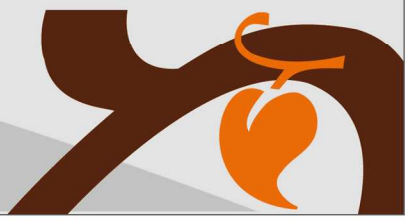
Högskolan på Gotland
Gotland University

Trådlösa nätverk
-säkerhet och GPU

Högskolan på Gotland

Avdelningen för datorkommunikation och programvaruteknik
Uppsatsarbete: Kandidatnivå 15 hp
Höstterminen: 2009

Författare: Johnny de Laval
Handledare: Thomas Aggesjö
Examinator: Håkan Mattsson



Sammanfattning

Trådlösa nätverk är av naturen sårbara för avlyssning för att kommunikationen sker med radiovågor. Därför skyddas trådlösa nätverk med kryptering. WEP var den första krypteringsstandarden som användes av en bredare publik som senare visade sig innehålla flera sårbarheter. Följden blev att krypteringen kunde förbigås på ett par minuter. Därför utvecklades WPA som ett svar till sårbarheterna i WEP. Kort därefter kom WPA2 som är den standard som används i nutid.

Den svaghet som kan påvisas med WPA2 finns hos WPA2-PSK när svaga lösenord används. Mjukvaror kan med enkelhet gå igenom stora uppslagsverk för att testa om lösenord går att återställa. Det är en process som tar tid och som därför skyddar nätverken i viss mån. Dock har grafikprocessorer börjat användas i syfte för att återställa lösenord. Grafikkorten är effektivare och återställer svaga lösenord betydligt snabbare än moderkortens processorer. Det öppnar upp för att jämföra lösenord med ännu större uppslagsverk och fler kombinationer. Det är vad denna studie avser att belysa; hur har grafikkortens effektivitet påverkat säkerheten i trådlösa nätverk ur ett verksamhetsperspektiv.

Nyckelord:

Trådlösa nätverk, GPU, CPU, grafikkort, processorer, säkerhet, WEP, WPA, WPA2, Elcomsoft.

Abstract

Wireless networks are inherently vulnerable for eavesdropping since they use radio waves to communicate. Wireless networks are therefore protected by encryption. WEP was the first encryption standard what was widely used. Unfortunately WEP proved to have several serious vulnerabilities. WEP could be circumvented within few minutes. Therefore WPA was developed as a response to the weak WEP. Shortly thereafter WPA2 was released and are now being used in present.

The only weakness with WPA2 is in the subset WPA2-PSK when weak passwords are being used. Software could easily go through large dictionaries to verify if a password could be recovered. But that is time consuming and therefore providing wireless networks limited protection. However a new area of use with advanced graphic cards has showed that it is providing a faster way of recovering passwords than the ordinary processor on the motherboard. That opens up for the larger use of dictionaries and the processing of words or combinations of words. That is what this study aims to shed light on. How the efficiency of the graphic cards have affected security in wireless networks from a corporate perspective of view.

Keywords:

Wireless network, GPU, CPU, graphic cards, security, processor, WEP, WPA, WPA2, Elcomsoft.

Förord

Det har varit en utvecklande och intressant tid att skriva om säkerheten i trådlösa nätverk. Många lösa ”trådar” har nu förts samman till en röd tråd där en klar uppfattning nu kan frambringas. Det är också min förhoppning att detta arbete tillför ny kunskap till ämnesområdet där många tidigare angränsande studier genomförts. Framförallt önskar jag att intresserade läsare får tillfredställande svar på frågeställningarna i uppsatsen.

Vladimir Katalov från mjukvaruföretaget Elcomsoft tackas allra ödmjukast för att ha skänkt programvaran som har använts i denna studie. Tack Vladimir.

Jag vill också rikta ett stort tack till min familj som har givit mig den tid som uppsatsen tagit i anspråk. I synnerhet till mina barn som varit så snälla att kvällar och nätter har kunnat användas för att skriva denna uppsats, så tack David och Sofie. Även Thomas Aggesjö skall ha ett stort tack för den vägledning och det stöd som genom åren nu har lett fram till denna uppsats. Tack Thomas! Ett stort tack går också till Håkan Mattsson för att ha inkommit med värdefulla synpunkter.

Stockholm, februari 2010

Johnny de Laval

Innehållsförteckning

1. Inledning

Flera upptäckter i historien har uppmärksammats med att de har till en början saknat användningsområde för att i ett senare skede förekomma inom mängder av olika ämnesområden. Lasern är ett bra exempel på det som dessutom i början kallades för ”a solution looking for a problem”.[1] Upptäckten av elektromagnetismens strålning är ingalunda ett undantag. För ungefär ett sekel sedan påvisades elektromagnetismens existens av forskaren Hertz som fick frågan hur denna upptäckt skulle påverka världen. Hertz besvarade frågan med: ”Ingenting förmodar jag”.[2] Hertz fann ingen praktisk användning av upptäckten.

I nutid används denna upptäckt inom flertalet användningsområden. Ett av dessa områden är trådlösa nätverk som numera påträffas nästan överallt.[3] Anledningen till den stora förekomsten av trådlösa nätverk beror troligen på en stark efterfrågan på mobila och flexibla lösningar. Andra drivande faktorer kan vara att de trådlösa nätverken införlivas med enkelhet i allehanda miljöer och att priset på dessa har sjunkit i takt med att tekniken har utvecklats.

Fördelarna med trådlösa nätverk är flera. Bland annat så är skalbarheten hög med ett perspektiv på infrastruktur samtidigt som det också är behändigt att arbeta med ur ett användarperspektiv. Det är enkelt att förlänga ett stamnätverk samtidigt som det också är möjligt att dela upp nätverk. Medarbetare och konsulter kan åtskiljas med olika säkerhetsnivåer och ändå kan de båda nyttja de trådlösa nätverkens resurser. De trådlösa nätverken har också stora fördelar som att alla kan dela på en enda anslutning och det ifrån valfri plats.

Det som bland annat kan åtskilja de trådlösa nätverken som verksamheter använder kontra trådlösa nätverk som medarbetarna själva handhar är säkerhetslösningarna, vilket denna studie avser att belysa; nämligen säkerheten hos de trådlösa nätverken med avseende på medarbetarna inom verksamheten med ett verksamhetsperspektiv.

Säkerheten i de trådlösa nätverken skiljer sig åt från trådburna nätverk. Anledningen är att de trådlösa nätverken använder sig av elektromagnetisk strålning som är både osynlig och ohörbar. Det innebär att lås, dörrar och väggar eller andra liknande skydd av fysiskt slag kan vara verkningslösa.

---

[1] http://en.wikipedia.org/wiki/Laser
Översättning: ”En lösning som söker ett problem”.
http://www.press.uchicago.edu/Misc/Chicago/284158_townes.html

[2] Scambray *J, s.446*

[3] http://en.wikipedia.org/wiki/Hotspot_%28Wi-Fi%29

Skydden som skall förse de trådlösa nätverken med säkerhet kommer istället i form av algoritmer. Dessa är implementerade i standarder som ska skydda vår osynliga kommunikation som utgörs av radiovågor. Standarden som oftast åsyftas är den trådlösa nätverksstandarden 802.11 som tagits fram av den icke vinstdrivande organisationen IEEE *(se begreppslista)*. Begreppet ”802.11” inrymmer en mängd standarder som oftast följs åt av en bokstav. De mest använda standarderna är bland annat 802.11a, 802.11b, 802.11g och 802.11n.

1999 släpptes standarden 802.11b ut på marknaden. Det var den första standarden som nådde acceptans av den bredare publiken och förblev väldigt populär i många år.[4] I standarden 802.11b så följde WEP med.[5] Det var en kryptering för trådlösa nätverk som skulle skydda nätverket och dess kommunikation mot obehöriga. WEP visade sig dock ha allvarliga sårbarheter.

Redan 2001 uppmärksammades sårbarheter i WEP av kryptoanalytiker. Tidigare hade Wagner observerat svagheter i algoritmen RC4 som används i WEP.[6] Det kom senare att visa sig att det fanns flera sårbarheter i WEP. Bland annat så påvisade FBI 2005 att det gick att kringgå WEP på 3 minuter med mjukvaror som fanns fritt tillgängliga på Internet.[7] Säkerheten som WEP skulle förse de trådlösa nätverken med hade blivit en utebliven framgång. De osynliga låsen som skulle skydda de trådlösa nätverken kunde förbigås med enkla medel. Ersättningen till WEP kom 2003. WEP ersattes först med WPA *(Wi-Fi Protected Access)* och sedan WPA2 *(2004)*.[8]

Den eventuella sårbarhet som man hittar hos WPA2, är den del som kallas för WPA2-PSK *(Pre Shared Key)* när svaga lösenord används. Under 2008 kom uppgifter om att man har börjat använda grafikprocessorer för att återställa lösenord baserat på WPA2-PSK.[9] Anledningen till att man har börjat använda grafikkort till detta syfte beror på grafikprocessorernas utmärkta egenskaper att utföra beräkningar, vilket dekrypteringen är avhängig. Denna innovativa användning av grafikprocessorer väcker en hel del frågor som denna uppsats avser att avhandla.

