Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Institut für Wissenschaftliche Weiterbildung (IWW)

Die 10 größten Bedrohungen für Computer-Netzwerke

ECSM

Tobias Scheible, M.Eng.

Tobias Scheible, M.Eng.

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

- 1999 GeoCities Website, 2000 eigene Domain, 2001 Kundenprojekte
- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- Seit 2012: Wissenschaftlicher Mitarbeiter
  - Aktuelle & ehemalige Lehrmodule (Auswahl):
    - Netzsicherheit I: IT-Sicherheit von Netzwerken Hochschulzertifikatsprogramm
    - Grundlagen der digitalen Forensik Masterstudiengang IT GRC Management
    - Internettechnologien Hochschulzertifikatsprogramm
    - Cloud Technologies and Cloud Security Architectures Masterstudiengang IT GRC Management
    - Digitale Forensik Bachelorstudiengang IT Security
    - Internet Grundlagen Masterstudiengang Digitale Forensik
    - Informationssicherheit Bachelorstudiengang Wirtschaftsinformatik
- Buch- & Zeitschriftenautor, Blogger, Referent, …

Die 10 größten Bedrohungen für Computer-Netzwerke

Hochschule Albstadt-Sigmaringen

- 1971 Gründung der Fachhochschule Sigmaringen
- 1988/89 Campus Albstadt
- 2004 Fachhochschule wird in Hochschule umbenannt
- 32 Bachelor- und Masterstudiengänge

Fakultät Engineering

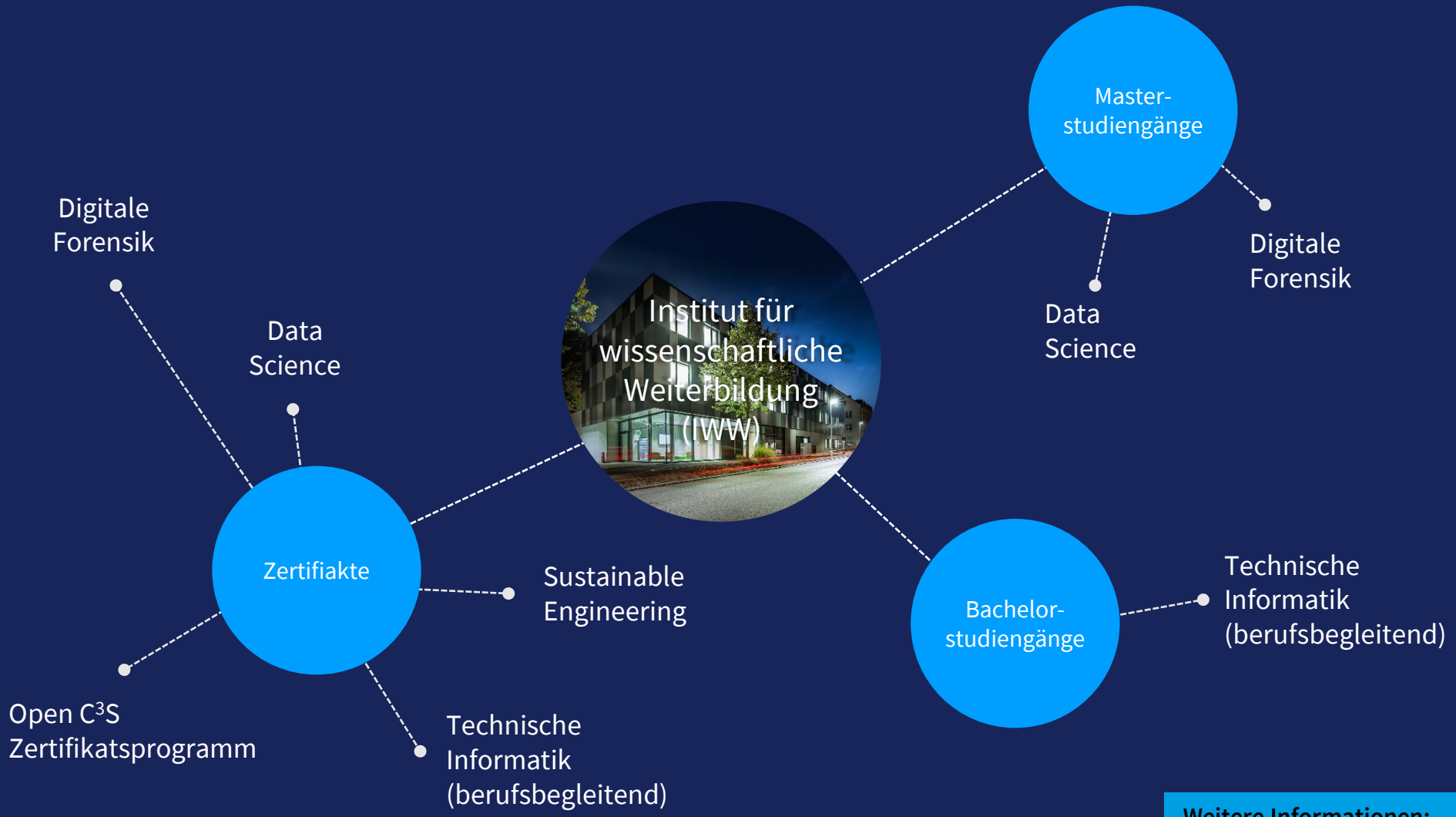
Fakultät Business Science and Management

Fakultät Life Sciences

Fakultät Informatik

Die 10 größten Bedrohungen für Computer-Netzwerke

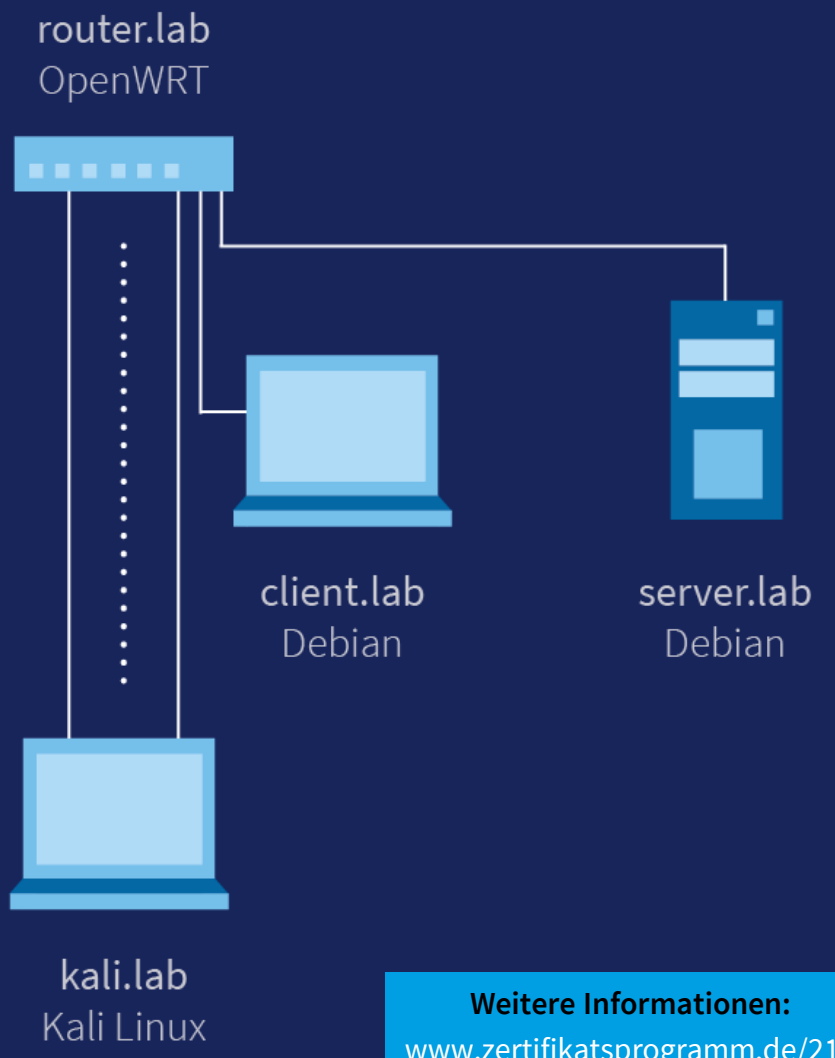
Institut für wissenschaftliche Weiterbildung



