TDDC03 Projekt, Våren 2006

Kryptologi ur användarens perspektiv

Pontus Karlsson och Oskar Särnholm

Handledare: Viiveke Fåk

Pontus Karlsson Oskar Särnholm
Linköpings universitet
E-post: {ponka209, osksa144}@student.liu.se

Sammanfattning

Kryptologi används alltmer i vardagen av vanliga användare. Denna rapport tar upp säkerheten i mobiltelefonnätverk, på Internet, i trådlösa Internetanslutningar samt i blåtand. I samtliga fall är kryptologi en viktig del av säkerheten. Men hur säkra är de egentligen, och är användarinformation och marknadsföringsmaterial i paritet med den faktiska säkerheten?

Säkerheten i GSM är knäckt, och inget som avses hemlighållas bör skickas över GSM. Användarna informeras inte om detta av operatörer och enhetstillverkare. 3G-nätverket är säkrare än GSM-nätverket, och informationen till användarna har förbättrats från enhetstillverkarnas sida. Information som skickas krypterad med SSL/TLS och SSH är väl skyddad. Däremot är teknikerna sårbara för angrepp där falska servrar används. WEP är inte en säker standard och lider av en rad säkerhetsproblem, vilket WPA till stor del rättar till. Användare får inte någon rättvisande bild av WEP:s svagheter från kända tillverkares informationsmaterial. Blåtand erbjuder hög säkerhet men det finns enheter med bristfälliga implementationer som sålts innan säkerhetsproblemen uppdagats. Den som använder blåtandsprotokollet bör använda långa PIN-koder för att uppnå hög säkerhet.

1. Inledning

I takt med att användningen av informationsteknik ökar blir också behovet av säkerhetslösningar för konsumentprodukter allt större. Människor väljer att utföra bankärenden och handla på Internet. Många är också de som använder sig av trådlös informationsöverföring. Det kan till exempel röra sig om trådlösa hemmanätverk till datorn, mobiltelefoni eller blåtand. I den här rapporten har vi tittat närmare på några av de kryptografiska tekniker som används i ovannämnda produkter

Vi har studerat två typer av nätverk för mobiltelefoni, nämligen GSM och 3G. GSM valde vi att undersöka då standarden har väldigt många användare över hela världen. GSM Association hävdar exempelvis att GSM-nätverk har mer än 1,6 miljarder användare i fler än 210 olika länder och territorier [1]. Med 3G avser vi den europeiska standarden, UMTS. 3G har långt ifrån lika många användare som GSM, enligt UMTS forum har UMTS cirka 50 miljoner användare. Dock investeras det mycket i 3G, och tekniken kommer troligtvis att få ökad betydelse. UMTS forum själva spår en miljard användare år 2012 [2].

Vi har även valt att titta på SSL/TLS och SSH. SSL/TLS har väldigt stor spridning och används för att skydda datatrafik över Internet. Stöd för SSL/TLS finns inbyggt i princip alla moderna webbläsare och används extensivt för att skydda exempelvis elektronisk kommers och internetbankstrafik. SSH används även det för att skydda trafik på Internet. Typiska tillämpningar är säker fjärrinloggning. SSH har även det mycket stor spridning. Både SSH-klient och server finns normalt som standard på alla nyare operativsystem i familjerna Unix och Linux.

Vi ska också undersöka trådlösa nätverk för datakommunikation av typen IEEE 802.11. Trådlösa nätverk har mycket stor spridning idag. Enbart under 2005 såldes över 120 miljoner enheter enligt WiFi alliance [3].

Blåtand är en standard för trådlös kommunikation och finns idag i allt ifrån mobiltelefoner till handdatorer. Antalet enheter med Blåtand uppskattades år 2004 av Bluetooth Special Interest Group (SIG) ha överstigit 250 miljoner enheter. Trenden pekade vid detta tillfälle starkt uppåt och SIG bedömde att antalet enheter vid slutet av 2005 skulle vara 450 miljoner. [4]

Siffror av det slag som vi presenterat ovan kan givetvis ifrågasättas men faktum kvarstår ändå att användningen av de tekniker som nämnts är betydande. Vilket skydd erbjuder då dessa tekniker och hur säker kan slutanvändaren vara? Detta är frågor som den här rapporten kommer att besvara.

1.1 Syfte

Syftet med rapporten är att undersöka huruvida användaren av de undersökta teknikerna kan få en rättvisande bild av det skydd han/hon erhåller via användarinformation och marknadsföringsmaterial.

1.2 Metod

Vi har valt ut några olika tekniker som använder kryptologi. De tekniker vi valt är sådana som används av gemene man samt har stor spridning. Genom att studera tillgänglig litteratur kommer varje teknik att undersökas

på djupet. Därefter skapar vi oss en uppfattning om hur kryptografisk säker den är. Genom att studera marknadsföringsmaterial och för användaren tillgänglig information kan vi sedan dra slutsatser om informationen till användaren är rättvisande och begriplig.

2. Mobila nätverk

Vi behandlar två typer av mobila nätverk: GSM-nätverk och 3G-nätverk. Med 3G menar vi den europeiska standarden för 3G-nätverk kallad Universal Mobile Telecommunications System.

2.1 GSM

Säkerheten i GSM designades för att ge motsvarande säkerhet som finns i det fasta telefoninätverket. Från användarens synvinkel finns det främst två punkter: Han/hon vill inte att 1) vem som helst med en radiomottagare ska kunna avlyssna datatrafiken samt 2) kunna bestämma användarens position. Operatören i sin tur är naturligtvis mest intresserad av att autentisera användarna så att endast de som är betalande abonnenter kan använda nätverket.

Dessa tre krav hanterar GSM-nätverk som följer: All trafik som sänds genom luften krypteras. Det unika nummer som identifierar varje användare byts ut mot ett temporärt under handskakningen. Detta gör det svårare för tredje part att lokalisera användaren. Slutligen genomför nätverket en challange-response-autentisering av användaren.

Nedan följer en mer detaljerad genomgång av handskakningsprocessen. Då inte annat anges är informationen hämtat från [5]. Användaren ansluter till basstationen. Är det första gången så måste likväl det för abonnenten unika numret IMSI skickas. Har användaren varit ansluten tidigare kan det temporära tilldelade numret TMSI användas. Basstationen skickar sedan ett 128 bitars slumptal RAND som utmaning. Användaren använder en algoritm som kallas A3 med RAND och Ki som indata. Ki är en 128 bitars nyckel som finns på varje SIM-kort. A3 ger ett 32 bitars svar SRES på utmaningen, som returneras till basstationen.

