UPPSALA
UNIVERSITET

UPTEC IT 12 008
Examensarbete 30 hp
Augusti 2012

Analys av säkerheten av RFID i inpasseringssystem

Tiina Loukusa

UPPSALA
UNIVERSITET

Teknisk- naturvetenskaplig fakultet
UTH-enheten

Besöksadress:
Ångströmlaboratoriet
Lägerhyddsvägen 1
Hus 4, Plan 0

Postadress:
Box 536
751 21 Uppsala

Telefon:
018 – 471 30 03

Telefax:
018 – 471 30 00

Hemsida:
http://www.teknat.uu.se/student

Abstract

Analys av säkerheten av RFID i inpasseringssystem

Analysis of the security of RFID in entrance systems

Tiina Loukusa

Radio Frequency Identification, RFID, is a convenient way to enable contactless identification which does not require any physical nor optical contact. As with any radio-based communication the signal can be intercepted, thus making the technology vulnerable to several kinds of attacks. Interception of communication is not the only threat. Since RFID tags might contain personal information or information that will grant the owner access to secure areas, skimming and spoofing attacks are also major threats against this technology. In this thesis report, the perspective of an adversary is portrayed in an RFID-enabled environment by presenting where RFID is used and how it could be abused. We also perform cloning attacks against two common types of RFID tags, EM4100 and Mifare Classic, and assess the threat against security that this could present. The likelihood of executing this attack is based on the required competence, equipment needed and its cost and under what conditions the attack actually can be performed in a real life situation. These results are presented and discussed in this report.

Handledare: Mikael Simovits
Ämnesgranskare: Björn Victor
Examinator: Arnold Pears
ISSN: 1401-5749, UPTEC IT 12 008
Tryckt av: Reprocentralen ITC

Sammanfattning

Radiofrekvensidentifiering (RFID) är en teknik för att göra det möjligt att utföra kontaktlös identifiering mellan en identifieringsenhet (RFID-etikett) och en läsare (RFID-läsare). För att kunna utvärdera säkerheten hos ett system som använder RFID måste kunskap finnas om hur ett sådant system kan angripas för att kunna göra en riskanalys, vilket är kärnan i detta examensarbete. RFID-etiketter används för kontaktlös identifiering och de finns i ett flertal former och de kan variera stort i komplexitet. De enklaste typerna av RFID-etiketter har bara ett ID som tas emot av en läsare. Det finns också betydligt mer avancerade RFID-etiketter, så kallade smart cards, som kan ha olika säkerhetsmekanismer och ett minne som kan modifieras. Fördelarna med RFID-lösningar är att de inte behöver vara synliga vid avläsning, dessutom kan signalerna penetrera olika material. För att kartlägga möjliga angrepp mot ett system som använder RFID är det bra att tänka sig in i en angripares roll. Många angrepp mot RFID kan jämföras med andra angrepp mot radio-baserade kommunikationsmedel, så som avlyssning av kommunikation. I vissa fall vill angriparen att ett system ska sluta fungera för att kunna utnyttja situationen som följer detta, exempelvis om det leder till att säkerheten i en fastighet sjunker. I andra fall kan angriparen vara intresserad av innehållet på RFID-etikett för att kunna spåra någon eller utvinna information. Med kunskap om innehållet på en etikett kan det också vara möjligt att skapa en klon.

