OTH Amberg-Weiden

Cybersicherheit

Netzwerksicherheit

Prof. Dr. Daniel Loebenberger

Amberg, 13. November 2024

Hinweis

OTH Amberg-Weiden

- Bitte beachten Sie das Urheberrecht!
- Alle Materialien dieser Vorlesung sind – auch wenn sie nicht ausdrücklich gekennzeichnet sind – urheberrechtlich geschützt.
- Sie dienen ausschließlich Ihrem persönlichen Gebrauch im Rahmen dieser Vorlesung.
- Die Materialien dürfen insbesondere nicht weiter verbreitet werden.
- Eigene Aufzeichnungen (Video, Foto, Ton) der Vorlesung sind nicht gestattet.

Gliederung

OTH Amberg-Weiden

1. Einführung
2. Kryptographie
3. Netzwerksicherheit
4. Systemsicherheit
5. Anwendungssicherheit
6. Kritische Infrastrukturen und staatlicher Geheimschutz
7. Sicherheitsmodelle und -evaluierung
8. Sicherheit im Unternehmen
9. Hacking und Pentesting (extern)
10. Ausblick

Überblick

OTH Amberg-Weiden

01 Wiederholung: Netzwerke

02 Klassische Netzwerksicherheit

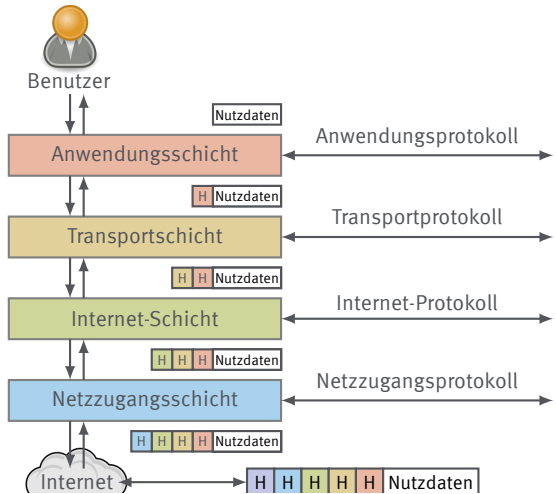
03 Kryptographische Sicherungsschichten

04 Instant Messaging

Überblick

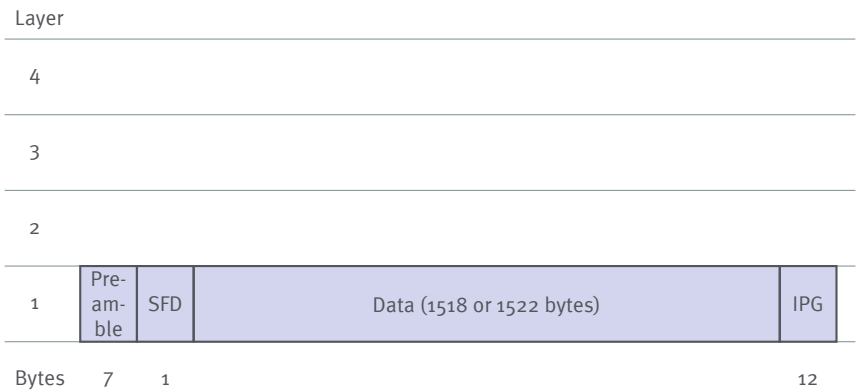
OTH Amberg-Weiden

Das TCP/IP-Modell



Datenübertragung

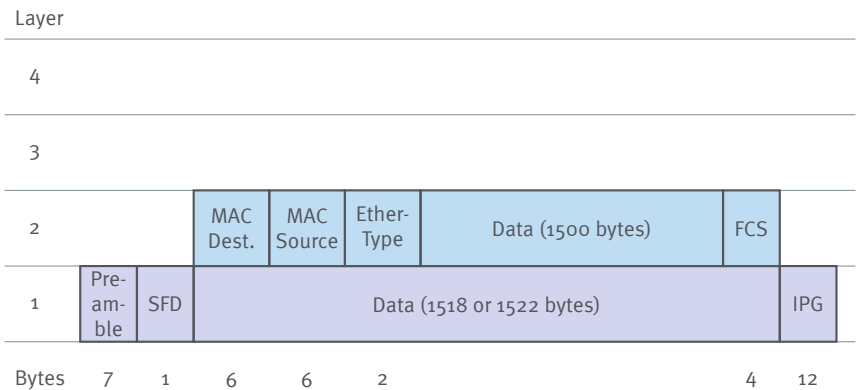
Ethernet-Frame mit maximalen IPv4- und TCP-Daten



Quelle: Andreas Aßmuth, IT-Sicherheit

Datenübertragung

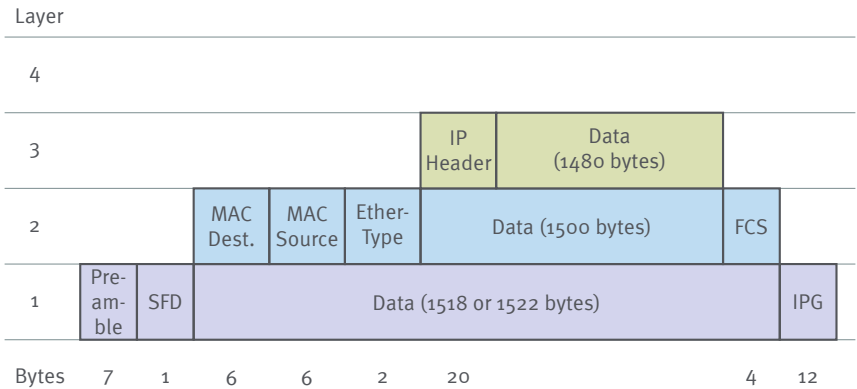
Ethernet-Frame mit maximalen IPv4- und TCP-Daten



Quelle: Andreas Aßmuth, IT-Sicherheit

Datenübertragung

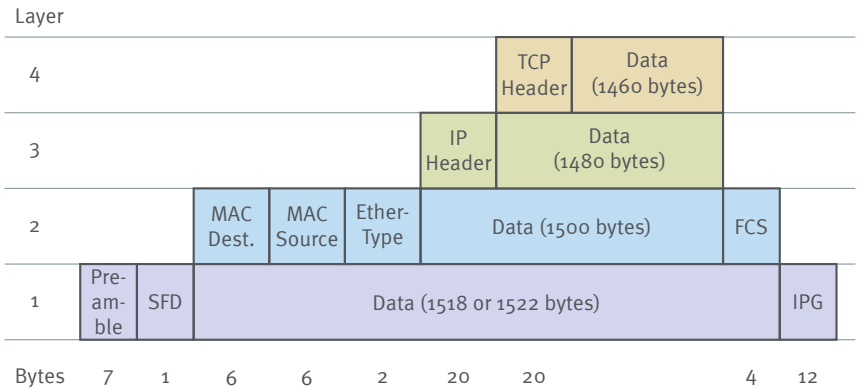
Ethernet-Frame mit maximalen IPv4- und TCP-Daten



Quelle: Andreas Aßmuth, IT-Sicherheit

Datenübertragung

Ethernet-Frame mit maximalen IPv4- und TCP-Daten



Quelle: Andreas Aßmuth, IT-Sicherheit

Das TCP/IP-Modell
Funktionen der Schichten

OTH Amberg-Weiden

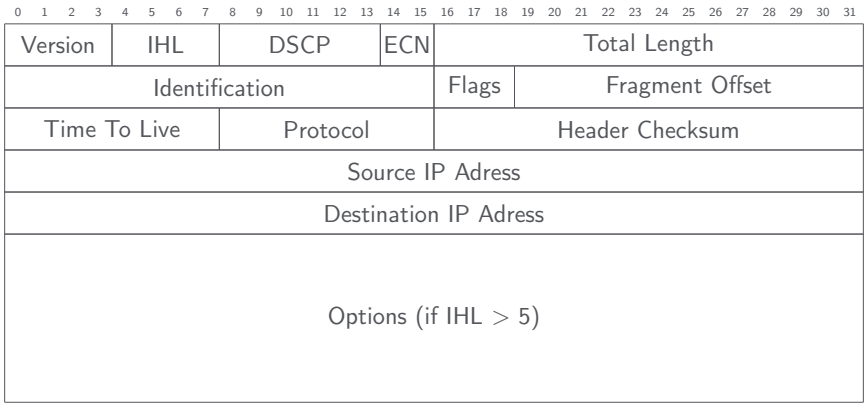
Schicht	Funktion	Protokolle
Anwendungsschicht	Datentransport	HTTP, IMAP, SMTP
Transportschicht	Ende-zu-Ende Verbindungen	TCP, UDP
Internet-Schicht	Ende-zu-Ende Übertragung	IP
Netzzugang	Punkt-zu-Punkt Übertragung	Ethernet, WLAN
Physikalische Schicht	Bit-Übertragung	1000BASE-T/X

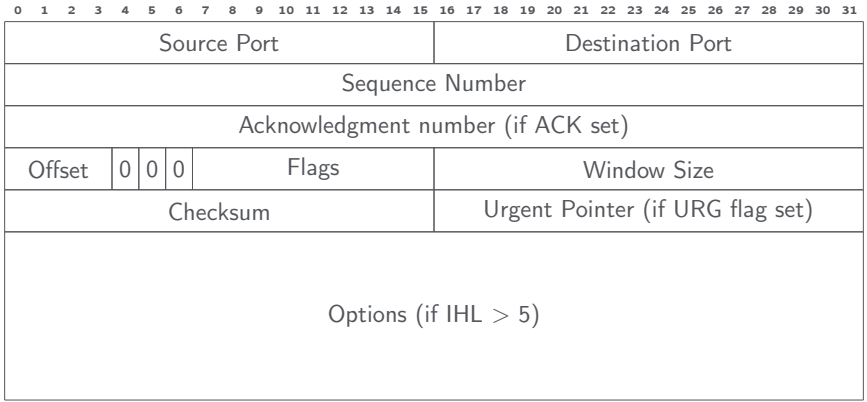
Adressierung auf unterschiedlichen Schichten