Operatören genomför samma beräkning, och om SRES matchar så är användaren autentiserad. Användare och basstation genererar nu en sessionsnyckel genom algoritmen A8, som även den tar RAND och Ki som indata men producerar en 64 bitars nyckel Kc som utdata. Både A3 och A8 implementeras normalt som samma envägs hashalgoritm.[6] Många operatörer har valt att sätta de 10 sista bitarna till 0, varför Kc ofta bara är 54 bitar lång i praktiken.[7] För själva krypteringen används ett flödeskrypto, det vill säga nyckelströmmen adderas binärt med meddelandet bit för bit.

Nyckelströmmen skapas av en algoritm A5, som tar ett 22 bitars ramnummer (frame number) samt sessionsnyckeln Kc och producerar en 228 bitars nyckelström. Då ramnummret ändras för varje ram (frame) så krypteras varje ram med en egen nyckel. A5 implementeras genom kombinationer av lineära återkopplade skiftregister.

2.1.1 Säkerhetsproblem

Ett problem med säkerheten i GSM är att autentiseringen endast är envägs. Det gör det möjligt för en angripare att använda sig av en falsk basstation, och på så sätt bli man-in-the-middle. Ett annat problem är att endast trafiken mellan användaren och basstationen är skyddad. Det betyder att den kan gå vidare på exempelvis en mikrovågslänk eller kabel i klartext. Vidare så kan man med fysisk tillgång till ett SIM-kort lätt lista ut Ki och skapa ett klonat SIM-kort.

En stor säkerhetsbrist i GSM är att nyckeln Kc kan återskapas med hjälp av endast kryptotext. Barkan, Biham och Keller [8] beskriver en sådan attack där det endast krävs några dussin millisekunder med kryptotext och en persondator för att kunna knäcka Kc på mindre än en sekund. När angriparen väl har Kc kan han/hon exempelvis avlyssna offrets röst och datatrafik, överta samtal och ändra sms-meddelanden avsedda för offret samt ringa på offrets bekostnad.

Vidare kan nämnas att användarens unika nummer, IMSI, sänds i klartext första gången handsskakning sker. Sedan tilldelas enheten ett temporärt unikt nummer TMSI. Det kan även noteras att kryptonycklar och autentiseringsdata skickas i klartext inom och mellan nätverk [9]. Då GSM använder sig av ett flödeskrypto erhåller användarens data inte heller integritet.

2.1.2 Användarperspektiv

Användaren av ett GSM-nätverk har väldigt lite information tillhands. Vanliga standardtelefoner visar ingen information om huruvida samtalet är krypterat eller ej. Användaren kan alltså tro att hans samtal erhåller skydd av den kryptering som finns i GSM-standarden, medan operatören i själva verket slagit av krypteringsfunktionen. Detta är nämligen upp till operatören i GSM, och många operatörer gör det när belastningen i nätet är hög [10]. De svenska operatörerna Telia, Vodafone och Tele2 har ingen lättillgänglig information om säkerheten i sina GSM-nät som riktar sig till kunder på sina respektive hemsidor. Användaren av GSM-nätverket har alltså nästan ingen information om det begränsade skydd som finns och kan heller inte se om detta skydd används.

2.2 3G

Säkerheten i 3G-nätverk är baserad på säkerheten i GSM. Designmålen inbegrep att behålla det som var

beprövat och fungerade i GSM och förbättra det som visat sig vara undermåligt.[9] I 3G-nätverk autentiseras både användaren till nätverket och nätverket till användaren, till skillnad mot GSM. Detta skyddar mot falska basstationer. Det finns även en mekanism som säkerställer för både nätverk och användare att nycklar inte återanvänds inom en viss tid. Detta saknas i GSM. I 3G-nätverk skyddas användarens data mot både avlyssning och förändring. Data krypteras liksom i GSM med ett flödeskrypto, men i 3G-nätverk kan flera olika algoritmer användas. En svaghet i GSM var svårigheten att byta ut en algoritm som blivit knäckt, då endast en algoritm i taget stöds. En vanlig implementation i 3G-nätverk är att använda en blockchiffersalgoritm vid namn Kasumi i Output FeedBack mode för att generera nyckelströmmen. Dataintegriteten skyddas av en annan algoritm som genererar en MAC, Message autentication code. Ofta är även den implementerad i form av Kasumi, men i Cipher Block Chaining mode för att skapa en MAC [11]. En annan skillnad är att nyckellängden har ökats i 3G för att möta ökningen i beräkningskraft, från 64 till 128 bitar. Det finns även mekanismer för att skydda nycklar och annan information inom och mellan nätverk [12].

2.2.1 Säkerhetsproblem

Ett säkerhetsproblem med 3G är att International Mobile Subscriber Identity, IMSI fortfarande skickas i klartext i vissa fall. Detta sker dock mindre ofta än i GSM. Om krypteringen är avslagen så kan en angripare även i 3G överta en användares inkommande samtal.

2.2.2 Användarperspektiv

Den största skillnaden mot GSM-nätverk är att det i 3G-nätverk finns synlighet och konfigurerbarhet för användaren. Det finns möjlighet för användaren att se vilken slags kryptering som används (i vissa enheter) samt själv konfigurera sina säkerhetsinställningar. Användaren kan exempelvis välja att inte ta emot okrypterade samtal eller kräva en viss algoritm. En annan stor skillnad är att 3G har mer avancerade säkerhetsfunktioner än GSM. Designprocessen var jämfört med den för GSM väldigt öppen, och man baserade designbesluten på erfarenhet från GSM.

3. Kryptering på Internet – SSL/TLS och SSH

Två protokoll med stor spridning på Internet är SSL/TLS och SSH.

3.1 SSL/TLS

SSL står för Secure Socket Layer och utvecklades av Netscape under slutet av nittiotalet. Det har sedan dess blivit de-facto standard för säker överföring av webbsidor på Internet, samt andra användningar. TLS är en officiell standard utgiven av Internet Engineering Task Force. Den består i princip av SSL version 3 med några tillägg. Hädanefter kommer vi att använda termen SSL synonymt med SSL version 3 och TLS då inte annat anges. SSL ger konfidentialitet, autentisering av server (och av klient om så önskas) samt dataintegritet. SSL kan ses som ett extra lager i nätverksmodellen, inklämt mellan applikationen och TCP. SSL finns inbyggt i nästan alla moderna webbläsare och många andra typer av applikationer. Förinstallerat i alla SSL-klienter finns en lista (kan vara tom) över av tillverkaren betrodda certifikatutfärdare samt respektive publik nyckel.

