Säkerheten kring internetpoker

Richard Bolinder, Johan Uppman, Jim Utter, Antonio Vahabi,
Pontus Wallberg, Robin Westin

Linköpings universitet

Linköping
2007-11-05

Sammanfattning

Syftet med studien har varit att granska säkerheten kring poker på internet. Detta genom att redogöra för vilka säkerhetsåtgärder som företag bakom pokersidor vidtar, samt påvisa eventuella brister. För att göra detta kontaktade vi, via mail, sju företag som tillhandahåller pokertjänster på internet. Utifrån informationen de delade med sig av, samt den från deras hemsidor kunde vi fördjupa oss inom specifika säkerhetsaspekter. De aspekter vi valt att titta närmare på är brandväggar, kryptering, slumptalsgeneratorer, vad så kallade botar är och hur de förhindras. I stort kom vi fram till att säkerheten är hög men att det finns vissa mindre brister att förbättra.

En annan del av syftet har varit att jämföra den uppfattning studenter i allmänhet har om säkerheten kring internetpoker med vår uppfattning grundad på studien av spelsidorna. Vi genomförde därför en enkätundersökning bland studenter vid Linköpings universitet. I enkäten ställde vi frågor rörande hur de uppfattar säkerheten kring poker på internet. Resultaten visade att personerna i fråga hade en tvetydig syn på säkerheten. I allmänhet pekade studenternas svar på en relativt god säkerhet, men även att de uppfattar att det är vanligt förekommande med fusk, pengatvätt och annan brottslig aktivitet. Detta anser vi till viss del kan bero på de bilder media förmedlar. Vi menar att många uppfattar säkerheten som sämre än vad den är. Vi tror att människor lägger mindre tilltro till processer de saknar kunskap om och det är därför vi har en större tillit till säkerheten kring poker på internet.

Innehållsförteckning

Inledning

Poker har på senare tid blivit mer och mer populärt och pokersidorna på internet har blivit fler. I och med att mer pengar har kommit i omlopp den senaste tiden har säkerhetsfrågan blivit mer uppmärksammad, bland annat av media. Det finns många uppfattningar om hur bra säkerheten egentligen är, bland annat finns det de som tror att det är säkrare att spela över internet än att sitta runt ett bord med andra människor och riskera fuskblandningar, tjuvkikningar eller annat liknande. Andra tror att internetpoker inte alls är säkert.

Syfte

Projektets syfte är att kontrollera vilka åtgärder spelbolagen vidtar för att garantera säkerhet, samt undersöka hur väl studenters uppfattning av säkerheten kring internetpoker stämmer överens med en säkerhetsbild grundad på resultaten av detta arbete. Frågeställningarna vi jobbat med är följande: Hur säkert skyddas användares person- och kontouppgifter? Hur säkert skyddas informationsflödet mellan server och klient från utomstående? Kan man lita på den slumpningsmetod som används för att ”dela ut” spelkorten? Vad är och hur förhindras användandet av så kallade botar? Hur är studenters uppfattning om säkerhet kring internetpoker jämfört med vår uppfattning efter denna studie?

Avgränsningar

Vi har avgränsat oss till att endast behandla specifika protokoll eller funktioner istället för att ta upp hur den typen av protokoll/funktioner fungerar i allmänhet. Vi har inriktat oss på Secure Socket Layer (SSL) vad det gäller krypteringprotokoll och Message-Digest algorithm 5 (MD5) vad det gäller hash-funktioner. Anledningen till detta är att de är de mest använda enligt den uppfattning vi fått när vi kontaktat företagen eller läst på deras hemsidor. Vi har valt att fokusera på etablerade pokersidor eftersom de har flest användare och därmed är mest relevanta för denna undersökning.

Metod

Eftersom ingen av oss hade några större förkunskaper kontaktade vi sju pokersidor som verkar stora, då de syns mycket i media. Via mail ställde vi frågor (se bilaga 2) om hur de garanterar sina spelare säkerhet. För att få ytterligare information läste vi också på deras hemsidor. Utifrån denna information fördjupade vi oss i vissa säkerhetsåtgärder som företagen vidtagit, detta för att kunna reflektera kring säkerheten.

Vi gjorde även en undersökning där vi bad 100 studenter fylla i en enkät (se bilaga 1). Vi valde att fråga 100 studenter eftersom vi anser att det ger en någorlunda representativ bild samtidigt som sammanställningsprocessen blir relativt smidig. Vi utformade denna enkät så att även de med begränsad teknisk kunskap och som inte spelat poker på internet skulle kunna svara på frågorna. Vi valde att ställa frågor som skulle ge oss inblick i vad studenter tänker om olika säkerhetsaspekter och ge oss en uppfattning om hur olika grupper ser på säkerheten.

Källor

I vår källdiskussion har vi valt att granska de fem källor som varit mest centrala för arbetet, en för varje område.

Informationen om brandväggar har vi främst tagit från boken *Brandväggar, 2:a upplagan*. Den är skriven 2002 av Matthew Strebe och Charles Perkins. När de skrev boken var Strebe Chief Technology Officer vid Consulting Network Integration Corporation (Connectic) och Perkins Senior Network Systems Analyst vid samma konsultföretag. Den information vi använt är relativt allmän och eftersom brandväggar i grund fungerar på samma sätt idag som då boken skrevs, anser vi att informationen är trovärdig trots bokens ålder.

I avsnittet om SSL var *Security Technologies for the World Wide Web (Second Edition)* den viktigaste källan. Denna är skriven 2002 av Rolf Oppliger som då var doktor inom datavetenskap. Boken är relativt gammal när man tänker på hur snabbt utvecklingen går inom tekniska områden. Men vi anser att den trots allt är trovärdig eftersom senaste versionen av SSL funnits sedan 1996.

