Säkerhet i trådlösa nätverk

Jonas Karlsson och Richard Ingemannsen

2002-05-30

Institutionen för programvaruteknik och datavetenskap
BLEKINGE TEKNISKA HÖGSKOLA

Sammanfattning

Användandet av trådlösa nätverk ökar med rask takt och blir allt vanligare. Enligt en artikel i Computer Sweden kommer de trådlösa näten att ha 20 miljoner användare om 4 år. Analysföretaget Gartner Group har nyligen gjort en undersökning bland företag, vars syfte var att ta reda på hur stort intresset var för WLAN. Resultatet visade att 50% av företagen funderar på att köpa och installera WLAN-lösningar (Planet Wireless september 2001).

Syftet med detta arbete var att beskriva hur den inbyggda krypteringsfunktionen WEP som står för Wired Equivalent Privacy fungerar och hur säker den är, dvs hur lätt man kan knäcka krypteringen. Följande frågeställningar har besvarats genom litteraturstudier och ett praktiskt försök:

Hur är trådlösa nät uppbyggda?
Hur fungerar den inbyggda krypteringen WEP och hur säker är den?
Vad kan man göra förutom att använda sig av WEP för att skydda sig mot avlyssning/intrång?

Det praktiska försöket bestod av att knäcka WEP-krypterade filer med hjälp av programmet WEPCrack. Resultatet från detta försök visade att det var praktiskt möjligt att få fram den hemliga nyckeln.

Vi har fått bekräftat att vårt antagande, ”Baserat på de artiklar och tidningar vi har läst, antar vi att säkerheten i WLAN inte är tillfredsställande och nu vill vi på djupare plan ta reda på hur det ligger till med detta”, stämmer överens med den slutsats vi har kommit fram till. Slutsatsen är att WLAN är osäkra och att WEP går att knäcka.

Författare: Jonas Karlsson, it99jca@student.bth.se
Richard Ingemannsen, it99rin@student.bth.se
Examinator: Bengt Carlsson
Handledare: Bengt Carlsson
Huvudämne: Datavetenskap
Nivå: C
Poäng: 10
Datum: 2002-05-30

Summary

The use of Wireless networks is increasing rapidly and is becoming more and more common. According to an article in Computer Sweden, will the wireless networks have 20 million users in four years. The market analysis company Gartner Group has recently done a survey among companies, to find out the level of interest for WLAN. The result showed that 50% of the companies considering buying and installing WLAN-solutions (Planet Wireless, September 2001).

The purpose of this examination paper was to describe the built in encryption function WEP, that stands for Wired Equivalent Privacy works and how safe it is, in other words how easy it is to crack the encryption. The following questions has been answered through literature studies and a practical attempt:

How is Wireless Networks built-up?
How does the built in encryption WEP work and how safe is it?
What can you do besides using WEP to protect yourself against sniffing/intrusion?

The practical attempt consisted of cracking WEP-encrypted files with the program WEPCrack. The result from this attempt showed that it was practical possible to retrieve the secret key.

We have confirmed that our assumption, "Based on the articles and magazines we have read, we assume that the security in WLAN is not satisfying and now we want to examine this in a deeper level, match our conclusion. The conclusion is that WLAN is insecure and that WEP is crackable.

Authors: Jonas Karlsson, it99jca@student.bth.se
Richard Ingemannsen, it99rin@student.bth.se
Examiner: Bengt Carlsson
Advisor: Bengt Carlsson

Subject: Computer Science
Level: C
Points: 10
Date: 2002-05-30

Innehållsförteckning

1 INLEDNING

1.1 Bakgrund

Trådlösa nätverk är något som blir allt vanligare både för företag och privatpersoner. När produkter för trådlösa nätverk började komma ut på marknaden för några år sedan var överföringshastigheterna låga och olika tillverkares produkter stödde inte varandra. Nu finns det en standard framtagen av ”Institute of Electrical and Electronics Engineer” (IEEE) som är en standardiseringsorganisation. Överföringshastigheten har blivit mycket bättre och även kostnaden för installera ett WLAN (Wireless LAN) har blivit lägre. Alla dessa faktorer har bidragit till att WLAN nu anses av många företag som ett intressant alternativ till ett ”vanligt” LAN. Enligt en artikel i Computer Sweden kommer de trådlösa näten att ha 20 miljoner användare om 4 år. Analysföretaget Gartner Group har nyligen gjort en undersökning bland företag vars syfte var att ta reda på hur stort intresset var för WLAN. Resultatet visade att 50% av företagen funderar på att köpa och installera WLAN-lösningar (Planet Wireless september 2001). Baserat på de artiklar och tidningar vi har läst, antar vi att säkerheten i WLAN inte är tillfredsställande och nu vill vi på djupare plan ta reda på hur det ligger till med detta.

1.2 Syfte och frågeställningar

Syftet är att ta reda på hur säkert ett lokalt trådlöst nät är mot avlyssning/intrång. Det kommer vi att göra genom att beskriva hur den inbyggda krypteringsfunktionen WEP som står för Wired Equivalent Privacy fungerar och hur säker den är, dvs hur lätt man kan knäcka krypteringen. Vi kommer även att se på om det finns något mer att ta till förutom att använda WEP för att minska risken för avlyssning/intrång. För att läsaren lättare skall kunna ta till sig uppsatsen i sin helhet kommer vi i början av uppsatsen att ge en förklaring till hur WLAN är uppbyggda.

Följande frågeställningar kommer vi att besvara:

Hur är trådlösa nät uppbyggda?
Hur fungerar den inbyggda krypteringen WEP och hur säker är den?
Vad kan man göra förutom att använda sig av WEP för att skydda sig mot avlyssning/intrång?

2 METOD

Vi har utfört en explorativ undersökning där kunskap har inhämtats genom en mängd olika källor, dessa är:

- Vetenskapliga artiklar
- Tidningar
- Böcker
- Diskussionsgrupper och email
- Artikeldatabaser på Internet

Enligt Patel och Tebelius (1994) kan en explorativ undersökning genomföras för att generera intressanta frågor för framtida undersökningar. Likväl kan en explorativ studie ingå som en hypotesprövande undersökning, då man saknar viss information. Syftet med explorativa undersökningar är enligt Patel och Tebelius att inhämta så mycket information som möjligt om ett bestämt problemområde. Man kan också använda olika tekniker för att inhämta information i ämnet beroende på forskningsproblemet.

En deduktiv ansats har använts för att utifrån allmänna principer och befintliga teorier dra slutsatser hur säkert WEP är. Enligt Patel och Tebelius (1994) arbetar en deduktiv ansats efter ”bevisandets väg”. Ett praktiskt försök användes för att bevisa och verifiera vår teori och slutsats. Försöket bestod av att köra testdata i programmet WEPCrack, som finns att ladda ner från Internet.

