Man-In-The-Middle (MITM) Angriffe

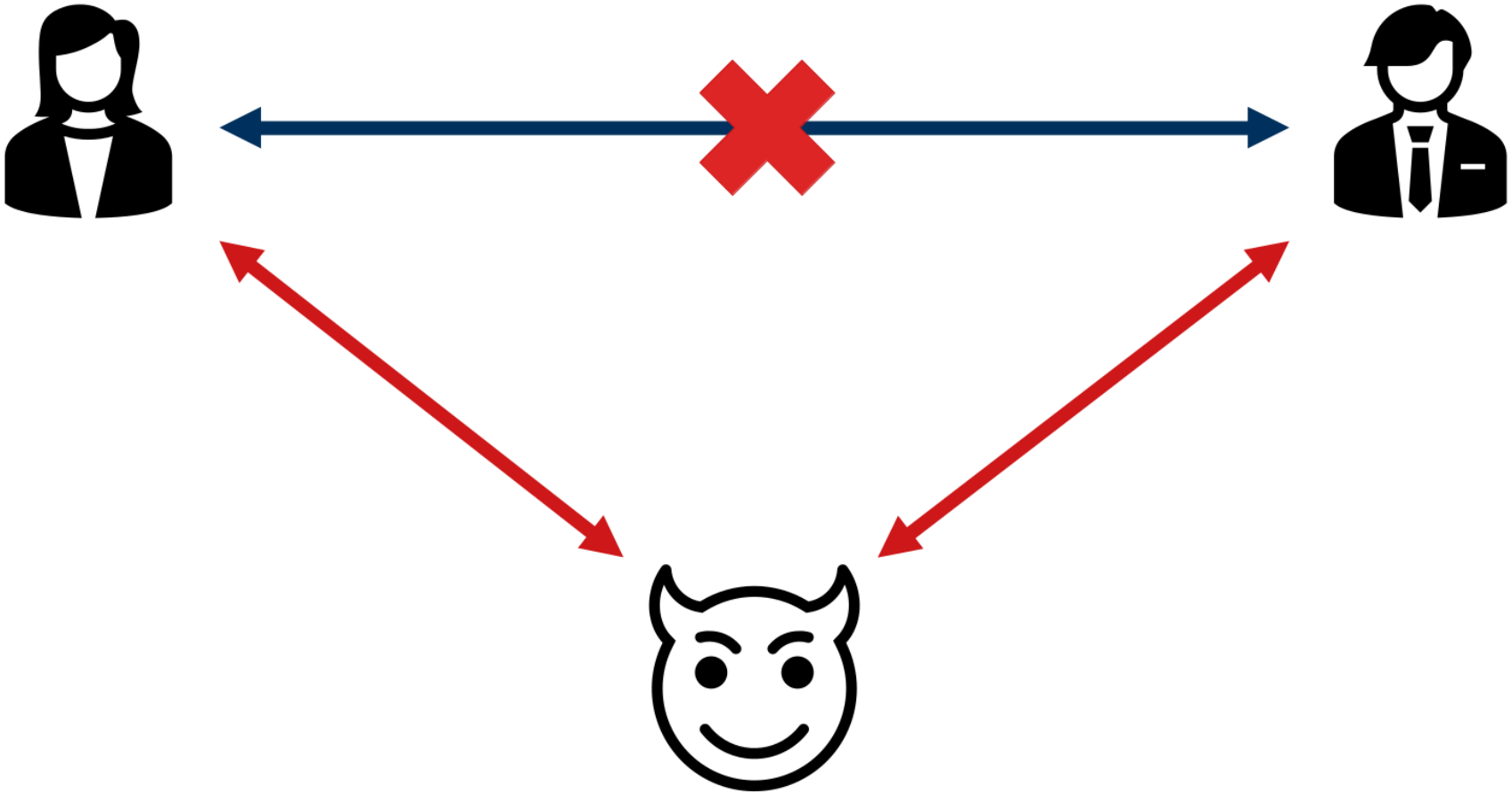
Systemsicherheitslabor

Sebastian Rehms & Franz Glöckner

TU Dresden

June 24, 2024

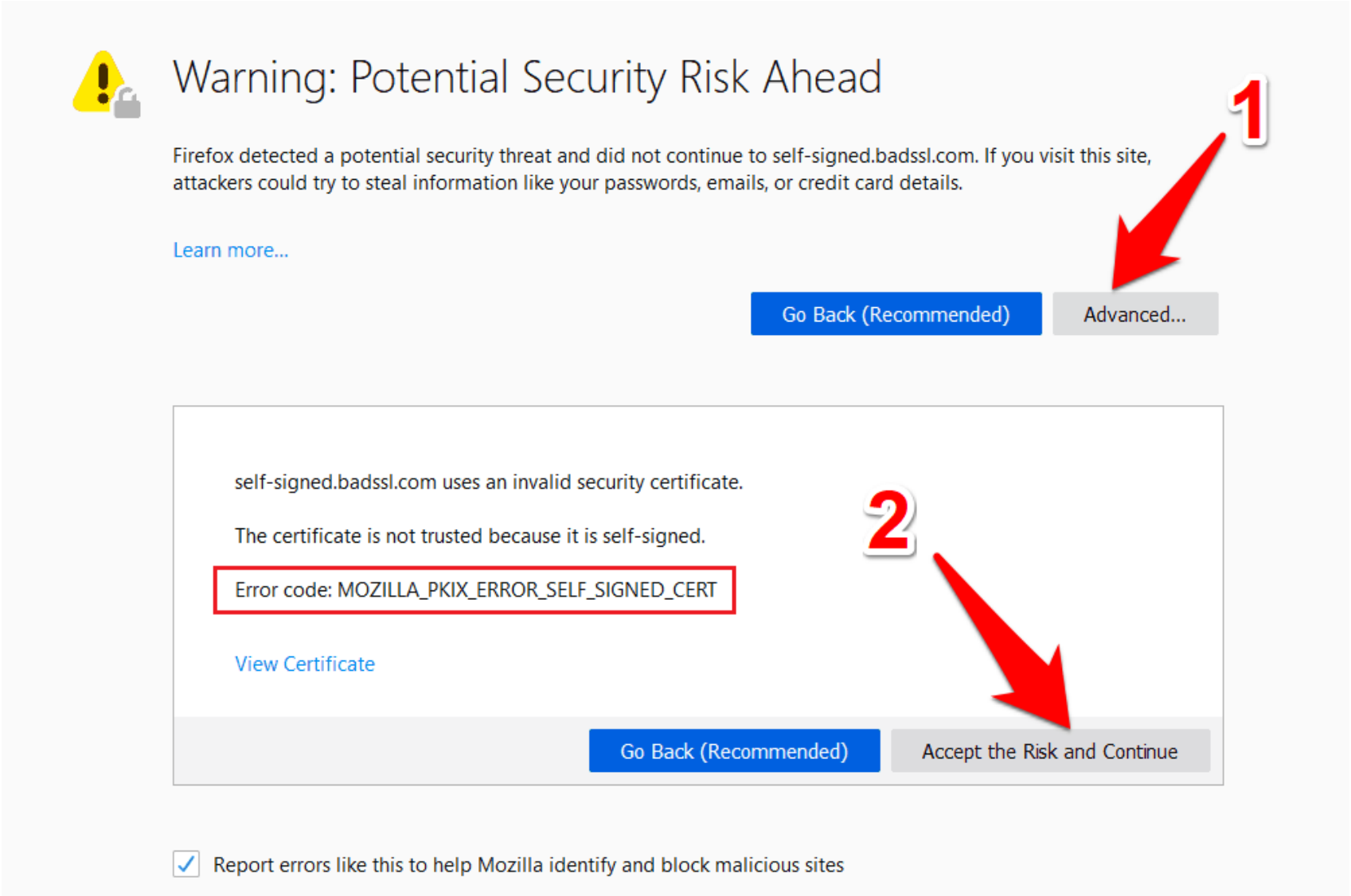
Man-In-The-Middle?



Bedrohungen

Unbemerktes Abfangen und Modifizieren

Risiken


Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to self-signed.badssl.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
Learn more...
Go Back (Recommended)
Advanced...
1
self-signed.badssl.com uses an invalid security certificate.
The certificate is not trusted because it is self-signed.
Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT
View Certificate
2
Go Back (Recommended)
Accept the Risk and Continue
Report errors like this to help Mozilla identify and block malicious sites

Risiken

(Unbemerktes) Abfangen und Modifizieren

Risiken

(Unbemerktes) Abfangen und Modifizieren
Bedrohungsspektrum:

- Vertraulichkeit
- Integrität
  - Inhalt
  - Authentizität / Identitätsfälschung
