View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Göteborgs universitets publikationer - e-publicering och e-arkiv

GÖTEBORGS UNIVERSITET

Säkerhet i öppna WiFi-nätverk

En studie om hur användares medvetenhet om säkerhetsrisker vid interaktion med öppna WiFi-nätverk kan ökas

Security in public WiFi networks

A study regarding how users risk perception in public WiFi networks can be improved

Erik Leijon
Joachim von Hedenberg

Kandidatuppsats i Informatik

Rapport nr. 2014:038
ISSN: 1651-4769

Abstrakt

Öppna WiFi-nätverk är i dagsläget en av de dominerande teknikerna för användare att få internetåtkomst på allmänna platser. Problematiken ligger i att de är designade med fokus på tillgänglighet snarare än säkerhet – något som användare överlag inte är medvetna om. Användare som oaktsamt använder sig av nätverken utsätter sig för risken att känslig information råkar i fel händer, vilket bland annat kan leda till identitetsstölder. Då användare ofta saknar kunskaper om säkerhetsaspekter vid interaktion med öppna WiFi-nätverk tyder all forskning på att de måste utbildas och informeras om de risker de utsätter sig för – men talar inte om hur det skall gå till. Därför ställde vi oss frågan:

Hur kan medvetenheten om säkerhetsrisker i öppna WiFi-nätverk ökas?

Utifrån tidigare forskning kring tekniska och psykologiska aspekter kopplade till problemområdet valdes relevanta metoder för datainsamlingen. Genom en enkätundersökning kunde användares kunskap om problemområdet analyseras och med hjälp av en intervju med en områdesexpert fick vi ta del av hans syn på problemområdet samt fick värdefulla råd om var arbetets fokus bör ligga. Slutligen utfördes en rad observationer där vi visade hur enkelt det är att ta del av informationen som skickas över öppna nätverk. Då ingen information från observationerna kunde presenteras, på grund av etiska och juridiska skäl, valde vi att exemplifiera genom ett praktikfall där vi visar hur användarnamn och lösenord skickas i klartext.

På grund av områdets komplexitet var vi tvungna att avgränsa diskussionen till det område vi fann vara mest problematiskt. Juridiskt sett är området en gråzon där ett flertal lagrum är involverade, men övervakning av trafik i öppna WiFi-nätverk kan i Sverige göras lagligt. Slutsatsen grundar sig på tidigare forskning samt visar på att det finns ett flertal säkerhetsrisker vid interaktion med öppna WiFi-nätverk och att det går att utnyttja informationen utan svårigheter – även för en angripare utan omfattande tekniska kunskaper. Genom att visualisera potentiella säkerhetsrisker och tvinga användaren att göra aktiva val kan dennes medvetandegrad höjas och vidare kan de informeras om riskerna.

Nyckelord: Öppna WiFi-nätverk, WiFi-säkerhet, säkerhetsmedvetenhet, säkerhetsrisker

Abstract

Public WiFi networks is one of the dominant technologies for users to get public internet access. The problem is that the networks are designed for accessability rather than security – a problem users seldom are aware of. Users who carelessly access WiFi networks may reveal sensitive information which, among other things, can lead to an identity theft. Previous research suggests that users must be educated and informed about the risks they incur, but not how this should be done. Thus, we asked the question:

"How can users' awareness of security threats in public WiFi networks be improved?"

Based on previous research related to the technical and psychological aspects of the subject, relevant methods for data gathering were selected. Using a questionnaire we examined the users' knowledge and attitudes towards the problem area. Through an interview with a security expert we got an experts view on public WiFi security, as well as valuable advice on what to focus on in our study. Finally, a series of observations were made where we showed how easy it is to access the information sent over the networks. Since no information from the observations could be presented, due to the ethical and legal aspects, we chose to illustrate a case study, where we presented how usernames and passwords are sent in clear text format.

As the area of the study was found to be very complex, we narrowed down our discussion to the area we thought to be the most relevant. Legally, our research method was found to be somewhat in a gray zone where multiple Swedish laws came in to play. However, we were able to determine that monitoring public WiFi networks is legal in Sweden. Our conclusion is based on previous research, which shows that there are many security risks involved in interactions with public WiFi networks and can be abused by an attacker even without extensive technical knowledge. By visualizing potential threats and force users to make active choices, their awareness could be increased when using public WiFi networks.

Keywords: Public WiFi, WiFi security, riskperception, security threats

Tack

Vi vill tacka till vår handledare Lennart Peterson som gett oss återkommande feedback och ständigt funnits tillgänglig under arbetets gång.

Vi vill även rikta ett stort tack till Jakob Schlyter som utöver deltagande informant i vårt arbete, även gav oss värdefulla råd och inspiration till vidare utforskande av området.

Innehållsförteckning

1 Inledning

1.1 Bakgrund och problemområde

”It’s what you don’t know that makes you vulnerable.” (Codenomicon, 2014)

I ett samhälle som blivit allt mer beroende av att människor är uppkopplade mot nätet har öppna, trådlösa nätverk framträtt som en av de mest populära teknikerna för att erbjuda internetåtkomst. Den vanligaste standarden för trådlösa nätverk är Wireless Fidelity (Attipoe, 2013; Park & Dicoi, 2003) och förkortas WiFi. Flera platser, så som caféer, flygplatser, tågstationer och hotell, tillhandahåller WiFi-hotspots för att stärka sitt varumärke. En av de största fördelarna med öppna WiFi-nätverk är deras lättillgänglighet, men nackdelen är att säkerheten ofta är undermålig. Data skickas okrypterat över nätverken vilket medför stora säkerhetsrisker (Attipoe, 2013; Chenoweth, Minch & Tabor, 2010). Nätverket delas av alla användare som kan ta del av informationen och utnyttja den i kriminella syften, exempelvis genom förfalskande av identiteter eller andra bedrägerier.

Forskning inom området visar på att användare ofta är omedvetna om de säkerhetsrisker de utsätter sig för vid interaktion av öppna WiFi-nätverk och om att de själva aktivt behöver bidra för att kunna använda nätverken på ett säkert sätt. Ett flertal användare tror också att nätverksleverantören eller någon annan skyddar dem (Attipoe, 2013; Chenoweth, Minch & Tabor 2010; Greenstadt, Afroz & Brennan, 2009; Klasnja, Consolvo, Jung, Greenstein, LeGrand, Powledge & Wetherall, 2008). Användarna visar på viss oro vid interaktion med nätverken och då främst för att deras identitet skall bli stulen (Garg & Camp, 2012). Identitetsstöld är även en av de vanligast förekommande typerna av informationsstöld (Lawson, 2013).

Oberoende hur omfattande problemet är i dagsläget finns risken att fler och fler angripare kommer utnyttja den undermåliga säkerheten i öppna WiFi-nätverk. Enligt Gabriel (2013) kommer mängden publikt tillgängliga WiFi-nätverk att ha ökat med 350 % mellan 2012 - 2015, vilket innebär att det år 2015 kommer finns över 5 miljoner öppna WiFi-nätverk världen över. Risken är stor att både antalet angripare och nätverksattacker ökar parallellt med nätverken, varför det är viktigt att användare är medvetna om riskerna kopplade till dem.

Idag kan i princip vilken näringsidkare eller organisation som helst sätta upp ett trådlöst nätverk och låta sina kunder eller gäster använda det (Klasnja et al. 2008). Det är inte bara enkelt att sätta upp en WiFi-hotspot, det förväntas även i allt större utsträckning av företagen att de erbjuder tjänsten. I Göteborg finns det 51 stycken öppna WiFi-nätverk med gratis uppkoppling som tillhandahålls av staden (Göteborgs stad, 2014). Vidare hänvisar Göteborgs stad till *Wifikartan.se* som ger förslag på över 100 andra platser i Göteborg med gratis WiFi-uppkoppling (Wifikartan, 2014). Trots att *Wifikartan.se* endast presenterar de platser registrerade på sidan visar de på en omfattande tillgänglighet där användare har möjlighet att koppla upp sig på nätet oberoende av var de befinner sig. Tillgängligheten har dock en baksida, som Lawson (2013) beskriver i sin artikel om WiFi-säkerhet: “*However, what consumers still seem not to understand is that the majority of WiFi hotspots were designed for convenience, not security*” (Lawson, 2013, s 1).

För att undersöka problemområdet krävs kunskaper från ett flertal vetenskapsgrenar, både rörande själva tekniken bakom nätverken och om människors riskperception och risktagande. Forskning kring riskperception hos användare i liknande situationer, till exempel vid surfande på ett krypterat nätverk, visar att människor har svårt att förstå säkerhetsvarningar och agera utifrån dem (Egelman, Cranor & Hong, 2008). Majoriteten av forskningen kring öppna WiFi-nätverk och angränsande problemområden drar slutsatsen att

användare måste informeras och utbildas, men beskriver inte hur det ska gå till och hur användare skall förstå de risker de utsätter sig för (Chenoweth, Minch & Tabor, 2010; Garg & Camp, 2012; Koved, Trewin, Swart, Singh, Cheng & Chari, 2013; Gebauer, Kline & He, 2011). Klasnja et al. (2008) nämner dock att de i samband med sin studie arbetat med att ta fram en teknisk lösning för att visualisera nätverkstrafiken för användarna.

1.2 Syfte och frågeställning

Utifrån det ovan beskrivna problemområdet är syftet med vårt arbete att ur ett användarperspektiv undersöka hur medvetenheten om säkerhetsrisker i öppna WiFi-nätverk kan ökas. Därmed formulerar vi frågeställningen:

Hur kan medvetenheten om säkerhetsrisker i öppna WiFi-nätverk ökas?

För att besvara frågeställningen har vi formulerat tre underfrågor som hjälper oss besvara vår frågeställning.

Har användare med IT-relaterad sysselsättning högre medvetenhet om säkerhetsrisker vid interaktion med öppna WiFi-nätverk än andra?

Hur svårt är det att utnyttja informationen som skickas i öppna WiFi-nätverk?

Hur kan når man ut till användarna?

Genom att besvara den första underfrågan vill vi undersöka ifall ökad kunskap om ämnet faktiskt resulterar i en ökad medvetenhet om riskerna. Svaret på den andra underfrågan kan användas för att påvisa för användare hur information de skickar i nätverken enkelt kan utnyttjas. Den tredje frågan undersöker hur information om de risker användare utsätter sig för kan presenteras för användarna.

För att bättre förstå hur användare interagerar med öppna WiFi-nätverk och vilka säkerhetsrisker det kan innebära krävs en grundlig men överskådlig genomgång av teknologin bakom nätverken samt de säkerhetsrisker som existerar i dagsläget. Vidare krävs kunskap om hur användare uppfattar, bedömer och agerar utifrån potentiella risker. Teoriavsnittet kommer belysa aspekterna med hjälp av tidigare forskning och ligger sedan till grund för vår datainsamling och diskussion.

2. Teori

Första delen av teoriavsnittet kommer behandla den tekniska aspekten av problemområdet under rubriken *Teknik och säkerhet*. Avsnittet är medvetet förenklat för att även mindre tekniskt insatta läsare skall kunna ta del av det, även om det är omöjligt att frångå viss teknisk terminologi. För att läsaren bättre skall förstå varför säkerhetsaspekten vid interaktion med öppna WiFi-nätverk är viktig kommer även de vanligaste attackerna och säkerhetsriskerna att presenteras i teoridelen. Den andra delen av teoriavsnittet kommer att behandla den mänskliga aspekten av problemområdet under rubriken *Användaren och risktagande.* Fokus i den andra delen ligger på att presentera relevant forskning som behandlar användares riskperception och risktagande i relaterade situationer.

2.1 Teknik och säkerhet

I avsnittet presenteras inledningsvis en övergripande bild av WiFi-teknologin. Vidare presenteras ett urval av de potentiella hot som finns samt säkerhetsteknik kopplat till nätverkssäkerhet.

2.1.1 WiFi-teknologin

WLAN (Wireless Local Area Network) är en samlingsterm för olika typer av trådlösa nätverk. En av de mest populära varianterna är Wireless Fidelity (fortsättningsvis WiFi). Det finns flera olika versioner av WiFi som är baserade på IEEE (Institute of Electrical and Electronics Engineers) Standard 802.11. WiFi-tekniken möjliggör att en enhet trådlöst kan utbyta data med en annan enhet eller trådlöst ansluta sig till internet via en så kallad Access Point (fortsättningsvis AP) med hjälp av UHF (Ultra High Frequency)-radiovågor (Attipoe, 2013; Englander, 2010, s 468). För att adressera data används Internet Protocol adress (Fortsättningsvis IP-adresser). IP-adresser består av en sifferkombination och används som adress för datapaket som färdas över internet, vilket gör att miljarder digitala enheter som är anslutna till internet kan särskiljas från andra enheter (WhatIsMyIPAddress, 2014).

WiFi-teknologin är en av orsakerna till det ökade användandet av internet utanför hemmet och arbetsplatsen p.g.a. att det är ett billigt sätt att erbjuda tjänsten till allmänheten (Attipoe, 2013). Tack vare den omfattande tillgängligheten är det idag inte bara datorer och telefoner som har WiFi-funktionalitet. Det utvecklas allt från kylskåp till klockor med stöd för WiFi (Yoo, 2010). Den breda användningen av WiFi öppnar samtidigt upp möjligheten till missbruk så som datorintrång, avlyssning, åtkomstattacker och identitetsstöld, p.g.a. att all data som överförs mellan en klient och en AP i ett öppet WiFi-nätverk är exponerad för andra användare i nätverket (Attipoe, 2013; Hamid, 2003; Mülec, Vasiu, Frigura-Iliasa & Vatau, 2011; Pfleeger & Pfleeger, 2007; Rahman, Nowsheen, Khan & Khan, 2007).

Några av de andra fördelarna med WiFi-nätverk är att de är lätta att installera och underhålla, de gör att behovet av att dra kablar genom väggar och tak elimineras samt gör nätverket tillgängligt för ett stort antal användare samtidigt. I nätverket skickas data från användarens enhet via en radiolänk till en basstation, Access Point, som ofta samtidigt innehåller en router. Basstationen är normalt trådbundet anslutet direkt till internet genom en Ethernet-kabel eller till ett DSL-modem (Hamid, 2003).

2.1.2 Potentiella risker

Trots de många fördelar som öppna WiFi-nätverk erbjuder medför teknologin även en säkerhetsrisk då nätverk och användare kan bli angripna och information kan utnyttjas i kriminella syften. Nedan presenteras de vanligaste attackerna en användare kan råka ut för.

2.1.2.1 Man-in-the-middle-attacker

Man-in-the-middle-attacker (fortsättningsvis MITM-attacker) är en form av tjuvlyssning eller manipulation av datatrafik. För att utföra en MITM-attack måste angriparen komma in mellan en klient och den AP som offret använder för att komma åt privat data (Pervaiz, Cardei & Wu, 2007; Waliullah & Gan, 2014). Den genuina AP kommer då att se angriparen som en auktoriserad användare, vilket resulterar i att bägge parterna misslyckas med att upptäcka angriparen och fortsätter att överföra data (Mulëc et al. 2011; Pervaiz, Cardei & Wu, 2007; Waliullah & Gan, 2014). Eftersom det i öppna nätverk inte finns någon säkerhetsmekanism som kontrollerar integriteten eller verifieringen av användaren är det en potentiell säkerhetsbrist som kan utnyttjas i MITM-attacker (Mulëc et al. 2011).

Det finns två typer av MITM-attacker, tjuvlyssning och manipulation. Tjuvlyssning kan delas upp i två kategorier, passiv tjuvlyssning och aktiv tjuvlyssning. Passiv tjuvlyssning går ut på att en angripare övervakar all data som användaren skickar ut och därmed har möjlighet att spara och analysera datatrafiken (Mülec et al. 2011). Vid en aktiv tjuvlyssning sätter angriparen upp en egen AP med ett namn som lockar användare att ansluta sig till den (Waliullah & Gan, 2014), exempelvis ”FREE AIRPORT WiFi” (se avsnitt 2.1.2.4). När användaren väl har anslutit sig till angriparens AP kan angriparen avlyssna all data som användaren skickar över nätverket (Mülec et al. 2011). Manipulation tar tjuvlyssning ett steg längre, då angriparen kan manipulera och maskera datan skickad i nätverket och ändå få mottagaren att tro att datatrafiken är skickad från en legitim källa (Mülec et al. 2011).

I öppna WiFi-nätverk är det relativt enkelt att utföra tjuvlyssning eftersom åtkomsten till data inte är begränsad av någon viss fysisk punkt och radiosignalerna går att övervaka med enkla programvaror, både i realtid och i efterhand (Mülec et al. 2011). Med fysisk punkt menas att nätverkssignalerna kan gå igenom tak, väggar och fönster långt utanför själva byggnaden där AP finns (Rahman et al. 2007). Då signalerna färdas genom luften är det lättare för en obehörig att komma åt signalerna än vid trådbunden kommunikation. Trådlös kommunikation sker på olicensierade offentliga frekvenser som enkelt kan avlyssnas av vem som helst. Datatrafiken i ett öppet trådlöst nätverk blir därmed mycket svår att skydda (Hamid, 2003; Rahman et al. 2007).

Ett stort problem är att det är oerhört svårt att upptäcka en MITM-attack. Johnston (2014) menar att även om principerna för att upptäcka attackerna är kända finns det inget utarbetat arbetssätt för att göra det. Han presenterar vidare de tekniskt specifika detaljerna som undersöks för att upptäcka attackerna, vilka kräver omfattande kunskaper för att kunna förstås. Då en normalanvändare inte har sådana kunskaper är det näst intill är omöjligt för denne att upptäcka en MITM-attack.

2.1.2.2 MAC-address spoofing

En MAC-adress är en enhets unika, fysiska adress som hjälper klienter och AP att identifiera vem de kommunicerar med. MAC-adresser kallas även för maskinvaruadresser, finns i varje enhet med ett nätverkskort och består av 12-siffriga hexadecimala tal (Mitchell, 2014). Olyckligtvis är MAC-adressen aldrig krypterad varpå en angripare kan konfigurera sin egen AP att ha en legitim MAC-adress. Attacken kallas MAC-adress spoofing och angriparen kan då utnyttja MAC-adressen för att utföra någon typ av bedrägeri (Hamid, 2003; Mülec et al. 2011; Pfleeger & Pfleeger, 2007; Rahman et al. 2007). De flesta protokoll för

nätverkskommunikation har inga rutiner för att styrka källan eller destinationen för ett meddelande, vilket gör dem sårbara för MAC-adress spoofing-attacker eftersom möjligheten att kontrollera identiteten på avsändare eller mottagare saknas. MAC-adress spoofing kan bl.a. användas i samband med tidigare nämnda MITM-attack (Mülec et al. 2011; Pfleeger & Pfleeger, 2007; Rahman et al. 2007).

2.1.2.3 Denial-of-Service

Denial-of-Service-attacker (fortsättningsvis DoS-attacker) är ett försök att göra en maskin eller nätverksresurs otillgänglig för de avsedda användarna (Guynes, Wu & Windsor, 2011; Hamid 2003; Pfleeger & Pfleeger, 2007; Rahman et al. 2007). DoS-attacker är ett stort problem i internetsammanhang (Guynes, Wu & Windsor, 2011) och är den vanligaste typen av attacker för att angripa ett specifikt offer (Waliullah & Gan, 2014). Vid en DoS-attack kan en angripare göra ett nätverk otillgängligt för en användare, något som vanligtvis inte orsakar några större skador för den enskilda användaren utan endast skapar frustration över att inte komma åt nätverket. En angripare kan dock använda attacken för att få användare att ansluta till ett annat nätverk istället (se avsnitt 2.1.2.4).

2.1.2.4 Rogue Access Point

Rogue Access Points (fortsättningsvis RAP), även kallad Evil Twin, utgör en stor fara för användare av öppna WiFi-nätverk (Waliullah & Gan, 2014). Attacken startar genom att angriparen installerar en öppen AP med ett SSID (namn på nätverket) dit användare kan koppla upp sig (Nussel, 2010; Waliullah & Gan, 2014;). SSID kan vara i princip vad som helst, men angripare använder ofta redan existerade nätverksnamn som användare tidigare har varit uppkopplade till. Vanligtvis är användarnas enheter konfigurerade så att de kopplar upp sig automatiskt till kända nätverk när de kommer inom räckvidden av en AP (Nussel, 2010; Waliullah & Gan, 2014). Genom att angriparens AP har en bättre signalstyrka eller genom att ha placerat åtkomstpunkten på en plats där det ursprungliga nätverket inte är tillgängligt kan angriparen få offret att koppla upp sig på angriparens nätverk. Problemet är särskilt stort på offentliga platser som inte använder någon kryptering på sina nätverk, vilket resulterar i att klienten inte kan skilja mellan en harmlös och en skadlig AP (Nussel, 2010). Angriparen kan sedan övervaka och manipulera trafiken på nätverket och komma åt känslig information (Rahman et al. 2007).

Ett exempel på en RAP-attack kan vara att en angripare sätter sig på ett café som har ett öppet WiFi-nätverk med SSID ”Café Free WiFi”. Om angriparen stänger ner caféets AP, till exempel genom tidigare beskrivna DoS-attack, eller kan tillhandahålla en starkare signal med SSID ”Café Free WiFi” kommer alla användare som tidigare kopplat upp sig på ”Café Free WiFi” nu att koppla upp sig på angriparens AP.

