Examensarbete

HÖGSKOLAN I SKÖVDE

WIRELESS PROTECTED SETUP (WPS)

Prestandajämförelse mellan Reaver och Bully

2015-09-12

Examensarbete inom huvudområdet Datalogi med inriktning mot nätverks- och systemadministration
Grundnivå 15 högskolepoäng

Fredrik Alm
920904-2812

Handledare: Mikael Lebram
Examinator: Jonas Mellin

Abstrakt

Wireless Protected Setup (WPS) är ett säkerhetsprotokoll för trådlösa nätverk. Dess design medför en allvarlig säkerhetsbrist som kan möjliggöra att obehöriga kan få åtkomst till ett lösenordskyddat trådlöst nätverk. Vid attack finns det olika verktyg tillgängliga att använda.

I denna rapport jämförs mjukvaruverktygen Reaver och Bully i attack mot WiFi's WPS-protokoll, där Bullys prestanda tidigare har påvisats vara mer effektiv och förutsätts snabbare utföra brute-forceattack jämfört med Reaver. Ett praktiskt laborationsexperiment har utförts för att undersöka vilken skillnad i hastighet som kan ses mellan verktygen Reaver och Bully i en brute-forceattack. Experimentet utfördes genom att mäta tiden det tog för de två verktygen att testa 100 PIN-nycklar mot en router utan skyddsmekanismer hos WPS.

Resultatet visar att Bully utför en brute-forceattack i högre hastighet jämfört med Reaver. Dock, med den högre attackhastigheten som Bully innehar, kan stabilitetsproblem vid attack medföras, vilket öppnar upp för framtida diskussion om högre hastighet bör prioriteras över stabilitet för lyckade attacker.

Nyckelord: Wi-Fi, Wireless Protected Setup, WPS, Reaver, Bully, IT-Säkerhet.

Abstract

Wireless Protected Setup (WPS) is a security protocol for wireless networks. Its design contains a serious security flaw that could allow an attacker access to a password-protected wireless network. An attack can be executed using various tools available.

In this report, the software-tools Reaver and Bully are compared in performance against WiFi's WPS-protocol, where Bully previously has been shown to be more effective and predicted faster to execute a bruteforce-attack. A practical laboration has been executed in order to determine differences in speed that can be seen between the tools Reaver and Bully in a bruteforce-attack. The experiment was done by measuring the time it took both tools to test 100 PIN-numbers against a router without protection for WPS.

The result shows that Bully performs a bruteforce-attack in higher speed compared to Reaver. However, with the higher attack-speed that Bully uses, some stability issues may follow, opening the topic of future discussion regarding priorities of speed vs. stability for successful attacks.

Keywords: Wi-Fi, Wireless Protected Setup, WPS, Reaver, Bully, IT-Security.

Förord

Jag vill tacka min handledare Mikael Lebram, familj samt vänner för stöd och bidrag till detta arbete. Jag vill dessutom tacka mina före detta programansvariga Jakob Ahlin, Helen Persson och Dennis Modig för stöd och god vägledning genom utbildningen.

Skövde, 2015-06-14
Fredrik Alm

Innehållsförteckning

1. Introduktion

Wireless Protected Setup (WPS) är ett säkerhetsprotokoll i IEEE 802.11 (Wi-Fi) som, sedan dess officiella introduktion 2006, har fått en bred implementering i utrustningar från olika tillverkare för både konsumenter och företag (Wi-Fi Alliance, 2014).

WPS blev vid lansering snabbt populär hos tillverkare och väl implementerad i trådlös utrustning, tack vare dess användarvänlighet (Cert, 2011). 2011 rapporterades en allvarlig sårbarhet i WPS som möjliggör att säkerhetsprotokollet kan forceras på kort tid med tillgänglig hård- och mjukvara (Viehböck, 2011). Säkerhetsbristen kan fortfarande vara aktiv hos många konsumenter på grund av felkonfigurerad och icke-uppdaterad utrustning. Sårbarheten i WPS-protokollet är ett fortsatt allvarligt hot mot integritet och informationssäkerhet i samhället, eftersom internetroutrar som fortfarande används av konsumenter kan vara påverkade av sårbarheten (Juhlin & Wangberg, 2014).

Mjukvaruverktygen Reaver och Bully är två Linux-baserade säkerhetsverktyg som är designade för att utnyttja den sårbarhet Viehböck (2011) presenterat genom brute-forceattack. Vid en sådan typ av attack är tidsåtgång vanligtvis den mest kostsamma faktorn. Tidsåtgången beror på en attackerares prestanda samt en nyckels komplexitet. Ju fler teckenkombinationer en nyckel har, desto mer ökar den uppskattade tiden som krävs för att slutföra en attack (McClure et al., 2009). Vilket verktyg som föredras att använda vid en brute-forceattack kan därför stå i relation till högst effektivitet.

Det finns tidigare forskning kring Reaver, i relation till WPS-sårbarheten, som visar att verktyget kan utföra en brute-forceattack (Aked et al., 2012). Det saknas dock dokumentation kring prestanda och attackhastigheter. Likt Reaver saknas även denna typ av dokumentation för verktyget Bully. Purcell (2013) beskriver Bully som mer prestandaoptimerat och effektivare än Reaver tack vare faktorer som förbättrad processor- och minneshantering. Då tidigare studier inte utförts kring Bullys påstådda prestandaoptimering saknas vetenskapligt resultat om huruvida Bully effektivare utför en brute-forceattack mot WPS i jämförelse med Reaver.

På grund av bristande forskning om prestanda i brute-forceattack, för både Reaver och Bully, syftar detta arbete till att följa en praktisk jämförelse mellan de båda verktygen. Denna undersökning ska följa ett experiment där prestanda i Reaver och Bully mäts och jämförs för att eventuellt kunna avgöra vilket verktyg som snabbast kan utföra en brute-forceattack.

2. Bakgrund

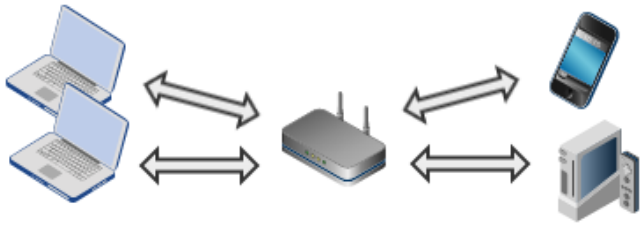
Majoriteten av den elektronik som kan kommunicera trådlöst via Wi-Fi till internet idag är baserad på en protokollstandard kallad IEEE 802.11. Den består av en uppsättning specifikationer för implementering av trådlös kommunikation. Denna standarduppsättning definierar hur en enhet ska kommunicera och konstrueras för att kunna kommunicera med övriga noder som använder samma standard (Radio Electronics, 2015).

En fördel med trådlöst Wi-Fi är att enheter som inte är beroende av fysiska inkopplingar, som smarta telefoner, kan i princip användas överallt tack vare den trådlösa uppkopplingen. En nackdel med den trådlösa tekniken är att trafiken som trådlöst skickas mellan noder inte alltid når sin destination på grund av hinder eller störningar. Detta kan resultera i varierade bandbredder och ojämna tidsintervaller. En ännu större nackdel med Wi-Fi är säkerhet och integritet eftersom information skickas i luften. Detta är ett ytterst känsligt område som bör beaktas vid distribuering och användning av Wi-Fi (Coleman & Westcott, 2012).

2.1 Modeller av trådlösa nätverk

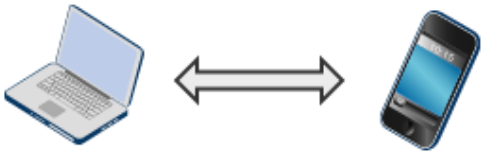
Vid användning av Wi-Fi mellan olika enheter brukar oftast två teorier om nätverkstyper appliceras för hur enheter ska ansluta till varandra; Infrastruktur och Ad-Hoc.

Infrastruktur. Anslutning sker trådlöst till en central åtkomstpunkt som kan kopplas vidare till ytterligare nätverk och förslagsvis internet (Se Figur 1). Detta är den vanligaste nätverkstypen och används oftast i nätverk där internetåtkomst ska distribueras till trådlösa enheter. I denna nätverkstyp kommunicerar en ansluten klient med andra enheter anslutna via samma nätverk, antingen fysiskt eller trådlöst (Coleman & Westcott, 2012).



Figur 1 “Infrastruktur”-nätverkstyp

Ad-Hoc. Vid användning av en ”Ad-Hoc”-nätverkstyp ansluter klienter direkt till varandra istället för via en central accesspunkt. Detta möjliggör direkt punkt-till-punkt kommunikation där infrastruktur-nätverkstyp anses olämplig eller inte är applicerbar (Coleman & Westcott, 2012). Denna nätverkstyp kräver inte en separat trådlös accesspunkt för att enheterna ska kunna kommunicera (Se Figur 2).



Figur 2 “Ad-Hoc”-nätverkstyp

2.2 Säkerhet i trådlösa nätverk

Eftersom trådlös trafik mellan noder skickas via radiovågor finns det möjligheter för obehöriga användare i närheten att fånga upp dessa radiovågor och avläsa trafik som skickas. Vid anslutning till ett trådlöst nätverk kan en attackerare utnyttja resurser och utföra såväl aktiva som passiva attacker på nätverket. Som åtgärd mot säkerhetshot och risker, i form av oönskad avlyssning och icke-autentiserad anslutning, har olika typer av säkerhetslösningar utvecklats, implementerats och kontinuerligt förbättrats i IEEE 802.11-standarden. Den vanligaste säkerhetslösningen är att skydda ett trådlöst nätverk via kryptering (Coleman & Westcott, 2012).