---

[4] http://en.wikipedia.org/wiki/IEEE_802.11
Barken L, s.5

[5] http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

[6] http://www.cs.berkeley.edu/~daw/my-posts/my-rc4-weak-keys

[7] http://www.smallnetbuilder.com/index.php?option=com_content&task=view&id=24251&Itemid=100

[8] http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

[9] http://wifinetnews.com/archives/2008/10/commercial_wpawpa2_cracking_software_accelerated_by_gpus.html

1.1 Syfte

Ett nytt användningsområde för grafikkort har på senare tid publicerats i olika medier som hänsyftar till säkerheten i WPA2-PSK för trådlösa nätverk. Det som avses i dessa artiklar är att avancerade grafikkort numera kan användas för att återställa lösenord med en ansenlig högre hastighet än traditionella processorer som är flerkärniga.[10]

Det föranleder frågan huruvida trådlösa nätverk är säkra numera? Är användningen av grafikprocessorer i syfte att återställa lösenord så effektiv att lösenord som tidigare ansågs vara säkra, numera är osäkra? Var går gränsen nu för vad som kan anses vara säkert? Hur komplexa bör lösenorden vara? Det är väsentliga frågor som man önskar utreda tillsammans med verksamheten *(se 2.1)* där medarbetarna använder sig av just WPA2-PSK.

Verksamhetens medarbetare använder sig av trådlösa nätverk för att kunna ansluta sig till verksamhetens huvudkontor. Därför vill man i verksamheten veta om grafikkortens nya användningsområde påverkar säkerheten i verksamheten i något avseende och om det i så fall också finns lämpliga motåtgärder.

[10] http://www.elcomsoft.com/ewsa.html

1.2 Frågeställning

I enlighet med syftet för uppsatsen så har följande frågor uppkommit.

1. Huvudfråga:
   - Har användningen av grafikprocessorer som avser att återställa lösenord påverkat säkerheten för WPA2-PSK?

2. Delfrågor:

   Om det finns en påverkan:
   - Finns det motåtgärder som tillfredställer verksamhetens krav på säkerhet?
   - Vad är sannolikheten att lösenord kan återställas i WPA2-PSK?

1.3 Avgränsningar

Studien är befattad med begränsade resurser och därför har följande avgränsningar tilldelats studien:

- Studien avgränsar sig till att ta reda på om säkerheten i trådlösa nätverk har påverkats ur ett verksamhetsperspektiv.
- Man avser att belysa trådlösa nätverk som använder sig av WPA2-PSK.
- Mjukvaran som används i denna studie är densamma som media har uppmärksammat vilket är också motivet till detta val *(se 2.4)*.[11]
- Hårdvaran som har använts i denna studie har utgått ifrån mjukvaruföretagets uppfattning vad som kan anses vara godtagbar hårdvara. I synnerhet vad som avses med ett avancerat grafikkort *(se bilaga hårdvara och mjukvara)*.
- Studien avhåller sig från att förklara allehanda tekniker som avser krypteringar eller liknande med djupdykningar som sådant. Endast övergripande förklaringar som bidrar till ökad läsbarhet och förståelse i ämnet kommer vara inkluderad.

[11] http://www.nordichardware.se/index.php?news=1&action=more&id=14624

2. Metod

Studien använder sig av en kvantitativ metod som i strikt mening innebär att data som insamlas har mätbara egenskaper. Den värld av kunskap *(ontologi)* som man söker kunskap om *(epistemologi)* utmynnar i en metodologisk huvudinriktning som är empirisk-atomisk. Det innebär att man redan på förhand har bestämt vilka tänkbara slutsatser studien kan leda till, vilket står i kontrast till en empirisk-holistisk kunskapsansats (paradigm) där man på förhand inte bestämt vet vad som kan komma fram i studien. Kunskapen framkommer av studier utifrån observationer av verkligheten där enskilda moment analyseras avgränsat och isolerat. Ledorden i studien är reliabilitet, validitet och reproducerbarhet. Validiteten innebär att man mäter det man faktiskt avser att mäta. Reliabiliteten handlar om pålitligheten av mätningarna och reproducerbarheten avser att det är möjligt att återupprepa mätningarna. Samtliga ledord är uppfyllda till sin helhet.

2.1 Val av studieobjekt

Som studieobjekt har man valt en verksamhet som är etablerad inom finansbranschen vars nisch är att tillhandahålla information som utgör underlag för säkra och lönsamma affärer. Underlagen säljs runtom i landet av säljorganisationen i verksamheten. Anledningen till att denna verksamhets har valts till studieobjekt beror på dess förutsättningar som faller väl samman med studiens syfte.

2.2 Säkerhetskraven i verksamheten

I verksamheten finns endast generella policys hur säkerheten bör vara beskaffad. Det pågår för närvarande ett arbete som syftar till att man också ska implementera säkerheten även i en detaljerad skala. Studien är dock avgränsad till de trådlösa nätverken och där står det i generella ordalag att säker kommunikation skall användas tillsammans med väl utvalda lösenord. Dock inte hur detta ska implementeras i realiteten eller hur ett säkert lösenord är uppbyggt.

2.3 Val av komponenter

Följande hårdvara har använts:

- En trådlös accesspunkt.
- En arbetsstation utrustad med dubbla kärnor.
- Ett avancerat grafikkort *(Gigabyte GTX 260)* [12].
- Två bärbara datorer.

En trådlös accesspunkt har behövts för att kunna sätta lösenord. Handskakningarna har sedan avlyssnas i kommunikationen mellan klient och accesspunkt men också insamlas för att senare processas i arbetsstationen med hjälp av programvaran *(se 2.4)*. En av de bärbara datorerna har använts för att avlyssna trafiken och för att samla in handskakningar som utväxlas. Den andra bärbara datorn användes för att skapa just denna trafik som då simulerar en vanlig klient som utväxlar handskakningar med accesspunkten.

2.4 Val av mjukvara

- Elcomsoft Wireless Security Auditor *(hädanefter EWSA).*
- Backtrack 4 *(Linux distribution)*.
- Programvara i *air* serien som medföljer Backtrack 4.

Motivet till att EWSA har valts för att användas i denna studie beror på medias uppmärksamhet kring mjukvaran. Det finns andra program såsom Pyrit om man önskar göra en jämförande studie.[13]

EWSA är ett program som återställer lösenord med hjälp av uppslagsverk. Till underlag ligger beräkningar och jämförelser av en handskakning mellan klient och accesspunkt.

---

[12] http://www.gigabyte.com.tw/Products/VGA/Products_Overview.aspx?ClassValue=VGA&ProductID=3129&ProductName=GV-N26OC-896I

[13] http://code.google.com/p/pyrit/

2.5 Uppslagsverk

Ett svenskt och ett engelskt uppslagsverk har använts i studien. Det svenska uppslagsverket innehåller cirka 13 000 ord och det engelska uppslagsverket innehåller cirka 310 000 ord.

2.6 Datainsamling av lösenord

För att kunna samla in lösenord så har man använt sig av Linux distributionen Backtrack4 och ett trådlöst nätverkskort samt en accesspunkt.

Följande kommandon används för att samla in lösenordsutväxling mellan accesspunkten och klienten:

1. airmon-ng start [device]

   Försätter kortet i avlyssningsläge.

2. airodump-ng [device]

   Kommandot ger en bild av samtliga trådlösa nätverk som kan uppfattas av det trådlösa nätverkskortet.

3. airodump-ng –c [channel] –w [password.txt] ––bssid [bssid] [device]

   Det här kommandot kommer att samla in handskakningen som utväxlas mellan accesspunkten och klienten.

2.7 Databearbetning

En klient och en accesspunkt sätts upp för att kunna samla in handskakningar som utväxlas. Insamlingen sker varje gång ett nytt lösenord skall testas. Det sker genom användningen av Linux distributionen Backtrack4. Bearbetningen processas därefter av EWSA. Endast essentiella processer är igång under bearbetningen. Tjänster och andra programvaror än de som är relevanta har stängts av för att effektivera processen.

2.8 Definitioner

Studien använder sig av flera termer och definitioner för att skapa ett gemensamt språkbruk för olika företeelser. Meningen är att det ska skapa en utgångspunkt där dessa termer och definitioner ökar förståelsen för vad som testas ur ett avgränsat perspektiv utan att behöva utveckla dem varje gång de används. Avsikten är att förenkla och skapa en större förståelse för vad som avhandlas där dessa ord används som samlade begrepp. Ibland används engelska istället för svenska då det saknas passliga översättningar.