OTH Amberg-Weiden

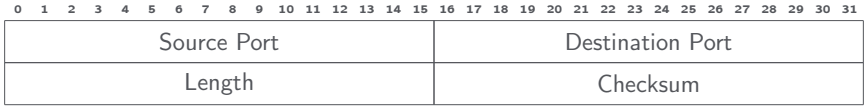
Schicht	Protokoll	Adresse	Beispiel
Anwendungsschicht	(Anwendung)	(logisch)	—
Transportschicht	TCP/UDP	Ports	`192.168.0.1:80`
Internetschicht	IP	IP-Adresse	`192.168.0.1`
Netzzugangsschicht	Ethernet	MAC Adresse	`00:81:15:7f:ad:ee`
Physikalische Schicht	(physikalisch)	(direkt)	—

Das TCP/IP-Modell
IPv4 Paket

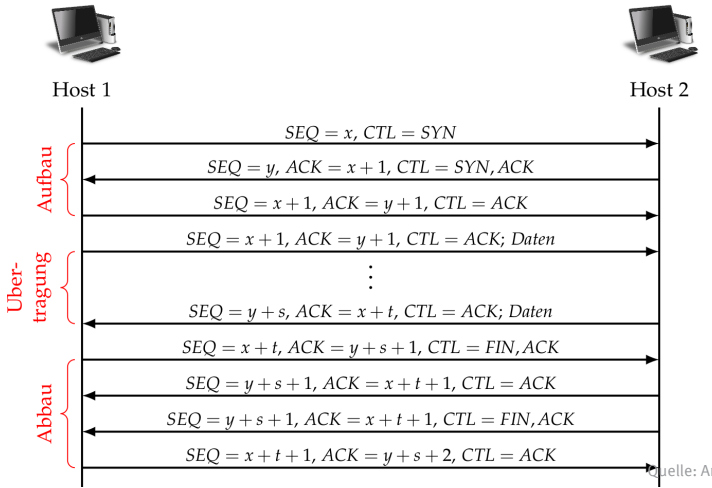



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Source Port
Destination Port
Sequence Number
Acknowledgment number (if ACK set)
Offset
0
0
0
Flags
Window Size
Checksum
Urgent Pointer (if URG flag set)
Options (if IHL > 5)

Das TCP/IP-Modell
UDP Paket



Das TCP/IP-Modell
TCP Handshake



Quelle: Andreas Aßmuth, Cybersicherheit

Dienste

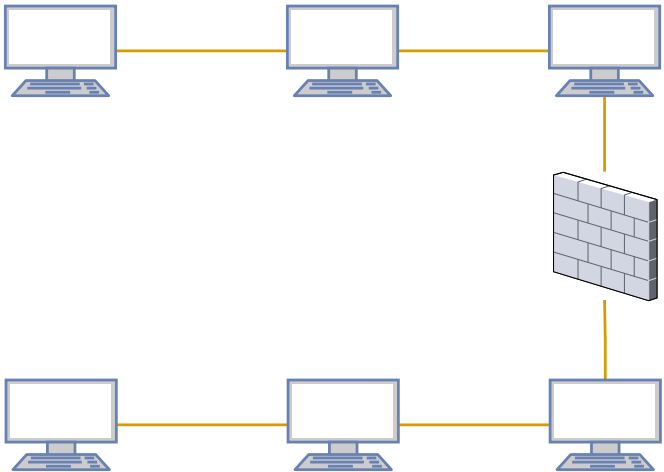
OTH Amberg-Weiden

- Abstrahierte Funktion, die von einem Computernetzwerk bereitgestellt wird
- Geschlossene Funktionskomponente aus Anwendersicht
- Realisierung über Netzwerkprotokolle
- Adressierung durch Ports
- Festlegung durch die Internet Assigned Numbers Authority (IANA)
- Basisdienste sind beispielsweise
  - Datentransfer via FTP (Port 21/TCP)
  - Namensauflösung via DNS (Port 53/TCP und Port 53/UDP)
  - Adressierung via DHCP (Port 67/UDP Server, Port 68/UDP Client)
  - Webseitenauslieferung via HTTP (Port 80/TCP)
  - Zeitauflösung via NTP (Port 123/TCP, Port 123/UDP)
  - E-Mail Abholung via IMAP (Port 143/TCP, Port 143/UDP)
  - …
- Vgl. unter Linux: `/etc/services`

Überblick

OTH Amberg-Weiden

Anwendung: Netzsegmentierung



Paketfilter Firewalls

Beispiel: IMAP Server

OTH Amberg-Weiden

Sendeadresse	Sendeport	Zieladresse	Zielport	Regel
extern	> 1023	intern	143	erlauben
extern	> 1023	intern	$\neq 143$	blockieren
intern	143	extern	> 1023	erlauben
intern	$\neq 143$	extern	> 1023	blockieren

Application-Layer Firewalls
zur Umsetzung erweiterter Filter-Funktionalitäten

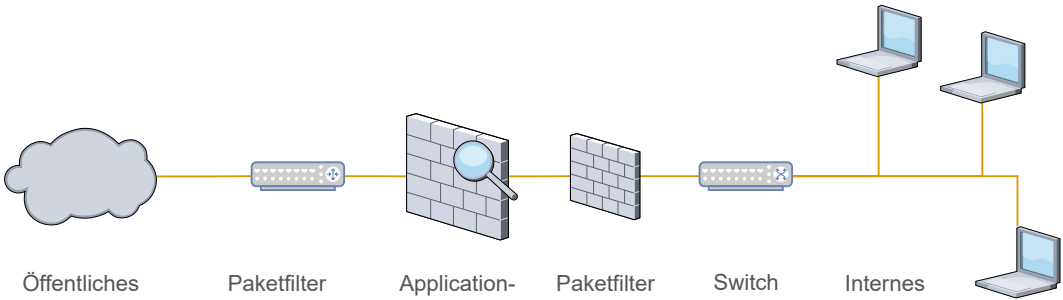
OTH Amberg-Weiden

- Unterbrechung des direkten Datenstroms zwischen internen und externen Kommunikationspartnern (z.B. Client und Server)
- Ggf. Entschlüsselung von HTTPS- und SSH-Verbindungen
- Untersuchung sowohl ein- als auch ausgehender Verbindungen
- Port-unabhängige Erkennung von Internet-, Cloud- und Geschäftsanwendungen
- Möglichkeit zur Positiv-Validierung von Applikationen und Verbindungen
- Organisations-, gruppen- bis hin zu nutzerspezifischen Firewallregeln
- Tageszeitabhängige Firewallregeln
- URL-Filter für Black- und Whitelisting von Webseiten

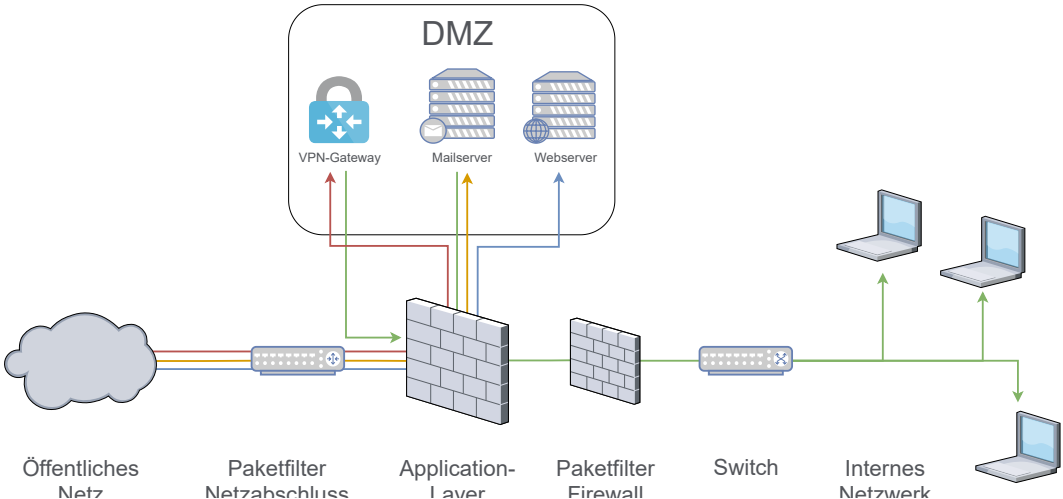
Perimeterabsicherung

P-A-P Methode

OTH Amberg-Weiden



Demilitarisierte Zone DMZ



IP-Spoofing
Struktur

OTH Amberg-Weiden

- Versenden von IP-Paketen mit gefälschter Absender-IP-Adresse
- Dazu Änderung der Quelladresse im IP-Header
- Zustellung an Opfer möglich
- Gleichzeitig Verschleierung des Absenders
- Angriff nur möglich, wenn Antworten für den Angreifer vorhersehbar oder nicht notwendig sind
- Insbesondere sind bidirektionale Verbindungen nicht betroffen

