Teoretiska och praktiska attacker mot magnetkort och smarta kort

Rapport i kursen TDDC03, 2003

Erik Hallbäck eriha009@student.liu.se Magnus Mischel magmi821@student.liu.se

Sammanfattning— **Denna rapport diskuterar uppbyggnad och säkerhet kring magnetkort och smarta kort. Den fysiska uppbyggnaden av magnetkort är standardiserad. Magnetremsan består av tre spår som kan lagra olika mängd information. Spårens användning och kodningen av data är standardiserade. I de flesta kort ligger informationen helt öppet, vilket medför att känslig information inte bör lagras på korten. Kopiering av magnetremsan är möjlig med enkla medel och kan göras på några få sekunder. Vi har tittat på några olika vanligt förekommande kort med hjälp av en kortläsare som klarar av att läsa spår två på magnetremsan. Smarta kort är till utseendet lika magnetkorten men är istället för magnetremsa utrustade med en mikroprocessor. Kortet är programmerbart och kan användas för alla möjliga ändamål där man vill kunna beräkna och lagra data direkt på kortet. Vad gäller smarta kort så har vi i första hand studerat förhållandevis enkla tekniker för att knäcka, emulera och klona kort.**

1. Inledning

I dagens informationssamhälle förlitar vi oss alltmer på de kort vi har i plånboken för identifikation och betalningar. Detta gör oss också sårbara om vi inte vet vilka begränsningar de små plastbitarna har. Hur stor insats krävs egentligen för att knäcka de säkerhetsmekanismer som vi alla förlitar oss på?

2. Syfte

Vi kommer att ta reda på hur magnetkort och smarta kort fungerar och vilka möjliga attacker som är tänkbara och som praktiskt har utförts. Vi ska även undersöka magnetkort och den kodning som används för dem, för att själva undersöka hur sårbara de är.

3. Metod

Vår metod är att studera tidigare studier och avhandlingar inom området samt att använda en magnetkortsläsare för att få ut information lagrad på vanligt förekommande kort. Då läsaren vi har tillgång till enbart klarar av att läsa av spår två på korten så är vi något begränsade i vilka kort vi kan undersöka.

4. Magnetkort

A. Uppbyggnad

Ett magnetkort består av ett vanligt plastkort i storleken 85,6 mm gånger 54 mm. Den information som lagras på kortet sparas på en magnetremsa. Remsan består av ett ferromagnetiskt material med små laddade partiklar. Det ferromagnetiska materialet klarar av att behålla en magnetisering, även sedan det yttre magnetfält som använts för att åstadkomma denna har avlägsnats. De magnetiska partiklar som finns i magnetremsan är ungefär 5 nm långa. Under tillverkningsprocessen får magnetremsan stelna under inflytande av ett magnetfält. Detta gör att partiklarna ligger uppradade i samma riktning som magnetremsans längd.

Genom att lägga på ett yttre magnetfält kan man få partiklarna att byta polarisation, d v s nordpolen byter plats med sydpolen på magnetpartikeln, och tvärtom. Den styrka på det yttre magnetfält som behövs för att åstadkomma detta mäts genom partiklarnas koercivitet. Magnetkort tillverkas i både låg- och högkoercivitetsversioner. Magnetkort som har remsor med låg koercivitet löper högre risk att oavsiktligt raderas om de t ex läggs på en högtalare eller på något annat sätt utsätts för ett externt magnetfält. Högkoercivitetskort är svårare att radera, men kräver därför speciell utrusning för skrivning. De flesta bankkort och andra typer av kort som används idag är av lågkoercivitetstypen. Bankkort brukar dock bytas ut efter några år, så det spelar antagligen ingen roll i det fallet. Koercivitet mäts i enheten ørsted (Oe), efter den danska fysikern Hans Ørsted. Magnetkortsremsor brukar ha en koercivitet som ligger mellan 300 och 4000 Oe. Ett kort på 300 Oe har således låg koercivitet, medan ett på 4000 har hög koercivitet.

B. Kodning

Magnetkort kodas nästan alltid på ett av två sätt - antingen med en kodningsmetod som heter F2F, eller en annan som heter MFM. Alla standardiserade kort, såsom t ex bankkort, använder F2F-kodning, medan MFM-kodning används för kort som inte är standardiserade [1].

