Hochschule
Ravensburg-Weingarten

Systemadministration

WS18/19

# Raspberry PI als VPN-WLAN Zugangspunkt

*Autoren:*
Florian Pfeffer
Dennis Erdelean

*Professor:*
Prof.Dr. Tobias
Eggendorfer

December 6, 2018

# Inhaltsverzeichnis


**1 Einleitung** **2**

**2 Grundlegendes** **2**
2.1 Funktionsweise Virtual Private Network . . . . . 2
2.1.1 IPsec . . . . . 3
2.1.2 Sicherheitsprotokolle . . . . . 4
2.1.3 Transport-und Tunnelmode . . . . . 5

**3 Zielbestimmung** **7**
3.1 Musskriterien . . . . . 7
3.2 Wunschkriterien . . . . . 7

**4 Vorgehen** **7**
4.1 Aufbau . . . . . 7
4.2 Grundkonfiguration . . . . . 7

**5 Einsatz** **11**
5.1 Anwendungsbereiche . . . . . 11
5.2 Zielgruppen . . . . . 11

**6 Umgebung** **11**
6.1 Software . . . . . 11
6.2 Hardware . . . . . 12

**7 Glossar** **13**
7.1 Internet Service Provider (ISP) . . . . . 13
7.2 Man in the middle (MIT) . . . . . 13
7.3 Replay-Angriff . . . . . 13
7.4 Secure Shell(SSH) . . . . . 13
7.5 Dnsmasq . . . . . 14
7.6 Wide Area Local Network (WLAN) / (Wi-Fi) . . . . . 14
7.7 Virtual Private Network(VPN) . . . . . 14
7.8 WiFi Protected Access (WPA2) . . . . . 15
7.9 WLAN Hotspot . . . . . 15
7.10 Hostapd . . . . . 15

# 1 Einleitung

Durch den kürzlichen Angriff auf WLAN-Router, wobei die darunterliegende WPA2 Verschlüsselung umgangen wurde, sind nun Heimnetzwerke per se nicht mehr sicher. Der Grund, die Verbindung zwischen einem Endgerät und dem Router ist generell unverschlüsselt. Somit kann ein Angreifer der sich im selben Netzwerk befindet jegliche Daten mitschneiden. Bei unverschlüsselten Verbindungen benutzen versierte Angreifer Angriffstechniken wie den "Man-in-the-middle"-Angriff , bei dem sie sich im gleichen Netzwerk zwischen dem Endgegerät und dem Router positionieren, um Daten abzugreifen. Sitzt man generell im selben Netzwerk ist es kein Problem durch innovative Tools wie Wireshark oder Ettercap, den Netzwerkverkehr abzuhören.
Durch die Technologie eines virtuellen privaten Netzwerkes kann man diese Lücke schließen und somit den Inhalt der Daten die man überträgt, verschlüsseln. Da der Ottonormalverbraucher oft fehlendes Hintergrundwissen für diese immer komplexer werdende digitale Welt besitzt, gilt es Lösungen für dieses Problem zu erschließen. Eine VPN-Technologie wäre hiermit ein möglicher Ansatz, welche in dieser Ausarbeitung unter die Lupe genommen wird.

# 2 Grundlegendes

## 2.1 Funktionsweise Virtual Private Network

Unterschiedliche Standorte lassen sich über zwei verschiedene Klassen von Netzwerken verbinden: private Netzwerke und öffentliche Netzwerke. Ein privates Netzwerk entsteht, indem man auf Leitungstypen zurückgreift, die ausschließlich vom eignenen Unternehmen oder Zuhause benutzt werden, etwa Wählleitungen wie ISDN, DSL oder Festbverbindungen. Man mietet sich von Providern Leitungen und stellt eine eigene Infrastrukutur(mittels Routern), die auch selbst betrieben werden muss.
Verschlüsselt man den Datenverkehr über öffentliche Netze und sorgt für eine vernünftige Authentifikation der Gegenstellen, entsteht ein Virtual Private Network VPN .
Grundsätzlich kann man sagen, dass wenn zwei oder mehr Rechner oder lokale Netze miteinander über eine durch Verschlüsselung gesicherte Verbindung miteinander verbunden sind, man von von einem VPN spricht. Der Ausdruck