2.1.3 Säkerhetsteknik

Nedan presenteras ett urval av de tekniska säkerhetsåtgärder som finns tillgängliga för att säkra anslutningar på internet. De är inte alla specifikt kopplade till öppna WiFi-nätverk, men relevanta för studien för att få en helhetsbild av området.

2.1.3.1 WEP

WEP (The Wired Equivalent Privacy) är en krypteringsstandard som skapades 1999 av IEEE för 802.11-standarden. Standarden implementeras för att skydda datakommunikationen mellan en klient och en AP. WEP skulle tillhandahålla samma säkerhetsstandarder som i trådbundna nätverk med privatisering, autentisering och dataintegritet. Redan när WEP

introducerades var man dock medveten om säkerhetsbristerna i WEP, men det var den enda säkerhetsstandarden som fanns på den tiden och användes därför. Problemet med WEP var bl.a. att det krypterade datat bestod av 64 bitars statiska paket som var så pass små att det snabbt gick att dekryptera dem (Pervaiz, Cardei & Wu, 2007). Paketen var även statiska, vilket innebar att det endast krävdes en dekryptering för att komma åt informationen (Lehembre, 2005). Idag finns inte WEP längre på marknaden men en del äldre enheter använder sig fortfarande av tekniken.

2.1.3.2 WPA/WPA2

År 2003 lanserade Wireless Fidelity Alliance säkerhetsstandarden WPA (Wi-Fi Protected Access) för att hantera de kryptografiska bristerna i WEP. En av de stora fördelarna med WPA gentemot WEP var användandet av utbytbara nycklar istället för statiska nycklar för att kryptera paketen. Även MIC (Message Integrity Check) infördes för att bekräfta att ett paket inte hade blivit manipulerat under överföringen. Storleken på de krypterade paketen utökades också vilket skulle göra dem svårare att dekryptera (Pervaiz, Cardei & Wu, 2007).

År 2004 infördes WPA2 som baserade sig på samma teknologi som WPA men använde sig av en förbättrad krypteringsteknologi, CCMP (Counter Mode CBC-MAC Protocol). Efter lanseringen av WPA2 blev det obligatoriskt att alla enheter med WiFi skulle stödja WPA2-teknologin (Lehembre, 2005). Ett problem som uppkom vid lanseringen av WPA och WPA2 var att de flesta AP som var tillverkade före år 2003 inte stödde standarderna, vilket ledde till att flera nätverk förblev osäkra även om en ny och säkrare standard hade införts (Pervaiz, Cardei & Wu, 2007). Det har även bevisats att det går att dekryptera lösenord för ett nätverk med WPA/WPA2 (Lehembre, 2005).

2.1.3.3 VPN

VPN (Virtual Private Network) är en teknik som används för att skapa en säker uppkoppling mellan två punkter i ett osäkert nätverk. VPN-tekniken använder sig av IPSec (Internet Protocol Security) som gör att anslutningen blir autentiserad samtidigt som den tillhandahåller integritet och sekretess för anslutningen. I praktiken innebär det att en ”tunnel” skapas mellan två punkter i ett nätverk. IPSec utvecklades specifikt för att stödja säkert utbyte av paket vid anslutning till osäkra nätverk. I en typisk VPN-koppling startar en klient en virtuell punkt-till-punkt-anslutning till en fjärrserver över internet. Fjärrservern besvarar samtalet och autentiserar klienten för att möjliggöra dataöverföring mellan VPN-klienten och det nätverket klienten vill koppla sig till. VPN används flitigt i organisationer och företag för att möjliggöra säkert arbete på internet utanför kontoret (Pervaiz, Cardei & Wu, 2007).

2.1.3.4 SSL

SSL (Secure Socket Layer) är ett av de mest använda säkerhetsprotokollen i internetsamfundet där HTTPS är den mest kända tillämpningen av protokollet (Symantec, 2012). SSL tillför ett krypterat säkerhetsprotokoll till internetkommunikationen som säkrar identitetsautentisering genom certifikat och tillhandahåller en säker anslutning genom integritetskontroll (McKinley, 2003). SSL säkerställer att den känsliga informationen som utbyts via webbplatsen och användaren inte kan avlyssnas eller läsas av någon annan än den avsedda mottagaren (Symantec, 2012).

När en person startar sin webbläsare för att navigera till en webbplats med SSL-certifikat sker en SSL-handskakning. Handskakningen är ett utbyte av en publik nyckel som används för att kryptera informationen och en privat nyckel som används för att dekryptera informationen (Symantec, 2012). Handskakningen sker mellan webbläsaren (klienten) och applikationen (servern) (McKinley, 2003; Symantec, 2012). När handskakningen har genomförsts uppenbarar sig i de flesta webbläsare ett lås samt adress-prefixet HTTPS och krypteringen är klar. Krypteringen skapar en säker ”tunnel” till webbplatsen som förhindrar obehöriga från att läsa data utan att bli upptäckta (Blue Coat, 2008).

2.2 Användaren och risktagande

I avsnittet nedan presenteras forskning kring riskmedvetenhet, risktagande och människans förmåga att ta till sig varningar. Vidare presenteras forskning kring phising-sidor, där skillnader mellan aktiva och passiva varningar och hur varningarna bör utformas undersökts. Avslutningsvis presenteras forskning kring användares beteende på öppna WiFi-nätverk.

2.2.1 Riskmedvetenhet

> *"Security is both a feeling and a reality. And they're not the same."* (Schneier, 2008 s. 1)

En av anledningarna till att attacker mot användare som kopplar upp sig på öppna WiFi-nätverk är genomförbara är att användarna inte är medvetna om de säkerhetsrisker de utsätter sig för, vilket resulterar i att de inte är rädda för att någonting ska gå fel (Klasnja et al. 2008). Även om det kan vara svårt att avgöra hur stor potentiell säkerhetsrisk öppna WiFi-nätverk utgör, går det enligt Schneier (2008) att beräkna säkerhetsrisker under alla omständigheter, givet att det finns tillräckligt med data. Genom att använda sig av parametrar som antal attacker, frekvens i användandet av öppna WiFi-nätverk, säkerheten i nätverken och andra faktorer som påverkar, bör det således även gå att räkna ut säkerhetsrisker vid interaktion med öppna WiFi-nätverk. Problemet är dock att användare ofta känner sig säkra trots att de i själva verket inte är det (Attipoe, 2013) och att det i princip är omöjligt för användare att upptäcka en attack (Johnston, 2014). Schneier (2008) beskriver flera orsaker till varför en användare kan ha en falsk säkerhetsbild. I likhet med *prospect theory*, en teori som vanligtvis används för att förklara ekonomiskt risktagande, väljer användaren bort säkerhet till förmån för enkelhet och tillgänglighet. Ett antal mänskliga fördomar spelar också in, framför allt den *optimistiska fördomen*. Fördomen innebär att människor inte tror att någonting som inträffar andra ska kunna hända dem själva, eftersom det känns allt för avlägset. De upplever en känsla av säkerhet, vilket inte är samma sak som att faktiskt vara det. En felaktig bild av säkerhetsriskerna kan få negativa konsekvenser (Schneier, 2008).

Garg och Camp (2012) menar på att människor har svårare att utvärdera virtuella säkerhetsrisker än fysiska risker. Det beror bland annat på avsaknad av mätparametrar och svårigheter att förstå säkerhetsvarningar. Schneier (2008) är inne på samma tema när han talar om att personifierade risker uppfattas som ett större hot än anonymiserade risker, vilket beror på att användaren inte kan koppla hotet till verkligheten. Ett system, oberoende av vilken typ av system det rör sig om, utformas utifrån ett antal experters mentala modell av säkerhet. Modellen stämmer dock sällan överens med användarnas bild av säkerhet, vilket resulterar i att användarna inte beter sig så som experterna förväntat sig. För att på ett effektivt sätt kunna förmedla risker och möjliggöra ett säkert systemanvändande krävs därför förståelse för hur användarna uppfattar risker och vilka risker de är villiga att ta (Garg & Camp, 2012).

Människor fattar beslut genom att väga risker mot potentiella vinster (Garg & Camp, 2012) och föredrar en liten säker vinst framför en osäker större vinst (Schneier, 2008). Attityden verkar dock inte återspeglas i människans vilja att ta risker, där en potentiell stor förlust är att föredra framför en liten, säker förlust. Att hantera risk handlar enligt Schneier (2008) om att kompromissa. Problemet som uppstår i virtuella miljöer är att människan har lätt att se vinsterna och fördelarna med IT, men har svårare att uppfatta riskerna. Schneier (2008) menar också på att användare kan ha svårt att ta till sig siffror och statistik, medan en personlig historia kan lämna ett mer bestående avtryck. En person som berättar att deras identitet blivit kapad kan därför ge ett kraftfullare intryck än statistik som visar hur många

människor som årligen får sin identitet kapad. Vidare pekar Schneier (2008) på fem aspekter där kompromissen mellan risk och vinst kan gå fel:

1. Hur allvarlig är risken?
2. Hur troligt är det att något går fel?
3. Hur stor omfattning har potentiella kostnader?
4. Hur effektivt dämpar motåtgärderna risken?
5. Hur kan risker och kostnader jämföras?

Om en aspekt bedöms felaktigt av användaren kan det få oönskade konsekvenser. En undersökning av Attipoe (2013) visar att användare har en falsk säkerhetskänsla när de använder sig av öppna WiFi-nätverk, att de generellt sett saknar kännedom om säkerhetsriskerna eller att de helt enkelt inte förstår sig på dem. 60 % av deltagarna i undersökningen ansåg även att det inte var deras ansvar att skydda sig när de var uppkopplade mot nätverket och 58 % litade på att nätverksleverantören eller de som satt upp nätverket såg till att det var säkert. Det visar på en övertro på att det Schneier (2008) kallar motåtgärderna, som över hälften av användarna inte anser sig behöva ta ansvar för, skall hålla dem säkra. Attipoe (2013) hävdar vidare att ansvaret för att skapa säkerhet i öppna WiFi-nätverk är delat mellan leverantörer och användare, men endast 40 % av användarna ansåg att de aktivt behövde göra något för att bli säkra. Undersökningen visar att 21 % av användarna uppfattade publika trådlösa nätverk som säkra medan 44 % inte visste vad de trodde om säkerheten. Återigen har användarna en felaktig bild av verkligheten, eftersom de inte förstår hur allvarlig riskerna är. 62 % av deltagarna kände inte till någon säkerhetsrisk vid interaktion med nätverken och de med kännedom om riskerna ansåg att “hacking” var det största hotet (Attipoe, 2013). Det finns uppenbarligen en naivitet hos användarna och en attityd som pekar på att de inte tror att någonting kan gå fel.

I en artikel i USA Today skriver Lawson (2013) att 12,5 miljoner amerikaner under 2012 utsattes för identitetsstöld - många på grund av oaktsamhet vid interaktion med öppna WiFi-nätverk. Även om användarna kan ha en felaktig säkerhetsbild visar Garg och Camp (2012) i sin undersökning att integritetskränkningar som identitetsstöld toppar listan över vad anvndarna inte vill råka ut för, följt av virus, spionprogram och trojaner. De menar att det kan vara formuleringarna i sig som kan påverka användarnas oro - ord som stöld, virus och spion är vardagliga ord som användaren kan relatera till, vilket kan hjälpa dem att få grepp om de virtuella och anonyma säkerhetsriskerna (Garg och Camp, 2012).

2.2.2 Visualisering av risker

Tekniker för att visualisera potentiella risker har bland annat använts för att motverka phishing-sidor på internet. Phishing innebär att en angripare sätter upp en webbplats snarlik en organisations legitima hemsida i syfte att utnyttja användarna som besöker den. Verktyg för att motverka phishing har fokuserat på att varna användarna snarare än att blockera sidor, då det varit svårt att automatiskt upptäcka sidorna. Historiskt sett har teknikerna inte haft någon större genomslagskraft och användarna har stannat kvar på sidan trots varningar (Egelman, Cranor & Hong, 2008). En studie av Egelman, Cranor och Hong (2008) pekar på att användare inte tror eller litar på passiva varningar, till exempel pop-up-rutor med varningar som inte kräver att användare gör ett aktivt val (se bild 1), något som också bekräftas av Cranor (2006) och Dhamija, Tygar och Hearst (2006). Egelman, Cranor och Hong (2008) ställde i sin undersökning deltagarna inför valet att fortsätta på en webbsida trots att de fått en varning om att sidan eventuellt kan vara en phising-sida. Endast 13 % av deltagarna valde att agera utifrån en passiv varning (se bild 1) och lämna sidan, medan 79 % lämnade sidan efter en aktiv varning (se bild 2). Undersökningen av Dhamija, Tygar och Hearst (2006) visade även att 23 % av användarna inte ens lade märke till de passiva varningarna och att upp till 90 % av användarna blev lurade av en väldesignad phising-sida. Det kan bero på att säkerhet inte är användarens primära mål och att de därför inte uppfattar varningarna, eftersom de är allt för fokuserade på sitt huvudsakliga mål (Dhamija, Tygar &

Hearst, 2006). Om en varning då inte förmedlar riskfaktorer på ett tillräckligt genomslagskraftigt sätt kommer användaren att ignorera den och därmed kommer den inte fylla sitt syfte (Egelman, Cranor & Hong, 2008; Schneier, 2008). En väldesignad varning måste förmedla en känsla av fara och presentera åtgärder användaren kan ta för att motverka faran (Egelman, Cranor & Hong, 2008; Kahneman, 2003). Om det går att visualisera potentiell fara på ett bra sätt kan även faktorn som Schneier (2008) beskriver, att användare tenderar att känna sig säkra trots att de inte är det, motverkas.

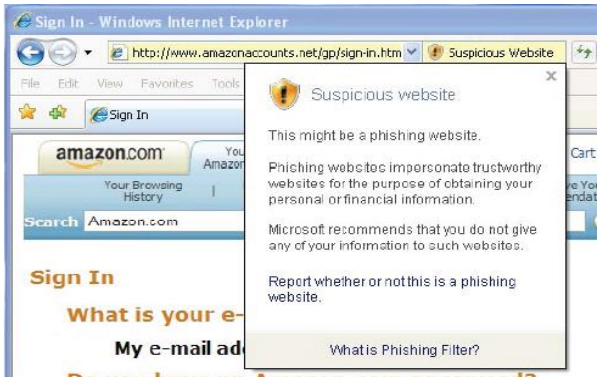

Bild 1. Passiv varning *Bild 2. Aktiv varning*

*Skillnaden mellan en passiv och en aktiv varning (*Egelman, Cranor & Hong*, 2008, s 2)*

Det finns flera faktorer som påverkar hur en användare uppfattar en säkerhetsvarning. Wogalter (2006) och Cranor (2006) menar att det finns ett antal frågor som måste besvaras för att ta reda på om ett varningsmeddelande är effektivt. Modellerna är snarlika och innefattar stegen:

1. Uppfattar användare varningsindikationerna?
2. Förstår användarna vad indikationerna syftar till? Vet de vad de ska göra när de ser indikationerna?
3. Tror de på varningarna?
4. Är användarna motiverade att agera utifrån indikationerna?
5. Kommer användarna att agera?
6. Hur interagerar indikationerna med andra indikationer?

Om något steg inte uppnår den avsedda effekten påverkas användarens förmåga att uppfatta och agera utifrån säkerhetsriskerna i likhet med det ovan nämnda aspekterna presenterade av Schneier (2008). Cranors (2006) modell innefattar ytterligare steg som behandlar frågan om huruvida användare fortsätter med sitt beteende över tid och även berör mer tekniska aspekter, bland annat genom att undersöka om varningen går att manipulera av en angripare. Även om användaren skulle uppfatta varningen är det dock inte säkert att användarna vidtar säkerhetsåtgärder, trots att de finns lättillgängliga (Garg & Camp, 2012). Därmed är det det viktigt att förstå om användaren tänker över sina val eller om de agerar spontant utan vidare reflektion. Egelman, Cranor och Hong (2008) studerade hur användare reagerade på säkerhetsvarningar. Användarna visade på ett spontant beteende och avfärdade säkerhetsvarningarna med förklaringen att de alltid kom upp eller att de tidigare ignorerat dem och ändå inte råkat ut för något. Dhamija, Tygar och Hearst (2006) drar även slutsatsen att varken ålder, kön eller datorvana spelar roll för hur användare uppfattar säkerhetsvarningar på phising-sidor eller hur de agerar utifrån dem. Så vad är det som påverkar användaren att tänka över sina val när de ställs inför en säkerhetsvarning?

Det finns två typer av tänkande och beslutsfattande: det resonerande och det intuitiva (Kahneman, 2003; Slovic & Peters, 2006). Resonerande är en medveten handling, t.ex. en

reflektion eller en beräkning. Ett intuitivt beslutsfattande är däremot spontant och något vi människor gör per automatik. Forskningen visar att de flesta tankar och handlingar sker på en intuitiv basis, även om människan inte agerar på alla impulser (Kahneman, 2003; Schneier, 2008; Slovic & Peters, 2006). Det intuitiva beslutsfattandet baseras på intryck som kan kopplas till Wogalters (2006) och Cranors (2006) modell över hur användare uppfattar, förstår, tror och reagerar på varningar. En varning måste dra till sig uppmärksamhet och göra intryck på användaren. För att intrycket skall ge någon bestående effekt måste användaren förstå vad indikationen syftar på och hur de ska agera utifrån informationen. Kahneman (2003) visar tre specifika ordval för att få användaren att förstå omfattningen av en säkerhetsrisk: Danger, Warning och Caution. Orden används i en fallande skala där Danger anses ha störst genomslagskraft, men endast bör användas om det finns en fara för användarens liv. Wogalters (2006) menar att användare som har kännedom om området där den potentiella faran kan uppstå har en tendens att lita på sina tidigare erfarenheter istället för att reagera på varningssignaler. Om användaren däremot saknar erfarenhet om området är det troligare att de tvivlar på källan och litar på säkerhetsvarningen. Tvivel hamnar i kategorin resonerande beslutsfattande, medan medvetenhet och tidigare erfarenheter hamnar i intuitivt tänkande (Kahneman, 2003). För att få användarna att reflektera över sin säkerhet är det därför viktigt att få dem att hellre lita på säkerhetsvarningar än på tidigare erfarenheter.

2.2.3 Användares beteende på öppna WiFi-nätverk

För att ta reda på vad användarna faktiskt gör när de interagerar med öppna WiFi-nätverk genomförde Klasnja et al. (2008) en undersökning som visade att deltagarna använde en rad olika applikationer, så som internethandel, internetbank och sociala medier, när de var uppkopplade mot nätverken. Undersökningen visade även att användarna hade god kunskap om hur de skulle använda sig av öppna WiFi-nätverk, men att de inte visste hur den bakomliggande teknologin fungerade eller vilka säkerhetsrisker de utsatte sig för. Vidare visade det sig att användarna hade en god uppfattning av hur långt en WiFi-signal sträcker sig, erhållet via egna erfarenheter, och att signalstyrkan på nätverket var en bidragande faktor till att de valde just det nätverket (Klasnja et al. 2008).

Klasnja et al. (2008) visar vidare att användarna i undersökningen var oroliga för att en “hacker” skulle ta sig in i deras dator och läsa deras filer, även om de trodde att risken för det var låg eftersom de ansåg att det behövdes en oerhört skicklig person för att kunna genomföra en sådan attack. Värt att anmärka är att användarna var nästan lika oroliga för “hackers” som för att någon fysiskt närvarande skulle titta vad de gjorde på datorn. Det användarna oroade sig allra mest för var att någon skulle stjäla deras bankinformation eller deras identitet. Majoriteten av användarna gjorde inte bankärenden eller handlade online när de var anslutna till ett öppet nätverk, även om vissa utförde de aktiviteterna eftersom de litade på att bankens hemsida skötte säkerheten. Ingen av användarna trodde att det fanns en risk för att nätverket var uppsatt av någon med intentioner att avlyssna deras trafik, även vid de tillfällen då nätverksnamnen var okända för dem. När användarna fick reda på vilken information de exponerat under en månads tid blev de oroliga och reflekterade över hur de egentligen beter sig på öppna WiFi-nätverk. Resultatet från undersökningen visar att hoten kan orsaka allt från mild oro till allvarliga problem och att användare är reaktiva och inte proaktiva (Klasnja et al. 2008), något som bekräftas av Schneiers (2008) beskrivning av hur vi människor lär oss vad som är farligt först efter det inträffat. Klasnja et al. (2008) föreslår en teknisk lösning för att visualisera användarnas nätverkstrafik men poängterar att användarna inte vill gå runt och vara rädda när de egentligen är säkra.

3. Metod

För att besvara vår frågeställning har vi använt oss av metoder som undersöker både den tekniska och den mänskliga aspekten av problemområdet. Vi tog fram en teoretisk bakgrund som gav oss en bred grund för vår undersökning. Vi valde även att utföra en semi-strukturerad intervju med en områdesexpert för att fördjupa vår kunskap om aktuella säkerhetsfrågor och få riktlinjer för vad vi borde fokusera på. För att undersöka om medvetenheten om säkerhetsriskerna kan ökas genom att enbart informera användarna genomfördes en enkätundersökning där skillnader mellan användare med IT-relaterad sysselsättning och övriga användare undersöks. Vi gjorde även observationer av nätverkstrafiken i öppna WiFi-nätverk för att undersöka vilken information vi kunde ta del av. Vi ansåg att det enda sättet att skaffa en tillräckligt bred grund för att besvara vår frågeställning var att använda oss av varierande metoder. Patel och Davidsson (2011) menar även att användandet av flera metoder ger en tydligare och bättre bild när informationen från de olika metoderna slås ihop.