Vid F2F-kodning finns klockningsbitar kodade regelbundet. En etta kodas som en magnetfältsväxling mellan två klockbitar. En nolla kodas genom att ingen växling inträffar mellan två klockbitar. Ett spår inleds alltid med klockningsbitar som ger kortläsaren möjlighet att synkronisera sig själv mot dataströmmen. Kodad data inleds sedan med ett s k Start Sentinel-tecken. End Sentinel-tecknet signalerar på samma sätt slutet på dataströmmen. Allra sist ligger en kontrollsumma kallad LRC (Longitudinal Redundancy Character) samt ytterligare klockningsbitar för att möjliggöra att kortet kan dras åt båda hållen genom läsaren.

C. Standarder

Uppbyggnaden av magnetkort beskrivs i ISO-standarderna 7810, 7811 och 7813. Magnetremsan delas upp i tre stycken

s k tracks, eller spår. Varje spår är 3 millimeter brett.

Informationstätheten på spåren mäts i Bits Per Inch (BPI). Spår ett och tre har densiteten 210 BPI, d v s ca 83 bitar per cm. Spår två har densiteten 75 BPI, motsvarande ca 30 bitar per cm. ISO 7810 beskriver de fysiska egenskaperna hos korten såsom material, tjocklek och krav på värmeresistans. ISO 7811 beskriver hur prägling av bokstäver ska göras, samt de tre magnetspåren och koerciviteten hos magnetremsan. Den sista standarden, ISO 7813, berör kort som används för finansiella transaktioner, såsom t ex kreditkort.

1) Spår 1: Det första spåret på magnetremsan kodas enligt en standard som konstruerades av IATA (International Air Transport Association). Varje tecken på det här spåret kodas med den minst signifikanta biten först (längst till höger), och består av sex bitar plus en paritetsbit för varje tecken. Pariteten är udda, så varje tecken ska ha ett udda antal ettor om det inte har blivit ett fel vid avläsningen [2]. Totalt kan 79 tecken sparas på spår ett.

2) Spår 2: Spår två på magnetremsan kodas i ett format som specificerats av American Bankers Association. Tecknen på detta spår kodas enligt standarden ANSI/ISO-BCD (Binary Coded Decimal). Varje tecken kodas med fyra bitar plus en udda paritetsbit - totalt kan alltså 16 tecken kodas. De första nio binärkoderna används för att representera siffrorna noll till nio, medan de övriga sex kodorden används som kontrolltecken. Kodningen på det här spåret går till enligt tabellen nedan. Totalt kan 40 tecken sparas på spåret.

Kodning					Värde	Funktion
0	0	0	0	1	0 (0H)	Data
1	0	0	0	0	1 (1H)	”
0	1	0	0	0	2 (2H)	”
1	1	0	0	1	3 (3H)	”
0	0	1	0	0	4 (4H)	”
1	0	1	0	1	5 (5H)	”
0	1	1	0	1	6 (6H)	”
1	1	1	0	0	7 (7H)	”
0	0	0	1	0	8 (8H)	”
1	0	0	1	1	9 (9H)	”
0	1	0	1	1	: (AH)	Kontrolltecken
1	1	0	1	0	; (BH)	Start Sentinel
0	0	1	1	1	$<$ (CH)	Kontrolltecken
1	0	1	1	0	$=$ (DH)	Fältmarkör
0	1	1	1	0	$>$ (EH)	Kontrolltecken
1	1	1	1	1	? (FH)	End Sentinel

3) Spår 3: Spår tre kallas THRIFT, och kodas med samma BCD-kodning som spår två. Spåret har dock en högre bitdensitet (210 BPI), vilket gör att man får plats med 107 tecken på det. Det som är speciellt med det här spåret är att det enligt ISO-standarden är det enda spår som kan återskrivas efter att kortet har programmerats för första gången.

D. Säkerhet

Den information som sparas på kortet kan läsas av alla som har en magnetkortsläsare. För praktiska syften måste man alltså räkna med att vem som helst kan läsa av informationen.