Positivismen har varit vårt vetenskapliga förhållningssätt där vi har på ett logiskt, analytiskt och objektivt sätt relaterat till forskningobjektet. Positivismens ”fader” är den franske filosofen Auguste Comte (1798-1857). Han utvecklade vetenskapsfilosofin utifrån rötter i både upplysningstidens empiri och Aristoteles logik. Positivism som han kallade vetenskapsfilosofin skulle enligt Comte (Egidius 1986) bli en tredje våg i mänskligheten andliga historia, där den första vågen hade varit den religiösa och den andra den metafysiska. Comte lanserade själv beteckningen ”positivism” på denna ”tredje våg” i utvecklingshistorien (Egidius). Förebild för denna hämtades från naturvetenskapen, framför allt från fysiken. De centrala tankarna i positivism är enligt att det finns bara en sann verklighet som vi får vetskap om genom iakttagelser. Enligt Comte består allt av företeelser som förändras, kombineras och upplöses efter vissa givna matematiska lagar. Han menade att det finns bara en enda vetenskaplig metod: att matematiskt bearbeta säkert fastställda objektiva data.

I vår tid står oftast positivismen för krav på logiskt-rationellt tänkande samt noggrann prövning av teorier och påståenden. Egidius (1986) menar att Comtes grundtankar i stort står sig bra också i vår tid. Det bör dock uppmärksammas att ordet ”positivism” används i flera olika betydelser med olika grad av precisering. Vad som framför allt skiljer senare positivism från tidigare positivism är att kravet på verifikation har mildrats, eftersom det ofta är svårt att uppfylla. Kravet inom positivismen är att forskaren ska ta fram fakta som har hög grad av säkerhet – forskningen ska vara objektiv. (Egidius).

3 WLAN:S UPPBYGGNAD

3.1 Protokollarkitektur

IEEE 802.11b är den mest kända WLAN standarden idag, vilket man även kan kalla trådlöst Ethernet. Man ser på numret att IEEE 802.11b standarden tillhör 802.x familjen. Detta innebär att man har samma interface för att få tillgång till de högre lagren i protokollstacken. Den tekniska standarden 802.11b täcker in det fysiska lagret (FYS) och media access lagret (MAC) vilket alla 802.x standarder gör.

Här nedan visas en figur över hur protokollets arkitektur är uppbyggt. Vi har valt att även visa standarden 802.3 för att belysa kompatibiliteten mellan de olika standarderna i 802.x familjen.

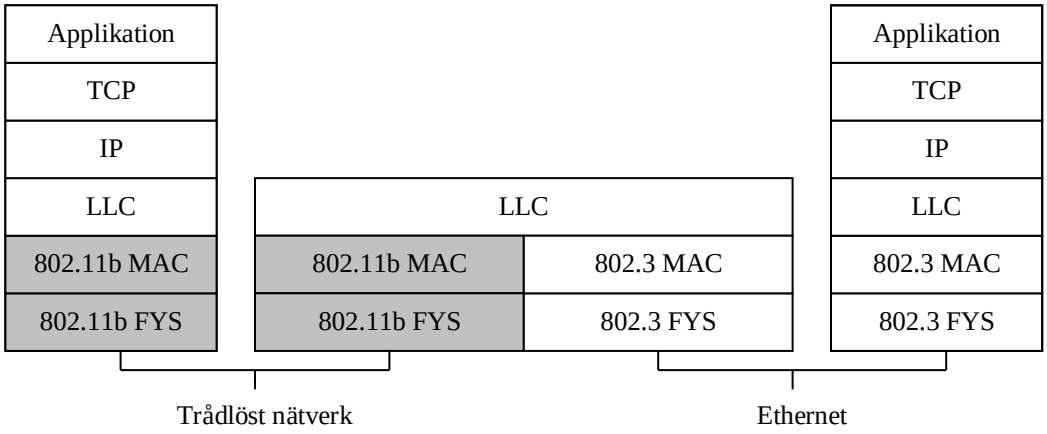

Bild.3.1 IEEE 802.11b protokollets arkitektur.
LLC - Logical Link Control, IP – Internet Protocol, TCP – Transfer Control Protocol

3.1.1 Fysiska lagret

IEEE802.11b stödjer tre olika fysiska lager. Ett av lagren är för infraröda signaler och de andra två är för olika radiobaserade signaler. Samtliga tre varianter använder sig av en s k Clear Channel Assessment (CSA) signal. Detta är en signal som kontrollerar om mediet är upptaget eller fritt för att sända.

3.1.2 MAC-lagret

MAC-lagret har flera uppgifter. Den primära uppgiften är att kontrollera accessen till det specifika mediet. MAC-lagret kan även användas för behörighetskontroll, strömsparande och flytt av enheter. De grundläggande tjänster som MAC-lagret erbjuder är den obligatoriska asynkrona data tjänsten och den valfria tidsbundna tjänsten. Den asynkrona tjänsten stödjer ”broadcast” och ”multicast” paket. MAC mekanismerna kallas också för DFWMAC (Distrubuted Foundation Wireless Medium Access Control).

Det finns tre olika accesmekanismer definierade i IEEE802.11b:

- DFWMAC-DFC - CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)
- DFWMAC-DCF - RTS (Request to Send)/CTS (Clear to Send)
- DFWMAC-PCF (polling)

4 KRYPTERING

4.1 WEP

Som vi har nämnt tidigare står WEP för Wired Equivalent Privacy och är en inbyggd krypteringsfunktion som finns i WLAN av standarden 802.11 och 802.11b. WEP arbetar på de två lägsta lagren i OSI-modellen, vilka är datalänk och det fysiska lagret och som resultat av detta erbjuder inte WEP en end-to-end lösning. Syftet med WEP när det togs fram var att få en likvärdig säkerhet i WLAN som i vanliga Ethernet nät genom att skydda den trådlösa länken mellan centralenheterna och klienterna.

Detta innebär att WEP skulle hindra att attacker där personer utrustade med bara enkel utrustning, dvs bärbar dator, ett WLAN nätverkskort och en programvara installerad för avlyssning skulle kunna ta sig in i och avlyssna trafiken i näten. Med andra ord skulle WEP göra så att det skulle krävas stora resurser och arbetsinsatser att komma åt hemlig information i näten precis som i ”vanliga” Ethernet nät. Även om WEP långt ifrån är en säker lösning är det bättre att använda WEP än ingenting alls, men vill man ha en riktig säker lösning får man kombinera WEP med andra säkerhetslösningar (se avsnitt 6).

Man kan säga att det finns tre mål med WEP.

- **Konfidentialitet**

Detta går ut på att förhindra stor del av tänkbar tjuvlyssning.

- **Åtkomstkontroll**

Här handlar det om att förhindra åtkomst till den trådlösa nätverksstrukturen.
Det finns en funktion i 802.11b som fungerar på så sätt att den kastar ut alla paket som inte är korrekt krypterade med WEP. Det är denna funktion som produkttillverkare marknadsför som åtkomstkontroll.