"privat" bedeutet, dass die Verbindung genauso gut gesichert ist, wie wenn Rechner zusammen in einem geschützten Netz stehen würden. Da sie aber räumlich getrennt sind, handelt es sich um ein "virtuelles privates Netz". Grundlegende Eigenschaft eines VPN ist die völlige Unabhängigkeit von den unteren OSI-Schichten 1-3. Es spielt keine Rolle, wie die IP-Pakete transportiert werden, es gibt keinen festen Weg. Es gibt auch andere Technologien, die auch zu den VPN-Technologien gezählt werden oder mit denen sich virtuelle private Netzwerke erstellen lassen. Ihnen ist aber die fehlende Unabhängigkeit auf den unteren OSI-Layern gemeinsam. Der Provider legt die Route fest, die ein Paket nimmt, und verhindert so den Zugriff von "außen" auf das virtuelle private Netzwerk. Zu diesen Technologien gehören unter anderem das Protokoll L2F (Layer 2 Forwarding Protocol) oder das L2TP( Layer 2 Transport Protocol). Aber auch Frame Relay läßt sich von Providern für diese Einstellung eines VPNs einsetzen.
Wir aber fokussieren uns auf die VPN-Technologie die unabhängig der OSI-Schichten 1-3 agieren kann.

Für ein IP-basiertes VPN gibt es verschiedene Möglichkeiten, Daten verschlüsselt zu übertragen. Das anerkannt sichere und sehr weitverbreitete IPsec (IP Security) ist auf fast allen Plattformen, auch auf hardware-basierten Routern verfügbar. Man kann IPsec als Standard für IP-basierte VPNs betrachten.
Im nächsten Abschnitt gehen wir näher auf die funktionsweise von IPsec ein.

### 2.1.1 IPsec

Die Hauptaufgabe von IPsec ist es bei IP-Verbindungen für Integrität und Vertraulichkeit zu sorgen. Integrität im Sinne von, kommen die zu übertragenden Daten unverändert am Ziel an? und Vertraulichkeit im Sinne von, kommen die Daten auch wirklich vom erwarteten Absender?. Aufgrund der Tatsache dass, das eigentliche IPv4-Protokoll keine Mechanismen besitzt die beiden Grundwerte der IT-Sicherheit garantieren zu können, kommt das Verfahren von IPsec uns hier zugute. IPsec wird in 4 Teile untergliedert:

- Sicherheitsprotokolle: die Basis von IPsec bilden die drei Sicherheitsprotokolle "Authentication Header(AH)" und "Encapsulating Security Payload(ESP)" und Internet Security Association Key Management Protocol (ISAKMP)

- Security Association(SA): Verbindungen werden über Security Associa-

tions abgebildet. Jedes Sicherheitsprotokoll benötigt seine eigene Security Association SAs sind zeitlich begrenzt. Nach Ablauf des Gültigkeitszeitraumes müssen diese wieder neu verhandelt werden.

- Schlüsselmanagement: Für die Authentifikation und Verschlüsselung wird mit verschiedenen Schlüsseln gearbeitet. Neben der Möglichkeit, Schlüssel auch manuell auszutauschen, gibt es das "Internet Key Exchange (IKE)-Protokoll", das den automatischen Schlüsselaustausch erlaubt.

- Verschlüselungsalgorithmen: IPsec kennt eine Reihe verschiedener Algorithmen, die aber nicht immer alle implementiert sein müssen. Von der Qualität des Algorithmus hängt letztenendes auch die Sicherheit der Verbindung ab.

### 2.1.2 Sicherheitsprotokolle

- **Authentication Header(AH)** Um einen Absender eindeutig zu identifizieren und Integrität der Daten zu gewährleisten das ganze aber ohne Verschlüsselung, ist Aufgabe des Authentication Headers. Der Integritätsschutz umfasst die Header-Informationen inklusive Quell- und Zieladressen. Es gibt durchaus Anwendungsbereiche wo keine Verschlüsselung angewendet wird, wie zu Beispiel aufgrund gesetzlicher Vorschriften eines Staates. AH kann man auch als eine digitale Unterschrift der Datenpakete betrachten.

- **Encapsulating Security Payload(ESP)** Für die Vertraulichkeit, also für die eigentliche Verschlüsselung der Daten, ist der Encapsulating Security Payload verantwortlich. Zusätzlich verfügt ESP noch über Mechanismen zur Authentifikation. Verwendet man diesen, kann das Verfahren mit dem Authentification Header in den meisten Fällen außer Acht gelassen werden, da ESP die Funktionalität der Authentifizierung auch beinhaltet.