  - Vollständigkeit
  - ...
- Verfügbarkeit
  - DOS
  - QoS

Warum MITM Angriffe?

Vorbedingung für viele Ansätze

Warum MITM Angriffe?

Vorbedingung für viele Ansätze

- Zugriff auf *(potentiell verschlüsselte)* Daten
  $\Rightarrow$ Ausspähen von sensiblen Informationen
- Manipulation der Kommunikation
- Schwachstellen in Netzwerken und Protokollen
- ...

Umgebungen und Vektoren

Einsatzbereiche:

- Netze (z.B.Lokal, "Inter-Net")

Umgebungen und Vektoren

Einsatzbereiche:

- Netze (z.B.Lokal, "Inter-Net")
  - Physical
  - Data Link
  - Network/Transport
  - Session – Application

Umgebungen und Vektoren

Einsatzbereiche:

- Netze (z.B.Lokal, "Inter-Net")
  - Physical
  - Data Link
  - Network/Transport
  - Session – Application
- Other Information Flow (e.g. DLL)

Umgebungen und Vektoren

Einsatzbereiche:

- Netze (z.B.Lokal, "Inter-Net")
  - Physical
  - Data Link
  - Network/Transport
  - Session – Application
- Other Information Flow (e.g. DLL)

Zwei Aspekte von Angriffen:

1. Rerouting
2. Lauschen/Modifizieren

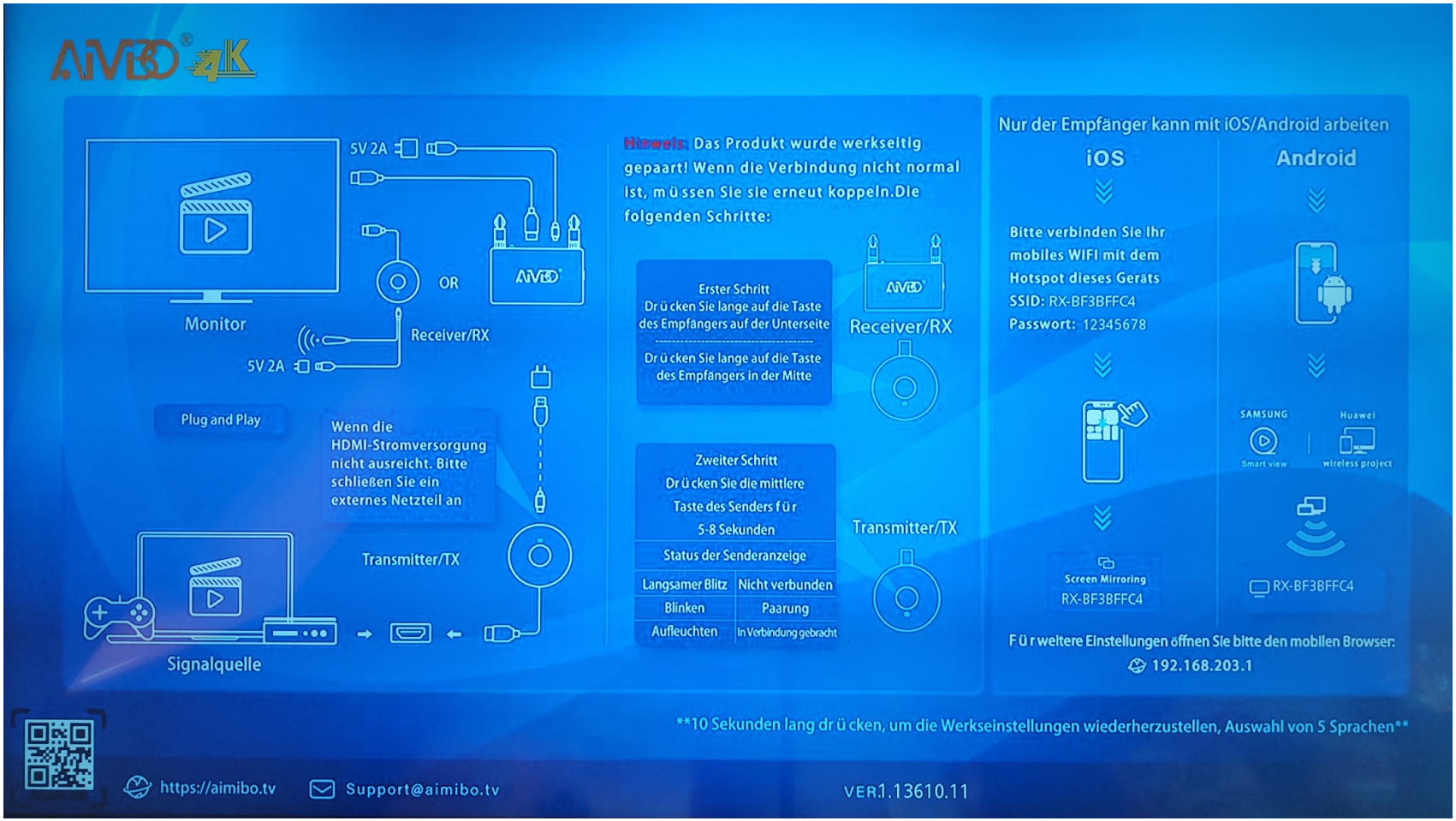
MITM-Angriffsvektoren

- **ARP-Spoofing:** Umleitung des Netzwerkverkehrs durch manipulierte MAC-IP-Zuordnungen.
- **IP-Spoofing:** Tarnung der Identität durch gefälschte IP-Adressen, um Sicherheitsfilter zu umgehen.
- **DNS-Spoofing:** Umlenkung von Benutzern auf gefälschte Websites durch manipulierte DNS-Antworten.
- **SSL-Stripping:** Erzwingung einer Verbindung von HTTPS zu HTTP zur Umgehung der Verschlüsselung.
- **Session Hijacking:** Übernahme von Benutzersitzungen durch Interzeption von Session-Tokens.