- **Dataintegritet**

Dataintegritet går ut på att förhindra att någon kan förändra innehållet i meddelanden som sänds. I WEP uppnås detta genom att en integritetskontrollsumma c(M) används.

Trots att WEP är lätt att använda är det väldigt många företag som inte använder det enligt olika undersökningar som har gjorts. Detta gäller både i Sverige och i övriga världen. Bl a har RSA Security tillsammans med konsultföretaget Orthus gjort en praktisk undersökning i Londons innerstad genom att promenera runt med en bärbar dator, ett nätverkskort och två gratisprogram. Resultatet de kom fram till var att bara 41 av de 124 nät de undersökte var krypterade med WEP. Ett grundläggande problem med WEP är att samlar man tillräckligt med data återkommer startvektorn(IV) och det går att knäcka krypteringen. Hur lång tid detta tar varierar. Är hastigheten på nätet hög tar det oftast inte mer än några timmar innan man har samlat tillräckligt med data för att få det antal ”intressanta” paket som man behöver för att dekryptera.

WEP finns både som 40 och 128 bitars RC4-kryptering. Det fullständiga namnet är egentligen RC4 PRNG vilket står för ”Ron´s Code 4 Pseudo Random Number Generator”. Enligt en artikel i tidningen Datormagazin som heter ”Säkra ditt trådlösa nätverk” finns båda dessa alternativ p.g.a.

att för 128-bitars kryptering finns exportrestriktioner från USA. Tidningen Nätverk och Kommunikation i artikeln ”Teknikanalys” säger i och för sig att denna lagstiftning nu är ändrad. Egentligen är det rätta att säga 40 bitars och 104 bitars kryptering för i realiteten är 128 bitars en 104 bitars men anges oftast som 128 bitars kryptering. Det händer även att 40 bitars kryptering kallas 64 bitars av en del leverantörer men det är inte lika ofta. De 24 bitarna(IV) utöver 40 och 104 bitar skickas som en inledning i kryptot och är automatiskt genererade. Det användaren själv kan ställa in är därmed antingen 40 eller 104 bitar.

40 bitars krypteringen går att knäcka genom en ”brute force-attack”. Vilket betyder att man genom en direktattack slumpar lösenord tills man lyckas hitta rätt. För att knäcka 104 bitars versionen krävs alternativa angreppssätt. Dessa lösningar går självklart att även använda på 40 bitars krypteringen. Det olika angreppssätt som finns presenteras lite längre fram under denna rubrik. Det finns inte definierat i standarden för WEP hur nycklarna skall skapas och distribueras, men när man har lyckats knäcka WEP och fått en nyckel är de normala 802.11b-näten uppbyggda så att man kan nå hela nätet eftersom samma nyckel används i alla ingående stationer. Egentligen skulle mycket bättre tekniker för nyckelhantering kunna användas men tyvärr finns inget stöd i de kommersiella system som finns på marknaden för en sådan hantering. Nycklarna är alltså gemensamma för alla och dessutom är de statiska, vilket innebär att de inte ändras över tiden. För att skydda nätet på nytt efter att någon har knäckt krypteringen och fått fram nyckeln krävs att alla nycklar byts ut manuellt på alla nätverkskort.

Ett antal företag, bl a Microsoft och Cisco arbetar med ett standardförslag som heter 802.1X. 802.1X skall fungera både för WLAN och för vanligt Ethernet. En av de saker som är bra med denna standard är att nycklarna kommer att bytas ut automatiskt efter en tid genom ett förbestämbart schema. Det är även föreslaget inom detta standardförslag att öka säkerheten vid inloggning av användaren genom bättre behörighetskontroll. T.ex. skulle Kerberos eller RADIUS kunna användas för detta ändamål (Se avsnitt 6.5 och 6.6).

802.1X ingår inte i standardiseringsorganet IEEE:s arbete att förbättra WEP där en ny standard för trådlösa nät kallad IEEE802.11i håller på att arbetas fram. I IEEE802.11i är det föreslaget att en ny standard för WEP kallad WEP2 skall finnas. I WEP2 kommer fortfarande RC4 algoritmen att användas men i annan form, förmodligen som en rullande 128 bitars algoritm baserad på RC4. Även WEP2 kommer troligen att erbjuda alldeles för dålig säkerhet. Det är inte omöjligt att 802.1X kommer bli en ingående del i 802.11i. En arbetsgrupp i IEEE arbetar även med ett annat förslag. Förslaget går ut på att använda en algoritm på 128 bitar som heter AES. Fördelen med WEP2 jämfört med AES är att för att kunna använda AES krävs ny hårdvara, medan för WEP2 räcker det att bara ladda ny firmware(det är en mjukvara som går att uppdatera men inte att ändra och ligger i själva hårdvaran) för att uppgradera 802.11b kortet.

4.1.1 Krypteringsprocessen i WEP

Man använder algoritmen CRC-32 för att beräkna integritetskontrollsumman c(M), där M är meddelandet. Dessa länkas sedan samman för att skapa klartexten P=(M, c(M)). Därefter krypterar man P med den symmetriska(samma nyckel används för kryptering och dekryptering) algoritmen RC4. En startvektor(Initialization Vector-IV) v väljs. Det genereras sedan en nyckelström som en funktion av v och den hemliga krypteringsnyckeln k, som anges som RC4(v,k). Ciphertexten(krypterad klartext) fås genom att använda funktionen XOR mellan klartexten och nyckelströmmen. XOR(exclusive or)är en matematisk funktion.

> ”XOR betecknar inom programmering en exklusive disjunktion eller exklusivt or. Det står alltså för ”A eller B men inte båda”. Alla andra logiska villkor kan skrivas om till kombinationer av XOR-villkor. XOR används också för kryptering. Texten som ska kodas jämförs i binär form med nyckeln i binär form, bit för bit. Om det råkar finnas samma tecken i klartexten och nyckeln sätts en nolla- om det är olika tecken sätts en etta. Exklusive disjunktion är för övrigt i formell algebra detsamma som ”A eller B men inte båda”.”
> Nätverk och kommunikation

Slutligen sänds ciphertexten och IV:n över radiolänken.

Krypteringsprocessen ser ut grafiskt på följande sätt

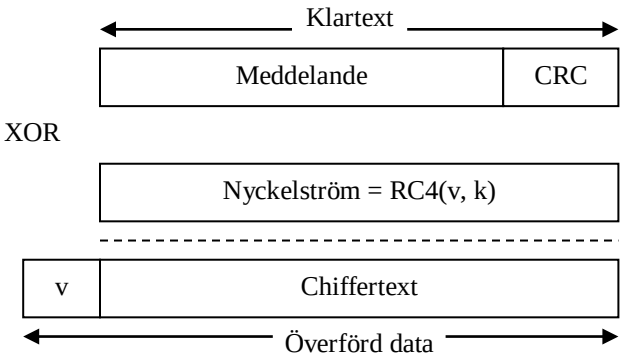

Bild 4.1 Krypterad WEP ram.