- **Internet Security Association Key Management (ISAKMP)**ist ebenfalls ein Sicherheitsprotokoll, definiert aber selbst keine Algorithmen die zum Erzeugen der Schlüssel für AH und ESP benutzt werden. Das Internet Key Exchange- (IKE) Protokoll benutzt das ISAKMP-Framework mit speziellen Schlüsselaustauschalgorithmen, um kryptografische Schlüssel für AH und ESP einzurichten. Die Trennung von IKE

und ISAKMP bedeutet nur, dass das gleiche IPSec-Framework mit verschiedenen Schlüsselaustauschalgorithmen verwendet werden kann (einschließlich des guten alten manuellen Schlüsselaustauschs).

Sowohl AH als auch ESP sind auf die Verwendung gemeinsam genutzer Schlüssel angewiesen. Sie bieten beide nicht die Möglichkeit, sie von einer Maschine auf die andere zu verschieben. Will man die Schlüssel automatisch erzeugen, erledigt dies das ISAKM-Protokoll. Wir aber, entscheiden uns bewusst für den manuellen Schlüsselaustausch da generell beide Endgeräte sich auf den automatischen Austausch einigen müssen, schlägt diese Fehl und man bemerkt es nicht, verlassen die Daten unverschlüsselt das Endgerät. Zusätzlich ist durch die erläuterten Schritte des manuellen Schlüsselaustauschs ein Lerneffekt gegeben.

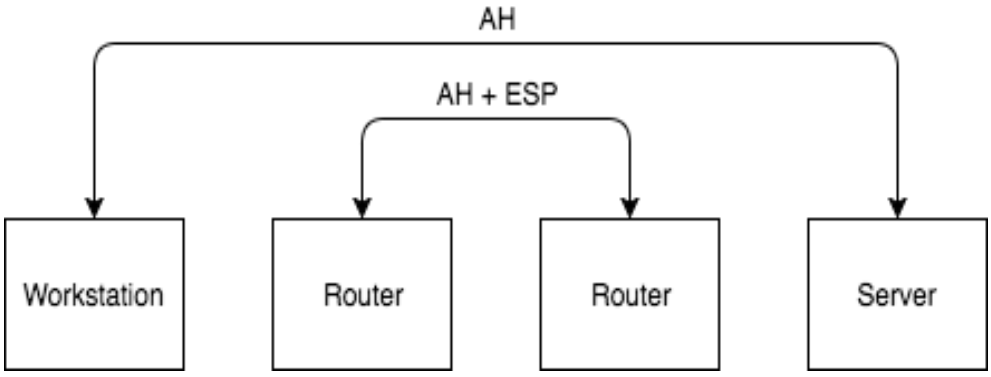


Figure 1: IPSec Authentication Header und Encapsulating Security Payload

Beide Sicherheitsprotokolle verfügen über Sicherheitsmechanismen, die sogenannte Replay-Attacken verhindern. Bei einer Replay-Attacke 7.3 wird Datenstrom mitgeschnitten und dann dem Zielsystem wieder vorgespielt.

### 2.1.3 Transport-und Tunnelmode

IPSec stellt 2 verschiedene Betriebsmodi zur Verfügung. Den Transportmodus und den Tunnelmodus.

- **Transportmodus** Der Transportmodus dient zum Schutz von Host zu Host. Hierbei werden die Daten erst durch ESP verschlüsselt oder durch AH signiert und dann das Paket eingekapselt bzw. mit einem IP-Header versehen.