Artikeln *Improved Collision Attacks on MD4 and MD5* var viktigaste källan om MD5. Den är skriven av två studenter och två doktorer. Studenterna studerade Information and Computer Engineering. Båda doktorerna jobbar med informationssäkerhet. Artikeln publicerades 2007 av Institute of Electronics, Information and Communication Engineers (IEICE). De utger sig för att vara ett av världens främsta institut inom området.

Sidan random.org var den mest centrala källa rörande slumptalsgeneratorer. Sidans ansvarige är Doktor Mads Haahr. Han föreläser på avdelningen ”School of Computer Science and Statistics” vid Trinity College, Dublin. Han leder en forskningsgrupp som heter Distributed Systems Group. Gruppen består av doktor Peter Barron och just nu fem forskarstudenter. Trots att sidan inte ingår i en edu-domän känns den seriös med tanke på utbildningsnivån på personen bakom sidan.

Den viktigaste källan om pokerbotar var *Improved Opponent Modeling in Poker*. Denna artikel är skriven av Aaron Davidson, Darse Billings, Jonathan Schaeffer och Duane Szafron vilka alla tillhör Department of Computing Science, Univeristy of Alberta. Detta gör att vi anser källan trovärdig. Källan är relativt gammal, då den utkom 2000. Vi anser att det inte gör så mycket eftersom vi tar upp pokerbotar i stort och konceptet är detsamma.

Resultat

Undersökning

Vi skickade ett mail (se bilaga 2) till sju olika sidor vilka tillhandahåller pokertjänster på internet. Vi valde att skicka till: 24hPoker.com, Betsson.com, Betway.com, PacificPoker.com, PartyPoker.com, Pokerstars.com och Svenskaspel.se. Anledningen till att vi valde just dessa sidor var att de syns mycket i media och därför uppfattar vi dem som bland de största. Det vi ville få ut av mailen var främst vilka metoder och typer av säkerhetsåtgärder företagen vidtar så att vi kunde läsa vidare om dessa.

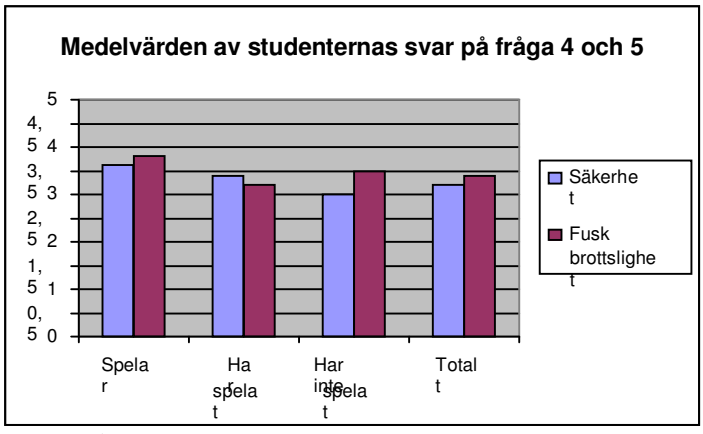
Vi fick endast svar från tre sidor, Betsson.com, Betway.com samt Pokerstars.com. Detta tror vi delvis beror på att de inte vill ge ut specifik information om säkerheten. Dessutom hade vi endast tillgång till kundtjänsternas mailadresser på de olika sidorna och förmodligen saknar de ingående kunskap om den tekniska delen av säkerhetsåtgärderna.

Svaren vi fick var dock inte speciellt detaljerade. I två fall hänvisades vi till speciella tekniska enheter för mer information, dock fick vi inga kontaktuppgifter till dessa. Den enda användbara informationen var i stort sett samma som den vi hittade på företagens hemsidor. Via svaren och hemsidorna uppgav de att de använder sig av SSL version 3 för att kryptera dataflödet mellan klienter och servrar, brandväggar för att skydda sina databaser där de lagrar person- och kontouppgifter samt program som letar efter kända botar.

Studenters uppfattning

För att sedan jämföra säkerhetsbilden, grundad på studien av dessa säkerhetsaspekter, med studenters uppfattning delade vi ut 100 enkäter med frågor om vad de anser om säkerheten kring internetpoker. Av studenterna var 68 män och 32 kvinnor och alla studerade på Linköping universitet. Totalt var det sex av dessa som aktivt spelar poker på internet, 29 som har spelat tidigare och 65 som aldrig har spelat. Att sex personer spelar låter kanske lite, men sex procent av studenterna utgör en relativt stor grupp. De 29 som har spelat slutade huvudsakligen på grund av pengabrist, intressebrist, tidsbrist eller så ville bara prova på.

Bredvid finns medelvärden uträknade från svaren vi fick på enkäterna. Vi har valt att ta ett medelvärde på de tre delfrågorna till frågorna 4 och 5 (se bilaga 1) och kategorisera dem som säkerhet respektive frekvens av fusk eller brottsliga aktiviteter. Detta för att skapa en mer överskådlig bild av resultatet.



Figur 1

Resultatet (se bilaga 1) tyder på att kvinnor i allmänhet har mindre tilltro till säkerheten än män. De tror även att fusk förekommer mer frekvent. Om vi hade haft en jämnare fördelning mellan könen så är det troligt att vi fått ett snitt med mindre tilltro till internetpoker.

I de följande kapitlen förklarar vi närmare några av de åtgärder pokersidor använder sig av för att garantera säkerhet. En viktig del av säkerheten är att skydda konto- och personuppgifter, vilket innebär att neka utomstående åtkomst till servrar där informationen finns lagrad. Det vanligaste sättet för att göra detta är att använda brandväggar, som vi allmänt beskriver nedan.