Exempel på hur XOR ser ut:

A	**0 0 1 1**
B	**0 1 0 1**
UT	**0 1 1 0**

Bild 4.2 A=Klartext, B=Nyckelström, UT=Chiffertext(krypterad klartext).

För att dekryptera görs samma sak fast omvänt. Som nämnts tidigare har mottagaren samma nyckel som sändaren (RC4 är en symmetrisk algoritm). Dekryptering går alltså till så att mottagaren använder sin nyckel för att generera nyckelströmmen. XOR används mellan

nyckelströmmen och ciphertexten och på så sätt fås klartexten P. P delas upp i M och c, därefter beräknas c(M) som jämförs med den mottagna checksumman c för att se om meddelandet har ändrats under överföringen.

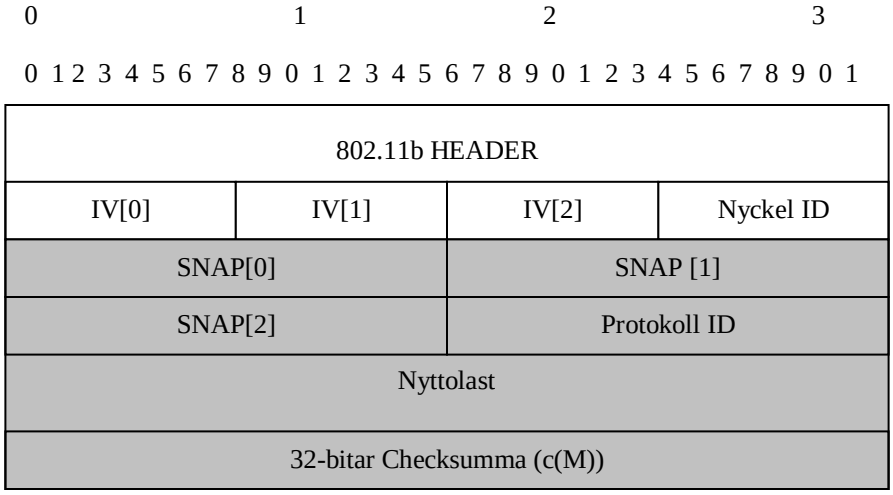

Bild 4.3 Paketens innehåll.
(De fält som är markerade med grått utmärker den krypterade delen av paketet.)
SNAP - Sub-Network Access Protocol

4.1.2 Attacker för att knäcka WEP

- *Passiv attack för att kryptera trafik*

Eftersom IV:n är på 24 bitar tar det inte mer än 5 timmar att gå igenom alla IV-kombinationer om centralenheten sänder med en hastighet på 11Mbps vilket är maxhastigheten. Den verkliga hastigheten är i och för sig oftast lägre än maxhastigheten p.g.a. faktorerna overhead och paketkollisioner. Detta innebär att det kan ta upp till 12 timmar innan en nyckelström återanvänds. När en IV-kollision inträffar kan attackeraren XOR:a två paket som använder samma IV och få ut XOR:en från de två klartextmeddelandena. Denna resulterande XOR kan användas för att dra slutsatser om innehållet i de två meddelandena. IP-trafiken är ofta lätt att förutsäga och innehåller mängder av redundans. På så sätt kan attackeraren utesluta olika varianter för innehållet i meddelandena. Genom vidare kvalificerade gissningar om innehållet i ett eller i båda meddelandena kan man statistiskt reducera möjliga varianter. Om det inte räcker med två meddelanden för att dra en slutstats kan attackeraren leta efter fler kollisioner med samma IV.

En variant på denna attack finns. Attackeraren sänder trafik utanför WLAN:et till centralenheten. När attackeraren snappar upp ciphertexten kan han återskapa nyckelströmmen genom att han även vet klartexten, det var ju han som skapade den.

- *Aktiv attack för att lägga in ny trafik*

Denna attack bygger på problemen presenterade i föregående attack. Om en attackerare vet den exakta klartexten för ett meddelande, kan han använda denna kunskap till att skapa korrekt krypterade paket. Det går till på så sätt att man skapar ett meddelande, beräknar en CRC32 och

utför bitförändringar på det ursprungliga krypterade meddelandet för att ändra klartexten till det nya meddelandet. Paketen skickas till centralenheten eller till en klient och det kommer att accepteras som ett giltigt paket.

Det går att göra denna attack ännu mer lömsk genom en mindre modifiering. Även utan fullständig kunskap om ett paket är det möjligt att ändra valda bitar i ett meddelande och på ett lyckosamt sätt justera den krypterade CRC:en, för att erhålla en korrekt krypterad version av ett modifierat paket. Om en attackerare har delvis kunskap om innehållet i ett paket kan han uppfatta det och utföra vissa modifieringar av det.

- *Aktiv attack för att dekryptera trafik*

Denna attack är en utökning av ovanstående attack och den kan användas för att dekryptera vilken trafik som helst. Antag att attackeraren spekulerar enbart om ramens header och inte själva innehållet. Det är relativt enkelt att gissa eller få reda på denna information, det räcker faktiskt att gissa mottagarens IP-adress. Om attackeraren känner till IP-adressen kan han modifiera lämpliga bitar för att ändra mottagaradressen till IP-adressen på en dator ute på Internet som han själv kontrollerar. Då kan paket dekrypteras av centralenheten och sändas som klartext till attackerarens maskin. Även om centralenheten är belägen bakom en brandvägg, går det oftast att komma igenom, för om man lyckas att gissa TCP-huvudet på paketet går det att ändra destinationsporten på paketet till port 80(HTTP).

- *Tabellbaserad attack*

Genom att det inte finns så många möjliga IV-kombinationer går det att bygga upp en dekrypteringstabell. När en attackerare har fått fram klartexten av ett paket kan han beräkna RC4-nyckelströmmen som genereras av den använda startvektorn. Denna nyckelström kan användas för att dekryptera alla andra paket som använder sig av samma IV. Efter en tid kan då kanske attackeraren genera en tabell av IV:s och motsvarande nyckelströmmar. Denna tabell kan bestå av upp till 16 miljoner (2^{24}) värden och storleksmässigt inte vara större än 24 GB. Om en attackerare har lyckats att bygga en dekrypteringstabell kan han dekryptera alla paket som sänds över den trådlösa länken.

4.1.3 RC4

RC4 består till huvudsak av två delar, dels en algoritm(KSA, Key Scheduling Algoritm) som ändrar en slumpvis vald nyckel till en inledande permutation S av {0,…,N-1}, och dels av PRGA(PRGA, Pseudo-Random Output Sequence) som använder denna permutation för att generera en slumpvis falsk utskrifts sekvens[1]. PRGA börjar med att initiera två index *i* och *j* till 0. Därefter ”loopar” den igenom fyra enkla operationer

1 sätter *i* som räknare.
2 sätter *j* som slumpvis falsk.
3 byter de två värdena S besitter genom variablerna *i* och *j*.
4 Skriver ut värdet av S som tagits fram med hjälp av variablerna *i* och *j*.

