Vulnerabilities connected to using Public Wi-Fi

Security eksamensrapport

Gruppe 14 – Klasse A

Amanda Juhl Hansen: cph-ah433
Sofie Amalie Landt: cph-sl307
Benjamin Kongshaug: cph-bk131

Afleveres: 29-05 2020

Antal anslag: 35.118 ≈ 14,6 sider

Indholdsfortegnelse

Projekt formulering

Vi vil kigge på de sikkerhedssvagheder der er i forbindelse med at være forbundet til public Wi-Fi, samt tiltag der kan tages for at minimere disse svagheder. Herunder vil vi gå i dybden med VPN, og hvordan den er med til at skabe en sikker forbindelse, med udgangspunkt i et praktisk eksempel.

Indledning

Langt størstedelen af befolkningen ejer i dag en smartphone, 91 % ejer en computer og omkring 80 % ejer en tablet. Dette er bl.a. også en af grundene til at offentligt Wi-Fi i dag er mere udbredt end nogensinde før, og det ses bl.a. på kaffebarer, restauranter og lufthavne. Offentligt Wi-Fi gør det muligt at holde os opdateret på de sociale medier, tjekker e-mail og andre praktiske ting, mens vi bevæger os i det offentlige rum. Hvad de fleste dog ikke er klar over, er at det offentlige Wi-Fi slet ikke er designet til det 21'ende århundrede. Befolkningen er simpelthen for uvidende om de risici der følger med at logge på et offentligt Wi-Fi, og derfor også om de tiltag som alle almindelige mennesker bør tage stilling til inden de logger på[1]. Dette er hvad vi i denne rapport vil undersøge nærmere. Både de risici der er forbundet med at logge på et offentlig Wi-Fi, men også hvad man kan gøre for at sikre sig mod disse.

Arbejdsfordeling

Vi har i vores rapport, fordelt arbejdet således at vi hver især har skrevet afsnit til både Security Risks og How to Prevent. Benjamin har skrevet om Malware Distribution og VPN. Amalie har skrevet Rogue Access Point, Fake Access Point/Evil Twin, WEP/WPA og WPA2 Krack attack, samt Force HTTPS. Amanda har skrevet om Network Sniffing og session hijacking, samt firewalls og fildeling. Det praktiske VPN-eksempel samt indledning og diskussion/konklusion er udført og skrevet i fælles samarbejde.

[1] Kilde: 1.1

Security Risks

Uanset hvor du opretter forbindelse til internettet vil der altid være sikkerhedsrisici forbundet med dette. Det kan være din egen forbindelse eller den ressource du har oprettet forbindelse til, som kan være kompromitteret. Alle disse risici gør sig særligt gældende når man opretter forbindelse til et offentligt netværk, og det er disse vi vil uddybe i dette afsnit.

Malware distribution - Worm Attack

Har en klient, der er logget på et offentlig Wi-Fi, ikke slået filedeling fra, kan en hacker udnytte dette ved at lægge malware i klientens public folder, som er tilgængelig for andre klienter tilknyttet samme netværk. Hvis en hacker har inficeret en klients enhed med et "worm attack", kan en klient der er forbundet på et netværk, inficere andre klienter uden at være klar over det.

Et worm attack (orm) er et ondsindet program der kan sprede sig selv. Normalt vil en computer inficeret med en orm f.eks. sende en kopi af ormen via e-mail til alle klientens kontakter. Downloader kontakterne den vedhæftede fil, med ormen, vil den sende kopier af sig selv videre til den nye klients kontakter og så videre.

I 2014 blev en trojansk hest kaldet Emotet opdaget. Emotet var udviklet til at sniffe bankoplysninger og andre personlige informationer. Igennem de sidste 6 år har Emotet udviklet sig en del. Den 12. februar 2020 skrev thehackernews.com en artikel om et cybersecurity firma der for nylig har opdaget en ny version af Emotet der kan sprede sig selv over Wi-Fi, ved hjælp af et nyt "Wi-Fi spreader module". Cybersecurity firmaet siger at modulet, som findes i den nye version af Emotet, har et timestamp fra 16. april 2018. Det vil sige at modulet har været i brug i 2 år uden at blive opdaget[2].

Denne version af Emotet er et 2 lags orm angreb, der spreder sig selv over et netværk. Først scanner Emotet efter et Wi-Fi. Finder den et Wi-Fi, laver den et brute-force angreb for at komme ind. Når den er inde, scanner den alle klienterne på netværket, og brute-force'er så igen alle klienter. Herefter kopier den sig selv og gemmer kopierne på klienternes enheder under navnet "Windows Defender System Service". Denne form for Malware distribution blev allerede påvist som mulig uden nogen form for klient aktivitet i 2007 af Indiana University[3], og er især farlig i urbane områder som f.eks. København. Dette skyldes at densiteten af netværksforbindelser giver ormen mange ruter til at sprede sig. Bruger klienten sit hjemme netværk, hvor klienten selv står for sikkerhedsopsætningen, kan man sikre sig mod Emotet. Når klienten benytter en offentlig Wi-Fi, vil netværket ofte sat op med et lavere sikkerhedsniveau, og således være en nem rute for Emotet at sprede sig, både fra Wi-Fi til Wi-Fi og fra klient til klient.

[2] Kilde: 2.1
[3] Kilde: 2.2

Session Hijacking

Session hijacking, også kaldet Sidejacking, er en måde, hvorpå en hacker giver sig ud for at være en anden. Dette gøres ved at få fat på den cookie, der sendes mellem en server og en klient, når klienten logger ind på en hjemmeside. Når en klient logger ind, krypteres loginoplysninger og en cookie sendes retur. I modsætning til login oplysninger, krypteres denne oftest ikke af hjemmesiden, men gemmes i browseren. Cookien bruges bl.a. til at holde klienten logget ind og inkluderes efterfølgende i de requests der sendes til serveren. En cookie vil kun blive krypteret, hvis klienten befinder sig på et Wi-Fi der har en sikkerhedsprotokol, som f.eks. WPA2, og/eller hvis der er HTTPS-forbindelse til hjemmesiden.

I nedenstående afsnit, vil vi forklare om Network Sniffing, som er et værktøj en hacker kan anvende, til at opsnappe klientens cookie, fra en pakke i den forbipasserende netværkstrafik. På det offentlige Wi-Fi, hvor der sandsynligvis ikke er en sikkerhedsprotokol angivet, vil det også være muligt for hackeren at få fat i den pågældende cookie uden at den er krypteret. Når først en hacker har den pågældende cookie, kan hackeren, helt uden at kende brugernavn og adgangskode, logge ind som klienten.

Network Sniffing

Sniffing er et værktøj, som oprindeligt er designet til professionelle netværks ingeniører, for at monitorere netværkstrafikken. Dette inkluderer bl.a. at indsamle pakker af data, dekryptere pakkerne, analysere trafikken, teste systemer såsom firewalls, samt sikre at trafikken flyder jævnt. I dag bruges værktøjet også af hackere, hvis primære formål er identitets snyd, tyveri, at optage e-mail- og besked korrespondancer, samt at hente private informationer, bl.a. brugernavne, adgangskoder og kreditkortoplysninger.

Enheder forbundet til et netværk, er konfigureret således at al netværkstrafik adresseret til andre, bliver ignoreret. Hackere kan ved brug af software (f.eks. WireShark), ændre denne konfiguration til "promiscuous mode". Således kan hackeren/sniffer, samle og hente alle pakker fra netværkstrafikken der passere enheden, uanset adressering. Disse pakker analyseres efterfølgende af softwaren og præsenteres som læseligt data for hackeren.