2.9 Lösenordsterminologi

Lösenord kan ha olika mängder utfall beroende på vilka kriterier som definierar utfallsområdet. Programvaran EWSA använder följande termer för att beskriva hur de olika utfallen skapas:

- **Case mutation**: alla variationer av stora och små bokstäver kontrolleras.
- **Digit mutation**: lägger till flera siffror, både som prefix och suffix till uppslagsverket.
- **Border mutation**: Använder sig av digit mutation men lägger också till de mest vanligaste kombinationerna såsom $$$, 123, qwerty etc.
- **Freak mutation**: Ersätter en eller flera tecken från lösenordet, så att lösenord kan bli l@senord,lö$en@rd.
- **Abbreviation mutation**: Förkortningar såsom politiskt korrekt-pk, ihateyou-ih8u.
- **Order mutation**: Vänder ordningen på orden, upprepar orden, lägger till det omvända ordet, lösenord blir dronesöl, lösenordlösenord, lösenorddronesöl etc.
- **Vowels mutation**: Testar vokalerna, tar bort och blandar och stora vokaler. Lsrd, LÖsenOrd, LösenOrd etc.
- **Strip mutation**: Ett tecken tas bort, ösenord, lsenord, lösenor etc.
- **Swap mutation**: Byter ordningsföljd på lösenorden, så lösenord, blir ölsenord, lösenodr etc.
- **Duplicate mutation**: Duplicerar tecken, lösenord blir, llösenord, lööösenord, etc.
- **Delimiter mutation**: Lägger till avskiljare till ord, lösenordet blir l-ö-s-e-n-o-r-d, l+ö+s+e+n+o+r+d etc.
- **Year mutation**: Lägger till år till ord, lösenord blir, lösenord1984 etc.

2.10 Definierade lösenord

I denna studie mäter man återställande av lösenord i antalet testade lösenord per sekund eller totalt antal sekunder. Man har också avgränsat sig till att studera några specifika lösenord. Kategorierna är uppdelade i enkla, medellätta, medelsvåra och svåra lösenord. Meningen är att skapa en utgångspunkt för att kunna utreda hur användningen av grafikprocessorer har påverkat säkerheten för trådlösa nätverk. Denna definiering utgör också underlag för vidare diskussioner.

- **Enkla lösenord:** Det omfattar ord som finns i uppslagsverk. Även ord som är något förändrade som antingen har ett prefix eller suffix bestående av siffror.
- **Medellätta lösenord**: Det omfattar ord som finns i uppslagsverk. Även ord som är något förändrade som antingen har ett prefix eller suffix bestående av slumpmässiga bokstäver eller symboler.
- **Medelsvåra lösenord**: Det omfattar slumpmässiga lösenord bestående av blandade stora och små bokstäver samt siffror.
- **Svåra lösenord**: Det omfattar genomtänkta lösenord som består av konstens alla regler för att skapa komplexa lösenord. Dessa består av blandade bokstäver stora och små samt siffror och symboler.

2.11 Litteraturstudier

Internet har varit en betydande källa i denna studie. Anledningen är att ämnet i sig själv är relativt nytt och har en viss tendens att göra sig väl tillgänglig på nätet och mindre tillgänglig i litteratur. Därför har litteraturstudierna till övervägande del använts för att förklara vad trådlösa nätverk är och hur de fungerar. I övrigt har programmen som använts varit självförklarande eller så har det varit möjligt att läsa dokumentationen om programmen via kommandot *man* i Linux eller hjälpfilerna till programmet i Windows.

3. Introduktion till trådlösa nätverk

Det finns flera fördelar med att använda trådlösa nätverk. Några av fördelarna är mobilitet, skalbarhet och bättre produktivitet. Bland annat så kan exempelvis medarbetare nå nätverksresurser utan att vara hänvisade till specifika platser såsom i fasta nätverk. Man kan förlänga stamnätverket med enkelhet och till låga kostnader. Det går också att avgränsa nätverken så att man delar upp verksamhetens olika behov beträffande resurser och säkerhet. Sammanfattningsvis så är fördelarna många och vad är det som gör detta möjligt? Att exempelvis vara så mobil och ändå ha tillgång till allt?

Svaren på dessa frågor finns inom våglären. Det är vågor som gör detta möjligt. Det är dock inte vilka vågor som helst utan vågor som återfinns i det elektromagnetiska spektrumet så kallade elektromagnetiska vågor. Där solstrålar, radiosändningar med mera befinner sig. Dessa vågor tar sig fram utan att vara bunden till varken trådar eller någon annan materia. Det medför att medarbetare kan vara mobila i verksamheten och ändå komma åt allehanda resurser där de elektromagnetiska vågorna kan ta sig fram.

Men vad menas med vågor i det elektromagnetiska spektrumet? Man kan tänka sig att en våg utgörs av något som svänger i ett periodiskt mönster såsom en gitarrsträng. Det är en form av energi som överförs från en plats till en annan och denna överföring utgör kommunikationen i etern. Dessa vågor skapas av trådlösa nätverkskort eller accesspunkter som också kan ta emot vågor.

Skolor, flygplatser, tågstationer, städer, bostäder, arbeten med mera är oftast numera utrustade med accesspunkter, offentliga såväl som privata. En betydande anledning till denna spridda förekomst kan troligen härledas till Internet som en viktig portal för verksamheter och konsumenter.

3.1 WEP

Redan från början var WEP avsett för att skydda de trådlösa nätverken med motsvarande säkerhet som finns hos de trådburna nätverken, vilket namnet också antyder *(Wired Equivalent Privacy)*. Det var inte utvecklat för att vara supersäkert och dessutom så begränsades arbetet med standarden på grund av amerikanska exportregler som reglerade nyckellängden i WEP.

WEP var dock en kryptering som fick stor spridning bland de trådlösa nätverken. Tyvärr hade WEP flera sårbarheter som medförde att lösenordsgissning i den vanliga bemärkelsen var överflödig.[14] WEP kunde kringgås och olika metoder utvecklades genom åren som påvisade detta. Sårbarheterna i WEP kom att kallas för ”Wiretap Equivalence, Please”.[15]

Sårbarheterna var många i WEP och en anledning till det var bland annat hur RC4 *(se begreppslista)* algoritmen implementerades.[16] Algoritmen skapade svaga nycklar något som Wagner anade långt innan WEP släpptes och det var något Scott Fluhrer, Itsik Mantin och Adi Shamir uppmärksammade *(2001)* i sin rapport.[17] Därefter förfinades upptäckterna vilket innebar att tiden det tog att kringgå WEP minskades drastiskt. Orsaken var att algoritmen läckte information genom att den producerade en nyckelström som delvis inte var slumpmässig och som genom olika metoder möjliggjorde att lösenorden kunde härledas.

Trots bristerna, så förser WEP de trådlösa nätverken med skydd i en viss mån, vilket är ett bättre skydd än inget skydd alls.[18] Äldre teknologi stödjer inte WPA2 och det kan vara en anledning till att WEP fortfarande används. WEP ges som ett förstahandsalternativ i somliga routrar vilket kan bidra till att WEP fortfarande implementeras istället för WPA2 som är det säkrare alternativet.

[14] Hurley C, s.142
[15] Gast M, kap.18
[16] Olsson F, s.32
[17] http://aboba.drizzlehosting.com/IEEE/rc4_ksaproc.pdf
[18] Olsson 2007,s.33

3.2 WPA

Till sin natur så är de trådlösa nätverken sårbara för avlyssning därför att kommunikationen sker via elektromagnetiska vågor som kan avlyssnas.[19] Därför togs WEP fram redan 1997 för att råda bot mot avlyssning och att tillföra användarna säker kommunikation *(inkluderades i 802.11 1999)* motsvarande trådburen säkerhet. Dock visade sig WEP ha allvarliga säkerhetsbrister.

Därför tog man fram WPA som var det nya namnet på standarden som skulle råda bot på säkerhetsbristerna i WEP som ett första steg. De trådlösa nätverken blev återigen säkra för de som implementerade den nya tekniken. Det var en mellanlösning som togs fram för att existerande hårdvara skulle kunna uppgraderas. Det löste man via TKIP som också använder sig av RC4, dock på ett annat sätt än i WEP.[20]

Det skulle dock inte dröja länge innan nästa krypteringsstandard släpptes. 2004 kom WPA2 som var ersättaren till WPA som numera anses vara tagen ur bruk.

3.3 Förbättringen WPA2

Den senaste standarden WPA2 använder sig av AES och uppfyller alla obligatoriska delar av standarden 802.11i.[21] WPA2 använder sig av funktionen PBKDF2.[22] Denna funktion använder sig bland annat av parametrar såsom SSID *(se begreppslista)* och lösenord. Utöver det så använder metoden sig av funktionen HMAC-SHA1 *(närmare 4096 iterationer)* för att stärka nyckeln.[23] Syftet med denna beräkning är att försvåra arbetet med att kunna härleda lösenordet.

De stora säkerhetsskillnaderna som särskiljer WEP från WPA och WPA2, är att svagheter i krypteringen kan utnyttjas för att återställa lösenord i WEP. Det kan inte åstadkommas i WPA-PSK och WPA2-PSK utan där är man tvungen att använda ”bruteforce”[24] för att kunna återställa lösenord. I WPA2-PSK inriktar man sig också på svaga lösenord.

[19] Carpenter T, 2008, s.441
[20] Temporal Key Integrity Protocol
[21] Advanced Encryption Standard
[22] Password-Based Key Derivation Function
[23] (HMAC) Hash-based Message Authentication Code (SHA) Secure Hash Algorithm
[24] ”Bruteforce” innebär att man testar alla möjliga utfall inom utfallsområdet.

3.4 De trådlösa nätverken i verksamheten

De flesta medarbetarna arbetar på huvudkontoret. Därutöver finns det lokalkontor av varierande storlek. Det finns också medarbetare som arbetar hemifrån dagligen som säljare.

Samtliga använder sig av någon form av kommunikation antingen i eller till huvudkontoret. De större arbetsplatserna inom verksamheten har fasta linjer till huvudkontoret. Det är endast medarbetare som arbetar hemifrån eller från fältet som använder sig av krypterade förbindelser till verksamheten.