Weitere Informationen:
www.hs-albsig.de/iww

Die 10 größten Bedrohungen für Computer-Netzwerke

Netzsicherheit I: IT-Sicherheit von Netzwerken



Weitere Informationen:
www.zertifikatsprogramm.de/214

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Institut für Wissenschaftliche Weiterbildung (IWW)

Die 10 größten Bedrohungen für Computer-Netzwerke

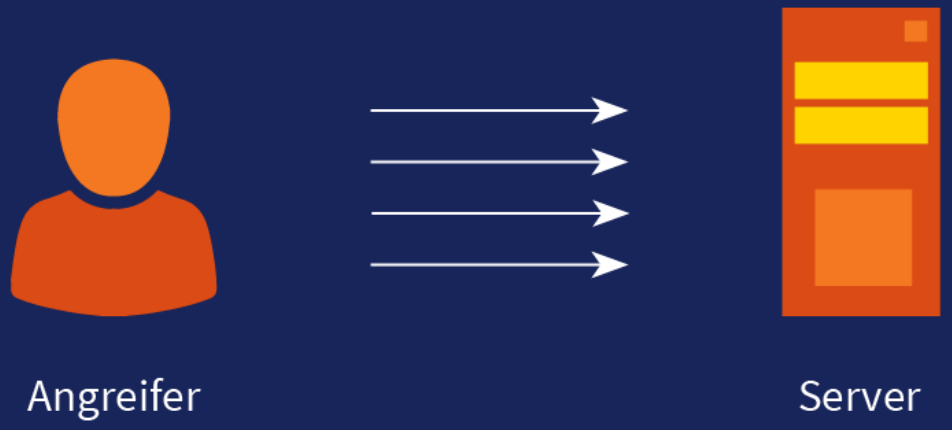
Agenda

- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Hinweis
Die komplette Präsentation wird im Anschluss unter *www.scheible.it* bereitgestellt.

10 Bedrohungen für Computer-Netzwerke

Scanning



Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

PRAXIS Scanning

Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Extrafolie

Scanning

Sobald sich ein Angreifer innerhalb eines Netzwerkes befindet, verschafft er sich als Erstes mit einem Scan einen Überblick über das Netzwerk. Dies wird auch als Recognition (dt. Erkundung oder Aufklärung) bezeichnet. Als Erstes wird eine Übersicht erstellt, welche Rechner im Netzwerksegment aktiv sind. Dann wird analysiert, welche Dienste genutzt werden. Dabei werden alle Ports auf eine Reaktion überprüft. Ist ein Port gefunden, wird versucht, herauszufinden, welche Software auf diesem Port einen Dienst bereitstellt. Wurde dies auch erfolgreich durchgeführt, wird als Nächstes versucht, die Version herauszufinden.

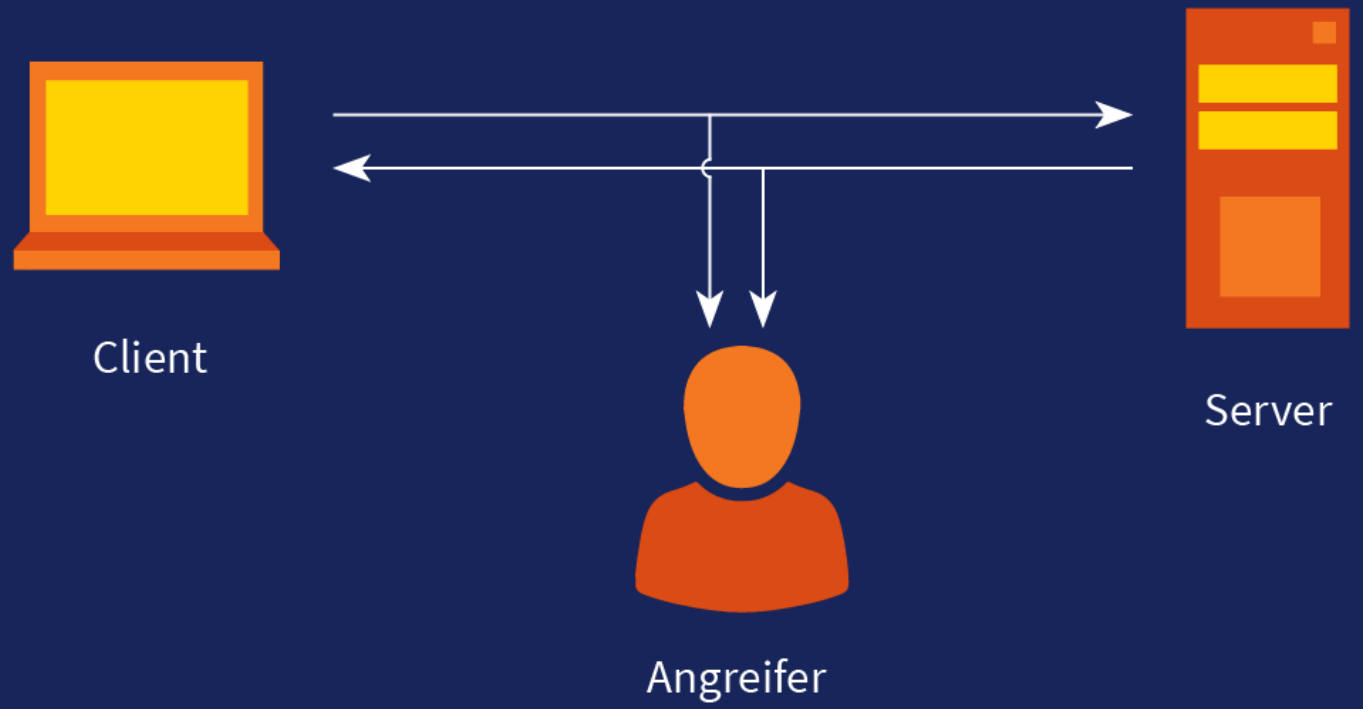
- Gegenmaßnahmen
  Nur notwendige Ports sollten nach außen geöffnet sein und Versionsnummern dürfen niemals kommuniziert werden. Aggressive Scans sollten erkannt und der Urheber geblockt werden.

Sniffing

Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Sniffing



Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

EXKURS Sniffing

Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Extrafolie

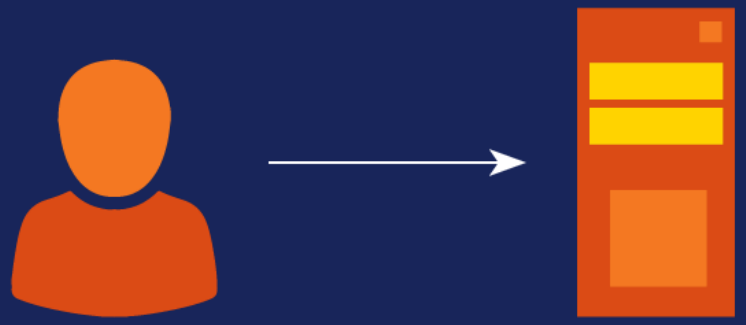
Sniffing

Sniffing (dt. schnüffeln) bezeichnet das Mitschneiden oder Mitlesen des Datenverkehrs einer Netzwerkverbindung. Dabei handelt es sich um einen passiven Angriff, da der Datenverkehr nur abgehört und nicht verändert wird. Der Zugriff auf die Kommunikation erfolgt dabei je nach Netzwerkart auf unterschiedliche Art und Weise. Zum Beispiel kann ein Notebook mit zwei Netzwerkadaptern genutzt und zwischen einer Verbindung platziert und somit ein Sniffer realisiert werden.

Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

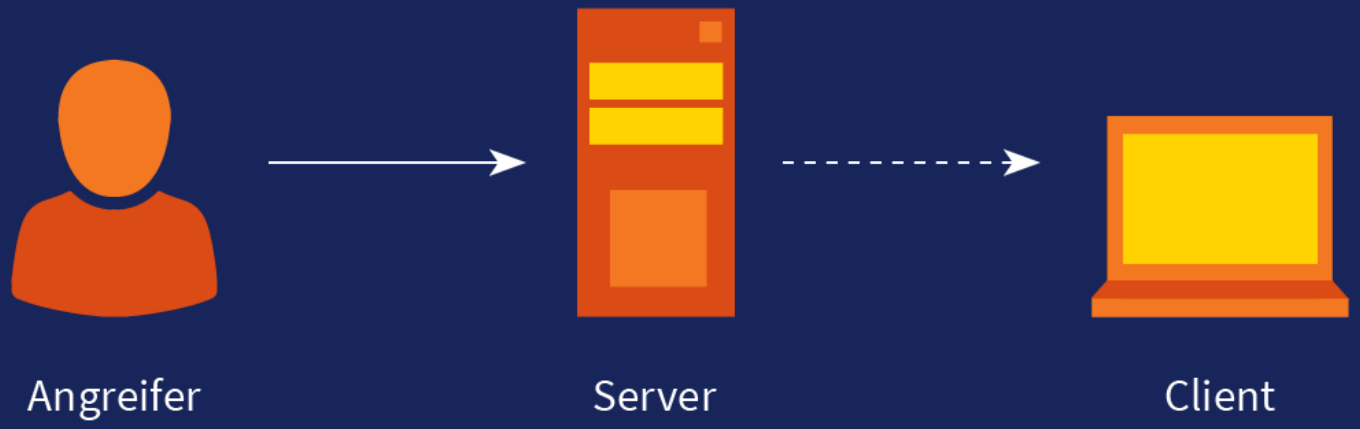
Spoofing



Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Spoofing



Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

PRAXIS Spoofing

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Institut für Wissenschaftliche Weiterbildung (IWW)

Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Extrafolie

Spoofing

Spoofing (dt. Manipulation, Verschleierung oder Vortäuschung) werden in der Informationstechnik verschiedene Täuschungsmethoden genannt, bei denen ein Angreifer entweder seine eigene Identität verschleiern möchte oder eine andere Identität vortäuscht, welcher der Empfänger vertraut. Im Bereich Netzsicherheit gehört dazu etwa ARP-Spoofing, IP-Spoofing und DNS-Spoofing.

Die 10 größten Bedrohungen für Computer-Netzwerke

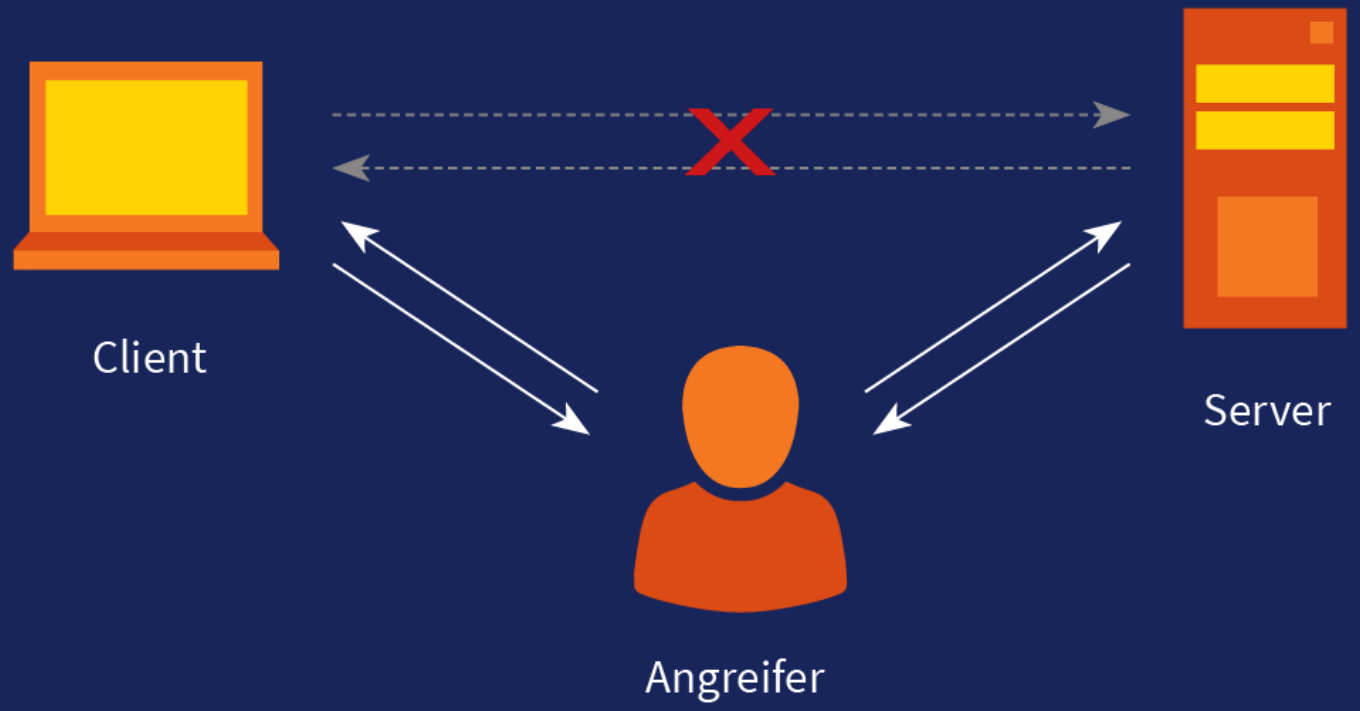
Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Man-in-the-Middle

Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Man-in-the-Middle



Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Extrafolie

Man-in-the-Middle

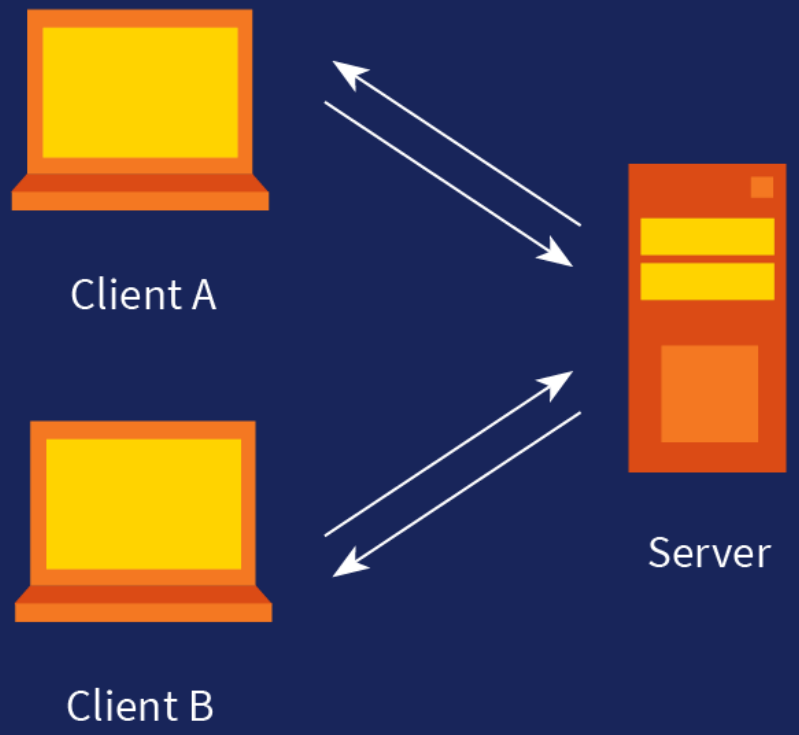
Bei einem Man-in-the-Middle-Angriff (MitM-Angriff) oder auch Person-in-the-Middle-Angriff positioniert sich ein Angreifer zwischen zwei Kommunikationspartnern. In dieser Position können Nachrichten abgehört, manipuliert, geblockt oder gefälscht werden. Es gibt verschiedene Arten, wie ein Angreifer in eine Verbindung eingreifen kann, etwa den Spoofing-Angriff. In der Netzsicherheit wird das Umleiten eines Datenstroms auch als Redirect- oder Routing-Angriff bezeichnet.