IP-Spoofing
Anwendungen

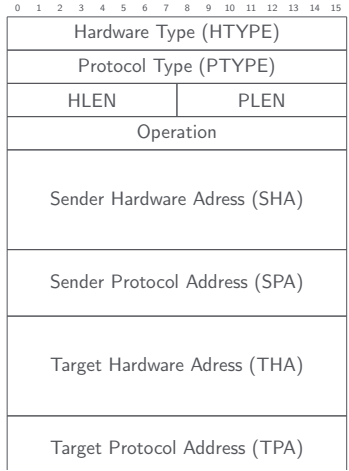
OTH Amberg-Weiden

- Umgehung IP-adressbasierter Authentifizierung im Netzwerk
- Besonders effektiv, wenn zwischen Maschinen Vertrauensbeziehungen bestehen
- Realisierung von Distributed Denial of Service Angriffen
  - SYN-Flooding: Abbruch des Threeway-TCP-Handshake von Seiten des Angreifers, wodurch beim Opfer viele offene Verbindungen auflaufen
  - DNS Amplification Attack: Missbrauch des Domain Name Systems, sodass extrem große Datenströme auf den Internetanschluss des Opfers gelenkt werden
- Mögliche Gegenmaßnahme: Paketbasierte Firewall
  - eingehende Filterung: blockiere von außen kommende Pakete mit einer internen Absendeadresse
  - ausgehende Filterung: blockiere von innen kommende Pakete mit einer externen Absendeadresse

ARP Request Poisoning
(Wo)man-in-the-middle Angriff in der Praxis

OTH Amberg-Weiden

- ARP Pakete beinhalten Zuordnung zw. IP-Adresse und physikalischer MAC-Adresse
- Zuordnung wird in den Endgeräten in Tabellen abgelegt
- Idee: Flute beide Kommunikationspartner mit ARP Paketen, die eine „falsche“ MAC-Adresse (nämlich die des Angreifers) beinhalten
- Damit wird die IP-Kommunikation über den Angreifer umgeleitet!
- Dies realisiert einen praktischen Man-in-the-middle Angriff



Übungsaufgaben

OTH Amberg-Weiden

In der Vorlesung haben wir über klassische Netzsegmentierung gesprochen. Eine zentrale Komponente stellt hier die (paketbasierte) Firewall dar. Ihre Aufgabe ist nun, eine Sicherheitsanalyse zu Firewalls zu erstellen.

3.1.1. Welche Bedrohungen im Kontext von Manipulation durch Dritte sehen Sie bei Firewalls?

3.1.2. Um was handelt es sich bei einer Distributed Denial of Service (DDoS) Attacke?

3.1.3. Welche Anforderungen im Hinblick auf die (Filter-)Konfiguration der Firewall sehen sie?

3.1.4. Welche Anforderungen an die Administrationsschnittstelle gibt es?

3.1.5. Welchen Nutzen hat die penible Protokollierung im Firewall-Kontext?

3.1.6. Welche Grenzen der Filterung sind generell bei pakterbasierten Firewalls zu erwarten?

3.1.7. Wie kann man diese Grenzen durch eine „Application Layer Firewall“ aufheben? Wie funktioniert das?

Übungsaufgaben

OTH Amberg-Weiden

Studieren Sie den Artikel `https://cr.yp.to/syncookies.html`

3.2.1. Welches Problem wird adressiert?

3.2.2. Was sind SYN-Cookies genau?

3.2.3. Wie ist die Struktur von SYN-Cookies definiert?

3.2.4. Wie werden diese eingesetzt?

3.2.5. Nennen Sie drei Gründe für die weite Verbreitung von SYN-Cookies in der Praxis.

Überblick

OTH Amberg-Weiden

01 Wiederholung: Netzwerke

02 Klassische Netzwerksicherheit

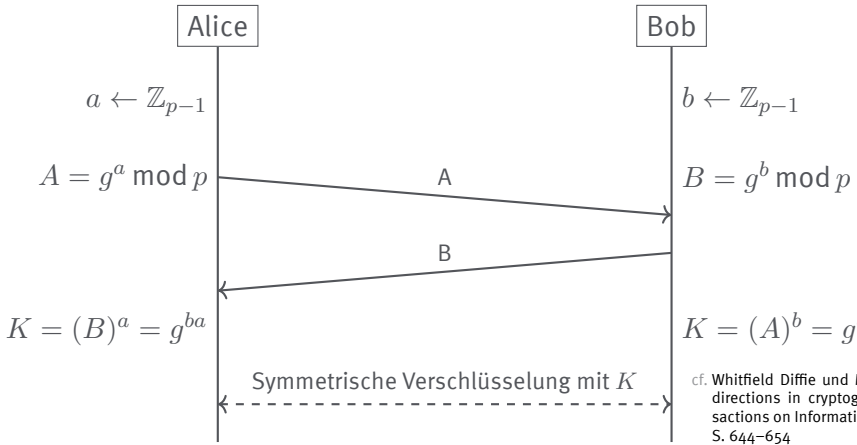
03 Kryptographische Sicherungsschichten

04 Instant Messaging

Wiederholung: Schlüsselaustausch

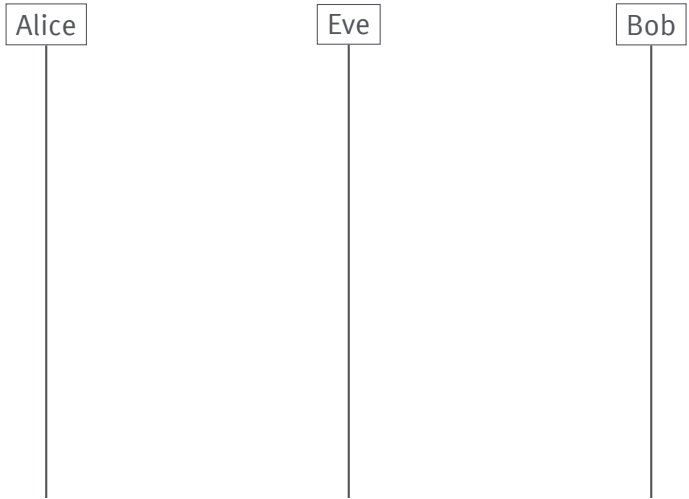
Diffie-Hellman Protokoll

Parameter: p Primzahl, g Generator von $\mathbb{Z}_p^\times$



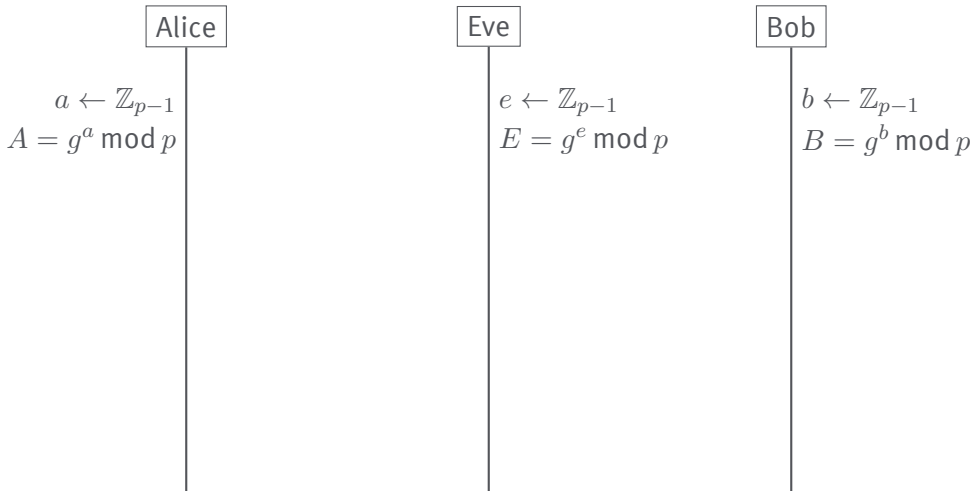
cf. Whitfield Diffie und Martin Hellman. "New directions in cryptography". In: IEEE transactions on Information Theory 22.6 (1976), S. 644–654