[1] Fluhrer, S. , Mantin, I. och Shamir, A. *Weakness in the Key Scheduling Algoritm of RC4* , s.2. http://www.wisdom.weizmann.ac.il/~itsik/RC4/Papers/Rc4_ksa.ps

KSA består av N antal loopar som liknar de operationer som finns i PRGA. KSA initierar S som permutation och sätter variablerna *i* och *j* till 0. KSA använder sedan PRGA:s operation N antal gånger, går igenom S, uppdaterar j genom att lägga till S(i) och nyckelns nästa ord (i cyklisk ordning). Varje runda av KSA kallas steg[2]. Figuren här nedan visar alla steg som de två delarna av RC4 utför.

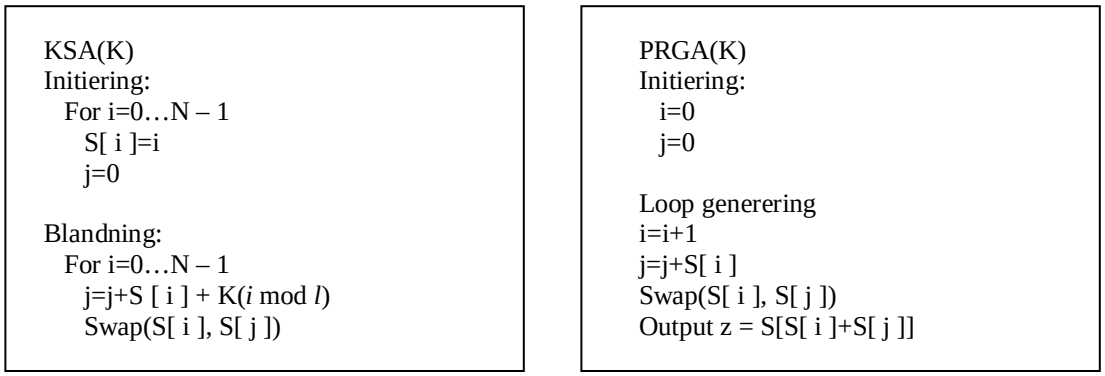

Bild 4.4 Key Scheduling Algorithm (KSA) och Pseudo-Random Generation Algorithm (PRGA)
l är antalet ord av K (nyckeln), där varje ord består av n bitar.

RC4 är som vi nämnt tidigare, ett symmetriskt ström chiffer och använder samma nyckel vid kryptering som vid dekryptering. Detta gör att alla som kan kryptera också kan dekryptera ett meddelande, vilket gör att man måste vara mycket försiktig med nyckeln om man vill uppnå hög säkerhet.

Fördelar med symmetriska chiffer är att de är mycket snabba och det är teoretiskt möjligt att konstruera chiffer som är oknäckbara. En stor nackdel är att det är samma nyckel vid kryptering som vid dekryptering. Sändaren XOR:ar nyckelströmmen med klartexten för att skapa chiffertexten. Mottagaren har en kopia av samma nyckel, och använder den till att skapa en identisk nyckelström. XOR:ar nyckelströmmen med chiffertexten vilket ger klartexten i ursprungsformatet. En känd svaghet när det gäller strömchiffer är att om kryptering av två paket sker med samma initieringsvektor(IV), kan nyckeln avslöja information om båda meddelandena[3].

Om $C_1 = K_1$ XOR RC4(v, k)
Och $C_2 = K_2$ XOR RC4(v, k)

Blir C_1 XOR $C_2 = (K_1$ XOR RC4(v, k)) XOR (K_2 XOR RC4(v, k)) = K_1 XOR K_2

Detta innebär att när man XOR:ar de två chiffertexterna (C1 och C2) tillsammans gör att de två chiffertexterna tar ut varandra och resultatet blir XOR av de två meddelandenas klartext K_1 och K_2 .

[2] Fluhrer, S. , Mantin, I. och Shamir, A. *Weakness in the Key Scheduling Algoritm of RC4* , s.3. http://www.wisdom.weizmann.ac.il/~itsik/RC4/Papers/Rc4_ksa.ps
[3] Borisov, N., Goldberg, I., Wagner, D., Intercepting Mobile Communications: The Insecurety of 802.11. s.3.

5 PRAKTISKT FÖRSÖK

5.1 Fas 1: Beskrivning av försöket

Syftet med detta försök är att bevisa att teorin som vi presenterat i denna uppsats för att knäcka WEP går att tillämpa praktiskt. För att åstadkomma detta använder vi oss av ett program som finns tillgängligt på Internet. Vi vill poängtera att vi inte har sniffat något trådlöst nätverk, utan använt oss av filer vi fått (se fas 2).

5.2 Fas 2: Förberedelser inför försöket

Vi började med att titta på vilka program som var tillgängliga på Internet. Vid den tidpunkten, i början av februari 2002, fanns två program släppta till allmänhetens förfogande. Dessa var dels WEPCrack som var det första programmet för att knäcka WEP och dels AirSnort. WEPCrack version 0.0.10 släpptes den 12 augusti 2001 och är fortfarande den enda publicerade versionen. AirSnort version 0.0.9 släpptes ungefär en vecka efter WEPCrack och har uppdaterats två gånger, dels som version 0.1.0 den 2 september 2001 och dels den 28 februari 2002 som version 0.2.0. Den senare versionen är utrustad med ett grafiskt gränssnitt.

Vi satte oss in i WEPCrack som vi valde att använda oss av på grund av att WEPCrack är ett rent crackningsverktyg medan AirSnort är en kombination av sniffning- och crackningsverktyg.

Nästa steg var att försöka hitta testmaterial för vårt försök. Detta gjorde vi genom att lägga ut förfrågningar i olika diskussionsforum med inriktning mot trådlös säkerhet. Vi emailade även ett antal personer, bl a skaparna bakom WEPCrack och Airsnort. Utöver detta så gjorde vi en omfattande sökning på säkerhetssidor, hackersidor och crackersidor efter testmaterial.

5.2.1 Beskrivning av WEPCrack:

WEPCrack består av fyra skript skrivna i programmeringsspråket Perl. Verktyget är en implementation av attacken som beskrivs i artikeln ”Weaknesses in the Key Scheduling Algorithm of RC4” av Fluhrer, Mantin, och Shamir.

Här nedan beskriver vi hur de fyra olika skripten används:

- WeakIVGen.pl – Detta skript möjliggör simulering av hur IV-krypterad output kan se ut när man avlyssnar en basstation.

- prism-getIV.pl – Detta skript använder sig av dump-filer för att hitta svagheter i IV:na. Alla svaga IV:s som hittas läggs i en loggfil (IVFile.log) tillsammans med den första krypterade output byten.