Medarbetare som arbetar utanför lokalkontoren och huvudkontoret ansvarar själva för sina uppkopplingar mot huvudkontoret. Därför varierar säkerheten kring dessa uppkopplingar avsevärt. En del medarbetare använder inte några säkerhetsinställningar alls medan andra implementerar fullskalig säkerhet med bland annat brandväggar, antivirus och trådlösa nätverk med kryptering.

Resonemangen varierar hur medarbetare ser på säkerhet och trådlösa nätverk. En del medarbetare anser att de litar på sin omgivning, en del bor så avlägset och ensligt att de enda människorna som finns belägna i området är dem själva. En del uppger att de har använt sitt eget öppna nätverk ute på vägen vilket är fullt möjligt.[25] Resonemangen varierar efter omständigheter och kunskapsnivåer. Dock så saknar de flesta kunskap om säkerhet inom IT.

Det är ett bekymmerskapitel för verksamheten eftersom det skapar säkerhetshål och kan ställa till problem av allehanda slag (*se risker 5.2*). Man strävar inom verksamheten att samtliga medarbetare skall använda ett fullgott skydd enligt de generella regelverk som är fastställda. Det innebär att man från verksamheten strävar efter att samtliga skall använda sig av WPA2-PSK. Det är dock mycket svårt att säkerställa att medarbetarna använder just WPA2-PSK i praktiken därför att det är helt enkelt svårt att följa upp samt också att medarbetarna generellt saknar kunskaper om detta i praktiken.

[25] Gast M, kap.1

4. Jämförelse av CPU och GPU

I takt med tiden har utvecklingen av processorer ständigt utvecklats mot nya höjder beträffande hastigheter och effektivitet. Nuförtiden begränsas tillväxten av fysiska lagar såsom ström och värme. Så istället har man bytt spår och implementerar nu istället flera kärnor under samma skal som arbetar oberoende av varandra.

Som en jämförelse så har man i denna studie använt ett grafikkort med 216 streamprocessorer i en dator som är utrustad med två kärnor. Grafikkortet har speciella processorer som är lämpade för parallella beräkningar medan processorn är lämpade för en annorlunda exekvering.

Nu är det svårt att jämföra en GPU med en CPU just för att de har åtskilda arkitekturer. Dock inser man ganska snabbt att grafikkorten är tillverkade med ett speciellt ändamål i åtanke och det är på just beräkningar.

Grafikprocessorer är designade för snabb exekvering av många parallella trådar samtidigt medan en CPU är tillverkad för att exekvera en tråd i taget så snabbt den kan. Även minneshanteringen skiljer de olika processorerna åt. En GPU har mycket snabbare minne vilket är essentiellt för parallella beräkningar med stora dataströmmar. Det skiljer sig också hur "cachen" används. En CPU använder "cachen" för att undvika fördröjningar i minneshanteringen medan en GPU löser problemet med att exekvera tusentals trådar samtidigt. När en tråd väntar på data från minnet så kan ändå grafikprocessorn arbeta vidare med en annan tråd.

Andra stora skillnader är att en CPU kan exekvera 1-2 trådar per kärna medan en GPU kan hålla 1024 trådar under en enda multiprocessor *(grafikkort har oftast flera sådana)*. Dessutom kostar det en CPU hundratals cykler att byta från en tråd till en annan medan en GPU byter flera trådar per cykel.

Sammanfattningsvis kan man konstatera att grafikprocessorer har en arkitektur som är väl lämpade för beräkningar där vanliga processorer med flera kärnor står sig släta i just detta avseende. Just detta har man också tagit tillvara på hos företaget Elcomsoft som har utvecklat produkten EWSA som återställer lösenord genom att använda sig av grafikkortens enorma beräkningskapaciteter.

5. Lösenordsteori

Lösenord ska skydda tillgångarna i verksamheten mot obehöriga samt också tilldela resurser för behöriga såsom kunder och användare både inom verksamheten och utanför. Denna del är så pass viktig att man önskar i studien belysa några aspekter hur lösenord kan vara beskaffade. Vad lösenordens komplexitet har för betydelse ur olika perspektiv samt vad som motiverar säkra lösenord i sammanhanget.

5.1 Lösenord

Det primära syftet med lösenord är att förhindra åtkomst till resurser för obehöriga och att omvänt tilldela resurser för behöriga i olika avseenden. Lösenordet bestämmer vilken tillgång man har till diverse resurser. Trots sitt namn så behöver inte ett lösenord bestå av ett ord. Helst så ser man att lösenorden består av en harang av blandade tecken med omväxling av både stora och små bokstäver samt gärna någon siffra och någon symbol. Komplexiteten ökar säkerheten i systemen men minskar också oftast förmågan att minnas lösenorden och det kan vara kontraproduktivt.

Att minnas komplexa lösenord är en svår konst för människor som gärna väljer enkla lösenord när möjlighet ges.[26] Avvägningen för hur komplexa lösenord bör vara beskaffade kan vara snårigt att definiera. Dock är det lämpligt att det finns en balans mellan säkerhet och användarvänlighet så att användarna kommer ihåg sina lösenord.

Lösenordets komplexitet avgör hur mycket tid som kommer att tas i anspråk när man ska återställa ett lösenord. Tiden det tar att gissa sig fram till ett lösenord är också en måttstock på hur säkert lösenordet är. Indirekt är det också ett mått på hur säkert systemet i sig självt är beroende på vems konto lösenordet tillhör. Även mindre betydelsefulla konton kan användas för att eskalera rättigheter i system. Därför är också mindre betydelsefulla konton viktiga att skydda eftersom dessa kan bereda väg för vidare intrång av obehöriga till konton med större befogenheter. Exemplifiering av det när samma lösenord används till olika ändamål. Vilket innebär att lösenord som återställs vid ett system också kan användas i andra system.

[26] http://www.acsac.org/2005/papers/89.pdf
http://homepages.cs.ncl.ac.uk/jeff.yan/jyan_ieee_pwd.pdf

5.2 Risker

Ett avbrott i verksamhetens produktion innebär att man förlorar inkomster i samma sekund. Det är av yttersta vikt att systemen fungerar eftersom hela verksamhetens existens vilar på det. Det finns flera hotbilder i nutid som kan leda till produktionsstop. Virus, maskar, bakdörrar, attacker av olika slag och sårbarheter i existerande programvaror är några hotbilder för att nämna några. Det finns även andra hotbilder där ekonomiska motiv eller hämnd kan utgöra ett hot mot verksamhetens fortlöpande affärsverksamhet.[27] Insiderhot finns det också där personalen otillbörligen kan utnyttja systemen.[28]

5.3 De obehörigas motiv

Det saknas ett entydigt svar på vilka de obehöriga är eller vad det är som motiverar dem. Dock finns det många anledningar till varför trådlösa nätverk kan vara intressanta objekt för obehöriga.[29] Bland annat kan obehöriga ha ett behov att vara anonyma. En del sysselsätter sig med olagliga aktiviteter medan andra drivs av ren nyfikenhet. Anledningarna är många och det viktiga i sammanhanget är kanske inte att utreda vilka de obehöriga är eller vad det är som driver dem, utan att veta att de finns och att de utgör ett hot mot verksamheten ur olika säkerhetsperspektiv. Oavsett om de obehöriga är människor eller utgörs av illasinnade mjukvaror så bör verksamheten ha motsvarande beredskap att hantera dessa.

[27] Olsson F, s.13
[28] Mitrovic P, s.47
[29] Vladimirov A, 2004, kap 2

6. Tillvägagångssätt

Studien utförs genom att testa utvalda lösenord. Avsikten med utvalda lösenord är att man ska få en uppfattning av hur definitionerna *(se definierade lösenord 2.10)* motsvarar reella lösenord samt också få en god förståelse för hur realiteten korrelerar med teorin beträffande återställande av lösenord.

6.1 Valda lösenord

I kategorin *enkla lösenord* så har flera lösenord valts på grund av dess varierande uppbyggnad som antas vara vanligt förekommande.

Kategorin *medellätta lösenord* fick ett lösenord tilldelat. Meningen med studien är att illustrera typiska lösenord och hur de påverkas och man anser att det syftet är tillfredställt med ett valt lösenord i denna kategori. Samma resonemang följer även för kategorin *medelsvåra och svåra lösenord*.

- **Enkla lösenord:** johnjohn, sommar66, summer66
- **Medellätta lösenord:** Tgnhand@
- **Medelsvåra lösenord:** TgnC3Ef7
- **Svåra lösenord:** A@u4b$1A

6.2 Inställningar

Det finns många inställningsmöjligheter i programvaran EWSA. Därför har man valt att specificera testerna. Anledningen är att man önskar skapa ett underlag för att man senare ska kunna analysera, jämföra och diskutera resultaten och även kunna återupprepa testerna objektivt.

Samtliga tester har använt sig av *valet* i EWSA att testa ord i uppslagsverken som är mindre än 8 positioner och som är längre än 64 positioner. Det är för att ord som är mindre än 8 positioner i uppslagsverket skall komma med. Ord som får ett prefix eller ett suffix tillagt i EWSA kan bli större än 7 positioner och utgöra ett giltigt lösenord. En förklaring till varför EWSA har med detta som ett val är för att WPA2-PSK stödjer inte lösenord färre än 8 positioner eller längre än 64 positioner. Sammanfattningsvis så kommer alla ord att testas även om de är mindre 8 positioner därför att suffix eller prefix kan förlänga orden till att bli längre än 7 positioner och därför utgöra ett giltigt WPA2-PSK lösenord.