(Wo)man-in-the-middle Angriff

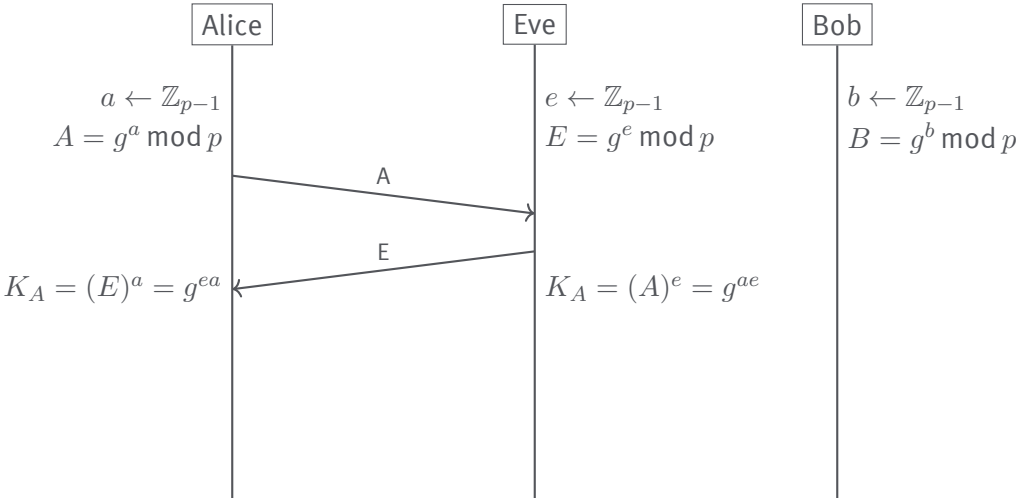


(Wo)man-in-the-middle Angriff

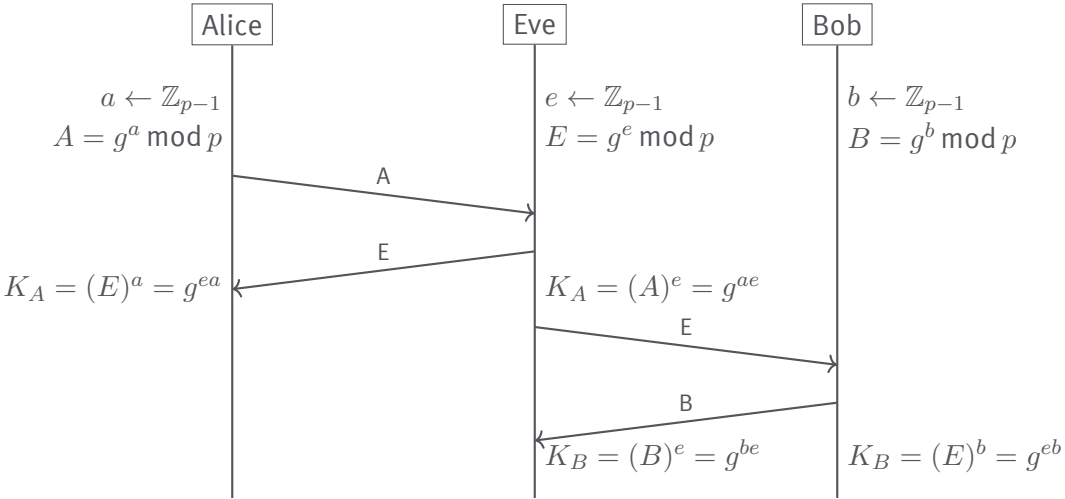
OTH Amberg-Weiden



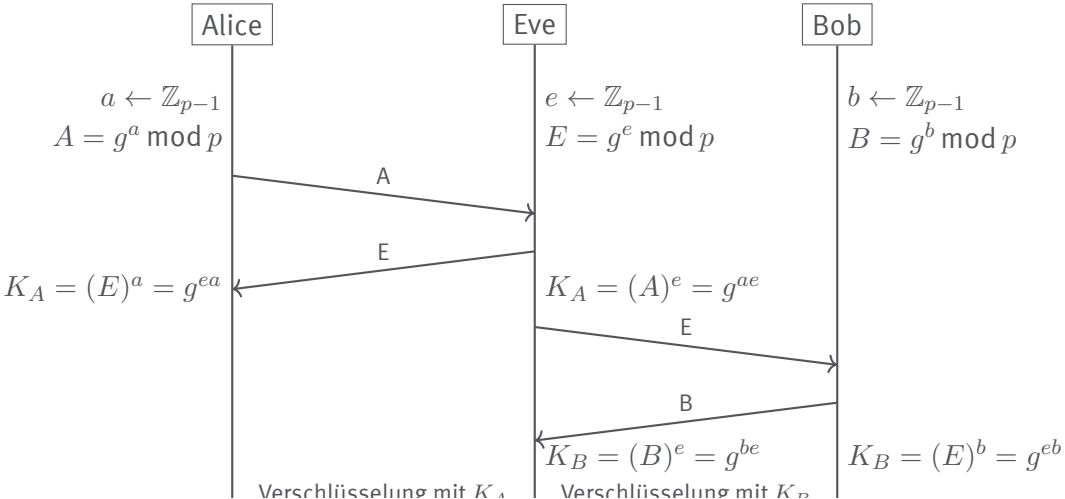
(Wo)man-in-the-middle Angriff



(Wo)man-in-the-middle Angriff



(Wo)man-in-the-middle Angriff



Zertifikate

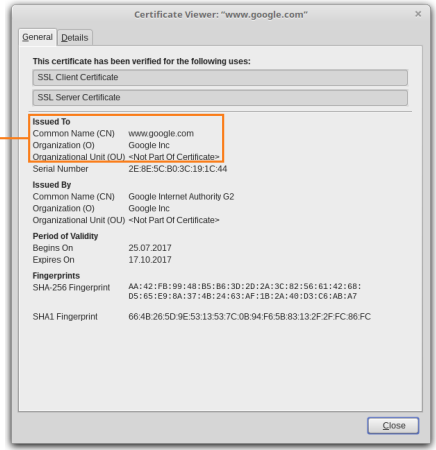
Subjekt

Aussteller

Gültigkeit

ID-Nr.

Schutz gegen Manipulation



Zertifikate

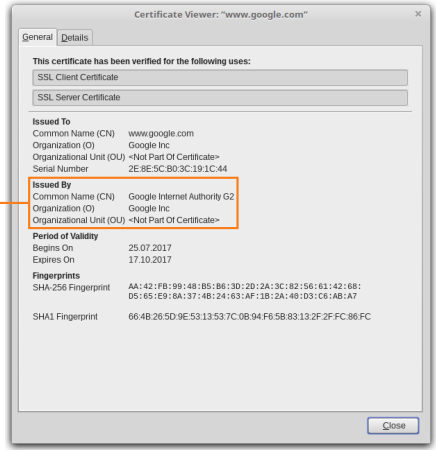
Subjekt

Aussteller

Gültigkeit

ID-Nr.

Schutz gegen Manipulation



Zertifikate

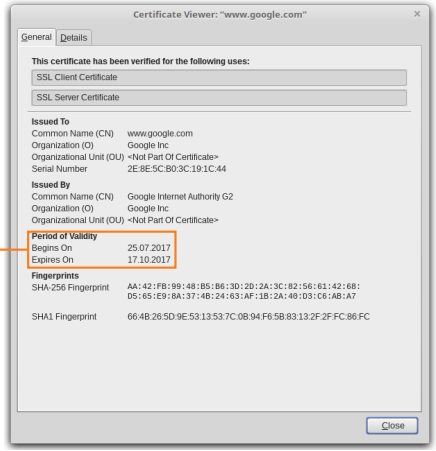
Subjekt

Aussteller

Gültigkeit

ID-Nr.

Schutz gegen Manipulation



Zertifikate

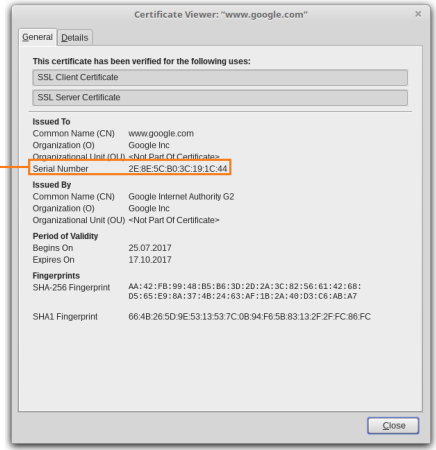
Subjekt

Aussteller

Gültigkeit

ID-Nr.

Schutz gegen Manipulation



Digitale Zertifikate zur Authentisierung

Detaillierter Aufbau von X.509 Zertifikaten

OTH Amberg-Weiden

- Struktur formal ausgedrückt in Abstract Syntax Notation One (ASN.1)
- Speicherung typischer Weise Base64-codiert
- Relevante Felder (Auswahl):
  - Signatur-Algorithmus: Name des verwendeten Algorithmus
  - Aussteller/Zertifikatsinhaber: Eindeutiger Bezeichner (Common Name `CN`, Organisation Unit `OU`, Organization `O`, ...)
  - Schlüsselinformationen: Public-Key Algorithmus, Public-Key
  - Signatur: Digitale Signatur des Austellers gemäß Signaturalgorithmus
  - Erweiterungen: Optionale Erweiterungen
- Ungültige Zertifikate werden in Zertifikatsperrlisten abgespeichert

Digitale Zertifikate zur Authentisierung

Hierarchische Public-Key Infrastruktur

OTH Amberg-Weiden

- Jedes Zertifikat wird von einer Zertifizierungsstelle (engl. certification authority CA) unterschrieben
- Die CA weist sich wieder durch ein Zertifikat aus
- Dessen Gültigkeit wird widerum von einer (höheren) CA durch eine Signatur beglaubigt
- Dieser Prozess setzt sich bis zur Wurzelinstanz rekursiv fort, diese signiert ihr Zertifikat selbst
- Die Gültigkeit des Wurzelzertifikats wird explizit durch Speicherung auf den Endgeräten der Nutzer festgestellt

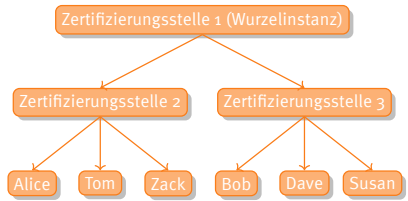
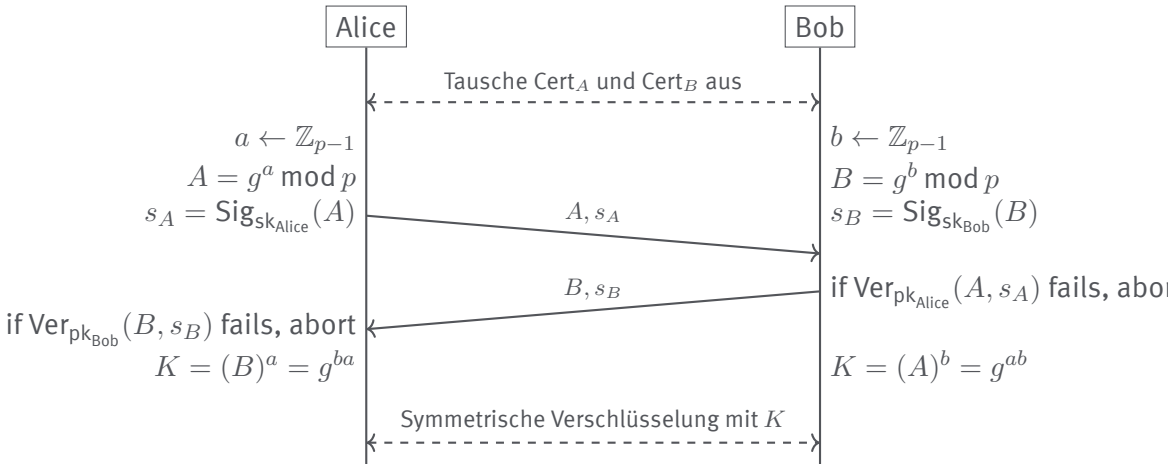


