Nein

Aufgabe 1b - DPI und ALG im Einsatz

- b) Vergleichen Sie jeweils welche Angriffe mit einer DPI Firewall und welche mit einer ALG Firewall verhindert bzw. erkannt werden!

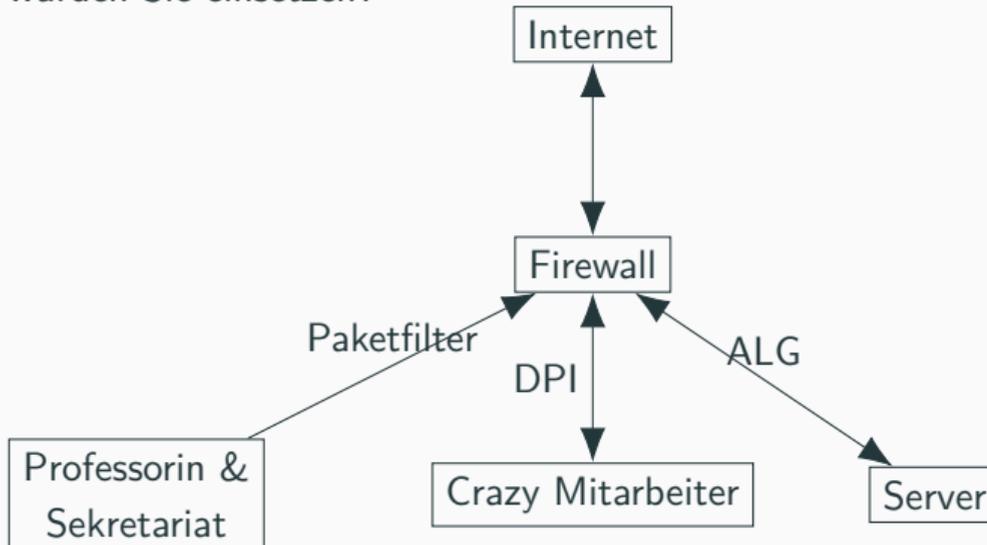
Angriff	DPI	ALG
Fehlkonfiguration (z.B. offene Ports)	Ja, aber eine reine Paketfilter-Firewall reicht aus	
Denial of Service	Ja, aber eine reine Paketfilter-Firewall reicht aus	

Aufgabe 1c - Netzwerkdesign

c) Folgende Akteure im IT-Sec Lehrstuhl-Netzwerk untergebracht werden:

- Hacking affine Mitarbeiter, die gerne Malware ausprobieren
- Server mit Webseite, E-Mail-Server, etc.
- Professorin, SekretärInnen

Wie würden Sie das Netzwerk designen? Welche Firewall-Technologie würden Sie einsetzen?



- d) Ist der Einsatz einer Firewall für *essenziell* für die Sicherheit eines Netzwerkes?
- **NEIN!**
 - Wenn in einem Netzwerk alle Services sicher sind, ist eine Firewall nicht notwendig
 - Firewalls sind lediglich eine VorsichtsmaSSnahme
 - Firewalls erzeugen Aufwand für Betrieb und Wartung und sind ein single point of failure!

Aufgabe 2e - ALG - immer gut?

- e) Könnte der Einsatz eines Application Layer Gateways die Sicherheit eines Netzwerkes auch verringern?
- **JA!**
 - Wenn das ALG eine Sicherheitslücke hat, wird es zum Angriffspunkt
 - Angreifer könnte potenziell den gesamten Netzwerkverkehr manipulieren

Aufgabe 2

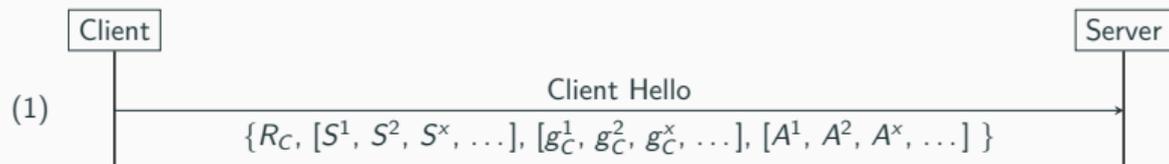
Aufgabe 2a - Dieser Kanal ist sicher?

a) Was ist ein *sicherer Kanal* und wofür wird er benötigt?