Kryptering är en av historiens mest omtalade och välanvända metoder för skydd av känslig information. Tack vare krigsföring och det moderna IT-samhället har utveckling av denna kunskap spelat stor roll för vissa av historiens vändpunkter och för personlig integritet (Schneier, 1996). Kryptering av information i ett trådlöst nätverk kan ske med olika säkerhetsprotokoll som WEP, WPA och WPA2 (Coleman & Westcott, 2012).

2.3 WPS

Wireless Protected Setup (WPS) är ett säkerhetsprotokoll utvecklat av Wi-Fi Alliance. Till skillnad från WEP och WPA medför protokollet inte extra säkerhet till trådlös utrustning, utan används endast som ett komplement för användarvänlig autentisering mot trådlösa nätverk som skyddas av WPA/2-PSK. Protokollet introducerades först 2006 och blev snabbt implementerat i utrustning av diverse tillverkare. Syftet med detta protokoll och tillhörande metoder är att underlätta anslutning till skyddade trådlösa nätverk. WPS kan användas av till exempel en hemanvändare vid autentisering av nya enheter, för att undvika inmatning av komplexa WPA-PSK-lösenordsfraser (Wi-Fi Alliance, 2014).

Via WPS finns nedanstående fyra metoder, som kan användas för autentisering mot ett trådlöst nätverk som alternativ till den WPA/2-PSK-nyckel som används:

- **Knapptryckmetod**
  En fysisk eller virtuell knapp på accesspunkten aktiveras samtidigt som en klients motsvarighet. Dessa enheter upprättar en tillfällig krypterad session via WPS-protokollet där WPA/2-PSK-nyckel översförs till klienten.

- **USB-metod**
  Ett USB-minne används för att överföra en WPA/2-PSK-nyckel från accesspunkt till klient.

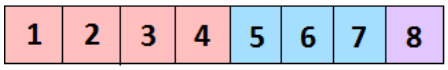
- **Nära-Fälts-Kommunikationsmetod**
  Nya enheter som kommer tillräckligt nära enheten kan autentiseras utan behov av att en användare manuellt skriver in WPA/2-PSK-nyckeln.

- **PIN-kodsmetod**
  En 8-siffrig PIN-kod, oftast förkonfigurerad på den trådlösa accesspunkten och fysiskt märkt på enheten. Denna kan användas som en alternativ lösenordsfras vid anslutning mot en accesspunkt. Vid användning av denna metod hämtar den anslutande klienten respektive WPA/2-PSK-nyckel för accesspunkten.

2.3.1 Sårbarhet

I december 2011 presenterade Viehböck (2011) en utförlig och detaljerad rapport på ett allvarligt designfel i PIN-kodsmetoden hos WPS, som gör den sårbar för brute-forceattack. Denna form av attack är en kryptoanalysattack där en angripare, slumpmässigt eller sekventiellt, gissar och blir nekad olika kombinationer av en nyckel, denna process upprepas tills rätt kombination är funnen. Målet med att utföra en brute-forceattack är att hitta en dold bit information, i detta fall en nyckel. Tidsåtgång vid en sådan attack är beroende av en attackerares datorprestanda och en nyckels komplexitet. Ju fler teckenkombinationer en nyckel har, desto mer ökar den uppskattade tiden som krävs för att slutföra en attack (McClure et al., 2009).

Sårbarheten som Viehböck (2011) presenterat avser bekräftelsemeddelanden som sänds mellan en anslutande klient och accesspunkt vid valideringsprocessen av en PIN-kod. Denna PIN-kod, som vanligen är fysiskt märkt på en Wi-Fi-router, består av 8 siffror. Den åttonde och sista siffran används som en checksumma och kan beräknas från de sju resterande siffrorna. Det finns därför sju okända siffror i varje nyckel, vilket ger totalt 10^7(10'000'000) möjliga kombinationer. De fyra första, och de tre resterande siffrorna i nyckeln, valideras i två separata block. Via bekräftelsemeddelanden rapporteras om blockens nyckel matchar eller inte (Se Figur 3).



Figur 3 WPS-Pinkod uppdelad i två block och checksumma.

Eftersom PIN-nyckeln är uppdelad i två block minskas antalet gissningar som krävs för att hitta rätt nyckel till totalt 11'000 möjliga kombinationer: 10^4(10'000) från de fyra första siffrorna, adderat med 10^3(1'000) möjliga kombinationer från de resterande tre siffrorna. Det totala antalet av endast 11'000 krävda gissningar är en drastisk minskning i jämförelse med 10^7(10'000'000) kombinationer.

Viehböck (2011) poängterar verifieringen av två separata block som ett designfel, eftersom det minskar antalet kombinationer som behöver testas. Denna brist möjliggör en praktisk attack som kan vara klar inom några timmar och en angripare kan då efterfråga accesspunktens WPA/2-PSK-nyckel i klartext för att själv kunna ansluta till nätverket.

Möjligheten att utnyttja denna sårbarhet beror på tillverkare och modell av trådlös enhet som erbjuder WPS-funktionalitet. Efter Viehböcks (2011) publicering av sårbarheten har tillverkare av trådlös utrustning vidtagit åtgärder genom att utveckla produkter utan WPS-tillgänglighet, alternativt med funktion att bromsa flertal misslyckade nyckelförsök. En trådlös enhet med aktiverad WPS-funktionalitet, och utan skydd för attack, är ytterst sårbar för denna form av brute-forceattack. Säkerhetsbristen kan dock utan större svårigheter oskadliggöras genom att WPS-autentisering via PIN-nyckel manuellt avaktiveras.

Sårbarheten är officiellt registrerad med identifikationsnummer CVE-2011-5053 (National Vulnerability Database, 2013).

2.4 Mjukvara och verktyg mot Wi-Fi-säkerhet

Med en ökad användning av Wi-Fi runt om i världen (ABIresearch, 2013) ökar även behovet av säkerhet och kryptering som skydd mot anslutning av icke-autentiserade användare. Mot de säkerhetsbrister som uppmärksammats i protokollen WEP, WPA och WPS finns det enligt Cache et al. (2010) mjukvaruverktyg speciellt utvecklade för att utnyttja dessa. De rekommenderar att ägare och administratörer av trådlösa nätverk bör införskaffa kunskap om bristerna i säkerhetsprotokollen WEP och WPA.

2.4.1 Aircrack-ng

Aircrack-ng (next generation) suite är ett samlingspaket med mjukvaruverktyg som kan användas för att undersöka och utnyttja säkerhetsbrister i trådlösa nätverk. ”Next Generation”-versionen introducerades 2007 som en efterföljare med nya funktioner till det populära Aircrack-verktyget. Detta samlingspaket kan utföra olika metoder av informationsinsamling, paketavlyssning, injicering av krypterade paket (WPA-TKIP) och brute-forceattacker (Aircrack, 2011).

2.4.2 Airodump-ng

Verktyget *airodump-ng* är del av aircrack-ng-paketet och kan, enligt Aircrack-ng Suite (2011), avlyssna tillgängliga trådlösa nätverk i närheten och dess kommunikation. Vid ett säkerhetstest kan detta verktyg användas för att samla in trådlös krypterad datatrafik. Dessa data kan vid senare tillfälle avkrypteras av en icke-autentiserad angripare via en brute-forceattack. Vid insamling av krypterad trafik från en trådlös router gynnar en hög användardensitet möjligheten för en lyckad attack att forcera en WEP eller WPA-nyckel (Cache et al., 2010).

2.4.3 Reaver

Verktyget Reaver är ett säkerhetsverktyg utvecklat för Linux-operativsystem av Tactical Network Solutions (2011) i öppen källkod. Det utvecklades som ett konceptbevis efter den sårbarhet Viehböck (2011) presenterande gällande WPS.

Vid användning exekveras Reaver i en terminal på en kompatibel[1] dator tillsammans med information om vald access-punkt att attackera. Reaver utför sin attack genom att exekvera en brute-forceattack mot en vald accesspunkt med aktiv WPS-funktionalitet. Brute-forceattacken utförs mot alla åtta siffror samtidigt och validerar de båda nyckelblocken separat. När en del av nyckeln (ett block) är korrekt gissad fortsätts attacken med nya kombinationer endast mot det resterande blocket. När båda block är korrekt gissade beräknas nyckelns checksumma, vilket resulterar i den sista siffran. Verktyget utför till sist en anslutning mot accesspunkten och efterfrågar nätverkets WPA-nyckel, vilket returneras i klartext till angriparen (Tactical Network Solutions, 2011).

2.4.4 Bully

Verktyget Bully är ett säkerhetsverktyg utvecklat för Linux-operativsystem av Brian Purcell (2013) i öppen källkod. Detta verktyg utvecklades efter Reaver och har till uppgift är att utföra brute-forceattacker mot WPS.

| 1 . Krav på linux-operativsystem med programbibliotek *ibcap* och *livsqlite3t. Är inkluderat i Kali Linux.*

Bullys koncept är identiskt med Reavers; att utnyttja det designfel som Viehböck (2011) presenterat. Purcell (2013) menar på att Bully har flera fördelar i jämförelse med Reaver. Dessa inkluderar färre beroenden, bättre minne- samt CPU-prestanda, korrekt hantering av endian och en ökad uppsättning alternativa inställningar.

Precis som Reaver har Bully testats mot olika accesspunkter från flera routerleverantörer, med olika konfigurationer och varierad framgång (Purcell, 2013). Vid användning av Bully exekveras verktyget, med liknande inställningar som Reaver, via en terminal i ett Linux-operativsystem.