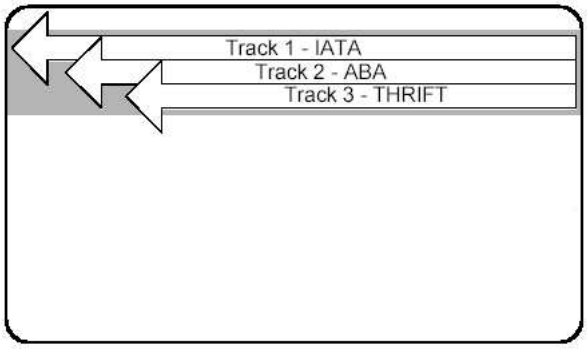

Fig. 1. Spårens placering på kortet.

Om känslig information ska sparas på ett kort måste den ovillkorligen krypteras, och då på ett sådant sätt att användarna av kortet inte har tillgång till nyckeln. I fall där man bara behöver verifiera information, t ex PIN-koder (Personal Identification Number), sparar man med fördel informationen på kortet efter att den har genomgått en hemlig envägsfunktion. Detta gör att man kan verifiera t ex en PIN-kod utan risk för att någon som läser informationen på magnetremsan kan återskapa PIN-koden.

E. Teoretiska attacker

1) Kopiering: Magnetremsan på ett magnetkort går på ett enkelt sätt att kopiera med billig utrustning. Att på detta sätt göra en kopia av ett kort kräver bara tillgång till det under de få sekunder det tar att dra det genom en kortläsare. Att förlita sig enbart på kortet för t ex identifiering eller passerkontroll är därför en mycket dålig idé. Som minsta säkerhetsåtgärd bör magnetkort kompletteras med en personlig kod el dyl.

2) Tryckta kortnummer: Om ett kortnummer finns tryckt på magnetkortet, och detta även är vad som används för identifikation eller passerkontroll så kan man på ett mycket enkelt sätt kopiera kortet genom att notera det tryckta numret och sedan använda en kortskrivare för att koda motsvarande information på rätt spår. För att undvika detta bör man inte trycka kortnumret på kortet, alternativt bara trycka en del av det.

3) Denial of Service: Eftersom magnetkorten kan raderas genom påverkan av ett yttre magnetfält kan man göra kort obrukbara genom att introducera ett starkt magnetfält i närheten av dem. Visserligen har författarna aldrig hört talas om att något liknande skett, men det är ändå värt att nämna eftersom det går att göra på ett omärkbart sätt och dessutom på avstånd, i viss mån. Ett vanligt exempel på situationer där avmagnetisering kan ske är vid kassor där avlarmningsutrustning med starka magnetfält används.

F. Praktiska undersökningar och attacker

1) Bankkort: Spår ett på ett bankkort/kreditkort används för att spara kontoinnehavarens namn, landskod, kortets giltighetstid, samt något som kallas “discretionary information” (övrig information) [3], vilket innebär att kortutfärdaren kan spara den information han finner lämplig här.

Spår två, som ju har specificerats av American Bankers Association, innehåller samma information på alla bankkort världen över. På spåret sparas kontonummer, och PIN-koden efter att den har gått igenom en envägsfunktion, samt andra data efter utfärdande banks godtycke.

Det återskrivningsbara spår tre används inte alls på amerikanska bankkort.

På svenska bankkort finns ytterligere ett spår, "spår noll", som används för att öka kortens säkerhet. [4] Detta spår, som är kodat med en icke-standardiserad kodningsmetod, innehåller ett serienummer som skrivits dit av korttillverkaren. När kortet används i en bankomat läser denna av serienumret och försöker sedan radera spår noll. Om radering misslyckas indikerar detta att kortet ej är kopierat.

En attack som bevisligen har förekommit är den som kallas "skimming". Attacken utförs så att man med hjälp av en kortläsare tar en kopia av bankkortets magnetremsa. Informationen från magnetremsan kopieras över till ett blankt kort, och kan sedan användas för att olovligt ta ut pengar från någon annans konto med hjälp av en bankomat. Detta kräver naturligtvis att man även har tillgång till kortinnehavarens PIN-kod, men oseriösa servitörer på restauranger kan även sälja enbart kortkopian till element inom den organiserade brottsligheten som sedan använder informationen för att massproducera plagierade bankkort [5]. Bara i Storbritannien uppgick förlusten p g a skimming till 2 miljarder kronor år 2002 [6]. Det är mycket svårt att förebygga den här sortens attack eftersom en liten kortläsare som döljs bakom disken är allt som krävs för att utföra den. Kunden märker oftast inget förrän i slutet av månaden när han får kontobeskedet från banken, och de brottslingar som använder de förfalskade korten slänger dem oftast efter ett par dagar, efter att ha köpt varor för stora summor med dem. I Sverige krävs alltid antingen legitimation eller PIN-kod när man handlar med ett kort, men i andra länder där man bara behöver kortet för att handla är problemet mer utbrett. Visserligen verifieras namnteckningen på kortet i sådana länder, men man kan anta att den extra säkerheten inte är speciellt stor p g a bristande nit hos kassapersonal.

