



# Säkerhetsrisker i öppna Wi-Fi-nätverk

<b>Namn</b>	Simon Arnar & Jessie Mårtensson
<b>Utbildning</b>	.NET-Utvecklare 23-25
<b>Datum</b>	25/5-2025

## Sammanfattning

Detta examensarbete undersöker praktiska sårbarheter i Wi-Fi-nätverk, med fokus på Evil Twin-attacker och Deauthentication-attacker. Syftet är att belysa hur angripare kan utnyttja svagheter i Wi-Fi-protokollet för att avlyssna datatrafik samt att utvärdera hur tekniker som VPN kan kryptera trafiken och därmed effektivt skydda mot dataläckage i osäkra nätverk under förutsättning att VPN-tjänsten är korrekt konfigurerad och aktiv.

Arbetet har genomförts med en kvalitativ och induktiv ansats, där praktiska tester utförts i en kontrollerad testmiljö. Med hjälp av verktyg som Wireshark, tcpdump och en egenutvecklad WiFi Pineapple-klon simulerades attacker mot klienter anslutna till fördefinierade Wi-Fi-nätverk. Fokus låg på att observera vilka typer av data som kunde fångas upp.

Resultaten visar att både Evil Twin- och Deauthentication-attacker är relativt enkla att genomföra med lättillgängliga verktyg och begränsad teknisk kunskap. Testerna visade att utan kryptering skickas känslig information ofta i klartext, medan användning av VPN effektivt förhindrade insyn i trafiken. Arbetet belyser även strukturella svagheter i Wi-Fi-protokollet, särskilt användningen av okrypterade management-ramar, samt vikten av att implementera skydd som WPA3, 802.11w och säkra användarvanor.

# Innehåll

1. Inledning.....	5
1.1 Bakgrund .....	6
1.2 Syfte.....	7
1.3 Problemformulering.....	7
1.4 Avgränsningar och fokus .....	7
1.5 Metod.....	8
1.5.1 Syfte och angreppssätt .....	8
1.5.2 Testmiljö och utrustning .....	8
1.5.3 Planerade tester.....	9
1.5.4 Etiska överväganden .....	9
2. Teori .....	10
2.1 Wi-Fi-teknologi och sårbarheter .....	10
2.1.1 Uppkomsten av Wi-Fi-teknologin .....	10
2.1.2 Wi-Fi-teknologin.....	11
2.2 Cyberattacker .....	11
2.2.1 Deauthentication Attack.....	11
2.2.2 Evil Twin Attack.....	12
2.3 Säkerhetsteknik och skyddsåtgärder .....	13
2.3.1 WEP .....	13
2.3.2 WPA .....	13
2.3.3 WPA2.....	14
2.3.4 WPA3.....	14
2.3.5 SSL / TLS.....	15
2.3.6 VPN.....	15
2.4 Informationssäkerhet.....	16
2.4.1 CIA-triaden.....	16
3. Empiri/iakttagelser .....	17
3.1 Empiri: Evil Twin Attack (iPhone).....	17
3.1.1 Testmiljö .....	17
3.1.2 Procedur.....	17

4. Analys av resultatet.....	21
4.1 Tekniska sårbarheter i Wi-Fi.....	22
4.2 Hur fungerar Evil Twin-attacker i praktiken.....	22
4.3 Verktygens tillgänglighet .....	23
4.4 Skyddsåtgärder mot attacker.....	24
4.5 Hur användare kan minska risken att bli utsatt .....	25
4.6 Validitet och reliabilitet.....	26
5. Slutsatser .....	26
5.1 Rekommendationer.....	27
6. Referenslista .....	29

# 1. Inledning

I dagens uppkopplade samhälle är Wi-Fi (Wireless Fidelity) den vanligaste metoden för trådlös internetanslutning på offentliga platser, såsom caféer, flygplatser och bibliotek. Wi-Fi-tekniken är utformad för att erbjuda smidig och snabb åtkomst till internet, men denna tillgänglighet medför även betydande säkerhetsrisker, särskilt i öppna nätverk där ingen autentisering krävs.

En vanlig metod som angripare använder är att sätta upp ett falskt Wi-Fi-nätverk som efterliknar ett till synes harmlöst nätverk, ofta på en allmän plats. När användare ansluter till det falska nätverket, ofta utan att märka någon skillnad, kan angriparen börja övervaka datatrafiken och i vissa fall fånga upp känslig information.

En global undersökning visar att sex av tio pendlare använder internet, och att lika många av dessa åtminstone ibland kopplar upp sig mot offentliga Wi-Fi-nätverk ([URL1](#)). Detta bekräftar att uppkoppling mot offentliga nätverk är vanligt, vilket medför en ökad risk för cyberattacker.

Eftersom många användare saknar kunskap om de säkerhetsrisker som är förknippade med dessa nätverk har vi valt att fördjupa oss i cybersäkerhet, med särskilt fokus på Wi-Fi-nätverk som använder radiovågor på 2,4 GHz-bandet. Det är ett område som ofta förbises, trots kända tekniska sårbarheter. Genom att kombinera teori med ett eget tekniskt projekt vill vi belysa dessa risker och öka medvetenheten kring dem.

## 1.1 Bakgrund

I takt med att digitaliseringen har ökat har vårt beroende av trådlösa nätverk blivit allt större. Wi-Fi-nätverk används i dag både i hemmet, på arbetsplatser och på offentliga platser, där de ofta delas av många användare eller är helt öppna.

Trots att många har tillgång till obegränsad mobildata väljer vissa fortfarande att ansluta till offentliga Wi-Fi-nätverk av bekvämlighets- eller kostnadsskäl, särskilt på enheter utan SIM-kort, exempelvis bärbara datorer. Detta medför säkerhetsrisker eftersom användaren sällan vet vem som faktiskt kontrollerar nätverket.

En grundläggande svaghet i Wi-Fi-tekniken är att den bygger på radiovågor. Det innebär att signalerna inte begränsas till enbart den avsedda mottagaren. Alla enheter inom räckhåll kan potentiellt fånga upp kommunikationen, vilket möjliggör olika typer av cyberattacker.

Exempel på sådana attacker är Deauthentication-attacker, där användare tvingas kopplas bort från nätverket, samt Evil Twin-attacker, där en angripare skapar ett falskt nätverk som imiterar ett legitimt för att lura användare att ansluta. Dessa metoder kan användas för att stjäla inloggningsuppgifter, övervaka datatrafik eller störa kommunikationen genom att utnyttja sårbarheter i Wi-Fi-protokollet.

I detta examensarbete undersöker vi säkerhetsriskerna i offentliga Wi-Fi-nätverk genom att kombinera teoretisk förståelse med ett praktiskt projekt. Vi har byggt en enklare version av det kommersiella verktyget WiFi Pineapple med hjälp av en billig mini-router (GL.iNet Mango), externa Wi-Fi-adaptrar samt en öppen källkodsklon tillgänglig via GitHub.

WiFi Pineapple är i grunden utvecklat för att genomföra säkerhetstester och simulera attacker i kontrollerade miljöer, exempelvis inom penetrationstester och utbildningssyfte. Syftet är att identifiera och åtgärda sårbarheter i trådlösa nätverk.

Sådana verktyg används tyvärr även ibland för otillåtna syften, vilket gör det ännu viktigare att förstå hur dessa attacker fungerar, hur lättillgängliga verktygen är och vilka säkerhetsåtgärder som krävs för att förebygga dem.

## 1.2 Syfte

Syftet med denna rapport är att belysa de säkerhetsrisker som finns i öppna Wi-Fi-nätverk som använder radiovågor på 2,4 GHz-bandet. Vi strävar efter att öka förståelsen för dessa hot, särskilt i samband med offentliga och okrypterade nätverk, som är vanligt förekommande. Genom denna undersökning hoppas vi kunna bidra till ökad medvetenhet och ett säkrare användande av trådlösa nätverk.