Brandväggar

När man ansluter ett lokalt nätverk till internet ansluts det egentligen direkt till alla andra nätverk som är kopplade till internet. En oskyddad anslutning gör det enkelt för hackare att utnyttja privata nätverksresurser. Det finns ingen centralt inbyggd säkerhetskontroll eller internetmyndighet som håller reda på alla som är anslutna. (Strebe, 2002)

Stora företag, exempelvis spelföretag, har interna datanät. På grund av internets öppenhet vill man inte direktansluta dessa känsliga nät. Istället avgränsar man företagsnätet och ansluter det till internet på ett kontrollerat sätt med hjälp av brandväggar. (Strebe, 2002)

Med brandväggar skapar man kontrollpunkter vid gränserna för det privata nätverket. Det är brandväggen som avgör om informationen ska skickas vidare eller stoppas och detta beror på hur brandväggen är programmerad. Om den är rätt konfigurerad och inte innehåller brister som kan utnyttjas, kommer nätverket vara relativt säkert. (Strebe, 2002)

Hos ett företag är brandväggen en separat nätverksenhet som sitter mellan internet och det lokala nätet och filtrerar trafiken. Privatpersoner använder oftast mjukvarubrandväggar som installeras direkt på persondatorn. Båda varianterna stänger helt av vissa portar och tjänster som inte används, vilket effektivt hindrar missbruk av dessa. Andra portrar lämnas öppna, men övervakas och trafik tillåts endast mot kända och accepterade adresser. (Strebe, 2002)

Det finns två vanliga typer av brandväggar, paketfiltrerande och proxy. Fördelen med de paketfiltrerande är att de är snabba och inte tar kraft från nätverket. Det beror på att datorn kommunicerar med kända adresser genom att kontrollera IP-adresser i varje paket och accepterar inte okänd trafik. Proxy däremot kräver mer resurser för att fungera och arbetar på applikationsnivå. De är mer avancerade och svårare att konfigurera. (Strebe, 2002)

Svagheter

Många privatpersoner med internetanslutning saknar dessvärre det grundläggande skydd som en brandvägg ger. Dock är ingen brandvägg helt säker och många vet inte hur man konfigurerar en brandvägg för maximalt skydd. Det krävs även andra åtgärder för att säkerställa en god datasäkerhet. I större system och nätverk brukar det finnas program som övervakar trafiken och slår larm om något ovanligt eller otillåtet sker. Problemet med detta sätt att övervaka trafiken är att det är svårt att skilja normal trafik från onormal. Sätter man gränsen för högt kommer man att översvämmas av larm, sänker man gränsen riskerar man att missa de verkliga attackerna. (Strebe, 2002)

Då de som försöker tränga in i olika system hela tiden vidarutvecklar sina angreppsmetoder måste även försvaret ständigt utvecklas. Tyvärr är det omöjligt att upptäcka alla angrepp och ofta hinner säkerhetansvariga inte åtgärda något innan attacken är i full gång. (Strebe, 2002)

Ovan har vi tagit upp hur lagrad information skyddas. Vid användandet av internetpoker skickas även ständigt information mellan server och klienter. Detta informationsflöde skyddas från

”avlyssning” och manipulation bland annat genom att man krypterar informationen. Ett protokoll som används av många pokersidor är SSL version 3, vilket vi beskriver nedan.

Kryptering med Secure Socket Layer

Secure Socket Layer (SSL) arbetar över TCP/IP-protokollet, vilket används för all internettrafik idag. Detta innebär att alla olika typer av överföringar på internet kan ske säkert med SSL, allt från e-post (POP3) till filöverföring (FTP) och HTTP. SSL version 3 har funnits sedan 1996 och är ett av de mest använda säkerhetsprotokollen av sitt slag och det finns inbyggt i alla ledande webbläsare. (Oppliger, 2002)

Uppbyggnad

Protokollet består av fem delar: SSL Handshake Protocol, SSL Change Cipherspec Protocol, SSL Alert Protocol, SSL Application Data Protocol och SSL Record Protocol. Nedan kommer förklaringar främst på SSL Handshake Protocol och SSL Record Protocol som är de två viktigaste delarna, men även kortare förklaringar på de övriga delarna. (Oppliger, 2002)

SSL Record Protocol

Det här protokollet är huvudprotokollet och alla andra protokoll arbetar mot detta. Men det är inte bara en länk mellan de övriga underprotokollen utan har även en mycket viktig uppgift själv. (Oppliger, 2002)

SSL Record Protocol är den del som krypterar och dekrypterar den data som skickas. Protokollet får all sina data från övriga protokoll och från TCP/IP-protokollet. När den får en mängd data så delar den upp datan i fragment som den senare komprimerar. Därefter så krypterar eller dekrypterar den de komprimerade datafragmenten. För att kryptera/dekryptera dessa använder sig protokollet av de nycklar, certifikat och algoritmer som bestämts av handskakningsprotokollet. (Oppliger, 2002)

SSL stödjer ett antal olika algoritmer för kryptering, nyckelframtagning och signering och använder sig av kryptering för både symmetriska och asymmetriska algoritmer. Vanligen används de asymmetriska algoritmerna endast vid utbyte av nycklar då de är betydligt långsammare, medan de symmetriska algoritmerna används efter att det steget är fullbordat. I regel tar det längre tid att överföra data med hög säkerhet än med låg, vilket medför att man inte alltid använder algoritmer av högsta möjliga säkerhet. (Smas, 2002)

Protokollet har också hand om en annan mycket viktig säkerhetsparameter, den lägger nämligen till ett MAC till varje sändning. Denna SSL MAC innehåller dels information om hur mycket data som sänds men också en stor mängd andra parametrar för att garantera att datan förblir oförändrad. En av de parametrar som används för att garantera att datan inte förändras av någon på vägen är unika värden som genereras av MD2 och MD5 (se kapitel Message-Digest Algorithm 5). (Oppliger, 2002; Elgamal & Hickman, 1997)