Der findes to typer af sniffing, både Passive- og Active Sniffing, men eftersom at Active Sniffing kun er mulig hvis netværket er sat op med en switch, er det ikke relevant i forhold til offentlig Wi-Fi. Af denne grund, vil vi kun gå i dybden med Passive Sniffing.

Passive Sniffing er svær at opfange, og kan kun lade sig gøre, hvis netværket er sat op til at bruge hubs. Det vil sige at flere enheder er forbundet på et netværk, og netværkstrafikken flyder frit mellem alle enheder. Denne opsætning af netværket ses som regel på offentlige Wi-Fi. Endvidere betyder dette, at enheder forbundet til netværket modtager al netværkstrafik

der passerer, men ignorerer det, som ikke er adresseret til enheden selv. En sniffer har derfor mulighed for passivt at følge med og absorbere al netværkstrafik der passerer netværket.

Rogue Wi-Fi Access Points

For at kunne forstå hvad et Rogue Wi-Fi Access Point er, er det vigtigt at kende forskellen på en router og et Access point (AP). En router har primært to funktioner, den giver enheder adgang til et kontrolleret lokalt netværk (LAN), derudover modtager og sender den data fra internettet til det lokale netværk. Et AP kan ses som den trådløse del af en trådløs router, og er en form for portal til det lokale netværk (LAN). Dette betyder at et AP ikke giver forbindelse til internettet i sig selv, men i stedet giver adgang til et LAN, som har en eksisterende internetforbindelse.

Et offentligt Wi-Fi kan ofte have flere AP tilknyttet, da dette giver mulighed for at flere kunder kan oprette forbindelse til internettet ad gangen, samtidig kan det forlænge det trådløse internet signal. Rogue AP er et uautoriseret AP, som ikke nødvendigvis er sat op af en ondsindet hacker, men ligeså vel kan være sat op af en godtroende medarbejder, med intentionen om at gøre netværket mere tilgængeligt. Disse kan udgøre en betydelig trussel, da de ikke nødvendigvis er konfigureret med de samme sikkerhedsforanstaltninger som det egentlige LAN. Derfor fungerer Rouge AP som en åben bagdør for hackere, der gør det endnu nemmere at udnytte et offentligt Wi-Fi med henblik på at hacke klienterne på det.

Fake Access Points og Evil Twins

Et Fake AP er et trådløst netværks angreb, hvorved en hacker laver et ondsindet AP, med det formål at få klienter til at oprette forbindelse til dette AP. Det vil sige at et Fake AP er et Rogue AP. Fake AP's er ofte konfigureret med tiltalende Service Set Identifiers (SSID), som f.eks. "Free Wi-Fi" for at lokke andre klienter af netværket til. Formålet med Fake AP's, er man-in-the-middle attacks. Ofte vil klientens webbrowser kryptere websessionerne ved hjælp af SSL/TLS. Ved at logge på et Fake AP har hackeren mulighed for at downgrade denne type beskyttelse, hvis ikke den trådløse klient er opmærksom. Når klienterne opretter forbindelse til det Fake AP, kan de stadig få adgang til internettet, og det er derfor usandsynligt at de fleste vil opdage at der er noget galt. Men når de først er tilsluttet, kan alt hvad de gør online overvåges af hackeren, og følsomme oplysninger, som indtastes online, kan og vil blive stjålet.

En Evil Twin er en version af et Fake AP, som forsøger at efterligne et legitimt AP på det pågældende Wi-Fi, og derved skabe et næsten identisk AP. Dette gøres ved at efterligne indstillingerne på det legitime AP, således at de begge har samme SSID, og eventuelt også adgangskode og krypteringstype, hvis hackeren kender disse. En hacker vil ofte kombinere en Evil Twin med et Wi-Fi deauthentication attack, som er en type denial-of-service attack. Dette vil smide trådløse klienter af det legitime AP, og øger samtidig signalstyrken til "The Evil Twin", som derved tvinger klienterne til at oprette forbindelse til den.

Evil Twins er særligt grumme, da de fleste operativsystemer "husker" de Wi-Fi man tidligere har været tilknyttet, ved at cache deres SSID. Dette vil sige at operativsystemet automatisk vil oprette forbindelse til ethvert netværk med samme SSID, uanset om det er det samme netværk eller ej. Derfor vil et AP på et offentligt Wi-Fi være et oplagt valgt for en hacker, da alle klienter som har været tilknyttet dette Wi-Fi før, automatisk vil blive logge på deres Evil Twin når de er i nærheden. Fake AP's og Evil Twins er nogle af de mest almindelige Wi-Fi angreb. De er nemme at udføre, kræver begrænset tekniske færdigheder, og er yderst effektive. Et studie indikerer at mere end en tredjedel af brugerne ikke tager nogle foranstaltninger når de opretter forbindelse til et offentligt Wi-Fi, og at de ofte opretter forbindelse til usikre netværker[4].

Wired Equivalent Privacy (WEP) og Wi-Fi Protected Access (WPA)

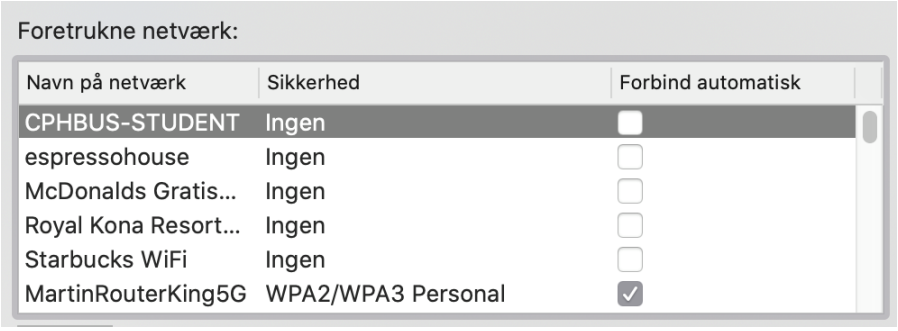
Når man taler om WEP og WPA er der tale om forskellige trådløse kryptering protokoller. De anvendes til at beskytte oplysninger, der sendes og modtages via et trådløst netværk. Disse trådløse krypteringsprotokoller blev oprettet af Wi-Fi Alliance[5]. Den første protokol, som Wi-Fi Alliance oprettede, var WEP der blev introduceret i slutningen af 1990'erne. WEP havde dog en del sikkerheds svagheder, og blev derfor erstattet af WPA i 2003, som en lappeløsning indtil introduktionen af WPA2 det efterfølgende år. På trods af dette er WEP stadig i brug, og giver en falsk følelse af sikkerhed til de mennesker, der vælger at sikre deres netværk med denne protokol.

Nogle af de væsentlige ændringer, der kom med WPA, var Temporal Key Integrity Protocol (TKIP), som er et nøglesystem, der dynamisk genererer en ny 128-bit nøgle til hver pakke. TKIP er derfor mere sikkert end WEP's 64-bit eller 128-bit krypteringsnøgle, som indtastes manuelt og ikke ændres. Desuden implementere TKIP "message integrity checks", som tjekker om pakkerne er blevet ændret af en potentiel hacker mellem AP og klient. Dette erstattede WEP's Cyclic Redundancy Check (CRC), som er en hashfunktion designet til at detektere tilfældige datafejl. TKIP blev senere, med introduktionen af WPA2, erstattet af Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), som er baseret på Advanced Encryption Standard (AES) algoritmen. AES er den mest sikre krypterings algoritme. TKIP er dog stadig bevaret i WPA2, som fallback-system og til interoperabilitet med WPA.