3.1 Dokumentanalys

Genom studier av tidigare forskning skaffade vi en bred kunskapsbas att bygga vår intervju, enkätundersökning och observation på. Litteraturen söktes upp från Göteborgs universitetsbibliotek och fokus låg på att hitta artiklar rörande WiFi-teknologi, säkerhetsrisker i öppna WiFi-nätverk, användares riskperception och användares förmåga att ta till sig varningar. Då teknologin hela tiden utvecklas har vi tvingats välja bort forskning som inte längre är relevant, på grund av att teknologin har utvecklats, och kompletterat med ett antal källor från internet. Studierna grupperades i två huvudkategorier, den tekniska aspekten av säkerheten och den mänskliga aspekten av risktagande och riskperception. Även om uppsatsens fokus ligger på användaren och dennes uppfattning av säkerhet krävdes en övergripande teknisk förståelse för att kunna angripa problemområdet.

3.2 Kvalitativ intervju med områdesexpert

Vi har genomfört en kvalitativ, semi-strukturerad intervju med Jakob Schlyter, nätverks- och IT-säkerhetsexpert på företaget Kirei, som arbetat med kunder som Finansdepartementet, Försvarsmakten, SEB och .SE (Stiftelsen för internetinfrastruktur). Intervjun genomfördes på ett av informanten föreslaget café. I intervjun använde vi frågeställningar framtagna utifrån Patel och Davidssons (2011) riktlinjer för semi-strukturerade intervjuer, som lämnade utrymme åt informanten att svara fritt utan att tappa fokus från huvudområdet. Intervjun gav oss en djupare förståelse för nätverkssäkerhet, risker vid nätverksanvändning samt nya aspekter och tankar kring området. Då Schlyters expertis var omfattande kom även hans egna åsikter om säkerhet och problematiken kring öppna WiFi-nätverk att ligga i fokus. Vår strävan var att hålla intervjun på en övergripande nivå för att få relevant information angående sambandet mellan tekniken och användaren istället för att fokusera för mycket på tekniken. Intervjun spelades in på en mobiltelefon och pågick i ungefär en timme. Genom att spela in intervjun gavs vi en möjlighet att fånga informantens uppfattningar och tolkningar, samtidigt som vi på ett smidigt sätt kunde hålla igång samtalet (Patel och Davidsson, 2011). Intervjun avslutades med att informanten reflekterade över vårt arbete och gav diverse tips och råd om vad vi kunde undersöka djupare. Det var viktigt att vi hade läst på om ämnet innan vi utförde intervjun för att kunna få ut så mycket som möjligt av den, men även för att hålla informanten motiverad. Att visa intresse och förståelse för informanten är något även Patel och Davidsson (2011) beskriver som nödvändigt.

3.3 Enkätundersökning

En del av studiens empiri baserar sig på en enkätundersökning enligt Patel och Davidsons (2011) struktur för enkäter med fasta svarsalternativ. Vi fick in 173 svar från varierande ålders- och yrkeskategorier. Utifrån resultatet från undersökningen kunde vi dra slutsatser rörande hur användare interagerar med öppna WiFi-nätverk, hur de uppfattar riskerna kopplade till nätverken samt undersöka skillnader mellan användare med IT-relaterad sysselsättning och övriga användare. En fördel med metoden var att vi hade möjlighet att nå ut till ett stort antal användare för att på så sätt få ett brett perspektiv på frågan. Enkäten utformades och distribuerades i olika intressegrupper på Facebook för att nå så många människor som möjligt. Vi strävade efter att nå användare i olika åldrar och med varierande yrken, varpå vi valde varierande grupper med olika sorters användare. En stor del av svaren kom från studenter, något som Schneier (2008) beskriver som vanligt i forskningssammanhang. Enkätsvaren har gjorts anonymt vilket ökar chansen att vi har fått sanningsenliga svar.

Deltagarna i enkäten delades upp i två kategorier, de med IT-relaterad sysselsättning och de med övrig sysselsättning. Utifrån kategoriseringen kunde vi undersöka om medvetenheten om säkerhetsrisker i öppna WiFi-näterk skiljer sig mellan de som har en teknisk kunskap och de som inte har det. Genom att jämföra resultaten från IT-relaterade användare och övriga kunde vi dra slutsatser om en ökad kännedom om problemområdet medför en ökad medvetenhet. Weber och Hsee (1998) visar att det finns kulturella skillnader som påverkar användarnas riskmedvetenhet och därmed ansåg vi inte att forskning kring användares säkerhetsmedvetande i andra länder var direkt applicerbara på svenska användare.

3.4 Observation

För att undersöka hur enkelt det är att ta del av information som skickas i öppna WiFi-nätverk genomförde vi en observation av nätverkstrafiken och satte upp vårt egna öppna WiFi-nätverk. Då observationer kan hjälpa forskaren att förstå undersökningens målgrupp på ett bättre sätt (Sharp, Rodgers & Preece, 2007) har vi genom att anta rollen som det Patel och Davidson (2011) kallar en okänd, icke deltagande observatör kunnat observera användare i deras naturliga miljö. Eftersom det i princip är omöjligt att studera användandet av öppna WiFi-nätverk genom en rent visuell observation, då det inte går att avgöra vilken typ av aktiviteter som sker på nätverken, valde vi att observera trafiken på nätverken. En viktig framgångsfaktor var att i förväg studera verktyget Wireshark, ett gratisprogram som möjliggör övervakning av nätverkstrafik. Verktyget gör det bland annat möjligt att se vilka användare som är uppkopplade till nätverket i form av MAC-adresser och att övervaka trafiken de skickar och tar emot.

Observationen delades upp i två delar, då vi ville undersöka vilka sidor användare besöker på öppna WiFi-nätverk och även se hur många som aktivt ansluter sig till ett tidigare okänt nätverk. I den första delen låg fokus på att utföra övervakning av trafiken på öppna WiFi-nätverk. Nätverken vi övervakade tillhandahölls av platserna vi utförde observationen på, vilka valdes baserade på svaren vi fått från enkätundersökningen. Undersökningen visade att användare ofta kopplar upp sig på öppna WiFi-nätverk på caféer och restauranger (se bild 3), varpå första delen av observationen utfördes på sådana platser. Under de åtta timmar vi övervakade trafiken filtrerade vi datan med hjälp av Wireshark för att få fram IP-adresser tillhörande olika webbsidor. Genom observationen fick vi reda på vilka sidor användare besöker på öppna WiFi-nätverk och kunde därmed även undersöka vilka risker de utsätter sig för.

För att undersöka användarnas inställning till att ansluta sig till tidigare okända nätverk satte vi upp en egen WiFi-hotspot på en allmän plats i Göteborg. Kravet på platsen för vår observation var att det skulle finnas mycket människor i omlopp, samtidigt som de inte enbart fick passera förbi. Vi valde Göteborgs Centralstation och bestämde nätverksnamn baserat på olikheterna i namnens betoning. Utifrån forskningen av Kindberg et al. (2008) formulerade vi en hypotes att användare har en benägenhet att koppla upp sig på nätverk med ett SSID knutet till platsen de befinner sig på, medan de undviker allmänna SSID. För att undersöka hypotesen varierade vi namnet på vårt nätverk. Det första namnet betonade att det var ett gratis WiFi (”Free WiFi”), det andra var ett platsspecifikt namn (”Centralen WiFi”) och det tredje var ett allmänt, tillintetsägande namn (”WiFi”). Där vi befann oss under vår observation fanns det sex andra öppna WiFi-nätverk tillgängliga: “SJ”, “WLAN Zone The Cloud”, “espressohouse”, “All Station Guests”, “homerun” och “mycloud”. Inget av nätverken gav vid vår position full signalstyrka, något som förmodligen gynnade vår observation eftersom användare tenderar att välja det nätverk som har starkast signalstyrka (Klasnja et al. 2008; Mülec et al. 2011). Syftet med observationen var att studera användarnas benägenhet att ansluta sig till tidigare okända öppna WiFi-nätverk, att försöka förstå vilka underliggande faktorer som kan spela roll för användandet samt undersöka hur enkelt det är för en angripare att få användare att ansluta sig till deras nätverk. Observationen liknar de förberedelser som krävs för att utföra en RAP-attack (se avsnitt 2.1.2.4) och resultatet visar därmed även hur många användare som utsatt sig för risken av denna specifika typ av attack. Vårt nätverk var okrypterat och krävde inget lösenord för att få tillgång till internet.

Då många av de risker användare utsätter sig för kan kännas abstrakta och svåra att definiera ville vi också testa hur informationen vi fick fram kunde utnyttjas Då vi ur ett etiskt och lagligt perspektiv inte kunde använda data från våra observationer valde vi att exemplifiera med ett praktikfall, där vi visar hur bland annat användarnamn och lösenord skickas i klartext över nätverken. För att besvara frågan skapade vi en kontrollerad laboratoriemiljö där vi kunde visa vilken information vi kunnat ta del av. Vi arbetade med två datorer, en placerad som angripare och en som en normalanvändare, uppkopplade till samma öppna nätverk. Inga andra enheter var anslutna till nätverket under laborationstillfället och nätverket sattes upp och kontrollerades av oss själva. Då vår enkätundersökning visade att många användare inte ens vet hur de skiljer mellan ett öppet och ett krypterat nätverk (se bild 8) valde vi att även undersöka vilken information som i dagsläget presenteras för användarna vid anslutning till öppna WiFi-nätverk.

3.4.1 Ramverk

Eftersom det i en öppen observation på fält kan vara svårt att hantera och analysera all data som genereras, samt att hålla fokus på rätt frågor och svar har vi följt ramverket presenterat av Sharp, Rodgers och Preece (2007):

The person – Vem använder tekniken under en speciell omständighet och tid? Vilka enheter används?
The place – Var används det? Vilka omkringliggande faktorer påverkar användaren?
The thing – Vad gör de på nätverken? Kopplar de upp sig mot okända nätverk?

Upplägget på observationen krävde att vi tog hänsyn till ytterligare aspekter. En viktig fråga var huruvida observationen var laglig och vilka etiska aspekter som berörde vår metod. Inför observation var vi kontakt med Polisen, Datainspektionen, Post- och Telestyrelsen samt ett antal jurister. Datainspektionen bekräftade att så länge vi inte sparade eller spred några personuppgifter skulle Personuppgiftslagen följas[1]. De jurister vi kontaktade kunde inte ge ett entydigt svar på frågan men hänvisade till lagen om elektronisk kommunikation (SFS 2003:389). Samma lag hänvisar Eva Fredriksson, advokat med specialkompetens inom IT- och telekomrätt, till då tidningen *PC för alla* genomförde en liknande observation (PC För

[1] Jurist på Datainspektionen, telefonsamtal den 15 april 2014

Alla, 2012). Fredriksson menar att flertalet lagar berörs, men att det inte är olagligt att övervaka trafiken i öppna WiFi-nätverk i Sverige eftersom den skickas via radiosignaler som finns tillgängliga för alla. För att säkerställa att det inte var olagligt att övervaka trafiken kontaktade vi Post- och Telestyrelsen som hänvisade oss till Polisen. Till slut fick vi tag på Jens Ahlstrand, chef för IT-forensiska sektionen i Västra Götaland. Han bekräftade att så länge det inte finns avtal mellan användaren och leverantören av nätverket och inga personuppgifter sparas är det inte olagligt[2].

Utifrån våra samtal med olika parter kunde vi dra slutsatsen att vi kunde utföra vår observation så länge det inte gick emot nätverkets användaravtal och inga personuppgifter sparades. När vi valde våra platser för observation kontrollerade vi om det fanns ett avtal och ändrade plats för observationen ifall vi stötte på användaravtal som förbjöd nätverksövervakning.

Även om observationen må vara laglig att utföra vill vi ta upp den etiska aspekten för observationen. Vi tog i vår observation hänsyn till de studerades integritet och anonymitet. Då ingen information om specifika användare eller deras IP-adresser sparades bröt vi inte heller mot personuppgiftslagen. Observationen registrerades enbart i form av att antalet inloggade användare under en session ökade och genom att de typer av webbplatser som besöktes registrerades.

3.4.2 Etiskt ställningstagande

Enligt The British Psychological Society (2010) skall inte observationsdeltagare utsättas för någon risk de inte hade råkat ut för i ett normalt sammanhang. Då mängden öppna WiFi-nätverk är såpass omfattande och något användarna troligtvis använder sig av anser vi att situationen räknas som ett normalt, om än av oss kontrollerat, sammanhang. Syftet med observationen medförde att användarnas godkännande inte gick att erhålla i förhand och därmed kunde vi inte söka det. Kindberg et al. (2008) genomförde en liknande observation och drar slutsatsen att ett av de främsta resultaten av arbetet var att slå fast att deras arbetssätt, “experimentiell metodologi”, var en avgörande faktor för deras resultat. När användare observeras i sin naturliga miljö påverkas inte deras beteende av några fabricerade faktorer vilket ger undersökningen ett mer trovärdigt resultat (Kindberg et al. 2008). För att undersöka hur frekvent användare ansluter sig till ett okänt WiFi-nätverk var det därmed av yttersta vikt att de inte var medvetna om vår observation.

3.5 Urval

Vi har använt oss av varierande skriftligt material som behandlar såväl tekniska som mänskliga aspekter och samlat material från flera olika källor för att kunna göra en omfattande studie. Valet av dokument gjordes utifrån Patel och Davidsons (2011) beskrivning för att få en så fullständig bild som möjligt av problemområdet. Kraven för våra tekniska källor var att de var relativt nyutgivna och aktuella, eftersom IT är ett område i ständig förändring. Vi valde att avgränsa undersökningen kring den tekniska delen då vi ansåg att omfånget vi redan hade var tillräckligt tidskrävande och omfattande. Valet att avgränsa just den tekniska delen togs eftersom fokus på vår undersökning låg på användaren och dennes interaktion med nätverket. Dock ansåg vi att det var nödvändigt att ge en övergripande bild av den tekniska delen för att kunna tydliggöra säkerhetsriskerna och för att läsaren skulle kunna förstå vårt resonemang.

[2] Jens Ahlstrand, chef för IT-forensiska sektionen hos Polisen, telefonsamtal den 24 april 2014

3.5.1 Presentation av urvalsgruppen

Intervju av Jakob Schlyter, rådgivare i nätverks- och IT-säkerhetsfrågor, Kirei.
Genom att intervjua en expert inom området fick vi synpunkter på vad vi skulle tänka på i vår undersökning. Vi fick även chansen att undersöka huruvida forskningsresultat vi tagit del av kunde tillämpas i verkligheten. Under intervjun ställde vi inga ledande frågor eller visade intentioner att vi var ute efter något specifikt svar, vilket är viktig för att få objektiva svar (Patel & Davidson, 2011).

Enkätundersökning med 173 stycken svarande från varierande ålders- och yrkeskategorier.
Urvalet av deltagarna var slumpartat eftersom vem som helst kunde fylla i vår internetenkät. Vi fokuserade dock på att i enlighet med Patel och Davidson (2011) distribuera undersökningen till varierande ålders- och yrkesgrupper för att få ett så täckande resultat som möjligt. Det gjordes genom att länka undersökningen i ett antal Facebook-grupper med olika typer av medlemmar, så som studentgrupper, föreningar och grupper kopplade till olika företag.

Observation på allmänna platser med slumpmässiga användare.
För att få ett resultat motsvarande ett realistiskt scenario valde vi att utföra vår observation på ett antal caféer och på Göteborgs centralstation. Vi ansåg även att det var av vikt att låta användare vara omedvetna om observationen för att få ett så sanningsenligt resultat som möjligt.

Det finns flera orsaker till att urvalsgrupperna ansågs vara intressanta för vår studie. Genom de olika metoderna fick vi åsikter och synpunkter av en expert, användarnas uppfattning över öppna WiFi-nätverk samt en verklig bild av hur användaren beter sig vid interaktion med öppna WiFi-nätverk. Enligt Patel och Davidson (2011) finns det inget rätt eller fel hur en kvalitativ studie skall genomföras utan man bör istället anpassa metoderna efter den rådande situationen och dess förutsättningar, vilket vi därför gjorde.

4. Resultat

4.1 Enkätundersökning

Resultatet av enkätundersökningen gav en tydlig bild av vilka aktiviteter användare utför på öppna WiFi-nätverk. Majoriteten av deltagarna (90 %) var mellan 19-39 år. Drygt hälften av deltagarna arbetade eller studerade inom IT medan resten hade annan huvudsaklig sysselsättning. 53 % av användarna uppgav att de ansluter till öppna WiFi-nätverk några gånger i veckan eller några gånger i månaden medan endast 6 % uppgav att de aldrig ansluter sig till öppna WiFi-nätverk.

Åldersfördelning	
Ålderskategori	**Antal svaranden**
0-18	1
19-24	75
25-29	55
30-39	25
40-49	10
50-59	5
60+	2
Totalt antal svar	**173**

Tabell 1

Huvudsaklig sysselsättning	
Sysselsättning	**Antal svaranden**
Studerar – IT-relaterat	72
Studerar – Övrigt	39
Arbetar – IT-relaterat	19
Arbetar – Övrigt	41
Annat	2
Vill inte uppge	0
Totalt antal svar	**173**

Tabell 2

Undersökningen visade vidare att användandet av och medvetenheten kring säkerhetsaspekter skiljer sig mellan användare med IT-relaterad sysselsättning och användare med övrig sysselsättning.

4.1.1 Beteende på öppna WiFi-nätverk

Nedan presenteras resultatet på de allmänna frågorna som berör användningen av WiFi. I de svaren hittade vi inga skillnader mellan användare med IT-relaterad sysselsättning och

övriga, därför presenteras de tillsammans. Först presenteras data i tabellform och sedan i en grafisk presentation.

Var har du kopplat upp dig till ett öppet WiFi-nätverk under de senaste 12 månaderna? (flervalsalternativ)	
Svarsalternativ	**Antal svar**
Hotell	111
Café/restaurang	100
Flygplats	83
Skola	69
Bibliotek	39
Butik	24
Tåg/buss	19
Annat	9
Stadsnät	5
Centralstation	3
Totalt antal svar	**462**

Tabell 3

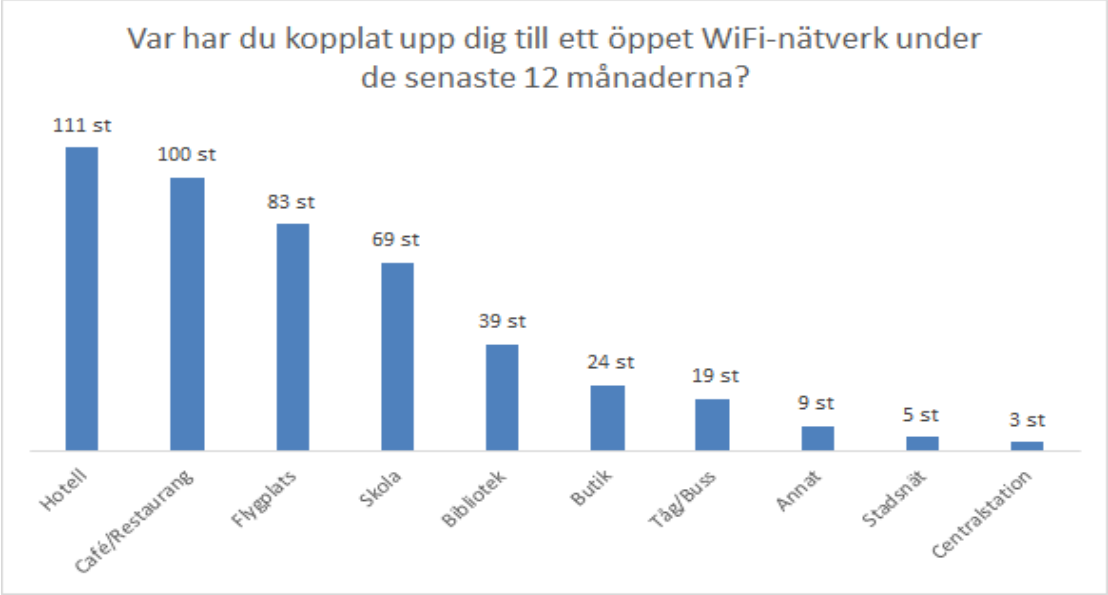

Bild 3. Överblick över var användare kopplar upp sig på öppna WiFi-nätverk

Oberoende av användarkategori visar undersökningen att öppna WiFi-nätverk framför allt används på hotell, caféer, restauranger och flygplatser. Flygplatser och hotell kan tillsammans med tåg och buss knytas samman med resor då användare behöver tillgång till internet på sina datorer. Över hälften av användarna föredrog att använda mobiltelefonen för att ansluta till nätverken, en tredjedel använde datorn och ett fåtal använde surfplatta.