2) Kopieringskort: Vi har inte lyckats läsa av något kopieringskort. Antagligen lagras tillgodobeloppet på spår tre för att det ska kunna ändras genom återskrivning.

3) Busskort: Vi hade som mål att undersöka de busskort som Östgötatrafiken använder för kollektivtrafiken i Östergötland. Den läsare vi har fått låna klarar bara av att läsa spår två, och vi har inte lyckats få ut någon information från det spåret när vi provat några olika busskort. Vi sluter oss alltså till att en del av busskortets data lagras på spår tre, vilket verkar logiskt eftersom det är det enda spår som är återskrivningsbart. Vi gissar att det belopp med vilket busskorten har laddats ligger lagrat på spår tre, och såvida det inte är krypterat skulle man på ett enkelt sätt kunna tillverka egna busskort. Försvaret mot detta skulle kunna vara att kryptera informationen på kortet, vilket dock inte är en optimal lösning. Om kryptonyckeln läcker ut kan vem som helst sedan tillverka egna busskort (algoritmen förutsätts känd). Bättre är i så fall kryptering i kombination med en central dator som kontrollerar att det inte finns två kort med samma serienummer i omlopp. Om denna situation skulle uppträda kan sådana kort då spärras ur systemet.

5. Smarta kort

A. Uppbyggnad

Smarta kort är till storlek och utseende lika vanliga magnetkort men har en speciell egenskap; en egen processor med tillhörande minne och serieport.

Det finns även passiva kort som saknar processorkraft. De har bara ett minne och någon sorts logik för att adressera minnet samt säkerhetslogik för att kontrollera läsning och skrivning till kortet. Förbetalda telefonkort är typiskt av den här modellen.

För att ett smart kort ska vara användbart i sammanhang där asymmetriska kryptografiska algoritmer (exempelvis RSA) används utrustar man även kortet med en hjälpprocessor avsedd att räkna med stora heltal och exponenter.

B. Standarder

Standarden för smarta kort är ISO7816 som bygger på ISO7810 ID-1 (det vanliga kreditkortsformatet). Standarden innehåller tre dokument.

- ISO7816-1 Kortets fysiska egenskaper
- ISO7816-2 Kortets dimensioner och placering av kontakter
- ISO7816-3 Elektriska signaler och protokoll

Man har noga definierat hur ultraviolett ljus, röntgen, magnetfält m m får påverka kortet och vilka doser det ska klara. Processorn kan klockas med extern klocka och är specificerad för att köras i mellan 1 och 5 MHz [8].

C. Kryptografiska egenskaper

Den stora fördelen med smarta kort jämfört med exempelvis magnetkort är att processorn kan innehålla din privata nyckel som du kan signera och dekryptera med utan att några hemligheter behöver lämna kortet. Nyckeln är skyddad med PIN-kod för att enbart innehav av kort inte ska räcka för att använda någons privata nyckel. I dessa sammanhang använder man kort med ovan beskrivna hjälpprocessor. Korten klarar av 512, 768 eller 1024 bitars nyckelstorlekar. Ett smart kort med hjälpprocessor har kapacitet att utföra en signering med en 1024-bitars nyckel på under en sekund.

D. Säkerhet

För att skydda kortet mot angrepp så har det inbyggda försvarsmekanismer i hårdvara.

- För att förhindra kloning så finns ofta ett unikt serienummer inbränt i minnet.
- Korten är designade att nollställa sig till starttillståndet vid ändringar i matningsspänning, temperatur eller klockfrekvens.
- En säkring som bränns av hindrar att kod kan läggas in i kortets EEPROM.

Skyddsmekanismerna måste balansera på den tunna skiljelinjen mellan säkerhet och användbarhet. Gör man kortet för känsligt för fluktuationer i klockfrekvensen så är det inte säkert att man kan få det att fungera i alla kortläsare.