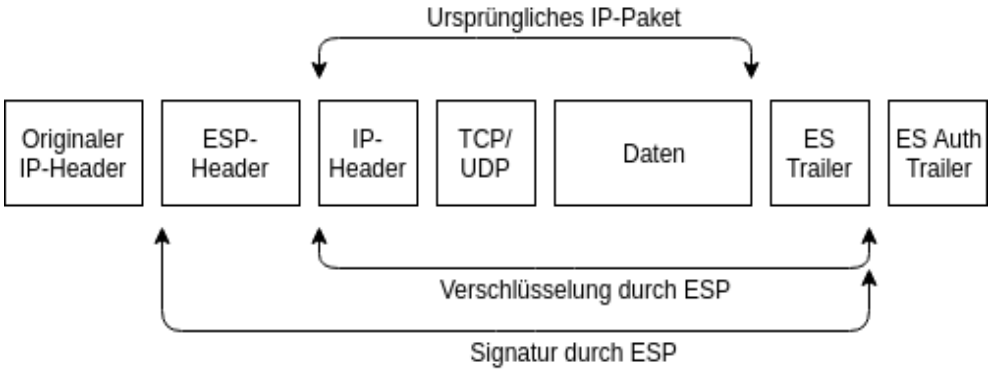


Figure 2: IPSec Authentication Header und Encapsulating Security Payload

- **Tunnelmode** Der Tunnelmodus hingegen dient zum Schutz von einem Router zu einem Host oder von Router zu Router. Hierbei verschlüsselt bzw. signiert IPSec das gesamte IP-Paket inklusive IP-Header und kapselt dieses Paket in ein neues. Der eingekapselte ursprüngliche IP-Header bleibt somit unangetastet. Insgesamt bekommt das Paket aber einen neuen IP-Header. Genau dieser Mechanismus erlaubt es uns ein virtuelles privates Netzwerk zu errichten und damit Integrität, Vertraulichkeit und auch Anonymität zu gewährleisten.

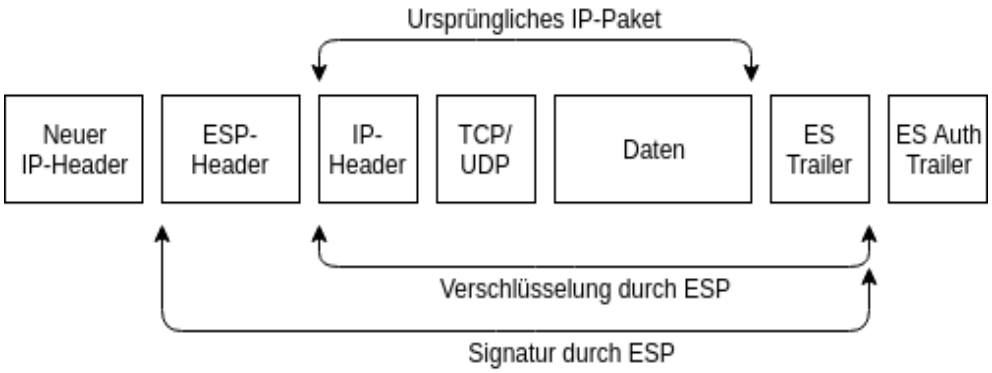


Figure 3: IPSec Authentication Header und Encapsulating Security Payload

NACHTEILE VORTEILE PROBLEME TUNNELING

# 3 Zielbestimmung

## 3.1 Musskriterien

- Internetzugang nur durch Verschlüsselung
- Verschlüsselung der Verbindung zwischen Endgerät und WLAN Zugangspunkt
- Firewall lässt nur VPN-Verbindungen passieren
- eigener VPN-Server auf dem Raspberry Pi durch OpenVPN
- zusätzliche Hardware zum ISP-Router (Raspberry Pi)
- Abhörsicherheit im eigenen Netzwerk

## 3.2 Wunschkriterien

- Erreichbarkeit außerhalb des lokalen Heimnetzwerkes
- Clientauthentifizierung beim VPN-Server mittels SSL-Zertifikat

# 4 Vorgehen

## 4.1 Aufbau

Der Grundaufbau sollte so ausschauen, dass wir durch ein Ethernetkabel dem Raspberry eine Internetverbindung bereitstellen. Dieser wird als Zugangspunnkt genutzt mit dem sich Endnutzer verbinden. Auf dem Raspberry selbst läuft die OpenVPN-Software welcher als Server für Authentifikation und das Weiterleiten der Pakete fungiert. Dieser Server kreiert ein Interface auf dem Betriebssystem welche die

## 4.2 Grundkonfiguration

Zuerst bekommt der Raspberry das Betriebssystem "Raspbian Jessie 4.14.79" aufgesetzt. Dazu lädt man von der offiziellen Raspberry Homepage die aktuellste Version herunter. Nun öffnet man ein Terminal, in unserem Fall das