Vilka av följande tjänster använder du på ett öppet nätverk? (flervalsalternativ)	
Svarsalternativ	**Antal svar**
Sociala medier	153
Nyhetssidor	123
Mail	123
Banktjänster	42
Sidor kopplade till arbetet	34
Spel	33
Online shopping	29
Annat	8
Totalt antal svar	**545**

Tabell 4

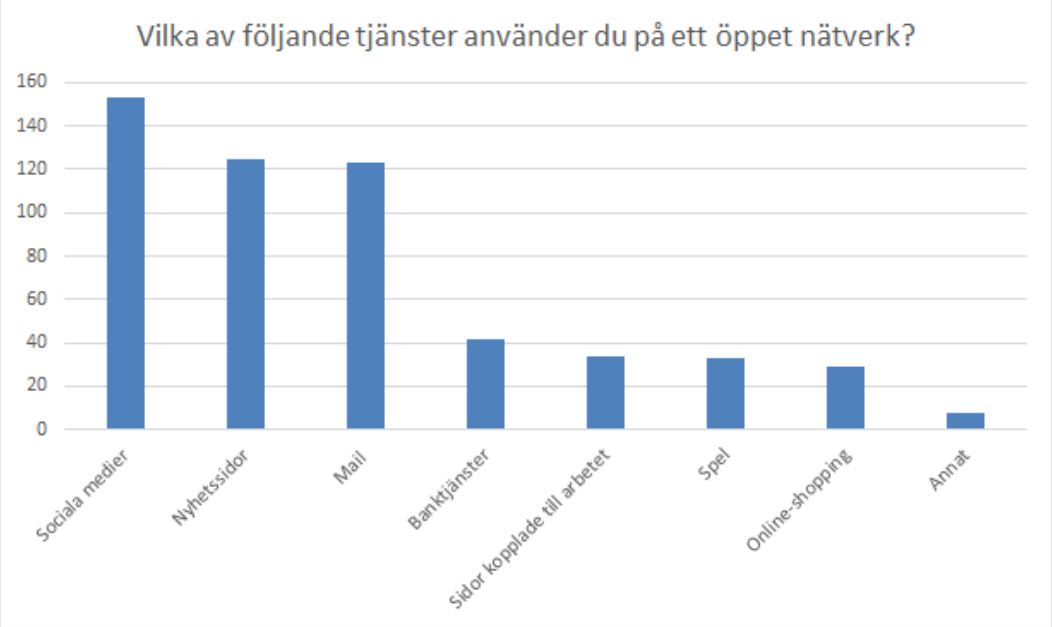

Bild 4. Överblick över de tjänster som används på öppna WiFi-nätverk

Vi fann att sociala medier, nyhetssidor och mail var det som användarna främst använde nätverken till. I kategorin ”annat” återfanns sidor med programmerings-API och varierande föreningssidor.

Stänger du av WiFi på din enhet efter användning?	
Svarsalternativ	**Antal svar**
Ja	62
Nej	99
Vet ej	12
Totalt antal svar	**173**

Om ja: Varför?	
Svarsalternativ	**Antal svar**
Spara batteri	32
Säkerhetsorsaker	14
Annat	9
Totalt antal svar	**55**

Tabell 5

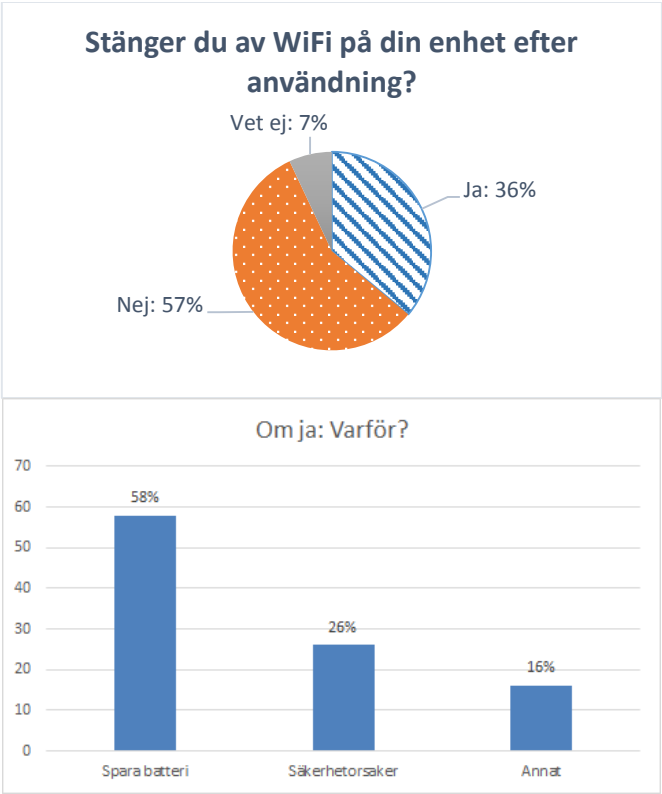

Bild 5

Över hälften av användarna svarade att de inte stängde av WiFi på sin enhet efter användning. De som stängde av WiFi gjorde det främst för att spara batteri. 26 % uppgav att de gjorde de av säkerhetsorsaker. Användare som inte stänger av WiFi på sin enhet riskerar bland annat att automatiskt kopplas upp mot en SSID de tidigare anslutit sig till, vilket kan utnyttjas en tidigare beskriven RAP-attack (se avsnitt 2.1.2.4).

4.1.2 Skillnad mellan IT-relaterade användare och övriga

Det övergripande resultatet visar en skillnad mellan IT-relaterade och övriga användare. Nedan presenteras de områden där användarkategorierna skiljde sig från varandra. Först presenteras data i tabellform och sedan i en grafisk presentation.

Hur känner du dig när du surfar på öppna WiFi-nätverk		
Svarsalternativ	**IT-relaterade, antal svar**	**Övriga, antal svar**
Inget av alternativen	2	2
Surfar inte på öppna WiFi-nätverk	3	7
Obekymrad	9	14
Relativt obekymrad	60	41
Orolig	11	12
Väldigt orolig	6	6
Totalt antal svar	**91**	**82**

Tabell 6

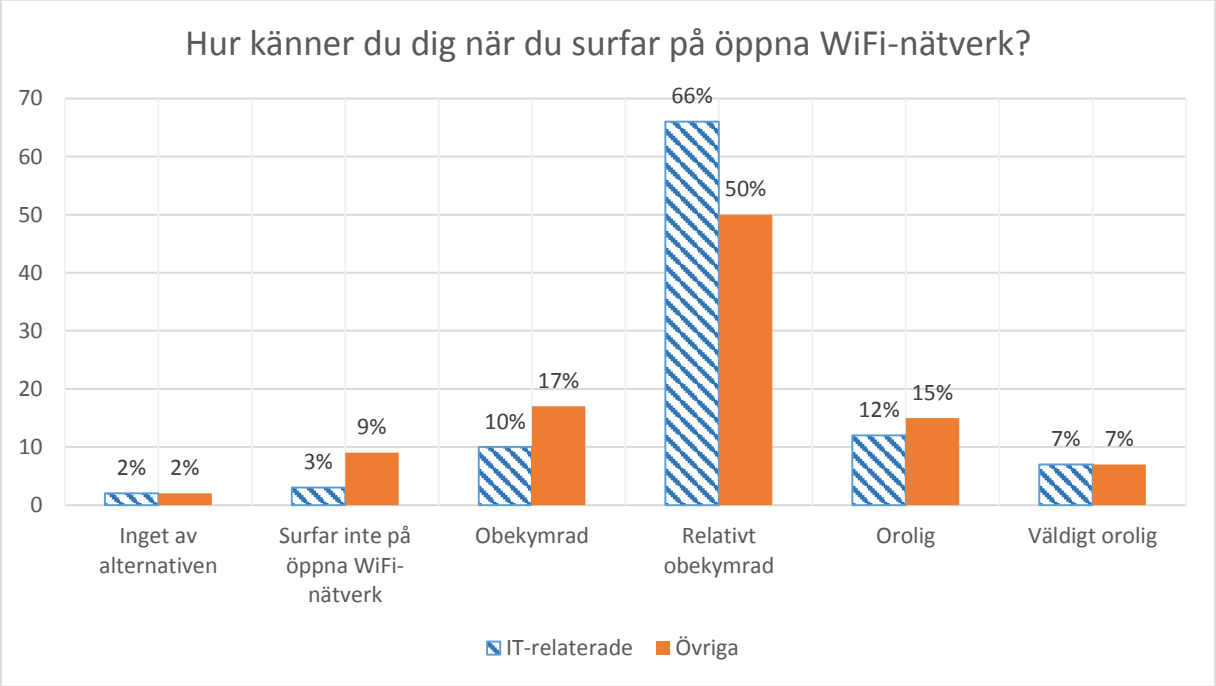

Bild 6. Överblick över hur användare känner sig då de surfar på öppna WiFi-nätverk

Användarkategorierna uppvisade en viss skillnad när det gäller hur de känner sig när de surfar på öppna WiFi-nätverk. Något fler av de övriga användarna surfade inte på nätverken, men när de gjorde det var 67 % obekymrade eller relativt obekymrade, jämfört med 76 % av de IT-relaterade användarna. Ungefär 20 % ur de bägge användarkategorierna vara oroliga eller väldigt oroliga, vilket dels kan bero på att de känner till riskerna men också på att de saknar kunskap om de åtgärder de kan vidta för att surfa säkrare.

Vilken eller vilka av följande tror du skyddar kommunikationen när du surfar på ett öppet WiFi-nätverk? (flervalsalternativ)		
Svarsalternativ	**IT-relaterade, antal svar**	**Övriga, antal svar**
Brandvägg	27	25
Antivirus	15	10
WPA/WPA2	27	6
WEP	11	4
HTTPS	35	20
Virtual Private Network (VPN)	38	16
Ingen av dem	22	25
Känner inte till någon av dem	1	21
Totalt antal svar	**176**	**127**

Tabell 7

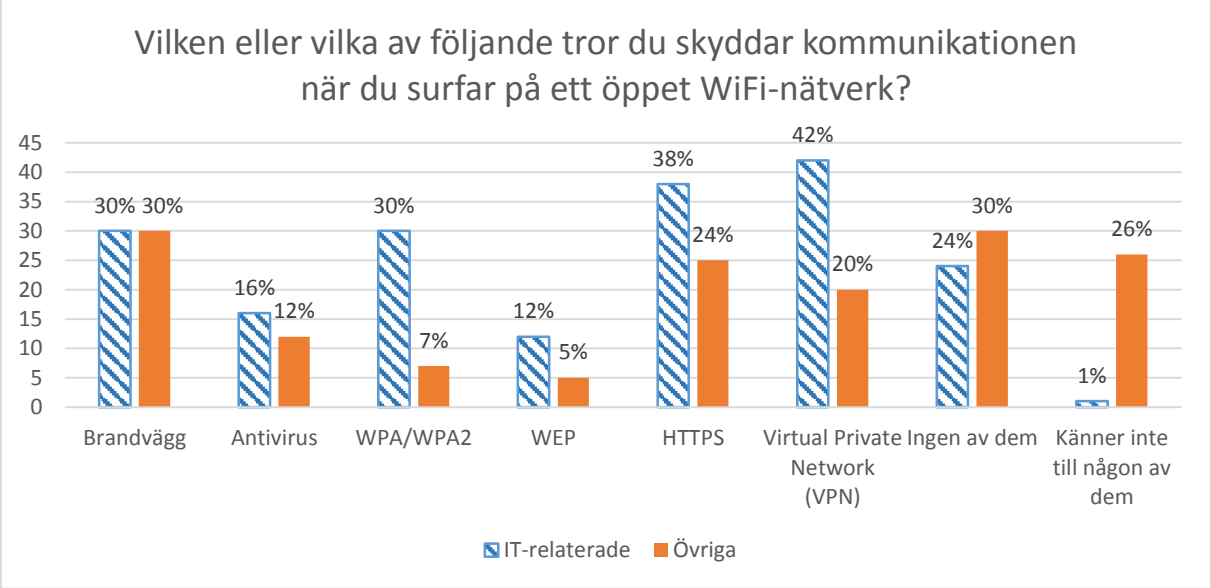

Bild 7. Överblick över vad användarna tror skyddar deras kommunikation på öppna WiFi-nätverk

Användarkategorierna skiljde sig avsevärt åt på frågan om vad de trodde skyddade deras kommunikation vid surfande på öppna WiFi-nätverk. De IT-relaterade användarna hade högre kännedom om tekniker som faktiskt skyddar kommunikationen, så som WPA/WPA2-kryptering, HTTPS och VPN. 30 % av de övriga användarna trodde inte att någon av ovanstående tekniker skyddade dem och 26 % kände de inte till dem över huvud taget.

Jag vet hur man skiljer ett öppet nätverk från ett krypterat nätverk		
Svarsalternativ	**IT-relaterade, antal svar**	**Övriga, antal svar**
Ja	67	47
Nej	24	35
Totalt antal svar	**91**	**82**

Tabell 8

"Jag vet hur man skiljer ett öppet nätverk från ett krypterat nätverk"

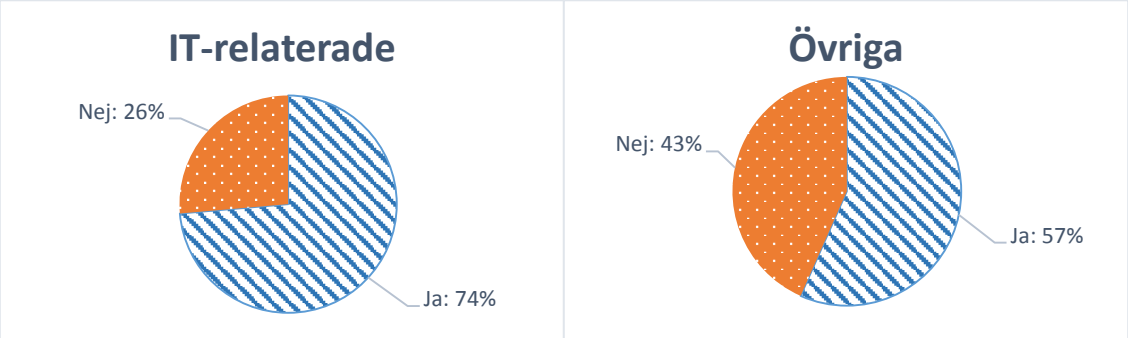

Bild 8

En fjärdedel av de IT-relaterade användarna menar att de inte kan skilja ett öppet nätverk från ett krypterat nätverk. Kännedom kring huruvida ett nätverk är krypterat eller inte är en av de grundläggande kunskaperna för att kunna motarbeta säkerhetsrisker. Bland de övriga användarna var siffran ännu högre, där 43 % uppgav att de inte vet vilken typ av nätverk de surfar på.

Jag anser att jag känner till riskerna jag utsätter mig för när jag använder öppna WiFi-nätverk		
Svarsalternativ	**IT-relaterade, antal svar**	**Övriga, antal svar**
Ja	72	31
Nej	19	51
Totalt antal svar	**91**	**82**

Tabell 9

"Jag anser att jag känner till riskerna jag utsätter mig för när jag använder öppna WiFi-nätverk"

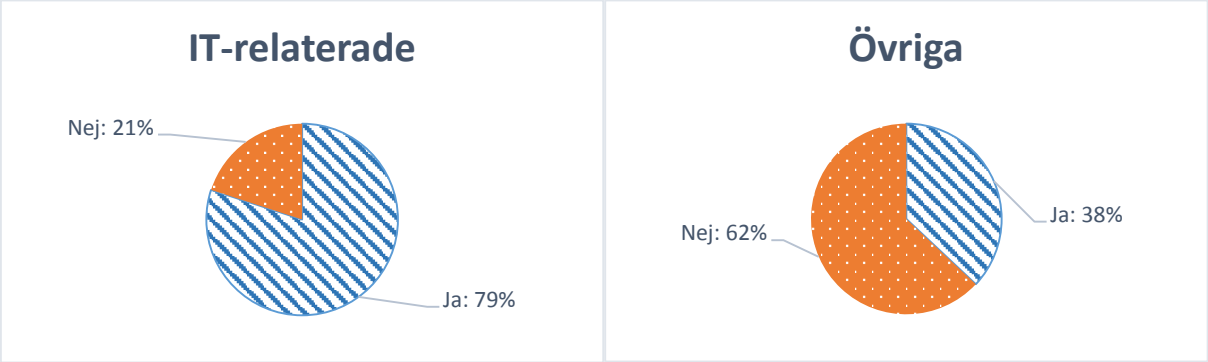

Bild 9

En femtedel av de IT-relaterade användarna anser att de inte känner till riskerna de utsätter sig för på öppna WiFi-nätverk, vilket är fler än de som vet hur de skiljer ett öppet nätverk från ett krypterat nätverk (se bild 8). Det väcker frågan om de IT-relaterade användarna faktiskt känner till riskerna eller om de har en felaktig bild av området. Bland de övriga användarna ansåg 62 % att de inte känner till riskerna.

Jag behöver vidta åtgärder för att kunna surfa säkert på ett öppet WiFi-nätverk		
Svarsalternativ	**IT-relaterade, antal svar**	**Övriga, antal svar**
Ja	71	38
Nej	3	6
Vet ej	17	38
Totalt antal svar	**91**	**82**

Tabell 10

"Jag behöver vidta åtgärder för att kunna surfa säkert på ett öppet WiFi-nätverk"

Bild 10

Återigen visar undersökningen att de IT-relaterade användarna har en större medvetenhet om de risker de utsätter sig för vid användande av nätverken och möjligen agerar utifrån den ökade kunskapen. Oberoende av användarkategori tror få användare att de inte behöver göra någonting för att surfa säkert. Istället är det okunskapen, framför allt hos de övriga användarna, som är en stor faktor.

Det är lagligt att manipulera trafiken på öppet WiFi-nätverk		
Svarsalternativ	**IT-relaterade, antal svar**	**Övriga, antal svar**
Ja	13	7
Nej	38	37
Vet ej	40	38
Totalt antal svar	**91**	**82**

Tabell 11

"Det är lagligt att manipulera trafiken på ett öppet WiFi-nätverk"

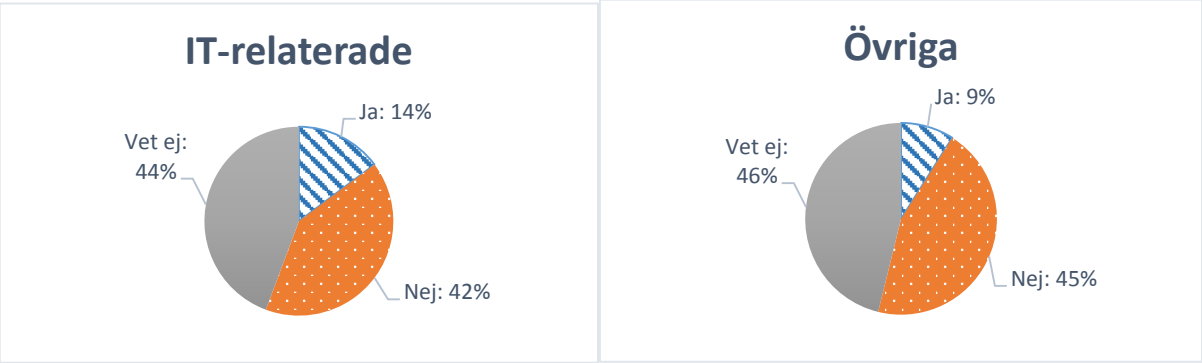

Bild 11

På frågan om det är lagligt att manipulera trafiken på ett öppet WiFi-nätverk är skillnaden mellan användarkategorierna inte stor, däremot visar undersökningen på ett överraskande resultat. Det är enda gången där de övriga användarna visar en större medvetenhet än de IT-relaterade, om än en obetydlig sådan. Bland de IT-relaterade användarna tror 14 % att det är lagligt att manipulera trafiken på nätverken, medan 9 % av de övriga tror likadant. På frågan om de tror att det är lagligt att analysera trafiken svarar användarkategorierna likadant, med 40 % som tror det, 16 % som inte tror det och 44 % som inte vet.

När jag surfar på öppna WiFi-nätverk utsätter jag mig för risken att få personuppgifter, lösenord och annan information kapad		
Svarsalternativ	**IT-relaterade, antal svar**	**Övriga, antal svar**
Ja	76	51
Nej	2	4
Vet ej	13	27
Totalt antal svar	**91**	**82**

Tabell 12

"När jag surfar på öppna WiFi-nätverk utsätter jag mig för risken att få personuppgifter, lösenord och annan information kapad"

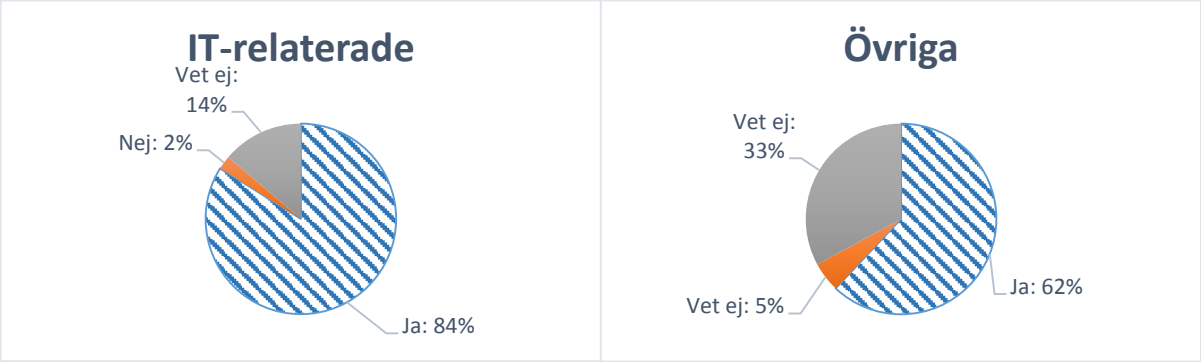

Bild 12

På frågan om användarna tror att de utsätter sig för risken att få känsliga uppgifter kapade följer de övriga användarna det övergripande mönstret där fler är osäkra jämfört med de IT-relaterade.