Termerna som är angivna i *2.9* är befattade med en kontinuerlig skala. De två extremvärdena som symboliserar varandras motsatser i detta sammanhang är valen *hastighet* och *effektivitet*. Däremellan hastighet och effektivitet ligger valet *medel* enligt denna studie. Dessa är studiens direkta översättningar från engelska till svenska och egen definiering av *medel*.

Hastighet är precis som namnet antyder baserat på att det ska gå fort att återställa lösenord enligt valda kriterier. Det innebär att man ska undvika att kombinera uppslagsorden i en större omfattning utan satsa på enkelhet och snabbhet.

Motsvarigheten till valet hastighet är valet *effektivitet*. Det innebär att man satsar extra mycket på att ta fram flera kombinationer till varje ord från uppslagsverk som testas. Det innebär att det tar längre tid att för programmet att ta sig igenom uppslagsverk.

Däremellan hastighet och effektivitet, ligger valet *medel* som symboliserar ett mittenvärde. Denna definition av medel kan antas vara en avvägning mellan effektivitet och hastighet.

Exakt hur omfattande termerna är i kapitel *2.9* är inte specificerade i EWSA eller i programmets dokumentation. Därför saknas det möjligheter att ange exakt hur utfallen tas fram. På den punkten utgår studien från att programmet är konstruerat på ett sådant sätt att de optimala avgränsningarna sätts utifrån rimliga antaganden samt inställningar.

Det finns flera alternativ att välja i programmet EWSA. Testerna är specificerade enligt *tabell 1* utifrån intressanta utgångspunkter som senare kan jämföras och analyseras enligt studiens syfte.

Tabell 1. Sammanställning av hur lösenorden kommer att testas

Lösenord	Processor[30]	Val – inställning	Uppslagsverk
sommar66	GPU	Alla – medel	Svenskt
sommar66	GPU	Digital mutation – effektivt	Svenskt
sommar66	CPU	Alla – medel	Svenskt
summer66	GPU	Digital mutation – effektivt	Engelskt
sommar66	GPU	Digital mutation – effektivt	Engelskt
Johnjohn	GPU	Border mutation – medel	Svenskt
Johnjohn	GPU	Border mutation – effektivt	Svenskt
Tgnhand@	GPU	Alla – effektivt	Svenskt
TgnC3Ef7	GPU	Alla – effektivt	Svenskt
A@u4b$1A	GPU	Alla – effektivt	Svenskt

6.2.1 Processorer

Det är två val som studien tar ställning till när val av processorer görs. Det ena valet går ut på att enbart testa med moderkortets processor och det andra valet består av att testa med grafikprocessorn och moderkortets processor. Anledningen till dessa två val är när grafikprocessorn väljs så används alltid också moderkortets processor och det är inte möjligt att välja bort moderkortets processor.

6.3 Uppslagsverk

Det finns mängder med uppslagsverk som man kan använda sig av. Vissa uppslagsverk är flera hundra megabyte stora och andra kan vara av storleken gigabytes. Det är mycket stora uppslagsverk. I denna studie har man valt att använda sig av mindre uppslagsverk av praktiska skäl. För att få en jämförelse så består det svenska uppslagsverket av ca 13 000 ord och är ungefär 130 kilobyte. Det engelska uppslagsverket består av ca 310 000 ord och är ungefär 4 megabyte. Uppslagsverken är inte bearbetade i någon form utan innehåller ord med varierande antal positioner.[31]

[30] CPU motsvarar enbart moderkortets processor. GPU motsvarar grafikkortets processor och moderkortets processor.

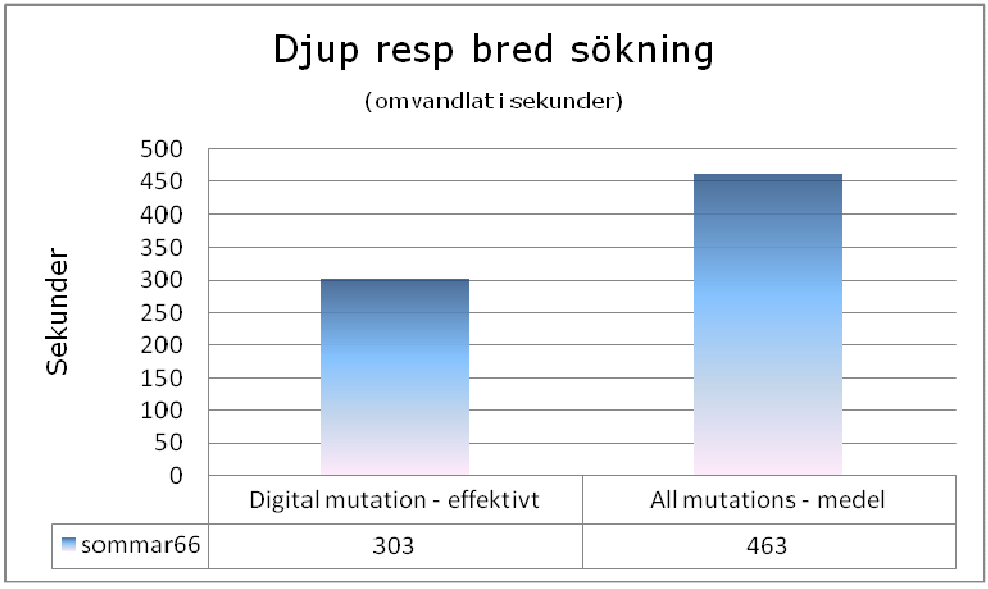
[31] www.laval.se/filer/passwordlists

7. Resultat

Varje försök att återställa ett lösenord tar en viss tid i anspråk och därför begränsar lösenordens komplexitet vad som kan återställas vid beaktandet av tid som en begränsad resurs. Därför kan man utgå från att medelsvåra och svåra lösenord kommer att ta mycket tid i anspråk att återställa medan enkla och medellätta lösenord kommer att ta mycket mindre på grund av det mindre utfallsområdet. Studiens resultat påvisar även andra faktorer som kan påverka sannolikheten att kunna återställa lösenord däribland djup och bredd på sökningar men även hur uppslagsverken är konstruerade samt också vilket uppslagsverk som används.

7.1 Djup eller bredd

Ett stort antal utfall kan öka chansen att återställa lösenord. Det är också viktigt att inte bara antalet utfall ökas utan också att rätt sorts kombinationer används. Det är en stor skillnad på att använda kombinationer på bredden eller djupet. Med bredd avses att man söker på flera områden efter specifika kombinationer. Sökningen på djupet gör det omvända det vill säga söker efter maximalt antal möjliga utfall inom specificerat delområde. Det påvisas i figur 1, att en djup sökning inom rätt delområde har en större sannolikhet att kunna återställa lösenord än en bred sökning. Lösenordet ”sommar66” kunde återställas på 5 minuter och 3 sekunder med hjälp av det svenska uppslagsverket *(se tabell 1)*. Sökningen genomfördes då på djupet med grafikprocessorn vilket innebar att flera utfall testades än vad som hade gjorts med inställningen medel.

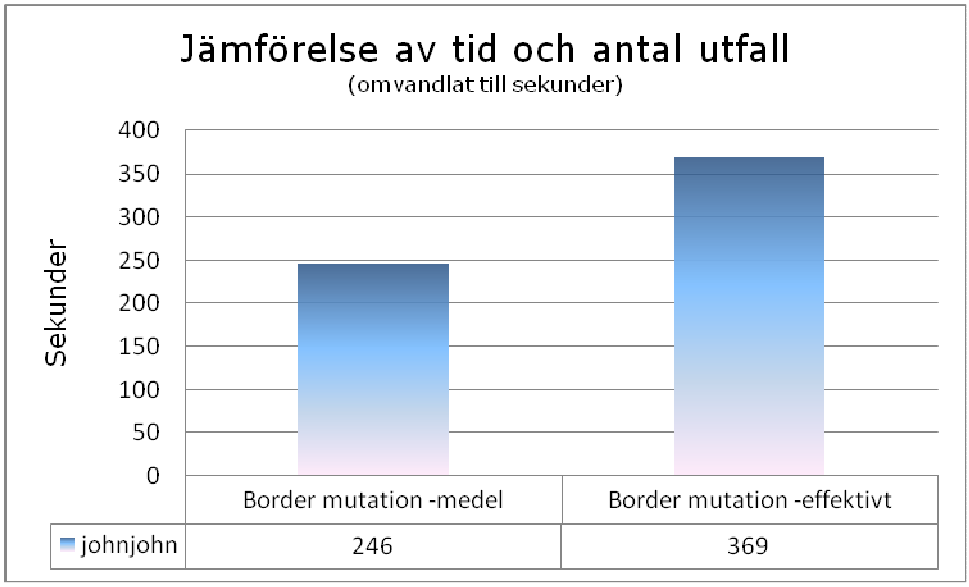


Figur 1. Sökning med djup respektive bredd.