2.4.5 Kali Linux

Linux-operativsystemet Kali Linux, utvecklat av Offensive Security (2013), är speciellt framtaget för säkerhetstestare och IT-forskare då operativsystemet kommer med ett stort antal förinstallerade säkerhetsverktyg. Bland dessa verktyg inkluderas tidigare nämnda Aircrack-ng, Airodump-ng, Reaver och Bully (Kali Linux Tools, 2015). Förinstallerad skivavbild av Kali för virtualisering i VMware finns tillgänglig för nedladdning via utvecklarnas hemsida Offensive Security (2015).

2.4.6 Alfa AWUS036H

Ett USB-nätverkskort för anslutning mot trådlösa nätverk, tillverkat av Alfta Networks Inc. Detta nätverkskort har blivit populärt hos säkerhetstestare av trådlösa nätverk, tack vare sin räckvidd, stabilitet och kompatibilitet med olika operativsystem. Främst bygger populariteten på nätverkskortets chip kallat RTL8187L. Detta chip har stöd för så kallad paketinjicering som kan användas vid attack mot WEP och WPA (Reaver Systems, 2014).

2.5 Internet-router

Konsumentbeteckningen ”internet-router” avser en nätverksenhet för hemmet dit en bredbandsanslutning kan kopplas och delas. En sådan enhet kommer vanligen med funktionen att kunna dela en internetanslutning via ett lokalt trådlöst nätverk som den själv distribuerar. Eftersom fler noder centralt kan ansluta till dessa typer av enheter klassas denna nätverkstyp som ”Infrastruktur”. Konsumentsanpassade internet-routrar är ofta användarvänliga och lätthanterliga med hårdvaruprestanda anpassad till färre enheter (i jämförelse med hårdvara riktad mot större nätverk som hos företag). Flera routermodeller från olika tillverkare levereras med ”plug-and-play”-support, vilket möjliggör minimal konfiguration för ett fungerande nätverk hos en slutanvändare (PCMag, 2015).

Internet-routrar går att köpa i svenska och utländska elektronikaffärer från olika tillverkare. Svenska internetleverantörer som Bredbandsbolaget, Tele2 och TeliaSonera har under flera år levererat internet-routrar åt sina bredbandskunder för att de ska kunna koppla upp sina digitala enheter mot internet (TeliaSonera, 2014).

2.5.1 BELKIN F7D4302 v1

Modell F7D4302 v1 av BELKIN är en äldre konsumentanpassad internet-router med inbyggt Wi-Fi (IEEE 802.11), tillverkad sedan februari 2010. Denna router kommer förkonfigurerad med WPS-funktionalitet aktiverad och är ytterst sårbar för säkerhetsbristen presenterad av Viehböck (2011). Denna modell och liknande modeller av BELKIN såldes till konsumenter innan Viehböcks rapport publicerades och sårbarheten uppmärksammades. Därför saknar modellens original-firmware (v1.00.2b) säkerhetsfunktioner som bromsar en attack mot WPS (Xiaopan, 2013).

3. Förstudier

Viehböck (2011) var först med att publicera information kring sårbarheten gällande PIN-kodsmetoden vid WPS-protokollet i en utförlig rapport. Denna rapport beskriver designfelet med att en PIN-nyckel verifieras i två separata block och hur en attackerare teoretiskt kan utnyttja denna säkerhetsbrist. Viehböcks (2011) beskrivande av bristen lade grund för utvecklingen av säkerhetsverktygen Reaver och Bully som kan utnyttja sårbarheten.

Aked et al. (2012) skriver i en artikel ett metodförslag för att testa sårbarheten presenterad av Viehböck (2011) genom att använda sig av verktyget Reaver (Tactical Network Solutions, 2011). I denna artikel reflekterar de över problemet som Viehböck (2011) presenterat i hans rapport. I artikeln presenterar de metod och resultat där de använt verktyget Reaver för att verifiera sårbarheten i WPS. I metoden beskrivs exekvering av verktyget och vilka parameterar som krävs vid attack. MAC-adress (BSSID) för det sårbara nätverket samt parameter för attackerarens nätverkskort var den enda information som Reaver krävde vid exekvering. Aked et al. (2012) beskriver i sin slutsats eventuell påverkan av användandet vid uppdaterad router-firmware. De menar på att om en router som har ett skydd mot WPS-attack i en nyare firmware, kan en återställning till hårdvarans ursprungliga firmware eliminera skyddet.

Juhlin och Wangberg (2014) vid Linnéuniversitet i Växjö undersökte, via intervjuer, spridning på säkerhetsbristen som Viehböck (2011) presenterat. De diskuterade dessutom olika försvarsmekanismer runt WPS-protokollet som uppdaterats med nyare internet-routrar, tillverkade eller uppdaterade efter publicering av sårbarheten. De använde sig av verktyget Reaver för att verifiera sårbarheten hos en lyckad attack i en laborationsmiljö med Kali Linux.

4. Problemformulering

Syftet med denna studie är att undersöka hastighetsskillnader mellan verktygen Reaver och Bully vid brute-forceattack mot WPS. Det som kommer undersökas är hur snabbt de båda verktygen kan testa 100 PIN-nycklar mot en sårbar internet-router i en laboration.

4.1 Frågeställning

Vilken hastighetsskillnad kan ses mellan verktygen Reaver och Bully i en brute-forceattack av 100 PIN-nycklar mot en trådlös internet-router utan skyddsmekanismer för WPS?

4.2 Motivering

Likt Reaver saknar verktyget Bully vetenskaplig dokumentation gällande prestanda. Utvecklaren av Bully beskriver dock sitt verktyg som mer effektivt än Reaver, tack vare faktorer som förbättrad processor- och minneshantering (Purcell, 2013). Eftersom det saknas tidigare studier som undersökt, eller stöder Bullys påstådda prestandaoptimering mot Reaver, syftar denna studie till att undersöka hastighetsskillnader mellan Reaver och Bully.

Denna studie riktas till de användare som utför WPS-attacker och/eller använder verktyg som Bully eller Reaver. För denna målgrupp kan studien vara intressant eftersom dessa verktyg används vid brute-forceattack. Målet med att utföra en brute-forceattack mot WPS är att hitta dess PIN-nyckel genom upprepade gissningar. Tidsåtgång för brute-forceattack beror vanligtvis på en attackerares datorprestanda och en nyckels komplexitet. Eftersom en PIN-nyckel i WPS endast består av åtta siffror kan en attackerare räkna ut max antal kombinationer som behöver testas. Hastighet vid brute-forceattack mot WPS baseras därför på en attackerares hårdvara och mjukvara. Det bör ligga ett intresse hos en attackerare av att använda det mest prestandaoptimerade verktyget, som snabbast kan utföra en brute-forceattack för den hårdvara som attackeraren har tillgänglig.

4.3 Delmål

Studiens experiment har delats in i sju delmål:

1. Konstruera en experimentell design för att kunna besvara studiens frågeställning.

2. Beskriva och analysera applicerbara hot som kan påverka studiens validitet.

3. Installera och konfigurera en laborationsmiljö enligt angiven experimentell design. I detta stadie konfigureras hårdvara och mjukvara för router och angripardator.

4. Verifiera konfigurationen av router och eventuella närliggande störmoment i form av andra trådlösa accesspunkter.

5. Utföra en testattack med Reaver för att verifiera WPS-sårbarheten i routern innan mätning, enligt den metod som Juhlin och Wangberg (2014) använde i sin studie.

6. Systematiskt starta 25 attacker för både Reaver och Bully, där varje attack avbryts efter att 100 PIN-nycklar testats. Tidsförloppet för varje mätning dokumenteras.

7. Sammanställa, analysera och utvärdera data från de utförda mätningarna.

4.4 Avgränsning

För att påvisa och verifiera säkerhetsbristen i WPS hos den trådlösa routern, utförs ett liknande test som Juhlin och Wangberg (2014) använde i sin studie. De använde sig av en laptop med Kali Linux i en virtuell miljö tillsammans med en äldre D-Link-router som rapporterats sårbar för den säkerhetsbrist Viehböck (2011) presenterat.

Varje mätning avgränsas genom att varje attack kommer avbrytas efter att 100 st PIN-nycklar testats. Totalt kommer 25 mätningar per verktyg utföras. Dessa avgränsningar bygger på den begränsade tillgången av tid inom studiens ramar.

Till skillnad från Bully utför Reaver brute-forceattack med en fördefinierad väntetid på 1 sekund som gör attacken långsammare. Denna väntetid kan dock kopplas bort genom att använda inställningen `-d 0` vid exekvering av Reaver (Tactical Network Solutions, 2011). Om funktionen inte kopplas bort vid mätning kommer Reaver inte utföra sin attack med maximal hastighet, vilket är det värde som ska jämföras mot Bullys respektive.

Både Reaver och Bully kan exekveras med inställningar som medvetet begränsar hastigheten vid en attack för att motverka aktivering av eventuella skyddsmekanismer i trådlösa routrar. I denna undersökning används inte dessa inställningar vid attack, eftersom det är den maximalt möjliga attackhastigheten som ska undersökas.

Utförande av detta experiment innebär tekniska processer som berör nätverk och säkerhet. Denna studie har med avsikt utformats och beskrivits för yrkesverksamma personer inom IT-säkerhet eller med motsvarande kompetensnivå för nätverksutrusning och hantering av Linux. Därför kommer instruktioner om hantering av laborationsutrustning inte beskrivas djupgående utan lämnas som specifikation i Appendix A och Appendix B.