SSL Handshake Protocol

SSL Handshake Protocol är det protokoll som inleder en överföring. Det går till på följande sätt. Klienten börjar med att skicka information till servern. Denna information handlar bland annat om vilken SSL-version klienten använder och vilka algoritmer som stöds, samt slumpmässigt framtagen data som senare kommer att användas för att skapa så kallade sessionsnycklar. När servern fått detta skickar den tillbaka information om vilka av algoritmerna den klarar, ett certifikat som identifierar servern och slumpmässigt framtagen data. Servern kan här kräva att klienten identifierar sig om det är av betydelse. (Smas, 2002)

När klienten får datan från servern börjar den med att kontrollera att certifikatet den fick har en utfärdare som finns med på listan över godkända utfärdare. Även signaturen kontrolleras så att den stämmer överens med servern och den som äger certifikatet. (Smas, 2002)

Efter detta tillverkar klienten en ”premaster key” från de unika data som servern och klienten skickat till varandra under sessionen. Nyckeln som skapas krypteras med serverns publika nyckel som finns i certifikatet och skickas sen till servern. Om servern har krävt identifikation signerar klienten data som skickas tillsammans med klientens certifikat. Om servern fått in ett certifikat kontrolleras detta av servern. Om allt är som det ska skapar server en ny nyckel, ”master key”, utifrån den premaster key som servern fick från klienten. (Smas, 2002)

Denna master key används sedan i sin tur för att generera de sessionsnycklar som ska användas för kryptering, dekryptering och signering. När detta är utfört skickas ett meddelande ut från klienten att kommunikationen från denna punkt och framåt skickas krypterad utefter de sessionsnycklar som skapats för just den här sessionen. Vilket innebär att nu måste klienten också utföra processen att utifrån sin premaster key generera en master key samt utifrån den skapa sessionsnycklarna som behövs. Sen skickas ett meddelande, vilket är krypterat, för att tala om att initieringen av sessionen är avklarad. Därefter gör servern samma sak, det vill säga skickar ett meddelande för att tala om att kommunikationen övergår nu till krypterad form och skickar sedan ett krypterat meddelande som talar om att även servern är klar med initieringen. (Smas, 2002)

De övriga protokollen

När handskakningsfasen är klar och man ska gå över till en annan typ av algoritmer och kryptering anropas SSL Change Cipherspec Protocol. Det används också när man ska byta algoritmer mitt i en pågående överföring. SSL Alert Protocol sköter de olika larmmeddelanden som kan skickas. Varje larm innehåller information om hur allvarligt felet är och en beskrivning på vad som gått fel. SSL Application Data Protocol används för att skicka och ta emot datan som färdas över internet. Man skulle kunna säga att det är en länk mellan SSL Record Protocol och HTTP, FTP, POP3, med flera. (Oppliger, 2002)

Säkerhet

Ett tecken på att SSL är ett mycket säkert protokoll är att det fortfarande efter tio år är det mest ändvända protokoll för säker dataöverföring. Trots detta så har SSL ett par brister även om de inte är stora. Blanda annat så skyddar det inte mot attacker som går ut på att man analyserar faktorer, som mängd skickad data eller vilka som sänder data mellan varandra. Detta kan ge insikt i vad datan innehåller. (Oppliger, 2002)

Att SSL arbetar över TCP/IP-protokollet har många fördelar, men det medför också att de typer av attacker som är riktade direkt mot TCP/IP-protokollet inte kan stoppas av SSL. Det finns attacker som riktar sig mot TCP/IP och går ut på att man tar över någon annans anslutning och på så sätt får tillgång till all data i ett okrypterat format. (Oppliger, 2002)

Som vi redan nämnt används MD5 för att säkerställa att informationen inte har ändrats. MD5 är en så kallad hash-funktion. Hash-funktioner kan användas till mycket, men vi kommer här endast ta upp hur de används inom kryptografi. I detta område används de för att skapa en liten sträng av tecken från en längre text, exempelvis en fil. Denna lilla sträng kallas ibland för digitalt fingeravtryck och används för säkerhetskontroller. (Alström, 2007)

Hash-funktionen Message-Digest algorithm 5

Message-Digest algorithm 5 (MD5) är en hash-funktion som funnits sedan 1992. Eftersom funktionen är så gammal kan man tycka att den borde vara föråldrad och osäker. Det stämmer att den innehåller brister. Men faktum är att MD5 fortfarande används, exempelvis i SSL och som slumptalsgenerator. (Cassava Enterprises (Gibraltar) Limited, 2007; Sasaki m.fl., 2007)

Som nämnt skapar en hash-funktion en liten teckensträng från en längre text. Den lilla sträng som genereras kallas hash-värde och det varierar inte i storlek beroende på textens längd utan är av en bestämd storlek. MD5 skapar hash-värden som är 128 bitar. Utifrån hash-värdet ska man inte kunna återskapa eller gissa originaltexten. Värdet ska också vara unikt för originaltexten. Det ska inte finnas två olika texter med samma hash-värde. Att skapa ett unikt värde är dock omöjligt att uppnå eftersom hash-värdet har en bestämd längd. Detta då antalet olika hash-värden är mycket färre än möjliga kombinationer i originaltexter. (Alström, 2007)

När MD5 beräknar hash-värdet börjar funktionen med att anpassa texten så att den kan delas upp i delar där varje del är 512 bitar stor (T_0, T_1, T_2, ..., T_{n-1}). Ett värde beräknas för varje del utifrån värdet från föregående del och delen själv (H_1 beräknas exempelvis med T_0 och H_0). Värdet på H_0 är förbestämt. H_n blir hash-värdet för hela texten. (Sasaki m.fl., 2007)