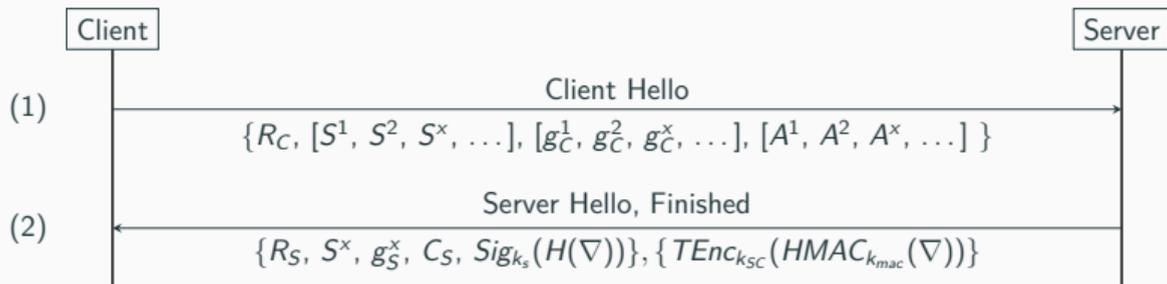
- Viele Protokolle benötigen ähnliche Schutzziele (Vertraulichkeit, Integrität, Authentizität, ...)
- Ein sicherer Kanal implementiert diese Schutzziele
- Nicht jedes Protokoll muss diese Schutzziele selbst implementieren

Aufgabe 2b - TLS



- R_C : Zufallszahl (verhindert Replay-Angriffe)
- S^x : vom Client unterstützte Cipher Suites
- $[g_C^1, g_C^2, g_C^x, \dots]$: Vom Client unterstützte DH-Verfahren sowie zugehörige Public-Keys
- A^x : vom Client unterstützte Signaturverfahren

