

Man-in-the-Middle und HTTPS

Carsten Eschenhorn
Sven Nähring

Man-in-the-Middle

Der unsichtbare Dritte:

Darunter ist zu verstehen, dass die Kommunikation zwischen zwei Verbindungspartnern *transparent* für eine dritte Person ist.

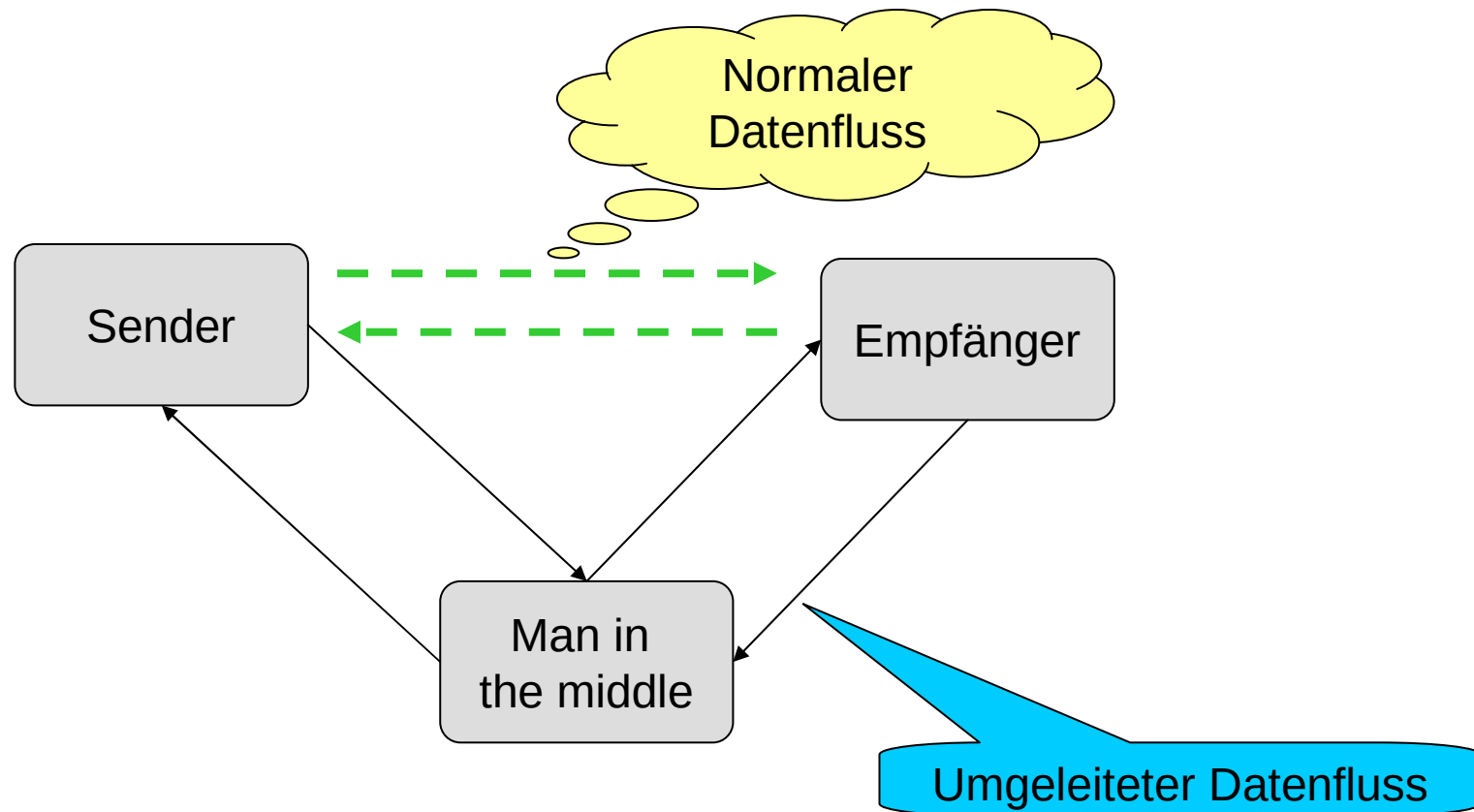
Man-in-the-Middle

- Transparent

heißt in diesem Zusammenhang, dass weder der Absender noch der Empfänger bemerken, dass sie eigentlich nicht direkt miteinander verbunden sind.

Sondern über einen dritten miteinander Kommunizieren der jegliche Datenströme abfangen kann.

Man-in-the-Middle



Man-in-the-Middle

Wo finden solche Angriffe statt

- Ein Angriff dieser Art kann in jeglichen Rechnernetzen Anwendung findet.
- Internet
- LAN
- Ethernet

Man-in-the-Middle

Was passiert bei dieser Form von Angriff

- Der Angreifer hat mit seinem System die komplette Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern
- Er kann die abgefangenen Informationen nach belieben einsehen und sogar manipulieren

Man-in-the-Middle

Wie finden solche Angriffe statt

- Der Angreifer muss im gleichen Netz eingebunden sein.
- Der Angreifer muss den Datenstrom über sein System umleiten.
- Der Angreifer muss Zugriff auf einen Verbindungsknoten haben

Man-in-the-Middle

Gegenmaßnahmen

- Sicherung durch Geheimhaltung
- Sicherung vor Manipulation
- Sicherung von kurzen Einträgen

Man-in-the-Middle

Sicherung durch Geheimhaltung

- Eine Verschlüsselung der Datenpakete ist die beste Lösung dieser Angriffsform entgegen zu wirken.

Jedoch müssen die Schlüssel vor der ersten Kommunikation auf einem sicheren Datenweg ausgetauscht werden.

Um nicht doch in falsche Hände zu gelangen.

Man-in-the-Middle

Sicherung vor Manipulation

- Eine Sicherung vor Manipulation bietet die sogenannte Integrity Protection.

In diesem Fall erhält jede übertragene Nachricht einen Identitätsstempel, den Message Authentication Code. DES(EC-Karte)

Man-in-the-Middle

Sicherung von kurzen Einträgen

- TAN
- ITAN
- TAN mit Bestätigung
- mTAN, sprich Mobile TAN
- Smart TAN Generator
- PIN Bank Generator

HTTPS

HTTPS

- Asymetrische Verschlüsselung
- Symetrischer Sitzungsschlüssel