Själva beräkningen av nästa hash-värde sker via en kompressionsfunktion. Hur denna fungerar är relativt komplicerat och kommer därför bara ytligt beskrivas här. Textdelen som är 512 bitar stor delas in i 16 delar där varje del blir 32 bitar. Värdet beräknas i 64 steg och beror på 4 stycken variabler. En av variablerna ändras utifrån en booleansk funktion i varje steg. Denna funktion ändras i sin tur fyra gånger under de 64 stegen. (Sasaki m.fl., 2007)

Kollisioner

En kollision sker då två olika texter har samma hash-värde. Wang Xiaoyun med flera arbetade 2005 fram en procedur som generar kollisioner. Denna har sedan förbättrats vilket har gjort attacken bättre. Då det är en alltför komplicerad procedur för att tas upp här hänvisas intresserade till *Improved Collision Attacks on MD4 and MD5*. (Sasaki m.fl., 2007)

Hash-värden används ofta vid digital signering av en fil eller ett meddelande. Stämmer värdet överens med texten tolkar man det som att texten är oförändrad och alltså trovärdig. Detta är en säkerhetsrisk i vissa sammanhang. Om exempelvis Olle skickar en bekräftelse till Kalle där det står att Kalle ska få 40 kr av Olle. Med bekräftelsen skickas även hash-värdet så att äktheten ska kunna bevisas. Men om Kalle kan hitta ett meddelande med samma värde fast det står att Kalle ska få mer pengar kan han utnyttja detta eftersom han kan bevisa att hash-värdet stämmer. (Alström, 1997)

När man spelar poker i verkligheten blandar man kortleken för att vara säker på att spelarna inte vet vilken ordning korten kommer i. Men hur blandar man en digital kortlek? Man använder sig av så kallade slumptalsgeneratorer. Hur dessa fungerar beskrivs i följande kapitel.

Slumptalsgeneratorer

Att kunna slumpa fram tal är en viktig egenskap och används idag till många olika saker. Det används bland annat för att skapa krypteringsnycklar, simuleringar, skapa modeller av komplexa fenomen, datorspel eller hasardspel. Att slumpa fram tal idag görs med datorer. Det är inte så enkelt att göra, eftersom en dator följer instruktioner, vilket gör att den är förutsägbar. Det har kommit fram lösningar på problemet och idag används två typer av slumptalsgeneratorer. Första varianten

heter pseudoslumptalsgenerator (eng. pseudo-random number generator), vilket brukar förkortas till PRNG och beräknas i mjukvaran. Den andra kallas för äkta slumptalsgenerator (eng. true random number generator) och brukar förkortas som TRNG, och beräknas med hårdvara. (Haar, 2007)

Pseudoslumptalsgenerator, PRNG

PRNG är en algoritm, som använder en matematisk formel eller en redan färdiguträknad tabell, för att producera sekvenser av nummer. Det första talet i en nummersekvens brukar kallas för frö. Ett vanligt sätt är att man bygger resten av siffrorna beroende av fröet. Man använder en så kallad rekursiv algoritm, som beräknar nästkommande tal genom föregående tal. Tanken med PRNG är att de ska se så naturligt slumpmässiga ut som möjligt. Det har lagts ner mycket pengar på forskning inom PRNG-algoritmer, vilket har lett till att många moderna PRNGs ser ut att vara helt slumpmässiga. Ett exempel på en PRNG-algoritm är linjär kongruensgenerator. Den är enkel och mycket snabb. Formeln ser ut på följande sätt:
$X_{n+1} = aX_n + c \pmod m$, där a, c samt m är heltalskonstanter. (Haar, 2007; Nijm 2007)

PRNG är användbar exempelvis till simulering och modellering eftersom den är effektiv och kan producera nummer snabbt, vilket är bra om programmet den används i använder många olika nummer. Den genererade nummersekvensken kan återskapas senare, om man vet startpunkten, vilket är nyttigt om man behöver använda samma nummersekvens vid ett senare tillfälle. Dock är den periodisk, vilket inte är en önskvärd egenskap. Därför är moderna PRNGs perioder så långa att de i praktiken oftast inte blir en negativ faktor. (Haar, 2007)

Äkta slumptalsgenerator, TRNG

TRNG kan enkelt förklaras på följande sätt. En dator läser av ett fysikaliskt fenomen som generar ett värde, vilket sedan kommer tolkas av datorn på ett visst sätt, genom förbestämda regler. Sedan när reglerna har uppfyllts på ett eller annat sätt, kommer ett tal att produceras, ett äkta slumptal. Det är ett äkta slumptal, eftersom hur talet genererades inte kan återskapas. Det innebär att siffror kan upprepas, men vägen fram skiljer sig alltid. (Haar, 2007)

Det finns mängder av olika källor, fysikaliska fenomen, som kan användas för att fånga in slumpmässighet. Det är nästan bara fantasin som sätter gränserna, men man ska vara noga med att räkna in alla faktorer. Ett exempel på källa kan vara bakgrundsljudet från ett kontor. Här måste man akta sig för mönster i ljudet. Till exempel kan ljudet från en datorfläkt vara en bidragande faktor. En fläkt är en roterande maskin och därmed kan ljudet upprepas. I slutändan kan detta ha lett till att vi inte fått äkta slumpmässighet. Det finns däremot fenomen som är helt slumpmässiga, ett exempel är nedbrytningstiden för radioaktiva ämnen. Tjänsten HotBits använder sig av det radioaktiva ämnet Cesium137. De mäter tiden mellan varje skapat betapar, det vill säga när Cesium137 skjuter ifrån en elektron, omvandlar en neutron till en proton och förändras till Barium137. De sparar värdet för tiden, för att jämföra med värdet för nästa. Om första tiden är större än andra blir det till en etta. Är första däremot mindre än andra blir det till en nolla. Skulle tiderna vara samma, slängs jämförelsen och nästa två värden jämförs. (Haar, 2007; Walker, 2007)
TRNG är bra till exempelvis hasardspel, datorspel och kryptering eftersom den återger äkta slumptal och inte har någon period. En given sekvens av nummer som genererats av TRNG kan heller inte återskapas. Dock är den ineffektiv jämfört med PRNG. (Haar, 2007)

Svenska Spel

För att demonstrera hur slumptalsgeneratorer används i realiteten har vi valt att beskriva den slumptalsgenerator som används av Svenska Spel. Vi valde den eftersom Svenska spel är en stor pokersida och ger ut generös information om hur deras slumptalssystem är uppbyggt.