## 1.3 Problemformulering

1. Vilka tekniska sårbarheter i Wi-Fi-nätverk möjliggör dessa attacker?
2. Hur fungerar attacker som Deauthentication och Evil Twin i praktiken?
3. Hur lättillgängliga är de verktyg som krävs för att genomföra sådana attacker?
4. Vilka försvar eller skyddsåtgärder finns det mot dessa attacker?
5. Hur kan man som användare minska risken att bli utsatt?

## 1.4 Avgränsningar och fokus

I detta examensarbete fokuserar vi uteslutande på säkerhetsrisker i öppna Wi-Fi-nätverk som använder 2,4 GHz-frekvensbandet. Särskild tonvikt läggs vid Deauthentication- och Evil Twin-attacker. Andra former av cyberattacker, såsom ransomware, phishing eller angrepp mot trådbundna nätverk, omfattas inte av studien.

Inte heller mobilnätverk (exempelvis 3G, 4G eller 5G) eller företagsnätverk med avancerade säkerhetslösningar ingår i arbetet. Studien är avgränsad till attacker i en kontrollerad testmiljö, där vi använder en enklare klon av WiFi Pineapple. Syftet är inte att genomföra avancerade penetrationstester, utan att demonstrera hur förhållandevis enkla vissa attacker kan vara att genomföra samt vad användare kan göra för att skydda sig.

## 1.5 Metod

I detta examensarbete används en kvalitativ och induktiv ansats där praktiska tester mot egna Wi-Fi-nätverk genomförs först, varefter resultaten tolkas mot vald teori. Testerna utförs i en kontrollerad miljö, med fördefinierade SSID och kanaler för att undvika störningar, och dokumenteras genom paketfångst (Wireshark/tcpdump) och skärmdumpar från vår WiFi Pineapple-klon. Syftet är att observera och förstå hur Evil Twin-attacker fungerar i praktiken samt hur VPN kan förhindra att okrypterad information läcker vid anslutning till osäkra nätverk.

### 1.5.1 Syfte och angreppssätt

Vårt mål med testerna är att undersöka hur enkelt det är att genomföra vissa typer av cyberattacker mot Wi-Fi-nätverk med relativt billig och lättillgänglig utrustning. Vi vill även fördjupa vår förståelse för hur dessa attacker fungerar i praktiken, samt undersöka vilka åtgärder som kan vidtas för att skydda sig mot dem.

Eftersom syftet med vårt examensarbete är att förstå och förklara dessa angreppssätt snarare än att kvantifiera dem, har vi valt att arbeta med en kvalitativ metodansats. Vi utgår från observationer och dokumentation snarare än mätdata. Vi använder dessutom en induktiv metod, där vi testar i praktiken först och kopplar till teori efteråt.

### 1.5.2 Testmiljö och utrustning

Alla tester genomförs i en kontrollerad miljö mot våra egna nätverk och enheter, utan att påverka tredje part. Vi specificerar manuellt SSID och kanal för att säkerställa att inga andra nätverk störs eller påverkas under våra tester.

De primära verktyg vi använder är:

- **MangoApple:** vår egenbyggda Pineapple-klon baserad på en GL.iNet Mango-router och öppen mjukvara från GitHub.
- **Wi-Fi-adaptrar:** vi använder externa USB-adaptrar som stöder både monitor mode och packet injection, vilket är nödvändigt för att genomföra Deauthentication-attacker och för att avlyssna datatrafik.



För att analysera nätverkstrafik använder vi två verktyg:

- **Wireshark**, ett grafiskt analysverktyg för nätverkstrafik som gör det möjligt att visualisera och inspektera varje datapaket i detalj.
- **Tcpdump**, ett terminalbaserat verktyg som används för att fånga och spara trafik direkt från nätverksgränssnittet, vilket sedan kan analysera vidare i Wireshark.

### 1.5.3 Planerade tester

De attacktyper vi fokuserar på är:

- **Deauthentication-attacker:** för att störa ut anslutningen mellan enheter och åtkomstpunkter.
- **Evil Twin-attacker:** där vi skapar ett falskt nätverk med samma SSID som ett legitimt, för att se om enheter automatiskt ansluter.

Tester dokumenteras genom skärmdumpar från Pineapple-klonens gränssnitt, uppkoppling av våra egna enheter till falska nätverk, samt trafikövervakning över HTTP för att analysera eventuell okrypterad data. Vi använder även verktygen tcpdump och Wireshark för att inspektera paket och innehåll på nätverksnivå.

### 1.5.4 Etiska överväganden

Vi är medvetna om det etiska ansvar som följer med ett arbete inom IT-säkerhet. Därför genomförs samtliga tester enbart på våra egna nätverk och enheter. Inga attacker riktas mot andra användare eller nätverk.

Projektets syfte är att utbilda och öka medvetenheten om de risker som finns i publika nätverk – inte att utföra skadliga handlingar. Vi kommer i analys- och resultatdelen att belysa hur lätt det är att utsättas för attacker, men även vad man kan göra för att skydda sig, exempelvis genom VPN eller medvetna val av nätverk.

## 2. Teori

I detta kapitel presenteras den teoretiska grunden för examensarbetet. Fokus ligger på Wi-Fi-teknologins funktion och sårbarheter, vanliga cyberattacker samt de säkerhetsåtgärder som finns för att skydda trådlösa nätverk. Kapitlet avslutas med en introduktion till grundläggande principer inom informationssäkerhet.

### 2.1 Wi-Fi-teknologi och sårbarheter

I detta avsnitt beskrivs Wi-Fi-teknologins framväxt och tekniska grund, med särskilt fokus på Wi-Fi-nätverk som använder 2,4 GHz-frekvensbandet.

#### 2.1.1 Uppkomsten av Wi-Fi-teknologin

Hedy Lamarr var en av upphovspersonerna bakom den teknologi som i dag utgör grunden för bland annat Wi-Fi. Under andra världskriget ville hon bidra till de allierade styrkorna och undersökte därför möjliga militära tillämpningar av radioteknik ([URL2](#)).

År 1942 patenterade Hedy Lamarr, tillsammans med George Antheil, ett system kallat "Secret Communication System", vilket möjliggjorde frekvenshoppning mellan 88 olika kanaler ([URL3](#)).

År 1997 utvecklades den första Wi-Fi-standarden av Institute of Electrical and Electronics Engineers (IEEE). Standarden fick namnet IEEE 802.11 och möjliggjorde trådlös dataöverföring med hastigheter upp till 2 Mbit/s via det olicensierade 2,4 GHz-bandet ([URL4](#)).

År 1999 lanserade Apple AirPort och iBook baserade på IEEE 802.11b-standarden, som tillät dataöverföring upp till 11 Mbit/s. Detta blev början på den trådlösa revolutionen. Genom åren har den fortlöpande utvecklingen av IEEE 802.11 Wi-Fi-standarden lett till snabbare dataöverföringshastigheter, längre räckvidd och förbättrad säkerhet ([URL5](#)).

### 2.1.2 Wi-Fi-teknologin

WLAN (Wireless Local Area Network) är ett lokalt nätverk som använder trådlös kommunikation för att ansluta enheter. En vanlig form av WLAN är Wi-Fi (Wireless Fidelity), vilket är den benämning som kommer att användas härnäst.

Wi-Fi är en trådlös nätverksteknik som, likt mobiltelefoner, TV-apparater och radioapparater, använder radiovågor för att överföra data mellan enheter och routrar via frekvenser ([URL6](#)). Överföringen sker vanligtvis via 2,4 GHz- eller 5 GHz-bandet, och teknologin är standardiserad genom IEEE (Institute of Electrical and Electronics Engineers) 802.11-serien, vilken utgör grunden för Wi-Fi-standarderna.

Wi-Fi-nätverk kan vara antingen öppna, vilket innebär att de inte kräver något lösenord för åtkomst, eller säkrade, där autentisering krävs ([URL7](#)). Denna undersökning kommer att fokusera på öppna Wi-Fi-nätverk som använder 2,4 GHz-frekvensbandet.

## 2.2 Cyberattacker

För att ge en tydlig förståelse av de säkerhetsproblem som kan uppstå i samband med Wi-Fi-nätverk, presenteras i detta avsnitt vanliga typer av cyberattacker och de säkerhetsrisker som är förknippade med dem. Vidare förklaras hur dessa attacker genomförs, med syfte att ge läsaren insikt i olika angreppsmetoder och därigenom underlätta identifiering av potentiella hot.