- WEPCrack.pl – I detta skript används filen IVFile.log, som genererades när Prism-getIV.pl kördes, för att få fram den hemliga nyckeln genom att använda erhållna svaga IV:s tillsammans med den krypterade outputen.

- prism-decode.pl – Detta skript används för att avkoda 802.11 ramar.

Vi kommer i vårt försök enbart att använda oss av skripten prism-getIV.pl och WEPCrack.pl.

5.3 Fas 3: Genomförandet och resultat av försöket

Vi började med att installera Mandrake Linux med kernel 2.2 eftersom WEPCrack endast fungerar i Linux. Sedan installerade vi WEPCrack genom att packa upp programfilen, och erhöll då fyra skript. Skripten är redo att exekveras och behöver inte konfigureras. Efter att ha studerat de olika skripten kom vi fram till att endast två av skripten är intressanta för vårt försök, nämligen prism-getIV.pl och WEPCrack.pl.

Till en början fick vi tag endast i en testfil. Denna fil körde vi med skriptet prism-getIV.pl och en IVLogg-fil ska skapas. Flera försök utfördes men resultatet var inte som det skulle vara. Den IVLogg som skapades innehöll antingen 0- eller 2 byte. Detta innebar att det inte placerades några svaga IV:s i loggfilen.

Vi hade till en början två teorier om varför försöket inte gav önskat resultat. Den första teorin var att filen innehöll för lite intressanta paket. Detta medförde att vi på nytt sökte efter testmaterial enligt den beskrivningen som ges i Fas 2. Efter en veckas sökande utan resultat började vi parallellt med sökandet efter fil, att testa vår andra teori. Den teorin gick ut på att vi behövde version 2.4 av Kerneln. Information om vilken Kernel version WEPCrack behöver för att kunna köras existerade inte. Denna teori baserade vi dock på att AirSnort kanske kräver Kernel 2.4 enligt skaparna av programmet. Efter mycket om och men, så lyckades vi att uppgradera Kerneln. Därefter testade vi den första testfilen med den nya Kernel versionen, men fick samma resultat som innan.

Vi erhöll strax efter detta en ny testfil, men den gav samma resultat som i de föregående försöken. Vi började ana att det var något annat med filerna som inte stämde. För att få besked på vad som var fel söktes efter information som kunde bekräfta vår teori. Efter en tids sökande hittades ett antal inlägg i ett diskussionsforum där problemet togs upp. Det ligger till så att det finns olika typer av libpcap data. Hur datan ser ut beror på vilket nätverkskort som har använts vid sniffningen. Vissa typer av nätverkskort lägger till leverantörsspecifika ”driver headers” i paketen medan andra inte gör det. WEPCrack klarar inte de libpcap paket som har ”driver headers”.

För att kunna använda WEPCrack behövs alltså att man använder rätt kort vid sniffningen, så att man får rätt format på datan i paketen. Med denna vetskap till hands kunde vi specificera vilken typ av fil vi ville ha. Vi lyckades få tag på några filer med det rätta formatet. Därefter testade vi att köra prism-getIV.pl på nytt. Nu skapades en IVLogg-fil på 44 Kbyte. Nästa steg var att exekvera skriptet WEPCrack.pl på IVLogg-filen. Detta skript genererade den hemliga nyckeln. Den var på 128-bitar (104-bitar), vilket innebär det hexadecimala formatet xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx. Varje ”xx” motsvarar 8-bitar, dvs nyckeln är på 13*8=104-bitar.

6 ÅTGÄRDER FÖR ÖKAD SÄKERHET

Det finns flera olika tekniker för att skydda sig och bekämpa eventuella attacker på WEP. De tekniker som idag finns är bl a VPN, IPSec, SSL, SSH och autentiseringsmekanismer som Kerberos och RADIUS.

6.1 VPN

VPN står för virtuella privata nätverk och är ett brett koncept snarare än en specifik teknik eller protokoll, men det innebär i huvudsak tunnling av privata data via Internet med valfri kryptering. Fördelen med VPN är att det är en relativt billig och bekväm lösning. Genom att utnyttja redan befintliga Internet-anslutningar för kommunikation med andra användare kan man minska kostnaderna.

VPN-lösningar kan se ut på en mängd olika sätt. Tunnling innebär inkapsling av ett eventuellt krypterat datagram inom ett annat. Det kan t.ex. vara IP inom IP.

I bilden nedan illustrerar vi tunnlingskonceptet i ett VPN mellan enheterna A och B. Dessa kan i verkligheten utgöra enskilda värddatorer eller hela kompletta nätverk. B skickar ett paket till A via Gateway 2 (GW2). Gateway 2 kapslar in paketet i ett annat paket med destinationen Gateway 1 (GW1). Gateway 1 tar bort det tillfälliga huvudet och levererar originalpaketet till A. Originalpaketet kan krypteras över Internet.

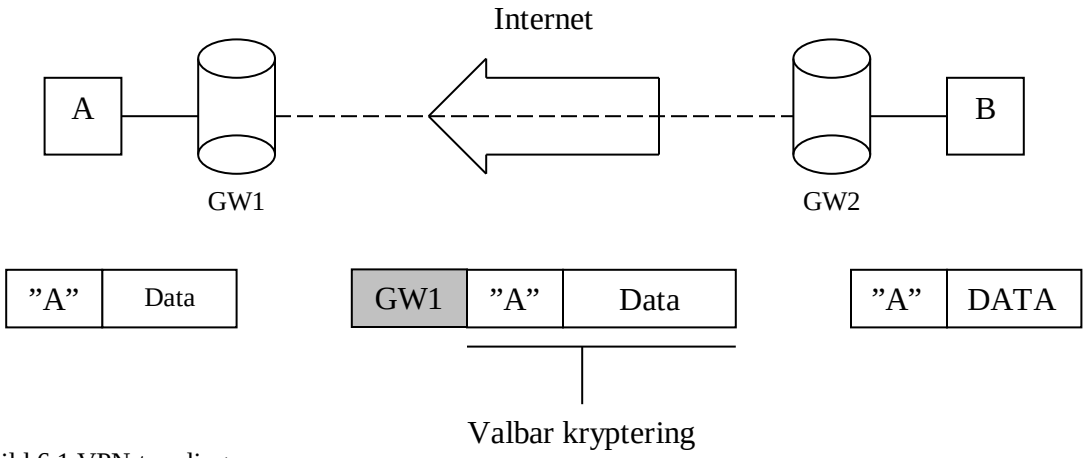

Bild 6.1 VPN-tunnling

Under senare år har VPN-tekniken utvecklats starkt och idag används den i allt högre utsträckning i både offentliga som privata nätverksarkitekturer. Olika operatörer erbjuder administrerade VPN-lösningar för organisationer och företag som inte vill eller har kunskapen att bygga egna.

6.2 SSH

SSH (Secure Shell) är ett program som används för att på ett säkert sätt logga in på datorer i nätverk. SSH kan även användas för att flytta filer från en maskin till en annan. Till skillnad från äldre program, som skickade all information i klartext som t. ex. Telnet, så använder SSH kryptering vid överföringen.