4.5 Förväntat resultat

Resultat av studiens frågeställning förväntas enligt fyra möjliga scenarier.

1. Verktygen Reaver och Bully presterar likvärdigt i det omfång där högsta och/eller lägsta mätresultat från ett av verktygen i huvudsak motsvarar värden från andra det verktyget.

2. Reaver utför alla mätningar (högsta och lägsta värde) snabbare än Bullys.

3. Bully utför alla mätningar (högsta och lägsta värde) snabbare än Reavers.

4. Resultatet hos ett eller båda verktygen kan inte påvisa tillräcklig presenterbar data på grund av eventuella problem och oförutsedda händelser vid experimentets utförande, som exempelvis störningar i laborationsmiljön eller fel i hård-och mjukvara.

5. Metod

Andersen (1994) beskriver två generella ansatser inom vetenskapliga undersökningar kallade kvalitativ och kvantitativ metodik. Kvalitativ metodik syftar till att tolka och förstå resultat som framkommer av forskning. Andersen (1994) menar även på att denna metodform lämpar sig väl för undersökningar inom analys och samhällsvetenskap. Andersen (1994) beskriver, förutom kvalitativ och kvantitativ metodik, ansatsen litteraturstudie som kan studera och jämföra tidigare forskning. På grund av den bristande dokumentationen kring Reaver och Bully hade en litteraturstudie troligtvis inte kunnat besvara frågeställningen i denna studie.

Holme (1991) beskriver kvantitativ metodik som att kunna rikta sig till att bestämma frekvens av ett fenomen eller en egenskap, vilket kan vara ett eller flera fasta värden. Denna studie efterfrågar fasta värden istället för kvalitativa data som förmedlar mening. Därför lämpar sig en kvantitativ metod för denna studie.

5.1 Experimentell design

Utförande av detta experiment kräver grundläggande kunskap kring hantering av Linux i terminal, konfiguration av router, virtuella klienter och nätverkskort. Information kring användande av Bully och Reaver finns i dokumentation för respektive verktyg (Purcell, 2013; Tactical Network Solutions, 2011).

I detta experiment ska effektivitet undersökas hos Reaver och Bully. Effektivitet i detta sammanhang innebär hastighet vid brute-forceattack och kommer undersökas genom att mäta hur lång tid det tar för respektive verktyg att testa ett fast antal PIN-nycklar. De båda säkerhetsverktygen Reaver och Bully kommer att appliceras i en laborationsmiljö där WPS-sårbarheten finns tillgänglig. Vid laborationen kommer följande komponenter användas:

- En virtuell klientdator i VMware med operativsystem Kali Linux och ett trådlöst direktanslutet nätverkskort av modell ALFA AWUS036H. Då versionerna av Reaver (1.4) och Bully (1.0-22) är förinstallerade i Kali Linux (version 1.1.0a) kommer dessa att användas vid mätning. Se Appendix A för hård- och mjukvarudetaljer.

- En trådlös internet-router av modell *BELKIN F7D4302 v1* med original-firmware (v1.00.28) konfigurerad som en ”Infrastruktur”-nätverkstyp med WPA2-PSK och WPS-säkerhet aktiverad. Se Appendix B för detaljerad konfiguration.

5.1.1 Utförande

Vid mätning startas attack och tidtagning samtidigt. Varje attack och tidtagning stannas när 100 PIN-nycklar har provats. Därefter utförs nästa mätning med respektive mätkonfiguration. Endast ett verktyg mäts åt gången och varje verktyg mäts totalt 25 gånger. Tidsenhet i mätningar avrundas uppåt till hela sekunder. En attack mot WPS kan innebära maximalt test av 11’000 PIN-nycklar (Viehböck, 2011).

Vid varje mätning dokumenteras:

- Total tid från start till slut av 100 testade PIN-nycklar.
- Eventuella störningar och avbrott.

Ett medelvärde och median kommer därefter räknas ut efter de värden som mätningarna påvisar hos varje verktyg. Detta medelvärde kommer visa ett snitt på hur lång tid det tar för respektive verktyg att testa 100 PIN-nycklar. Om en mätning inte kan slutföras kommer den klassificeras som defekt. En defekt mätning kan exempelvis bero på faktorer som störningar eller oanade problem.

5.2 Reliabilitet

Bryman (2011) menar att ett flertal mätningar ökar undersökningars reliabilitet. Därför måste flera mätningar utföras för att minska potentiella avvikelser orsakade av störningar eller övriga påverkande faktorer. Båda verktyg kommer utföra sina attacker i så liknande miljö som möjligt. För att undvika kamp om resurser hos både klient och router utförs endast mätning av ett verktyg åt gången.

Enligt Coleman och Westcott (2012) kan prestandamätningar i trådlösa nätverk påverkas av potentiella störningar från andra nätverk. Enligt deras rekommendation bör en omgivning undersökas innan mätning efter närliggande trådlösa nätverk. Testutrustningen bör konfigureras på en trådlös frekvens (kanal) som inte belastar många radiovågor och potentiell överlappning av övrig trådlös trafik. En trådlös avsökning via Airodump-ng kan utföras för att undersöka vilka kanaler som trådlösa nätverk i omgivningen arbetar på. Testutrustrustningen kan därefter konfigureras till att använda den minst upptagna kanalen för att undvika potentiella störningar från de övriga trådlösa enheterna i omgivningen (Cache et al., 2010).

Båda verktygen utför enligt standard sina brute-forceattacker i slumpmässig ordning, vilket medför att den totala attacktiden kan variera beroende på vilken nyckel som slumpas fram. Detta innebär att en attack kan avslutas om rätt nyckel slumpmässigt gissas fram innan en mätning är slutförd. För att minska risken för detta problem kommer mätningar ske på ett begränsat antal PIN-nycklar.

Mätningarna utförs mot routern BELKIN F7D4302 v1 som har original-firmware. Enligt kalkylarket publicerat av Xiaopan (2013) har vissa påverkade router-modeller uppdaterats med skydd i nyare firmware-versioner. Juhlin och Wangberg (2014) beskriver att en attack kan försvåras och eventuellt oskadliggöras om en router uppdaterats med firmware-version innehållande skydd mot WPS. I denna studie har original-firmware i routern bevarats för att eventuella skyddsmekanismer inte ska kunna påverka mätningarnas resultat.

5.3 Validitet och validitetshot

Enligt Wohlin et al. (2012) är validiteten hos ett forskningsresultat en grundläggande fråga. Validitet handlar om huruvida en studie undersöker det den säger sig undersöka. Det finns olika former av validitet:

Intern validitet handlar om trovärdigheten i en studie, om rätt mätinstrument har använts vid rätt tillfälle. I denna studie kan mätningar vid olika tidpunkter påverkas av en omgivning som ändras med tiden. Alla mätningar utföras vid samma tillfälle för att motverka eventuella ändringar som kan ske i laborationsmiljön och minimera denna typ av validitetshot. För att bland annat uppnå en hög intern validitet kommer en testattack utföras innan mätning (Wohlin et al., 2012).

Extern validitet handlar om i vilken omfattning det går att generalisera resultat av en studie. Att förhålla sig till extern validitet är viktigt vid tolkning av studiers resultat eftersom generaliserbarheten kan variera mellan olika studier (Wohlin et al., 2012). I denna studie kommer 25 mätningar att utföras. Ju fler mätningar som utförs, desto mer ökar möjligheten att generalisera utifrån resultatet. Ett lägre antal mätningar ökar hotet mot den externa validiteten.

Validitet i Konstruktion avser förhållandet mellan konstruktion av ett experiment och dess utfall. Problem med denna validitet berör huruvida ett resultat påverkas av en studies tillvägagångssätt och designval. Val av tillvägagångsätt för en undersökning bör planeras och utvärderas innan applicering. Ett hot mot denna validitet kan vara att ett experiment kan ge olika resultat beroende på hur experimentet är konstruerat. Hotet *Inadequate Preoperational Explication of Constructs* innebär att beskrivningen av undersökningens metod och konstruktion eventuellt är otydlig. Att upprepa ett experiment efter en otydlig beskrivning öppnar upp för risken av annorlunda tolkning för hur experimentet ska utföras (Wohlin et al., 2012).

Med hänsyn till detta hot har ambitionen i denna studie varit att försöka beskriva den experimentella designen så tydligt och ingående som möjligt, dock kvarstår alltid en risk för eventuell feltolkning av andra läsare. Ett sätt att försöka minska detta hot är presentation av kommandon om hur verktygen exekveras tillsammans med grafiska figurer som visar dess resultat. Jämförelse med dessa figurer kan indikera om annorlunda utfall presenteras. Ett sådant utfall tyder på att någon faktor i experimentet skiljer från denna studie.

Ett annat nämnvärt hot mot validiteten i konstruktion är *Mono-method bias*. För ett experiment som endast utförs i en specifik miljö, vid ett visst tillfälle och vid en viss plats, med specifika mjuk- och hårdvaror etc. finns det en risk att resultatet kan bli missvisande eller snedvridet. Detta eftersom bredden av alla scenarier eller alternativ inte undersökts.

I denna studie har designval, som val av virtuell dator istället för fysisk, gjorts för att arbeta med en fördefinierad virtuell hårdvaruspecifikation. Denna specifikation kan därmed återskapas utan vidare konfiguration för att ge liknande prestanda på en annan hårdvara och minskar risken för större prestandaskillnader hos en värddator. Denna studie kommer inte kunna visa resultat från många olika scenarier eftersom endast ett specifikt scenario kommer undersökas. Ett tillvägagångsätt att minska detta hot mot validiteten hade varit att utföra experimentet utifrån flera variationer av de ovan nämnda faktorerna.