### 2.2.1 Deauthentication Attack

Deauthentication Attack är en typ av DoS-attack (Denial-of-Service) som stör kommunikationen mellan routrar och anslutna enheter. Attacken utnyttjar en sårbarhet i IEEE 802.11-standarden, vilken används i Wi-Fi-nätverk. Dessa nätverk är sårbara eftersom standarden tillåter användning av så kallade Deauthentication frames ([URL8](#)).

Attacken genomförs genom att angriparen skickar ett stort antal Deauthentication frames till en specifik åtkomstpunkt (t.ex. en router), vilket tvingar klienten att kopplas bort från nätverket. Detta är möjligt eftersom Deauthentication frames är formella instruktioner för fränkoppling. De är inte förfrågningar utan notifikationer, vilket innebär att de inte kan avvisas ([URL9](#)).

Denna attack används ofta i samband med en Evil Twin-attack för att tvinga användare att ansluta till en falsk åtkomstpunkt som angriparen kontrollerar.

### 2.2.2 Evil Twin Attack

Evil Twin Attack är en typ av MITM-attack (man-in-the-middle) där en angripare sätter upp en falsk åtkomstpunkt för Wi-Fi-nätverk. Målet är att få användare att ansluta till denna falska åtkomstpunkt i stället för den legitima åtkomstpunkten ([URL10](#)). När användare ansluter till den falska Wi-Fi-åtkomstpunkten kan angriparen övervaka nätverkstrafiken och därigenom få tillgång till känslig information, såsom inloggningsuppgifter. Eftersom många använder samma inloggningsuppgifter för flera tjänster kan detta snabbt leda till allvarliga konsekvenser. Evil Twin-attacker är svåra att upptäcka eftersom de har samma eller liknande SSID (Service Set Identifier) som det legitima Wi-Fi-nätverket.

Attacken genomförs ofta på platser med många människor, exempelvis caféer, flygplatser och bibliotek, där gratis och öppna Wi-Fi-nätverk är vanliga. Det är också vanligt att flera nätverk med samma eller liknande namn förekommer, vilket gör det enkelt för en falsk Wi-Fi-åtkomstpunkt att förbli oupptäckt ([URL11](#)).

När en lämplig plats för attacken har identifierats, sätts en falsk Wi-Fi-åtkomstpunkt upp med samma eller liknande SSID som det legitima Wi-Fi-nätverket som efterliknas ([URL12](#)). För detta kan olika typer av enheter användas, till exempel mobiltelefoner, laptops och WiFi Pineapple.

Många offentliga Wi-Fi-nätverk har en så kallad "Captive Portal Page" där användare i vissa fall måste ange inloggningsuppgifter för att få tillgång till nätverket. Angripare kan skapa kopior av dessa sidor och på så sätt få tillgång till användarens inloggningsuppgifter, eftersom användaren är uppkopplad till den falska Wi-Fi åtkomstpunkten utan att vara medveten om det och därmed blir övervakad ([URL13](#)). Det är däremot inte nödvändigt att skapa en falsk Captive Portal Page, eftersom inte alla offentliga Wi-Fi-nätverk använder sig av detta.

När angriparen har satt upp en falsk Wi-Fi-åtkomstpunkt och eventuellt en Captive Portal Page kan angriparen flytta sin enhet eller router närmare potentiella offer. Detta underlättar utförandet av cyberattacken eftersom offret då får en starkare signal från den falska Wi-Fi-åtkomstpunkten än från den legitima ([URL14](#)). Det tvingar dessutom vissa enheter att ansluta automatiskt, något som offret kanske inte märker eftersom enheten tidigare anslutit till vad den tror är det legitima Wi-Fi-nätverket.

Efter att användare har anslutit till den falska Wi-Fi-åtkomstpunkten kan angriparen övervaka och stjäla känslig information, såsom inloggningsuppgifter och bankuppgifter, om offret loggar in på exempelvis sociala medier eller banken. Därför är det viktigt att använda olika inloggningsuppgifter för olika tjänster, annars kan angriparen i princip få tillgång till allt genom ett enda inloggningsförsök.

## 2.3 Säkerhetsteknik och skyddsåtgärder

I detta avsnitt presenteras teorier och tekniker inom nätverkssäkerhet, med särskilt fokus på skydd mot de cyberattacker som beskrivits tidigare. Syftet är att ge läsaren en fördjupad förståelse för de skyddsåtgärder som finns tillgängliga för att stärka säkerheten i Wi-Fi-nätverk.

### 2.3.1 WEP

Wired Equivalent Privacy (WEP) är en del av IEEE 802.11-standarden (Institute of Electrical and Electronics Engineers) och introducerades 1997 som det första försöket att skydda trådlösa nätverk. Syftet var att förbättra säkerheten i trådlösa nätverk genom att kryptera data ([URL15](#)). Eftersom Wi-Fi-nätverk använder radiovågor kan vem som helst inom räckhåll fånga upp signalerna, vilket innebär en betydande säkerhetsrisk.

Detta säkerhetsprotokoll använder RC4, ett strömchiffer, för att upprätthålla sekretess samt CRC-32 som kontrollsumma för att säkerställa dataintegritet ([URL16](#)). Krypteringen av datatrafiken sker med nycklar på 64 eller 128 bitar, uttryckta i hexadecimal form (siffrorna 0–9 och bokstäverna A–F) ([URL17](#)).

Protokollet visade sig däremot ha allvarliga säkerhetsbrister, framför allt på grund av att krypteringsnycklarna var förutsägbara, vilket gjorde det sårbart för så kallade brute force-attacker ([URL18](#)).

År 2004 drog Wi-Fi Alliance tillbaka stödet för WEP på grund av dess sårbarheter, och det anses i dag vara ett föråldrat säkerhetsprotokoll.

### 2.3.2 WPA

Wi-Fi Protected Access (WPA) introducerades år 2003 som Wi-Fi Alliances ersättning för WEP. Säkerhetsprotokollet använder Temporal Key Integrity Protocol (TKIP) för att dynamiskt ändra krypteringsnyckeln, i stället för att autentisera alla användare med en och samma nyckel ([URL19](#)). WPA använder 256-bitars nycklar för att kryptera datatrafiken, till skillnad från WEP:s 64- eller 128-bitars nycklar, men anses i dag inte längre vara tillräckligt säkert ([URL20](#)).

### 2.3.3 WPA2

Wi-Fi Protected Access 2 (WPA2) introducerades år 2004 som en förbättrad version av det tidigare WPA och använder krypteringsprotokollet CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol). CCMP bygger på algoritmen Advanced Encryption Standard (AES), vilket möjliggör verifiering av både meddelandets autenticitet och integritet. Detta gör WPA2 säkrare, eftersom AES ersätter det äldre TKIP-protokollet som användes i WPA ([URL21](#)).

Även om WPA2 innebär en betydande förbättring jämfört med WPA, är det till exempel sårbart för så kallade KRACK-attacker (Key Reinstallation AttaCKs) ([URL22](#)). Dessa attacker utnyttjar sårbarheter i säkerhetsprotokollet för att avlyssna och stjäla data som överförs över nätverket.

### 2.3.4 WPA3

Wi-Fi Protected Access 3 (WPA3) introducerades år 2018 av Wi-Fi Alliance och är den senaste generationen av säkerhetsprotokoll för Wi-Fi-nätverk. WPA3 är utformat för att stärka säkerheten i trådlösa nätverk och innebär en betydande förbättring jämfört med föregångaren WPA2. Protokollet introducerar flera viktiga uppdateringar, bland annat förbättrat skydd mot svaga lösenord, kryptering även i öppna nätverk samt starkare krypteringsmetoder för företagsnätverk ([URL23](#)). Likt både WPA och WPA2 erbjuder även WPA3 två huvudsakliga lägen: WPA3-Personal och WPA3-Enterprise.