E. Attacker

1) Chip-invaderande attacker: Attacker mot smarta kort finns i flera varianter. Man kan ge sig på själva chippet och försöka frilägga det med hjälp av salpetersyra och studera det under kraftig förstoring.

Attacker har sedan gått ut på att modellera de olika lagren i chippet genom att använda tekniker från CMOS VLSI-design och mikrokontrollarkitetkurer. Med modellerna kan man sedan rekonstruera och identifiera de olika delarna på chippet för att lättare kunna disassemblera den extraherade maskinkoden.

Korttillverkarna har inte lagt ner särskilt mycket möda för att förhindra dessa attacker som trots allt kräver en ganska stor insats och dyr utrustning. Man har gjort försök till att göra bussledningarna på chippet något ostandardiserade för att förhindra att standardmallar appliceras. Varje försök till att använda icke-standardiserade ASIC[1] höjer layout-komplexiteten och bara tillverkare av de dyrare kryptokorten har ansett att detta är värt besväret [9].

Det har också gjorts lyckade försök med att sätta mikro-prober på bussledningar och läsa av data som kommer [8].

Ross Andersson och Sergei Skorobogatov från Cambridge University beskriver i ett dokument hur de med en fotoblixt och en laserpekare lyckades ändra på individuella bitar i en mikroprocessor i ett smart kort [10]. Skyddet mot den här typen av attacker som de presenterade i samma dokument var att lägga till en extra ledningsbana och koda informationen som hög-låg och låg-hög på de olika banorna. Processorn detekterar om någon är inne och försöker mixtra med signalerna och nollställer processorn om hög-hög eller låg-låg skulle uppträda på ledningsbanorna.

2) Icke chip-invaderande attacker: Genom att ändra på klocksignalen under korta tidsintervall och på precis rätt ställe så kan man få programflödet att "hoppa över" kod så att processorn skickar ut data som inte var tänkt att lämna kortet på sin serieport.

Ett annat tillvägagångssätt för att attackera ett kort är att undersöka hur mycket ström det drar när det genomför vissa operationer och få information om vad processorn håller på med [11] [12]. Denna information kan exempelvis minska sökrymden betydligt om man bestämt sig för genomföra en uttömmande sökning.

3) Falsk läsare: Varje gång du stoppar in ditt smarta kort i en läsare som någon annan har kontroll över så måste du lita på den läsaren. Möjligheten finns att någon har fifflat och gjort så att något annat sker i bakgrunden trots att det ser ut som om allt går rätt till. Detta är en möjlig attack mot exempelvis Cash-kort, där automaten säger att den drar ett visst belopp men i verkligheten kan dra ett annat belopp.

4) Tejpattacken: Tidiga varianter av smarta kort hade en kontakt för att ge ström till att driva processorn och en kontakt för programmeringsströmmen. Programmeringen kräver en högre spänning vilket var orsaken till att man löste det så. Detta ändrades dock snabbt efter upptäckten att man kunde klistra en bit tejp över kontakten för programmeringsspänningen. Tejpbiten hindrade kortläsaren från att skriva till kortet. Denna enkla attack genomfördes på betal-TV-kort som kom laddade med alla kanaler och programmerades av mottagarenheten till att inte ta in de kanaler man inte hade betalat för. Även telefonkort gick det att sätta en bit tejp på för att inga markeringar skulle tas från kortet då man ringde. Korten ändrades till att bara ta in spänning på en kontakt och internt på chippet byggde man upp ett switchat nät av kapacitanser och dioder som höjde spänningen för att klara bränningen.

5) Emulering av smarta kort: Det här är ingen attack mot själva kortet utan ett sätt att lura en kortläsare till att tro att det är ett riktigt smart kort den läser från. Detta har varit det absolut vanligaste sättet att få tillgång till betalkanaler via parabol och kabelnätet utan att betala.

Det finns huvudsakligen två sätt att emulera ett smart kort på; med ett kort med passiv elektronik kopplad till serieporten på en PC eller ett kort med en mikroprocessor och ibland extra EEPROM tillkopplat.

Gränssnittet för att koppla ett ISO7816-kort till datorn heter "season" [7]. Datorn kör ett program som kommunicerar med avkodarboxen via detta gränssnitt. I programmet skriver man in nycklar för de olika kanalerna.