Boss Media (se www.bossmedia.com) har skapat det elektroniska spelsystemet för poker som Svenska Spel använder. Först använder de sig av TRNG. Eftersom det är en TRNG måste den använda sig av fysikaliska fenomen, vilket den gör genom två oberoende analoga Zener-dioder. Dioderna framkallar elektroniskt vitt brus, vilket enkelt förklarat är oförutsägbara elektriska signaler. Bruset används för att skapa slumpmässiga bitströmmar. Dessa kommer sedan att filtreras genom von Neumann-korrigering, vilket innebär att ett par bitar analyseras. Är bitarna olika används första biten som värde, skulle bitarna vara lika kastas paret. De resulterande bitarna, äkta slumptal, kommer att sparas i buffertar, som är kopplade till kanaler. Ett slumptal kommer sedan skickas genom kanalen, slumptalet kommer vara fröet för en PRNG. Det är sedan denna PRNG som skapar slumptal för klienten, till exempel vilket kort ur leken som ska dras i en pokerrunda. (www.svenskaspel.se, 2007; ICATT Interactive Media, 2007)

I spel som poker där beräkningar, kring exempelvis sannolikhet, har en ganska stor betydelse är det vanligt att så kallade botar utvecklas. Botar är datorprogram som agerar istället för mänskliga spelare. Dessa program kan sedan användas på pokersidor vilket klassas som fusk.

Pokerbot

En pokerbot är ett komplicerat dataprogram som spelar poker. Det bygger på artificiell intelligens (AI). Pokerbotar ska genom AI-system ta sig an ett av de svåraste problemen som finns inom datateknik, det vill säga hur man hanterar kunskap som är ofullständig eller felaktig. Inom poker är faktorerna väldigt många och alla dessa ska räknas in när ett beslut ska tas. Man måste räkna med gömd information, exempelvis de andra spelarnas kort. Boten måste kunna bluffa för egen vinning och kunna upptäcka och agera om motståndaren gör det. Den ska kunna planera sin satsning i förhållande till kort, andra spelares intäkter, pottstorlek och chansen att vinna med en viss hand. (Davidson m.fl., 2007)

Idag finns ett flertal pokerbotar, de flesta är skapade av olika universitet. De bästa botarna deltar i den årliga tävlingen, AAAI Computer Poker Competition. Några exempel på botar är BluffBot skapade av Teppo Salonen, Polaris skapad av University of Alberta och GS3 skapad av Carnegie Mellon University. (Salonen, 2007 & University of Alberta, 2007).

Skydd mot botar

Vanligtvis när man spelar poker på internet måste man ladda ner ett klientprogram till datorn. Medan man spelar kan programmet söka igenom aktiva filer och program efter misstänksam aktivitet. Upptäcks något suspekt skickas en rapport till pokerföretaget, som vidtar vidare åtgärder. (www.partypoker.com, 2006)

Avslutande diskussion

”Hur säkert skyddas användares person- och kontouppgifter?” var den första frågan vi ställde i arbetet. Som vi tidigare nämnt utgör brandväggar en stor del av skyddet. Vi tror att det är detta som är den svagaste delen av alla säkerhetsåtgärder runt internetpoker. Trots att brandväggarna ständigt utvecklas så kommer de förmodligen aldrig bli riktigt säkra. Då brandväggar är en av de vanligaste säkerhetsåtgärderna är det också vanligt att hackare vill ta sig runt dem. Detta har skapat en viss efterfrågan av fungerande attacker, vilket driver på utvecklingen av dem. Företagens servrar, där uppgifterna finns lagrade, är förmodligen skyddade av brandväggar som är konfigurerade på ett säkrare sätt än de brandväggar privatpersoner använder. Det borde alltså vara lättare att ta sig in i någons privata dator som också skulle kunna innehålla konto- eller personuppgifter. Dock är det antagligen mer attraktivt för en hackare att komma åt en databas med många användares uppgifter. Alltså ligger fortfarande mycket av säkerhetsansvaret på företagen.

En annan av frågorna vi ämnade besvara var ”Hur säkert skyddas informationsflödet mellan server och klient från utomstående?”. Informationen skyddas med kryptering. Men hur säker är den kryptering som används av pokersidorna? Många sidor använder SSL, vilket har ett par brister: attacker som bygger på analyser av faktorer och TCP/IP-attacker. ”Analysattackerna” går ut på att ta reda på vad den krypterade informationen handlar om och inte det exakta innehållet. Vi anser att det inte är en säkerhetsbrist om hackare kan ta reda på när exempelvis kontouppgifter skickas eftersom de sedan är tvungna att knäcka själva krypteringen för att informationen ska vara användbar. TCP/IP-attacker är något som riktar sig mot de två datorer som kommunicerar. För att lyckas med en sådan attack måste man alltså ta sig förbi brandväggar och dylikt. Spelarnas datorer är den svaga delen eftersom servern troligtvis har bättre skydd. Att någon knäcker själva krypteringen är enligt vår uppfattning inte troligt.

Svagheten hos MD5 tror vi heller inte är farlig när man använder funktionen vid dataöverföring. En bluffsida skulle kanske kunna utnyttja kollisioner för att kräva folk på pengar (om sidan är Kalle och användaren är Olle i exemplet i avsnittet om kollisioner, sid 7). Omvänt är detta troligtvis mycket svårare då seriösa sidor förmodligen gör detta i flera steg och därmed försvårar förfalskningen. Dessutom används kryptering som borde göra det i princip omöjligt.