Beispiel: Wireless HDMI

Beispiel

Beispiel


AIMIBO 4K
5V 2A
OR
Monitor
Receiver/RX
5V 2A
Plug and Play
Wenn die HDMI-Stromversorgung nicht ausreicht. Bitte schließen Sie ein externes Netzteil an
Transmitter/TX
Signalquelle
Hinweis: Das Produkt wurde werkseitig gepaart! Wenn die Verbindung nicht normal ist, müssen Sie sie erneut koppeln.Die folgenden Schritte:
Erster Schritt
Drücken Sie lange auf die Taste des Empfängers auf der Unterseite
Drücken Sie lange auf die Taste des Empfängers in der Mitte
Receiver/RX
Zweiter Schritt
Drücken Sie die mittlere Taste des Senders für 5-8 Sekunden
Status der Senderanzeige
Langsamer Blitz | Nicht verbunden
Blinken | Paarung
Aufleuchten | In Verbindung gebracht
Transmitter/TX
Nur der Empfänger kann mit iOS/Android arbeiten
iOS
Android
Bitte verbinden Sie Ihr mobiles WIFI mit dem Hotspot dieses Geräts
SSID: RX-BF3BFFC4
Passwort: 12345678
Screen Mirroring
RX-BF3BFFC4
SAMSUNG
Smart view
Huawei
wireless project
RX-BF3BFFC4
Für weitere Einstellungen öffnen Sie bitte den mobilen Browser:
192.168.203.1
10 Sekunden lang drücken, um die Werkseinstellungen wiederherzustellen, Auswahl von 5 Sprachen
https://aimibo.tv
Support@aimibo.tv
VER1.13610.11

Beispiel


vurde werkseitig
bindung nicht normal
eut koppeln.Die
Receiver/RX
Nur der Empfänger kann mit iOS/Andr
iOS
Bitte verbinden Sie Ihr
mobiles WIFI mit dem
Hotspot dieses Geräts
SSID: RX-BF3BFFC4
Passwort: 12345678

Beispiel

Gegenmaßnahmen

- Verschlüsselung
- Authentifizierung
- Sonstige Integritätsmechanismen (z.B. Certificate Pinning, Content Security Policies, ...)
- Netzwerk/Tabellen-Monitoring

Gegenmaßnahmen

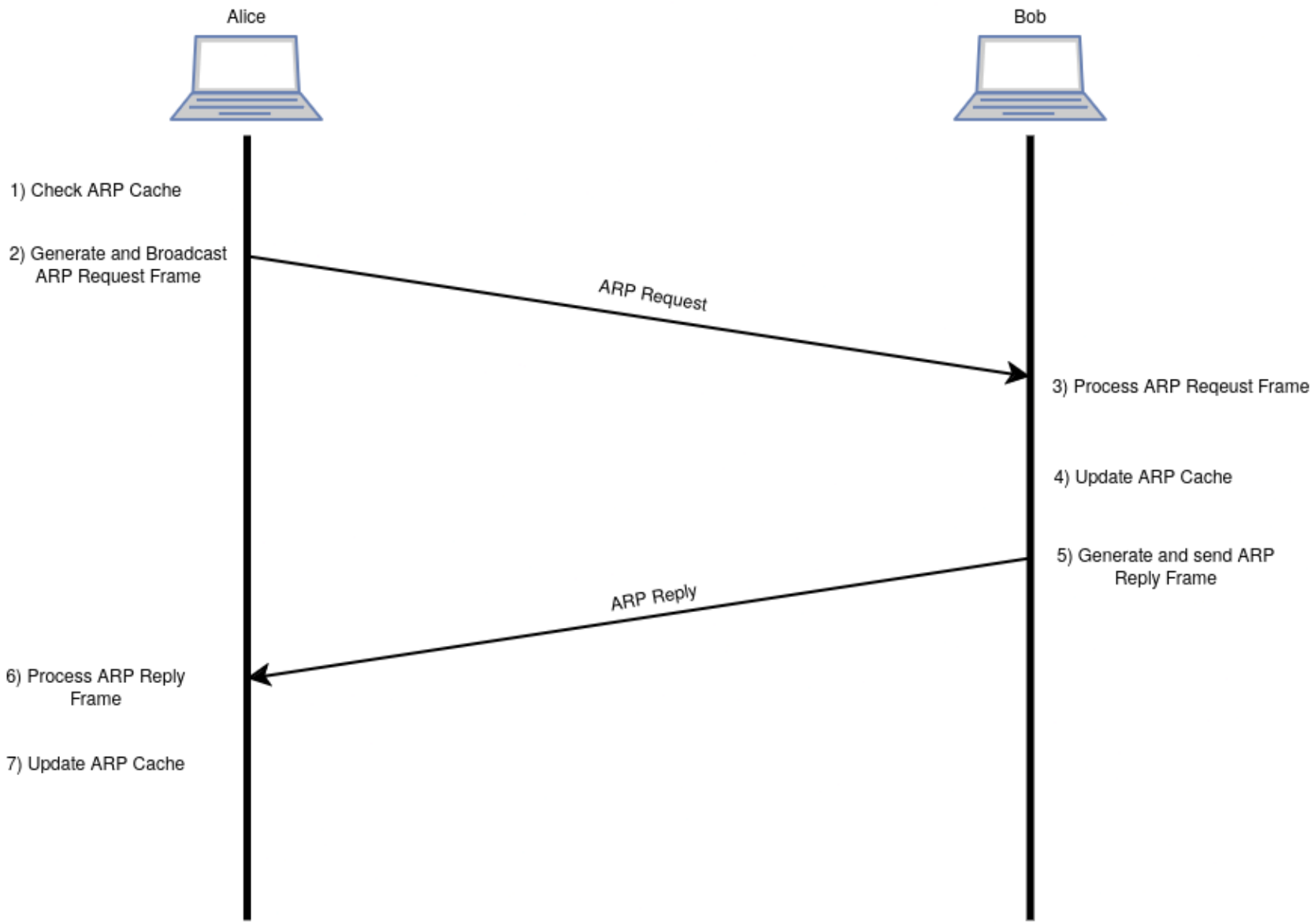
- Verschlüsselung
- Authentifizierung
- Sonstige Integritätsmechanismen (z.B. Certificate Pinning, Content Security Policies, ...)
- Netzwerk/Tabellen-Monitoring