- Gegenmaßnahmen
  Um Kommunikationsverbindungen dagegen zu schützen, müssen mittels kryptografischer Funktionen sichere Verschlüsselungen realisiert werden.

Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

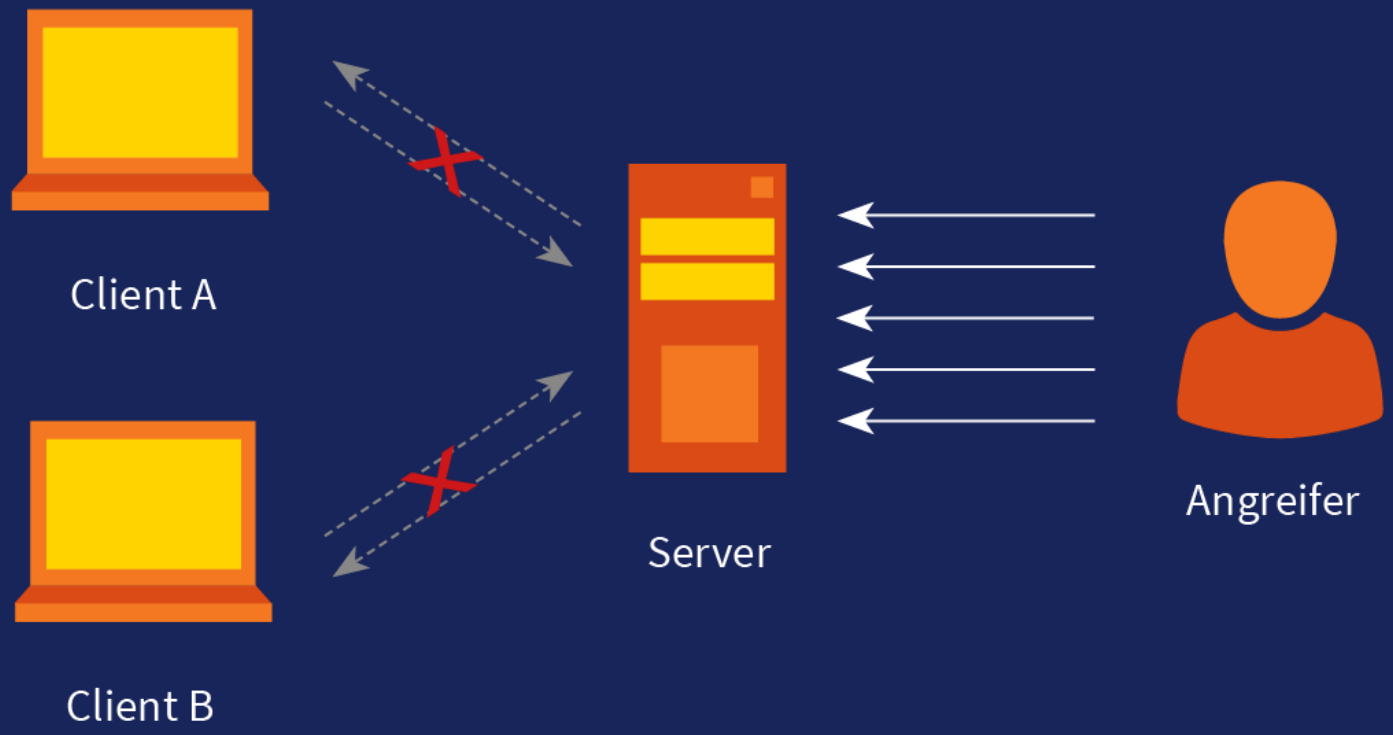
Denial-of-Service



Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Denial-of-Service



Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

PRAXIS Denial-of-Service

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Institut für Wissenschaftliche Weiterbildung (IWW)

Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Extrafolie

Denial-of-Service

Eine Denial-of-Service-Attacke (auch als DoS-Attacke abgekürzt) ist ein Angriff, der dazu führen soll, dass ein Server temporär oder in besonders extremen Fällen auch über einen längeren Zeitraum hinweg nicht mehr erreicht werden kann. DoS-Attacken sind häufig nichts weiter als Cyber-Vandalismus, die bei Unzufriedenheit mit einer Situation eingesetzt werden. Dies kommt häufig vor, da viele Tools existieren, die ohne tieferes Know-how bedient werden können. Es werden auch illegale Dienstleistungen angeboten, bei denen DoS-Angriffe eingekauft werden können.

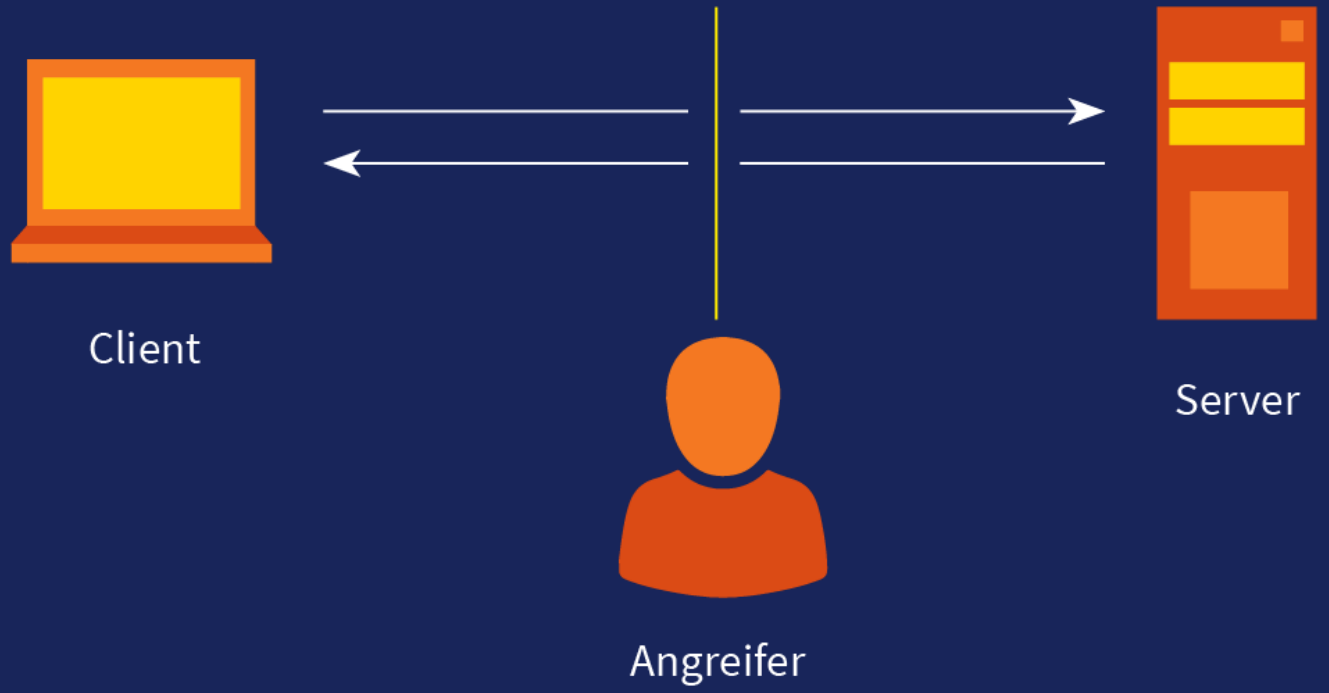
- Gegenmaßnahmen
  Systeme müssen gegen DDoS-Attacke gehärtet und präventive Maßnahmen vorab initiiert werden. Die Netzwerkinfrastruktur muss vorbereitet werden, damit Angriffe gefiltert und geblockt werden können.