Hostsystem unter Linux Ubuntu und schreibt die .img Datei auf die mitgelieferte SD-Karte mit folgendem Befehl

```
$ sudo dd bs=4M if=path/to/os.img of=/dev/sdcardX
 status=progress conv=fsync
```

Durch die Option status=progress wird der Fortschritt angezeigt, da dieser standardmäßig nicht zu sehen ist und es einige Minuten in Anspruch nehmen kann, bietet diese Option sich an. Jetzt wird mittels eines HDMI-Kabel und einer Tastatur der Raspberry an einen Bildschirm angeschlossen. Sobald der Raspberry hochgefahren ist wird man aufgefordert einen Loginname und Passwort einzugeben, welches für den Login:pi und Passwort:raspberry ist. Ist man ein deutsches Layout der Tastatur gewöhnt treten schon bei eingabe des Passworts Probleme auf, da dieses auf englisch voreingestellt ist. Y und Z sind daher vertauscht. Bei der Konfiguration des Raspbian Betriebssystems empfiehlt es sich SSH zu aktivieren und das Tastaturlayout, Region und Zeitzone auf deutsch einzustellen. Der Raspberry wird jetzt neu gestartet und dann kann nun per SSH angesteuert werden. Nun ist das Betriebssytem passend für die Anforderungen konfiguriert und der Raspberry wird jetzt als WLAN-Zugangspunkt konfiguriert. Dazu öffnen wir die Datei im Pfad **/etc/network/interfaces** und editieren diese folgendermaßen:

```
# Localhost
auto lo
iface lo inet loopback

# Ethernet
auto eth0
iface eth0 inet dhcp

# WLAN-Interface
allow-hotplug wlan0
iface wlan0 inet static
address 192.168.22.1
netmask 255.255.255.0
```

Mit diesem Eintrag wird dem wlan0 Interface die statische IP-Adresse 192.168.22.1 zugewiesen, diese ist notwendig da der DHCP- und DNS-Server später über diese Adresse erreichbar sein soll. Der Raspberry muss nun neu gestartet

werden. Nach dem Systemneustart können wir nun den DHCP-Server konfigurieren, dazu öffnet man die Datei **/etc/dnsmasq.conf** und ändert diese wie Folgt ab:

```
# DHCP-Server aktiv fuer WLAN-Interface
interface=wlan0

# DHCP-Server nicht aktiv fuer bestehendes Netzwerk
no-dhcp-interface=eth0

# IPv4-Adressbereich und Lease-Time
dhcp-range=192.168.22.100, 192.168.22.150,24h

# DNS
dhcp-option=option:dns-server,192.168.22.1
```

In der Datei wird festgehalten, welcher Adressbereich von dem DHCP-Server vergeben werden soll, in unserem Fall ist Platz für 50 Clients mit einem Adressbereich von 192.168.22.100-192.168.22.150. Als letztes wird noch die zuvor in der **/etc/network/interfaces** vergebene Statische IP-Adresse 192.168.22.1 als DHCP-Server-Adresse festgelegt. Die Konfiguration kann nun mit dem Befehl

```
$ dnsmasq --test -C /etc/dnsmasq.conf
```

auf Korrektheit überprüft werden. Ist die Syntaxprüfung mit einem "OK" erfolgreich gewesen, kann nun dnsmasq mittels folgendem Befehl neu gestartet werden.

```
$ sudo systemctl restart dnsmasq
```

Um nun das WLAN-Netzwerk nutzbar für Clients zu machen muss das Programm Hostapd geladen werden. Hostapd macht unser interface wlan0 zu einem Zugangspunkt. Hostapd kann nun über die Datei /etc/hostapd/hostapd.conf eingestellt werden. Die Konfiguration sieht folgendermaßen aus:

```
#Interface und Treiber
interface=wlan0
driver=nl80211
```

```
#SSID des WLAN's
ssid=VPN_WLAN

#WLAN-Konfiguration
hw_mode=g
channel=7
wmm_enabled=0
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0

#WLAN-Sicherheit
wpa=2
wpa_passphrase=89_-hOXf31DZ.27
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
rsn_pairwise=CCMP
```

Die dort vorgenommenen Konfigurationen bieten uns nun ein WLAN mit der SSID "VPN-WLAN" an. Als Sicherheit für das WLAN wird WPA2 benutzt. Um hostapd in einem Deamon im Hintergrund zu starten muss noch die Datei **/etc/default/hostapd** mit folgendem Parameter ergänzen:

```
DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

Nun kann hostapd mit folgendem Kommando in Betrieb genommen werden:

```
$ sudo systemctl start hostapd
```

Um hostapd bei jedem Systemstart automatisch zu starten kann man noch mittels:

```
$ sudo systemctl enable hostapd
```

diese Funktion aktivieren.

# 5 Einsatz

## 5.1 Anwendungsbereiche

Anwendungsbereiche sind im eigenen Heimnetzwerk oder in öffentlichen unverschlüsselten WLAN-Hotspots 7.9. In beiden Fällen schafft ein eigener VPN-Server eine sichere Verbindung ins Internet. Zusätzlich ist man Herr seiner eigenen Daten, da diese nicht auf Server von Drittanbietern liegen.

## 5.2 Zielgruppen

**Nutzer die Herr der eigenen Daten sein wollen:** Wenn man einen VPN-Service nutzt, beauftragt man ein Unternehmen seine Daten durch das Internet zu routen damit diese privat und sicher bleiben. Da aber einige Nutzer diese Idee nicht gerade gut heissen sich auf einen Drittanbieter zu verlassen der die Privatsphäre schützen soll, offenbart sich hier die Lösung eines eigenen VPN-Servers.
**Kleinere Unternehmen mit einem sicheren lokalen Netz, welches per Fernzugriff erreichbar sein soll:** Viele Unternehmen haben eigene Netzwerke in denen sensible Daten gespeichert sind. Aus Sicherheitssicht möchte man das dieses Netzwerk nur innerhalb des Firmengeländes erreichbar ist. Bestimmten Mitarbeitern könnte man durch eine VPN-Technologie den Zugriff von außen gewähren.
**Neugierige Nutzer die einfach die Funktionsweise von VPN erforschen möchten:** Das Aufsetzen eines VPN's ist ein Puzzle mit verschiedenen Lösungen. Einen VPN-Server kann man durch seinen Router, Desktop-PC, Raspberry Pi oder aus Kombinationen daraus betreiben. Somit hat man eine Vielzahl an Möglichkeiten wie man seine Daten sicher zwischen verschiedenen Geräten bewegt.

# 6 Umgebung

## 6.1 Software

- OpenVPN VPN-Software
- Arch Linux ARM
- iptables (Linux-Kernel)

## 6.2 Hardware

- Raspberry Pi 3 Model

  A 900MHz quad-core ARM Cortex-A7 CPU

  4 USB-Ports

  40 GPIO Pins

  Full HDMI-Port

  Ethernet-Port

  1GB RAM

  Kombinierter 3.5mm Kinkenanschluss-und Farbschirmanzeige

  Kamerainterface (CSI)

  Display Interface (DSI)

  Micro-SD-Kartenslot

  VideoCore IV 3d graphics core

# 7 Glossar

## 7.1 Internet Service Provider (ISP)

Ein Internet Service Provider ist ein Anbieter von technischen Leistungen oder Inhalten für die Nutzung oder den Betrieb von Inhalten und Diensten im Internet. [1]

## 7.2 Man in the middle (MIT)

Wie der Name schon andeutet, platziert bei diesem Angriff der Hacker sich selbst – oder seine schädliche Software – zwischen dem Opfer und der aufgerufenen Ressource, etwa einer Bank-Webseite oder einem E-Mail-Konto. [2]

## 7.3 Replay-Angriff

Ein Replay-Angriff basiert auf der Wiedereinspielung von vorher gesammelten Daten für die Authentifizierung und die Zugriffskontrolle. Der Angreifer arbeitet mit Identitätsdiebstahl und benutzt dabei die erfassten Daten mit denen er eine fremde Identität vortäuscht um mit falscher Identität auf Ressourcen und Datenbestände zugreifen zu können. Der Angriff auf die Authentifizierungs- und Zugangsdaten kann über einen Man-in-the-Middle-Angriff erfolgen. [3]

## 7.4 Secure Shell(SSH)

SSH ist die Abkürzung für Secure Shell. Mit Hilfe von Secure Shell lassen sich sichere Netzwerkverbindungen zu anderen Geräten herstellen, etwa von einem PC zu einem Webserver. SSH ermöglicht die gegenseitige Authentifizierung und eine verschlüsselte Datenübertragung, so dass sensible Daten wie Passwörter oder Benutzernamen nicht von Unberechtigten ausgespäht werden können. Secure Shell bietet dabei ein hohes Sicherheitsniveau. [4]