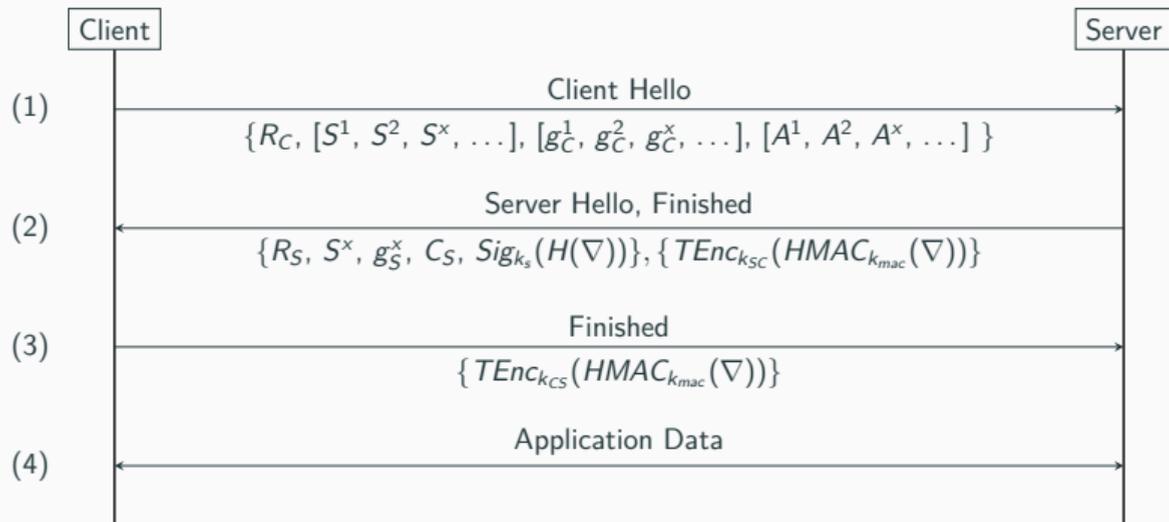
Aufgabe 2b - TLS



∇ alle Nachrichten des Handshakes bis zu diesem Punkt

- R_S : Zufallszahl (verhindert Replay-Angriffe)
- S^x : Antwort des Servers für die ausgewählte Cipher-Suite
- g_S^x : DH-Public-Key des Servers für das ausgewählte DH-Verfahren
- C_S : Zertifikat des Servers, verknüpft den öffentlichen Schlüssel mit Domain
- k_S : Privater Schlüssel des Servers
- $\text{Sig}(k_S, \nabla)$: Authentisierung von g_S^x und Beweis, dass Server K_S hat.
- $TEnc_{k_{SC}}(\text{HMAC}_{k_{mac}}(\nabla))$: Nachweis, dass der das DH-Secret kennt und Authentisierung und Integritätssicherung des Handshakes (inkl. g_S^x).

Aufgabe 2b - TLS



∇ alle Nachrichten des Handshakes bis zu diesem Punkt

- $TEnc_{k_{CS}}(HMAC_{k_{mac}}(\nabla))$ in (3): Nachweis, dass der Client das DH-Geheimnis besitzt.
- **WICHTIG:** Es gibt drei verschiedene Schlüssel: k_{SC} , k_{CS} und k_{mac} !

Aufgabe 2c - Verschiedene Schlüssel

- c) Wozu werden verschiedene Schlüssel für die beiden Kommunikationsrichtungen (k_{SC} und k_{CS}) benötigt?
- Als Replay-Schutz führt TLS auf beiden Seiten separat Sequenznummern
 - Wenn beide Seiten an derselben Sequenznummer sind und denselben Schlüssel verwenden würden, wäre es möglich, eine Nachricht wieder an den Sender zurückzusenden (*Reflection Attack*)
 - Durch die Verwendung von zwei Schlüsseln wird dies verhindert

Aufgabe 2d - TLS Parameter

- **Schlüsselaustausch Gruppe:** x25519
- **Signatur Schema:** RSA-PSS-SHA256
- **Cipher Suite:** TLS_AES_256_GCM_SHA384

d) Was ist die Bedeutung der obigen TLS Parameter?

Key Exchange: Bei TLS 1.3 wird immer ECDH verwendet. In diesem Fall über die Curve25519.

Authentifizierung des Key Exchange: RSASSA-PSS als Signatur Schema, SHA256 als Hash-Funktion.

Verschlüsselung der Nutzdaten: Die Nutzdaten werden mittels AES256 im GCM Betriebsmodus verschlüsselt.

Pseudorandomfunktion: SHA384 für Schlüsselableitung

Aufgabe 2d - TLS Parameter

- **Schlüsselaustausch Gruppe:** x25519
- **Signatur Schema:** RSA-PSS-SHA256
- **Cipher Suite:** TLS_AES_256_GCM_SHA384

d) Was ist die Bedeutung der obigen TLS Parameter?

Key Exchange: Bei TLS 1.3 wird immer ECDH verwendet. In diesem Fall über die Curve25519.

Authentifizierung des Key Exchange: RSASSA-PSS als Signatur Schema, SHA256 als Hash-Funktion.

Verschlüsselung der Nutzdaten: Die Nutzdaten werden mittels AES256 im GCM Betriebsmodus verschlüsselt.

Pseudorandomfunktion: SHA384 für Schlüsselableitung

Aufgabe 2e - 0-RTT Handshake

- Der 0-RTT Handshake erlaubt es, bereits in der ersten Handshake-Nachricht verschlüsselte *Early Data* mitzuschicken.
 - Dafür wird der Schlüssel einer vorherigen Verbindung gespeichert und wiederverwendet.
- e) Welches Problem bringt der Einsatz des *0-RTT Handshakes* von TLS 1.3 mit sich?
- Replay der ersten Nachricht möglich! →kann aber z.B. bei HTTP GET unproblematisch sein
 - Die *Early Data* hat keine PFS!