WPA3-Personal använder Simultaneous Authentication of Equals (SAE), en teknik som är resistent mot så kallade offline dictionary attacks ([URL24](#)). Denna typ av attack genomförs genom att en angripare får tag på en chiffrerad text som genererats med en nyckel härledd från lösenordet, och sedan provar varje lösenord mot chiffrerad texten ([URL25](#)).

WPA3-Enterprise bygger vidare på grunden från WPA2-Enterprise och använder bland annat autentiseringskryptering med 128-bitars AES i Counter Mode med Cipher Block Chaining Message Authentication Code (AES-CCMP 128).

WPA3-Enterprise erbjuder dessutom ett valfritt 192-bitars säkerhetsläge som ger starkare skydd för känslig data. Detta inkluderar bland annat förbättrad autentiseringskryptering med 256-bitars Galois/Counter Mode Protocol (GCMP-256).

### 2.3.5 SSL / TLS

SSL (Secure Sockets Layer) och TLS (Transport Layer Security) är kryptografiska säkerhetsprotokoll som används för att säkra internetkommunikation genom att etablera en krypterad förbindelse mellan en klient (till exempel en webbläsare) och en server (till exempel en webbplats).

Protokollen använder digitala certifikat, vilka innehåller en offentlig nyckel och används för att autentisera webbplatsens identitet. Detta möjliggör att dataöverföring krypteras genom asymmetrisk kryptering eller kryptografi med publik nyckel, och att den matchande privata nyckeln hålls hemlig på servern ([URL26](#)). TLS är den modernare och säkrare efterföljaren till SSL, som i praktiken inte längre används.

### 2.3.6 VPN

Ett VPN (Virtual Private Network) är en tjänst som etablerar en säker nätverksanslutning när man använder offentliga nätverk. Genom att kryptera internettrafiken och dölja användarens identitet online fungerar ett VPN som ett effektivt skydd mot cyberattacker.

Detta uppnås genom att dölja användarens IP-adress (Internet Protocol), vilket är ett unikt nummer som tilldelas alla enheter som är anslutna till internet. En IP-adress används för att identifiera enheten och möjliggör kommunikation mellan olika enheter via nätet.

När ett VPN används omdirigeras internettrafiken genom en särskilt konfigurerad server som drivs av VPN-leverantören. Detta innebär att VPN-servern blir den synliga källan till användarens data, vilket ytterligare förstärker anonymiteten.

Användningen av VPN har ökat kraftigt i takt med det växande behovet av säker internetuppkoppling. Enligt en studie utförd av Forbes använder 66 % av internetanvändarna ett VPN för att skydda sin personliga information ([URL27](#)).

## 2.4 Informationssäkerhet

Detta avsnitt introducerar grunderna i informationssäkerhet (även kallat infosäk) och syftar till att ge användaren grundläggande kunskap om hur man skyddar värdefull information. Informationssäkerhet handlar om att säkerställa att information är konfidentiell, tillgänglig och korrekt. Detta kallas även för informationssäkerhetens CIA-triad.

### 2.4.1 CIA-triaden

CIA-triaden (Confidentiality, Integrity, Availability) är en grundläggande modell inom informationssäkerhet som används för att identifiera sårbarheter och utveckla säkerhetsåtgärder ([URL28](#)). Modellen består av tre principer: konfidentialitet, integritet och tillgänglighet, och kan ses som riktlinjer när man implementerar en informationssäkerhetsplan ([URL29](#)).

Konfidentialitet innebär att skydda information från att avslöjas eller spridas till obehöriga personer ([URL30](#)). Detta uppnås genom att kontrollera åtkomsten till information, exempelvis med autentisering och kryptering. Ett hot mot konfidentialiteten kan vara så kallade MITM-attacker (Man-In-The-Middle), där en angripare fångar upp och eventuellt manipulerar kommunikationen mellan två parter.

Integritet handlar om att säkerställa att informationen är pålitlig och korrekt. Hot mot integritet utförs ofta avsiktligt genom att till exempel kringgå ett intrångsdetekteringssystem (IDS) och ändra filkonfigurationer för att tillåta obehörig åtkomst ([URL31](#)). För att skydda integriteten i information kan man använda sig av bland annat versionshantering, filrättigheter, brandväggar och elektromagnetiska pulser (EMP) ([URL32](#)).

Tillgänglighet är den tredje principen i modellen och handlar om att säkerställa att åtkomst finns till informationen när det behövs ([URL33](#)). Hot mot tillgängligheten kan ske genom till exempel elfel, denial-of-service (DoS)-attacker och ransomware. För att säkerställa hög tillgänglighet finns det flera åtgärder som omfattar bland annat kris- och katastrofhantering, servrar med hög kapacitet och batterier för elförsörjning i kris ([URL34](#)).



### 3. Empiri/iakttagelser

Nedan redovisas objektivt de faktiska iakttagelserna från våra Evil Twin-tester mot iPhone. Presentationen sker i tabellform och genom skärmdumpar, så att varje steg i proceduren är möjligt att följa utan värderingar eller tolkningar. Detta utgör underlaget för den efterföljande analysen.

#### 3.1 Empiri: Evil Twin Attack (iPhone)

Syftet med testet är att undersöka hur snabbt en iPhone associerar till ett öppet, falskt nätverk (SSID "SecurityTest") efter manuell första anslutning, samt att verifiera att all HTTP-trafik krypteras via WireGuard/VPN.

##### 3.1.1 Testmiljö

- **SSID:** SecurityTest (öppet nätverk)
- **Kanal:** standardinställning på Wi-Fi Pineapple-klonen
- **Beacon Response Interval:** Aggressive (så att iPhone automatiskt väljer tillbaka efter första manuella anslutning)
- **Klient:** iPhone (iOS 18)
- **Utrustning:** MangoApple/WiFi Pineapple-klon (GL-iNet Mango + Pineapple mjukvara) i Evil Twin läge med 2x USB Wi-Fi adaptrar
- **VPN:** WireGuard (Integrity VPN)
- **Testwebbplats:** <http://testphp.vulnweb.com/> (HTTP)

##### 3.1.2 Procedur

1. Starta Evil Twin-nätverket "SecurityTest".
2. På iPhone: välj manuellt "SecurityTest" första gången. Därefter ansluter den automatiskt tack vare Aggressive Beacon Interval som förstärker att enheter som litar på nätverket ska ha större sannolikhet att ansluta.
3. Öppna webbläsare och surfa till <http://testphp.vulnweb.com/>. Logga in med testkonto utan VPN.
4. Koppla upp WireGuard VPN och upprepa inloggning med VPN.
5. Parallellt körs tcpdump på MangoApple för att fånga alla paket.
6. Laddar hem samlingsfilen med alla paket och analyserar dem i Wireshark.

Tabell 3.1: Rådata från Evil Twin tests (iPhone)

Omgång	Tid till associering	VPN-status	HTTP-paket synliga?	Kommentar
1	5s (manuellt första gången)	Av	Ja – POST /userinfo.php	Klartext: uname=test&pass=test
2	3s (automatiskt)	Av	Ja – JSON svar + formulärdata	Inga varningar
3	2s (automatiskt)	På	Nej – endast WireGuard	All trafik krypterad via VPN

Se Figurer 3.1–3.2 nedan för konfiguration och klientanslutning.