Valget af krypterings- /sikkerhedsprotokol indstilles på den pågældende router eller AP. Derfor kan en klient på det pågældende netværk, ikke selv vælge hvilken sikkerhedsprotokol der anvendes. Når der oprettes forbindelse til et Wi-Fi for klienten derfor adgang vha. den sikkerhedsprotokol, som allerede er fastlagt. Det største problem ved offentligt Wi-Fi, er at denne sikkerhedsprotokol skal aktiveres manuelt ved opsætning af netværket, og det er langt de færreste som er klar over dette, eller er opmærksom på relevansen i valget af

[4] Kilde: 6.1
[5] En sammenslutning af hundredvis af virksomheder indenfor den trådløse netværksindustri

sikkerhedsprotokol. Det er derfor også meget almindeligt, at der slet ikke er valgt en sikkerhedsprotokol. En af de mest synlige indikationer for at et netværk anvender WPA2 som sikkerhedsprotokol, er at man skal angive en adgangskode for at forbinde til netværket. Derfor anbefales det aldrig at oprette forbindelse til et netværk, som ikke kræver adgangskode. Nedenfor ses et udsnit af foretrukne netværk, altså de Wi-Fi som enheden har været forbundet til tidligere, og det ses at flere offentlige Wi-Fi som f.eks. CPH-Business og Espresso House, ikke har angivet en sikkerhedsprotokol.



Det er altid muligt at se den sikkerhedsprotokol, som er angivet på det netværk man er forbundet til. Dette kan gøres på en Mac ved at holde option knappen nede, og trykke på Wi-Fi ikonet. På Windows kan det ses i Properties under Wi-Fi connection. Her ses både sikkerhedsprotokollen, den IP-adresse som enheden har fået tildelt, samt routerens lokale IP-adresse osv.

WPA2 Key Reinstallation Attack (KRACK)

I 2016 opdagede man en sikkerhedssvaghed i WPA2 protokollen, som gør det muligt for en hacker at opsnappe netværkstrafik på sårbare enheder eller AP's, der antages at være krypteret. Det angreb som udnytter denne svaghed kaldes Key Reinstallation Attack (KRACK), og udføres med det formål at kunne stjæle data der transporteres over netværket. KRACK angriber "The 4 Way Handshake"[6] som laves for at etablere de krypteringsnøgler, der anvendes

[6] Se bilag 1

til at kryptere trafikken mellem klient og AP. Dette skyldes at WPA2 er udviklet således at man hurtigere kan genoprette forbindelsen til et velkendt netværk, ved kun at udføre den tredje del af "The 4 Way Handshake". Efter den tredje del er gennemført vil klientens enhed installere den modtagne krypteringsnøgle. Dette kan forekomme flere gange, hvis ikke AP modtager en passende bekræftelse på modtagelse, for at sikre at forbindelsen er vellykket. Gentagelsen udgør den sårbarhed som kan udnyttes.

Dette gøres ved f.eks. at oprette et Fake AP eller en Evil Twin. Når en klient opretter forbindelse til dette AP, kan hackeren placere sig selv som man-in-the-middle. Under genoprettelsen af forbindelsen til netværket kan hackeren gentagne gange sende den tredje del af "The 4 Way Handshake" til klienten, som hver gang vil geninstallere den samme krypteringsnøgle, der således gradvist kan knækkes. Når krypteringsnøglen er blevet kompromitteret, kan hackeren opsnappe og dekryptere al data der transporteres mellem klienten og AP. Dette angreb vil ikke virke for websites der anvender SSL/TLS-kryptering, medmindre der anvendes SSL-Strip, der tvinger klienten til at tilgå HTTP versionen af disse websites. Det er vigtigt at pointere at KRACK ikke kan lade sig gøre, medmindre at hacker og klient er forbundet til det samme Wi-Fi, hvilket også er grunden til at offentlige Wi-Fi udgør en særlig risiko for denne type angreb.

I 2018 blev WPA3 protokollen introduceret, som skulle være med til bl.a. at eliminere sikkerhedssvagheden fundet på WPA2. WPA3 er endnu ikke særlig udbredt, da det kun er enheder produceret efter 2018 der er kompatible med denne protokol. Derfor er WPA2 fortsat den protokol som oftest anvendes.

How to prevent?

Vælger man som klient, at oprette forbindelse til et offentlig Wi-Fi, er der en række tiltag man bør overveje for at sikre sig mod de risici der er forbundet med dette. Herunder basale tiltag, som bl.a. at forhører sig om navnet på det netværk, man ønsker at tilgå, undersøge om netværket har en sikkerhedsprotokol angivet, kun at besøge hjemmesider, der anvender HTTPS, slå fildeling fra samt at logge af sin konto, når man ikke længere behøver at være logget ind.

Det anbefales ikke at have Wi-Fi til auto-connect og generelt ikke have Wi-Fi eller Bluetooth til, hvis man ikke benytter sig af dem. Desuden anbefales det at undgå at besøge hjemmesider, der indeholder sensitive informationer, som f.eks. Netbank. Vil man sikre sig yderligere, er der andre mere tekniske tiltag man bør overveje. Disse vil blive uddybet i dette afsnit.

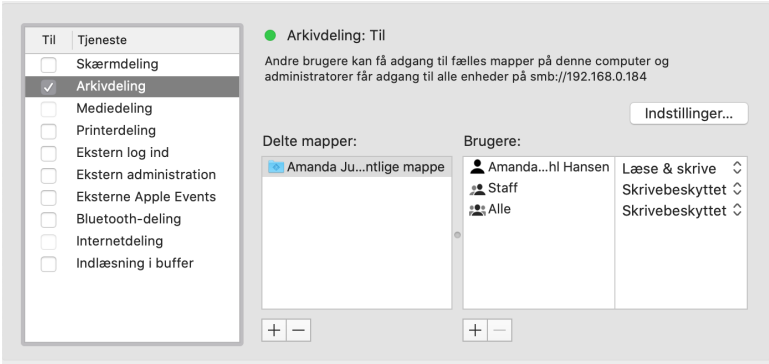
Fildeling TIL/FRA

På alle computere findes der en "public folder", som bruges til at dele filer/dokumenter med andre brugere på enten samme computer, eller klienter på samme netværk. Hvis fildeling er

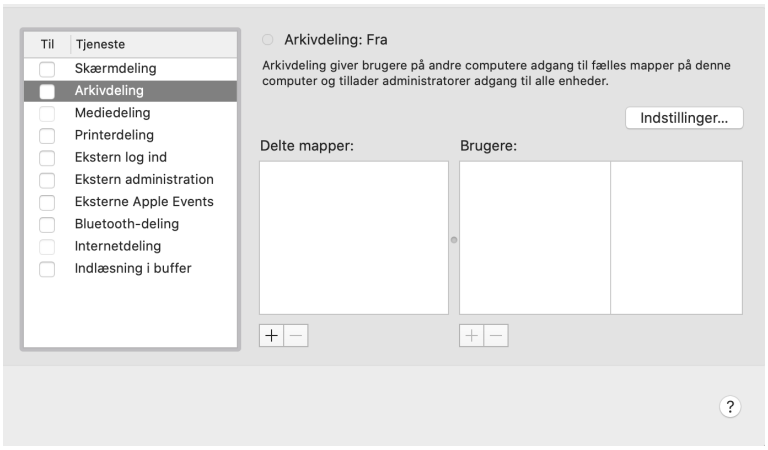
slået til, betyder det konceptuelt at alle på netværket, kan tilgå denne "public folder" og se de filer der findes i mappen. Det er i sig selv ikke betydeligt farligt, men har klienten lagt private dokumenter ind i mappen, vil disse potentielt set kunne ende i hænderne på en fremmed person, der befinder sig på det samme offentlige netværk. For at undgå at private dokumenter eller andet deles med fremmede, anbefales det at slå fildeling fra. Dette er også med til at beskytte mod malware distribution som f.eks. worm attack.