En SSL-session börjar med en handskakning. Klienten skickar en förfrågan innehållande bland annat egen SSL-version, samt kryptografiska inställningar. Servern svarar med sitt versionsnummer, inställningsparametrar samt sitt certifikat. Certifikatet består av serverns publika nyckel signerat av en Certificate Authority (CA). Om klienten begärt en resurs som kräver autentisering så begär servern även klientens certifikat. Klienten kommer nu att autentisera servern. Det gör klienten genom att kontrollera certifikatets giltighetstid, kontrollera att utfärdardande CA finns i listan över betrodda CA och validera signaturen med hjälp av CA:ns publika nyckel. Klienten bör även kontrollera att adressen i certifikatet är samma som servern som skickade det, även om det inte rent tekniskt är en del av SSL-protokollet [13]. Klienten har nu autentiserat servern. Klienten skapar nu en så kallad pre master secret. Denna krypteras med serverns publika nyckel och skickas. Om även autentisering av klienten önskas skickar klienten även sitt certifikat. Detta valideras på i princip analogt sätt som tidigare av servern. Servern använder sin privata nyckel för att dekryptera pre master secret. Både klient och server skapar nu en symmetrisk sessionsnyckel utifrån pre master secret. Klienten skickar nu ett sista meddelande i klartext där servern informeras om att all trafik fortsättningsvis kommer att krypteras med sessionsnyckeln. Klienten skickar även ett med sessionsnyckeln krypterat meddelande som meddelar att handskakningen är slutförd från klientens sida. Servern gör precis analogt, det vill säga skickar ett meddelande i klartext och ett krypterat enligt ovan. Nu kan båda parter kommunicera krypterat. Båda parter kan när som helst kräva en ny handskakning.

Typiskt sett används RSA för den assymmetriska krypteringen och AES, 3DES, DES, RC4 eller RC2 för den symmetriska [14] Vilka algoritmer som stöds beror även på vilken version av SSL som körs. Vanligtvis används MD5 eller SHA1 för dataintegritet [15].

3.1.1 Säkerhetsproblem

SSL är basen för mycket av säkerheten på Internet [16]. Det finns säkerhetsproblem med SSL i form av buggar i implementationen [17]. Detta kan innebära att säkerheten undergrävs. En annan aspekt är att många implementationer av SSH tillåter DES som chiffer. DES anses inte längre vara säker av säkerhetssamfundet på grund av sin korta nyckellängd, 56 bitar. Att hitta rätt nyckel kan på specialbyggd hårdvara gå på mindre än 35 minuter [18].

3.1.2 Användarperspektiv

Användaren av SSL har normalt någon slags information tillgänglig som talar om huruvida kryptering används. Detta är naturligtvis helt upp till implementationen och kan variera från applikation till applikation. Ett sätt för användare att komma i kontakt med SSL är genom att peka sin webbläsare på en webbplats för elektronisk kommers eller en internetbank. Informationen till användaren består i de flesta webbläsare av någon slags grafisk symbol. Det finns oftast möjlighet att få mer information, såsom vilken algoritm och nyckellängd som används.

3.2 SSH

Ett annat protokoll som har stor spridning på Internet är SSH. SSH står för Secure SHell och är standardiserat av Internet Engingeering Task Force. Det finns två versioner: 1 och 2. Version 1 är förkastad och icke kompatibel med version 2 [19]. I version 1 finns ett säkerhetsproblem med dataintegriteten: En angripare kan obemärkt injektera arbiträr data i dataströmmen. SSH går över TCP. I sin enklaste form ansluter SSH-klienten till SSH-servern. Exempelvis Diffie-Hellman används för att komma överrens om en gemensam symmetrisk nyckel. En krypterad överföring startar sedan. Olika algoritmer kan användas, typiskt sett blowfish, DES, 3DES eller AES. Klienten skickar användarnamn och lösenord genom den krypterade tunneln och om dessa stämmer öppnas en fjärrinloggning på servern [20]. SSH kan även användas tillsammans med asymmetrisk kryptografi. Då genereras ett nyckelpar, den privata sparas på servern och den publika kan fritt kopieras runt på nätverket. Detta möjliggör inloggning utan lösenordsautentisering, alternativt autentisering både med asymmetrisk kryptografi samt lösenord. Det finns även möjlighet att använda sig av Kerberos för nyckeldistribution [21].

3.2.1 Skillnaden mellan SSL och SSH

Det förekommer ibland hopblandning av begreppen SSL och SSH. Båda är protokoll för att säkra kommunikation över Internet. Syftet med SSH är främst säker fjärrinloggning och säker filöverföring även om det kan användas för mycket mer. Syftet med SSL är säker överföring av webbsidor. Det kan liksom SSH göra betydligt mer, men detta är huvudsyftet. När en SSL-handskakning är över krävs det en applikation för att få något gjort. Annars har man en meningslös krypterad förbindelse. När en SSH-handskakning är klar finns det direkt möjlighet att få saker gjorda, nämligen fjärrinloggning och säker filöverföring. Det är en del av protokollet. SSH kan också användas för att skapa en krypterad tunnel mellan två noder, och därigenom kan i princip vad som helst köras.

3.2.2 Säkerhetsproblem

Ett stort säkerhetsproblem med SSH är autentiseringen så som den utförs i praktiken i många fall. När en klient ansluter till servern för första gången är dess värdnyckel okänd för klienten. Detta löser många applikationer genom att fråga användaren om värdnyckeln är korrekt och stämmer överrens med värdnyckeln för servern som användaren avser att ansluta till. För att vara säkert förutsätter detta förfaringssätt att användaren på något sätt kontrollerar vad värdnyckeln är på den maskin han/hon önskar ansluta till. Görs inte detta är det möjligt att användaren egentligen ansluter till en falsk server, varpå exempelvis en man-in-the-middle situation kan uppstå. Om användaren godkänner nyckeln sparas den i ett cacheminne. Nästa gång klienten ansluter till samma server jämför klienten serverns värdnyckel med den i cacheminnet sparade nyckeln. Det finns möjlighet att komma runt detta problem genom att använda sig av en publik nyckelinfrastruktur. Detta används ofta inte av serveradministratörer på grund av kostnad och komplexitet. Att anskaffa ett certifikat av en CA kostar både pengar och tid, medan lösningen ovan fungerar direkt efter installation. Även SSH tillåter användning av DES som krypteringsalgoritm, vilket inte anses säkert enligt vad som påpekats i avsnittet om SSL.