Därefter genomfördes samma sökning med samtliga termer valda (*se 2.9*) med inställningen medel, en så kallad bred sökning. Tiden det tog var 7 minuter och 43 sekunder. Det resulterade i att lösenordet inte kunde återställas trots att termen ”Digital mutation” ingick. Anledningen till att lösenordet inte kunde återställas berodde på att djupet på sökningen inte var tillräcklig djup inom rätt sökområde.

7.2 Tid och antal utfall

Orden som används från uppslagsverk kan kombineras på en mängd olika sätt. Ju fler kombinationer som används med både bredd och djup desto flera utfall erhåller man. Det är direkt korrelerat med ökad sannolikhet och tid som tas i anspråk *(se figur 2).* Den ökade tiden påvisas i figur 2 där en djup och en medel sökning genomförs. Sökningen som genomförs på djupet *(effektivt)* tar ansenlig längre tid än sökningen som är inställd på *medel*.



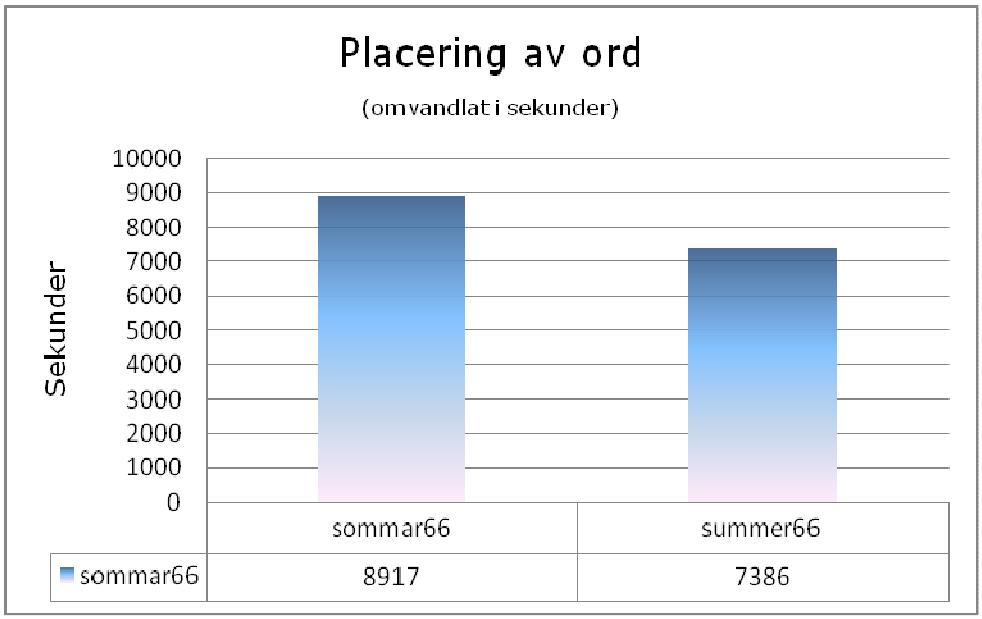
Figur 2. Korrelation mellan tid och utfall.

7.3 Ordets placering

Ordet placering i ett uppslagsverk har en stor betydelse för hur snabbt ett lösenord kan återställas. Om lösenordet som söks finns i början av uppslagsverket så kommer detta att hittas betydligt snabbare än om ordet är placerat längst bak.

I figur 3 åskådliggörs detta genom två tester. Det första testet skedde med sökning av lösenordet ”sommar66” mot det engelska uppslagsverket. Detta genomfördes på ca 2 timmar och 30 minuter utan att lösenordet kunde återställas (ordet finns inte uppslagsverket). Det innebär också att det tog så lång tid att gå från första ordet i uppslagsverket till det sista ordet. Därefter testades lösenordet ”summer66” som kunde återställas efter ca 2 timmar. Det ordet finns långt bak uppslagsverket. I båda testerna användes grafikprocessorn.

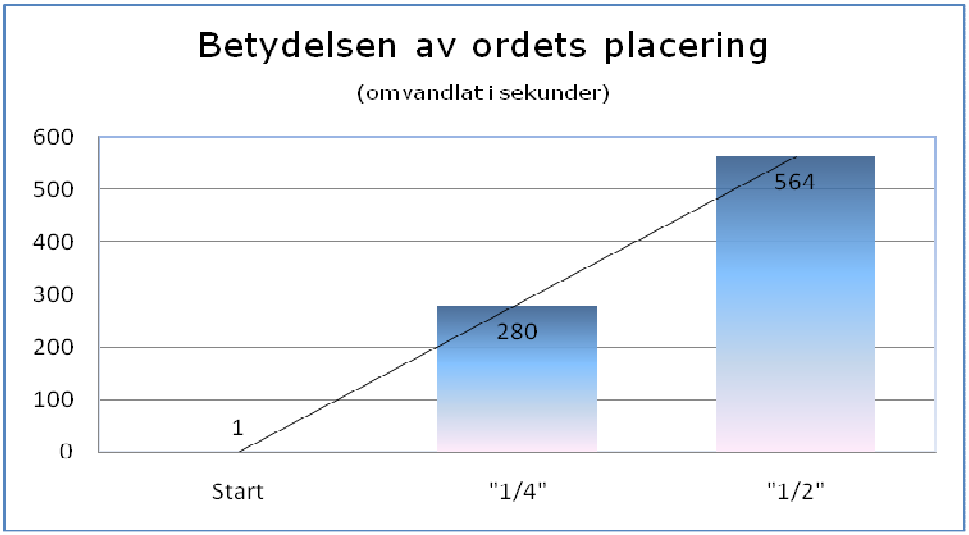
Resultatet påvisar att de lösenord som börjar på de första bokstäverna i alfabetet har en större sannolikhet att hittas snabbare än lösenord som börjar med bokstäverna i slutet av alfabetet. Det gäller förstås under förutsättningen att uppslagsverket är konstruerat enligt denna norm.



Figur 3. Betydelsen av positionen av ord i uppslagsverk.

7.3.1 Betydelsen av ordets placering

Vikten av ordens placering följer den räta linjens ekvation som visas i figur 4. Återställandet av lösenordet tog bara 1 sekund om ordet låg först i uppslagsverket. Proportionerligt med grafikprocessorns hastighet så tog det 4 minuter och 40 sekunder att återställa lösenordet om ordet var placerat en fjärdedel *(1/4)* in i uppslagsverket. Det följs åt av att om ordet placerades hälften *(1/2)* in i uppslagsverket så tog det 9 minuter och 24 sekunder vilket nästan är exakt dubbelt upp.

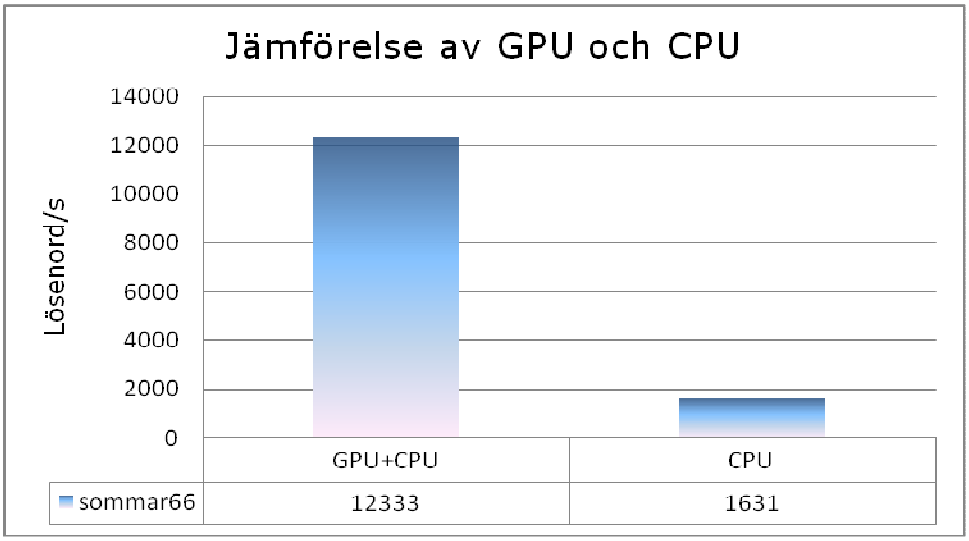


Figur 4.

7.4 Skillnaden mellan GPU och CPU

Beräkningshastigheten ökar markant när en kraftfull grafikprocessor används oberoende av vilken terminologi av lösenord som testas.[32] Studiens avancerade grafikkort kan i genomsnitt testa ca 12 000 lösenord per sekund *(inklusive CPU)*.