4.2 Intervju med Jakob Schlyter, rådgivare i nätverks- och IT-säkerhetsfrågor

Vi ville i vår intervju med Jakob Schlyter ge honom så mycket utrymme som möjligt att berätta om sin syn på säkerhet i öppna WiFi-nätverk. Vi hade förberett ett antal frågor som vi ville ha svar på, men lämnade öppet för diskussion. Då en stor del av intervjun även berörde vårt arbete i helhet har vi valt att nedan presentera ett antal citat vi anser väsentliga för vår undersökning. Jakob använder återkommande två kända nätverk som exempel, Eduroam och Homerun. Nätverken återkommer i intervjun bl.a. för att de är båda är välkända och för att Eduroam är WPA2-krypterat medan Homerun är ett öppet WiFi-nätverk.

"Generellt sätt kan man om WiFi-hotspots säga att det ser ju inte så himla bra ut. Det ser ganska dåligt ut. Sen skiljer det ganska mycket beroende på vad det är man ska skydda för någonting. Det kan man fundera på. Dels finns det helt öppna nät, som är bra när man inte har någon relation, dels finns ju öppna som i att de är okrypterade och sen finns det öppna som är allmänt tillgängliga om man känner till något lösenord, men dom är ändå krypterade och vem som helst kan få lösenordet. Sen finns det de som har lite bättre säkerhet. Från början fanns det vanliga WiFi och det är väldigt enkelt, dess styrka är att vem som helst kan sätta upp det och problemet är också att vem som helst kan sätta upp det. Det är icke-regulerat frekvensutrymme vilket är väldigt bra, men det är också väldigt dåligt ur andra synvinklar."

Citatet sammanfattar mycket av de slutsatser vi dragit från teoristudier; säkerhet i öppna WiFi-nätverk är ett komplext område utan någon universallösning. Det finns oerhört många aspekter att ta i beaktande, likt det Jakob poängterar att man måste fråga sig vad det är som skall skyddas.

"Risk är ju alltid kopplat till vad det är för sannolikhet att det inträffar. Vad är det för skada som kan ske om det inträffar? Det går att multiplicera ganska enkelt. Vad sitter folk och gör? Sitter och läser mail och loggar in på banken. Dels finns ju attackerna som är allmänna, när någon till exempel sätter sig och snor lite lösenord. Sen finns det ju riktade attacker och där finns det ju ett större problem. Ibland är man intressant och ibland är man ointressant. Om man till exempel sätter sig på en flygplats där mycket folk passerar, som affärsfolk och liknande, så kan man pyssla med industrispionage. Det är tacksamt att göra och det är

relativt enkelt att göra rätt. Om bara folk bara slutade trycka fortsätt på alla certifikatfrågor och körde mer krypterat så skulle det bli väldigt mycket bättre."

Jakob beskriver här två typer av attacker, de allmänna och de riktade. Stöld av lösenord i syfte att kapa någons identitet kan ses som en allmän attack, medan riktade attacker istället sker mot specifika individer, till exempel medarbetare med tillgång till ett företags intranät:

"Om du skulle sätta dig på Landvetter kan du MITM:a (MITM-attack, se avsnitt 2.1.2.1, författarnas anmärkning) *Homerun lite, antingen låna trafiken eller bara sitta och lyssna. Om jag snor trafiken där och så tar jag all trafik mellan Active Sync, som är vanligt för att prata med en Exchange-server på firman, så får jag någons lösenord baserat på det. Då får jag deras AD-lösenord in i firman och kommer åt hela deras kalender och kontakter och annan info. Det kan ju vara praktiskt. Har man då tänkt efter så har man ju konfigurerat företagstelefonerna, men det är inte så många som gör det."*

Om en angripare utför en MITM-attack på en användare som kommunicerar med sitt företags Exchange-server kan de få tillgång till flertalet känsliga uppgifter. Vår enkätundersökning visade att flygplatser och hotell hör till de vanligaste platserna där användare loggar in på öppna WiFi-nätverk, vilket är förståeligt eftersom de finns tillgängliga när användarna är ute och reser. Vår enkätundersökning visade även att det fanns en högre grad av medvetenhet bland användare med IT-relaterad sysselsättning, men att kommunicera med företagets server är idag inget exklusivt för den användarkategorin. De IT-relaterade användarnas ökade medvenhet behöver nödvändigtvis inte heller betyda att de agerar på ett sätt anpassat för situationen.

Även om nätverk som Eduroam och Homerun finns tillgängliga på ett stort antal platser är det inte alla som har tillgång till dem. Fristående aktörer väljer också att sätta upp öppna WiFi-nätverk för att erbjuda sina kunder internet.

"De flesta som sätter upp Hotspots har ju inget lösenord eftersom de vill att det ska vara lätt för folk att ansluta. Så då kör dom ett öppet nät och det kanske är helt okej, men då får man tänka på att man sitter på ett nät där det kan sitta andra på ett sätt som inte är lika vanligt när man sitter hemma. Så därför är det stor skillnad. Jämför man med till exempel Eduroam finns det andra risker, men det handlar ju om att autencieringen ska lyckas. Misslyckas man med den så är man ganska rökt. När det kommer upp en säkerhetsfråga så trycker användare oftast bara vidare, till exempel på frågan om de vill fortsätta ansluta. Alla klickar ja, precis som i certifikatvarningar i allmänhet. I Eduroam innebär det att du precis blev av med ditt lösenord."

Anledningen att de flesta WiFi-nätverk inte har något lösenord är, som Jakob beskriver, att det ska vara lättillgängligt. Jakob belyser även samma problematik som tagits upp i teoriavsnittet angående phising-sidor (se avsnitt 2.2.2), den att användare har en tendens att automatiskt klicka sig vidare trots säkerhetsvarningar. På Microsofts hemsida finns en FAQ om certifikatvarningar, där den sammanfattade rekommendationen är att aldrig ignorera dem (Microsoft, 2014). En certifikatvarning ser likartad ut oberoende av webbläsare (se bild 13) och klassas som en aktiv varning (se bild 2), vilket tyder på att inte ens aktiva varningar nödvändigtvis får användare att reagera och vidta korrekta åtgärder.

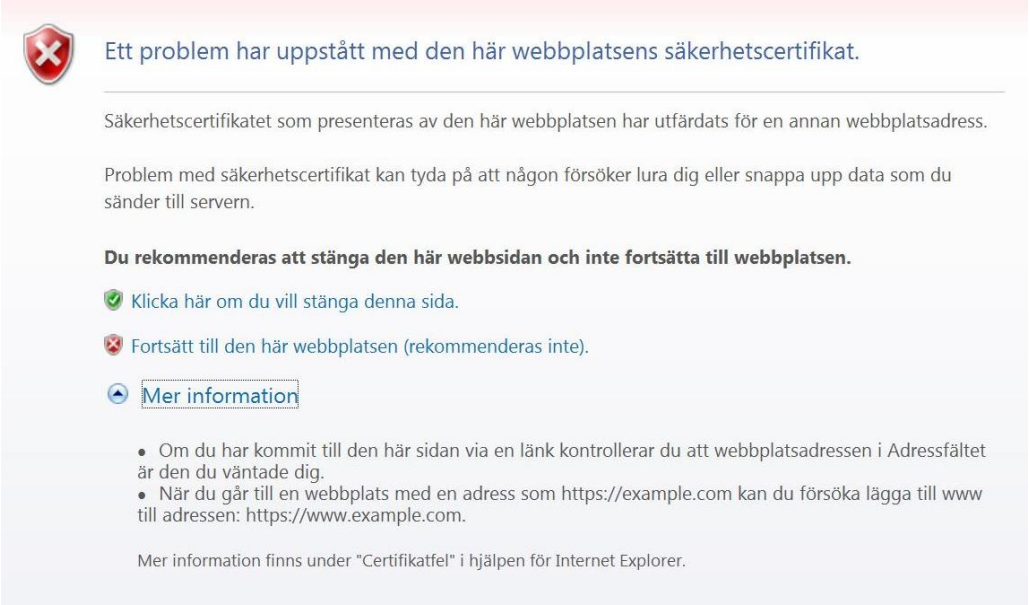

Bild 13. Certifikatvarning i Internet Explorer

Jakob beskriver vidare hur certifikatvarningar kan uppstå i öppna WiFi-nätverk:

"En typisk grej på trådlösa nät är om man till exempel ansluter till Homerun och ska ansluta till Facebook. Då startar du din webbläsare och trycker att du ska gå till Facebook. Då tror din webbläsare att du pratar med Facebook, men du har styrts om till Telias inloggningsportal som också kör HTTPS men som har snott trafiken. Då får du en certifikatvarning för din webbläsare tror Facebook, men du har kommit till Telia, som inte gör någon attack på dig utan de vill bara få pengar av dig så du kan logga in. Det gör att du trycker fortsätt automatiskt och då trubbar man av användarna så att de gör detta även när det verkligen gäller."

Likt Egelman, Cranor och Hong (2008) menar Jakob att användarna trubbas av och därmed kommer godkänna varningarna även vid kritiska situationer. Han påpekar också att det är en dålig lösning, eftersom allt för stort ansvar läggs på användaren som oftast inte har kunskap nog att fatta ett sådant beslut:

"Rätt lösning om man hade gjort det där nu hade varit att "Du försöker prata krypterat med Facebook. Vi vet inte att du pratar med Facebook, så du får inte fortsätta". Det är det rimliga sättet för användaren kan faktiskt inte ta det valet. Där är en jättestor skillnad mot till exempel Eduroam där du inte ens kan logga på utan att det blir krypterat."

Om alla WiFi-nätverk hade varit krypterade, hade problemet existerat då? Svaret på frågan kanske är irrelevant, eftersom kostnaden för en sådan lösning hade varit att tillgängligheten försämras, men precis som Schneier (2008) beskriver är säkerhet en kompromiss. Jakob menar dock att det är klart bättre med ett krypterat nätverk, även om lösenordet är allmänt tillgängligt:

"Det är mycket bättre att ha ett lösenord som alla känner till än att inte ha något alls."

Vidare berättar han dock att kryptering inte är en garanti för att trafiken är helt säker:

"Om fiket här skulle sätta upp Eduroam så skulle trafiken vara krypterad genom luften fram till deras router här i kaffestugan. Där slutar det vara krypterat och där skulle de mycket väl kunna attackera dig. Så det finns ingen garanti att bara för att det är ett säkert trådlöst nät så är det avlyssningsfritt."

Det krävs därmed att användarna är medvetna om de risker de utsätter sig för eftersom teknologin i sig inte är tillräcklig för att säkerställa kommunikationen. Jakob ger dock ett exempel på ny teknologi som är ett steg i rätt riktning:

"Telia har börjat rulla ut sitt andra nätverk, Homerun1x, där de kör SIM-kortsautenciering. Kör ni Telia i era telefoner och ser Homerun1x på stan och väljer det så kommer du bara loggas in. Då har den gjort en nyckelförhandling i 1x med en hemlis som finns i SIM-kortet, och det är ju rätt lösning. Du har inte behövt göra någonting. Och det blev säkert. Du vet att du pratar med Telia och Telia vet att de pratar med din telefon. Det är ju väldigt svårt att göra rätt säkerhet, sen kan man i många fall tycka att det är schysst med ett öppet nät som här, det använder jag ju när jag sitter och jobbar. Men jag skulle ju helst sätta något VPN hem till en lite, lite säkrare utgångspunkt."

Att skydda sin kommunikation är något som de flesta anser viktigt, men det finns även andra aspekter som är viktiga att beakta. Genom att ha WiFi påslaget på sin telefon kan den som har tillgång till Eduroam eller andra större nätverk spåra var en användare befinner sig och var de tidigare varit genom att analysera inloggningar. Jakob berättar om en person som verkligen tar problemet på allvar:

"Han (en kollega, författarnas anmärkning) *använder inte telefon för att han inte vill ha en spårenhet på sig och det ligger ganska mycket i det. Så fort din telefon går runt så ligger den och lyssnar efter trådlösa nät"*

"De som har nätet kommer ha ditt fulla spår var du har varit. Det går att konfigurera så att det inte syns genom olika konfigurationsprofiler till telefonerna, men det gör inte folk själva. Vanliga människor gör inte detta."

Ett intressant fall läckte nyligen ut på Wikileaks, där den kanadensiska underrättelsetjänsten spårade resenärer med hjälp av WiFi-hotspots (CBC, 2014):

"När du kommer till gränsen för passkontrollen så kan det finnas en antenn som sparar MAC-adresser och kopplar dem till personer i passkontrollen. När resenären fortsätter in i landet så kan man avlyssna lite trådlösa nät och se var personen befinner sig utifrån deras MAC-adress. De gjorde verkligen den här attacken, från nationens sida. De är det lite svårare att skydda sig mot. Man kan diskutera om man ska bli upprörd över detta, men luften är fri. De har bara suttit och lyssnat."

Det här var ett av fallen som läckt ut och vi kan bara spekulera i hur många liknande fall det finns i andra länder. Vad som gör fallet extra intressant är att underrättelsetjänsten knappt behövt göra något för att samla in informationen. Som Jakob säger, de har bara suttit och lyssnat. På frågan vad Jakob anser vara den största risken för användare vid interaktion med öppna WiFi-nätverk svarade han:

"Hotspots med captive portals (så som Homerun, författarnas anmärkning) *är det som är det farligaste. Det är mycket farligare än öppna nätverk utan inlogg. Man loggar in, man blir omstyrd och man tvingas till certifikatfrågorna. Annars vet man att det är ett helt öppet nät och man får gilla läget."*

Ett stort problem med att ”gilla läget” på helt öppna nätverk är dock att användarna enligt vår enkätundersökning ofta inte vet hur de skiljer ett öppet nätverk från ett krypterat eller vilka risker de utsätter sig för.

4.3 Observation

Nedan presenteras resultaten från våra två observationer och vårt praktikfall.

4.3.1 “Sniffing”

Syftet med första delen av observationen var att undersöka vad användare besöker för webbplatser på öppna WiFi-nätverk. Övervakningen utfördes på en allmän plats med hjälp av programmet Wireshark. Mängden data som skickades över nätverken var överväldigande, men genom enkla sökfunktioner och filter kunde vi avgränsa datat för att få fram den information vi sökte. Det visade sig att det var väldigt enkelt att se besökta webbsidor i klartext, vilket i sig inte utgör någon omfattande säkerhetsrisk, men det är värt att notera att på öppna WiFi-nätverk kan vem som helst lagligen se vad man besöker för sidor.

Nätverkstrafiken vi övervakade visade att resultaten från vår enkätundersökning (se bild 4) överensstämde med verkligheten eftersom sociala medier och nyhetssidor var de mest besökta sidorna. I den övriga trafiken återfanns bland annat sidor kopplade till restauranger, bloggar, Skatteverket samt en del holländska sidor. Variationen på sidorna sträcker sig från rena informationssidor som inte kräver någon inmatning av information till sidor där känslig information matas in. Vissa av sidorna var SSL-krypterade (t.ex. Skatteverket) medan vissa helt saknade kryptering. Information som matas in på sidor utan kryptering kan bland annat utläsas genom att söka efter händelser med prefixet POST. De gånger vi fann sådana händelser valde vi att inte öppna dem då de kunde innehålla känslig information som vi inte ville utnyttja.

4.3.2 Rogue Access Point

Vi hade inga mål eller förhoppningar angående hur många som faktiskt skulle ansluta sig till vårt nätverk och resultatet var överraskande. Vårt nätverk gav full signalstyrka upp till 10 meter från vår position och det var ständigt omkring 50 personer inom radien för nätverket. Under de åtta timmar observationen utfördes anslöt sig 23 enheter till nätverket och som mest var tre användare anslutna samtidigt (vid användandet av SSID ”Free WiFi”). Nedan visas hur många som kopplade upp sig på olika SSID under en specifik tidsperiod.

Tidpunkt	***SSID***	***Totalt antal anslutningar***	***Anslutningar från dator***	***Anslutningar från mobiltelefon***
14:00-16:00	Centralen WiFi	8	4	4
16:00-18:00	Free WiFi	9	7	2
18:00-20:00	WiFi	6	2	4

Tabell 13

Vi fann inga belägg för vår hypotes att användare väljer att ansluta sig till nätverk med ett SSID kopplade till platsen de befinner sig medan de undviker allmänna SSID. Användarna anslöt sig frekvent till nätverket oberoende av SSID och valde även våra allmänna SSID framför mer platsspecifika SSID (till exempel “SJ” eller “espressohouse”). Vad vi kan bekräfta är att många användare oaktsamt ansluter sig till öppna WiFi-nätverk och därmed utsätter sig för risken att en angripare manipulerar deras data.

Vid några tillfällen tror vi att vi lyckades identifiera några av personerna som använde nätverket genom att jämföra de enheter som användes inom radien för vårt nätverk med nätverkstrafiken. Dock finns möjligheten att de använde sig av samma enheter som andra personer på nätverket, men då vi visuellt kunde se majoriteten av alla personer som var inom nätverkets radie är det mindre troligt.

4.3.3 Praktikfall

Vi anser det vara av vikt att visa hur enkelt det är att få tillgång till information genom att avlyssna trafiken på öppna WiFi-nätverk. Det resultat som presenteras i praktikfallet liknar den information vi kunde ta del av under vår observation. Nedan visas hur det går att utläsa besökta webbsidor, både i realtid och vid en senare analys av insamlad data.

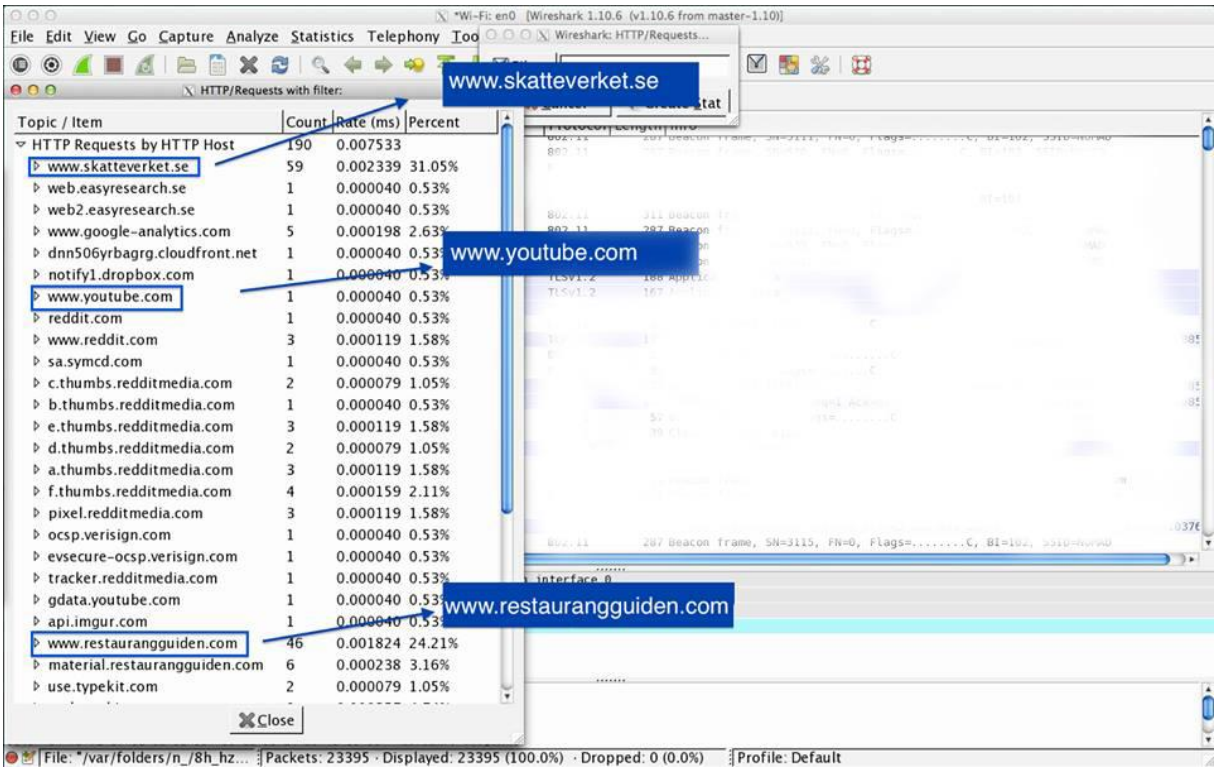

Bild 14. Data från programmet Wireshark från vårt praktikfall med exempel på hur enkelt det går att utläsa besökta webbsidor.

Vårt främsta resultat från praktikfallet var dock att det är väldigt enkelt för en angripare att få fram användarnamn och lösenord ifyllda på en sida som saknar SSL-kryptering. Majoriteten av alla större sidor använder idag SSL-kryptering. Det enklaste sättet att avgöra om en sida använder sig av SSL-kryptering är att titta efter den gröna "lås-symbolen" till vänster om adressen, samt kontrollera att sidan har prefixet https (se bild 15).