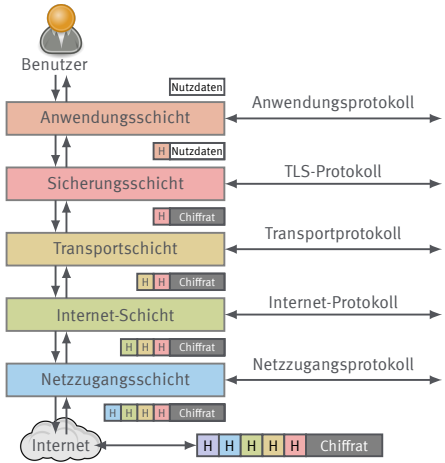
Bild: Andreas Aßmuth, IT-Sicherheit

Zertifikatbasierter Schlüsselaustausch

Parameter: p Primzahl, g Generator von $\mathbb{Z}_q^\times$. Cert_A, Cert_B Zertifikate



Das TCP/IP-Modell
mit Sicherungsschicht auf Transport-Ebene



Transport Layer Security (TLS)
Sicherungsschicht auf Transportebene

OTH Amberg-Weiden

- Transport Layer Security (TLS)
- Spezifikationen:
  - TLS 1.2 in RFC5246
  - TLS 1.3 in RFC8446
- Absicherung gängiger Anwendungsprotokolle wie z. B.
  - HTTP (Port 80/TCP) $\Rightarrow$ HTTPS (Port 443/TCP)
  - FTP (Port 21/TCP) $\Rightarrow$ FTPS (Port 989/TCP bzw. 990/TCP)
  - IMAP (Port 143/TCP) $\Rightarrow$ IMAPS (Port 993/TCP)
  - ...

Transport Layer Security (TLS)
Protokollkomponenten

OTH Amberg-Weiden

TLS Handshake: Sicherer Schlüsselaustausch

- Schlüsselaustausch typischer Weise mit Diffie-Hellman
- Authentisierung durch X.509 Zertifikate (RFC5280)
- Serverseitig verbindlich, clientseitig optional
- Ergebnis: Ableitung eines gemeinsamen Sitzungsschlüssels
- Wird der Sitzungsschlüssel für jede Verbindung neu berechnet, erreicht man Perfect Forward Secrecy
- Schlüsselaustausch bezeichnet man dann als kurzlebig (engl. ephemeral)

TLS Record: Sichere Datenübertragung

- Ende-zu-Ende-Verschlüsselung mittels symmetrischer Algorithmen
- Sicherung der Nachrichtenintegrität durch Message Authentication Codes

TLS Cipher Suites

OTH Amberg-Weiden

Festlegung verwendeter Kryptographie:

- Schlüsselaustausch (RSA, (EC)DH, …)
- Signaturverfahren (RSA, (EC)DSA, …)
- Symmetrische Verschlüsselung (AES, CAMELLIA, …)
- Operationsmodus (CBC, CTR, GCM, …)
- Hash-Funktion (SHA256, SHA512, …)

TLS Cipher Suites

OTH Amberg-Weiden

Festlegung verwendeter Kryptographie:

- Schlüsselaustausch (RSA, (EC)DH, …)
- Signaturverfahren (RSA, (EC)DSA, …)
- Symmetrische Verschlüsselung (AES, CAMELLIA, …)
- Operationsmodus (CBC, CTR, GCM, …)
- Hash-Funktion (SHA256, SHA512, …)

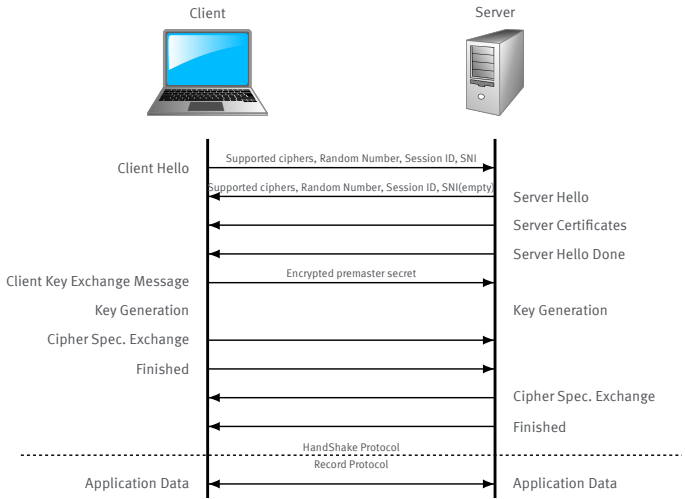
Auswahl der Form

```
TLS_<Schlüsselaustausch>[_<Signatur>]_WITH_<Verschlüsselung>_<Modus>_<Hash>
```

beispielsweise `TLS_DHE_RSA_WITH_AES_128_CBC_SHA256`, siehe TR02102-2

Es existieren auch viele RFCs mit Definitionen, z. B. RFC5246, RFC5288, RFC5289, RFC7251, ….

Transport Layer Security (TLS)
Nachrichtenfluss



Transport Layer Security (TLS)
ClientHello und ServerHello

OTH Amberg-Weiden

Parameter:

- TLS Version
- 32 Byte Zufallsinformation (4 Byte Zeitstempel + 28 Byte Zufall)
- Session-ID
- Cipher Suite
- In TLS 1.3 werden hier auch schon die Diffie-Hellman Teile übertragen

Transport Layer Security (TLS)
Authentisierung

OTH Amberg-Weiden

- Server identifiziert sich gegenüber dem Client
- Hierbei überträgt dieser ein X.509 Zertifikat
- Nun wird eine Signatur der bereits übertragenen Nachrichten übermittelt
- Der Client prüft Zertifikat und Unterschrift
- Schlägt irgendetwas davon fehl, wird die Verbindung abgebrochen
- Optional kann der Server ein Zertifikat vom Client anfordern

OTH Amberg-Weiden

Zunächst Ableitung des `pre-master-secret`

- Nutzung von RSA-Verschlüsselung:
  - Geheimnis wird vom Client aus der Zufallsinformation der Hello-Nachrichten abgeleitet
  - Dies wird mit dem öffentlichen Schlüssel aus dem Zertifikat des Servers verschlüsselt
  - Danach erfolgt die Übertragung an den Server
- Nutzung des Diffie-Hellman Schlüsselaustauschs
  - Ableitung des Geheimnisses durch beide Parteien
  - Realisiert Perfect Forward Secrecy, wenn die Hälften jedesmal neu gewählt werden!
  - Empfohlener Modus

Transport Layer Security (TLS)
Ableitung der Master Secrets

OTH Amberg-Weiden

Zunächst Ableitung des `pre-master-secret`

- Nutzung von RSA-Verschlüsselung:
  - Geheimnis wird vom Client aus der Zufallsinformation der Hello-Nachrichten abgeleitet
  - Dies wird mit dem öffentlichen Schlüssel aus dem Zertifikat des Servers verschlüsselt
  - Danach erfolgt die Übertragung an den Server
- Nutzung des Diffie-Hellman Schlüsselaustauschs
  - Ableitung des Geheimnisses durch beide Parteien
  - Realisiert Perfect Forward Secrecy, wenn die Hälften jedesmal neu gewählt werden!
  - Empfohlener Modus

Ableitung weiterer Schlüssel:

- Aus dem `pre-master-secret` kann das `master secret` abgeleitet werden
- Dieses stellt einen einmaligen Sitzungsschlüssel (engl. session key) dar
- Aus dem `master secret` erfolgt die Ableitung der Schlüssel
  - für die Ver- und Entschlüsselung
  - für die Integritätssicherung

Übungsaufgaben

OTH Amberg-Weiden

3.3.1. Prüfen Sie nach, dass bei einem authentisierten Schlüsselaustausch Woman-in-the-Middle Angriffe nicht mehr möglich sind.

3.3.2. Erkunden Sie die Darstellung „The Illustrated TLS Connection“ auf der Webseite

`https://tls12.xargs.org/`

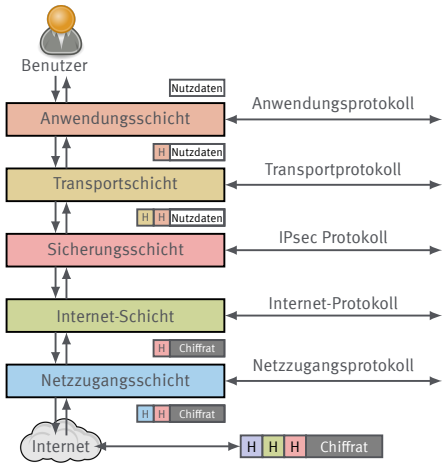
(a) Welches asymmetrische Schlüsseleinigungsverfahren wird verwendet?
(b) Ist das resultierende Protokoll flüchtig („ephemeral“)?
(c) Wie wird das `pre-master-secret` in dem konkreten Fall abgeleitet?
(d) Wie werden die für TLS Record notwendigen symmetrischen Schlüssel berechnet?
(e) Mit welchen Verfahren erfolgt die symmetrische authentisierte Verschlüsselung?