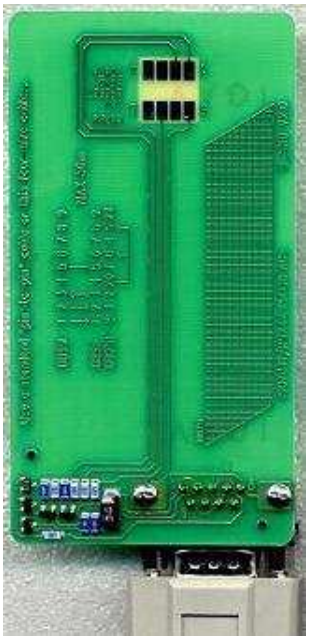

Fig. 2. Exempel på smart kort som kopplas till dator.

De som inte vill ha en dator på för att avkoda kanalerna kan skaffa sig ett kort med inbyggd mikroprocessor. Vanligast är att det sitter en av Microchips 16F84, ibland med ett extra EEPROM för att lagra fler nycklar än vad som ryms i processorns interna minne.

Det senaste är att man skaffar ett så kallat *wafer*-kort som är ett programmerbart smart kort. Processorn är av samma modell som innan men mycket mindre och får plats i kortläsaren.

Betal-TV-bolagen har numera uppmärksammat problemet och byter koderna mycket oftare än tidigare för att "trötta" ut de som inte betalar för sig.

[1] Application Specific Integrated Circuit, standard-byggblock för att bygga integrerade kretsar

Fig. 3. Programmerbart waferkort med processorn PIC16F84 och 24LC16 EEPROM.

En lösning på detta problemet har varit att skaffa kort med en så kallad *management*-nyckel. Dessa kort har alltid varit förprogrammerade med kod och nycklar för att inte information om vilken nyckel man knäckt ska läcka till betal-TV-bolagen så att de kan sluta använda den. Dessa kort kan fånga upp nya nycklar som skickas ut, dekryptera dem med managementnyckeln och använda dem utan att användaren behöver göra några manuella handgrepp.

När bolagen väl upptäcker vilken nyckel som har blivit knäckt så byter de till en annan. Varje kort innehåller bara en delmängd av de nycklar som finns för att inte en angripare ska kunna få tag på all information genom att bara ha tillgång till ett kort. Man ordnar nycklarna i en matris där varje kort bara får en väl vald delmängd av alla nycklar. Varje nyckel som crackarna får tag i svartlistas och bara de kort som enbart har nycklar som man vet har läckt ut byts ut, vilket är mycket färre kort än vad det skulle ha varit om man inte löst det på det här sättet [13].

Erfarenheter från betal-TV-pirater visar att alla försök att gömma hemligheter på chip som lämnar företagens kontroll kommer att reverse-engineeras inom några veckor om piraterna ser möjligheter att tjäna stora summor pengar på det.

6) GSM-kloning: Genom att utnyttja en svaghet i autentiseringsalgoritmen som används i SIM-kort för mobiltelefoner så kan man med enkla medel klona ett SIM-kort och ringa samtal som debiteras ägaren av originalkortet.

Varje smart kort som sitter i en GSM-telefon idag är unikt, det innehåller en nyckel som är kopplat till ett abonnemang hos en teleoperatör. Tillsammans med den nyckeln finns en autentiseringsalgoritm, COMP128. För att en telefon ska kunna koppla upp sig mot en basstation så skickas en utmaning från basstationen där svaret från telefonen bara kan vara korrekt om den har tillgång till rätt nyckel. Algoritmen utvecklades utan publik granskning vilket kan ha varit en bidragande orsak till att man inte upptäckte en svaghet i diffusionen. Genom att ställa 150.000 frågor till kortet och analysera svaren så kan man med lite datorkraft få ut hela nyckeln. Attacken tar runt 8 timmar med en helt vanlig kortäsare som klarar av att ställa 6.25 frågor i sekunden. Attacken fungerar bara om man har fysisk tillgång till det SIM-kort som ska klonas så det ska betonas att systemet inte är helt vidöppet. GSM-industrin har numera försökt att komma till rätta med problemen genom att släppa COMP128-2, men att byta ut något som finns hos 100 miljoner kunder kommer att ta sin tid. I nästa generations mobiltelefonsystem har man lärt sig av läxan att "security by obscurity" inte fungerar och låtit den nya algoritmen 3GPP granskas av forskare [14]. Erfarenheter från utvecklandet av bl a kryptoalgoritmer visar att öppen granskning leder till att många svagheter kan upptäckas redan på ett tidigt stadium och pinsamma misstag kan undvikas i större utsträckning.