Flexibilität vs statische Definitionen

Überblick: ARP-Protokoll

- **Zweck**: ARP (Address Resolution Protocol) verbindet IP-Adressen mit physischen MAC-Adressen in einem lokalen Netzwerk.
- **Funktionsweise**:
  - Sendet eine Broadcast-Anfrage, um die MAC-Adresse zu einer bekannten IP-Adresse zu ermitteln.
  - Das Gerät mit der entsprechenden IP-Adresse antwortet mit seiner MAC-Adresse.
- **Unsicherheit**: ARP besitzt keine Authentifizierungsmechanismen, was es anfällig für Spoofing-Angriffe macht.
- **Netzwerkbereich**: Typischerweise in lokalen Netzwerken (LANs) verwendet.

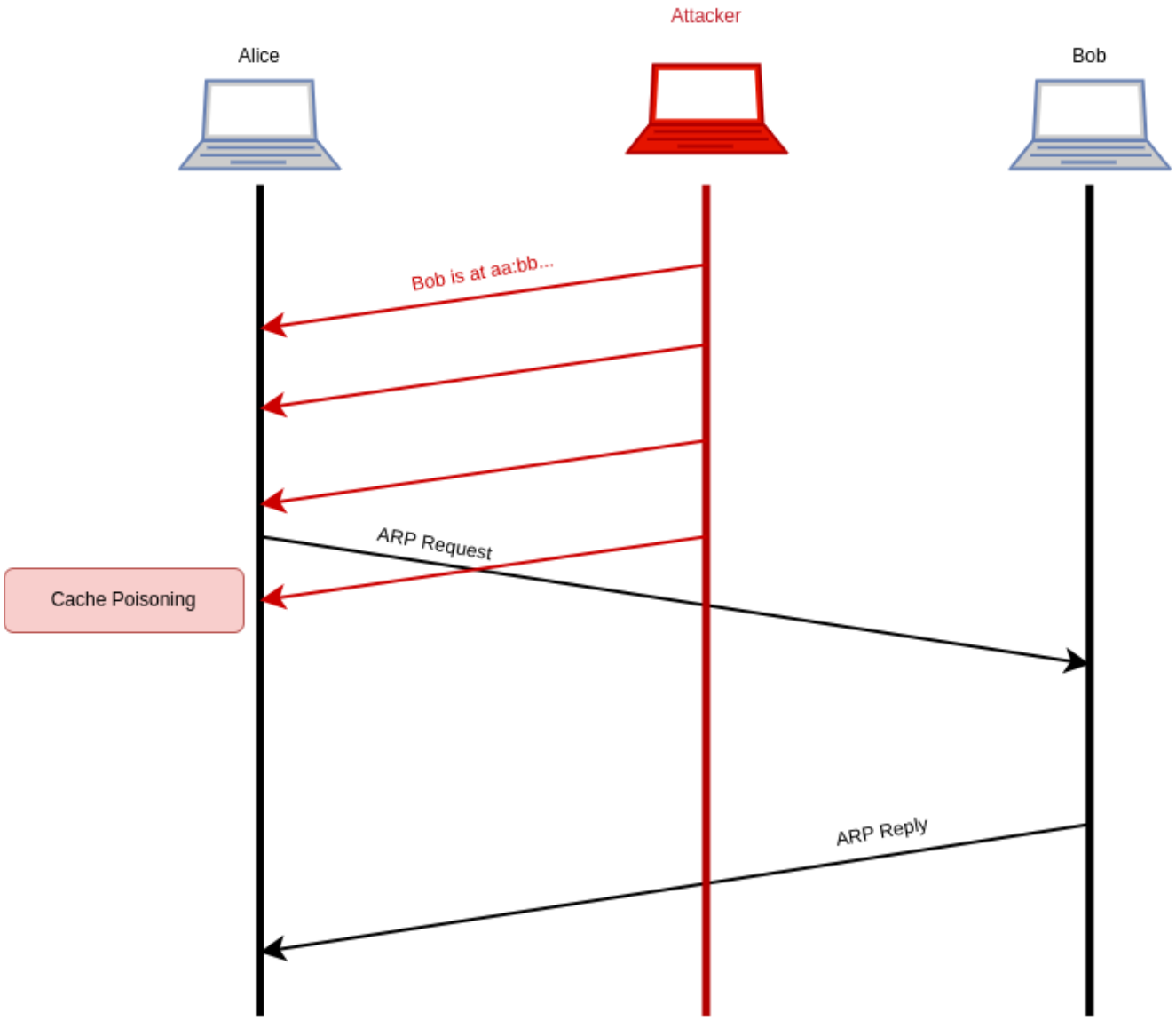
ARP Protokoll: Technische Details



ARP-Spoofing/Poisoning

- **Angriffsmechanismus**: Initiierung betrügerischer ARP-Antworten zur Manipulation der ARP-Tabelle. Ziel ist es, die MAC-Adresse des Angreifers fälschlicherweise mit der IP-Adresse eines Zielsystems zu verknüpfen.
- **Anwendungsziele**:
  - Man-in-the-Middle (MITM): Ermöglichung des Abfangens und der Modifikation von Netzwerkverkehr zwischen zwei Systemen.
  - Denial-of-Service (DoS): Störung der Netzwerkkommunikation durch Unterbindung des regulären Datenverkehrs.
- **Technische Werkzeuge**: Einsatz spezialisierter Software wie Ettercap für ARP-Spoofing und Wireshark für das Netzwerk-Monitoring.