For at slå fildeling fra på MacBook

1. → Systemindstillinger → Deling → Arkivdeling



2. Fjern ✓ ud fra arkivdeling, for at slå fildeling fra.



Firewall

En firewall fungerer som en dørmand, der kontrollere datatrafikken ind og ud igennem de mange porte, og kun det, som har fået tilladelse, får lov til at passere. En firewall er altså med til at blokere alle uautoriserede forbindelser til og/eller fra enheden.

Der findes både hardware- (network-based) og software- (host-based) firewalls. Som oftest er der en hardware firewall inkorporeret i et stykke hardware, f.eks. en router. Denne type

firewall blokerer normalt kun for indgående trafik på netværket, hvilket vil sige at alle porte vil være lukket, med undtagelse af dem som man selv åbner. Dog vil der typisk være få porte som er åbne på forhånd, f.eks. portene til at modtage e-mails og besøge hjemmesider. En software firewall installeres på selve enheden og vil som udgangspunkt kun stoppe indgående trafik til enheden, men ikke udgående trafik. Dette vil man som regel, selv skulle sætte sin firewall op til. Grunden til at begge typer af firewalls kun er sat til at blokere for indgående trafik, er hovedsageligt at enheden ser sig selv som troværdig, og kun sender data ud med god intention.

Det anbefales at gøre brug af begge typer, eftersom at en software firewall kun vil beskytte den enkelte enhed, som har installeret denne. En hardware firewall installeret på f.eks. en router, vil beskytte de enheder, som begår sig på netværket. Da man ikke kan forvente at et offentligt Wi-Fi har en hardware firewall, bør man som udgangspunkt have en software firewall, for at begå sig mere sikkert på det offentlige Wi-Fi.

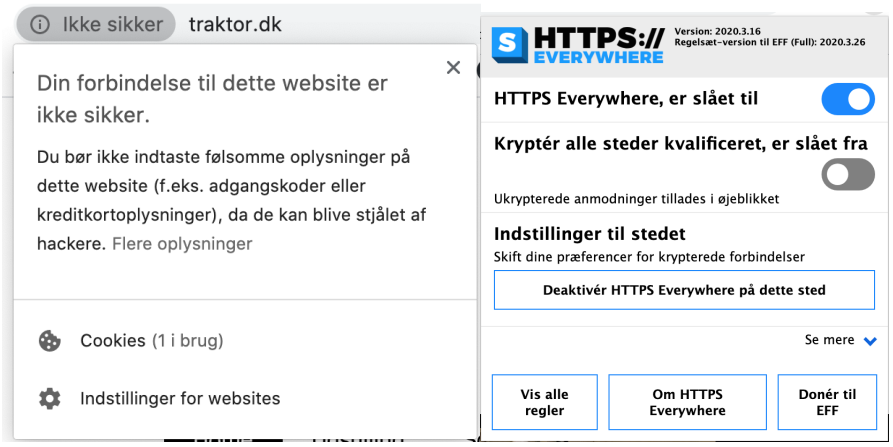
Hvis en uvidende klient tilgår et offentligt Wi-Fi igennem et Fake Access Point, ville klienten stadig være udsat for eventuelt ondsindet indgående trafik, selvom routeren har en hardware firewall installeret. Dette skyldes at hackeren ville være man-in-the-middle mellem klienten og routeren, og derfor bør klientens enhed være sat op med en software firewall. Dette betyder ikke at en hardware firewall er ubrugelig, f.eks. hvis en hacker forsøger at sprede et worm-attack på et netværk, gennem en åben port, som f.eks. en e-mail. Hardwarefirewallen på routeren vil forhindre den indgående trafik, fra den inficerede klient, i at sprede sige videre til de øvrige klienter på det samme offentlige netværk. Da det er udvist om opsætningen af et offentligt netværk inkludere en hardware firewall, anbefales det som minimum at have en software firewall installeret på sin enhed.

Force HTTPS

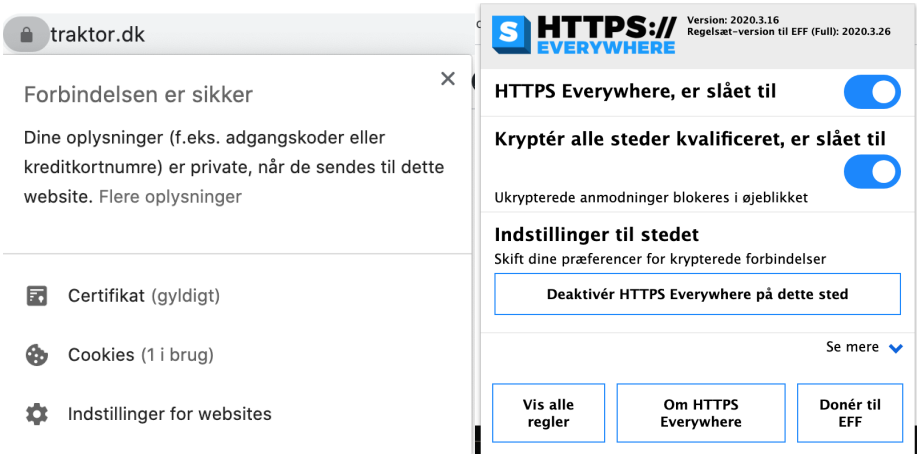
Hypertext Transfer Protocol Secure (HTTPS) beskytter trafikken mellem klienten og ressourcen ved at kryptere data, samt at anvende TLS til at verificere den anden ende af transaktionen. Dette kan være med til at sikre imod man-in-the-middle angreb på et offentligt netværk.

Selvom HTTPS er langt mere sikkert en HTTP, er der dog stadig visse sikkerhedsmæssige svagheder man bør tage højde for. HTTPS kryptere kun selve indholdet, og altså ikke de informationer, som er grundlæggende for selve transaktionen, herunder IP-adresser og port numre. Desuden er HTTPS langt fra idiotsikkert, da der er flere måder at omgå dette på, f.eks. ved at omdirigere til HTTP eller sende et falsk SSL-certifikat. Selvom klientens browser registrerer eventuelle manglende eller ugyldige certifikater, ignorere langt de fleste disse advarsler. Der findes dog en række udvidelser programmer til diverse browsere, som forcer HTTPS, og gør disse advarsler noget mere synlige. Nedenfor ses billeder af en Chrome browser, som har installeret "HTTPS Everywhere".

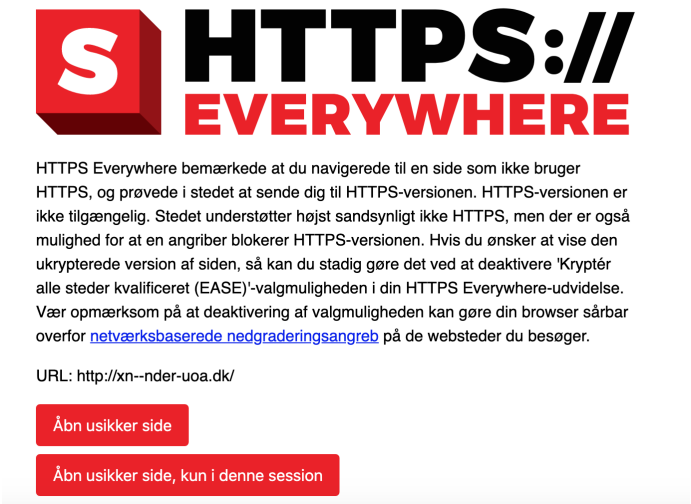
Her er udvidelsespakken deaktiveret.