Validitet i slutsatser handlar om problem med att dra korrekta slutsatser utifrån relationen mellan utförande och utfall i ett experiment. Ett sådant hot är *Low statistical power*. Kraften i en statistisk undersökning är dess förmåga att visa ett sant mönster i den insamlade datan. Om denna kraft är låg finns en hög risk att en felaktig slutsats dras (Wohlin et al., 2012). I denna studie kommer 25 mätningar utföras per verktyg. Valet av antal mätningar baseras på bedömningen att den summan kan ge en tillräckligt hög statistisk kraft att kunna dra meningsfulla slutsatser ifrån. Utförande av ett högre antal mätningar hade dock påvisat ännu ett starkare statistiskt resultat och gett högre validitet.

Fishing and the error rate. Enligt Wohlin et al. (2012) är det ett hot mot validitet att söka efter specifika resultat. Det kan resultera i att en analys inte längre blir självständig. Forskaren kan påverka resultatet genom att leta efter ett specifikt utfall. I denna studie kommer experimentet att genomföras med medvetenhet om detta hot. Laborationen kommer utformas så att båda verktyg exekveras under så lika förhållanden som möjligt. Objektivitet kommer eftersträvas genom alla steg i studien.

Ovannämnda validitetshot har beskrivits utifrån deras relevans till studien. Cook och Campbell (1979) har sammanställt en lista som beskriver övriga validitetshot. Se Appendix C för en komplett lista.

6. Genomförande

I detta kapitel presenteras utförandet av undersökningen. En inledande förberedelse av hård- och mjukvara utförs följt av en testattack för verifiering av sårbarheten som Viehböck (2011) presenterat. Efter lyckad testattack utförs mätningarna.

6.1 Förberedelse inför mätningar

För att förbereda routern inför mätningarna återställs den först till fabriksinställningar. Därefter, genom att ansluta en klient till routerns webbgränssnitt, konfigureras ett nytt nätverksnamn (SSID) till ”TestWIFI” och en WPA2-PSK nyckel till ”SecretPassword!”. Funktionen ”WPS via PIN-kod” kan i gränssnittet avaktiveras, men lämnas aktiv till attacken. En ny slumpmässig PIN-kod (11710905) genereras för att bevara integritet hos routern. Den nya konfigurationen sparas och routern startas om (Se Appendix B). För att verifiera inställningarna i den nya konfigurationen testansluts en iPhone 6 till routern via Wi-Fi med den nyangivna WPA2-nyckeln. Routern accepterade anslutningen och därmed validerades den nya konfigurationen positivt.

Kali Linux startas virtuellt i en VMware-miljö och förbereds för attack genom att det trådlösa nätverkskortet ansluts till klienten. Därefter exekveras följande kommando via en terminal för att Kali ska kunna avlyssna närliggande trådlösa nätverk:

```
$ airmon-ng start wlan0
```

Genom exekvering av ovanstående kommando skapar Kali Linux ett nytt virtuellt nätverksinterface kallat “mon0”, där det trådlösa nätverketskortet aktiveras i ett övervakningsläge. Denna process krävs för avlyssnande av data och för utförande av trådlösa attacker (Aircrack, 2011).

6.1.1 Avsökning

Innan mätningarna kan utföras måste routern verifieras sårbar mot WPS via en testattack. Kali Linux måste först hitta och verifiera den trådlösa routern som tillgänglig i sin omgivning. För detta används verktyget airodump-ng som kan söka efter tillgängliga trådlösa nätverk via följande kommando:

```
$ airodump-ng start mon0
```

Figur 4 Airodump avlyssnar omgivning efter trådlösa nätverket.

Airodump-ng identifierar då alla tillgängliga trådlösa nätverk i närheten. I detta fall hittas endast laborationens router ”TestWIFI” (Se Figur 4) vilket innebär att potentiella störningar från närliggande trådlösa nätverk inte behöver åtgärdas. Av den information som presenteras via airodump-ng dokumenteras routerns MAC-adress (BSSID), som senare kommer användas som identifierare i exekvering av Reaver och Bully.

6.1.2 Testattack med Reaver

En testattack med Reaver exekveras mot routern, med dess MAC-adress som identifierare, och med nätverksinterface angivet som mon0 via följande kommando:

```
$ reaver -i mon0 -b 94:44:52:DC:XX:XX -v
```

Figur 5 Reaver utför brute-forceattack.

Reaver tillåts arbeta mot målet att helt slutföra sin attack och avbryts inte manuellt. Under attacken visar Reaver vilka nycklar som testats (Se Figur 5) i konsolen och en angripare kan manuellt avläsa attackhastigheten i realtid utan större svårigheter. Efter var femte testad nyckel skriver Reaver ut medelhastighet för de fem senaste nycklarna. Under testattacken visar sig medelhastigheten stabil runt 2,51 sekunder per nyckel och varierar inte mer än ett tiotal hundradelar mellan var femte nyckel. Några timmar efter attacken påbörjats var hela WPS-nyckeln funnen. Reaver efterfrågade då routerns WPA2-PSK-nyckel som skrevs ut i klartext innan verktyget avslutades (Se Figur 6). Testattacken var därmed avslutad och routern verifierades sårbar av WPS-protokollet.

Figur 6 Lyckad attack med Reaver där WPS-PIN är funnen.

6.2 Mätningar

Efter att sårbarheten verifierats i routern utfördes de faktiska mätningarna. Vid varje mätning startas respektive verktyg samtidigt som en tidtagning. Varje attack avslutas manuellt efter att det aktiva verktyget testat 100 PIN-nycklar. Värden från alla mätningar dokumenteras, varav de eventuella defekta mätningar som saknar giltigt värde dokumenteras som N/A.

För mätning exekveras följande kommando för respektive verktyg:

Reaver: `$ reaver -i mon0 -b 94:44:52:DC:XX:XX -v -d 0`

Bully: `$ bully -b 94:44:52:DC:XX:XX mon0`

När 25 mätningar utförts med respektive verktyg anses laborationen som avslutad. Routern återställs till den ursprungliga konfigurationen och utrustningen stängs av.

7. Analys

Resultat av undersökningen presenteras i Tabell 1.

Mätning	Bully	Reaver	Kommentar
1	104	122	
2	**N/A**	126	Bully Defekt
3	106	133	
4	99	125	
5	105	129	
6	100	126	
7	102	125	
8	107	128	
9	**N/A**	123	Bully Defekt
10	101	131	
11	98	122	
12	**N/A**	130	Bully Defekt
13	102	124	
14	107	132	
15	100	126	
16	106	127	
17	104	122	
18	**N/A**	123	Bully Defekt
19	106	131	
20	108	130	
21	100	124	
22	102	129	
23	99	122	
24	100	126	
25	106	121	

Tabell 1 Resultat av mätningar i följden de utfördes.

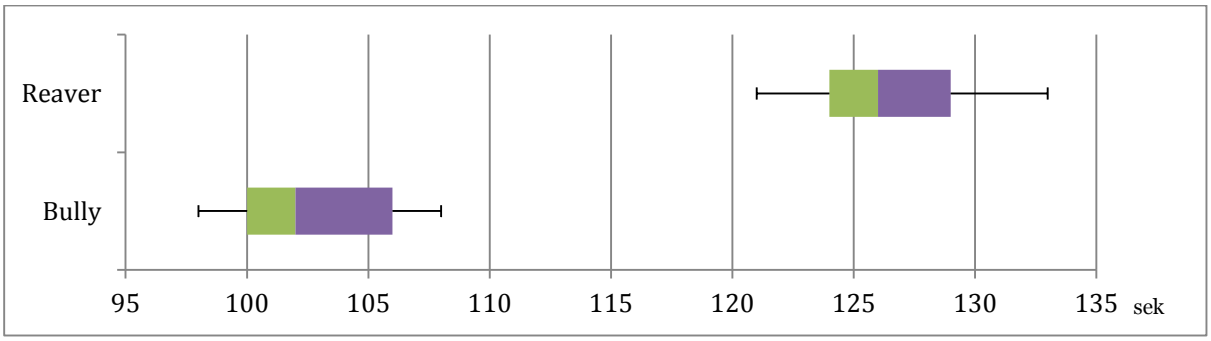
Alla mätningar med Reaver slutfördes utan problem och en tid för attack av 100 PIN-nycklar dokumenterades. Vid mätning 2, 9, 12 och 18 med Bully skedde timeouts där routern låste sig och slutade svara. Dessa fyra mätningar kunde inte slutföras, de avbröts och klassificerades som defekta. Eftersom tidsvärden inte kunde registreras på dessa defekta mätningar saknar de värden i tabellen (Se Tabell 1). Efter varje defekt mätning i experimentet startades routern om för att återställa låsningen och återstående mätningar återupptogs.

I resultatet visade det sig att alla attacker som utfördes med Reaver tog mellan 121 till 133 sekunder att slutföra. Bully utförde motsvarande attacker på tider mellan 99 till 108 sekunder (Se Tabell 1).

För att sammanställa resultaten kan de värden som uppmätts för respektive verktyg summeras i medelvärde och median. Vid uträknande av medelvärde adderas värdena i mätningarna från respektive verktyg samman och divideras på antal mätningar som utförts. Eftersom defekta mätningar saknar uppmätt tidsvärde sätts tidsvärdet till noll vid uträkning av medelvärde. Bortfallen hanteras genom att medelvärdet för Bully räknas på de 21 attacker som har ett uppmätt tidsvärde.