3.2.3 Användarperspektiv

Det användaren kan notera när han/hon använder SSH för att ansluta till en ny server är dialogrutan som upplyser om att värdnyckeln inte finns i cacheminnet. I exempelvis SSH-klienten WinSCP får användaren möjlighet att avbryta anslutningen, spara serverns värdnyckel i cacheminnet och ansluta eller ansluta utan att spara värdnyckeln. Detta ställer som ovan nämnt krav på användaren att kontrollera värdnyckeln.

4. Trådlösa nätverk

Trådlösa hemmanätverk har blivit en allt vanligare syn i många hem [3]. De vanligaste säkerhetslösningarna

bygger på antingen Wired Equivalent Privacy (WEP) eller Wi-Fi Protected Access (WPA).

4.1 WEP

WEP återfinns i 802.11 standarden är implementerad i länk-lagret. WEP bygger på att de enheter som ska kommunicera med varandra har en delad symmetrisk nyckel. Standarden säger inget om hur nycklarna ska administreras. [22]

Hur WEP fungerar finns beskrivet i en artikel av Geier [23]. WEP krypterar innehållet i varje frame med ett RC4 chiffer. För att försvåra gissningsförsök på den symmetriska nyckeln (som kan vara 40- eller 64-bitar lång) finns det även en initieringsvektor (IV) som kan ändras vid varje ny frame. Vektorn IV som är ett 24-bitars slumptal läggs ihop med den symmetriska nyckeln. Detta utgör sedan indata till en pseudoslumptalsgenerator som skapar en nyckel lika lång som innehållet i den krypterade framen. Till denna nyckel adderas också 32-bitar som kan används av mottagaren för att kontrollera att meddelandet inte har ändrats (integrity check value, ICV). Denna nyckel blir tillsammans med meddelandet indata till en XOR operation där utdatan blir det krypterade meddelandet. Detta meddelande skickas sedan tillsammans med IV (i klartext) till mottagaren. [23]

4.1.1 Säkerhetsproblem

Borisov et al [22] tar upp flera sätt att utnyttja svagheter i WEP-protokollet. Ett sätt är att avlyssna trafiken tills samma IV använts två gånger. Genom att utföra statistisk analyser kan sedan angriparen försöka lista ut meddelandenas innehåll. Desto fler paket angriparen har med samma IV desto lättare går det att knäcka nyckeln. En annan möjlighet är angriparen försöker infoga trafik i datanätet. Det första steget är att ha vetskap om meddelandet i ett paket, vilket kan ske på olika sätt. Nästa steg är att avlyssna paketet och själv försöka återskapa det med hjälp av kunskaper om dess innehåll. Med hjälp av denna kunskap kan sedan angriparen infoga frames, med annat innehåll, som mottagaren kommer att godta.

Det finns även möjlighet att, med vetskap om ip-adressen som paketet skickas till, försöka lura WEP-protokollet. Denna metod utgår ifrån att angriparen ändrar adressbitarna till en annan adress som är lokaliserad utanför det trådlösa nätverket och som angriparen kontrollerar. Vid denna dator kan sedan angriparen avlyssna trafiken eftersom trafiken endast är krypterad av WEP inom det trådlösa nätverket. Den kanske effektivaste metoden är dock att spara alla IV. Genom kunskap om olika fulltextmeddelanden kan angriparen sedan bygga upp en tabell innehållande information om hur man dekrypterar varje paket med en tillhörande IV. En sådan tabell allokerar 15 GB utrymme. [22]

AirSnort är ett exempel på ett program som automatiskt knäcker WEP och programmet finns tillgängligt gratis på adressen: http://airsnort.shmoo.com/.

4.1.2 Användarperspektiv

Eftersom WEP är en öppen standard och dess svagheter är allmänt kända för åtminstone vissa delar av den datorintresserade populationen finns det information tillgänglig för den som söker aktivt på Internet. För de användare som förlitar sig på tillverkarens information är situationen en annan. Vi har besökt tre tillverkare av trådlösa konsumentprodukters hemsidor nämligen Netgear, D-Link och 3com.

På 3coms hemsida (http://www.3com.com) lyckades vi inte hitta någon information om säkerhetsbristerna i WEP trots att företaget säljer otaliga produkter med WEP. I vissa produktinformationsblad gick det att hitta information som *"… and Wi-Fi Equivalent Privacy(WEP) packet encryption help ensure strong data security"* [24] eller *"40/64-, and 128/154-bit WEP shared key encryption and advanced WPA AES 256-bit encryption ensure the privacy of all wireless transmissions"* [25]

På D-Links hemsida (http://www.dlink.com) marknadsförs inte WEP i produktinformationen i samma utsträckning som för 3com. Där lyckades vi inte hitta information om hur säkert WEP är. Vi läste också några manualer från D-Link och konstaterade att den enda information som fanns tillgänglig för användaren var att WPA är säkrare en WEP vilket nämndes utan närmare förklaring.

På Netgears hemsida (http://www.netgear.com) hittade vi information om att WEP var en tidig standard och att det nu finns bättre standarder för säkerhet. Dock kunde vi samtidigt hitta produktinformation som hävdade *"… High-level WEP encryption gives you secure data communication and shields your network from wireless eavesdroppers – at no sacrifice to performance." [26]*

4.2 WPA

WPA är en efterföljare till WEP och innehåller Temporal Key Integrity Protocol (TKIP). TKIP använder en 48-bitars IV vilket medför att det blir långt färre dubbletter av IV:er i jämförelse med WEP. [27]

TKIP medför också att en unik nyckel används för varje frame. Nyckeln skapas utifrån en IV, MAC-adressen på den sändande enhet och den nyckel som delas mellan sändare och mottagare [28]

TKIP bidrar också till att dataintegriteten förbättras jämfört med WEP. Detta har uppnåtts genom en message integrity code (MIC) på 8-bitar lagts till protokollet. [27]

autentiseringen i WPA bygger på standarden 802.1x och kan antingen genomföras med hjälp av en server eller en förinstallerad gemensam nyckel.[27]

4.2.1 Säkerhetsproblem

Enligt Geier [27] löser WPA alla säkerhetsproblem som uppstått i WEP. WPA är dock fortfarande känsligt för denial-of-service attacker. Detta problem kan uppstå om en angripare skickar upprepade paket som är krypterade med en felaktig nyckel. WEP:s åtgärd mot detta är att stänga ner anslutningen i en minut för att skydda nätverket. Detta öppnar dock upp för denial-of-service attacker.