**Figur 3.1:** Pineapple-gränssnitt som visar öppet SSID ”SecurityTest”

Open SSID SecurityTest

Maximum Clients 100

☐ Hide Open SSID ☐ Disable Open SSID

Update Access Points

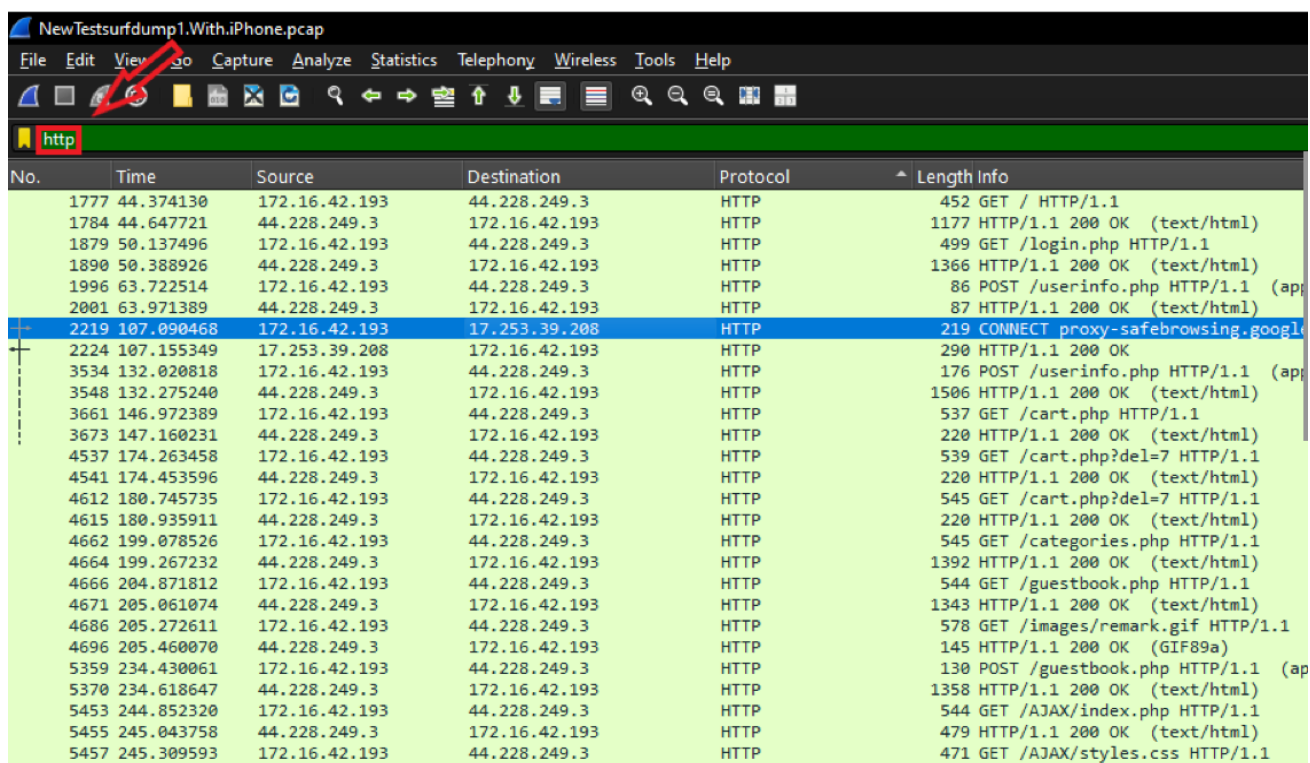
**Figur 3.2:** iPhone ansluten som klient på SSID ”SecurityTest”

WiFi Pineapple		
Dashboard		
Recon		
Clients		
Tracking		
Clients		
MAC Address	IP Address	SSID
00:04:4B:2B:A4:CE	172.16.42.144	SecurityTest

## Analys av HTTP-trafik utan VPN i Wireshark

Se figur 3.3-3.4 för en helhets vy av HTTP-paket och en detaljerad "Follow TCP Stream" med inloggningsuppgifter i klartext.

**Figur 3.3:** Översikt av HTTP-trafik utan VPN i Wireshark (filter `http`)



No.	Time	Source	Destination	Protocol	Length	Info
1777	44.374130	172.16.42.193	44.228.249.3	HTTP	452	GET / HTTP/1.1
1784	44.647721	44.228.249.3	172.16.42.193	HTTP	1177	HTTP/1.1 200 OK (text/html)
1879	50.137496	172.16.42.193	44.228.249.3	HTTP	499	GET /login.php HTTP/1.1
1890	50.388926	44.228.249.3	172.16.42.193	HTTP	1366	HTTP/1.1 200 OK (text/html)
1996	63.722514	172.16.42.193	44.228.249.3	HTTP	86	POST /userinfo.php HTTP/1.1 (ap
2001	63.971389	44.228.249.3	172.16.42.193	HTTP	87	HTTP/1.1 200 OK (text/html)
2219	107.090468	172.16.42.193	17.253.39.208	HTTP	219	CONNECT proxy-safebrowsing.google
2224	107.155349	17.253.39.208	172.16.42.193	HTTP	290	HTTP/1.1 200 OK
3534	132.020818	172.16.42.193	44.228.249.3	HTTP	176	POST /userinfo.php HTTP/1.1 (ap
3548	132.275240	44.228.249.3	172.16.42.193	HTTP	1506	HTTP/1.1 200 OK (text/html)
3661	146.972389	172.16.42.193	44.228.249.3	HTTP	537	GET /cart.php HTTP/1.1
3673	147.160231	44.228.249.3	172.16.42.193	HTTP	220	HTTP/1.1 200 OK (text/html)
4537	174.263458	172.16.42.193	44.228.249.3	HTTP	539	GET /cart.php?del=7 HTTP/1.1
4541	174.453596	44.228.249.3	172.16.42.193	HTTP	220	HTTP/1.1 200 OK (text/html)
4612	180.745735	172.16.42.193	44.228.249.3	HTTP	545	GET /cart.php?del=7 HTTP/1.1
4615	180.935911	44.228.249.3	172.16.42.193	HTTP	220	HTTP/1.1 200 OK (text/html)
4662	199.078526	172.16.42.193	44.228.249.3	HTTP	545	GET /categories.php HTTP/1.1
4664	199.267232	44.228.249.3	172.16.42.193	HTTP	1392	HTTP/1.1 200 OK (text/html)
4666	204.871812	172.16.42.193	44.228.249.3	HTTP	544	GET /guestbook.php HTTP/1.1
4671	205.061074	44.228.249.3	172.16.42.193	HTTP	1343	HTTP/1.1 200 OK (text/html)
4686	205.272611	172.16.42.193	44.228.249.3	HTTP	578	GET /images/remark.gif HTTP/1.1
4696	205.460070	44.228.249.3	172.16.42.193	HTTP	145	HTTP/1.1 200 OK (GIF89a)
5359	234.430061	172.16.42.193	44.228.249.3	HTTP	130	POST /guestbook.php HTTP/1.1 (ap
5370	234.618647	44.228.249.3	172.16.42.193	HTTP	1358	HTTP/1.1 200 OK (text/html)
5453	244.852320	172.16.42.193	44.228.249.3	HTTP	544	GET /AJAX/index.php HTTP/1.1
5455	245.043758	44.228.249.3	172.16.42.193	HTTP	479	HTTP/1.1 200 OK (text/html)
5457	245.309593	172.16.42.193	44.228.249.3	HTTP	471	GET /AJAX/styles.css HTTP/1.1

**Figur 3.4:** "Follow TCP Stream" som visar POST /userinfo.php med uname=test&pass=test och enhet använts markerat i klartext.

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 18_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.0 Mobile/15E148 Safari/604.1
Referer: http://testphp.vulnweb.com/login.php
Content-Length: 20
Accept-Language: sv-SE,sv;q=0.9