Physical Attacks

Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Physical Attacks



Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Extrafolie

Physical Attacks

Physische Angriffe auf Netzwerke haben eine reine Zerstörung zum Ziel, um Verbindungen zu unterbrechen. Das reicht im einfachsten Fall vom Durchtrennen eines Kabels bzw. Lichtwellenleiters bis hin zur Manipulation mit Stromstößen. Dabei wird eine offene Netzwerkbuchse gezielt einem starken Stromimpuls ausgesetzt. Hier hat ein Angreifer das Ziel, dass mehrere angeschlossene Komponenten im Netzwerk durch Überlastung zerstört werden.

- Gegenmaßnahmen
  Daher muss auch die Netzwerkinfrastruktur mit baulichen Maßnahmen gegen Angriffe und Manipulationen geschützt werden.

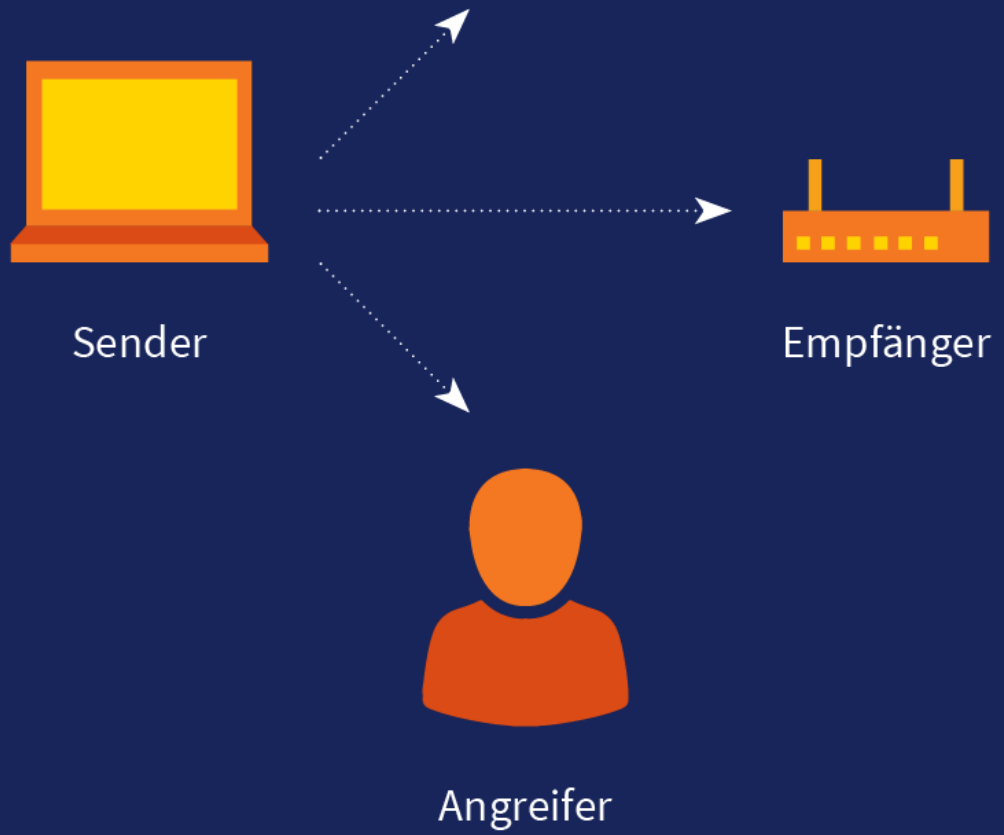
Die 10 größten Bedrohungen für Computer-Netzwerke