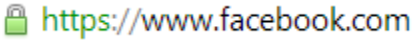

Bild 15. SSL-krypterad sida

Flertalet sidor är dock endast delvis SSL-krypterade. Viaplay visar på sin hemsida inga tecken på att använda sig av kryptering, men när html-koden för sidan undersöks noggrant visar det sig att inloggningsfunktionen anropar en SSL-krypterad sida (Viaplay, 2014).

Under vårt praktikfall sökte vi efter sidor som saknade SSL-kryptering och hittade flera stycken där användarnamn och lösenord skickas okrypterat i nätverket. Ett flertal bloggar, familjeliv.se och idgshop.idg.se (webbshop för att bland annat beställa Computer Sweden) var några av de sidor där vi lyckades få fram användarnamn och lösenord ur den insamlade nätverkstrafiken. Vi hittade sidorna genom att slumpvis leta oss fram bland mindre sidor med inloggningsfunktioner och vi hade inga svårigheter att hitta kandidater att undersöka.

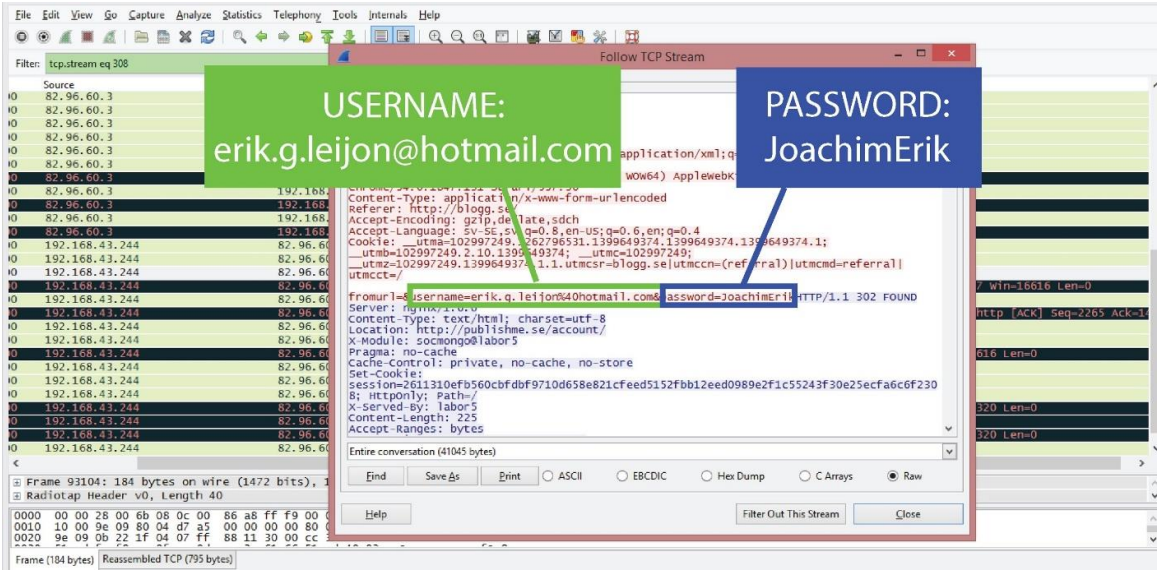

Bild 16. Användarnamn och lösenord för www.blogg.se

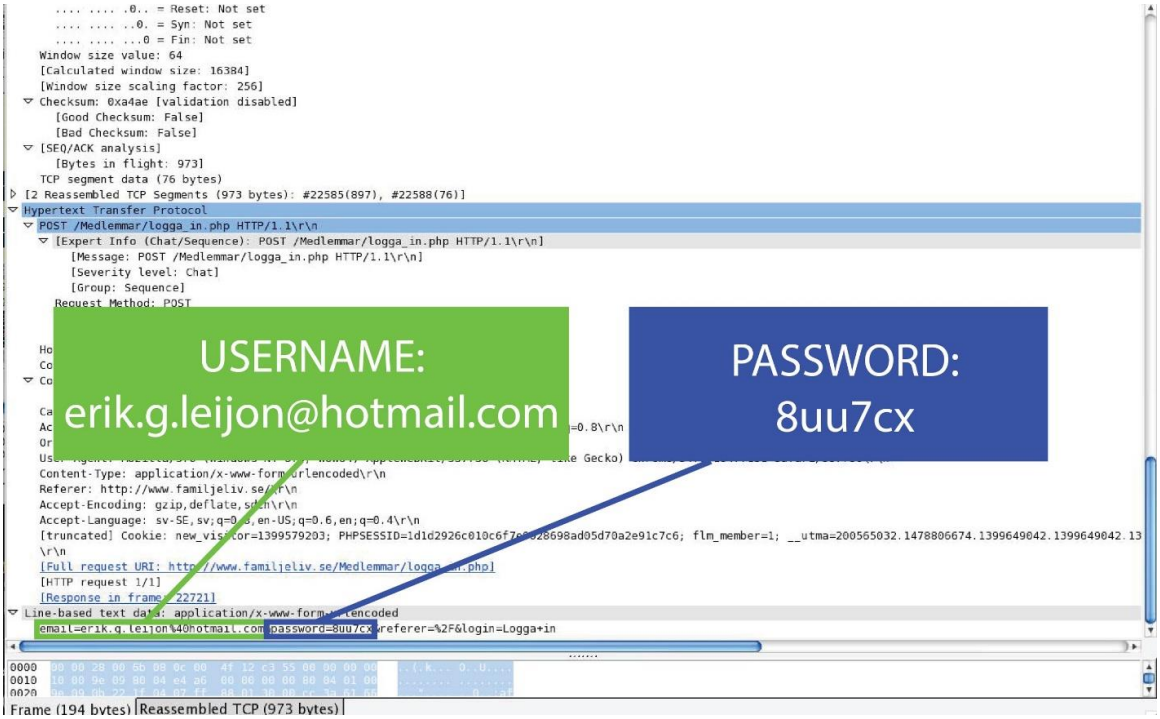

Bild 17. Användarnamn och lösenord för www.familjeliv.se

En angripare med tillgång till en användares användarnamn och lösenord kan orsaka olika typer av skada beroende på vilken typ av sida uppgifterna är kopplade till. Förutom att orsaka direkt skada på sidan i fråga finns även risken att användaren har samma inloggningsuppgifter på andra sidor. Värt att notera är att vi utförde laborationen utan tidigare kunskaper inom ämnet och vi anser oss själva vara amatörer. Vi använde oss av relativt enkla program och tekniker lärt oss genom att studera forum och guider på internet.

För att undersöka om användarna vid anslutning till öppna WiFi-nätverk i dagsläget får någon information presenterad för sig granskade vi under praktikfallet även de vanligaste förekommande operativsystemen på marknaden. Det finns i Apples produkter väldigt lite information om att det är ett öppet nätverk användaren försöker ansluta sig till. I iOS 7.1.1 (vid uppsatsens författande den senaste versionen för iPhone) visas ett krypterat nätverk

med ett litet hänglås medan ett öppet nätverk inte förklaras alls. Trycker användaren på informationsknappen bredvid det öppna nätverket presenteras teknisk information som innan anslutning är blank.

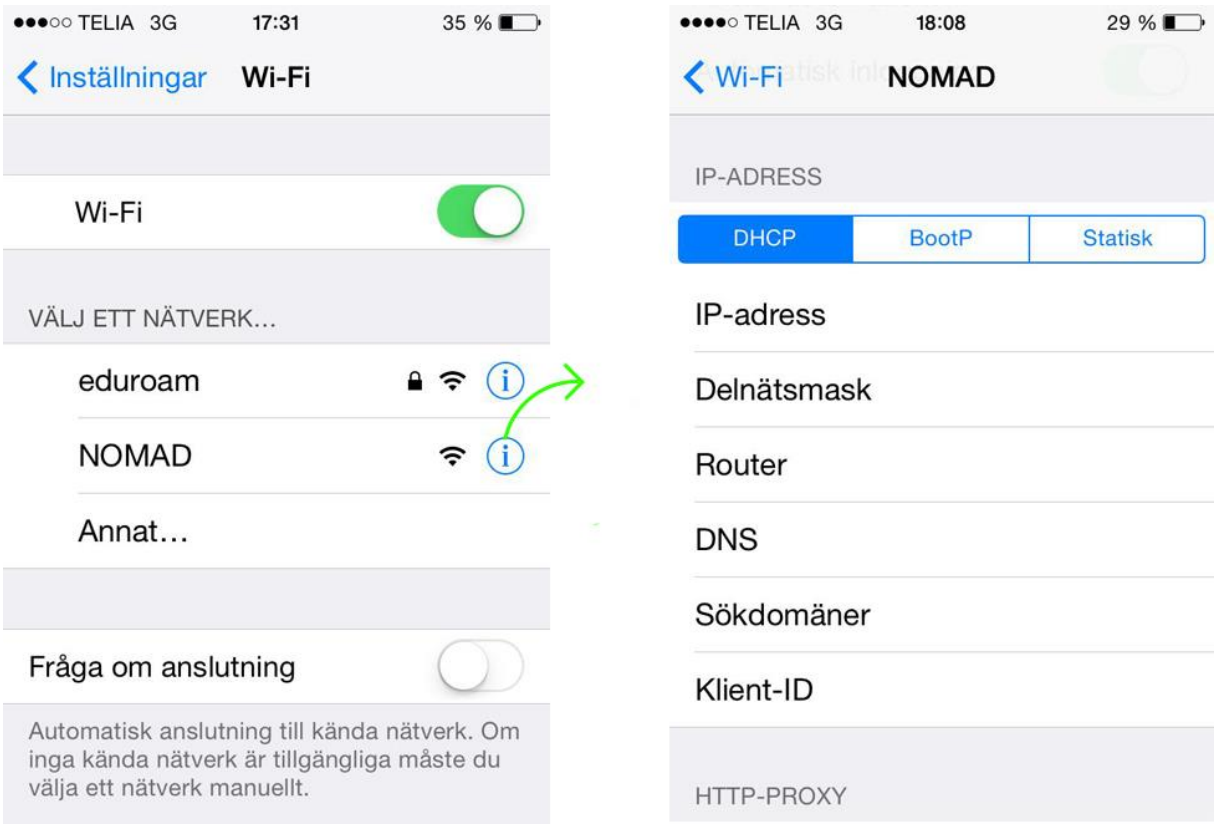

Bild 18. T.v. Lista över öppna WiFi-nätverk i iOS 7.1.1. T.h. Information om nätverket (innan anslutning)

På en Macbook Air med OS X 10.9.2 visade det sig vara ännu svårare att hitta information angående nätverket. Under Network Preferences - Advanced fanns en lista med tillgängliga nätverk. Under fliken säkerhet visades att ett öppet WiFi-nätverk inte hade någon säkerhet, utan att ge någon ingående förklaring till varför.

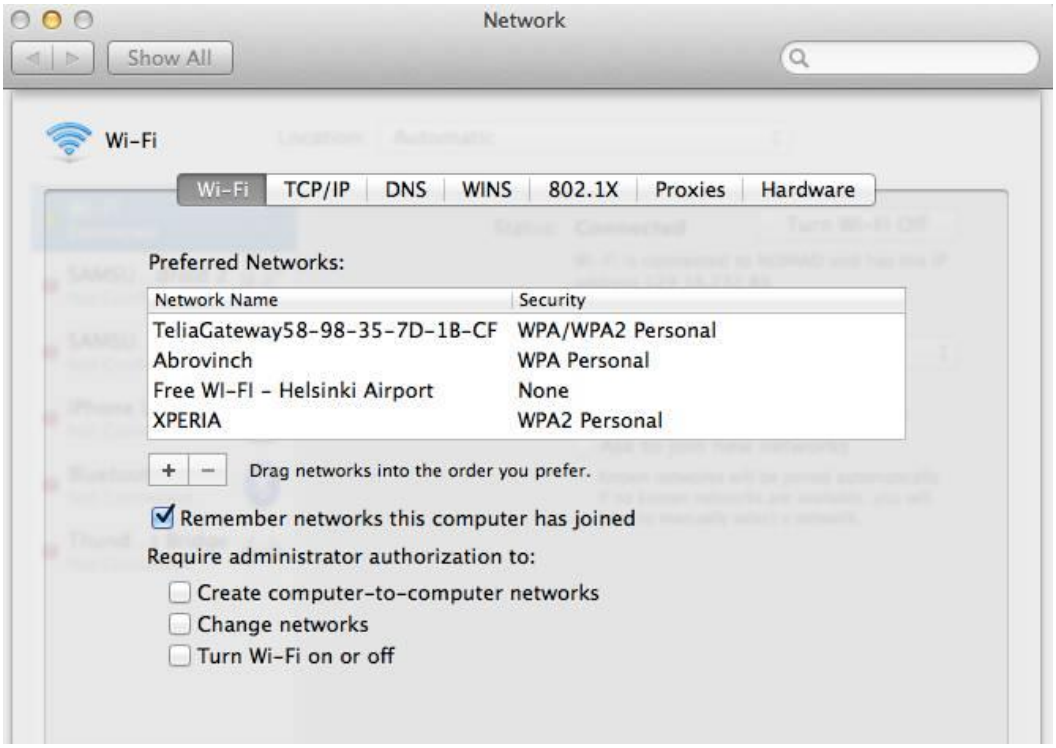

Bild 19. Lista över nätverk i OS X 10.9.2

I Android 4.4.2 framgår det tydligt av listan över tillgängliga nätverk vilka som är öppna och vilka som har någon form av säkerhet. Öppna nätverk beskrivs som “Öppen” medan krypterade nätverk beskrivs som “Skyddad”, något som i viss mån tydliggör deras säkerhetsnivå. Trycker användaren på nätverket får denne ytterligare information där det tydligt framgår att det inte är ett säkert nätverk. Skyddade nätverk har, liksom fallet med iOS, även en lås-symbol för att tydliggöra att nätverket är säkert. Symbolen återkommer i olika plattformar och webbläsare som en generell symbol för att anslutningen på något sätt är krypterad. Informationen är i större utsträckning tillgänglig på Android än på något av Apples operativsystem, men kräver ändå att användaren har en förståelse för vad ett öppet och ett skyddat nätverk är.

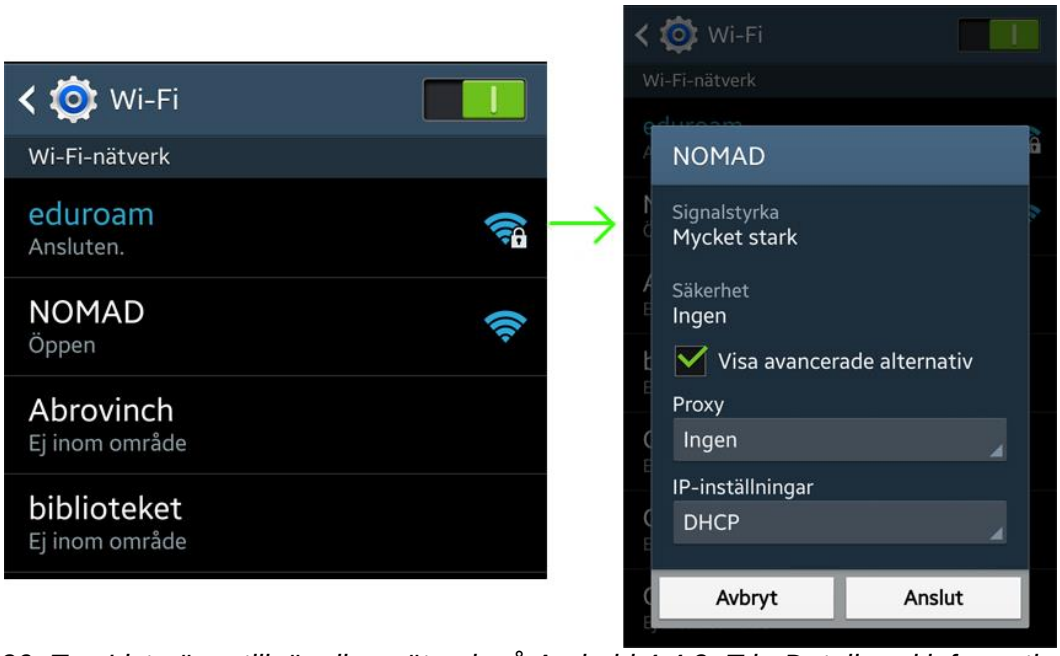

Bild 20. T.v. Lista över tillgängliga nätverk på Android 4.4.2. T.h. Detaljerad information om ett nätverk

De operativsystem som tydligast visualiserar potentiella risker i samband med öppna WiFi-nätverk är Windows 7 och Windows 8. I operativsystemen presenteras öppna nätverk vid anslutande med varningstexten “Andra personer kan eventuellt se informationen du skickar via nätverket” (i Windows 8) respektive “Information som skickas över detta nätverk kan vara synlig för andra” (i Windows 7). Det är en klart tydligare varning jämfört med Android och en stor förbättring jämfört med Apple, vars varningar knappt existerar. I Windows är symboliken även omvänd; ett säkert nätverk presenteras helt utan symboler medan ett öppet nätverk visas med en orange varningsikon.

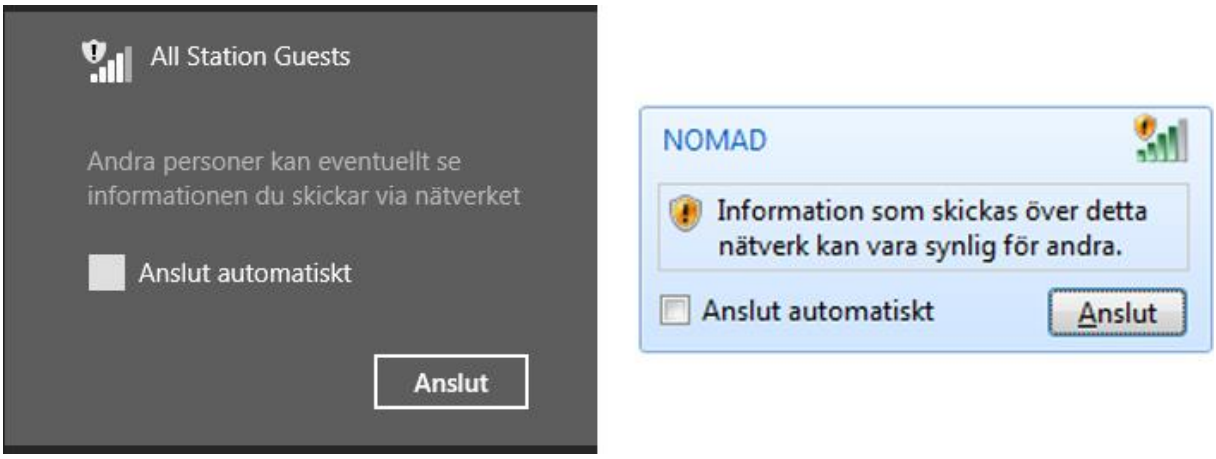

Bild 21. T.v. Varningsmeddelande i Windows 8. T.h. Varningsmeddelande i Windows 7

5. Analys/Diskussion

För att kunna presentera en så sanningsenlig bild som möjligt av problemområdet krävdes omfattande kunskap i såväl tekniska som psykologiska aspekter. Säkerhet i öppna WiFi-nätverk är ett komplext område där ett flertal faktorer spelar in. I ett samhälle där datorer, surfplattor och smartphones dagligen används till arbete, studier och sociala interaktion är tillgång till internet en viktig faktor. Öppna WiFi-nätverk ger en stor frihet, men det är en frihet under ansvar. De riskfaktorer som presenterades i teoriavsnittet utgör ett urval av de attacker användare riskerar att råka ut för vid interaktion med nätverken. Attackerna är inte enbart knutna till öppna nätverk, men bristen på säkerhet i dem gör att risken att drabbas av någon attack är större där än i ett krypterade nätverk.

5.1 WiFi-teknologin och säkerhetsrisker

Det finns ett antal risker kopplade till öppna WiFi-nätverk. Schlyter ansåg att den allvarligaste risken var så kallade “captive portals”, vilket innebär nätverk som till exempel Eduroam eller Homerun, som skickar vidare användaren till en inloggningsportal. Det kan leda till certifikatvarningar då webbläsaren tror att SSL-krypteringen är felaktig. Upprepade varningar gör att användarnas respekt för varningarna trubbas av, vilket troligen leder till att de godkänner varningen även i ett kritiskt läge (Egelman, Cranor & Hong, 2008). Användare i undersökningen av Egelman, Cranor och Hong (2008) godkände en liknande varning av den enkla anledningen att varningen dök upp regelbundet. Ett sätt att undvika certifikatvarningar är enligt Schlyter att trigga inloggningsportalen genom att besöka en harmlös sida utan SSL-kryptering. Andra stora hot mot enskilda individer är enligt vår undersökning Rogue Access Points (se avsnitt 2.1.2.4) och MITM-attacker (se avsnitt 2.1.2.1), något som över 200 säkerhetsexperter enligt Lawson (2013) även instämmer i. Det som gör RAP- och MITM-attacker extra besvärliga är att det nästan är omöjligt för en vanlig användare att avgöra om de blivit utsatta för en attack (Johnston, 2014).