Tredje frågan vi ställde var ”Kan man lita på den slumpningsmetod som används för att ”dela ut” spelkorten?” Vi anser att de tekniker som används för att slumpa fram korten fungerar tillräckligt bra för att man inte ska kunna förutsäga nästkommande kort. Då en TRNG används så är detta garanterat men för PRNG är det kanske teoretiskt möjligt att skriva ett program som tar reda på vilka slumptal som kommer genereras. Men vi tror att de serier som generas har för långa perioder för att det ska vara praktiskt möjligt.

”Vad är och hur förhindras användandet av så kallade botar?” Pokerbotar är program som agerar som en spelare utan en människas påverkan. Det var svårt att hitta information om hur användandet förhindras. Vi tror att det delvis beror på att företagen inte vill dela med sig av allt för detaljerad information om sina säkerhetssystem. En annan faktor tror vi är att detta är ett så pass specifikt problem för poker- och casinosidor att det inte finns några oberoende sidor, vad vi kunde hitta, som publicerar information om detta. Dock tror vi att risken att man stöter på en bot är relativt liten eftersom dagens botar inte är så bra och därmed inte eftertraktade.

En annan fråga vi ställde oss var ” Hur är studenters uppfattning om säkerhet kring internetpoker jämfört med vår uppfattning efter denna studie?” Undersökningen vi gjorde omfattade 100 studenter

från cirka 20 olika utbildningar. Eftersom vi fick svar från så många utbildningar så anser vi att undersökningen ger en trovärdig bild av studenters uppfattning om säkerheten.

Dock är det lite förvånande att vissa som litar på säkerheten ändå tror att förekomsten av fusk och dylikt är stor. Detta kan man även se på medelvärdena, dock syns det inte lika tydligt där. Detta tror vi i delvis kan bero på den tvetydiga bild media framställer. Där framhålls ibland att det är farligt och att man kan bli lurad av att spela på nätet. Samtidigt säger de att antalet som spelar blir fler och fler och att många tjänar mycket pengar på det, vilket kan skapa en bild av att det är säkert.

Ur resultaten kan vi också utläsa att studenter i genomsnitt inte har samma tilltro till säkerheten som vi anser vore befogat. De tror också att brottsliga aktiviteter och fusk förekommer oftare än vad vi fått uppfattning om. Resultaten antyder också att denna skillnad skulle öka om fördelningen mellan män och kvinnor varit jämnare eftersom kvinnor i snitt tror sämre om säkerheten och att fusk förekommer oftare (se figur 1). Dock är det kanske bättre att jämföra med snittet för de manliga deltagarna i undersökningen eftersom vi är män. Vid en sådan jämförelse har vi högre tilltro till säkerheten. Vi tror att detta till viss del beror på att människor generellt lägger mindre tilltro till processer de saknar kunskap om.

Som sammanfattning har vi kommit fram till att poker på internet är relativt säkert med avseende på de tekniska delarna. Den verkliga faran ligger exempelvis hos bluffsidor eller spelberoende.

Referenslista

Tryckta källor

Amström, Magnus (1997). *Digital Signature Service Module*. Linköpings universitet, LiTH, IDA.

Davidson, Aaron & Billings, Darse & Schaeffer, Jonathan & Szafron, Duane (2000). Improved Opponent Modeling in Poker. *Proceedings of the 2000 International Conference on Artificial Intelligence,* s 1467-1473.

Elgamal, Taher & Hickman, Kipp, E. B. (1997). *Secure Socket Layer Application Program Apparatus and Method*. [patent] US5657390.

Nijm, Toni (2002). *Slumptalsgeneratorer för Säkerhetssystem.* Linköpings universitet, LiTH, ISY.

Oppliger, Rolf (2002). *Security Technologies for the World Wide Web (Second Edition).* Artech House, Incorporated.

Sasaki, Yu & Naito, Yusuke & Kunihiro, Noboru & Ohta, Kazuo (2007). Improved Collision Attacks on MD4 and MD5. E90A: *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* nr 1, s 36-47.

Smas, Jörgen (2002). *Säker webaccess till ett samhällsviktigt datorsystem.* Linköpings universitet, LiTH, IDA.

Strebe, Matthew & Perkins Charles (2002). *Brandväggar, 2:a upplagan.* Pagina Förlag AB.

Otryckta källor

Haar, Mads (2007). *What's this fuss about true randomness?* [www] <http://www.random.org/> Hämtad 2007-10-23

Cassava Enterprises (Gibraltar) Limited (2007). *Fair Games* [www] <http://www.pacificpoker.com/en/online-poker-fairness/fair-games--4.htm> Hämtad 2007-10-23

ICATT Interactive Media (2005). *Random Numeber Generator* [www] <http://www.randomnumbergenerator.nl/> Hämtad 2007-10-23

PartyPoker (2006). *PartyGaming's Unfair Advantage Policy* [www] <http://www.partypoker.com/about_us/game_fairness/unfair_advantage.html> Hämtad 2007-10-29

Salonen, Teppo (2006). *BluffBot* [www] <http://www.bluffbot.com/> Hämtad 2007-10-23

Svenska Spel (2006). *Så fungerar slumptalsgeneratorn för poker* [www] <http://www.svenskaspel.se/media/pdf/slumptalsgenerator.pdf> Hämtad 2007-10-23

University of Alberta (2007). *The First Man-Machine Poker Championship* [www] <http://www.cs.ualberta.ca/~games/poker/man-machine/> Hämtad 2007-10-23

Walker, John (2006). *How HotBits Works* [www] <http://www.fourmilab.ch/hotbits/how3.html> Hämtad 2007-10-23

Bilaga 1: Studenters uppfattning

Vi gjorde en undersökning där vi riktade oss till studenter vid Linköpings universitet. Vi delade ut enkäter till 100 personer. I enkäten fick de svara på vad de anser i olika säkerhetsfrågor rörande internetpoker.