Medelvärde för Reaver: $\frac{\begin{pmatrix}122+126+133+125+129+\\126+125+128+123+131+\\122+130+124+132+126+\\127+122+123+131+130+\\124+129+122+126+121\end{pmatrix}}{25} = \mathbf{126,28}$ sek/100 PINs

Medelvärde för Bully: $\frac{\begin{pmatrix}104+0+106+99+105+\\100+102+107+0+101+\\98+0+102+107+100+\\106+104+0+106+108+\\100+102+99+100+106\end{pmatrix}}{(25-1-1-1-1)} = \mathbf{102,95}$ sek/100 PINs



Figur 7 Tidsåtgång för 100 testade nycklar visat i ett lådagram.

Resultatet har sammanställts i ett lådagram som visar en sammanställning av de utförda mätningarna (Se Figur 7). Bully utförde sina brute-forceattacker snabbast på en medeltid av 102,95 sekunder per 100 PIN-nycklar. Reaver utförde sina attacker på en högre medeltid av 126,28 sekunder per 100 PIN-nycklar. De båda medelvärdena påvisar, tillsammans med de individuella mätningarna, att Bully utför brute-forceattack i högre hastighet jämfört med Reaver. Dock kunde endast 84 % av mätningarna med Bully slutföras då de defekta mätningarna resulterade i att routern slutade svara.

7.1 Jämförelse med förstudier

Aked et al. (2012) beskriver vikten av firmware-version hos routrar i sin studie. De betonar skillnader mellan hur original- och uppdaterad firmware påverkar en attackerare. För många trådlösa routrar med WPS, som tillverkats och sålts innan Viehböcks (2011) publicerande, saknas skyddsmekanismer som motverkar attack. Detta problem har dock ett flertal tillverkare åtgärdat genom att publicera nedladdningsbara firmware-uppdateringar för sina router-modeller som blockerar WPS-attack (Xiaopan, 2013). Till följd av detta beaktades vikten av att använda original-firmware i denna laborationens router, så att studiens mätningar inte skulle riskera att påverkas av eventuella skyddsmekanismer i nyare firmware.

Juhlin och Wangberg (2014) bekräftar problematiken för en attackerare gällande uppdaterade firmwares som Aked et al. (2012) beskriver. De menar på att de förekommande skydd som kan implementeras via firmware innebär begränsningar på antal PIN-nycklar som kan testas per minut. Om en sådan begräsning överstigs, som vid en brute-forceattack, kan en router neka WPS-autentisering under en kortare period. I denna studie hade mätningarna med Reaver och Bully påverkats negativt av en sådan skyddsmekanism.

Till skillnad från tidigare förstudier används, förutom Reaver, även verktyget Bully i denna studie i attack mot WPS. Brist på tidigare förstudier kring Bully kan bero på att verktyget utvecklades och publicerades 2013, vilket är relativt nyligen.

8. Diskussion

I detta kapitel följer diskussion kring denna studies undersökning, reflektioner kring den beprövade sårbarheten i WPS samt generella reflektioner kring IT-säkerhet. Denna undersökning riktar sig främst till intressenter av säkerhet inom trådlösa nätverk. Resultatet som visar att Bully har en högre attackhastighet än Reaver kan vara en bidragande faktor i valet av vilket verktyg som bör användas vid attack. Val av verktyg påverkar enligt denna undersökning tidskostnaden för slutförd attack, vilket för en attackerare vill hållas minimal.

8.1 Metoddiskussion

I denna undersökning användes en kvantitativ metod för att utföra ett experiment. Detta visade sig ge ett mätbart resultat som kan användas för att besvara studiens frågeställning. I studiens förväntade resultat nämns fyra olika scenarier (Se kapitel 4.4). Av dessa visade sig det tredje nämnda scenariot överensstämma med studiens resultat; att Bully utför alla mätningar (högsta och lägsta värde) snabbare än Reaver.

8.1.1 Undersökning

Valet att använda en virtuell avbild av Kali Linux grundas på det minskade behovet av installationer, utbudet av förinstallerade mjukvaruverktyg och dess fördefinierade hårdvaruinställningar för optimal stabilitet. För denna undersökning innebär dessa faktorer optimala förhållanden för lyckade mätningar med Reaver och Bully. En hypotes är att mer prestandarik hårdvara, än den som användes i laborationen, kunde gett annorlunda mätresultat. Troligen hade dock skillnaden mellan verktygen inte påverkats nämnvärt.

Vid varje attack mättes tiden för test av 100 PIN-nycklar. Motivering till detta antal är dels bedömningen att det utgjorde ett rimligt antal PIN-nycklar att testa, utifrån undersökningens omfattning och syfte, men även för att minska risken av lyckad attack innan 100-nycklar kunnat testas. Förutom att verifiera sårbarheten med WPS kunde testattacken även användas för att undersöka om attackformen skalar linjärt med avseende på prestanda. Under den inledande testattacken visade sig medelhastigheten stabil runt 2,51 sekunder per nyckel och varierade inte mer än ett tiotal hundradelar mellan var femte nyckel. Om mätning utförts med annat antal PIN-nycklar, som 50 eller 200 stycken, hade godkända mätningar troligtvis påvisat liknande resultat eftersom testattacken hade en stabil attackhastighet från start till slut. Det är oklart exakt hur många nycklar som testades, eftersom det inte ingick i studiens syfte att undersöka exakt antal nycklar vid den inledande testattacken. Då attacken pågick i flera timmar kan det förutsättas att attacken testade över 3 000 nycklar.

Om den internet-router som användes vid mätning haft felaktig dokumentation gällande dess brist, hade det äventyrat möjligheten att få fram mätbara resultat. Därför användes den inledande testattacken med Reaver, i enlighet med Juhlin och Wangbergs (2014) studie, för att påvisa sårbarheten som aktiv hos routern innan mätning. Om testattacken resulterat negativt, där den inte kunnat slutföras, hade routern varit tvungen att bytas mot en annan router med dokumenterad sårbarhet hos WPS-protokollet.

8.1.2 Validitet

Hot mot validitet har tidigare beskrivits i denna studie (Se Kapitel 5.3). Dessa hot kan efter studiens genomförande diskuteras gentemot resultatet.

25 brute-forceattacker var utfördes av Bully och Reaver. För Bully slutfördes endast 84 % av mätningarna med ett dokumenterbart värde. Alla de slutförda mätningarna var dock snabbare än samtliga mätningar för Reaver, vilket talar för att Bully kan utföra en brute-forceattack med högre hastighet än Reaver. Den externa validiteten hade kunnat ökas genom ett högre antal mätningar. Ett högre antal mätningar hade också minskat hotet av *Low statistical power*. Tillgång av tid för denna studie begränsade möjligheterna att utföra fler mätningar. Genomförande av mätningar, med varierad mängd på antal PIN-nycklar att testa, hade dessutom kunnat påvisa ett bättre grundat resultat. Detta hade också kunnat motverka hotet *Mono-method bias*. Bedömningen är ändå att resultatet är generaliserbart i en viss mån då kraften i den statistiska undersökningen är relativt hög.

I det förväntade resultatet benämns de fyra möjliga scenarierna som troligen kunnat uppkomma. Vid motverkan av validitetshotet *Fishing and the error rate* bör inte förväntat resultat endast handla om de värden som önskas uppnås, som i detta fall mätvärden i alla mätningar. Det fjärde och sista sceneriet talar därför för en avvikelse där mätresultat från Reaver eller Bully inte kan uppnås.

8.2 Reflektioner

Då Viehböck (2011) visat på brister i WPS-protokollet rekommenderar Aked et al. (2012), Juhlin och Wangberg (2014) samt jag själv minimal användning av protokollet. Administratörer och ägare av routrar/accesspunkter bör verifiera tillgänglighet av eventuell WPS-funktionalitet med PIN-nyckel och, om möjligt, inaktivera denna funktion för att motverka framtida attacker.

Coleman och Westcott (2012) rekommenderar ägare att applicera kryptering på privata trådlösa nätverk med WPA2 (AES-kryptering). Om denna säkerhet inte finns tillgänglig hos en trådlös router kan den vara utsatt för risk vid potentiella attacker. Om WPA2 med AES-kryptering inte finns tillgänglig rekommenderar Coleman och Westcott (2012) användandet av den bästa tillgängliga krypteringen av säkerheten framför ingen alls. Även om en sämre kryptering kan forceras lättare innebär all kryptering en förhöjd säkerhet i jämförelse med ingen alls.

8.2.1 Etiska aspekter

Då IT-säkerhet berör parter med olika avsikter kan denna studies samhällspåverkan diskuteras. Information om attack av WPS-sårbarheten kan utnyttjas på olika sätt av olika intressenter. För yrkesverksamma IT-anställda, likt systemadministratörer och säkerhetskonsulter, kan denna information användas för att förhindra skada vid oönskade attacker. Informationen kan även användas av forskning och framtida studier för utveckling av högre säkerhet inom området trådlösa nätverk.