3.3.3. Die Version 1.3 von TLS wird dort ebenfalls illustriert:

`https://tls13.xargs.org/`

Vergleichen Sie die Struktur beider Protokolle. Wie erfolgt in TLS 1.3 eine Beschleunigung des Verbindungsaufbaus?

Das TCP/IP-Modell
mit Sicherungsschicht auf Internet-Ebene

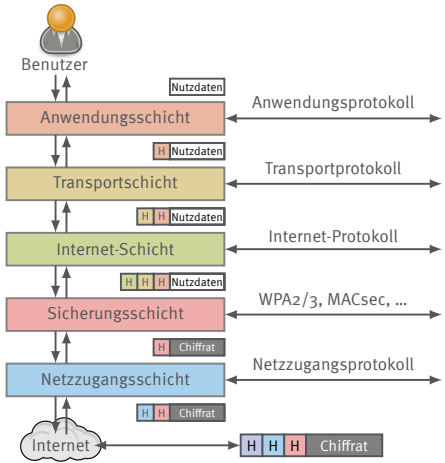


Internet Protocol Security (IPsec)
Sicherungsschicht auf Internet-Ebene

OTH Amberg-Weiden

- Absicherung auf Internet-Schicht, sog. Virtuelle Private Netze (VPNs)
- Ziel: verschlüsselungsbasierte Sicherheit auf Netzwerkebene
- IPsec ermöglicht damit eine verbindungslose Umsetzung der Schutzziele
- Sehr komplexes Protokoll, viele Konfigurationsmöglichkeiten
- Grobe Protokollstruktur ähnlich wie bei TLS
  - Erst Schlüsselaustausch (Internet Key Exchange, IKE)
  - Danach symmetrische Verschlüsselung der Nutzdaten
- Aktuell ist der Schlüsselaustausch IKEv2 nach RFC7296
- Details finden sich in RFC 4301 (aus dem Jahr 2005) und über 30 weiteren RFCs!

Das TCP/IP-Modell
mit Sicherungsschicht auf Netzzugangsebene



Wi-Fi Protected Access (WPA2)

Sicherungsschicht auf Netzzugangsebene

OTH Amberg-Weiden

- Standardisiert in IEEE 802.11i-2004
- Eine Client Station (STA) authentisiert sich mit dem Access Point (AP)
- Dazu Nutzung eines Pre-Shared-Key (PSK) oder eines RADIUS-Servers („Enterprise Mode“)
- Hier behandeln wir nur erstere Variante
- Protokoll beweist gegenseitig, dass der jeweils andere Kommunikationspartner PSK kennt
- Ziel des Protokolls:
  - Ableitung eines Pairwise Transient Key (PTK) unter Nutzung des PSK, zwei Nonces (ANonce, SNonce) und beiden MAC Adressen (AMAC, SMAC)
  - Erzeugung eines Group Temporal Key (GTK) für

Quelle: Raimond Spekking / CC BY-SA 4.0

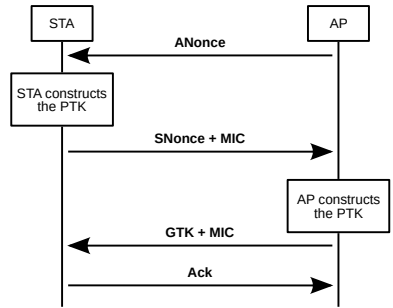
Wi-Fi Protected Access (WPA2)
Handshake mit Pre-Shared-Key

OTH Amberg-Weiden

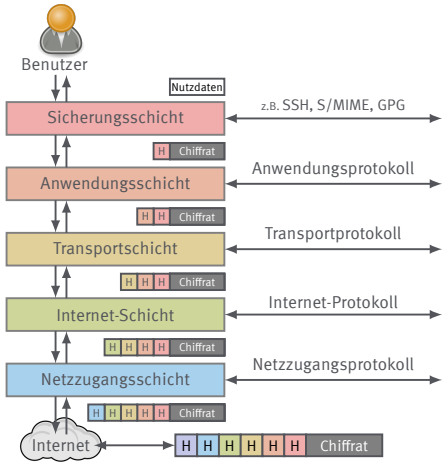
- AP schickt eine Nonce (ANonce) an STA mit einem Key Replay Counter. STA kann den PTK nun berechnen:

$$\text{PTK} = \text{PRF}(\text{PSK}, \text{ANonce}, \text{SNonce}, \text{AMAC}, \text{SMAC})$$

  PRF ist eine auf HMAC-SHA-1 basierende Funktion
- STA schickt ebenfalls eine Nonce (SNonce) zum AP zusammen mit einem Message Integrity Code (MIC) und dem gleichen Key Replay Counter
- AP verifiziert die Nachricht, berechnet PTK wie oben und schickt (verschlüsselt) einen Gruppenschlüssel GTK zusammen mit einem MIC zurück an den STA
- STA bestätigt dies



Das TCP/IP-Modell
mit Sicherungsschicht auf Anwendungs-Ebene



Secure Shell (SSH)

Sicherungsschicht auf Anwendungsebene

OTH Amberg-Weiden

- Meist genutzt, um sicheres Login auf entfernter Maschine zu erhalten
- Spezifiziert in multiplen RFCs (z. B. RFC425{0,1,2,3,4,5,6}, ..., RFC8332)
- Basiert auf Host-Schlüsseln, die bei erstmaliger Verbindung ausgetauscht werden
- In zwei verschiedenen Versionen verfügbar (SSH und SSH2)
- Offene Implementierung: `OpenSSH`
- Liste vertrauenswürdiger Schlüssel `~/.ssh/authorized_keys`

Secure Shell (SSH)
Anwendungen

OTH Amberg-Weiden

- Sichere Systemverwaltung
  - Fernverwaltung von Servern
  - Oft über Kommandozeile, aber auch X11 kann über SSH transportiert werden
  - Ersetzung unsicherer Alternativen wie `rlogin`
- Sicheres Tunneln
  - Tunneln beliebiger TCP/IP-Verbindungen
  - Sichere Portweiterleitung
  - jeweils Weiterleitung eines einzelnen Ports
  - von einem entfernten Server auf den Client oder umgekehrt
- Sichere Ausführung von Kommandos
  - Ausführung einzelner Befehle auf einem anderen Rechner
  - Weiterleitung von Standardein- und -ausgabe möglich
  - Beispiel: Sicherer Dateitransfer

Secure Shell (SSH)
Architektur

OTH Amberg-Weiden

- Transport Layer Protocol
  - Serverauthentisierung
  - Verschlüsselung
  - Integritätssicherung
  - optional: Datenkompression
  - setzt logisch auf dem TCP/IP-Protokoll auf
- User Authentication Protocol
  - authentisiert den Benutzer gegenüber dem Server
  - setzt auf dem Transport Layer Protocol auf
- Connection Protocol
  - Erzeugung und Verwaltung logischer Kanäle innerhalb des verschlüsselten Tunnels
  - setzt auf dem User Authentication Protocol

Secure Shell (SSH)
Transport Layer Protocol

OTH Amberg-Weiden

- Spezifiziert in RFC 4253
- Nutzung über TCP/IP
- Ausgetauscht werden stets Pakete mit MAC
- Normalerweise zwei Runden
- Key Exchange Init (`SSH_MSG_KEXINIT`):
  - Schlüsselaustauschverfahren für den initialen Schlüsselaustausch (inkl. Hash-Funktion)
  - Message Authentication Code für die Pakete
  - symmetrisches Verschlüsselungsverfahren für den späteren Datentransport
  - Signaturverfahren für die serverseitige Authentisierung
- Diffie-Hellman Key Exchange (`SSH_MSG_KEXDH_INIT`, `SSH_MSG_KEXDH_REPLY`):
  - Hälften des Diffie-Hellman Geheimnisses
  - der öffentliche Host-Key des Servers in der Antwort
  - eine serverseitige Signatur unter Nutzung dieses Host-Keys in der Antwort
- Ausgabe des Schlüsselaustauschs: Gemeinsames Geheimnis K und Session-ID H

Secure Shell (SSH)
User Authentication Protocol

OTH Amberg-Weiden

- Spezifiziert in RFC 4252
- Baut auf dem Transport Layer Protocol auf
- Authentisierung des Nutzers mittels:
  - Passwort
  - Öffentlichem Schlüssel
  - Host-Basiert
  - Keine
- Präferierte Wahl: mit öffentlichem Schlüssel

Secure Shell (SSH)
Connection Protocol

OTH Amberg-Weiden

- Spezifiziert in RFC 4254
- Baut auf dem User Authentication Protocol auf
- Erlaubt den Aufbau bidirektionaler Verbindungen
- Dadurch parallele Realisierung unterschiedlicher Funktionalitäten
  - Öffnen einer interaktiven Shell
  - Ausführen eines Kommandos
  - Weiterleiten graphischer Informationen (X11 Forwarding)
  - Ausführen eines ganzen Subsystems (z.B. Datentransfer)

Übungsaufgaben

OTH Amberg-Weiden

3.4.1. Konsultieren Sie die technische Richtlinie TR02102-2.
   (a) Welche TLS Versionen werden empfohlen?
   (b) Wie lautet die dortige Definition von Perfect Forward Secrecy?
   (c) Wie realisiert man diese im TLS Protokoll?
   (d) Was versteht man unter Schlüsseleinigung mit vorab ausgetauschten Daten?