ARP Protokoll: Technische Details



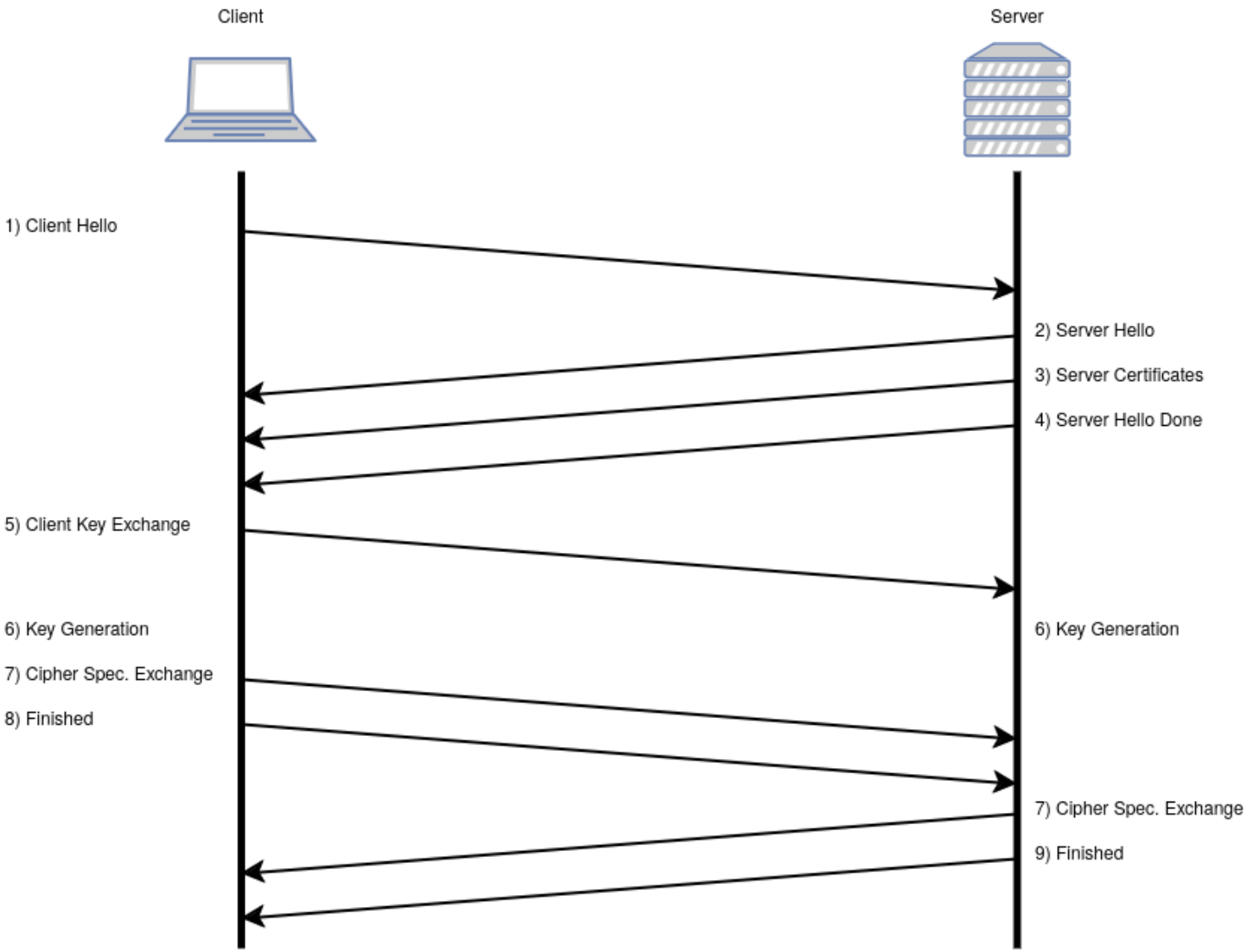
Schutzmaßnahmen gegen ARP Spoofing

- **Statische ARP-Tabellen**: Feste Zuordnung von IP- zu MAC-Adressen, um unautorisierte Änderungen zu verhindern.
- **Netzwerküberwachung**: Regelmäßige Überprüfung auf ungewöhnliche ARP-Muster und -Aktivitäten.
- **Sicherheitssoftware**: Einsatz von Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS).
- **VLANs**: Segmentierung des Netzwerks in VLANs reduziert den Umfang von ARP Spoofing-Angriffen.
- **Sicherheitsrichtlinien**: Schulung der Benutzer, um verdächtige Netzwerkaktivitäten zu erkennen und zu melden.
- **MACSec**: Integrität (+Vertraulichkeit) auf L2