För att utföra attacken behövs förutom kortläsare och programvara (som finns att ladda ner från Internet) ett season-gränssnitt som används för att koda av betal-TV-kanaler – total kostnad ett par hundra kronor.

6. Resultat och diskussion

Av vårt arbete har vi kommit fram till att enbart magnetkort för identifiering, passerkontroll och dylikt inte är tillräckligt. System som har terminaler som står i förbindelse med en central dator ger i de flesta kommersiella tillämpningar tillräcklig säkerhet i kombination med t ex en personlig kod. System som bygger på den felaktiga uppfattningen att det skulle vara svårt att läsa av magnetremsan och skriva tillbaka informationen till den är osäkra.

Smarta kort har försökt att lösa problemet med att informationen ligger öppen. Processorn hindrar i viss utsträckning försök att läsa skyddad information. Detta möjliggör att korten även kan användas för signering och dekryptering utan att kortets privata nyckel lämnar kortet.

7. Slutsatser

Alla försök till säkra kort kommer att attackeras och så småningom att knäckas. System som utvecklas bakom stängda dörrar tenderar att ha fler brister och säkerhetsluckor än system där publik granskning ingår i utvecklingsprocessen.

Precis som det är svårt för gemene man att förfalska sedlar på grund av de stora resurser som krävs, är smarta kort och svenska bankkort svåra att kopiera. Detta gör det troligt att dessa system inte kommer att attackeras genom att stora resurser satsas på att tilverka kopieringsmaskiner o dyl. Istället är en attack mot kortens användningsområde troligare genom emulering av korten (för smarta kort) eller stöld av kortnummer och inköp över nätet (för bankkort). Vår slutsats är att man företrädesvis måste skydda mot attacker där dessa är troligast genom att de kräver minst resurser.

En kedja är inte starkare än sin svagaste länk.

Referenser

[1] Best Practice Recommendations for the Use of Magnetic Stripes `http://www.aamva.com/documents/stdbestpracticesmagstripe2dot0.pdf?ct=all&qu=magnetic\%20&action=search`

[2] Anadigm App Note 006 - Applying the AN10E40 Magnetic stripe read head amplifier `http://www.anadigm.com/_doc/appnote006.pdf`

[3] Credit Check - Everything You Always Wanted to Know About Credit Cards `http://abcnews.go.com/sections/scitech/Geek/geek010118.html`

[4] Samtal med Viiveke Fåk, 2003-05-12

[5] Card fraudsters prey on high class diners http://money.guardian.co.uk/creditanddebt/creditcards/story/0,1456,830350,00.html
[6] Skimming Crackdown http://www.cardwatch.org.uk/html/skimming_what.html
[7] Beginner Guide to making TV Pirate Cards http://hem.passagen.se/sat/tutorial.htm
[8] Tamper Resistance - a Cautionary Note - Anderson, Kuhn (1996) http://www.cs.rice.edu/~dwallach/courses/comp527_s2000/tamper96.pdf
[9] Design Principles for Tamper-Resistant Smartcard Processors, Kuhn, Kömmerling (1999) http://www.cl.cam.ac.uk/~mgk25/sc99-tamper.pdf
[10] Optical Fault Induction Attacks http://www.cl.cam.ac.uk/~sps32/ches02-optofault.pdf
[11] Differential Power Analysis http://www.cryptography.com/resources/whitepapers/DPA.pdf
[12] Investigations of Power Analysis Attacks on Smartcards Thomas S. Messerges and Ezzy A. Dabbish, Motorola Labs; Robert H. Sloan, University of Illinois at Chicago http://www.usenix.org/events/smartcard99/full_papers/messerges/messerges.pdf
[13] Attacks on Pay-TV Access Control Systems, Kuhn (1997) http://www.cl.cam.ac.uk/~mgk25/vc-slides.pdf
[14] GSM Cloning, Marc Briceno, Ian Goldberg (1998) http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html

Alla webbreferenser fanns tillgängliga 2003-05-12