SSH tillhandahåller en stark autenticering och säker kommunikation över osäkra kanaler. Ofta används inte kryptering vid kommunikation över datanätverk. Det betyder att vem som helst som har tillgång till en dator ansluten till nätverket kan lyssna på all kommunikation.

6.3 IPSec

Det behövs kanaler för säker trafik över Internet. Den standard som blivit dominerande för detta ändamål heter IPSec (IP Security). IPSec är en standard som föregriper säkerhetsfunktionen i IP version 6. IPSec krypterar och autenticerar trafiken vilket gör att det lätt att bestämma vem som ska kunna läsa vad.

Protokollet IPSec täcker följande huvudområden:

- autenticering av avsändaren så att varje paket kan garanteras komma från den avsändare som uppges
- autenticering av data (data integrity) så att varje paket kan garanteras vara i oförändrat skick när det kommer fram; detta skyddar både mot tekniska fel och uppsåtligt sabotage
- kryptering som döljer innehållet i paketen
- skydd mot "återuppspelning" av data, så att det inte går att "spela in" en avlyssnad sekvens som sedan "spelas upp"
- automatiserad hantering av kryptonycklar och säkerhetsassociationer för att möjliggöra en flexibel implementering av VPN

De viktigaste protokollen som används av IPSec är Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE).

6.4 SSL

SSL(Secure Sockets Layer) är ett av de viktigaste och mest använda protokollen för datasäkerhet på Internet. SSL stöds i både Netscape och Internet Explorer. SSL protokollet är ursprungligen utvecklad av Netscape. SSL protokollet ger möjlighet för en klient/server applikation att kommunicera på ett sätt som inte kan avlyssnas och tjuvläsas.

Protokollet upprättar en så kallad säker kanal (secure channel) i vilken informationen transporteras. Denna kanal har tre huvudsakliga egenskaper. För det första är all information som skickas över kanalen krypterad. För det andra så är kanalen autenticerad, vilket innebär att både servern och klienten är autenticerade. För det tredje sker en integritetskontroll på all transport av meddelanden vilket gör att den är pålitlig.

6.5 Kerberos

Kerberos har sitt ursprung från mitten av 80-talet och har länge varit en vanlig säkerhetslösning inom UNIX-världen, men används även i Windows 2000 och XP där det är det standardiserade protokollet för behörighetskontroll. Kerberos använder sig av en databas där klienternas hemliga nycklar finns lagrade. Om klienten är en användare är den hemliga nyckeln ett krypterat lösenord.

Grundtanken i Kerberos är att låta en Kerberosserver autenticera användaren med användarnamn och lösenord istället för att användarna skall behöva autenticera sig för varje server eller tjänst i nätverket. Efter att användaren har autenticerat sig får han en biljett av Kerberosservern som ger

access till nätet, dvs. accesspunkterna. Biljetten har en viss giltighetstid och eftersom den ger tillgång till alla accesspunkter under denna tid uppstår inga problem med reautenticering vid byte till en annan accesspunkt.

Det finns flera fördelar med Kerberos, bl a dynamiskt nyckelbyte vilket innebär att det går att byta ut nycklarna automatiskt efter ett tidsintervall som systemadministratören har bestämt.

6.6 RADIUS

RADIUS står för Remote Authentication DIAL-in User Services. RADIUS är alltså ett autenticeringssystem för uppringda förbindelser. När man använder RADIUS i trådlösa nät är man tvungen att komplettera lösningen med olika tillägg beroende på att RADIUS egentligen inte är anpassat för trådlösa nät. Exempel på brister med RADIUS är att det saknas funktioner för automatisk växling av nycklar och ömsesidig autenticering som Kerberos erbjuder, så det måste lösas på annat sätt.

7 DISKUSSION

När vi började arbeta med detta examensarbete var våra kunskaper om säkerhet i trådlösa nät begränsade. Detta innebar att vi de första sex veckorna nästan enbart fick ägna oss åt litteraturstudier. Trots att området ”säkerhet i trådlösa nätverk” är nytt, var det relativt lätt att hitta information. När vi kände att vi hade inhämtat tillräckligt med information om ämnet, började vi med det praktiska försöket.

7.1 Problem med WEP

Skillnaden mellan 40- och 128-bitars kryptering är att den förra går att knäcka med en ”brute-force-attack”. Som vi har visat i vårt försök har denna skillnad i realiteten ingen betydelse, eftersom det går att utnyttja IV:n för att knäcka WEP. På grund av att storleken på IV:n är 24-bitar både vid 40- och 128-bitars kryptering är dessa lika lätta att knäcka med denna attackmetod. Med andra ord har det ingen betydelse hur många bitar den krypterade texten är på, utan det är längden på IV:n som avgör hur svårt det är att knäcka WEP. Till exempel skulle en 256-bitars kryptering bestående av 232-bitars chiffertext och 24-bitars IV inte försvåra knäckningen.

7.2 Förslag till ny standard

Baserat på de problem vi tog upp i föregående stycke har vi förslag till en ny standard. Denna standard borde innehålla:

- Ökad längd på IV:n
- Nyckelhantering
  - med automatik schemalagt nyckelbyte

Hur stor IV:n måste vara beror på hur ofta ett nyckelbyte sker. Attacken bygger ju på att man samlar tillräckligt med paket som innehåller återkommande IV, krypterade med samma nyckel. Nackdelen med utökad IV är att overheaden (allt utöver datan) blir större i varje paket. Detta innebär att överföringstiden blir längre.

7.3 Praktiska försöket

WEPCrack är ett bra verktyg att använda sig av såvida man vet vilket format datan har, som man ska knäcka, och få fram nyckeln. Dvs innan man skall sniffa ett trådlöst nät, bör man ta reda på vilket nätverkskort man använder. Är man osäker på om kortet kommer ge rätt format på datan som WEPCrack kräver, kan man använda AirSnort. AirSnort stödjer de flesta format, men kräver större Linux kunskaper för installation.

Som vi har nämnt tidigare krävs det bara en bärbar dator utrustad med trådlöst nätverkskort och program för sniffning för att samla data. En person kan sitta utanför ett företags byggnad med denna utrustning i några timmar, tills det att tillräckligt med information har inhämtats. Därefter kan personen ifråga använda sig av WEPCrack för att få fram den hemliga nyckeln. Denna hemliga nyckel ger tillgång till den information som sänds, ända tills att nyckeln byts, vilket inte sker så ofta. Detta innebär att en obehörig kan få tillgång till hemlig företagsinformation.

7.4 Publicering av verktygen
Som vi ser det är det en fördel att WEPCrack och AirSnort har publicerats till allmänhetens förfogande. På grund av den mediala uppmärksamhet detta inneburit, har säkerhetsmedvetandet hos företag som har eller som ska investera i trådlösa nät förbättrats. Förmodligen kommer detta medföra att utvecklare av nya standarder och leverantörer av trådlösa nät, prioriterar säkerhetstänkandet högre.