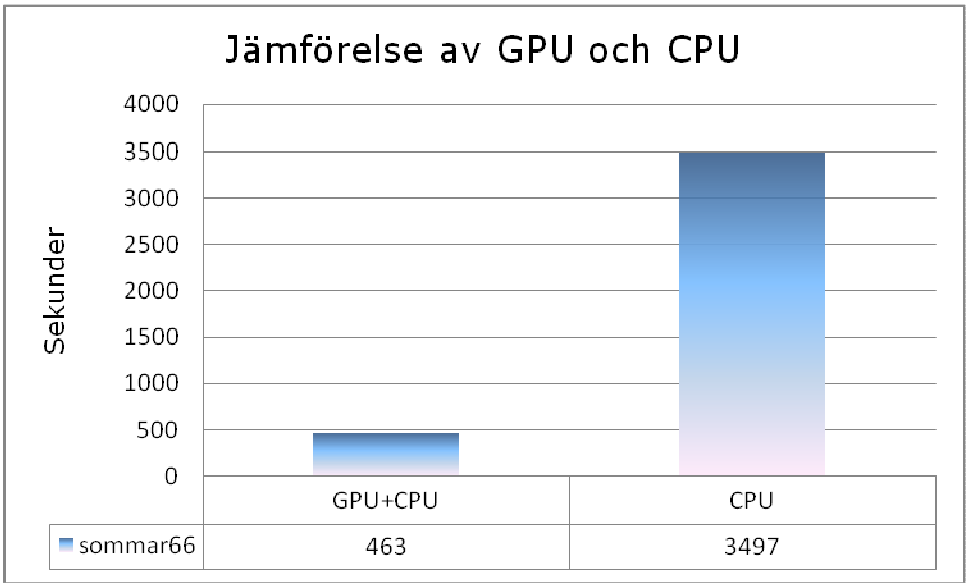
I jämförelse så kan moderkortets processor endast testa ca 1600 lösenord per sekund. Det illustreras i figur 5 när lösenordet ”sommar66” testades med grafikkortets processor jämte moderkortets processor. Testerna genomfördes med samma val (*se tabell 1*). Resultatet påvisar att processen går markant snabbare när grafikprocessorn inkluderas. Ungefär 10 000 lösenord/per sekund extra tillför grafikkortet vilket är betydligt snabbare än att enbart använda moderkortets processor. Det innebär att med grafikkortet så går det cirka 7 gånger snabbare att återställa lösenord där så är möjligt än med enbart moderkortets processor.



Figur 5. CPU och GPU+CPU i jämförelse.

[32] http://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html

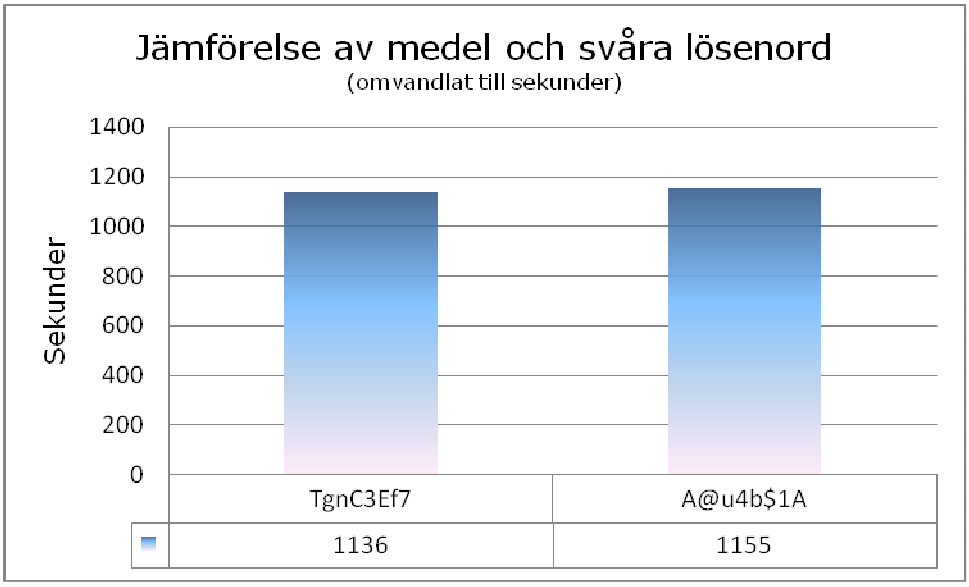
Samma test omräknat i total tid så behövde grafikprocessorn 7 minuter och 43 sekunder på sig för att processa uppslagsverkets alla ord. Betydligt längre tid behövde moderkortets processor som behövde 58 minuter och 17 sekunder för samma uppgift. Det är en markant skillnad på ca 50 minuter (*se figur 5*). Tiden är omräknad i sekunder för att man lättare skall se differenserna. Det påvisas i figur 6 att grafikkortet möjliggör ett återställande av lösenord cirka 7 gånger snabbare än med moderkortets processor.



Figur 6. Tidsperspektiv i sekunder.

7.5 Begränsningarna

Metoden i mjukvaran bygger på att kombinera ord från uppslagsverk med både djup och bredd. Dessa ord kan förändras genom en mängd olika kombinationer med och utan prefix samt suffix. Någonstans går det en gräns där orden från ett uppslagsverk övergår till att bli slumpmässiga kombinationer av bokstäver, siffror och symboler. Det är där medelsvåra och svåra lösenord kommer in bilden för att de representerar övergången från ord till slumpmässiga lösenord. Med alla mutationer (*se 2.9*) valda och med en sökning på djupet så tog det ca 19 minuter för medelsvårt och svårt lösenord att ta sig igenom det svenska uppslagsverket *(se figur 7)*. Inget av dessa lösenord kunde återställas. Inte ens medellätta lösenord kunde återställas trots att lösenordet består av ordet ”hand” från det svenska uppslagsverket med ett prefix och ett suffix.



Figur 7. Alla mutationer valda med inställningen effektivt.

7.6 Avvikelser

De avvikelser som kunde studeras var hastigheten som grafikprocessorn presterade. Normalt så kunde grafikprocessorn testa ca 15 000 lösenord per sekund. Dock så tog hastigheten sig ner på ca 8000 lösenord vid ojämna intervall i mycket korta perioder. Det sänkte medelprocessandet av lösenord till ca 12 000 lösenord per sekund i samtliga tester. I något ögonblick kunde också hastigheten stiga till 22 000 lösenord per sekund. Avvikelserna var mycket korta men påverkade medelhastigheten betydligt.

8. Diskussion och slutsatser

Storleken på utfallsrummet och begränsningar i tid är grundläggande faktorer som påverkar sannolikheten att kunna återställa lösenord. Man kan numera processa en betydligt större mängd utfall på mindre tid än förut *(se figur 5 och 6)* vilket innebär att sannolikheten har ökat väsentligt i vissa avseenden *(se figur 1 och 2)* men mindre i andra avseenden *(se figur 7)*. Även specifika uppslagsverk kan korta ner tiden genom att vanligt förekommande lösenord placeras först i uppslagsverket *(se figur 3 och 4)*.

8.1 Lösenord som påverkas markant

Enkla lösenord har varit möjligt att återställa sedan tidigare. Skillnaden från förr är att det nu går fortare att göra samma sak. Det innebär som en direkt följd att enkla lösenord utgör ett svagare skydd än tidigare eftersom sannolikheten att återställa enkla lösenord har sammanfattningsvis ökat i praktiken.

8.1.1 Sannolikheten att återställa lösenord

Med åtanke att det finns ca 125 000 ord i svenska akademins ordlista så finns det goda chanser att återställa lösenord som är baserade på svenska ord eller kombinationer av orden. Det gäller också även andra lösenord som är baserade på andra språk. Det enda förutsättningen som krävs är att man har motsvarande uppslagsverk till sitt förfogande.

Enkla lösenord är därför möjliga att återställa. Det beror på att orden ofta finns i uppslagsverk och används lättsamt modifierade. Om så är fallet så finns det en hög sannolikhet att de kan återställas.

Förklaringen till att människor använder sig av lätta lösenord, kan bero på människans relativt goda förmåga att minnas enkla och relevanta ting i vardagen. Det omvända verkar vara svårare för människor, att minnas talserier eller märkliga haranger av symboler och bokstäver blandade med varandra utan till synes mening. Troligen därför lär människor fortsätta använda sig av enkla lösenord även framöver.

Svåra och medelsvåra lösenord har man försökt återställa utan framgång *(se 7.5)*. Den uteblivna framgången beror på lösenordens komplexitet. Utfallsrummet är dels för stort men också att EWSA är avsedd att verka inom

en annan avgränsning. EWSA använder sig av ord från uppslagsverk som en utgångspunkt . Dessa ord kan sedan kombineras både på bredden och djupet. Denna utgångspunkt saknas i svåra och medelsvåra lösenord utan dessa är slumpmässiga av varierande komplexitet. De saknar ord från uppslagsverk som utgångspunkt.

Med matematikens förtjänst är det möjligt att beräkna tiden det skulle ta att återställa dessa lösenord med åtanke på grafikprocessorers beräkningskraft. Detta exemplifieras med lösenord som definieras som medelsvårt enligt följande:

- **Medelsvåra lösenord:** TgnC3Ef7

Med gemener och versaler samt också talserien från 0 till 9 ger:

∑ ((26+26+10)^8) = 218340105584896 möjliga kombinationer.

Med det avancerade grafikkort som har använts i denna studie skulle det ta cirka 600 år *(grovt avrundat)* att testa varje kombination som ett lösenord av denna magnitud utgör.[33] Med åtanke på utvecklingens rasande takt inom IT så är det föga troligt att varken krypteringsstandarden eller hårdvaran kommer att användas så länge.