För kontor och byggnader där många människor passerar används ofta just RFID i inpasseringslösningar. RFID-etiketter är enkla att distribuera och använda, det behövs ingen dörrvakt eller nycklar, utan verifiering av identiteter görs automatiskt. RFID i inpasseringslösningar har undersökts närmare i detta examensarbete och försök att klona två olika typer av etiketter har utförts. Att klona en RFID-etikett innebär att all data från en etikett skrivs till en annan etikett, som blir en klon som kan användas på samma sätt som originalet. För att verifiera de eventuella riskerna som användningen av RFID-etiketter i inpasseringslösningar kan medföra, klonades två RFID-etiketter som fungerar på olika sätt. Den ena, EM4100, har inte några säkerhetsmekanismer och består bara av ett ID och den andra, Mifare Classic, är ett smart card som kommunicerar krypterat och har ett modifierbart minne. För att skapa en klonad etikett behövs en dator och en läsare som kan utföra kloningen. I detta fall användes ett RFID-verktyg som kan läsa, skriva och emulera RFID-etiketter. Kloningsförsöken visade att genom att ha full tillgång till en RFID-etikett är det enkelt att klona båda EM4100 och Mifare Classic. Men att utvinna den information som behövs för en klon från en etikett som någon bär med sig, kan vara betydligt svårare. För att utföra ett kloningsangrepp i praktiken finns det ett flertal störningsmoment. Angriparen måste komma väldigt nära etiketten utan att dra till sig uppmärksamhet och andra signaler kan störa angreppet. För EM4100 som inte har några säkerhetsmekanismer kan angreppet göras väldigt snabbt eftersom en vanlig läsare kan användas, dessutom behövs bara ett svep över kortet för att läsa av ett ID. För att klona en Mifare Classic-etikett måste dess krypteringsnycklar först knäckas, innan läsning av data kan ske. Knäckningen av nycklar kan i värsta fall ta över en timme, vilket gör att ett angrepp mot ett ovetande offer kan ses som osannolikt. När angriparen har samlat all data från ett kort kan det skrivas till ett annat för att skapa en klon. Båda försöken visade att RFID-system kan vara sårbara. Det är viktigt att både ta hänsyn till att använda RFID-etiketter med tillräckliga säkerhetsmekanismer sätt och utnyttja säkerhetsfunktionerna till fullo. Det är också viktigt att bygga det bakomliggande systemet på ett sådant sätt att det förhindrar användandet av klonade etiketter.

Ordlista

Aktiv etikett – en RFID-etikett som har ett eget batteri och skickar data periodvis, hela tiden

Card-only angrepp – ett angrepp som endast kräver tillgång till en etikett

Denial of Service-angrepp, DoS-angrepp – ett angrepp som förhindrar normal användning av ett system

EM Microelectronics – tillverkare av mikrochipp, bl.a. EM4100

EM4100 – Lågfrekvent RFID-etikett, med endast ID som data

EPC – Electronic Product Code, en standard för identifiering av varor

Etikett, RFID-etikett, Transponder – en RFID-enhet som skickar (ibland även tar emot) signaler till (från) en RFID-läsare

Kontaktlös smart card – En RFID-etikett med säkerhetsmekanismer och modifierbart minne

Läsare, RFID-läsare – en enhet som tar emot/skickar signaler från/till en RFID-etikett.

Mifare Classic – Högfrekvent RFID-krets, med kryptering och 1k eller 4k minne

NFC – Närfältskommunikation (eng. Near Field Communication) en delmängd av RFID-tekniken, med kortare räckvidd.

Nonce – Number used once, ett engångstal

NXP Semiconductors – Tillverkare av RFID-chipp, bland annat Mifare

Passiv etikett – en RFID-etikett som inte har en egen strömkälla, istället får den ström från en läsares elektromagnetiska fält

Proxmark3 – ett RFID-verktyg som kan läsa, skriva och emulera etiketter.

Relay-angrepp – ett angrepp som sänder vidare ett meddelande från en sändare till en mottagare

Replay-angrepp – ett angrepp som spelar upp en inspelad kommunikationssession

RFID – eng. Radio Frequency Identification, Radiofrekvensidentifiering

Semi-aktiv etikett – en RFID-etikett som har ett eget batteri, men skickar inte data förrän den är i en läsares elektromagnetiska fält

Skimningsangrepp – ett angrepp för att i hemlighet avläsa innehållet på ett kort

Spoofingangrepp – ett angrepp som går ut på att lura en enhet

Innehållsförteckning

1 Inledning

1.1 Bakgrund

Detta examensarbete har genomförts på uppdrag av Simovits Consulting och Sveriges Riksbank för att kvantifiera hot mot RFID-system och särskilt angrepp mot RFID-baserade inpasseringslösningar i form av kloning.

Med ökningen av antalet system som förlitar sig på RFID ökar även intresset för att upptäcka deras brister och säkerhetsluckor som kan utnyttjas av angripare. RFID har ett flertal användningsområden och inpassering är bara ett av dem. RFID-etiketter fungerar kontaktlöst och behöver inte synas för att kunna läsas av vilket medför att det kan göras automatiskt utan inblandning av mänsklig verifiering.

Genom att identifiera risker kan det vara möjligt för någon som vill införa ett RFID-system att resonera kring eventuella risker och täppa till säkerhetshål. Vilken säkerhetsnivå som krävs i ett system beror på dess användningsområde och kräver en individuell riskanalys. Detta examensarbete undersöker olika typer av säkerhetsbrister som kan finnas i RFID-system och hur en angripare skulle kunna tänkas utnyttja dem. Eftersom många inpasseringssystem använder RFID utförs en närmare undersökning på hur en angripare skulle kunna klona en etikett för att erhålla tillträde för ett skyddat område.