4.2.2 Användarperspektiv

Vi kontrollerade netgear d-link, och 3coms hemsidor för användarinformation om WPA.

På netgears hemsida fanns det information om att WPA *"Provides extremely strong wireless security…"*. Hemsidan tar också upp nackdelar som risken för denial-of-service attacker och svårare administration. Information förutsatte dock en hel del datornätverkskunskaper. [29]

På D-links hemsida fick vi, som tidigare berättats, endast reda på att WPA erbjuder högre säkerhet än WEP.

3coms hemsida erbjuder heller inte någon utförlig beskrivning om WPA. WPA och WEP nämns ofta i samma mening i produktinformation som argument för hög säkerhet.

5. Blåtand

Blåtandstandarden utvecklas och underhålls av Bluetooth Special Interest Group (SIG) som är en organisation bestående av företag såsom Ericsson, IBM, Microsoft, Nokia, Motorola och Intel med flera. Protokollet har uppdaterats flera gånger och är i skrivande stund uppe i version 2.0. Mer om information om SIG finns tillgängligt på http://www.bluetooth.com.

5.1.1 Säkerhet i blåtandsprotokollet

Säkerhetsmekanismerna i blåntandsprotokollet finns bland annat beskrivna i artiklar av Juha T. Vainio [30], Jun-Zahio Sun med flera [31] samt Gyongsu Lee och Sin-Chong Park [32].

Det finns tre olika nivåer av säkerhet som en blåtandsenhet kan erbjuda. Det grundläggande tillståndet innebär att enheten inte har någon säkerhet för informationsöverföring implementerad. I den andra nivån är säkerheten implementerad på servicelagret. Detta får följden att olika program kan använda olika lösningar för autentisering. I det tredje tillståndet återfinns implementationen på länklagret. [33]

Till saken hör också att det finns två nivåer av säkerhet för enheter. Dessa är den betrodda nivån och den icke betrodda nivån. Som namngivningen avslöjar litar enheten blint på enheter tillhörande den betrodda nivån vilket inte är fallet för den icke betrodda.[33]

För att förstå nyckelhanteringen i blåtandsprotokollet måste man kunna skilja på en rad olika länknycklar. En länknyckel, som används vid säker kommunikation mellan enheter, består av 128-bitar och kan delas in i kategorierna: initieringsnyckel, semipermanent nyckel, och temporär nyckel. [30]

Initieringsnyckeln används för den para ihop två enheter och skapas utifrån den PIN-kod som användaren matar in vid ihopparning av enheter. Utifrån PIN-koden, dess längd och ett slumpvis valt nummer (som genereras av den ena enheten och skickas till den andra) kan båda enheterna skapa en gemensam initieringsnyckel. [10]

En semipermanent nyckel kan antingen vara en enhetsnyckel eller en kombinationsnyckel Med semipermanent menas att nyckeln kan lagras mellan sessioner. En enhetsnyckel skapas när enheten installeras utifrån ett slumpvis valt nummer och enhetens adress. En kombinationsnyckel genereras utifrån information från två ihopkopplade enheter, där enheterna efter att enskilt ha skapat en nyckel (med samma algoritm som för enhetsnyckeln) utbyter varandras slumptal och med hjälp av denna information skapar en ny gemensam nyckel. När två enheter ska kopplas samman avgörs det om de ska använda en kombinationsnyckel eller en enhetsnyckel för sin kommunikation. [30]

En temporär nyckel är en masternyckel som används för att skicka data från en enhet till flera enheter. För en utförligare redogörelse för ur de olika nycklarna genereras rekommenderas artikeln Bluetooth Security av Juha T. Vainio. [30]

autentisering i blåtandsprotokollet genomförs med hjälp av en challange-response-teknik. Den frågande enheten skapar ett slumpvis valt nummer, genererar en nyckel med hjälp av detta nummer, adressen till svarande enheten och initieringsnyckeln. Det slumpvis valda numret skickas sedan över till den svarande enheten som utför samma algoritm och skickar tillbaka resultatet. Den frågande enheten jämför svaret med sin egen framräknade nyckel och om de matchar har båda enheterna vetskap om initieringsnyckeln och enheterna är autentiserade.[32]

Krypteringen i blåtandsprotokollet bygger på ett flödeskrypto. Indata till nyckelgeneratorn är adressen till enheten, dess klocka och kryptonyckeln. Den genererade nyckeln och data som ska krypteras adderas binärt.

Resultatet från denna operation blir krypterad data . [30, 34]

5.1.2 Säkerhetsproblem

Sun med flera [31] har presenterat en sammanställning över kända svagheter i blåtandsprotokollet. De har dock åsikten att blåtand erbjuder en relativt bra säkerhet men lyfter fram svagheter såsom att PIN-koden kan väljas för kort och att slumptalsgeneratorn kan implementeras på ett sådant vis att talen kan gissas.

Vainio [30] tar också upp problemet med korta PIN-koder men beskriver också en annan attackmöjlighet. Scenariot bygger på att en enhet A och B kommunicerar med A:s enhetsnyckel som länknyckel. A kommunicerar också med en enhet C med hjälp av A:s länknyckel. Möjligheten finns då för enhet B att med hjälp av A:s enhetsnyckel och adress att räkna ut krypteringsnyckeln som används mellan A och C. På detta sätt kan B avlyssna trafiken mellan A och C eller felaktigt utge sig gör för att vara någon av enheterna till den andra. [30]

Shaked och Wool [35] beskriver en attack där de utnyttjar korta PIN-koder och hävdar att man kan knäcka de vanligaste PIN-koderna på 0.06-0.3 sekunder.

Laurie [36] listar säkerhetsbrister som uppkommit genom misstag i implementationen av blåtandsprotokollet. Genom att utnyttja dessa säkerhetshål kan personliga uppgifter som till exempel en telefons adressbok kommas åt. Dessa säkerhetsbrister gäller dock främst mobiltelefoner som tillverkades innan dessa säkerhetsbrister blivit kända.