Her er udvidelsespakken aktiveret.



Når udvidelsespakken er aktiveret, gives denne advarsel, hvis klienten forsøger at tilgå et website uden et gyldigt SSL-certifikat.



Ved at force HTTPS kan man som klient bl.a. beskytte sig selv mod WPA2 KRACK. Desuden vil SSL-krypteringen mindske muligheden for Network Sniffing og session hijacking, det er dog stadig er muligt at opsnappe forbindelsen mellem klient og server. Ikke alle websites har et SSL-certifikat og dermed heller ikke en HTTPS-version. Derfor vil dette tiltag ikke udelukkende være nok, hvis man ønsker at begå sig sikkert på et offentligt netværk. Man bør derfor kombinere dette med en VPN, bl.a. for at sikre en krypteret forbindelse, også på websites der ikke har et SSL-certifikat.

Virtual Private Network (VPN)

Ved at benytte en VPN kan man sikre sig mod mange af de risici der kan være forbundet med at være logget på offentlige Wi-Fi. De to mest grundlæggende fordele ved at anvende en VPN er sikkerhed og anonymitet. Langt de fleste VPN-tjenester krypterer forbindelsen mellem ressourcen og klientens enhed, hvilket er en effektiv beskyttelse mod eventuelle hackere. Privatliv er dog den helt store grund til at anvende en VPN. Dette skyldes at en VPN er med til at skjule klientens IP-adresse, som således ikke kan bruges af f.eks. internetudbydere eller hackere til logging af internetaktivitet. Det er altså ikke længere muligt når IP-adressen ikke kan spores tilbage til den egentlige klient.

Der bør tages højde for hvor nemt det er at blokere en VPN-tjeneste med en firewall. Det er i sig selv ikke et sikkerhedsproblem, at en VPN er nem at blokere. Det kan dog få klienter til at slukke for deres VPN, når de ikke kan tilgå den ressource de prøver at få adgang til. Det kunne f.eks. være at en skole ønskede at blokere for sociale medier og streaming tjenester på deres netværk. I den forbindelse kunne skolen også være interesseret i at blokere VPN-tjenester, da man ved hjælp af en VPN kan omgå skolens firewall og få adgang. Blokering af VPN-tjenester gøres ved at blokere for trafik på de porte VPN-protokollerne anvender. Det vil sige at protokoller der anvender mere gængse porte som f.eks. 443, eller varierende porte, vil være sværere at blokere.

Når der oprettes forbindelse til internettet via en VPN, anvendes tunneling. Tunneling kan ikke alene betragtes som privat, medmindre det ledsages at kryptering af de datapakker som sendes. Krypteringsniveauet som anvendes, afhænger af den tunnel protokollen. Der findes en række forskellige VPN-protokoller der specificere de krypteringsalgoritmer og tunneling metoder, som en VPN-tjeneste anvender.

Point-To-Point Tunneling Protocol (PPTP)

PPTP er en af de ældste VPN-protokoller, og bruges til at oprette en forbindelse. Point-to-Point refererer til forbindelsen skabt af PPTP. Denne type forbindelse tillader at en klients enhed (point) kan tilgå et eksternt netværk (specifikt point) over internettet. Tunneling er den måde hvorpå en protokol er indkapslet i en anden protokol. I dette tilfælde er der tale om at Point-To-Point Protocol (PPP) der indkapsles i TCP/IP protokollen, som giver internetforbindelsen.

Det vil sige at der ikke skabes en direkte forbindelse, men i stedet at forbindelsen efterlignes, så klienten kan tilgå det eksterne netværk. Denne protokol anvender port 1723, som gør den nem at blokere med en firewall. PPTP er en af de nemmeste protokoller at konfigurer, eftersom at den udelukkende kræver et brugernavn, en adgangskode samt en serveradresse, for at kunne oprette forbindelse. Det er en af de hurtigste VPN-protokoller, på grund af det lave krypteringsniveau.

Layer 2 Tunneling Protocol (L2TP)

L2TP er en udvidelse af PPTP, som gør den mere sikker. Tunneling protokollen anvender User Datagram Protocol (UDP) igennem port 1701. Dette gør også denne protokol nem at blokere med en firewall. L2TP inkludere ikke kryptering og anvendes derfor i sammenhæng med en krypteringsprotokol. Som oftest anvendes Internet Protocol Security (IPsec), der både kryptere header og data i de sendte PPP datapakker. Modtageren skal være IPsec kompatibel, for at kunne dekryptere datapakkerne. IPsec anvender Advanced Encryption Standard (AES) algoritmen, og L2TP betragtes derfor som sikker, men grundet den øgede kryptering er denne protokol også langsommere end PPTP.

Secure Socket Tunneling Protocol (SSTP)

SSTP gør det muligt at transportere data gennem SSL. SSTP er udviklet af Microsoft og understøttes derfor kun af Windows. SSTP transportere PPP pakker, på samme måde som PPTP, men modsat PPTP bliver dette gjort gennem en sikker SSL/TLS-forbindelse. Dette skyldes at SSL/TLS udfører integritetskontrol, anvender en sikker nøgleudveksling og krypterer data. Udover at anvende SSL/TLS, kan SSTP også anvende AES kryptering, for at øge sikkerheden. På trods af dette betragtes denne protokol ikke for at være 100 % sikker, da SSL/TLS ikke nødvendigvis er open source. SSTP anvender ikke en fast port, men kan f.eks. anvende port 443, som er den samme port som HTTPS. Det er derfor svært at blokere for denne protokol med en firewall.

OpenVPN

OpenVPN kan bruges på alle platformer og anvender openSSL til kryptering og authentication. For at styrke forbindelsens sikkerhed, kan OpenVPN anvende AES, som er open source-kryptering. OpenVPN kan anvende UDP og TCP til transmission af datapakker, men modsat TCP, udfører UDP ikke fejlhåndtering, hvilket gør forbindelsen ustabil. Til gengæld er UDP langt hurtigere end TCP. OpenVPN vil derfor først forsøge at lave en UDP-forbindelse, hvis forbindelsen fejler, vil den derefter forsøge at skabe en TCP-forbindelse, for at sikre at alle pakker kommer frem. OpenVPN anvender en selvvalgt port, hvilket også gør denne protokol svær at blokere med en firewall. OpenVPN er anset for at være den bedste VPN-protokol, og er i dag også den mest populære.

NordVPN

Services som f.eks. NordVPN benytter OpenVPN, men tilbyder også andre sikkerhedsfeatures, som f.eks. double VPN. Double VPN vil sige at der serieforbindes to servere, som begge kryptere data. Hvis det første lag af kryptering er stærkt nok i sig selv, er der umiddelbart ingen sikkerhedsmæssig gevinst ved dobbelt kryptering, men omvendt skader det ikke. Det kan dog have indflydelse på forbindelseshastigheden.

Visse andre VPN-udbydere krypterer kun pakker, der indeholder sårbare data, som f.eks. brugernavn og adgangskode. Dette gør udbyderne for at optimere forbindelseshastigheden, men det medfører en mindre sikker forbindelse. Dette aspekt er væsentligt at tage højde for når man skal vælge en VPN-udbyder. Det at anvende en VPN vil ikke nødvendigvis være mere sikkert på et offentligt netværk, hvis ikke udbyderen anvender en sikker tunnel protokol og en stærk kryptering. Omvendt skal krypteringsniveauet heller ikke være højere end nødvendigt, da dette medfører en langsom forbindelse, uden gevinst.

