Network security

Yann Gaspoz, 12.05.2021

1 Einführung

Auf diesem Handout werden die Basic Themen von der Präsentation zusammengefasst und erklärt.

2 Mac-Adresse[1]

2.1 Herkunft und Gebrauch

Die Mac-Adresse(Media Access Control - Adress) wird bei allen Geräten von ihren Herstellern eingebrannt, d.h. dass sie auf dem Read-only Abteil einer Netzwerk Karte gespeichert ist. Jede Mac-Adresse ist einmalig und kann im Regelfall nicht verändert werden. Die Mac-Adresse wurde als Network Adresse erfunden. Wäre die Mac Adresse nicht einmalig würde man Probleme mit der Netzwerkverbindung erhalten. Die Mac-A dresse ist eine physikalische Adresse und gehört zum osi Modell welches auch in der Präsentation vorkommt.

2.2 Aussehen

Eine Mac-Adresse ist 48 Bit gross und besteht aus 6 Gruppen mit je 2 hexadezimalen Zahlen. Ein beispiel einer Mac-Addresse: 8B:7E:04:07:37:74.

3 LAN

3.1 WLAN

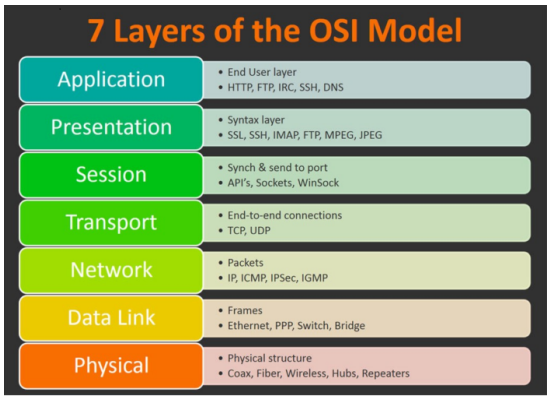

Abbildung 1: OSI-Modell[2]

Wi-Fi gehört zur Familie der wireless network protocols wie zum Beispiel auch Bluetooth dazu gehört. Wi-Fi versendet Pakete, welche z.b. Inhalte über eine Webseite enthalten, über Radio Wellen. Die ganze Idee mit den Wellen kann sehr verwirrend sein und wenn man mehr darüber erfahren möchte kann man bei der Quellenangabe 3 weiter darüber lesen. Das Problem mit dem LAN/WLAN ist dass sich ein Hacker zwischen Router und User stellen kann und dann eine MITM-attack(Man In The Middle) ausüben kann(mehr davon in der Präsentation). Im LAN gibt es ein Schichtenmodell namens OSI[2], man findet dort die 7 Schichten des LAN's.

4 HTTP/HTTPS[3]

HTTP oder Hypertext transfer protocol ist ein Protokoll welches beim laden einer Website Pakete anfordert und verschickt. Wenn zum Beispiel auf einer Seite ein Bild ist wird es von dem Webserver angefordert. Diese Anforderungen nennt man GET. Zu dem HTTP gibt es auch ein HTTPS, das S steht für secured. Mit dem HTTPS werden all diese Pakete entschlüsselt verschickt wie man es in der Präsentation sah.

5 Attacken

Heutzutage ist das LAN sehr unsicher, da man es auf viele verschiedene Arten angreifen kann. Hier eine kurze Liste von Attacken:

- **MITM-attack:** Die Man-In-The-Middle-attack ist ein Angriff bei welchem sich ein Hacker an das LAN schliesst und den Verkehr überwacht und manipuliert. In der Tabelle unten[4] sieht man wie vermehrt diese Attacke ausgeführt wird.

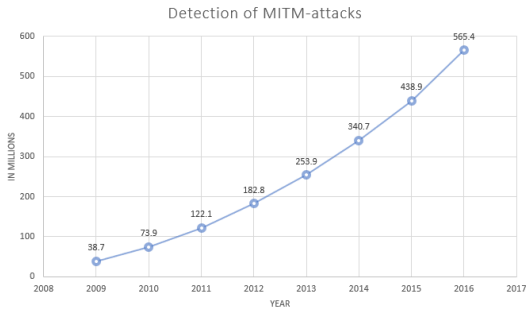

Abbildung 2: MITM-Attacken[4]

- **DDoS:** Distributed-Denial-Of-Service ist ein Angriff bei welchem die Ressourcen eines Servers überfüllt werden. Solche Attacken werden in den meisten fällen von einem BOT-NET ausgeführt, welches Anfragen an den Server stellt. Man kann sich die Anfrage als eine komplexere art von PING vorstellen.

- **SQL-injection:** Eine Structured Query Language injektion ist ein Angriff auf eine Datenbank mit welcher man alle Sicherungen umgehen kann und dann z.b. alle Inhalte kopieren kann oder ändern kann.

- **XSS:** Der Cross Site Scripting Angriff ist ein Angriff bei welchem man seine eigenen Skripte einfügen kann. Dies macht man indem man eine Zeile Code in ein Suchfeld eingibt bei welchem man dann z.b. ein Skript ausführt welches deine Login-Daten einsammelt.

6 Quellenangabe

Literatur

[1] (2021). „Mac address,“ Adresse: `https://en.wikipedia.org/wiki/MAC_address`.

[2] (). „7 OSI Layer dan Penje-lasannya,“ Adresse: `https://salamadian.com/pengertian-osi-layer/`.

[3] (2021). „Hypertext transfer protocol,“ Adresse: `https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol`.

[4] (). „Detection of Man-In-The-Middle attacks,“ Adresse: `https://bit.ly/2QOL5gr`.