VPN och SSL (se asnitt 2.1.3.3) är några av teknikerna som finns för att säkra kommunikationen över öppna WiFi-nätverk (Pervaiz, Cardei & Wu, 2007). Det finns idag VPN-tjänster som kan köpas av privatpersoner, men problemet är att användarna inte förstår nyttan av att använda VPN. För att användarna ska välja att utnyttja den utökade säkerhet VPN kan ge krävs det även att de är medvetna om riskerna, vilket både vår undersökning och tidigare forskning visar att de inte är. Således måste första steget vara att öka medvetenheten hos användare för att sedan presentera VPN och SSL som möjligheter att säkra kommunikationen.

Så om en användare enbart surfar på SSL-krypterade sidor eller använder sig av VPN, kan de då surfa säkert på öppna WiFi-nätverk? Tyvärr är det inte så enkelt. I april 2014 upptäcktes en bugg i den populära Open source-varianten av SSL, OpenSSL. Buggen fick namnet Heartbleed och visade sig vara en stor säkerhetsrisk. Sårbarheten gjorde att sidor som under normala förhållanden skyddas av SSL-kryptering, så som mail- och webbtjänster, nu kunde övervakas som om de helt saknade kryptering. Buggen gjorde det möjligt för angripare att avlyssna kommunikation samt stjäla data direkt från de tjänster som var utsatta, vilket uppskattas ha varit upp till en halv miljon (Heartbleed, 2014). Buggen har i sig ingen koppling till öppna WiFi-nätverk, men är ett exempel på hur saker och ting kan anses vara säkra trots att de inte är det. Det visar även att användares sociala beteende bör förändras så de ställer sig kritiska till tekniken och reflekterar över informationen de öppet delar med sig av.

5.2 Har användare med IT-relaterad sysselsättning högre medvetenhet om säkerhetsrisker vid interaktion med öppna WiFi-nätverk än andra?

Svaranden med IT-relaterad sysselsättning hade större kännedom om de tekniker som används för att säkra kommunikation i öppna WiFi-nätverk (se bild 7). 79 % av de IT-relaterade användarna ansåg sig även känna till riskerna de utsätter sig för på nätverken, jämfört med 38 % av de övriga användarna (se bild 9), näst intill identiskt med det resultat Attipoe (2013) fick på frågan om användarna kände till några säkerhetsrisker på öppna WiFi-nätverk (63 % kände inte till några). 84 % av de IT-relaterade trodde att de utsatte sig för risken att få känslig information kapad, jämfört med 62 % av de övriga (se bild 12). Det kan bero på hur frågan var vinklad på ett sätt som gjorde det lätt att svara ja, eftersom 38 % av de övriga inte ansåg sig känna till riskerna de utsatte sig för men 62 % av dem trodde att de utsatte sig för risken att bli av med känslig information. Hade frågan inte varit så specifik hade svaret kanske varit annorlunda.

78 % av de IT-relaterade användarna ansåg att de behövde vidta åtgärder medan 46 % av de övriga svarade att de ansåg det (se bild 10). Resultaten tyder på att de med IT-relaterat sysselsättning har en högre medvetenhet om säkerhetsrisker vid interaktion med öppna WiFi-nätverk, varpå det bör gå att öka medvetenheten hos de övriga användarna och få dem att vidta åtgärder genom att öka deras kunskap om ämnet. De IT-relaterade användarna säger sig i större utsträckning känna till de risker de utsätter sig för vid användande av nätverken (se bild 9), vilket kan förklara att de inte är speciellt bekymrade när de använder nätverken (se bild 6). Känner de till riskerna är chansen större att de vidtar åtgärder för att motverka dem och de IT-relaterade användarna hade även större kännedom kring tekniker som kan skydda deras kommunikation (se bild 7).

De IT-relaterade användarna visade dock i vissa fall en avsaknad av kunskap. 14 % av dem trodde att det var lagligt att manipulera nätverkstrafiken och 44 % visste inte om det var lagligt, något som tyder på att även deras kunskap bör ökas. 57 % av användarna, oberoende av användarkategori, stängde inte av WiFi på sin enhet efter användning (se bild 5) och även om de IT-relaterade hade en högre kännedom om riskerna visade det sig att 26 % av dem inte ens visste hur man skiljer ett öppet nätverk från ett krypterat (se bild 8). 43 % av de övriga kunde heller inte skilja nätverken åt varpå en förbättring inom just detta område borde prioriteras. Då vi i vårt praktikfall (se avsnitt 4.3.3) visar på att det i dagsläget saknas information om säkerhetsriskerna i öppna WiFi-nätverk är det inte konstigt att användarna inte vet hur de skiljer nätverken åt. För att öka medvetenheten om riskerna är det därför viktigt att tydliggöra för användarna vilken typ av nätverk de kopplar upp sig på.

5.3 Hur svårt är det att utnyttja informationen som skickas i öppna WiFi-nätverk?

Genom vår observation (se avsnitt 4.3) har vi kunnat visa på ett antal risker i öppna WiFi-nätverk, även bortsett från de attacker presenterade i teoriavsnittet som kräver omfattande teknisk kompetens. När vi satte upp vårt eget öppna WiFi-nätverk på en allmän plats kopplade flera användare upp sig på nätverket och riskerade därmed att en angripare manipulerade och dirigerade om trafiken (Lawson, 2013; Rahman et al. 2007). Det skulle kunna bero på att vår signalstyrka överträffade de andra nätverkens, något som Klasnja et al. (2008) och Mülec et al. (2011) i sin forskning beskriver som en avgörande faktor, men det skulle krävas mer omfattande observationer för att bekräfta detta. Då så många kopplade upp sig på nätverket bör det inte vara några svårigheter för en angripare att få användare att

ansluta sig till en RAP (se avsnitt 4.3.2). Angriparen behöver inte ens bemöda sig att ”lura” användarna med ett platsspecifikt SSID så länge de kan erbjuda en stark signalstyrka. Ingen av deltagarna i undersökningen utförd av Klasnja et al. (2008) trodde att ett öppet WiFi-nätverk tillhandahölls av en angripare med intentioner att utnyttja deras information, vilket tyder på en okunnighet som i sig utgör en säkerhetsrisk. Det är viktigt att användaren i så hög grad som möjligt säkerställer att nätverket är legitimt, vilket dock kan vara svårt eftersom en angripare genom en DoS-attack kan göra det legitima nätverket otillgängligt. Det som gör RAP- och MITM-attacker extra besvärliga är att det är nästan omöjligt för en vanlig användare att avgöra om de blivit utsatta för en attack (Johnston, 2014). Eftersom vi utan någon förkunskap kunde sätta upp ett nätverk och få användare att ansluta sig till det är det inte svårt för en angripare att få användare att ansluta sig till en RAP.

En angripare som “sniffar” ett nätverk kan enbart lyssna på datatrafiken som skickas över nätverket (Mülec et al. 2011), men vi visar i vårt praktikfall att även den typen av attack kan orsaka omfattande skador för användarna (se bild 16 och 17). Undersökningen av Klasnja et al. (2008) visade även att användarna initialt inte reflekterade över vilken information de delade med sig av, men när information presenterades för dem reagerade de och visade en oro över vad de faktiskt exponerade på nätverken. Användarna var även lika oroliga för ”hackers” som för risken att någon skulle se över axeln på dem när de arbetade med datorn. Genom att ta del av nätverkstrafiken är det i princip möjligt att ta del av samma information som genom att titta över axeln på användaren (se bild 14) och därför kan sådan information användas för att påverka användarnas beteende.

Att ”sniffa” ett nätverk är enkelt och kräver inga tekniska förkunskaper. Programvara för at övervaka nätverken kan hämtas gratis från internet och genom att följa tillhörande instruktioner kan vem som helst analysera nätverkstrafiken. Om en användare är tvungen att använda tjänster som kräver att känslig information matas in är det därför viktigt att det sker på en SSL-krypterad sida och att användaren inte har godkänt några certifikatvarningar. Majoriteten av de större sidorna, så som Facebook och Google, använder sig av SSL-kryptering men flertalet andra sidor saknar krypteringen vid inloggning. Inloggningsuppgifter, både användarnamn och lösenord, skickas i de fallen i klartext över nätverket och kan enkelt läsas av genom att “sniffa” nätverket. Användare som har samma lösenord för flera tjänster är exponerade i ännu högre grad då angriparen kan få tillgång till deras andra sidor. Då det i princip är omöjligt för en användare att upptäcka en väl utförd attack (Johnston, 2014) har angriparen tid att testa lösenorden mot andra tjänster eller att avvakta tills användaren exponerar mer känslig information. Genom att använda sig av olika lösenord för olika tjänster minimerar användaren risken att skadan blir omfattande, men bland annat Yan et al. (2004) visar att användare tenderar att återanvända lösenord. Flera lösenord kan verka problematiskt för användaren men, likt det Schneier (2008) menar, så är säkerhet en kompromiss där för- och nackdelar måste vägas mot varandra.

Vi lyckades övervaka nätverkstrafiken och skulle kunnat utnyttja lösenord som matades in på sidor utan SSL-kryptering, vilket visar att det är enkelt att utnyttja informationen som skickas över nätverken. Både Schneier (2008) och Klasnja et al. (2008) betonar att människor har svårt att uppfatta risker de inte kan greppa eller förstå och genom att konkret visa på vilken information en angripare enkelt kan få tag i kan den aspekten av riskuppfattningen minskas.

5.4 Hur når man ut till användarna?

Vårt lösningsförslag (se avsnitt 5.5) för att öka användarnas medvetenhet fokuserar på en visuell presentation av säkerhetsriskerna. Eftersom vår enkätundersökning visade att många användare i dagsläget inte kan skilja ett öppet nätverk från ett krypterat (se bild 8), bör första steget vara att tydligt varna användare om att det är ett öppet nätverk de ansluter sig till. Wogalters (2006) menar att användare med tidigare kännedom om området kopplat till en säkerhetsvarning brukar lita på sina egna erfarenheter framför varningarna. Då Klasnja et al.

(2008) visar att användare har stor kännedom om användning av WiFi är det troligt att de därför litar på sina erfarenheter. För att användare skall reagera på säkerhetsvarningar är det därmed viktigt att de är utformade på ett sådant sätt att de fångar användarens uppmärksamhet (Egelman, Cranor & Hong, 2008; Kahneman, 2003).

Varningarna i Windows 7 och 8 (se bild 21) är det enda tecken på någon varning vi kunnat hitta. De specifika varningarna klassas enligt Egelman, Cranor och Hongs (2008) beskrivning som passiva varningar (se bild 1 och 2) och de uppfyller knappt det första steget i modellen presenterad av Kahneman (2003) och Cranor (2006). I deras undersökning fastslogs att endast 13 % av deltagarna agerade utifrån passiva varningar medan 79 % agerade på aktiva. Därmed är det inte säkert att en aktiv varning får användaren att agera, men chansen att det sker får anses öka markant. Kahneman (2003) visar på hur användandet av specifika ord kan öka möjligheten att få användare att reagera, där t.ex. ord som ”Danger” har större genomslagskraft än ”Caution”. Garg och Camp (2012) är inne på liknande spår, men menar att det är viktigt att använda en terminologi som användaren kan relatera till. Ord som virus, trojan och spion är alla kopplade till en fysisk fara vilket underlättar för användaren att koppla det virtuella hotet till verkligheten (Garg & Camp, 2012). Användare har i samband med öppna WiFi-nätverk visat sig vara oroliga över ”hackers” och identitetsstöld (Attipoe, 2013; Klasnja et al. 2008), vilket tyder på att det bör gå att fånga deras uppmärksamhet genom att uttryckligen använda sig av de termerna i varningstexter. Då ordet ”hackers” blivit ett generellt samlingsnamn som saknar lämplig svensk översättning bör ordet även i svenska sammanhang användas i sin originalformulering.

Att använda aktiva varningar med välformulerad varningstext bör vara ett effektivt sätt att få användare att reagera på att det är ett öppet nätverk de försöker ansluta sig till, men de måste även förstå vad det innebär och vilka potentiella säkerhetsrisker som finns. Vår enkätundersökning, liksom undersökningen av Klasnja et al. (2008), visar att användarna (framför allt de utan IT-relaterad sysselsättning) inte känner till eller förstår säkerhetsriskerna vid interaktion med öppna WiFi-nätverk (se bild 9). Det är därför viktigt att ge dem möjlighet att få mer information kring det varningen avser. Användarna måste förstå varningen och bli tillräckligt motiverade att agera utifrån dem. Oberoende av användarkategori trodde få användare i vår enkätundersökning att de kan surfa säkert utan att vidta åtgärder (se bild 10). Istället är det okunskapen, framför allt hos de övriga användarna, som är en stor faktor och det är därför viktigt att informera dem om de motåtgärder de kan ta. Ett sätt att få användare att lära sig mer om säkerhet är att tillsammans med den aktiva varningen erbjuda en länk till en hemsida där problematiken presenteras för användaren. Där visas motåtgärder användaren kan göra för att förbättra sin säkerhet i likhet med det Egelman, Cranor och Hong (2008) och Kahneman (2003) beskriver. En liknande presentation finns bland annat i webbläsaren Google Chrome vid varningar om att hela webbplatsen inte är SSL-krypterad. Webbläsaren erbjuder användaren möjlighet att få mer information genom att klicka på “Vad innebär detta?”. Då presenteras alla symboler kopplade till varningen tillsammans med en beskrivning av vad de innebär. En varning om att hela sidan inte är SSL-krypterad beskrivs tillsammans med ikonen för varningen:

“Webbplatsen använder SSL, men Google Chrome har upptäckt osäkert innehåll på sidan. Var försiktig om du anger känslig information på sidan. Osäkert innehåll kan utgöra ett kryphål för någon som vill manipulera sidan.” (Google, 2014)

Tidigare på sidan finns en beskrivning av SSL, hur användaren skall avgöra om en sida är SSL-krypterad samt varför SSL-krypering används (Google, 2014). Informationen är presenterad på ett sådant sätt att användare utan omfattande datorkunskaper skall kunna förstå den, varpå även de kan agera på ett ändamålsenligt sätt.

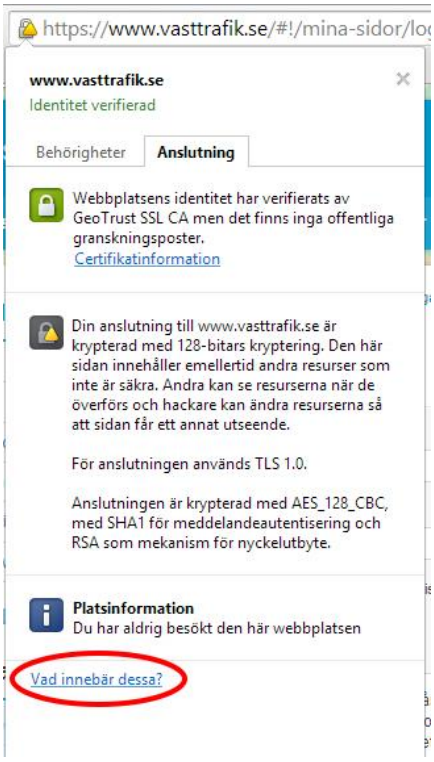

Bild 22. Varningsmeddelande i Google Chrome

Det är viktigt att användarna får varningarna utan att själva behöva installera någon extra programvara. Förslaget av Klasnja et al. (2008) att visualisera informationen användarna delar med sig av är en god idé, men kräver att användaren installerar verktyget för att kunna ta del av fördelarna. Då användarna visar en stor okunskap om säkerhetsaspekterna är det inte troligt att de aktivt skulle installera och använda sig av verktyget. Varningarna bör därmed implementeras direkt i operativsystemen där användarna inte kan välja huruvida de vill ta del av dem eller ej.

5.5 Lösningsförslag

Sammanfattningsvis presenteras nedan vårt förslag för att öka användarnas medvetenhet vid interaktion på nätverken genom att visualisera och informera om säkerhetsrisker.

- Användarnas uppmärksamhet måste tillkallas genom aktiva varningar, då de visat sig vara klart effektivare än passiva varningar (Egelman, Cranor & Hong, 2008). För att få användarna att reagera på varningar krävs formuleringar som påkallar deras uppmärksamhet (Kahneman, 2003) och får dem att lita på varningen framför sina egna erfarenheter (Wogalters, 2006). Genom att använda en terminologi som användarna kan koppla till verkliga hot (Garg & Camp, 2012) kan problemet med att användare har svårt att uppfatta virtuella och anonyma hot motverkas (Garg & Camp, 2012; Schneier, 2008). De hot användarna uppfattar som störst, såsom ”hackers” och identitetsstöld (Attipoe, 2013; Garg & Camp, 2012; Klasjna et al. 2008), bör användas för att få användarna att tro på varningarna och agera utifrån dem.
- Då användarnas medvetenhet om säkerhetsaspekter kopplade till nätverken visat sig vara låg krävs att varningarna tillhandahålls utan att användaren själv behöver agera. Det optimala vore att implementera varningarna direkt i enheternas operativsystem, men de största operativsystemen (Android, Apple och Windows) visar i dagsläget

knappt någon information om att nätverket vill ansluta sig till är osäkert sådant (se bild 18, 19, 20 & 21). Det kan vara en av anledningarna till att användarna har svårt att avgöra om ett nätverk är öppet eller krypterat (se bild 8). Genom att visualisera varningarna direkt i operativsystemen tvingas användarna att ta ställning till hur de vill fortsätta. En alternativ miljö att implementera varningarna i är direkt i webbläsaren, vilket dock medför risken att användarna misstar varningen för en certifikatvarning (se bild 13) och per automatik ignorerar den.

- För att användarna ska kunna vidta åtgärder för att motverka säkerhetsriskerna krävs att de förstår varningarna och vet hur de skall agera utifrån dem (Cranor, 2006; Wogalter, 2006). Genom att, i likhet med SSL-varningen i Google Chrome (se bild 22), erbjuda användarna möjlighet att få mer information angående säkerheten i nätverken erbjuds de underlag för att kunna väga riskerna mot kostnaderna (Schneier, 2008). De potentiella risker användarna utsätter sig för (se avsnitt 2.1.2) bör, tillsammans med liknande information som den vi visat i vårt praktikfall (se avsnitt 4.3.3), presenteras för användarna för att de ska förstå vilken information de öppet delar med sig av på nätverken. Det är även viktigt att användaren förstår att deras information även kan utnyttjas av personer utan omfattande tekniska kunskaper. En beskrivning av tillgängliga motåtgärder (se avsnitt 2.1.3) bör även förklaras på sådant sätt att även användare utan teknisk bakgrund förstår dem.

5.6 Aktivt förebyggande arbete

Då vi inför vår observation talade med Jens Ahlstrand på Polisen nämnde även han att fokus bör ligga på att öka användarnas medvetenhet. Han var även intresserad av att ta del av arbetet varpå vi även vill inkludera ett konkret lösningsförslag anpassat för Polisen. När tidningen *PC För Alla* publicerade sin artikelserie om säkerhet i öppna WiFi-nätverk visade de på hur enkelt det är att ta del av den information användare lämnar ifrån sig (PC För Alla, 2012). Problemet med artikeln var just att den publicerades i PC För Alla, en tidning som främst når ut till IT-intresserade användare. I vår enkätundersökning blev det uppenbart att användare utan IT-relaterad sysselsättning hade lägre medvetenhet om säkerhetsaspekterna kring nätverken och således bör informationen spridas i mer allmänt tillgängliga medier.

En av Polisens viktigaste uppgifter är att förebygga att nya brott sker (Polisen, 2014). För att kunna göra det samarbetar man t.ex. med externa aktörer som företag och organisationer av olika slag. Vårt förslag är att Polisen även utsträcker sitt samarbete till en större nyhetskanal för att kunna nå ut till så många användare som möjligt och kunna utföra ett aktivt förebyggande arbete. Tidningen Metro rapporterade bland annat om tidigare nämnda Heartbleed-buggen (Metro, 2014), vilket tyder på att det finns ett nyhetsvärde i liknande frågor.

Den största utmaningen med ett sådant tillvägagångssätt är att säkerställa att intresse väcks hos läsaren och att denne reflekterar över informationen. Schneier (2008) menar att människor uppfattar anonyma risker mindre hotfulla än personifierade risker och att individer har svårt att ta till sig statistik och siffror. Vi föreslår därför att artikelns förarbete bör bygga på det Kindberg et al. (2008) kallar ”experimentiell metodologi”, likt det vi gjorde i vår observation. Vi har i vår observation och vårt praktikfall visat hur enkelt det är att övervaka trafiken på öppna WiFi-nätverk och Klasnja et al. (2008) beskriver hur användarna blev oroliga och reflekterade över sitt internetanvändande när de fick veta vilken information de öppet hade delat med sig av. Genom att identifiera användare samtidigt som deras nätverkstrafik analyseras kan informationen de öppet delar med sig av presenteras för dem.

Artikeln bör vidare innehålla intervjuer med användarna där deras reflektioner kring säkerhetsaspekterna presenteras. På så sätt går det att belysa säkerhetsriskerna med hjälp av personliga historier snarare än statistik, något Schneier (2008) menar har en större påverkan på användarna. Då Klasnja et al. (2008) och Schneier (2008) menar att användare är reaktiva snarare än proaktiva är det viktigt att i förebyggande syfte arbeta med väcka medvetenhet om riskerna vid interaktion med öppna WiFi-nätverk. Klasnja et al. (2008) beskriver att attacker kan orsaka allt ifrån mild oro till allvarliga problem. Genom att arbeta enligt ovan beskrivna tillvägagångssätt kan effekten på användarna bli en mild oro som förhoppningsvis hjälper dem att undvika allvarliga problem.