Har en klient valgt en VPN med en sikker tunnel protokol, som f.eks. openVPN, vil klienten der sidder på et offentlig netværk, være beskyttet mod session hijacking. Det skyldes at den opsatte VPN vil kryptere al data, inklusiv en eventuel cookie, der sendes mellem serveren og klienten. Således er cookie ikke frit tilgængelig, for en potentiel hacker.
Den samme sikkerhed gør sig gældende når en potentiel hacker, anvender Sniffing eller har opsat et Fake AP/ Evil Twin, til at opsnappe de datapakker som transporteres over netværket. Selvom det er muligt for en potentiel hacker at opsnappe disse datapakker, vil det ikke være muligt at se selve indholdet eller den tilhørende information om klienten, som anvender en VPN.

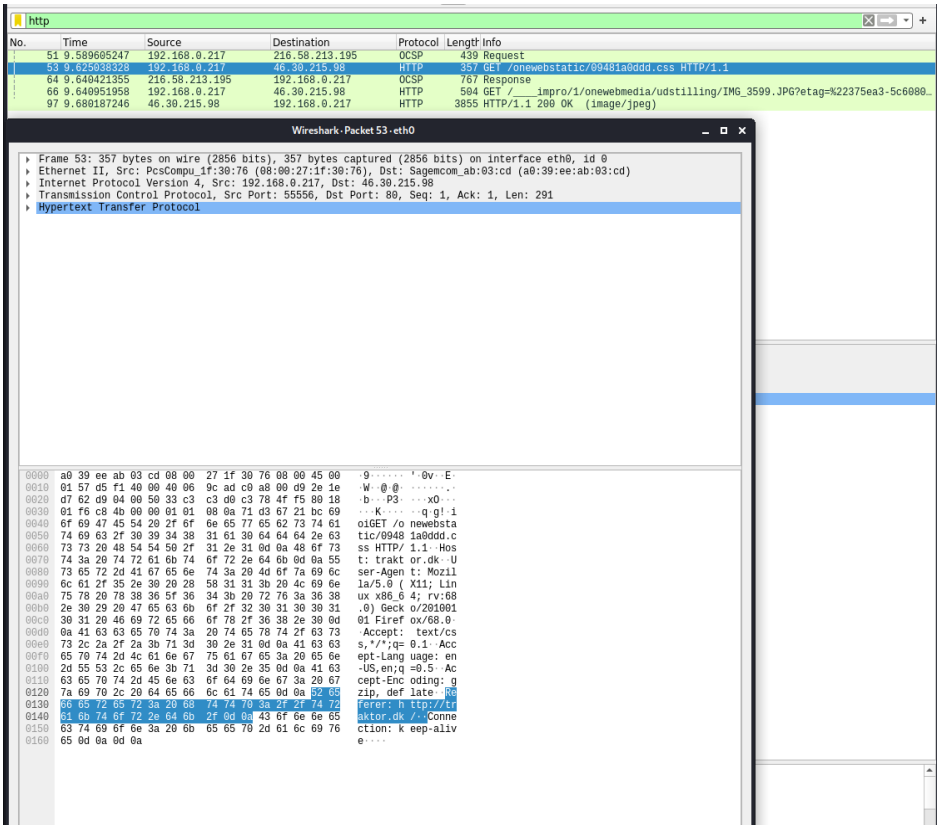
Med en VPN vil klienten altså være godt stillet, i forhold til potentielle hackere. Skulle klienten oprette forbindelse til et usikkert netværk, som ikke har angivet en sikkerhedsprotokol, vil dette være knap så risikabelt. Det skyldes at en VPN giver en sikker forbindelse og den nødvendige kryptering, alt afhængig af klientens VPN-udbyder. På trods af dette er det stadig ikke en god ide at oprette forbindelse til at usikkert netværk. Er det noget man ofte gør, bør man installere en VPN, som er det tiltag der beskytter klienten bedst i forbindelse med brug af offentligt netværk. Da det sikre mod et bredt spektrum af cyberangreb.

Praktisk eksempel: VPN

Vi har valgt at installere NordVPN på Kali Linux, for at kunne monitorere trafikken ved brug af WireShark. Denne VPN-udbyder anvender openVPN, som anses for at være den sikreste protokol. Når denne VPN anvendes, vil alle requests fra klienten blive sendt til VPN serveren, og derefter sendt videre til den ressource som klienten forsøger at tilgå. Det betyder at ressourcen ikke kan se klientens egentlige IP-adresse, men kun IP-adressen på den VPN, som anvendes mellem klienten og ressourcen.

Nedenfor ses et billede fra hjemmesiden https://minip.dk/. Her er internetudbyderen på det pågældende netværk Hiper A/S, og IP-adressen er 212.237.134.93, som er den eksterne IP-adresse på routeren. Derudover ses det at både IP-adressen og vores lokation, som er København, er offentligt tilgængeligt, og alt vores trafik på nettet betragtes derfor som værende usikker.

Uden en VPN har vi tilgået hjemmesiden www.traktor.dk, der bruger HTTP, som kan ses på nedenstående billede. Vores IP-adresse 192.168.0.217, er den IP-adresse der er tildelt enheden på det lokale netværk. Ved at kigge på requests fra denne, kan det ses at pakkerne indeholder plaintext. Vi kan aflæse at den søgte ressource har "Host: traktor.dk" og samtlige headere er læselig. F.eks. at operativsystemet er Linux, at forbindelsen er keep-alive og at der er tale om et GET-request.

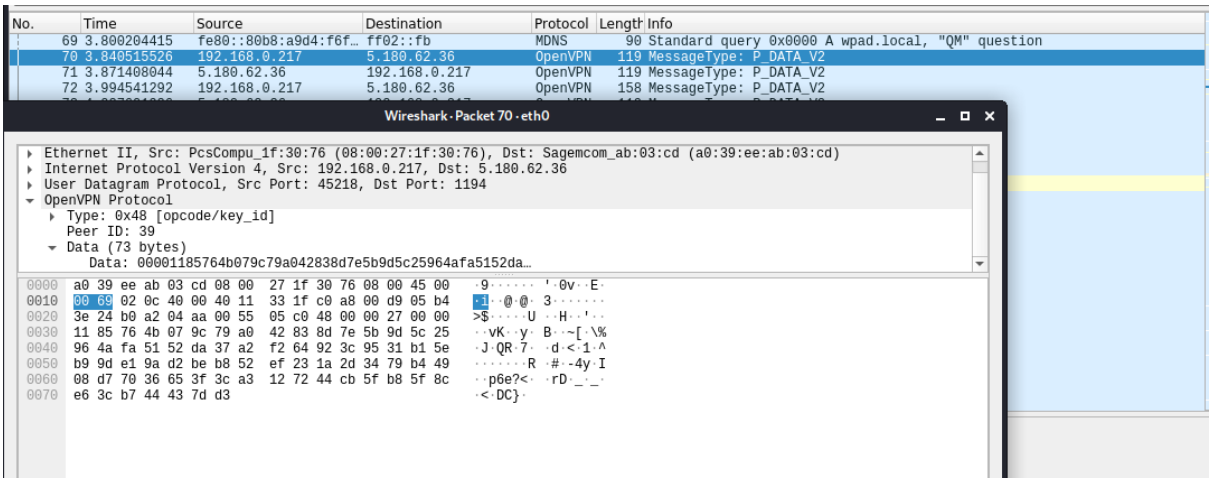


Herefter har vi tændt for vores VPN, som er forbundet til en VPN server i Frankfurt i Tyskland, og vi vil nu forsøge at tilgå samme hjemmeside, som før.

```
kali@kali:~$ nordvpn connect Germany Frankfurt
Connecting to Germany #799 (de799.nordvpn.com)
You are connected to Germany #799 (de799.nordvpn.com)!
kali@kali:~$
```

Det ses på nedenstående billede at IP-adressen nu er 5.180.62.37 og at den er lokaliseret i Gelsenkirchen, som er en by i Tyskland nær Frankfurt. Det kan altså ses at vores VPN nu har skabt en sikker forbindelse ved brug af tunneling, samt at den skjuler vores oprindelse /IP-adresse for den ressource vi tilgår.