uname=test&pass=test
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Mon, 19 May 2025 12:11:26 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip
```

## Analys av HTTP-trafik med VPN

Se Figur 3.5-3.6 för att verifiera att all HTTP krypteras när WireGuard är aktivt.

**Figur 3.5:** WireGuard-trafik i Wireshark med display-filtret `udp && ip.addr == 172.16.42.193`. Pilarna markerar både filterfältet, iPhones IP (172.16.42.193) och protokollet "WireGuard" för handshake och transportdata.

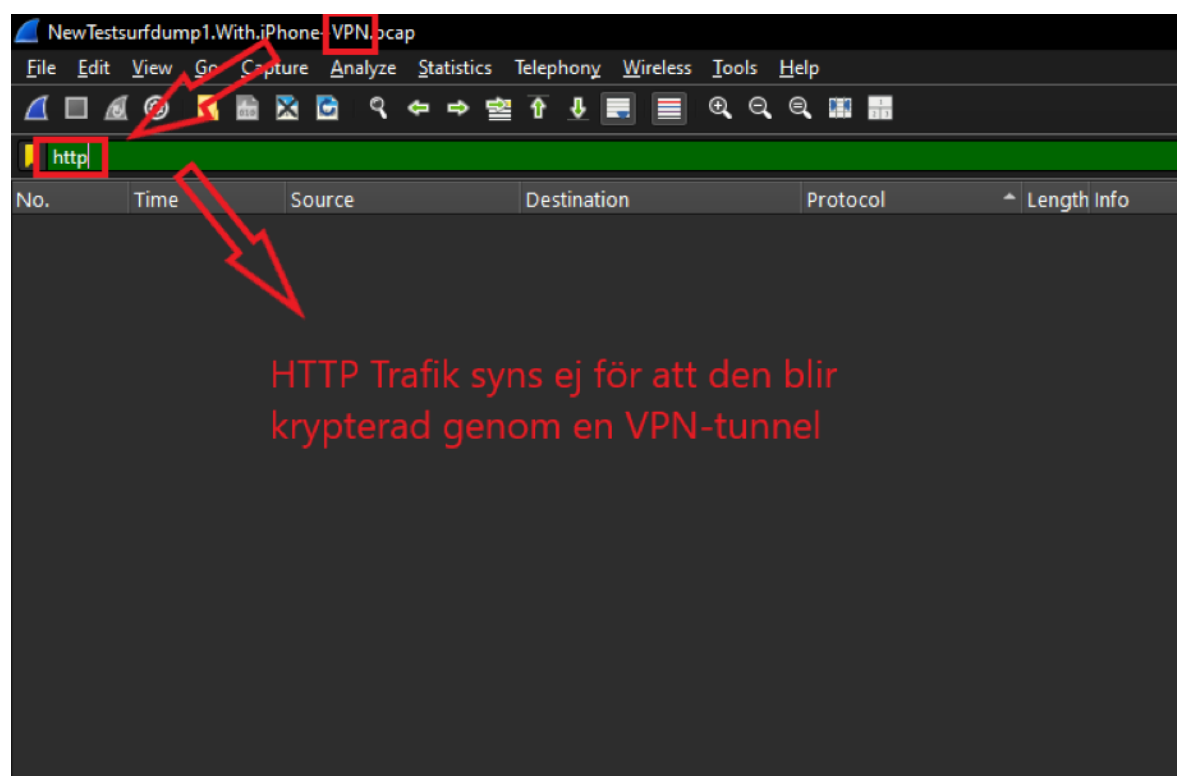
NewTestsurfdump1.With.iPhone+VPN.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp && ip.addr == 172.16.42.193

No.	Time	Source	Destination	Protocol	Length	Info
5	0.000418	172.16.42.193	176.10.248.206	WireGuard	122	Transport
6	0.000643	172.16.42.193	176.10.248.206	WireGuard	190	Handshake
7	0.013373	176.10.248.206	172.16.42.193	WireGuard	134	Handshake
8	0.019820	172.16.42.193	176.10.248.206	WireGuard	74	Keepalive
11	6.791407	172.16.42.193	176.10.248.206	WireGuard	170	Transport
12	6.791689	172.16.42.193	176.10.248.206	WireGuard	170	Transport
13	6.799364	176.10.248.206	172.16.42.193	WireGuard	298	Transport
14	6.799769	176.10.248.206	172.16.42.193	WireGuard	250	Transport
15	6.804239	172.16.42.193	176.10.248.206	WireGuard	138	Transport
16	6.806685	172.16.42.193	176.10.248.206	WireGuard	170	Transport
17	6.807091	172.16.42.193	176.10.248.206	WireGuard	170	Transport
18	6.807304	172.16.42.193	176.10.248.206	WireGuard	170	Transport
19	6.817740	176.10.248.206	172.16.42.193	WireGuard	362	Transport
20	6.818089	176.10.248.206	172.16.42.193	WireGuard	362	Transport
21	6.818410	176.10.248.206	172.16.42.193	WireGuard	314	Transport
22	6.821493	172.16.42.193	176.10.248.206	WireGuard	186	Transport
23	6.821826	172.16.42.193	176.10.248.206	WireGuard	186	Transport
24	6.823558	172.16.42.193	176.10.248.206	WireGuard	186	Transport
25	6.823986	172.16.42.193	176.10.248.206	WireGuard	186	Transport
26	6.824250	172.16.42.193	176.10.248.206	WireGuard	186	Transport
27	6.831113	176.10.248.206	172.16.42.193	WireGuard	250	Transport
28	6.831472	176.10.248.206	172.16.42.193	WireGuard	250	Transport

**Figur 3.6:** Wireshark med display-filtret `http` när WireGuard-VPN är aktivt, inga HTTP-paket visas eftersom all trafik är krypterad i VPN-tunneln.



## 4. Analys av resultatet

I detta kapitel besvaras rapportens frågeställningar utifrån de empiriska iakttagelserna (kapitel 3) och den teoretiska referensramen (kapitel 2). Varje underavsnitt knyter en eller flera frågeställningar till mätvärden, skärmdumpar och protokollkunskap, samt diskuterar giltighet (validitet) och mätnoggrannhet (reliabilitet). Analysen syftar till att förklara hur och varför testerna visade på sårbarheter i Wi-Fi-nätverk, och att bedöma vilka motåtgärder som kan skydda användare.

## 4.1 Tekniska sårbarheter i Wi-Fi

(Frågeställning: Vilka tekniska sårbarheter i Wi-Fi-nätverk möjliggör dessa attacker?)

Under vårt test med Evil Twin-attacken märkte vi hur lätt det var att sätta upp ett falskt nätverk som liknade ett äkta. Vi fokuserade inte så mycket på vilka typer av ramar som låg bakom detta från början, men när vi såg att klienten (iPhone) började ansluta automatiskt efter den första manuella kopplingen, blev det tydligt hur lite kontroll användaren har i sådana situationer. Det kändes både imponerande och lite skrämmande att det fungerade så bra, särskilt eftersom vi använde ganska enkel utrustning.

Teorin bakom detta säger att attacker som Deauthentication och Evil Twin fungerar eftersom Wi-Fi-standarden bygger på okrypterade management-ramar, som till exempel Beacon frames och Deauthentication frames. Dessa kan skickas ut utan någon autentisering, vilket gör det möjligt att lura enheter att ansluta till fel nätverk. När vi såg hur snabbt enheten återanslöt, utan att vi behövde göra något mer än sända ut beacons via Pineapple-klonen, förstod vi hur lätt det faktiskt är att manipulera detta beteende.

Vi tänker att det här delvis är en konsekvens av att Wi-Fi-teknologin från början fokuserade på enkelhet och användarvänlighet, att man ska kunna ansluta utan krångel. Men i takt med att tekniken blivit en självklar del av vardagen har det också blivit mer uppenbart att den här typen av sårbarheter kan utnyttjas. Det krävs inte ens särskilt avancerad utrustning eller kunskap för att sätta upp en attack som få användare skulle märka.

## 4.2 Hur fungerar Evil Twin-attacker i praktiken

(Frågeställning: Hur fungerar attacker som Deauthentication och Evil Twin i praktiken?)

Vi genomförde endast tester med Evil Twin-attacken, eftersom dokumentationen av Deauthentication visade sig vara mer tidskrävande än förväntat. Däremot diskuterade vi den tekniken och förstår att den ofta används tillsammans med Evil Twin. Till exempel kan en Deauthentication-attack tvinga bort en enhet från det riktiga nätverket, vilket får den att automatiskt försöka återansluta, då kan den av misstag ansluta till den falska accesspunkten i stället. Det gör en Evil Twin-attack ännu effektivare.

Själva processen började med att vi konfigurerade vår Pineapple-klon (baserad på GL iNet Mango) genom att sätta upp ett öppet SSID under Network-modulen. Under PineAP-modulen aktiverade vi inställningar som 'Allow Associations' (för att låta klienter ansluta), samt loggning av events och 'Beacon Response' med en aggressiv intervall. Det gör att klienter ser det falska nätverket oftare, vilket ökar chansen att det ansluter automatiskt.

Vi startade sedan tcpdump för att sniffa trafiken som gick genom wlan0, det gränssnitt som skickade ut vårt falska nätverk.

När vi testade med en iPhone såg vi att den efter en första manuell anslutning, började ansluta automatiskt till vårt falska nätverk. Det bekräftade våra förväntningar om hur sårbart det är när en enhet minns ett SSID och försöker återansluta till det utan att verifiera nätverkets äkthet.

Vi loggade in på en testhemsida via HTTP och kunde i Wireshark se bland annat vilken enhet som kopplat upp sig, vilka sidor som besökts och till och med inloggningsuppgifter i klartext. Det kändes nästan för enkelt – att vi bara med tcpdump och Wireshark kunde se så mycket känslig information direkt.

Vid testet med VPN aktiverat på iPhone såg vi nästan ingen information alls. Wireshark visade bara WireGuard-protokoll och att enheten kopplade upp sig mot en viss server IP, ingen HTTP-trafik var synlig. Det bekräftade att VPN fungerar som ett effektivt skydd i praktiken, inte bara i teorin.

Vi upplevde inte att attacken var särskilt tekniskt svår att genomföra. Gränssnittet krävde lite inläring, och man behöver ha en viss förståelse för hur Wireshark fungerar - särskilt vilka filter man bör använda. Men över lag är det fullt möjligt att sätta upp en attack som detta efter att följt en guide eller video. Vi testade oss fram mer än så eftersom vi var nyfikna på att förstå vad som faktiskt händer i bakgrunden.