3.4.2. Erläutern Sie, welchen Nutzen die Zufallsinformationen im ClientHello und ServerHello beim TLS Protokoll haben.

3.4.3. Wir betrachten sog. X.509 Zertifikate
   (a) Welchen Nutzen haben X.509 Zertifikate? Wie sind diese strukturiert?
   (b) Wo finden diese Anwendung?
   (c) Wie wird die Verbindung zwischen einem geheimen Schlüssel und der auf dem Zertifikat befindlichen Indentifizierungsinformation hergestellt?
   (d) Wer prüft diese Verbindung? Wie prüft man allgemein ein derartiges Zertifikat?
   (e) Prüfen Sie das Zertifikat der Webseite `https://www.oth-aw.de`. Welche Algorithmen werden eingesetzt?

Übungsaufgaben

OTH Amberg-Weiden

Betrachten Sie das SSH Transport Protokoll in RFC 4253

3.5.1. Welchen Zweck hat das Binary Packet Protocol in Kapitel 6?

3.5.2. Wie wird die MAC im Binary Packet Protocol berechnet?

3.5.3. Welche Informationen fließen in die Berechnung der MAC ein? Warum?

3.5.4. Wie geschieht die Berechnung des gemeinsamen Geheimnisses K?

3.5.5. Wie wird die Session-ID H abgeleitet? Welche Informationen fließen ein? Warum?

3.5.6. Wie wir die Gültigkeit des Host-Key geprüft?

3.5.7. Tricky: In der Nachricht `SSH_MSG_KEXINIT` findet sich vor der Algorithmenwahl ein zufälliges Cookie. Der RFC schreibt lapidar:

> „Its purpose is to make it impossible for either side to fully determine the keys and the session identifier.“

Allerdings kommt im restlichen RFC dieses Cookie nie wieder vor. Wo fließt dieses im späteren Verlauf in die Berechnungen dennoch ein?

Überblick

OTH Amberg-Weiden

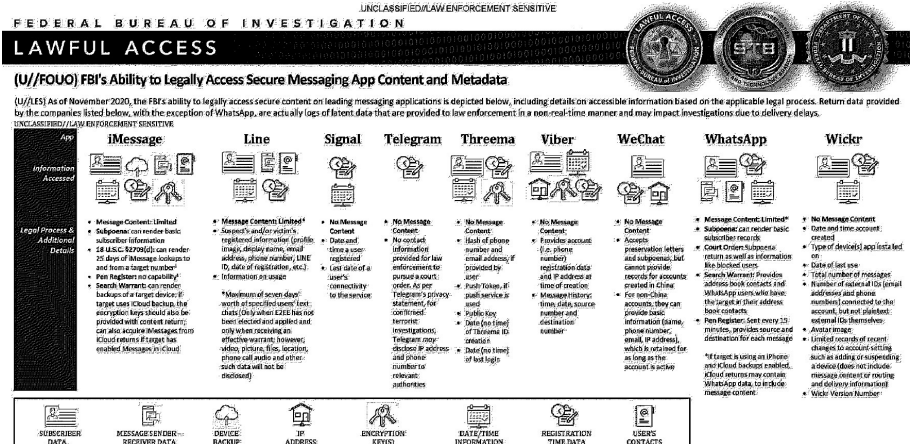
Instant Messaging

OTH Amberg-Weiden

- Übertragung von Textnachrichten von einem Gerät zu einem weiteren
- Alternativ: Sprachverbindungen, Videotelefonie
- Ursprünglich SMS bzw. Telefonate (unverschlüsselt)
- Sichere Alternativen:
  - WhatsApp: Erworben von Facebook Inc. im Jahr 2014 für 1 Mrd. Dollar
  - Threema: Schweizer Unternehmen Threema GmbH, Protokoll proprietär
  - Telegram: Client OpenSource, Server proprietär, betrieben von der Telegram Messenger LLP
  - Signal: OpenSource, betrieben von der gemeinnützigen Signal-Stiftung
  - ...
- Protokolle unterscheiden sich jeweils stark von einander und realisieren unterschiedlichste Sicherheitseigenschaften

Übersicht des FBI

OTH Amberg-Weiden



Das Signal Protokoll
Überblick

OTH Amberg-Weiden

- Kryptographisches Kommunikationsprotokoll für Nachrichtenaustausch
- Nutzung beim Instant Messaging:
  - Ende-zu-Ende-verschlüsselt
  - Authentisierung der Kommunikationspartner
- Es müssen nicht beide Kommunikationspartner gleichzeitig online sein
- Ziel: Nicht nur Verschlüsselung, sondern auch Begrenzung des Schadens bei Kompromittierung eines der Teilnehmer
- Dazu Nutzung kurzlebiger Sitzungsschlüssel, die in einem sog. Double-Ratchet-Verfahren erneuert werden.

Das Signal Protokoll
Eigenschaften

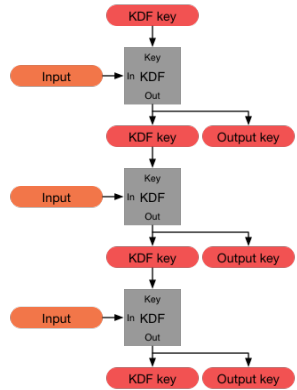
OTH Amberg-Weiden

- Verschlüsselung der Inhalte auf dem gesamten Transportweg
- Authentisierung der Gegenstelle
- Absicherung gegen Manipulation der Nachrichten
- Perfect Forward Secrecy bei Offenbarung des geheimen Hauptschlüssels
- Absicherung früherer und späterer Nachrichten nach der Offenbarung eines Sitzungsschlüssels
- Glaubhafte Abstreitbarkeit der Urheberschaft an einer Nachricht
- Möglichkeit der Schlüsselableitung ohne Interaktion
- Folgenlose Vorhaltung von Schlüsseln für außer der Reihe eintreffende Nachrichten
- Umsortierung, Auslassung und Wiedereinspielung von Nachrichten kann detektiert werden

Das Signal Protokoll
Schlüsselableitungsketten

OTH Amberg-Weiden

- Ableitung von Schlüsseln mittels einer Schlüsselableitungsfunktion (engl. key derivation function, KDF)
- Eigenschaften:
  - Widerstandsfähigkeit (engl. resilience): Ausgabe `Out` scheint für Angreifer zufällig, wenn der KDF-Schlüssel `Key` unbekannt ist. Auch korrekt, wenn der Angreifer den Input `In` manipulieren kann.
  - Rückwärtssicherheit (engl. backward security): Alle frühere Ausgaben `Out` scheinen für den Angreifer zufällig, wenn sie Kenntnis eines KDF-Schlüssels `Key` erhält.
  - Einbruchssicherheit (engl. break-in recovery): Künftige Ausgaben `Out` scheinen bei zufälligem Input zufällig für einen Angreifer, der einen KDF-Schlüssel `Key` kennt.
- KDF: z.B. HMAC-Konstruktion

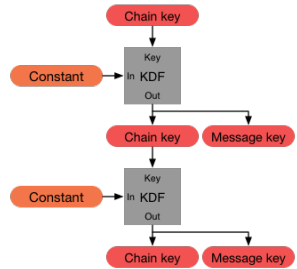


Quelle: Trevor Perrin und Moxie Marlinspike. “The double ratchet algorithm”. In: GitHub wiki (2016). URL: `https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf`

Das Signal Protokoll
Symmetrische Sperre

OTH Amberg-Weiden

- Ableitung von Nachrichtenschlüsseln (engl. message keys)
- Chain-Key `Key` ist ein Schlüssel, der jeweils zum Verschicken bzw. Empfangen erzeugt wird (siehe Diffie-Hellman Sperre)
- Die Eingabe `In` zur KDF ist hier konstant
- Auch hier ist Widerstandsfähigkeit und Rückwärtssicherheit, nicht aber Einbruchssicherheit gegeben!

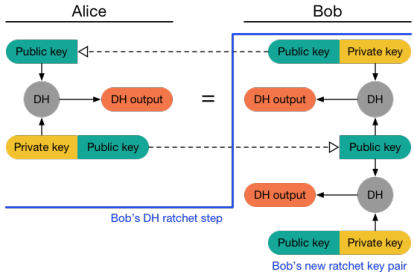


Quelle: Trevor Perrin und Moxie Marlinspike. “The double ratchet algorithm”. In: GitHub wiki (2016). URL: `https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf`

Das Signal Protokoll
Diffie-Hellman Sperre

OTH Amberg-Weiden

- Update der Kettenschlüssel (engl. chain-keys) durch wiederholten Diffie-Hellman Schlüsselaustausch
- Wechselseitiges Update des gemeinsamen Geheimnisses

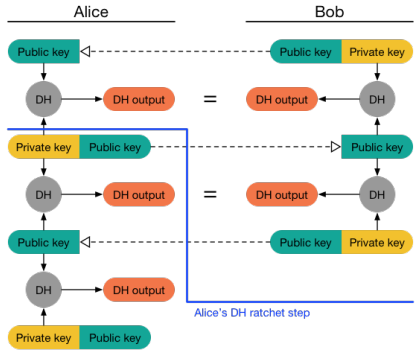


Quelle: Trevor Perrin und Moxie Marlinspike. “The double ratchet algorithm”. In: GitHub wiki (2016). URL: https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf

Das Signal Protokoll
Diffie-Hellman Sperre

OTH Amberg-Weiden

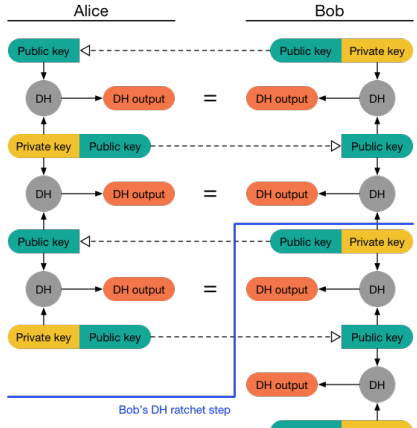
- Update der Kettenschlüssel (engl. chain-keys) durch wiederholten Diffie-Hellman Schlüsselaustausch
- Wechselseitiges Update des gemeinsamen Geheimnisses



Quelle: Trevor Perrin und Moxie Marlinspike. “The double ratchet algorithm”. In: GitHub wiki (2016). URL: https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf

Das Signal Protokoll
Diffie-Hellman Sperre

- Update der Kettenschlüssel (engl. chain-keys) durch wiederholten Diffie-Hellman Schlüsselaustausch
- Wechselseitiges Update des gemeinsamen Geheimnisses

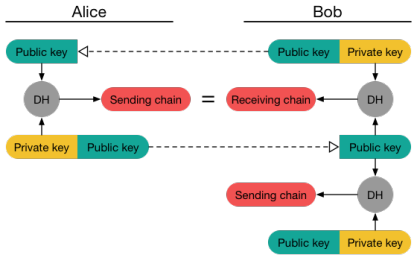


Quelle: Trevor Perrin und Moxie Marlinspike. "The double ratchet algorithm". In: GitHub wiki (2016). URL: https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf

Das Signal Protokoll
Diffie-Hellman Sperre

OTH Amberg-Weiden

- Update der Kettenschlüssel (engl. chain-keys) durch wiederholten Diffie-Hellman Schlüsselaustausch
- Wechselseitiges Update des gemeinsamen Geheimnisses
- Nutzung der Diffie-Hellman Geheimnisse für die Sende- bzw. Empfangs-Kette als Chain-Key `Key`
- Dabei wird die Sende- und Empfangskette jeweils passend zugeordnet

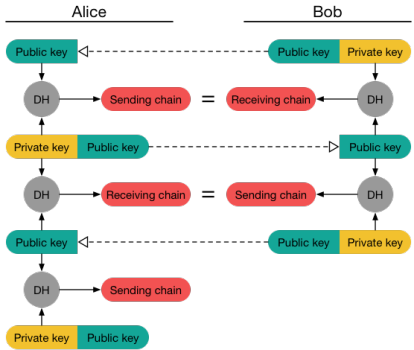


Quelle: Trevor Perrin und Moxie Marlinspike. “The double ratchet algorithm”. In: GitHub wiki (2016). URL: `https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf`

Das Signal Protokoll
Diffie-Hellman Sperre

OTH Amberg-Weiden

- Update der Kettenschlüssel (engl. chain-keys) durch wiederholten Diffie-Hellman Schlüsselaustausch
- Wechselseitiges Update des gemeinsamen Geheimnisses
- Nutzung der Diffie-Hellman Geheimnisse für die Sende- bzw. Empfangs-Kette als Chain-Key `Key`
- Dabei wird die Sende- und Empfangskette jeweils passend zugeordnet



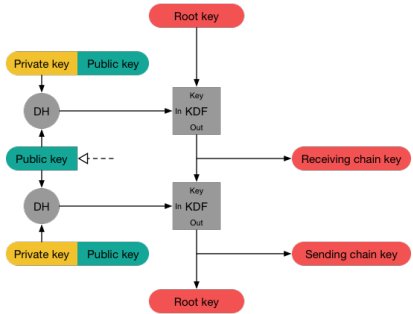
Quelle: Trevor Perrin und Moxie Marlinspike. “The double ratchet algorithm”. In: GitHub wiki (2016). URL: `https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf`

Das Signal Protokoll

Diffie-Hellman Sperre finale Konstruktion

OTH Amberg-Weiden

- Die vorherige Darstellung war leicht vereinfacht
- Korrekt ist die Ableitung der Sende- bzw. Empfangskettenschlüssel durch Schlüsselableitungsfunktion
- Der Root-Key wird dabei vorher mittels einem authentisierten Diffie-Hellman Schlüsselaustausch vereinbart.

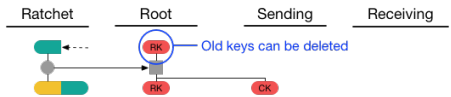


Quelle: Trevor Perrin und Moxie Marlinspike. “The double ratchet algorithm”. In: GitHub wiki (2016). URL: https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf

Das Signal Protokoll
Doppelte Sperre

OTH Amberg-Weiden

- Kombination aus symmetrischer und Diffie-Hellman Sperre
- Initialschlüssel werden (wie oben) mit einem authentisierten Diffie-Hellman Schlüsselaustausch vereinbart.

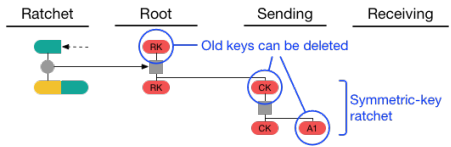


Quelle: Trevor Perrin und Moxie Marlinspike. “The double ratchet algorithm”. In: GitHub wiki (2016). URL: https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf

Das Signal Protokoll
Doppelte Sperre

OTH Amberg-Weiden

- Kombination aus symmetrischer und Diffie-Hellman Sperre
- Initialschlüssel werden (wie oben) mit einem authentisierten Diffie-Hellman Schlüsselaustausch vereinbart.

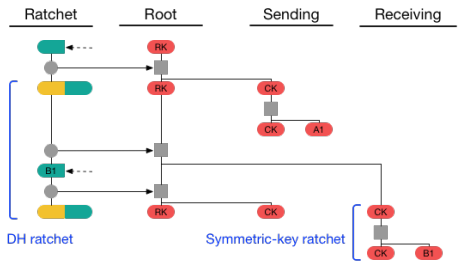


Quelle: Trevor Perrin und Moxie Marlinspike. “The double ratchet algorithm”. In: GitHub wiki (2016). URL: https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf

Das Signal Protokoll
Doppelte Sperre

OTH Amberg-Weiden

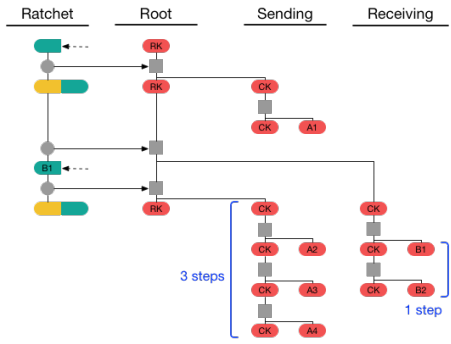
- Kombination aus symmetrischer und Diffie-Hellman Sperre
- Initialschlüssel werden (wie oben) mit einem authentisierten Diffie-Hellman Schlüsselaustausch vereinbart.
- Wird ein neuer Sperrenschlüssel empfangen, so wird vor der Ausführung der symmetrischen Sperre eine Diffe-Hellman Sperre ausgeführt, um die Kettenschlüssel zu erneuern



Quelle: Trevor Perrin und Moxie Marlinspike. “The double ratchet algorithm”. In: GitHub wiki (2016). URL: https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf

Das Signal Protokoll
Doppelte Sperre

- Kombination aus symmetrischer und Diffie-Hellman Sperre
- Initialschlüssel werden (wie oben) mit einem authentisierten Diffie-Hellman Schlüsselaustausch vereinbart.
- Wird ein neuer Sperrenschlüssel empfangen, so wird vor der Ausführung der symmetrischen Sperre eine Diffe-Hellman Sperre ausgeführt, um die Kettenschlüssel zu erneuern
- Wird eine Nachricht verschickt (oder empfangen), schaltet die symmetrische Sperre



Quelle: Trevor Perrin und Moxie Marlinspike. “The double ratchet algorithm”. In: GitHub wiki (2016). URL: https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf

Übungsaufgaben

OTH Amberg-Weiden

3.6.1. Um die initialen Schlüssel der Signal Schlüsselarchitektur aus der Vorlesung zu vereinbaren, wird ein sog. X3DH-Schlüsselaustausch durchgeführt. Die Spezifikation finden Sie hier:

`https://signal.org/docs/specifications/x3dh/`

(a) Erläutern Sie, welche Ausgaben das X3DH Protokoll produziert.
(b) Wo werden diese in der Schlüsselarchitektur aus der Vorlesung eingesetzt?
(c) Wie wird die Authentisierung sichergestellt?
(d) Welche weiteren Sicherheitseigenschaften realisiert das Protokoll?
(e) Beschreiben Sie eine weitere Sicherheitseigenschaft im Detail.

Übungsaufgaben

OTH Amberg-Weiden

Ein weiterer kryptographisch sicherer Instant-Messager ist Threema. Ein Whitepaper zur eingesetzten Kryptographie findet sich unter

`https://threema.ch/press-files/2_documentation/cryptography_whitepaper.pdf`

3.7.1. Wie authentisieren sich Gesprächspartner bei Threema?

3.7.2. Welche Vertrauensstufen gibt es?

3.7.3. Wie werden Daten gegenseitig sicher ausgetauscht? Beschreiben Sie sowohl die Verschlüsselung wie auch den Integritätsschutz der Nachrichten.

3.7.4. Wie wird bei Threema Gruppenkommunikation abgesichert?

3.7.5. Laut Dokumentation realisiert Threema perfekte Vorwärtssicherheit. Wie wird diese gewährleistet?

Gibt es Fragen?