5.1.3 Användarperspektiv

På SIG:s hemsida [37] finns det information om hur en användare ska undvika de attacker som bland annat beskrivits av Laurie. Informationen är skriven på en allmän nivå utan alltför mycket tekniska termer. Det går också att läsa allmänna råd som består av att inte koppla ihop sig med okända enheter eller använda en PIN kod som är längre än 8 siffror samt att vara i osynligt läge.

Vi har också besökt vissa mobiltelefontillverkares hemsidor Sony Ericsson (http://sonyericsson.se), Nokia (http://nokia.se) och Motorola (http://www.motorola.com). På Sony Ericssons och Nokias hemsida kan information om vilka modeller som kan vara utsatta för de säkerhetsbrister som uppkommit på grund av bristfälliga implementationer återfinnas. Det finns också allmänna råd liknande de från SIG:s hemsida. På Motorolas hemsida kunde vi inte hitta någon sådan information.

6. Diskussion

Nedan diskuteras teknikerna utifrån den säkerhet de kan erbjuda en användare och detta sätts i förhållande till marknadsföringsmaterial och information.

6.1.1 Mobila nätverk

Säkerheten i GSM-nätverk kan betecknas usel av två anledningar. Dels informeras inte användaren om kryptering är aktiverad eller inte. Dels är den erhållna säkerheten då kryptering används usel. Det finns en uppsjö olika dokument tillgängliga på Internet som beskriver hur man knäcker krypteringen i GSM på allt mellan några minuter och mindre än en sekund. Det finns även information om hur man sätter upp en falsk basstation, och kostnaden för detta. Designprocessen av krypteringen har varit ett skolexempel på dålig praxis. GSM association har ansett att det bästa sättet att upprätthålla säkerheten är att hemlighålla algoritmerna. Det har betytt att säkerhetssamfundet inte har kunnat bidra med förbättringar och synpunkter, och när sedan algoritmerna ändå blivit publika har säkerhetsbristerna funnits där. Det finns dock en strävan till förbättring inom GSM-industrin. Nyare versioner av knäckta algoritmer finns tillgängliga. Migreringen är dock i många fall besvärlig. Uppgradering var aldrig riktigt betänkt i standarden, varför endast en algoritm i taget kan köras. Dessutom kräver uppgradering till en ny algoritm i vissa fall att alla SIM-kort i nätverket byts ut. Vi anser även att mobiloperatörerna borde upplysa användaren om vilken typ av säkerhet som erbjuds i respektive nätverk, samt de säkerhetsbrister som finns med GSM. Det gör varken Telia, Tele2 eller Vodafone på sina respektive webbplatser visar en snabb sökning. Sammanfattningsvis kan sägas att GSM bör anses som osäkert, och ingen information som avses hemlighållas bör skickas via GSM-nätverket vare sig som röst eller data.

Vad gäller 3G-nätverken så är situationen avsevärt bättre. Lärdom har tagits från misstagen med GSM. Det är också bra att användaren kan både få information och möjlighet att konfigurera egna säkerhetsinställningar. Frågan är hur lättillgängliga information och konfigurationsinställningar är på de enheter som säljs till slutkonsument. Man kan vart fall notera att om man som kund vill utnyttja den högre säkerhetsnivå som finns i 3G-nätverken så krävs det att man kan konfigurera sin enhet med avseende på säkerhet. Annars finns det möjlighet för en angripare att helt enkelt störa ut de frekvenser där 3G opererar, varpå telefonen automatisk byter till GSM-nätverket med alla dess säkerhetsbrister.

6.2 Säkerhet på Internet

Det som verkligen äventyrar säkerheten med SSL är när användaren surfar till en sida som inte har ett servercertifikat som är signerad av en av användarens applikation betrodd CA. Då förväntas användaren själv kunna avgöra huruvida han/hon vill lita på serverns certifikat. Den information som då presenteras är av ett slag som en vanlig användare svårligen kan ta till sig, med risk att många bara klickar på ok och går vidare. Samma sak gäller SSH där användaren i vissa fall får upp en värdnyckel som han/hon förväntas ta ställning till. Det finns även här en risk att användaren bara klickar på ok utan vidare. Hur stor risk är då detta för säkerheten? Om användaren ansluter till en falsk server så är både konfidentialitet och dataintegritet förlorad. Det krävs dock av angriparen att han/hon sätter upp en falsk server, samt dirigerar om användaren dit. Vi anser att detta kan betraktas som en risk med liten sannolikhet att inträffa för vanliga användare, men dock med mycket grava konsekvenser om den inträffar. Det har dock förekommit i flera fall att angripare satt upp servrar som imiterar exempelvis en internetbanksinloggning eller annan ekonomisk institution. Vi tar även upp det faktum att både SSL och SSH tillåter DES som krytpteringsalgoritm. Man kan argumentera att det eroderar den erhållna säkerheten då DES inte längre anses vara säker. Dock har denna rapport sin utgångspunkt i vanliga datoranvändare, och det förefaller inte troligt att värdet av de uppgifter som krypteras av denna grupp överstiger kostnaden för att knäcka DES-nyckeln. Alla applikationer borde dock undvika att använda DES i möjligaste mån, och i de fall den ändå används bör användaren informeras.

6.3 Trådlöst Internet

Denna rapport har tagit upp två standarder som kan användas för att skydda trådlösa hemmanätverk nämligen WEP och WPA. Utifrån detta kan det konstateras att WEP inte erbjuder något reellt skydd mot en person med god kännedom om datorer som verkligen vill avlyssna trafiken. WPA är däremot en standard som inte innehåller de brister som finns i WEP och är därför ett betydligt bättre val för den säkerhetsmedvetne. Den som använder WPA bör dock vara uppmärksam på att inte välja för svagt lösenord i sin trådlösa anslutningspunkt eftersom nyckeln som krypterar data skapas bland annat utifrån denna.

Trots att svagheterna i WEP har varit kända sen 2001 går det fortfarande att hitta användarinformation som inte belyser detta. Förklaringen till detta är antagligen att det inte ligger i marknadsförarens intresse att plocka fram svagheter om den aktuella produkten. Det är också en konst att kunna förklara säkerhetsbristerna i protokollet på ett lättförklarligt språk som passar flertalet av konsumenterna. Av de tillverkare vi kontrollerade hade ingen någon utförlig information om bristerna i WEP.