På nedenstående billede, kan vi ligesom før se requests sendt fra vores enhed. Før vi tændte for vores VPN, var HTTP og Online Certificate Status Protocol (OCSP) angivet under protokolfanen, men med VPN'en tændt, angives kun OpenVPN. Desuden ses det at hvor destination før var den ressource vi forsøgte at tilgå, er destinationen nu IP-adressen på VPN-serveren. Således skjuler VPN'en ikke kun vores IP-adresse for ressourcen, men de ressourcer vi forsøger at tilgå, er også skjult for en potentiel hacker. Udover at skjule vores destination, kunne host og headers før aflæses i plain tekst, men nu er alt indholdet af pakkerne krypteret.



Konklusion

Vi kan på baggrund af denne rapport konkludere, at der er mange sikkerhedssvagheder forbundet med at begå sig på internettet, og at man som klient på et offentligt Wi-Fi er særligt udsat for disse. Dette skyldes især, at folk er splittet mellem brugervenlighed og sikkerhed. Generelt er det helt almindeligt at folk har Wi-Fi og Bluetooth slået til, når det ikke er i brug, og vi bekymrer os heller ikke over, at fildeling eller auto-connect på Wi-Fi er slået til eller om det netværk vi opretter forbindelse til, er usikkert. Folket ved langt fra nok om, hvilke konsekvenser dette kan have og hvilke tiltag man selv kan gøre, for at begå sig sikkert på et offentligt Wi-Fi.

Ved at force HTTPS og sætte en software firewall op på sin enhed, samt slå fildeling fra, har man som klient beskyttet sin enhed godt. Sikkerhed er dog ikke det samme som anonymitet, som er det en VPN tilbyder. Udover at en VPN er det tiltag der enkeltstående, giver den mest omfavnende beskyttelse, er det også det tiltag der går mest på kompromis med brugervenlighed. Spørgsmålet om en VPN gør en klient mere sikker på et offentligt Wi-Fi, bliver dog mere gråtonet, hvis man tager valget af tunneling protokol, krypterings -algoritme og -omfang i betragtning. Når en klient anvender en VPN, bliver klientens færden skjult med tunneling. En VPN er med til at skabe privatliv på nettet, men kan skabe et tillidsdilemma, da klientens VPN-udbyder stadig kan monitorere netværkstrafikken. Derfor er man ikke nødvendigvis sikret bare fordi man bruger en VPN. Man bør tage stilling til hvilken udbyder man vælger, samt hvilke tunneling- og krypteringsprotokoller de tilbyder.

Præsident Donald Trump underskrev mandag den 11. maj, en lov, der forhindrer privacy regler, der blev vedtaget sidste år, i at træde i kraft. Disse regler, ville forhindre internetudbydere i at sælge klienters browserdata. Ophævelsen af reglerne gør det muligt for internetudbydere, som Comcast og Verizon, at samle og sælge data om klienters browserhistorik til marketingfolk og andre virksomheder. Herunder oplysninger om geografisk placering, økonomisk status og hvad folk køber og søger efter[7].

Med ophævelsen af loven, vil det ikke længere kun være hackere vi bør bekymre os om, men også internetudbydere. Det betyder at man både kan risikere at blive overvåget på offentlige Wi-Fi, men nu også på ens eget private netværk, og at man potentielt set også kan være nødsaget til at benytte en VPN derhjemme, for at være anonym. Selvom det også er muligt for en VPN-udbyder at overvåge ens internetaktivitet, er det således langt bedre, end alternativet.

[7] Kilde: 13.1

Kildeliste

1. Indledning
   1.1. https://www.informationsecuritybuzz.com/articles/the-insecurities-of-public-wi-fi/

2. Malware distribution - Worm Attack
   2.1. https://thehackernews.com/2020/02/emotet-malware-wifi-hacking.html
   2.2. https://smallbusiness.chron.com/can-viruses-spread-over-wifi-75136.html

3. Session Hijacking
   3.1. https://www.hacker9.com/sidejacking-wifi-cookie.html
   3.2. https://www.welivesecurity.com/2010/11/09/cookie-theft-sidejacking-or-session-hijacking-for-normal- people/
   3.3. https://www.techopedia.com/definition/4105/sidejacking

4. Network Sniffing
   4.1. https://www.avg.com/en/signal/what-is-sniffer
   4.2. https://www.lifewire.com/what-is-a-packet-sniffer-2487312
   4.3. https://www.skillset.com/questions/how-is-sniffing-usually-categorized

5. Rogue Wi-Fi Access Points
   5.1. https://www.netkablet.dk/access-point/

6. Fake Access Points og Evil Twins
   6.1. https://www.webtitan.com/blog/most-common-wireless-network-attacks/
   6.2. https://thecybersecurityman.com/2018/08/11/pentest-edition-creating-an-evil-twin-or-fake-access-point-using-aircrack-ng-and-dnsmasq-part-1-setup/

7. WEP og WPA
   7.1. https://www.makeuseof.com/tag/tell-what-security-type-wi-fi-is/
   7.2. https://www.lifewire.com/what-are-wep-wpa-and-wpa2-which-is-best-2377353
   7.3. https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/
   7.4. https://www.cloudflare.com/learning/security/what-is-a-krack-attack/
   7.5. https://www.skillset.com/questions/how-is-sniffing-usually-categorized
   7.6. https://arstechnica.com/information-technology/2017/10/severe-flaw-in-wpa2-protocol-leaves-wi-fi-traffic-open-to-eavesdropping/
   7.7. https://www.csoonline.com/article/3246984/why-you-should-never-ever-connect-to-public-wifi.html
   7.8. https://www.howtogeek.com/339765/what-is-wpa3-and-when-will-i-get-it-on-my-wi-fi/

8. WPA2 Key Reinstallation Attack (KRACK)
   8.1. https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html
   8.2. https://www.inc.com/comcast/risks-of-using-public-wifi.html
   8.3. https://www.joe0.com/2017/11/11/kali-linux-virtualbox-instructions-for-testing-wi-fi-devices-against-wpa2-key-reinstallation-attack-krack-attack/
   8.4. https://medium.com/@alonr110/the-4-way-handshake-wpa-wpa2-encryption-protocol-65779a315a64

9. Fildeling TIL/FRA
   9.1. https://eu.usatoday.com/story/tech/columnist/2017/08/18/one-mistake-people-make-using-public-wi-fi/577791001/

10. Firewall
   10.1. https://www.digitalocean.com/community/tutorials/what-is-a-firewall-and-how-does-it-work
   10.2. https://www.webopedia.com/DidYouKnow/Hardware_Software/firewall_types.asp

11. Force HTTPS
   11.1. https://www.cloudwards.net/dangers-of-public-wifi/
   11.2. https://chrome.google.com/webstore/detail/https-everywhere/gcbommkclm-clpchllfjekcdonpmejbdp?hl=da
   11.3. https://www.cloudwards.net/http-vs-https/

12. VPN
   12.1. https://techterms.com/definition/pptp
   12.2. https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-sstp/
   12.3. https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-openvpn/
   12.4. https://vpninfo.dk/vpn/nordvpn/
   12.5. https://www.techradar.com/vpn/vpn-tunnels-explained-how-to-keep-your-internet-data-secure
   12.6. https://www.vpnoneclick.com/types-of-vpn-and-types-of-vpn-protocols/