## 7.5 Dnsmasq

Ist ein einfacher DNS- und DHCP-Server für kleine Netzwerke. Es werden die Namen aus dem lokalen Netz entsprechend der Datei /etc/hosts aufgelöst. Unbekannte Namensanfragen werden weitergeleitet und im Cache gespeichert. Dnsmasq ist somit:ein Nameserver-Forwarder, ein DHCP-Server und ein Namenscache. optimiert für Netzwerke mit Dialup-Außenverbindung [5]

## 7.6 Wide Area Local Network (WLAN) / (Wi-Fi)

Der Name Wireless Local Area Network (kurz: WLAN) ist der Oberbegriff für alle schnurlosen bzw. drahtlosen lokalen Netzwerke und meint meist Funknetz-Standards der Normierungsreihe IEEE-802.11x, die in anderen Ländern auch unter dem Begriff Wi-Fi zusammengefasst werden.

**Kunstbegriff Wi-Fi**

In einigen Ländern, wie etwa in Großbritannien, Kanada, Spanien, den Niederlanden, Italien, Frankreich oder den USA, wird synonym für WLAN respektive weitläufig auch der Kunstbegriff Wi-Fi verwendet. Strenggenommen ist dies aber von der Bedeutung her nicht korrekt. Denn während WLAN bzw. Wireless LAN das Funknetzwerk an sich bezeichnet, bezieht sich Wi-Fi auf die von der Wi-Fi-Alliance generierte Zertifizierung anhand der IEEE-802.11-Familie für WLAN. Da jedoch sämtliche Wi-Fi-zertifizierten Produkte immer WLAN-Standard-konform sind, werden die beiden Begriffe gerne auch synonym genutzt. [6]

## 7.7 Virtual Private Network(VPN)

Ein Virtual Private Network (VPN) ermöglicht eine verschlüsselte, zielgerichtete Übertragung von Daten über öffentliche Netze wie das Internet. Es etabliert geschützte und in sich geschlossene Netzwerke mit verschiedenen Endgeräten. Häufige Anwendung ist die Anbindung von Home Offices oder mobilen Mitarbeitern. [7]

## 7.8 WiFi Protected Access (WPA2)

WPA2 (WiFi Protected Access 2) bzw. IEEE 802.11i ist ein Standard aus dem Jahr 2004 für die Authentifizierung und Verschlüsselung von WLANs, die auf den IEEE-Spezifikationen 802.11 basieren. [8]

## 7.9 WLAN Hotspot

Hot Spots sind öffentliche drahtlose Internetzugangspunkte. Sie sind sowohl in öffentlichen Räumen (einige Bibliotheken, Krankenhäusern, Flughäfen, Bahnhöfen usw.) als auch in privaten wie z. B. Gastronomie, Hotels etc. installiert. Es kommt fast ausschließlich eines der Protokolle der IEEE 802.11-Familie (Umgangssprachlich WiFi oder WLAN genannt) zur Anwendung, eine Verbindung zum Hot Spot ist dadurch mit einer Vielzahl an Geräten möglich, weil die Protokoll-Familie in Mobilgeräten sehr häufig unterstützt wird.[9]

## 7.10 Hostapd

# Referenzen


[1] Experian. http://www.experian.de/glossar/internet-service-provider-isp.html .

[2] Kasperksy. https://www.kaspersky.de/blog/was-ist-eine-man-in-the-middle-attacke/905/.

[3] IT Wissen. https://www.itwissen.info/Replay-Angriff-replay-attack.html.

[4] Checkdomain. https://www.checkdomain.de/hosting/lexikon/ssh/.

[5] Ubunuusers. https://wiki.ubuntuusers.de/Dnsmasq/.

[6] IP Insider. https://www.ip-insider.de/was-ist-wlan-a-579430/.

[7] IP Insider. https://www.ip-insider.de/was-ist-ein-vpn-a-625331/.

[8] Elektronik-kompendium. https://www.elektronik-kompendium.de/sites/net/0907111.htm.

[9] Wikipedia. https://de.wikipedia.org/wiki/Hot$_S pot_(WLAN)$.