### **4.3 Verktygens tillgänglighet**

(Hur lättillgängliga är de verktyg som krävs för att genomföra sådana attacker?)

Vi har sedan tidigare haft viss kännedom om kommersiella WiFi Pineapple-enheter, men eftersom de är ganska dyra väcktes vårt intresse när vi såg en YouTube-video om hur man kan bygga en egen klon med billigare hårdvara. I videon fanns tydliga instruktioner om hur man laddar ner den öppna mjukvaran, flashar den på en billig mini-router (GL.iNet Mango) och konfigurerar ett eget Pineapple-gränssnitt.

De övriga verktygen var också relativt enkla att hitta. tcpdump gick att installera som modul direkt i systemet på Pineapple-klonen, Wireshark är tillgängligt som gratis nedladdning, och VPN-lösningen (WireGuard) hittade vi via vår internetleverantör. Allt som allt var det ingen svår process att få tag i rätt verktyg.

Kostnaden för hela bygget låg på cirka 300-500kr. Själva routern var enkel att köpa online, men det som tog tid var att hitta rätt typ av USB Wi-Fi-adaptrar.

För att kunna sniffa trafik och genomföra attacker behövde adaptrar som stödde både monitor mode och packet injection. Vi hittade till slut ett par modeller från Kina som fungerade. Installationen var i sig inte särskilt avancerad – med hjälp av videoguider och lite tålamod gick det att sätta upp klonen utan större problem. Inställningarna i gränssnittet krävde dock en del testande, Googlande och vägledning, bland annat via ChatGPT, för att förstå exakt vad de olika alternativen gjorde.

Vi tror att det flesta som har ett grundläggande teknikintresse och är villiga att följa guider kan sätta upp något liknande. Det krävs ingen avancerad IT-kunskap, men ett visst driv och nyfikenhet är helt klart till hjälp – särskilt om man vill förstå vad som händer under huven och inte bara följa instruktioner.

Vi ser det som både positivt och negativt att verktygen är så lättillgängliga. För den som är intresserad av nätverk och cybersäkerhet är det ett utmärkt sätt att lära sig hur Wi-Fi fungerar på riktigt. Samtidigt är det lite skrämmande att det är så enkelt att sätta upp en attackmiljö, med relativt låg tröskel. Vår egen utrustning var inte särskilt kraftfull, men med en starkare enhet hade det sannolikt varit ännu enklare att genomföra mer avancerade attacker.

## 4.4 Skyddsåtgärder mot attacker

(Frågeställning: Vilka försvar eller skyddsåtgärder finns det mot dessa attacker?)

I vår studie testade vi VPN som en praktisk skyddsåtgärd, och resultatet var tydligt. När vi analyserade nätverkstrafiken från enheten utan VPN såg vi både HTTP-paket, inloggningsuppgifter i klartext och vilken klient som var ansluten. Efter att WireGuard aktiverats såg vi i stort sett ingenting – endast VPN-protokollet och en IP-adress som tillhörde VPN-servern. Inga spår av besökta webbplatser eller sänd data fanns kvar, och HTTP-filtret i Wireshark visade ingen träff. Det bekräftar att VPN krypterar hela nätverkstrafiken och effektivt förhindrar att en angripare får tillgång till innehållet.

Utöver VPN finns flera teoretiska skyddsåtgärder vi läst om men inte testat själva, bland annat WPA2, WPA3, och TLS. WPA3 ger bland annat starkare kryptering även för öppna nätverk och bättre skydd mot så kallade ”offline dictionary attacks”. För att skydda sig mot Deauthentication-attacker används i WPA3 även ett tillägg i standarden (802.11w, även kallat MFP – Management Frame Protection), som skyddar management-ramar från att manipuleras.



På klientsidan används ofta SSL/TLS för att säkra webbsidor. Det skyddar användare om de surfar till en webbsida via HTTPS – men det kräver att webbplatsen är korrekt konfigurerad. Många sidor har fortfarande brister, eller tillhandahåller inloggning via okrypterad HTTP. Det gör VPN till ett extra skyddslager som inte är beroende av webbplatsens säkerhetsnivå.

Vi tycker att det är positivt att många av dessa skydd är enkla att använda. VPN-tjänster går ofta att installera med ett klick och kräver ingen djupare teknisk förståelse. Samtidigt är det viktigt att användaren är medveten om riskerna – tekniken i sig skyddar inte om den inte används. Därför tycker vi att VPN är den viktigaste skyddsåtgärden för vanliga användare i offentliga nätverk, eftersom det är både lätt att komma i gång med och ger ett starkt skydd oavsett vilken webbsida man besöker.

## **4.5 Hur användare kan minska risken att bli utsatt**

(Frågeställning: Hur kan man som användare minska risken att bli utsatt?)

Det tydligaste vi lärt oss under projektet är hur effektivt VPN fungerar som skydd. Därför tycker vi att det viktigaste en användare kan göra i offentliga nätverk är att alltid ha en VPN-tjänst aktiv. Det gör att trafiken krypteras oavsett om hemsidan använder HTTPS eller inte.

Vi insåg också hur lätt det är att bli lurad av ett falskt nätverk. Om namnet är trovärdigt – som till exempel ”Espresso House\_Guest\_Wifi”, så finns det stor risk att användaren kopplar upp sig utan att reflektera. Vi såg själva hur vår testtelefon anslöt automatiskt till det falska nätverket efter att vi bara kopplat upp oss en gång. Utan VPN hade det betytt att all trafik kunde snappas upp igen utan att användaren märkt något.

Vi tror att många inte vet att deras enheter har funktionen för automatisk återanslutning aktiverad. Att stänga av detta i miljöer man inte litar på kan vara en enkel och effektiv försiktighetsåtgärd. Hemma är det oftast inget problem, men i offentliga miljöer bör man vara mer medveten.

Vi tycker att det inte räcker att bara kontrollera om en hemsida har ”https://” - eftersom det inte hjälper om nätverket i sig är kapat. En VPN krypterar hela anslutningen, vilket gör det till ett bättre skydd.

Efter våra tester har vi själva blivit mer vaksamma. Om vi behöver använda offentliga nätverk kommer vi att slå på VPN först. Vi har också blivit noggrannare med att kontrollera SSID-namn innan vi ansluter, för att undvika att gå in i ett falskt nätverk utan att veta om det.

## 4.6 Validitet och reliabilitet

Våra teoretiska källor kommer främst från etablerade aktörer inom cybersäkerhet och standardisering, såsom Kaspersky, Fortinet, IEEE och Microsoft, vilket vi bedömer som hög validitet. Flera av dessa är internationellt erkända inom Wi-Fi-säkerhet och används även i utbildningssammanhang. Vissa källor är hämtade från bloggar och teknikartiklar online, vilket kan innebära något lägre validitet, men dessa har vi endast använt för att förklara praktiska angreppstekniker som dessutom har verifierats genom våra egna tester.