6. Slutsats

Vår studie visade att användarna hade svårt att urskilja ett öppet nätverk från ett krypterat, att säkerhetsriskerna på ett enkelt sätt måste presenteras för dem och att det krävs att användarna ställs inför aktiva varningar för att öka chansen att de påverkas av varningar. De slutsatser vi dragit från våra underfrågor ligger till grund för att besvara vår frågeställning och presenteras nedan.

Har användare med IT-relaterad sysselsättning högre medvetenhet om säkerhetsrisker vid interaktion med öppna WiFi-nätverk än andra?

Användare med IT-relaterad sysselsättning har bättre kunskap kring säkerhetsteknik kopplat till öppna WiFi-nätverk och visar en högre medvetenhet om riskerna kopplade till nätverken. Därmed bör det gå att öka medvetenheten hos övriga användare genom att informera dem om riskerna och öka deras kunskap kring de motåtgärder de kan ta.

Hur svårt är det att utnyttja informationen som skickas i öppna WiFi-nätverk?

Vi har genom våra observationer och vårt praktikfall visat på att det är relativt enkelt att utnyttja information som skickas i öppna WiFi-nätverk. Det krävs inga omfattande tekniska förkunskaper för att kunna utnyttja känslig information som användarnamn och lösenord.

Hur når man ut till användarna?

Användarna måste informeras om säkerhetsriskerna i en miljö de redan använder. Genom att implementera aktiva varningar i de operativsystem som finns tillgängliga kan användarnas uppmärksamhet tillkallas. Varningarna bör använda termer som användaren kan relatera till verkligheten för att de ska påverkas av dem och reflektera kring säkerheten i nätverken. Vidare är det viktigt att användaren erbjuds möjlighet att ta del av ytterligare information för att få en djupare förståelse för säkerhetsrisker vid interaktion med öppna WiFi-nätverk.

Med dessa slutsatser besvaras vår frågeställning; *Hur kan medvetenheten om säkerhetsrisker i öppna WiFi-nätverk ökas?*

Med hjälp av aktiva varningar med termer användarna kan relatera kan användarnas uppmärksamhet tillkallas och de kan informeras om att det är ett öppet WiFi-nätverk de ansluter sig till. Vidare måste användarna på ett enkelt sätt kunna ta del av information angående riskerna kopplade till nätverken. Informationen måste gå att förstå utan någon tidigare kunskap om området och motåtgärder användarna kan ta måste presenteras. Genom att tillsammans med motåtgärderna visa hur enkelt det är att ta del av informationen som skickas över öppna WiFi-nätverk ökar chansen att användarna verkligen tar till sig informationen, reflekterar över sin WiFi-användning och ändrar sitt beteende. Då användare med IT-relaterad sysselsättning visade en större medvetenhet än övriga användare drar vi slutsatsen att medvetenheten kan ökas genom att öka kunskapen om ämnet. Vårt lösningsförslag för att varna och informera användarna bör därför vid implementation bidra till att öka medvetenheten om säkerhetsrisker i öppna WiFi-nätverk.

Vi anser dock att vårt lösningsförslag endas är ett av alternativen till hur medvetenheten om säkerhetsrisker i öppna WiFi-nätverk kan ökas och det bör ses som ett första steg i strävan att öka användarnas medvetenhet. Områdets omfattning och komplexitet krävde dock att vi avgränsade vårt arbete. Då det är svårt att avgöra hur omfattande problemet är i dagsläget och hur stort det kan bli i framtiden, är det också av vikt att Polisen arbetar aktivt i förebyggande syfte för att öka användares medvetenhet. Under arbetet inför vår observation upptäckte vi att ämnet inte enbart är komplext för användaren, utan även för de som arbetar med lagar och regelverk kring öppna WiFi-nätverk. Reaktionerna vi fick från Datainspektionen, Post- och telestyrelsen samt de jurister vi varit i kontakt med var att de inte riktigt kunde ge några konkreta svar på våra frågor. Det är en av orsakerna till varför vi anser att ett aktivt arbete i förebyggande syfte kräver att Polisen involveras, då angreppssättet rör sig i gråzonen kring vad som är lagligt. Oavsett arbetets omfattning anser vi att det finns ett värde i att presentera konkret information som användarna gjort tillgänglig för att visa vad som lagligt kan mottas i nätverken. Det bör få användarna att reflektera över vad en angripare med kriminella avsikter skulle kunna utföra och därmed få dem att ändra sitt beteende. För att nå ut till en stor målgrupp och väcka vidare intresse för frågan är det viktigt att använda allmänt tillgängliga kanaler för att informera om riskerna.

6.1 Förslag till vidare forskning

Då säkerhet i öppna WiFi-nätverk är ett problemområde som påverkas av ett flertal andra områden finns det en mängd intressanta frågor att forska vidare kring. Vårt resultat fokuserar på att informera användare om säkerhetsrisker genom att tvinga dem att göra aktiva val och vi vill uppmana till vidare forskning kring hur varningarna kan designas, realiseras och implementeras. Mer tekniska frågor kan beröra hur VPN och andra tekniker kan göras tillgängliga och användarvänliga för att öka säker användning av nätverken.

Referenslista

Attipoe, E. K. (2013) End User's Perception about Security of the Public Wireless Network. International Journal of Societal Applications of Computer Science, Volume 2, Issue 8, Aug. 2013, s 434-438.

Blue coat (2008) Technology Primer: Secure Sockets Layer (SSL). USA: Blue coat systems. [Elektronisk] Tillgänglig: http://www.bluecoat.com/documents/download/0485e335-7437-4c4e-bfc0-ca5ffc5bfd4d/16f27cf7-5d59-44b4-b17f-fb04acea369f [2014-05-10]

CBC (2014) CSEC used airport Wi-Fi to track Canadian travellers: Edward Snowden documents [Elektronisk] Tillgänglig: http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-12517881 [2014-05-12]

Chenoweth, T., Minch, R. & Tabor, S. (2010) Wireless Insecurity: Examining user Security Behavior on Public Networks. Communications of the ACM, Vol. 53, No. 2, s 134-138.

Codenomicon (2014) [Elektronisk] Tillgänglig: http://www.codenomicon.com/ [2014-05-11]

Cranor, L. F. (2006) What do they "indicate?": Evaluating security and privacy indicators. Magazine interactions - A contradiction in terms? Volume 13, Issue 3, May + Jun. 2006, s 45-47.

Dhamija, R., Tygar, J. B. & Hearst, M. (2006) Why Phising Works. CHI '06, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, s 581-590, New York, NY, USA.

Egelman, S., Cranor, L. F., & Hong, J. (2008) You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phising Warnings. CHI '08 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Pages 1065-1074. ACM, New York, NY, USA.

Englander, I. (2010) *The architecture of computer hardware, systems software & networking, 4th edition*. s 468. John Wiley & sons, inc. (Asia).

Eriksson, M. (2007) An Example of a Man-in-the-middle Attack Against Server Authenticated SSL-sessions. Simovits Consulting. [Elektronisk] Tillgänglig: http://www.simovits.com/sites/default/files/simovits_artikel_maninthemiddle_0.PDF [2014-05-17]

Gabriel, C. (2013) Wireless Broadband Alliance Industry Report 2013: Global Trends in Public Wi-Fi. [Elektronisk] Tillgänglig: http://www.wballiance.com/wba/wp-content/uploads/downloads/2013/11/WBA-Industry-Report-2013.pdf [2014-05-10]

Garg, V. & Camp, J. (2012) End User Perception of Online Risk Under Uncertainty. System Science (HICSS), 2012 45th Hawaii International Conference, 4-7, Jan. 2012, s 3278 – 3287.

Gebauer, J., Kline, D. & He, L. (2011) Password Security Risk versus Effort: An Exploratory Study on User-Perceived Risk and the Intention to Use Online Applications. Journal of Information Systems Applied Research, Volume 4, No. 2, Aug. 2011, s 52-62.

Google (2014) Kontrollera om webbplatsen använder en säker anslutning (SSL) [Elektronisk] Tillgänglig: https://support.google.com/chrome/answer/95617?p=ui_security_indicator&rd=1 [2014-05-10]

Greenstadt, R., Afroz, S. & Brennan, M. (2009) Mixed-Initiative Security Agents. AISec '09 Proceedings of the 2nd ACM workshop on Security and artificial intelligence, s 35-38. ACM, New York, NY, USA.

Guynes, C. S., Wu, Y. A. & Windsor, J. (2011) E-Commerce/Network Security Considerations. International Journal of Management & Information Systems, Volume 15, Number 2, s 1-8.

Göteborgs stad (2014) City-card. [Elektronisk] Tillgänglig: http://www.goteborg.com/sv/Gora/City-Card-wifi/ [2014-04-07]

Hamid, R. A. (2003) Wireless Lan: Security issues and solutions. SANS institute, InfoSec reading room. [Elektronisk] Tillgänglig: http://www.scribd.com/doc/134484637/wireless-lan-security-issues-solutions-1009-pdf [2014-05-17]

Heartbleed (2014) The Heartbleed Bug [Elektronisk] Tillgänglig: http://heartbleed.com/ [2014-05-17]

Johnston, A. (2014) Detecting Man in the Middle Attacks on Ephemeral Diffie-Hellman without Relying on a Public Key Infrastructure in Real-Time Communications. Avaya, Inc., Washington University in St. Louis. [Elektronisk] Tillgänglig: https://www.w3.org/2014/strint/papers/51.pdf [2014-05-16]

Kahneman, D. (2003) Maps of Bounded Rationality: Psychology for Behavioral Economics. The American Economic Review, Vol. 93, No. 5 Dec. 2003, s 1449-1475.

Kindberg, T., O'Neil, E., Bevan, C., Jay, T., Kostakos, V. & Stanton, F. D. (2008) Measuring Trust in Wi-Fi Hotspots. CHI '08 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, s 173-182.

Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P. & Wetherall, D. (2008) When I'm on Wi-Fi I am Fearless: Privacy Concerns & Practices in Everyday Wi-Fi Use. Proceedings of CHI 2009, s 1993-2002. ACM Press, NY, USA.

Koved, L., Trewin, S., Swart, C., Singh, K., Cheng, P-C. & Chari, S. (2013) Perceived Security Risks in Mobile Interaction. Symposium on Usable Privacy and Security (SOUPS) 2013, Jul. 24-26, 2013, Newcastle, UK.

Lawson, K (2013) There Is No Vacation from Cybercrime in WiFi hotspots. USA Today Magazine; Jul. 2013, Vol. 142, Issue 2818, s 60.

Lehembre, G. (2005) WiFi sercurity - WEP, WAP and WAP2. [Elektronisk] Tillgänglig: http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_EN.pdf [2014-04-16]

McKinley, H., L. (2003) SSL and TLS: A Beginners Guide. SANS Institute; InfoSec Reading Room. [Elektronisk] Tillgänglig: http://www.sans.org/reading-room/whitepapers/protocols/ssl-tls-beginners-guide-1029 [2014-05-10]

Metro (2014) Nätets "största säkerhetsläcka någonsin" upptäckt. [Elektronisk] Tillgänglig: http://www.metro.se/teknik/natets-storsta-sakerhetslacka-nagonsin-upptackt/EVHndh!Wcv38F6U6n8Es/ [2014-05-14]

Microsoft (2014) Certifikatfel: Vanliga frågor och svar [Elektronisk] Tillgänglig: http://windows.microsoft.com/sv-se/internet-explorer/certificate-errors-faq#ie=ie-11 [2014-05-01]

Mitchell B.(2014) The MAC address - An introduction to MAC addressing. [Elektronisk] http://compnetworking.about.com/od/networkprotocolsip/l/aa062202a.htm [2014-05-21]

Mülec, G., Vasiu, R., Frigura-Ilasa, F. M. & Vatau, D. (2011) WLAN Security Performance Study. NEHIPISIC'11 Proceeding of 10th WSEAS international conference on electronics, hardware, wireless and optical communications, s 401-406.

Nussel, L. (2010) The evil twin problem with WPA2-Enterprise. SUSE Linux Products GmbH version 1.1. [Elektronisk] Tillgänglig: http://users.suse.com/~lnussel/The_Evil_Twin_problem_with_WPA2-Enterprise_v1.1.pdf [2014-05-17]

Park, J. S. & Dicoi, D. (2003) WLAN Security: Current and Future. Internet Computing, IEEE, Volume: 7, Issue: 5, s. 60-65.

Patel, R. & Davisson, B. (2011) Forskningsmetodikens grunder. Studentlitteratur, Lund.

PC för alla (2012) Så avlyssnas du när du surfar trådlöst på stan. [Elektronisk] Tillgänglig: http://pcforalla.idg.se/2.1054/1.440423/sa-avlyssnas-du-nar-du-surfar-tradlost-pa-stan/sida/2/sida-2-tillatet-att-avlyssna [2014-05-11]

Pervaiz, M. O., Cardei, M. & Wu, J. (2007) Security in wireless local are networks. I Xiao Y. & Pan Y. (red.) *Security in Distributed and Networking Systems*. World scientific publishing Co. Pte. Ltd. s 393-419.

Pfleeger, C. P. & Pfleeger, S. L. (2007) Security in computing, 4th Edition. Pearson education. USA. ISBN: 0-13-239-077-9.

Polisen (2014) Brottsförebyggande arbete. [Elektronisk] Tillgänglig: http://polisen.se/Dalarna/Om-polisen/Sa-arbetar-Polisen/Brottsforebyggande-arbete/ [2014-05-13]

Rahman, R. H., Nowsheen, N., Khan, M. A. & Khan A. H. (2007) Wireless LAN security: An in-depth study of the threats and vulnerabilities. Asian Journal of Information Technonology, Volume 6, Issue 4, s 441-446.

Schneier, B (2008) The Psychology of Risk. [Elektronisk] Tillgänglig: http://www.schneier.com/essay-155.html [2014-03-31]

SFS 2003:389. Lagen om elektronisk kommunikation. Stockholm. Post- och telestyrelsen.

Sharp, H., Rogers, Y. & Preece, J. (2007) Interaction Design: Beyond Human-computer Interaction. John Wiley & Sons; 2nd Edition edition.

Slovic, P. & Peters, E. (2006) Risk Perception and Affect. Current Directions in Psychological Science, Dece. 2006, vol. 15, no. 6, s. 322-325.

Symantec (2012) Beginner's guide to SSL certificates. USA: Symantec Corporation World Headquarters. [Elektronisk] Tillgänglig: https://www.symantec.com/content/en/us/enterprise/white_papers/b-beginners-guide-to-ssl-certificates_WP.pdf [2014-05-10]

The British Psychological Society (2010) Code of Human Resource Ethics. [Elektronisk] Tillgänglig: http://www.bps.org.uk/sites/default/files/documents/code_of_human_research_ethics.pdf [2014-04-02]

Viaplay (2014) [Elektronisk] Tillgänglig: http:/www.viaplay.se [2014-05-19]

Waliullah, K. N. & Gan, D. (2014) Wireless LAN Security Threats & Vulnerabilities. International Journal of advanced computer science and application. Vol 5, No. 1, s. 77-86.

Weber, E. U. & Hsee, C. (1998) Cross-cultural Differences in Risk Peception, but Cross-culture Similarities in Attitudes Towards Perceived Risks. Management Science, Vol. 44, No. 9, Sep. 1998, s 1205-1217.

WhatIsMyIPAddress.com (2014) What is an IP Address? http://whatismyipaddress.com/ip-address [2014-05-21]

Wifikartan (2014) Göteborg [Elektronisk] Tillgänglig: http://www.wifikartan.se/G%C3%B6teborg/ [2014-04-07]

Wogalter, M. S. (2006) Communication-Human Information Processing (C-HIP) Model. In M. S. Wogalter (red.) *Handbook of Warnings*, Ed. Lawrence Erlbaum Associates, 2006, s. 51–61.

Yan, J., Blackwell, A., Anderson, R. & Alasdair, G. (2004) Password Memorability and Security: Empirical Results. IEEE Security and Privacy, Vol. 2, Issue 5, Sep. 2004, s 25-31.

Yoo, Y. (2010) Computing in Everyday Life: A Call for Research on Experiential Computing. MIS Quarterly, Vol. 34, No. 2, Jun. 2010, s 213-231.

Bilaga 1 – Intervjufrågor till Jakob Schlyter

Allmänt

Personlig introduktion

Vilka risker finns vid interaktion med öppna WiFi-nätverk?

Vad bör användare inte göra när man använder ett oskyddat nätverk?

Bör man använda sig av öppna nätverk över huvud taget?

Användare

Vad kan användare göra för att öka sin säkerhet? Vad är enklast för användare i relation till den säkerhet det ger?

Hur tror du användare uppfattar säkerheten i öppna WiFi-nätverk?

Hur kan man öka användarnas kunskap om tekniker för att skydda sig?

Kan man utesluta användare ur ekvationen och eliminera dem som riskfaktor?

Vad finns det för sätt att skydda sig mot attacker?

Kan man se någon som ansvarig för att öka medvetenheten om säkerhetsriskerna?

Specifika frågor

Hur stor är skillnaden i säkerhet mellan ett WPA2-krypterat och ett öppet nätverk?

Använder man sig ännu av WEP, även om det har brister?

Hur stor påverkan har det för en angripare att vara uppkopplad till samma nätverk som offret? Vad kan de göra i en sådan situation som inte går annars?

Kommer skyddet att bli bättre eller kommer attackerna att öka i framtiden?

Forskning och artiklar vi studerat visar att MITM-attacker är relativt vanliga i USA, men inte lika vanliga i Sverige. Tror du att de kommer bli det i framtiden?

Vilken typ av attack är vanligast?

Hur skyddad är man om man använder sig av tekniker som VPN och SSL?

Bilaga 2 – Frågor i enkätundersökning

Ålder? (ett svarsalternativ)

- 0-18
- 19-24
- 25-29
- 30-39
- 40-49
- 50-59
- 60+

Vad är din huvudsakliga sysselsättning? (ett svarsalternativ)

- Studerar – IT-relaterat
- Studerar – Övrig
- Arbetar – IT-relaterat
- Arbetar – Övrigt
- Annat
- Vill inte uppge

Hur ofta kopplar du upp dig på öppna WiFi-nätverk? (ett svarsalternativ)

- Några gånger om dagen
- Några gånger i veckan
- Några gånger i månaden
- Några gånger per år
- Aldrig

Var har du kopplat upp dig på ett öppet WiFi-nätverk under de senaste 12 månaderna? (flervalsalternativ)

- Hotell
- Café/Restaurang
- Flygplats
- Bibliotek
- Butik
- Skola
- Annat (vänligen specificera)

Vilka enheter använder du dig av när du kopplar upp dig på öppna WiFi-nätverk? (flervalsalternativ)

- Dator
- Mobiltelefon
- Surfplatta
- Annan (vänligen specificera)

Hur känner du dig inför att dina aktiviteter kan ses av andra när du surfar på ett öppet WiFi-nätverk? (ett svarsalternativ)

- Jag är obekymrad
- Jag är relativt obekymrad
- Jag är orolig
- Jag är väldigt orolig
- Inget av ovanstående
- Jag surfar inte på öppna WiFi-nätverk

Stänger du av WiFi på din enhet efter användning? (ett svarsalternativ)

- Nej
- Vet ej
- Ja (vänligen specificera varför)

Vilken eller vilka av följande tror du skyddar kommunikationen när du surfar på ett öppet WiFi-nätverk? (flervalsalternativ)

- Brandvägg
- Anti-virus
- WPA/WPA2
- WEP
- HTTPS
- Virtual Private Network (VPN)
- Jag tror inte att någon av ovanstående hjälper
- Jag känner inte till någon av ovanstående

Vilka av följande tjänster använder du på ett öppet WiFi-nätverk? (flervalsalternativ)

- Banktjänster
- Online-shopping
- Sidor kopplar till jobbet (t.ex. intranät)
- Sociala medier
- Mail
- Nyhetssidor
- Spel
- Annat (vänligen specificera)

Vet du hur man skiljer mellan ett öppet och ett krypterat nätverk? (Ja/Nej)

När jag surfar på ett öppet WiFi-nätverk utsätter jag mig för risken att få personuppgifter och annan information kapad (Ja/Nej/Vet ej)

Det är lagligt att sätta upp ett öppet WiFi-nätverk (Ja/Nej/Vet ej)

Det är lagligt att analysera trafiken på ett öppet WiFi-nätverk (Ja/Nej/Vet ej)

Det är lagligt att manipulera trafiken på ett öppet WiFi-nätverk (Ja/Nej/Vet ej)

Ett nätverk som begär ett lösenord är automatiskt ett säkert nätverk (Ja/Nej/Vet ej)

Det är säkrare att surfa med en dator på ett öppet WiFi-nätverk än med en mobiltelefon (Ja/Nej/Vet ej)

Jag behöver vidta åtgärder för att kunna surfa säkert på ett öppet WiFi-nätverk (Ja/Nej/Vet ej)

Leverantören av ett öppet WiFi-nätverk tillhandahåller säkerhet för nätverket (Ja/Nej/Vet ej)

Jag anser mig känna till riskerna jag utsätter mig för när jag använder öppna WiFi-nätverk (Ja/Nej)