7.5 Framtiden
Med tanke på att det nu arbetas med flera förslag, både inom IEEE och även inom vissa företag med att ta fram nya standarder för trådlösa nät och WEP, är det svårt att sia om hur säkra trådlösa nät kommer att vara om t. ex. 1 år. Men en sak är säker, säkerheten i trådlösa nät kommer att förbättras efter hand hela tiden, för att till slut med all sannolikhet erbjuda likvärdig säkerhetsnivå som trådbaserade nät. Detta tror vi innebär att trådlösa nät, i en inte allt för avlägsen framtid kommer vara lika vanligt som trådbaserade nät, för att till slut passera trådbaserade som den mest frekvent använda tekniken för överföring av data i lokala nät.

Något som företaget bör tänka på, innan de tar ett trådlöst nät i drift, är att göra en fullständig analys över säkerhetsriskerna. Det första man måste ta reda på är vilken typ av information som skall skickas över det trådlösa nätet. Därefter bör en bedömning göras om den säkerhetsnivå som kan uppnås, är tillräcklig i förhållande till vikten av den information som ska skickas. Viss viktig information kanske lämpligen ska skickas över ”vanliga” LAN(Lokalt nätverk).

7.6 Förslag till fortsatt forskning
Som vi nämnde under föregående rubrik arbetas det med olika förslag för att förbättra WEP och säkerheten i trådlösa nät. Vi har inte undersökt närmare vad dessa förslag kan medföra säkerhetsmässigt för WLAN. Vårt förslag innebär att studera de olika alternativen, och utifrån detta analysera de olika för- och nackdelar dessa kan medföra. Denna analys skulle sedan kunna leda till ett eget förslag om vilka delar som bör vara med i nästa standard av trådlösa nät och WEP.

Ett annat förslag till vidare forskning är att ta reda på varför den nuvarande standarden för trådlösa nät och WEP inte är tillfredsställande säkerhetsmässigt. Frågor att ställa sig kan vara:

- Har kompetenta kryptografer använts vid utvecklingsarbetet av WEP?
- Gick utvecklingen av standarden 802.11 för snabbt?
- Hur högt prioriterade man säkerheten?
- Finns det andra möjliga orsaker?

8 SLUTSATS

Vi har fått bekräftat att vårt antagande, ”Baserat på de artiklar och tidningar vi har läst, antar vi att säkerheten i WLAN inte är tillfredsställande och nu vill vi på djupare plan ta reda på hur det ligger till med detta”, stämmer överens med den slutsats vi har kommit fram till, genom litteraturstudier och vårt praktiska försök. Slutsatsen är att WLAN är osäkra och att WEP går att knäcka. Det faktum att IV:n bara är på 24-bitar, är det grundläggande problemet som gör dessa attacker möjliga.

Om ett företags verksamhet kräver högre säkerhet än vad WEP kan ge, finns det möjligheter att kombinera WEP med andra säkerhetslösningar, såsom SSH, SSL, VPN, IPSec, Kerberos och RADIUS, för att uppnå detta.

9 REFERENSER

9.1 Litteratur

Davidson, Bo & Patel, Runa, 1994: *Forskningsmetodikens grunder*. Lund. Studentlitteratur.

Igidius, H, 1986: *Positivism-Fenomenologi-Hermeneutik.* Studentlitteratur.

Kurtz, George, McClure, Stuart & Scambray, Joel, 2002: *Hacking i Focus.* Sundbyberg. Pagina

Patel, Runa & Tebelius, Ulla, 1994: *Grundbok i forskningsmetodik.* Studentlitteratur.

Perkins, Charles & Strebe, Matthew, 2000: *Brandväggar*. Sundbyberg. Pagina Förlags AB Sundbyberg.

Stallings, William, 2000: *Network security Essentials: Application and standards.* New Jersey: Prentice Hall.

9.2 Internet

Borisov, N, Goldberg, I & Wagner, D. ”Intercepting Mobile Communications”
http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf
10 feb 2002.

Borisov, N, Goldberg, I & Wagner, D. ”Security of the WEP algorithm”
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
14 feb 2002.

Fluhrer, S , Mantin, I & Shamir, A. ”Weakness in the Key Scheduling Algoritm of RC4”
http://www.wisdom.weizmann.ac.il/~itsik/RC4/Papers/Rc4_ksa.ps
10 feb 2002.

Hammarberg, Per. ”WEP gör nätet hemlighetsfullt”
http://arkiv.idg.se/pdf/nok/2001/14/NK2001-04-402_Teknikanalys.pdf
3 mars 2002.

Hulton, David. ”Practical Exploitation of RC4 Weaknesses in WEP Environments”
http://www.dachb0den.com/projects/bsd-airtools/wepexp.txt
14 mars 2002.

Ioannidis, John, Rubin, Aviel D & Stubblefield, Adam. ”Using the Fluhrer, Mantin and Shamir Attack to Break WEP”
http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf
21 feb 2002.

Jonsson, K & Svensson, D. ”WLAN Security”
http://amy.udd.htu.se/~daniel/dokument/wlan_sec.pdf
15 feb 2002.

Jovan Dj. Golic. ”Linear Statistical Weakness of Alleged RC4 Keystream Generator”
http://link.springer.de/link/service/series/0558/papers/1233/12330226.pdf
15 feb 2002.

Larry, Loeb. ”What,s up with WEP?”
http://www-106.ibm.com/developerworks/security/library/s-wep/?
14 feb 2002.

Malmgren, Robert. ”Grunder i nätverkssäkerhet”
http://www.isk.kth.se/~fallsjo/NetSec.pdf
21 feb 2002.

Mannion, Patrick. ”Cipher attack delivers heavy blow to WLAN security”
http://www.eetimes.com/story/OEG20010803S0082
10 feb 2002.

Olofsson, Kent. ”WLAN - trådlös säkerhetsrisk”: Nätverk & Kommunikation.
http://arkiv.idg.se/pdf/nok/2001/14/NK2001-04-420_WLAN.pdf
3 mars 2002.

Princy C, Metha. ”Wired Equivalent Privacy Vulnerability”
http://rr.sans.org/wireless/equiv.php
14 feb 2002.

Sylvan, Mats. ”Säkerhet i Trådlösa nätverk”: Nätverk & Kommunikation.
http://www.symbol.com/sweden/valkommen/network.PDF
8 mars 2002.

9.3 Tidningar

Bergström, J, 2001: Hemliga data läcker ur trådlösa nätverk. *PC FÖR ALLA*
Dec 2001.

Olsson, F, 2002: Rätten till den trådlösa loggan. *DATORMAGAZIN*
Nr 2 2002.

Olsson, F, 2002: Säkra ditt trådlösa nätverk. *DATORMAGAZIN*
Nr 4 2002.