## 5. Slutsatser

### **Wi-Fi-protokollets struktur möjliggör attacker:**

Wi-Fi-standarderna använder okrypterade management-ramar (som Beacon och Deauthentication frames), vilket gör det möjligt att genomföra attacker som Evil Twin och Deauth utan att behöva autentisera sig mot nätverket. Detta är en grundläggande sårbarhet i designen.

### **Evil Twin-attacker är praktiskt genomförbara med enkla medel:**

Studien visar att det är fullt möjligt att genomföra en fungerande Evil Twin-attack med relativt begränsade resurser och utan avancerad teknisk bakgrund. Genom att följa tillgängliga guider och använda lättillgängliga verktyg kan en angripare skapa en falsk åtkomstpunkt som imiterar ett legitimt nätverk. Detta understryker att hotbilden inte enbart gäller avancerade aktörer, utan även personer med grundläggande kunskaper och enklare utrustning har praktisk möjlighet att genomföra denna typ av attack.

### **Säkerhetsfunktioner som VPN skyddar effektivt:**

När VPN aktiverades på testklienten kunde ingen känslig information längre observeras i klartext vid paketfångst. Detta indikerar att VPN utgör ett effektivt skydd mot attacker där angriparen försöker fånga upp okrypterad datatrafik, såsom vid en Evil Twin-attack.

### **Verktygen är lättillgängliga och billiga:**

De verktyg som användes för att genomföra attackerna var fritt tillgängliga, kostade lite eller inget, och krävde endast grundläggande teknisk kompetens för att konfigureras. Denna tillgänglighet bidrar till en förhöjd hotbild, då tröskeln för att genomföra Wi-Fi-attacker som Evil Twin och Deauthentication är låg även för icke-professionella angripare.

## **5.1 Rekommendationer**

### **För användare:**

- **Använd VPN aktivt, särskilt vid anslutning till offentliga eller osäkra Wi-Fi-nätverk.** VPN är en av de mest effektiva metoderna för att skydda datatrafiken från avlyssning och förhindra att känslig information exponeras för obehöriga.
- **Var vaksam vid anslutning till öppna Wi-Fi-nätverk.** Offentliga och öppna nätverk kan vara skapade av illasinnade aktörer för att lura användare att ansluta och därigenom utsätta deras data för avlyssning eller manipulation. Kontrollera alltid nätverksnamnet noggrant och undvik att utföra känsliga aktiviteter på sådana nätverk utan extra skydd, exempelvis VPN.

### **För utvecklare och leverantörer av nätverksutrustning:**

- **Implementera stöd för 802.11w (Protected Management Frames)** i både åtkomstpunkter och klienter. Detta minskar risken för vissa typer av attacker, bland annat Deauthentication-attack.
- **Gör användare mer medvetna om automatiska anslutningar** genom tydliga varningar eller inställningar som tillåter manuell hantering av kända nätverk.

**För utbildare och cybersäkerhetsutbildningar:**

- **Använd lättillgängliga verktyg i undervisningen** för att visa hur attacker fungerar i praktiken. Det ger bättre förståelse för hotbilden och hur skyddsåtgärder fungerar.
- **Lägg vikt vid etiska aspekter** av säkerhetstester och penetrationstester, särskilt när verktygen är så lättillgängliga.

**För beslutsfattare och standardiseringsorgan:**

- **Uppdatera riktlinjer för Wi-Fi-säkerhet** så att användning av VPN och andra skydd blir standard, särskilt i offentliga miljöer.
- **Driv på för bredare implementering av säkerhetsstandarder som WPA3 och 802.11w, även i konsumentutrustning.** Detta är avgörande för att förbättra den generella Wi-Fi-säkerheten och minska sårbarheter som kan utnyttjas av angripare.

## 6. Referenslista

URL 1: <https://nordvpn.com/sv/blog/studie-pendling-internet-2025/#offentligt-wifi-%C3%A4r-ett-riskfyllt-men-vanligt-val>,

[hämtad 250520]

URL 2: <https://www.si.edu/newsdesk/snapshot/hedy-lamarr-golden-age-film-star-and-important-inventor>,

[hämtad 250520]

URL3: <https://www.kth.se/biblioteket/anvanda-biblioteket/studera-i-biblioteke/vem-var/hedy-lamarr-1.991425>,

[hämtad 250520]

URL4: <https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/>,

[hämtad 250520]

URL5: <https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/>,

[hämtad 250520]

URL6: <https://www.britannica.com/story/how-does-wi-fi-work>,

[hämtad 250520]

URL7: <https://medium.com/@AlexanderObregon/what-is-wifi-and-how-does-it-work-a-simple-explanation-for-beginners-2e2cf7c16645>,

[hämtad 250520]

URL8: <https://nordvpn.com/sv/blog/Deauthentication-attack/>,

[hämtad 250520]

URL9: <https://blog.spacehuhn.com/wifi-Deauthentication-frame>,

[hämtad 250520]

URL10: <https://www.kaspersky.se/resource-center/preemptive-safety/evil-twin-attacks>,

[hämtad 250520]

URL11: <https://www.kaspersky.se/resource-center/preemptive-safety/evil-twin-attacks>,

[hämtad 250520]

URL12: <https://zimperium.com/glossary/evil-twin-attacks>,

[hämtad 250520]

URL13: <https://www.kaspersky.se/resource-center/preemptive-safety/evil-twin-attacks>,  
[hämtad 250520]

URL14: <https://www.varonis.com/blog/evil-twin-attack>,  
[hämtad 250520]

URL15: <https://www.kaspersky.se/resource-center/definitions/wep-vs-wpa>,  
[hämtad 250520]

URL16: <https://www.okta.com/identity-101/wep/>,  
[hämtad 250520]

URL17: <https://www.kaspersky.se/resource-center/definitions/wep-vs-wpa>,  
[hämtad 250520]

URL18: <https://nordvpn.com/sv/blog/wep-wpa-wpa2-och-wpa3/>,  
[hämtad 250520]

URL19: <https://www.okta.com/identity-101/wep/>,  
[hämtad 250520]

URL20: <https://nordvpn.com/sv/blog/wep-wpa-wpa2-och-wpa3/>,  
[hämtad 250520]

URL21: <https://www.okta.com/identity-101/wep/>,  
[hämtad 250520]

URL22: <https://www.kaspersky.se/resource-center/definitions/wep-vs-wpa>,  
[hämtad 250520]

URL23: <https://www.techtarget.com/searchsecurity/definition/WPA3>,  
[hämtad 250520]

URL24: <https://www.wi-fi.org/discover-wi-fi/security>,  
[hämtad 250520]

URL25: <https://web.mit.edu/kerberos/krb5-latest/doc/admin/dictionary.html>,  
[hämtad 250520]

URL26: <https://www.ssl.com/sv/Artikeln/vad-%C3%A4r-ssl-tls-an-in-depth-guide/>,  
[hämtad 250520]

URL27: [https://www.forbes.com/advisor/business/vpn-statistics/#sources\\_section](https://www.forbes.com/advisor/business/vpn-statistics/#sources_section),  
[hämtad 250520]

URL28: <https://www.fortinet.com/resources/cyberglossary/cia-triad>,  
[hämtad 250520]

URL29: <https://www.microsoft.com/sv-se/security/business/security-101/what-is-information-security-infosec>,

[hämtad 250520]

URL30: <https://www.safestate.com/artiklar/vad-ar-informationssakerhet/>,

[hämtad 250520]

URL31: <https://www.fortinet.com/resources/cyberglossary/cia-triad>,

[hämtad 250520]

URL32: <https://ciatriad.se/riktighet/>,

[hämtad 250520]

URL33: <https://www.safestate.com/artiklar/vad-ar-informationssakerhet/>,

[hämtad 250520]

URL34: <https://ciatriad.se/tillganglighet/>,

[hämtad 250520]