Det kan också vara befogat att ställa frågan hur stort hotet egentligen är för att bli avlyssnad för vanliga användare och vilken skada detta kan medföra. Den trafik som skickas via Internet av vanliga användare är oftast inte speciellt hemlig. Känslig information som till exempel banklösenord skickas ofta krypterat via SSL vilket ger ett skydd mot avlyssning i de fallen. Dock är det alltid ett brott mot den personliga integriteten att bli avlyssnad, vilket säkerligen kan vara otrevligt för den enskilda människan. Finns nätverket på ett företag kan skadan vid avlyssning möjligen bli större eftersom känslig företagsinformation kan skickas över nätverket.

Ett annat hot som uppkommer på grund av WEP:s svagheter är möjligheten att en angripare kopplar upp sig mot en anslutningspunkt i syfte att använda Internet för att begå brottsliga handlingar. En angripare kan även injektera arbiträr data i användarens meddelande, vilket kan vara allvarligt.

Trots att WEP är en kritiserad standard ger den högre säkerhet än ingen säkerhet alls. Många är säkert de användare som använder en okrypterad anslutning eftersom en del anslutningspunkter har detta som standardläge. Deras beslut att skicka okrypterad data skulle kanske i vissa fall omprövas om de fick vetskap om vad detta kan medföra. Enligt samma resonemang skulle många WEP-användare säkert byta till WPA om de hade vetskap om WEP:s svagheter.

Standardlösenord som inte behöver bytas ut och ger rättigheter att administrera en trådlös anslutningspunkt eller möjligheten att välja svaga nycklar som till exempel är för korta, är andra brister som tillverkarna bör lastas för snarare än protokollet. Detta skulle säkerligen vara enkelt för tillverkarna att åtgärda men de verkar i de flesta fall avstå från den möjligheten. Möjligen beror detta på att sådana åtgärder skulle göra produkterna svårare att installera vilket skulle kunna leda till att kundkretsen minskar eller att supporten skulle bli högre belastad.

6.4 Blåtand

Blåtandsprotokollet har så vitt våra efterforskningar sträcker sig inte några säkerhetsbrister i sig. Det en användare bör vara uppmärksam på är om enheten som innehas är en gammal modell som innehar de implementationsbrister som tidigare nämnts.

En användare som värnar om säkerheten bör också välja långa och varierade PIN-koder när det är möjligt för att stärka sitt skydd mot attacker som utnyttjar svaga PIN-koder. Det kan också vara bra att para ihop enheter i säkra miljöer för att undvika att PIN-koden blir känd

för obehöriga. Användaren bör också vara uppmärksam på vilka enheter som han valt att lita på och försäkra sig om att inte fler enheter än nödvändigt finns med i den listan.

Det skulle kunna tyckas att tillverkarna borde ta ett större ansvar i att tvinga användarna att välja längre PIN-koder för att attacker som grundar sig på svaga PIN-koder ska kunna undvikas. Varför detta inte alltid görs kan bero på att produkter skulle kunna få kompabilitetsproblem med äldre enheter som bara är gjorda för korta PIN-koder.

För den användare som aktivt söker information om blåtand finns det information om hur man ökar säkerheten. För privatpersoner är hotet antagligen störst för dem som använder gamla telefoner med bristfälliga implementationer.

7. Slutsatser

Säkerheten i GSM-nätverket är knäckt. Inga data som avses hemlighållas bör skickas genom GSM-nätverket. Användaren av GSM informeras inte om detta faktum, vare sig av operatörerna eller av enhetstillverkarna. Om GSM ska användas för känslig data måste ytterligare säkerhet appliceras innan data skickas. 3G-nätverket kan betraktas som tillräckligt säkert om en konfigurerbar enhet används, och denna konfigureras att inte godkänna osäker kommunikation. Görs inte detta så erhåller användaren av 3G-nätet analog säkerhet som användaren av GSM, det vill säga undermålig. Detta då en 3G-enhet automatiskt byter till GSM då 3G inte finns tillgängligt.

Både SSL/TLS och SSH anses säkra av säkerhetssamfundet. Dock finns alltid hotet från buggar i implementationen som kan göra den teoretiskt goda säkerheten värdelös. Det största problemet med dessa tekniker är dock autentiseringen. Den läggs i många fall över på användaren, som utifrån ytterst knapp information förväntas säkerställa att han/hon ansluter till rätt server.

En användare kan utifrån marknadsföringsmaterial få intrycket att WEP är en säker standard. I själva verket erbjuder WEP inget skydd mot en datorkunnig angripare. Trafiken kan avlyssnas, olovliga anslutningar kan upprättas och informationen i ett meddelande kan ändras av angriparen. WEP är dock ett bättre val än att helt avstå från någon säkerhetslösning. WPA standarden korrigerar bristerna i WEP men erbjuder inget skydd mot denial-of-service attacker. Användaren bör tänka på att välja ett starkt lösenord för sin trådlösa anslutningspunkt.

Blåtandsprotokollet är en relativt säker standard men användare bör se upp för bristfälliga implementationer och användandet av för korta PIN-koder. Användarinformation om säkerhetsaspekter finns för den som söker aktivt.

Referenser

1 GSMAssociation *About GSM Associatiom,* <http://www.gsmworld.com/about/index.shtml> Hämtat den 4 april 2006.

2 UMTS Forum <http://www.umts-forum.org> Hämtat den 4 april 2006.

3 WIFI alliance http://www.wi-fi.org/news/pressrelease-112805-120millionchipsets/ Hämtat den 4 april 2006.

4 Bluetooth special interest group (2005). *Bluetooth Awareness Nearly Doubled Among Consumers,* <http://bluetooth.com/Bluetooth/Press/SIG/iBluetoothi_Awareness_Nearly_Doubled_Among_Consumers.htm. Hämtat den: 4 april 2006.

5 GSM Security. *Frequently asked questions* <http://www.gsm-security.net/faq > hämtat 11 april 2006.

6 S. Sin. *COMP128 - An Algorithm for Authentication and Cipher Key Generation in GSM Networks.* Department of Electrical and Computer Engineering, University of Waterloo. <http://www.comsec.uwaterloo.ca/~ssjsin/COMP128.pdf> hämtat 11 april 2006.