Enkätens utformning

Säkerheten kring poker på nätet

☐ Man ☐ Kvinna
Ålder :_____
Utbildning (program):_____

1) Spelar du poker på nätet?
☐ Ja ☐ Nej ☐ Har spelat

Om du svarade ”Ja” på fråga 1:
2)Hur många timmar spelar du per vecka?
☐ 1-3 ☐ 3-7 ☐ Mer

Om du svarade ”Har spelat” på fråga 1:
3)Varför slutade du spela?
_____

4)Hur säkert tror du...	Inte säkert alls.				Helt säkert.
...pengar överförs till pokersidorna?	1	2	3	4	5
...dina personuppgifter skyddas av pokerföretagen?	1	2	3	4	5
...det är att spela?	1	2	3	4	5

5)Hur ofta tror du...	Aldrig				Ofta
...brottslig aktivitet förekommer (t.ex. pengatvätt)?	1	2	3	4	5
...s.k. botar (en dator som spelar, inte en människa) förekommer?	1	2	3	4	5
...fusk eller oschysst spel i allmänhet förekommer?	1	2	3	4	5

6)Vad anser du om säkerheten på pokersidor i stort?
_____

Tack för din medverkan!

Resultat

Nedan finns en resultattabell med de relevanta svaren. Svaren på vissa frågor har vi valt att inte ta med eftersom vi nu i efterhand insett att de inte hade så mycket att göra med vår frågeställning.

	Totalt																	100 st
Fråga	Spelar					6 st	Har spelat					29 st	Har inte spelat					65 st
	1	2	3	4	5	Medel	1	2	3	4	5	Medel	1	2	3	4	5	Medel
4a	0	1	2	2	1	3,5	1	2	10	14	2	3,5	2	12	24	25	2	3,2
4b	0	1	4	0	1	3,2	2	6	10	9	2	3,1	4	25	22	13	1	2,7
4c	0	0	2	2	2	4,0	0	4	7	18	0	3,5	3	13	25	20	4	3,1
5a	0	0	1	2	3	4,3	1	10	11	5	2	2,9	2	18	22	15	8	3,1
5b	0	2	1	3	0	3,2	0	6	9	11	3	3,4	1	11	13	29	11	3,6
5c	0	1	0	4	1	3,8	0	6	11	10	2	3,3	0	6	18	32	9	3,7
	Män																	68 st
Fråga	Spelar					5 st	Har spelat					26 st	Har inte spelat					37 st
	1	2	3	4	5	Medel	1	2	3	4	5	Medel	1	2	3	4	5	Medel
4a	0	0	2	2	1	3,8	0	1	9	14	2	3,7	2	5	11	19	0	3,3
4b	0	1	3	0	1	3,2	2	6	8	9	1	3,0	1	12	14	10	0	2,9
4c	0	0	1	2	2	4,2	0	3	5	18	0	3,6	1	7	13	13	3	3,3
5a	0	0	1	1	3	4,4	1	9	11	3	2	2,8	2	14	10	8	3	2,9
5b	0	2	0	3	0	3,2	0	6	7	10	3	3,4	1	7	11	15	3	3,3
5c	0	0	0	4	1	4,2	0	6	10	8	2	3,2	0	6	9	19	3	3,5
	Kvinnor																	32 st
Fråga	Spelar					1 st	Har spelat					3 st	Har inte spelat					28 st
	1	2	3	4	5	Medel	1	2	3	4	5	Medel	1	2	3	4	5	Medel
4a	0	1	0	0	0	2,0	1	1	1	0	0	2,0	0	7	13	6	2	3,1
4b	0	0	1	0	0	3,0	0	0	2	0	1	3,7	3	13	8	3	1	2,5
4c	0	0	1	0	0	3,0	0	1	2	0	0	2,7	2	6	12	7	1	3,0
5a	0	0	0	1	0	4,0	0	1	0	2	0	3,3	0	4	12	7	5	3,5
5b	0	0	1	0	0	3,0	0	0	2	1	0	3,3	0	4	2	14	8	3,9
5c	0	1	0	0	0	2,0	0	0	1	2	0	3,7	0	0	9	13	6	3,9

Vi har gjort en sammanställning av resultaten och lagt in frågorna under två olika rubriker. Delfrågorna till 4 lade vi under ”Säkerhet” och delfrågorna till 5 under ”Fusk och brottslighet”.

	Medelvärden					
	Spelar	Har spelat	Ej spelat	Män	Kvinnor	Totalt
Säkert	3,6	3,4	3,0	3,3	2,8	3,2
Fusk och brottslighet	3,8	3,2	3,5	3,3	3,7	3,4

Bilaga 2: Mail

Det mail vi skickade till pokersidorna:

Hej!

Vi är en grupp från Linköpings Universitet som gör ett projekt om säkerheten kring poker på internet. T.ex. gällande användarnas integritet. Vårt fokus ligger på den teknik som används.

Vi skulle uppskatta om ni kunde svara på dessa frågor, svara gärna med specefik teknisk information.

- Hur skyddar ni er server från intrång? T.ex. brandväggar och andra skydd på databaser.
- Vad gör ni för att upptäcka så kallade botar?
- Vad använder ni er av för teknik för att skapa slumptal och blandade lekar? Genererar ni sanna slumptal (true random numbers) eller oäkta slumptal (pseudo-random numbers)?
- Hur ofta gör ni kontroller av användarnas äkta identitet och hur gör ni det?

Vi tackar på förhand för era svar.

MVH Johan Uppman
Student LitH, LiU