13. Diskussion/konklusion
   13.1. https://www.zdnet.com/article/trump-signs-into-law-privacy-killing-rules-that-let-isps-sell-your-browsing-history/

14. Generelt

14.1. https://www.wikihow.com/Be-Safe-When-Using-WiFi

14.2. https://www.professionalsecurity.co.uk/products/computer-systems-and-it-security-news/dangers-of-using-public-wifi/

14.3. https://www.dignited.com/34393/5-security-risks-of-using-public-wi-fi/

14.4. https://bdtechtalks.com/2017/02/28/public-wifi-security-threats/

14.5. https://www.wikihow.com/Be-Safe-When-Using-WiFi

14.6. https://www.drivers.com/update/security-backup/public-wifi-security/

14.7. https://www.dignited.com/34413/public-wifi-102-staying-safe-on-public-networks/

14.8. https://us.norton.com/internetsecurity-wifi-the-dos-and-donts-of-using-public-wi-fi.html

Bilag

Bilag 1 - The 4 way handshake8

The 4 way handshake (håndtrykket), er en betegnelse for de første fire meddelelser i krypterings forbindelsens processen, mellem klienten, der ønsker at oprette forbindelse til Wi-Fi, og AP. For at kunne forstå disse 4 stadier i processen er det vigtigt at forstå de nøgler som processen omhandler.

Pairwise Master Key (PMK)

Når vi taler om WPA/WPA2 er PMK det samme som Pre-Shared key (PSK). Dette er den passphrase eller adgangskode som vi giver vores netværk. Altså den kode vi angiver når vi opretter forbindelse til et netværks AP. PSK/PMK er adgangskoden oversat til en 256 bit streng.

Group Master Key (GMK)

GMK er en fast streng baseret på AP'ets MAC-adresse samt GNonce (et tilfældigt tal).
Denne nøgle bruges til at generere The Group Temporal Key.

Group Temporal Key (GTK)

GTK genereres for hvert AP, og på baggrund af GMK. Denne nøgle består af 128 bits ved CCMP og 256 bits for TKIP, og deles med alle de enheder der er forbundet til AP. GTK anvendes til at kryptere broadcast og multicast trafik mellem klient og AP. Alle enheder der er forbundet til det samme AP har den samme GTK.

ANONCE og SNONCE

Nonce er et vilkårligt tal, der kan bruges i kryptografisk kommunikation. Det er bogstaveligt talt nonsens, deraf navnet. Dette er ofte tilfældigt eller pseudo-tilfældigt, og anvendes i authentication protokoller. I dette tilfælde er ANonce nonce som AP har genereret og SNonce er nonce som klienten har genereret.

Pairwise Transit Key (PTK)

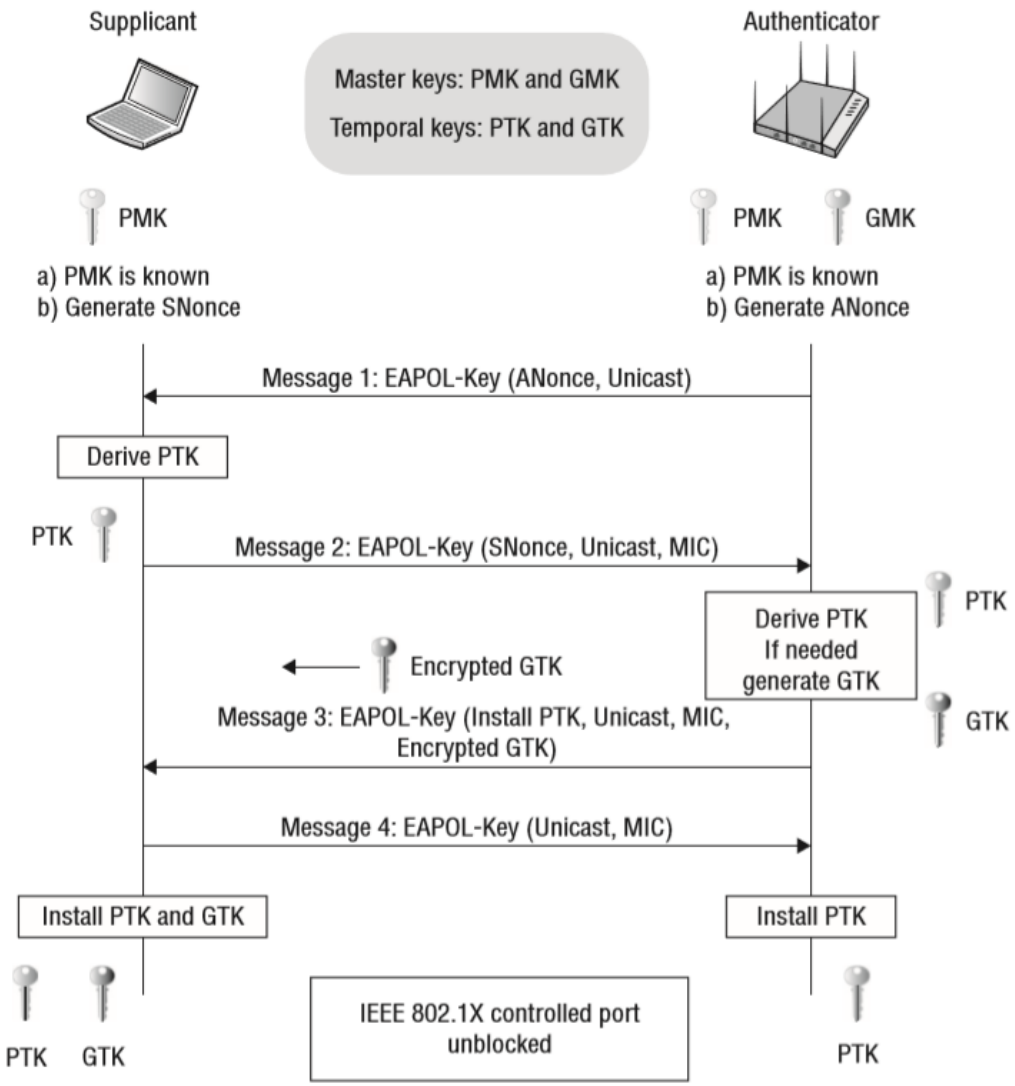
PTK anvendes til kryptering af unicast trafik mellem klient og AP. For at generere denne krypteringsnøgle kræves flere parametre:
PTK = PMK + ANonce + SNonce + MAC (AP) + MAC (klient)
Ved håndtrykket anvendes PTK til at kryptere GTK.

Message Integrity Code (MIC)

MIC er et synonym for Message Authentication Code (MAC), for ikke at forveksle det med MAC-adresser. MIC/MAC er et kort stykke information, der bruges til at autentificere en meddelelse

[8] Kilde: 8.4

- med andre ord bekræfte at meddelelsen kommer fra den angivne afsender, at indholdet ikke er blevet ændret, samt meddelelsens ægthed. Nedenfor ses en grafisk repræsentation af håndtrykket, som kan aflæses således.



1. AP sender sin ANonce til klienten, som nu kan generere PTK, eftersom at de resterende parametre er kendte i forvejen.
2. Klienten sender herefter sin SNonce, samt MIC som signatur, til AP som nu også kan generere PTK.
3. AP kryptere herefter GTK, med den genererede PTK, og sender denne samt MIC til klienten. Klienten kan nu installere den modtagede GTK.
4. Klienten sender MIC, som bekræftelse på den modtagede GTK.

Når håndtrykket er fuldført, vil AP havde installeret den nye generede PTK, og klienten vil have installeret PTK samt GTK, således at trafikken mellem klient og AP nu kan krypteres.