SSL-Stripping: SSL/TLS Protokoll

- **Ziel**: Sicherstellung einer sicheren Kommunikation über ein unsicheres Netzwerk.
- **Verschlüsselungstechniken:**
  - Symmetrisch
  - Asymmetrisch / Schlüsselaustausch
- **Handshake-Verfahren**:
  1. Verbindungsaufbau und Spezifikation der Kryptographie-Parameter.
  2. Authentifizierung des Servers (und optional des Clients).
  3. Generierung des gemeinsamen Sitzungsschlüssels.
- **Anwendungsbeispiele:**
  - HTTPS: Sichere Web-Kommunikation.
  - E-Mail-Sicherheit: SMTPS, IMAPS, POPS.
  - Sichere Dateiübertragung: FTPS.

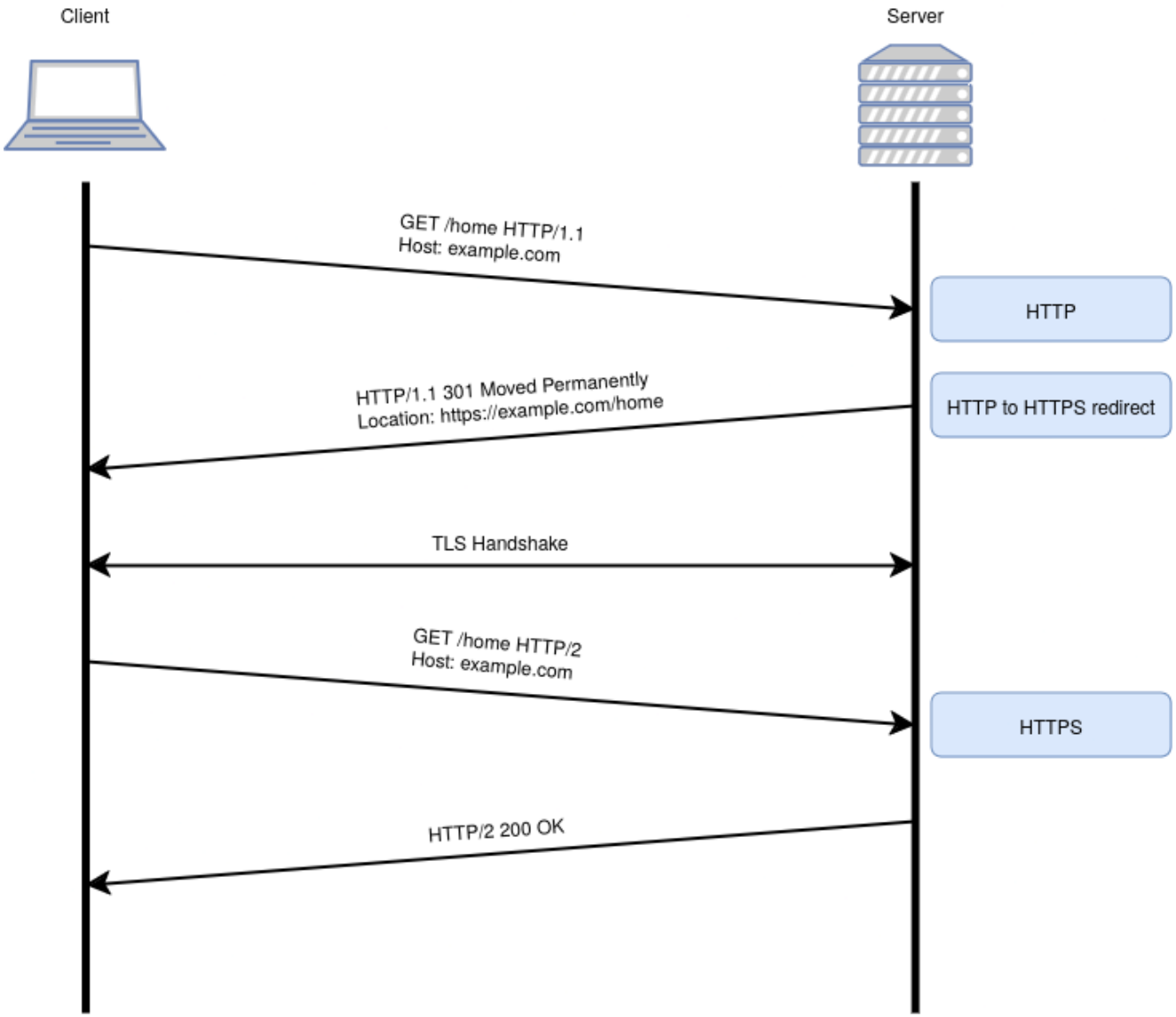
SSL-Stripping: SSL/TLS Handshake



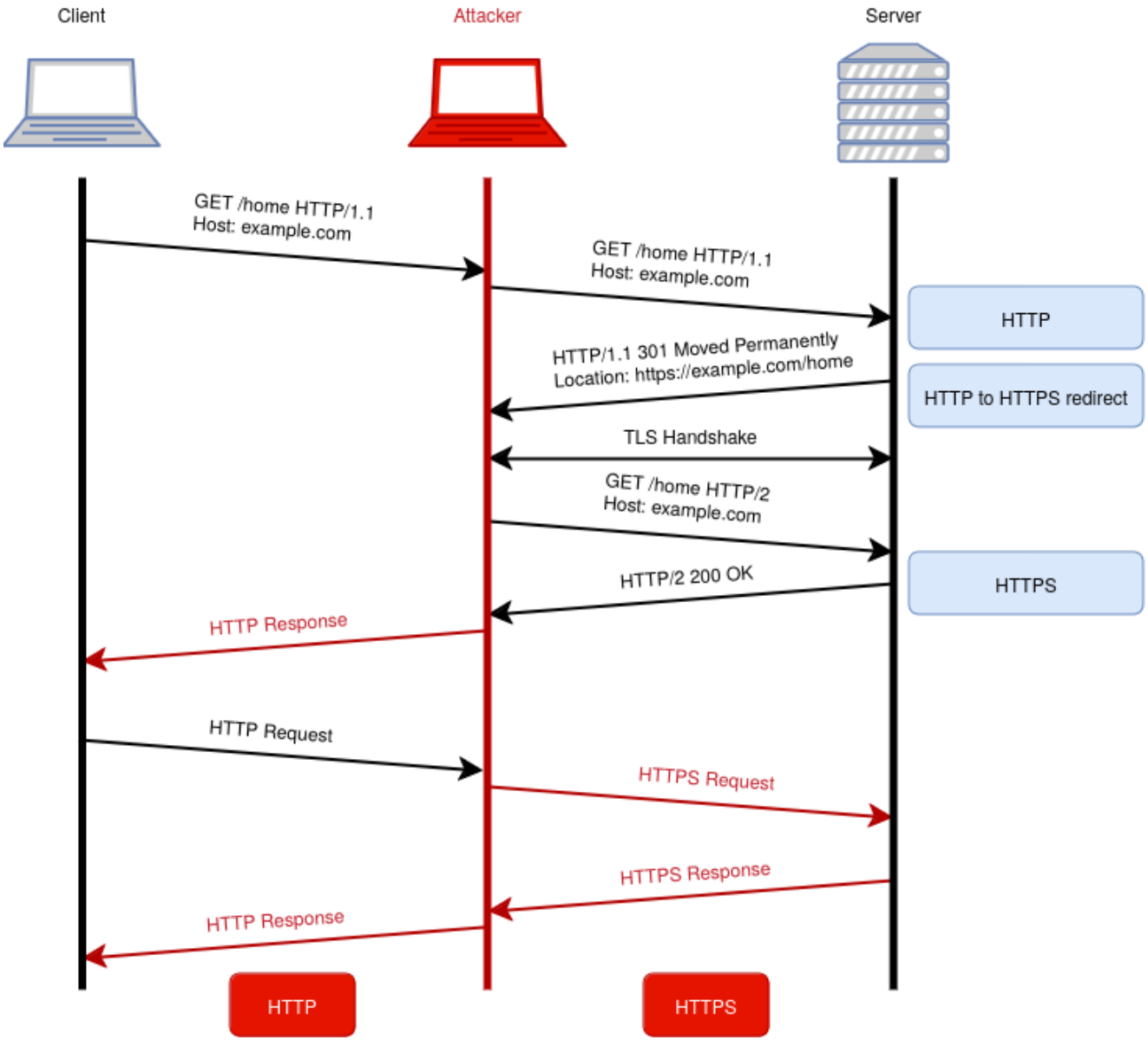
SSL-Stripping

- **Konzept**:SSL/TLS-Verschlüsselung in Webkommunikation umgehen. Ersetzen der HTTPS-Verbindungsanfragen durch unverschlüsselte HTTP-Anfragen.
- **Durchführung**:
  - Interzeption der initialen Handshake-Nachricht zwischen Client und Server.
  - Umleiten der Anfrage an den Server über eine unverschlüsselte Verbindung, während gleichzeitig eine verschlüsselte Verbindung zum Client aufrechterhalten wird.
  - Dem Client wird eine unverschlüsselte Version der Webseite präsentiert, was die Übertragung sensibler Daten über unsichere Kanäle ermöglicht $\Rightarrow$ Ersetzen der URLs, wo nötig!

SSL-Stripping: HTTP Redirect



SSL-Stripping: MITM Attack



SSL-Stripping: Schutzmaßnahmen

- **HTTPS-Enforcement:** Konsequente Durchsetzung von HTTPS, Vermeidung von Mixed Content.
- **HSTS (HTTP Strict Transport Security):** Einsatz von HSTS-Headern zur Erzwingung von HTTPS-Kommunikation. (Setzt vorherige Session voraus)
- **Sichere Cookies:** 'Secure'-Attribut für Cookies zur Übertragung nur über HTTPS. (Setzt vorherige Session voraus)
- **Mitdenken:** setzt of technisches Verständnis voraus

MITM Tools

- Ettercap
- Bettercap
- mitm-Proxy
- ...