7 GSM Security. *Have the A3 and A8 algorithms been broken?* <http://www.gsm-security.net/faq/gsm-a3-a8-comp128-broken-security.shtml> hämtat 11 april 2006.

8 E. Barkan, E. Biham, N. Keller. *Instant Cipertext-Only Cryptoanalysis of GSM Encrypted Communication.* Proceedings of CRYPTO2003. <http://cryptome.org/gsm-crack-bbk.pdf> Hämtat 11 april 2006.

9 V. C. Ramasami. *Security, Authentication and Access Control for Mobile Communications.* <http://www.ittc.ku.edu/~rvc/documents/865/865_securityreport.pdf> Hämtat 11 april 2006.

10 Tresor Data. *What about safety in mobile networks, specifically in the GSM networks?* <http://www.tresor.co.uk/product_T301B_FAQ.htm#What_about_safety_in_mobile_networks,_specially_in_the_GSM_nets> Hämtat 11 april 2006.

11 M. Walker. *On the Security of 3GPP Networks.* Vodafone AirTouch & Royal Holloway, University of London. <http://www.esat.kuleuven.ac.be/cosic/eurocrypt2000/mike_walker.pdf> Hämtat 11 april 2006.

12 Myagmar, Gupta. *Overview of 3G Security.* 2001. Software Research Group.
Department of Computer ScienceUniversity of Illinois at Urbana-Champaign. <http://choices.cs.uiuc.edu/MobilSec/posted_docs/3G_Security_Overview.ppt> Hämtat 11 april 2006.

13 Microsoft Knowledge Base. *Description of the Server Authentication Process During the SSL Handshake.* 2005. <http://support.microsoft.com/kb/257587/EN-US/> Hämtat den 11 april 2006.

14 Microsoft Knowledge Base. *Description of the Secure Sockets Layer (SSL) Handshake*. 2005. <http://support.microsoft.com/kb/257591/EN-US/> Hämtat den 11 april 2006.

15 IBM TPF Product Information Center. *SSL User's Guide - SSL handshake.* <http://publib.boulder.ibm.com/infocenter/tpfhelp/current/

index.jsp?topic=/com.ibm.ztpf.doc_put.01/gtps5/gtps5m0h.htm> Hämtat 11 april 2006.
16 M. Bishop. *Computer security - art and science.* 2003. Boston, MA : Addison-Wesley.
17 E. Young. *SSL implementation bugs* <http://www2.psy.uq.edu.au/~ftp/Crypto/ssleay/vendor-bugs.html> Hämtat 11 april 2006.
18 RSA Laboratiories. *Has DES been broken?* <http://www.rsasecurity.com/rsalabs/node.asp?id=2227> Hämtat den 11 april 2006.
19 SSH Communications Security Corp. *Securing Remote Connections with Secure Shell White Paper.* 2004. <http://www.ssh.com/documents/28/SecuringwithSecSh_WhitePaper.pdf> Hämtat 11 april 2006.
20 Connected: An Internet Encyclopedia. *SSH Protocol Overview.* <http://www.freesoft.org/CIE/Topics/139.htm> Hämtat 11 april 2006.
21 MIT Online help. *SSH Overview.* <http://web.mit.edu/olh/Remote/ssh.html> Hämtat 11 april 2006.
22 N. Borisov, I Goldberg och D Wagner. Security of the WEP algorithm <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html> Hämtat den 18 april 2006.
23 Geier, J *802.11 WEP: Concepts and Vulnerability.* 2002 <http://www.wi-fiplanet.com/tutorials/article.php/1368661> Hämtat den 18 april 2006.
24 3com Marknadsföringsmaterial <http://www.3com.com/products/en_US/detail.jsp?pathtype=purchase&tab=features&sku=3CRWX375075A> Hämtat den 18 april 2006.
25 3com Marknadsföringsmaterial <http://www.3com.com/products/en_US/detail.jsp?pathtype=purchase&tab=features&sku=3CRWE725075A> Hämtat den 18 april 2006.
26 Netgear Marknadsföringsmaterial <http://www.netgear.com/products/details/MA111.php> Hämtat den 18 april 2006.
27 J. Geier. *WPA Security Enhancements* 2003. <http://www.wi-fiplanet.com/tutorials/article.php/2148721> Hämtat den 8 april 2006.
28 J. Snyder och R. Thayer. 2004. *Explaining TKIP*. <http://www.networkworld.com/reviews/2004/1004wirelesstkip.html> Hämtat den 24 april 2006.
29 Netgear. Användarinformation. <http://kbserver.netgear.com/kb_web_files/n101190.asp> Hämtat den 18 april 2006.
J. Vainio *Bluetooth Security* 2000. Helsinki University of Technology <http://www.niksula.hut.fi/~jiitv/bluesec.html> Hämtat den 8 april 2006.
31 J-Z. Sun, D. Howie, A. Koivisto, och Sauvola ***Design, implementation, and evaluation of bluetooth security*** University of Oulu, Finland. <http://www.mediateam.oulu.fi/publications/pdf/87.pdf> Hämtat den 11 april 2006.
32 G. Lee och Sin-Chong Park *Bluetooth Security Implementation based on SoftwareOriented Hardware-Software Partition* Information and Communications University, Republic of Korea <http://ieeexplore.ieee.org/iel5/9996/32111/01494702.pdf?tp=&arnumber=1494702&isnumber=32111> Hämtat den 11 april 2006.
33 T. Muller *Bluetooth Security Architecture* . 1999.<http://bluetooth.com/NR/rdonlyres/C222A81E-D9F9-48CA 91DE-9C81F5C8B94F/0/Security_Architecture.pdf> Hämtat den 8 april 2006.
34 M. Björnsson *Bluetooth in Secure Products .2001* <http://www.lysator.liu.se/~martinb/Bluetooth/Bluetooth_in_Secure_Products.htm>
35 Y. Shaked och A, Wool *Cracking the Bluetooth PIN.* 2005. School of Electrical Engineering Systems <http://www.eng.tau.ac.il/~yash/Bluetooth/> Hämtat den 11 april 2006.
36 A. Laurie, *Serious flaws in bluetooth security lead to disclosure of personal data* <http://www.thebunker.net/security/bluetooth.htm> Hämtat den 11 april 2006
37 Bluetooth special interest group. ***Wireless Security*** <http://www.bluetooth.com/Bluetooth/Learn/Security/> Hämtat den 13 april 2006.