Replay Attack

Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

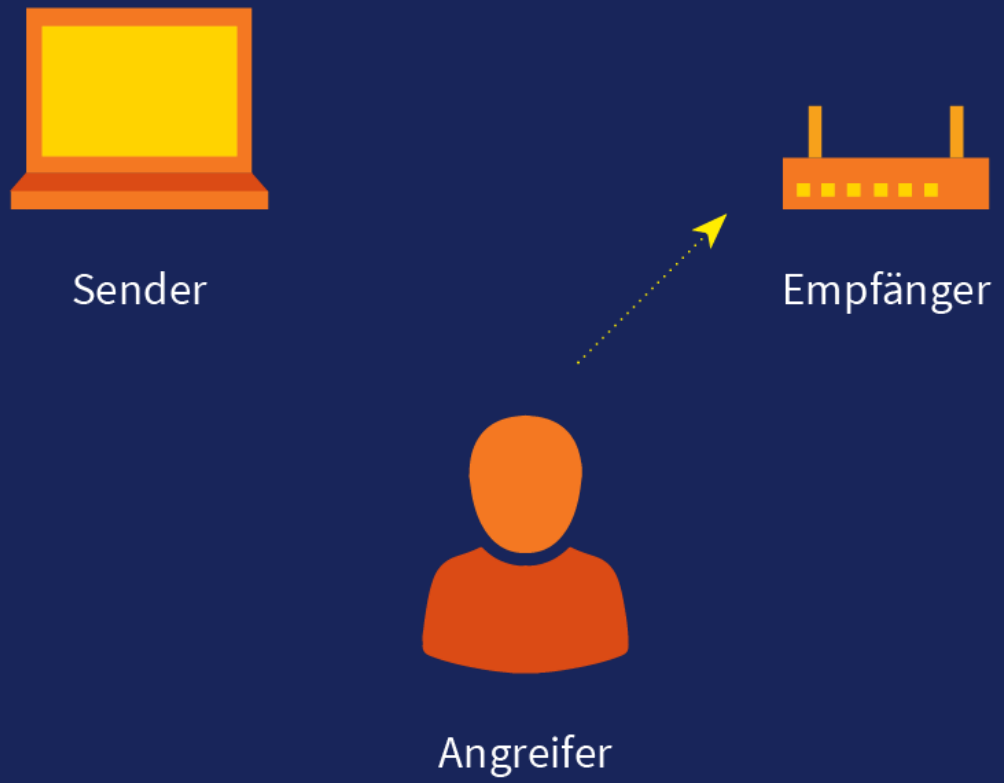
Replay Attack



Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Replay Attack



Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

EXKURS Replay Attack

Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

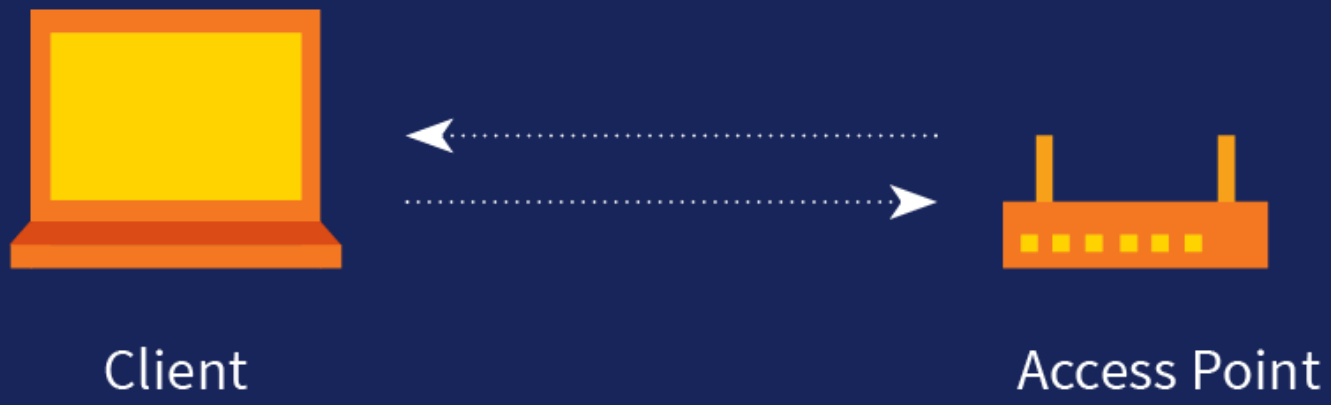
Extrafolie

Replay Attack

Bei einem Replay Attack wird ein Signal mit keiner oder nur schwacher Schutzmaßnahme aufgezeichnet und erneut gesendet. Findet hier auf der Empfängerseite keine Validierung statt, wird diese Übertragung einfach verarbeitet. Damit ist es einem Angreifer möglich, eine Übertragung mit etwa einem Befehl erneut einzuschleusen, ohne dass das eigentliche Signal dekodiert werden muss. Dies funktioniert zum Teil, auch wenn eine symmetrische Verschlüsselung mit immer dem gleichen Code verwendet wird.

- Gegenmaßnahmen
  Um diese zu verhindern, können Techniken wie eine Nonce, Sequenznummern, Message Authentication Code oder das Rolling-Code-Verfahren eingesetzt werden. Damit wird jede Übertragung so verändert, dass sie einmalig ist und erneut gesendete Übertragungen erkannt und geblockt werden können.

Jamming



Die 10 größten Bedrohungen für Computer-Netzwerke

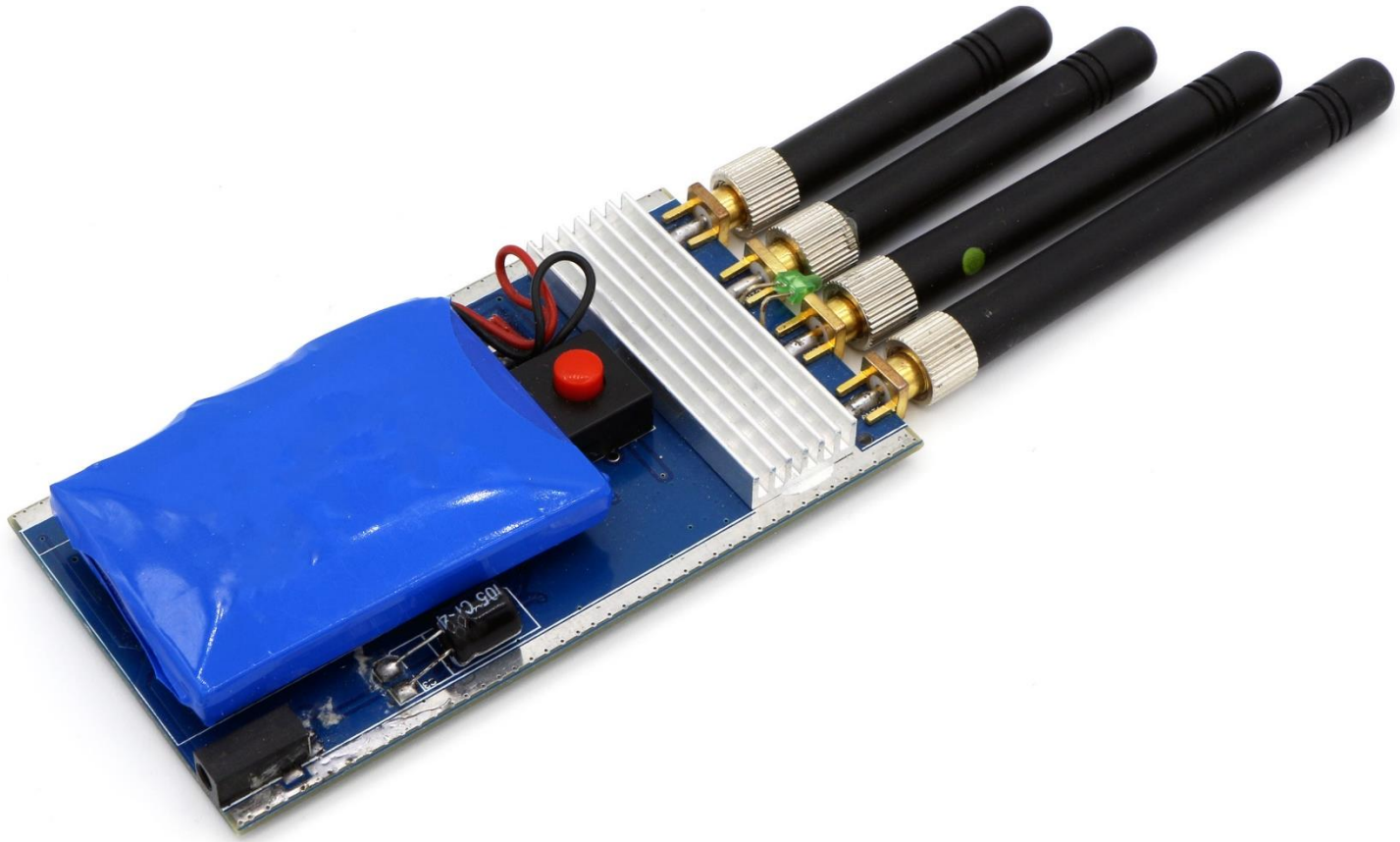
Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Jamming

Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

EXKURS Jamming



Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

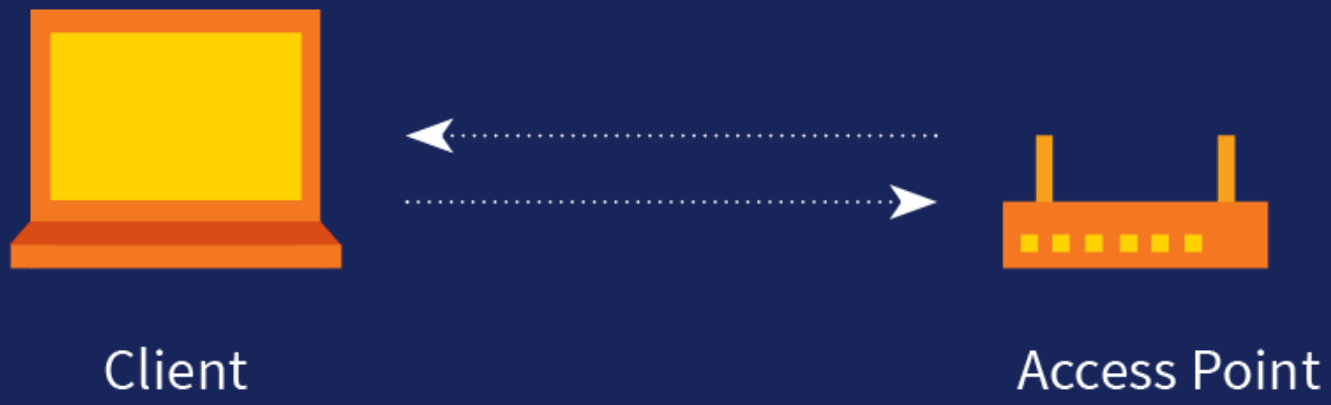
Extrafolie

Jamming

Per Jamming werden kabellose Übertragungen gestört, so dass der Empfang eines Signals nur noch schwer oder gar nicht möglich ist. Ein Störsender sendet etwa auf einer bestimmten Frequenz ein zufälliges Signal mit möglichst großer Stärke und überlagert so andere Übertragungen. Dadurch ist keine Kommunikation mehr möglich und eine WLAN-Verbindung bricht zum Beispiel zusammen. Störsender gibt es für verschiedene Funkprotokolle bzw. -frequenzen wie Bluetooth, WLAN, GSM, UMTS, LTE und GPS.