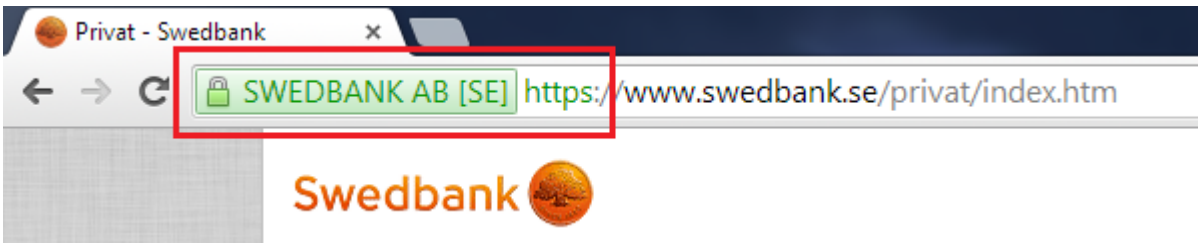
Informationen om WPS-sårbarheten och resultatet i denna studie kan också användas av en intressent i kriminella syften som kan orsaka skada för en person eller verksamhet. Olaga intrång via WPS skulle kunna innebära negativa följder, till exempel kränkning eller stöld av information. Intressenter uppmanas inte att använda denna studies bakgrund, metod eller resultat för olaga syfte.

8.2.2 IT-säkerhet i samhället

Säkerhet är ett område som inte bara berör trådlösa nätverk. Media, företag och organisationer varnar ständigt för olika hot, risker och sårbarheter som berör användandet av IT-utrustning, framförallt vid anslutning mot Internet (Microsoft, 2012). En större del av Sveriges befolkning använder internet dagligen till vardagssysslor som att söka information, besöka sociala nätverk, utföra bankärenden, näthandel och hantering av e-post. För många olika e-tjänster som används på internet rekommenderas, och ibland krävs, en viss grad av säkerhet med olika säkerhetslösningar för att förhindra negativa påföljder (Findahl, 2013).

Säkerhetslösningar som anti-virus, brandväggar och olika krypteringstjänster kommer ofta på tal när datorsäkerhet generellt diskuteras. Anledningen till detta är de stora skador som kan uppstå vid fallerande av dessa säkerhetsmodeller.

WPS-protokollet tillhör de säkerhetslösningar som ibland måste hanteras manuellt. Det finns dock flera vanligt förekommande säkerhetslösningar som automatiskt appliceras när de finns tillgängliga. Ett exempel på en sådan säkerhetslöning är kryptering via Secure Sockets Layer (SSL) som motverkar bl.a. avlyssnings- och fiskeattacker. Hemsidor som hanterar känslig data och information har ofta SSL-kryptering aktiverad för att skydda trafiken mellan dess webbserver och besökare (Trustwave, 2010). Moderna webbläsare kan påvisa information till en användare om en hemsida är skyddad eller inte. SSL-kryptering kan verifiera hemsidans certifierade ägare samt om en surfsession är intakt och krypterad (Se Figur 8). Om en trådlös router faller offer för en olaga WPS-attack kan automatiska säkerhetsfunktioner, som SSL-kryptering, skydda routerns användare mot diverse fiskeattacker och informationsstölder.



Figur 8 Krypterad SSL-Session mot www.swedbank.se

SSL är bara en av många tillgängliga säkerhetsfunktioner som illustrerar användning av automatiserad säkerhet. Tack vare automatiserad aktivering av SSL minskas behovet av kunskap gällande säkerhet hos en slutanvändare då säkerhetsmekanismen redan är applicerad och aktiv. Dock betyder det inte att all teknik som används mot internet är säkrad per automatik. En strävan för total automatiserad säkerhet hos slutanvändare kan i många fall vara önskvärd och kan dessutom ses som ett mål inom administration av säkerhet (Limoncelli et al., 2007).

8.3 Stabilitet i mätning

I denna studies resultat visas fyra av 25 defekta mätningar med Bully då routern slutade svara. Då problemet inte adresseras i tillverkarens manual om routern, och det saknas dokumentation för Bully gällande prestanda, är det svårt att avgöra vad dessa defekta mätningar beror på.

En hypotes om de defekta mätningarna relaterar till den höga effekten i brute-forceattack som Bully innehar. Vid en överbelastningsattack (DDOS) klarar inte ett attackoffer av den höga frekvensen med förfrågningar och kan eventuellt låsa sig. Likhet med detta fenomen kan finnas i denna situation. Vid brute-forceattack mot WPS kan en för hög hastighet orsaka överbelastning hos en router till den grad att den inte kan hantera alla förfrågningar och hänger sig.

Denna studies resultat visar att lyckade attacker med Bully är mer tidseffektiva jämfört med Reaver, tack vare dess högre attackhastighet. Dock kan en attack med Bully misslyckas då den högre hastigheten kan orsaka en överbelastning. Vid sådana fall blir verktyget ineffektivt. Ett verktyg som attackerar i lägre hastighet kan komma att arbeta mer stabilt och eventuellt gynna attackens tidsvinst i helhet.

Enligt Tactical Network Solution (2011) använder Reaver som standard en mycket lägre attackhastighet jämfört med Bully. Det framgår inte i Reavers dokumentation varför dess attackhastighet har utökats med en sekunds väntetid, men en hypotes är att verktyget utvecklats med hastighetsbegräsningen i syfte att upprätthålla en högre stabilitet. Purcell (2013) menar att Bully är mer prestanda-optimerat än Reaver. Det kan vara en avgörande anledning till dess högre attackhastighet, även när Reaver exekveras utan begräsning. Denna studie kan inte påvisa om hastighetsskillnaden mellan de båda verktygen endast beror på Bullys påstådda optimering.

Både Reaver och Bully har utvecklats med exekveringsalternativ för att utföra en brute-forceattack med en lägre manuellt angiven hastighet än den som är standard. Om en WPS-attack mot en router låser sig på grund av överbelastning kan en lägre hastighet testas vid attack för ett eventuellt bättre resultat. En fördel med en angiven lägre hastighet kan vara ökad stabilitet vid attack. En nackdel för attackerare kan vara att en attack med lägre hastighet kräver längre tid att slutföra, vilket kan innebära ineffektivitet till den grad att en attack avbryts eller bedöms som inte värd att utföra.

9. Slutsats

Syftet med denna studie var att undersöka hastighetsskillnad mellan verktygen Reaver och Bully vid brute-forceattack mot WPS. Frågeställningen var vilken skillnad i hastighet som kunde ses mellan verktygen Reaver och Bully i en brute-forceattack av 100 PIN-nycklar mot en trådlös internet-router utan skyddsmekanismer för WPS.

Sårbarheten kring WPS som Viehböck (2011) publicerat har återskapats i en laborationsmiljö och verifierats som aktiv. Mätningar med de båda verktygen Reaver och Bully har utförts via brute-forceattacker och dess hastighet har dokumenterats.

Inom studiens avgränsningar och förutsättningar genomförde Bully attacker mot 100 PIN-nycklar på en medeltid av 102,95 sekunder, jämfört med Reaver som utför motsvarande attacker på en medeltid av 126,28 sekunder. Detta innebär att Bully har en högre attackhastighet i jämförelse med Reaver i denna studie. Den ökade hastigheten behöver dock inte innebära en tidsvinst vid en hel attack eftersom det finns en hypotes om att den höga attackhastigheten orsakar stabilitetsproblem hos attackoffret. Denna hypotes har påvisats, genom fyra defekta mätningar, av totalt 25 utförda.

9.1 Framtida studier

Det finns fortfarande många outforskade områden kring WPS-sårbarheten, Reaver, Bully och övriga potentiella verktyg mot denna sårbarhet. Denna studie jämförde attackhastighet mellan verktygen Reaver och Bully utan manuellt angiven lägre hastighet där faktorer som relaterar till prestanda och stabilitet inte undersökts.

En rekommenderad framtida undersökning skulle därför kunna vara en stabilitetsjämförelse mellan dessa verktyg. Som diskussionen i denna studie nämner behöver en högre hastighet inte innebära en snabbare attack om stabilitet vid attack fallerar. Undersökningar kring Bullys höga attackhastighet i relation till stabilitetsproblem är därför ett intressant framtida forskningsområde.

Referenser

ABIresearch (2013). Growing Demand for Mobility will Boost Global Wi-Fi Hotspots to Reach 6.3 Million in 2013. Tillgänglig på Internet: https://www.abiresearch.com/press/growing-demand-for-mobility-will-boost-global-wi-f [Hämtad: 2014-02.28].

Aircrack-ng Suite (2011). *aircrack-ng* (Version: 1.2 Beta 2) [Datorprogram]. Aircrack-ng. Tillgänglig på Internet: http:// http://www.aircrack-ng.org/ [Hämtad 2014-02-28].

Aked, S., Bolan, C. M. & Brand, M. W. (2012). A Proposed Method for Examining Wireless Device Vulnerability to Brute Force Attacks via WPS External Registrar PIN Authentication Design Vulnerability. Proceedings of International Conference on Security and Management. (pp. 691-694). CSREA Press, Las Vegas, Nevada, USA.

Andersen, H. (1994). Vetenskapsteori och metodlära – en introduktion, Studentlitteratur, Lund.

Bryman, A. (2011). Samhällsvetenskapliga metoder. Malmö: Liber.

Cache, J., Wright, J. & Liu, V. (2010). Hacking Exposed Wireless: Wireless Security Secrets & Colutions. 2 Edition. Mcgraw-Hill Osborne Media.

Cert (2011). Vulnerability Note VU#723755. Tillgänglig på Internet: http://www.kb.cert.org/vuls/id/723755 [Hämtad 2015-02-17].

Coleman, D. & Westcott, D. (2012). CWNA: Certified Wireless Network Administrator: Official study guide. 3rd edition. Sybex.

Cook, T.D., Campbell, D.T. (1979). Quasi-experimentation – Design and Analysis Issues for Field Settings. Houghton Mifflin Company, Boston

Findahl, O. (2013). Svenskarna och internet. Tillgänglig på Internet: https://www.iis.se/docs/SOI2013.pdf [Hämtad: 2014-03-08].