Det är därför inte sannolikt att ett medelsvårt lösenord kommer att kunna återställas enligt studiens avgränsningar. Medelsvåra lösenord är dock påverkade fast i en obetydlig skala. Det utesluter inte att andra slutsatser kan tas med andra förutsättningar och metoder.[34] Svåra lösenord är ännu mindre påverkade än vad medelsvåra lösenord är och kan anses vara säkra att använda precis som medelsvåra lösenord enligt samma resonemang.

8.2 Mjukvaran och medellätta lösenord

Att kunna återställa lösenord bygger på principen att man använder ord som är tagna från uppslagsverk eller så modifierar mjukvaran dessa ord enligt en mängd uppsättningar *(se 2.9).* Hur kommer det sig då att medellätta lösenord inte går att återställa med vald mjukvara? Det svaret ligger i ett antal utfall ökar markant till sådana nivåer att tiden blir snabbt en avgörande faktor när antalet variabler är okända i ett lösenord. Dessa variabler kan dessutom bestå av både tecken, siffror och symboler. Utfallsområdet blir

[33] http://lastbit.com/pswcalc.asp
[34] http://www.renderlab.net/projects/WPA-tables/

snabbt väldigt stort. Mjukvaran är troligen konstruerad för optimala förhållanden som omges av både säkerheten som WPA2-PSK omgärdas av men också vad människor förväntar sig av mjukvaran.

8.3 Verksamhetens motåtgärder

Enligt studiens avgränsningar så rekommenderas att man använder medelsvåra eller svåra lösenord. Det är den enklaste och den mest säkra inställningen som kan göras i WPA2-PSK. Förslagsvis så bör man även förflytta det tekniska ansvaret ifrån användarna till en leverantörsmässig nivå där kraven på säkerhet kan uppfyllas professionellt. På så sätt uppfyller verksamheten kraven på tillfredställande säkerhet och uppnår också automatiserad utskjutning av dessa inställningar. Verksamheten får också en bättre överblick över säkerheten som helhet.

8.4 Avslutande ord

Sammanfattningsvis så påvisar denna studie att användningen av avancerade grafikkort i syfte att återställa lösenord har påverkat säkerheten i trådlösa nätverk som använder sig av WPA2-PSK. Det innebär även att en ökad risk även föreligger för verksamheten och dess medarbetare som använde sig av denna teknik. Därför bör verksamhetens medarbetare använda sig av medelsvåra och svåra lösenord som fortfarande anses vara säkra.

Verksamheten bör dock inte förlita sig på att enbart påtala detta utan också ansvara för att implementera detta. Därför rekommenderar denna studie att man delegerar ut säkerhetsarbetet kring de trådlösa nätverken som använder sig av WPA2-PSK till en leverantör som kan förse medarbetarna med tillfredställande säkerhet enligt verksamhetens krav. Det finns även andra säkerhetsåtgärder som tillbörligen kan tillämpas i verksamheten men dessa åtgärder faller utanför denna studies avgränsning och lämnas därför därhän.

Källförteckning

Litteratur

Barken L, Bermel E, Eder J, Fanady M, Mee M, Palumbo M, Koebrick A (2004). Wireless Hacking Projects for Wi-Fi Enthusiasts. USA, Syngress.

Carpenter T, Barret J (2008).CWNA Certified Wireless Network Administrator Official Study Guide. USA. Mc Graw Hill

Chandra P, Bensky A, Bradley T, Hurley C, Rackley S, Rittinghouse J, Ransome J, Stapko T, Stefanek G, Thornton F, Wilson J (2009). Wireless Security. USA, Newnes.

Gast M. The Definitive Guide. O´reilly.

Hurley C, Rogers R, Thornton F, Connelly D, Baker B (2007). Wardriving & Wireless Penetration Testing. Canada, Syngress.

Olsson, Fredrik (2007). Säkerhet i trådlösa nätverk. Lightning Source, Pagina.

Mitrovic P (2005). Handbok i IT-säkerhet. Scandbook Falun Sverige, Pagina

Rios B, Dhanjani N, Hardin B (2009). Hacking the next generation. USA, O´reilly.

Scambray J, MCclure S, Kurtz G. Hacking 6 exposed. USA, Mc Graw Hill.

Vladimirov A, Gavrilenko K, Mikhailovsky A (2004). Wi-foo . USA, Addison Wesley.

Internet

James Maxwell 2009-12-20
http://sv.wikipedia.org/wiki/James_Clerk_Maxwell

Hotspot 2009-12-20
http://en.wikipedia.org/wiki/Hotspot_%28Wi-Fi%29

IEEE 802.11 2009-12-20
http://en.wikipedia.org/wiki/IEEE_802.11

WEP 2009-12-20
http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

WPA WPA2 2009-12-20
http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

Wagners post 2009-12-20
http://www.cs.berkeley.edu/~daw/my-posts/my-rc4-weak-keys

Elcomsoft 2009-12-20
http://www.elcomsoft.com/ewsa.html

Password Calculator 2009-12-20
http://lastbit.com/pswcalc.asp

Hakin9 2009-12-20
http://www.hsc.fr/ressources/articles/hakin9_wifi/index.html.en

Wi-fi Net News 2009-12-25
http://wifinetnews.com/archives/2008/10/commercial_wpawpa2_cracking_software_accelerated_by_gpus.html

FBI 2010-02-14
http://www.smallnetbuilder.com/index.php?option=com_content&task=view&id=24251&Itemid=100

Wi-Fi Net News 2009-12-25
http://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html

Gigabyte GTX 260 2009-12-26
http://www.gigabyte.com.tw/Products/VGA/Products_Overview.aspx?ClassValue=VGA&ProductID=3129&ProductName=GV-N26OC-896I

Password memorability and security 2009-12-24
http://homepages.cs.ncl.ac.uk/jeff.yan/jyan_ieee_pwd.pdf

Graphical Passwords: A Survey 2009-12-24
http://www.acsac.org/2005/papers/89.pdf

Lösenordslistor 2009-12-27
www.laval.se/filer/passwordlists

Church of WiFi 2010-01-29
http://www.renderlab.net/projects/WPA-tables/

Laser 2010-02-12
http://en.wikipedia.org/wiki/Laser

Laser 2010-02-12
http://www.press.uchicago.edu/Misc/Chicago/284158_townes.html

Pyrit 2010-02-22
http://code.google.com/p/pyrit/

Rysk mjukvara knäcker lösenord med NVIDIAs grafikkort i rekordfart. 2010-04-12
http://www.nordichardware.se/index.php?news=1&action=more&id=14624

Bilaga 1. Begreppslista

WEP

Wireless Equivalent Privacy är en form av kryptering som numera anses vara föråldrad men som ändå går att finna implementerad och i drift än idag. WEP kryptering är relativt enkelt att förbigå men tillhandahåller ändå säkerhet för den oinvigde i dessa sammanhang. Det är trots allt bättre att ha kryptering än ingen alls. Dock om möjligheterna finns så rekommenderas WPA eller WPA2.

WPA

WiFi Protected Access är en form av kryptering som numera anses vara föråldrad, men dock säker. WPA2 har ersatt WPA.

WPA2

WiFi Protected Access är en form av kryptering som anses ge ett fullgott skydd. WPA2 är standarden som definieras i 802.11i som övertagit både WPA och WEP roll att tillhandahålla säker kommunikation.

SSID

Service set identifier, är namnet på det trådlösa nätverket. Detta sätts upp i accesspunkten.

EWSA

Elcomsoft Wireless Security Audit är namnet på programvaran som använts för denna studie.

Accesspunkt

Är självaste routern som handhar kommunikationen mellan nätverket och klienten.

Obehöriga

Är vad man uppfattar som hackers i vardaglig mening. Det är personer som olovligen tar sig in i de trådlösa nätverken i varierande syften.

IEEE

Organisationen IEEE är en internationell icke vinstdrivande organisation. Organisationen är lokaliserad i New York i USA. IEEE definierar organisationen som stödjande av utvecklingen inom en rad ämnen såsom det elektriska, elektroniska och datavetenskapliga med mera.

RC4

Inom kryptoområdet så kallas RC4 även för den så kallade RC4 för att undvika brott mot upphovslagen. Algoritmen är populär för att den är både snabb och enkel.

TKIP

WPA använder TKIP som är ett säkerhetsprotkoll. Anledningen till att man valde det för den nya standarden var att även TKIP använder sig av RC4 och gjorde därmed också sig kompatibel med den äldre standarden WEP.

AES

Krypteringsstandarden AES står för Advanced Encryption Standard. Denna standard är implementerad som ett säkerhetsprotokoll till den nya standarden WPA2.

PBKDF2

Funktionen PBKDF2 tillämpar en funktion där man skapa en krypterad nyckel från ett lösenord.

HMAC-SHA1

Konstruktionen HMAC-SHA1 används för att konstruera en MAC(Messege authentication code) som innebär att ett meddelande och en nyckel kan tas som input. Output blir en krypterad ström som skyddar både meddelandets integritet och dess äkthet.

Bilaga 2. Hårdvara och mjukvara

I laborationen bestod hårdvaran av följande huvudsakliga tekniska komponenter:

Processor	: Intel® Core™ 2 6600 @ 2.40 GHz
Bus	: 1066 MHz
RAM	: 4 Gb (667 MHz)
Grafikkort	: Gigabyte Nvidia GeForce GX 260

Mjukvaran som användes för att dekryptera lösenorden är från Elcomsoftware®.