- Gegenmaßnahmen
  Gegenmaßnahmen gegen das Stören eines Signals lassen sich nur schwer umsetzen. Grundsätzlich sollte bei der Unterbrechung eines Signals ein Alarm ausgelöst und solche Vorgänge dokumentiert werden. Systeme sollten in einen definierten Status schalten, wenn keine Verbindung mehr vorhanden ist.

Deauthentication



Die 10 größten Bedrohungen für Computer-Netzwerke

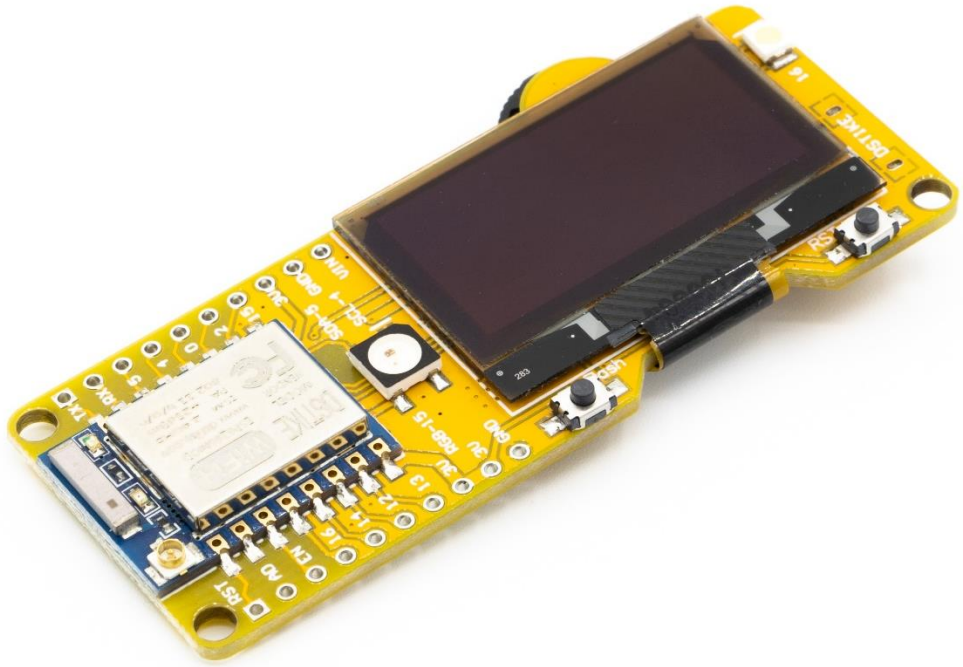
Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Deauthentication

Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

EXKURS Deauthentication



Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Extrafolie

Deauthentication

In kabellosen Netzwerken (WLAN) kann ein Angreifer einen Client vom Netzwerk abmelden. Dabei wird das Deauthentication-Signal des Access-Points (AP) imitiert und damit dem Endgerät fälschlicherweise eine Beendung der Verbindung signalisiert. Die Deauthentication-Funktion ist eigentlich dazu gedacht, dass ein Teilnehmer an einem System aus mehreren Access-Points von einer überlasteten Station abgemeldet wird und sich dann mit einem anderen Access-Point verbindet. Dieses Signal kann jedoch ohne großen Aufwand gefälscht werden – und damit kann man gezielt die WLAN-Verbindung unterbrechen. Um das Deauthentication-Signal zu senden, muss der Angreifer nicht die Zugangsdaten zum WLAN kennen, da es sich um einen Management-Frame handelt und nur die Datenübertragung verschlüsselt wird.

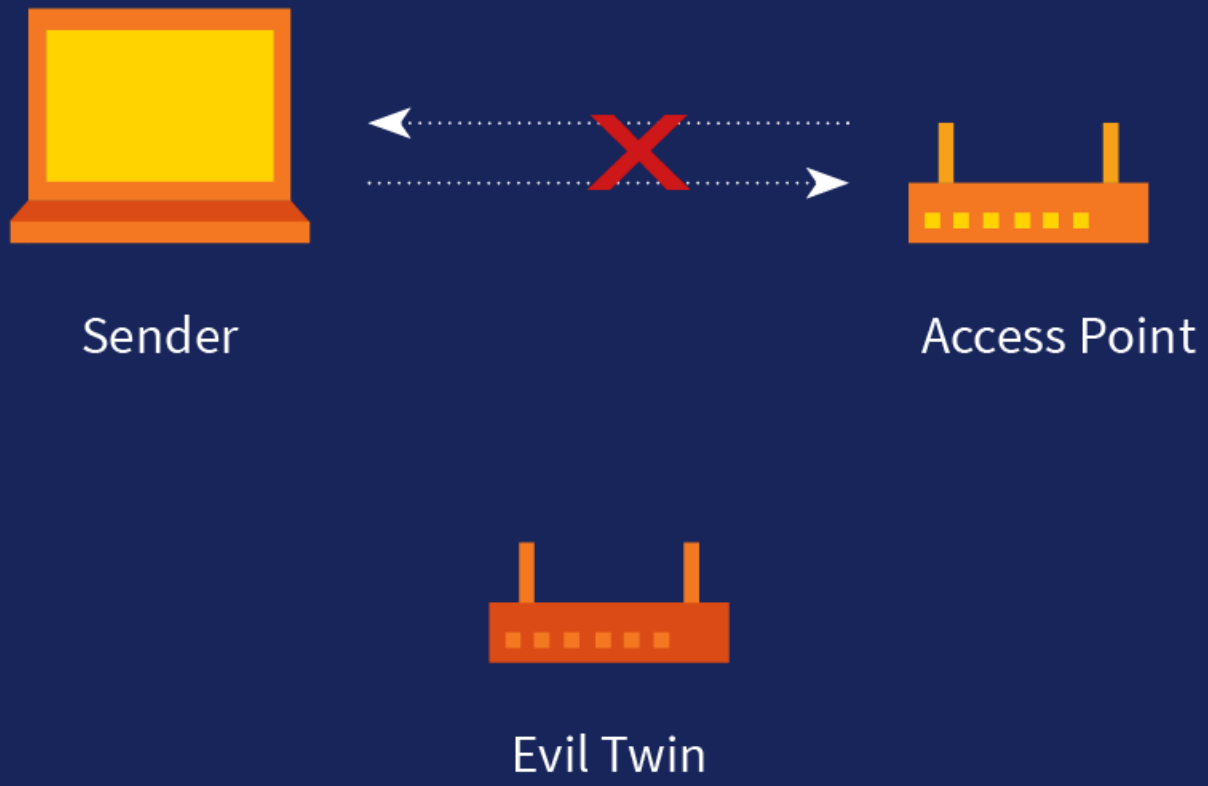
- Gegenmaßnahmen
  Der WLAN-Standard IEEE 802.11w kennt bereits Gegenmaßnahmen, um einen Schutz zu realisieren, dies wird als Protected Management Frames (PMF) bezeichnet. Allerdings wird die Funktion nicht von allen Geräten unterstützt und muss manuell aktiviert werden. Der Sicherheitsstandard WPA3 bietet ebenfalls eine Schutzmaßnahme und sollte daher aktiviert werden.