Holme, I. M. (1991). Forskningsmetodik: Om kvalitativa och kvantitativa metoder, Studentlitteratur, Lund.

Juhlin, T. & Wangberg, D. (2014). Bristfällig säkerhet inom trådlösa routrar med fokus på WPS. Institutionen för datavetenskap (DV), Linnéuniversitetet. Växjö, Kalmar.

Kali Linux Tools (2015). Kali Linux Tools Listening. Tillgänglig på Internet: http://tools.kali.org/tools-listing [Hämtad: 2015-02.22].

Limoncelli, T, A., Hogan, C, J. & Chalup, S, R. (2007). The Practice of System and Network Administration, Second Edition. 2 Edition. Addison-Wesley Professional.

McAfee (2014). Threat Activity. Tillgänglig på Internet: http://home.mcafee.com/virusinfo/threat-activity [Hämtad 2014-03.08].

McClure, S., Scambray, J., Kurtz, G. (2009). Hacking Exposed™ Network Security Secrets and Solutions, Sixth Edition. McGraw-Hill.

Microsoft (2012). Understanding security and safe computing. Tillgänglig på Internet: http://windows.microsoft.com/en-us/windows/understanding-security-safe-computing#1TC=windows-7 [Hämtad: 2014-03.08.].

National Vulnerability Database (2013). Vulnerability Summary for CVE-2011-5053. Tillgänglig på Internet: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-5053 [Hämtad: 2015-05-26].

Offensive Security (2015). Kali Linux Downloads. Tillgänglig på Internet: https://www.offensive-security.com/kali-linux-vmware-arm-image-download/ [Hämtad: 2015-02-22].

PCMag (2015). The 10 Best Wireless Routers 2015. Tillgänglig på Internet: http://www.pcmag.com/article2/0,2817,2398080,00.asp [Hämtad: 2015-06-12].

Purcell, B. (2013). *Bully* (Version 1.0-22) [Datorprogram]. Tillgänglig på internet: http://tools.kali.org/wireless-attacks/bully [Hämtad: 2015-02-22].

Radio Electronics (2015). IEEE 802.11 Wi-Fi Standards. Tillgänglig på Internet: http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php [Hämtad: 2015-04-13].

Reaver Systems (2014). Alfa 802.11 USB WiFi Adapter. Tillgänglig på internet: http://www.reaversystems.com [Hämtad: 2015-02-16].

Schneier, B. (1996). *Applied Cryptography - Second Edition*. John Wiley & Sons.

Tactical Network Solutions (2011). *reaver-wps* (Version 1.4) [Datorprogram]. Tillgänglig på Internet: https://code.google.com/p/reaver-wps/ [Hämtad: 2014-02-28].

TeliaSonera (2014). Pressmeddelande 2014-09-01. Tillgänglig på Internet: http://mb.cision.com/Main/1013/9636509/280926.pdf [Hämtad: 2015-02-25].

Trustwave (2010). How SSL Works. Tillgänglig på Internet: https://ssl.trustwave.com/support/support-how-ssl-works.php [Hämtad: 2014-03-08].

Viehböck, S. (2011). Brute forcing Wi-Fi Protected Setup. Tillgänglig på Internet: http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf [Hämtad: 2014-02-28].

Wi-Fi Alliance (2014). Wi-Fi Protected Setup. Tillgänglig på internet: http://www.wi-fi.org/discover-wi-fi/wi-fi-protected-setup [Hämtad: 2015-02-27].

Wohlin, C., Runeson, P., Höst, M., Ohlsson, C., Regnell, B. & Wesslén, A. (2012). Experimentation in software engineering. Springer, Berlin.

Xiaopan (2013). WPS Flaw Vulnerable Devices. Tillgänglig på internet: http://xiaopan.co/forums/attachments/wps-flaw-vulnerable-devices-xls.9/ [Hämtad: 2015-04-18].

Appendix A - Specifikation: Virtuell Dator

Hypervisor

Processor:	Intel Core i7 920 (2,67Ghz)
Internminne (RAM):	16 GB
USB-enheter:	ALFA USB WIFI AWUS036H
Hypervisor-mjukvara:	VMware Workstation
Version:	10.0

Virtuell klient

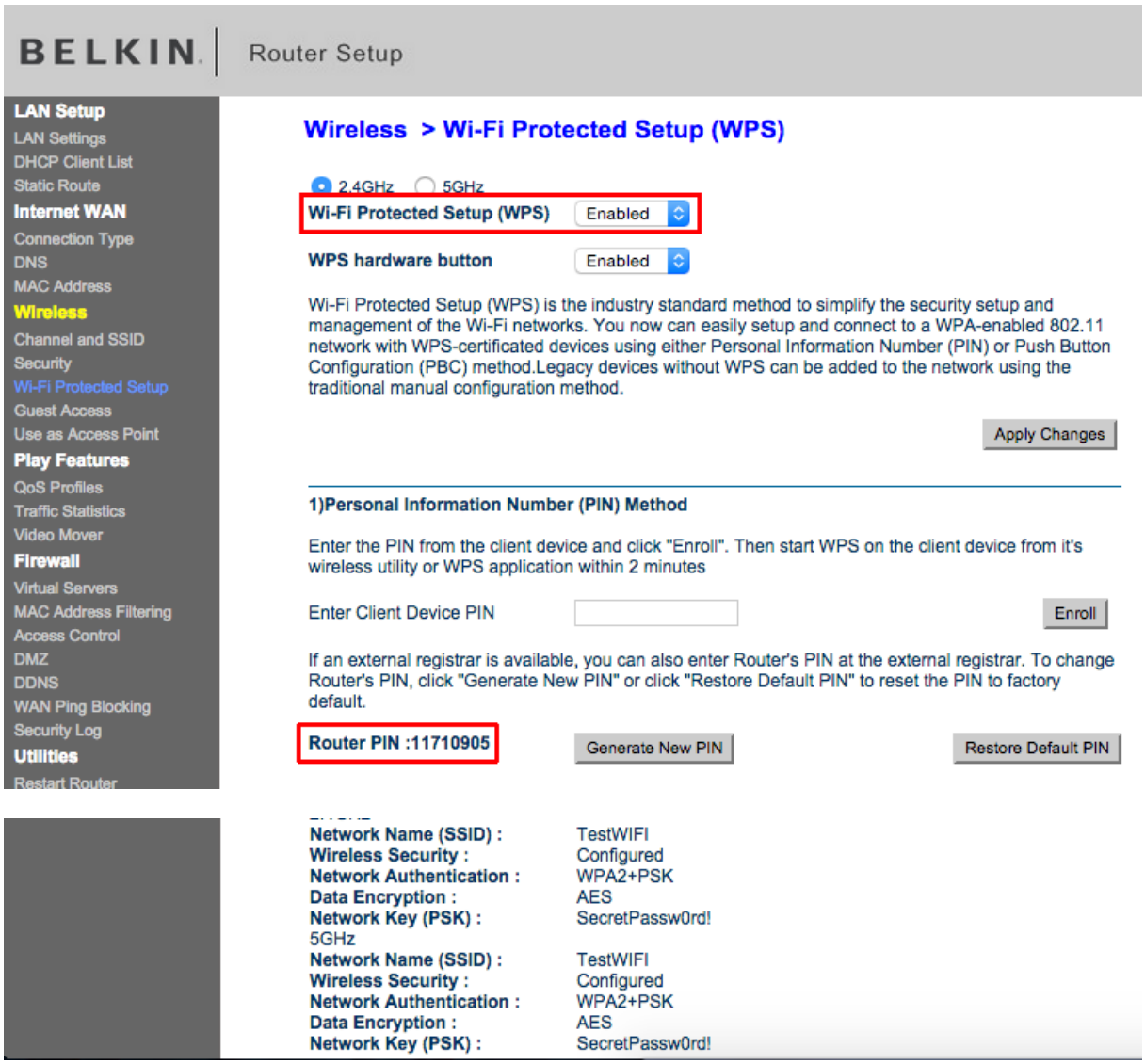
Operativsystem:	Kali Linux 64 bit 1.1.0a (Virtuell)	
Processor:	1 CPU, 1 Core	
Internminne (RAM):	2 GB	
Hårddisk:	30 GB	
Verktyg:	Reaver	Bully
	v1.4	v1.0-22

Appendix B - Konfiguration: Router

Konfiguration: Router

Version Info	
Hardware	F7D4302 v1
Firmware	1.00.28 (Dec 24 2010)
Boot Loader	0.07e
Serial No.	121043G4

LAN Settings	
LAN/WLAN MAC	94:44:52:DC:
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled (0 LAN, 1 WLAN Client)



Appendix C - Validitetshot

Hot mot validitet enligt Cook och Campbell (1979).

Conclusion validity	Internal validity
Low statistical power	History
Violated assumption of statistical tests	Maturation
Fishing and the error rate	Testing
Reliability of measures	Instrumentation
Reliability of treatment implementation	Statistical regression
Random irrelevancies in experimental setting	Selection
Random heterogeneity of subjects	Mortality
	Ambiguity about direction of causal influence
	Interactions with selection
	Diffusion of imitation of treatments
	Compensatory equalization of treatments
	Compensatory rivalry
	Resentful demoralization

Construct validity	External validity
Inadequate preoperational explication of constructs	Interaction of selection and treatment
Mono-operation bias	Interaction of setting and treatment
Mono-method bias	Interaction of history and treatment
Confounding constructs and levels of constructs	
Interaction of different treatments	
Interaction of testing and treatment	
Restricted generalizability across constructs	
Hypothesis guessing	
Evaluation apprehension	
Experimenter expectancies	