Evil Twin AP

Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

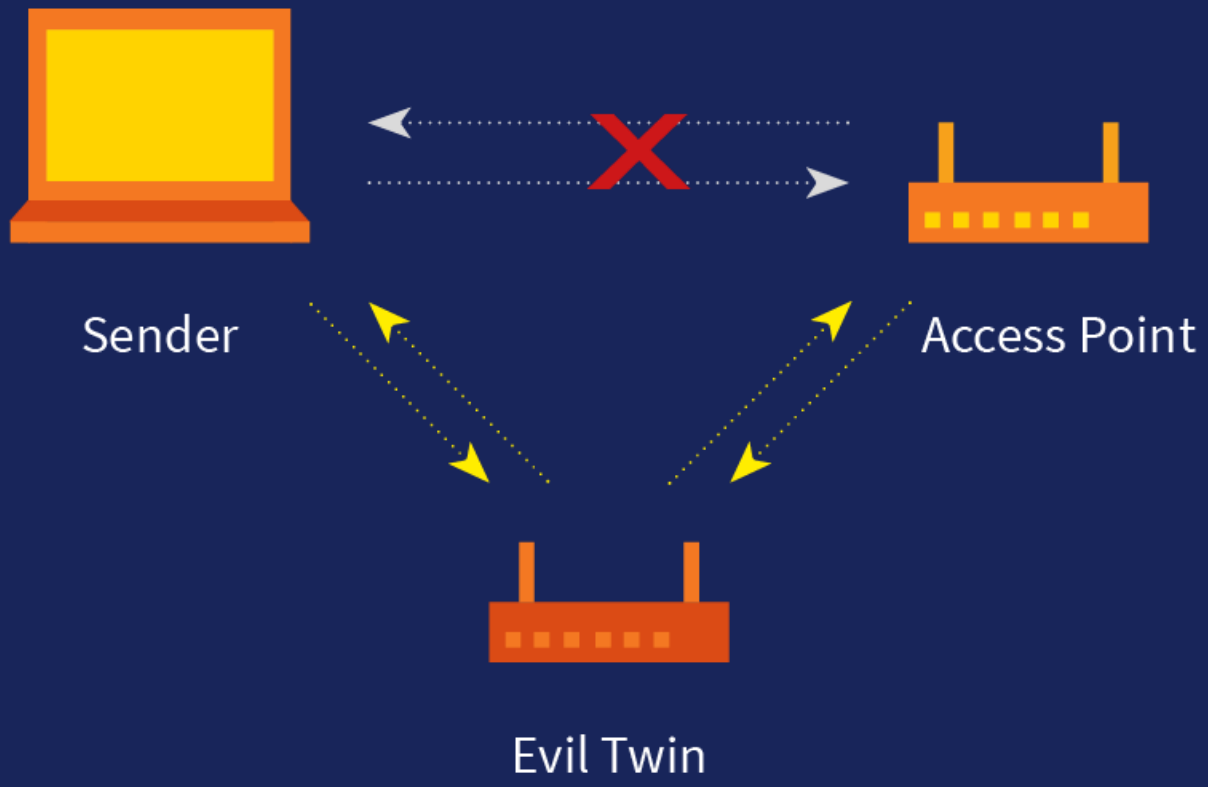
Evil Twin AP



Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Evil Twin AP



Die 10 größten Bedrohungen für Computer-Netzwerke

Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

EXKURS Evil Twin AP

Die 10 größten Bedrohungen für Computer-Netzwerke

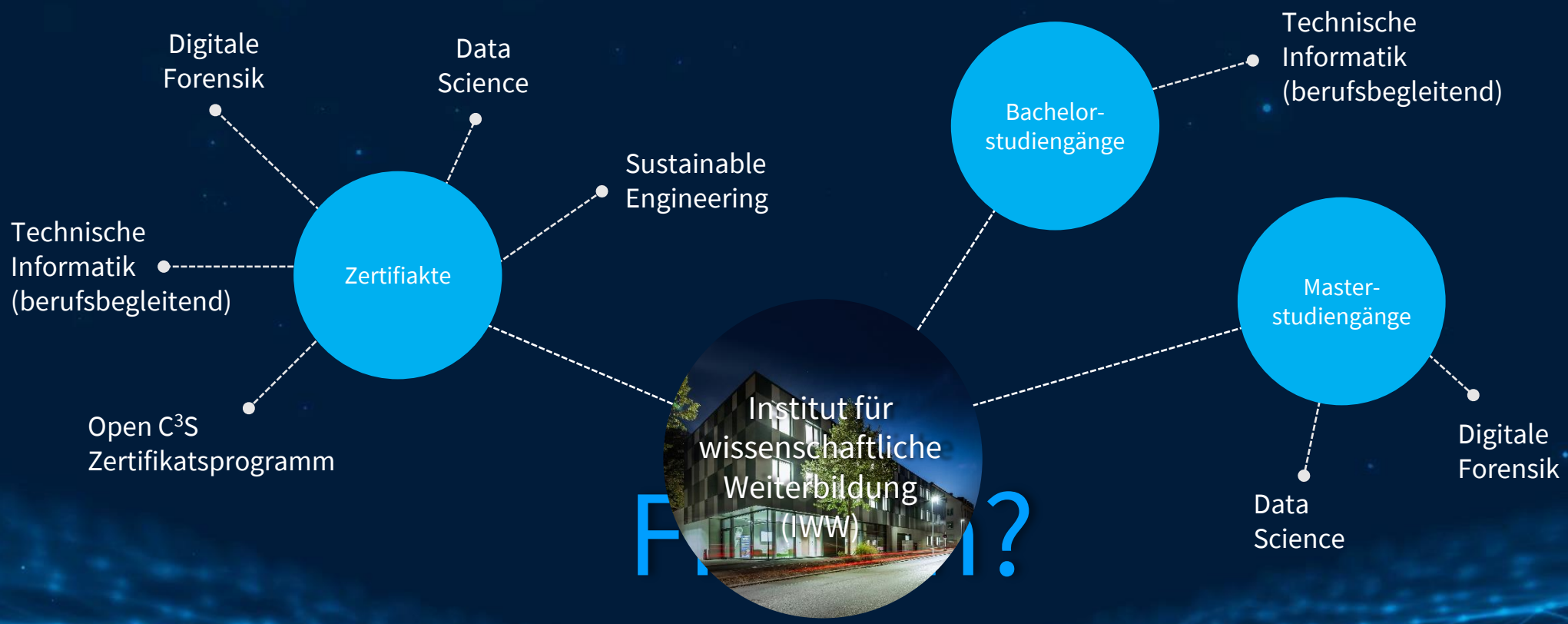
Angriffe gegen Netzwerke
- Scanning
- Sniffing
- Spoofing
- Man-in-the-Middle
- Denial-of-Service
- Physical Attacks
- Replay Attack
- Jamming
- Deauthentication
- Evil Twin AP

Extrafolie

Evil Twin AP

Angreifer versuchen mit einem Access Point ein WLAN zu erstellen, das den gleichen Namen trägt wie das ursprüngliche WLAN. Dabei wird eine Verbindung mit dem ursprünglichen Netzwerk durch den Angreifer hergestellt und der gesamte Datenverkehr weitergeleitet. Verbindet sich nun ein Opfer mit dem gefälschten Zwillings-WLAN, daher der Name Evil Twin AP, kann der Angreifer unverschlüsselten Datenverkehr mitschneiden und manipulieren.

- Gegenmaßnahmen
  Im Unternehmensumfeld sollte für die Authentifizierung die Variante WPA2 Enterprise eingesetzt und bei fremden WLANs immer zusätzlich eine VPN-Verbindung verwendet werden.



Vielen Dank für Ihre Aufmerksamkeit

Weitere Vorträge: weiter-bildung.info | Präsentation online unter: scheible.it