1.2 Syfte, problemformulering och metod

Syftet med detta arbete är att undersöka den verkliga risk som kan förekomma då RFID-baserade inpasseringssystem används. Resultaten gör det möjligt att dra vissa slutsatser om vilken säkerhetsnivå som behövs och om det krävs flera säkerhetsåtgärder för att ha ett säkert inpasseringssystem.

För att genomföra en kartläggning har arbetet delats upp i två delar: en teoretisk del och en praktisk del.

Den teoretiska delen baseras på en litteraturstudie och presenterar möjliga angrepp och användningsområden. Här presenteras svar på följande frågor:

1. Var används RFID?
2. Hur kan olika RFID-lösningar angripas?

I den praktiska delen utförs kloning av två olika typer av RFID-etiketter, EM4100 och Mifare Classic, som sedan kan användas för att lura en läsare att tro att det är en legitim etikett. EM4100 och Mifare Classic har valts för dessa kloningsförsök dels för att påvisa skillnaderna mellan två olika tekniker, men även för att de är två vanligt förekommande lösningar för inpasseringssystem. Dessa experiment genomförs för att kvantifiera riskerna, genom att faktiskt utföra dem utifrån en angripares tillvägagångssätt. Analysen av hotbilden baseras på kompetenskrav, vilken utrustning som krävs, kostnader och under vilka omständigheter angreppet kan utföras.

Det första experimentet utfördes på en EM4100-etikett som inte använder kryptering och har ett read-only-minne som endast består av ett ID.

Det andra experimentet utfördes mot en etikett som har ett läs- och skrivbart minne och dessutom använder kryptering, Mifare Classic. Denna etikett har valts för att det är ett populärt val för inpasseringssystem, till stor del för att det är en billig etikett för att vara en etikett som har krypterat data, trots att det är känt sedan några år tillbaka att krypteringen är möjlig att knäcka [1] [2]. För att utföra dessa experiment används ett RFID-verktyg som kallas Proxmark3 [3], som kan läsa, skriva och emulera flera olika typer av RFID-etiketter.

1.3 Avgränsningar

Den praktiska delen har i detta arbete varit begränsad till att endast genomföra kloningsexperiment på två typer av RFID-etiketter, EM4100 och Mifare Classic, genom att utföra ett card-only angrepp. Ett card-only-angrepp innebär att angreppet endast utförs mot RFID-etiketten och inte RFID-läsaren. Andra typer av etiketter som har en mer sofistikerad krypteringslösning använder krypteringsmetoder så som DES, 3DES och AES och kräver andra medel för att knäckas. Som exempel kan Mifare DESFire EV1 nämnas som använder 3DES kryptering av data [4].

I ett kloningsangrepp ingår ett flertal andra angrepp. Att använda en klonad etikett innebär att en läsare spoofas (avsnitt 2.4.3) vilket i korthet innebär att en läsare luras till att tro att etiketten är genuin. För att få ut informationen från en etikett som behövs för att kunna skapa en klon, måste antingen kommunikation mellan en legitim läsare och etikett avlyssnas (avsnitt 2.4.1) alternativt måste en etikett skimmas (avsnitt 2.4.2). Avlyssning är ett passivt angrepp och innebär att kommunikationen mellan en läsare och etikett registreras. Skimning av en etikett innebär att en otillåten läsning av etiketten utförs, utan ägarens vetskap. Vilket angrepp som utförs beror i sin tur på etiketten. En avlyssning kanske inte är tillräcklig i alla fall då den inte ger all information som krävs för att skapa en klon. Det card-only-angrepp som har utförts i den praktiska delen kräver endast tillgång till den etikett som ska klonas. Andra möjliga angrepp för att utvinna information på en etikett beskrivs i den teoretiska delen av rapporten.

För att kunna avläsa den informationen från en etikett som behövs för att göra en klon, är det avstånd som avläsningen kan utföras på en viktig faktor för en angripare. Det är däremot ingenting som har undersökts praktiskt i detta arbete. Men detaljer om detta ingår i den teoretiska delen och även i analysen av kloningsförsöken som baseras på studier som har gjorts och vilka andra läsare som kan användas för att utföra angreppen.

Rapporten gör inga som helst anspråk på att angreppen beskrivna mot EM4100 och Mifare Classic skulle vara generella mot alla typer av RFID-etiketter.

1.4 Relaterade arbeten

RFID är inte en ny teknik och den har varit i rampljuset ett flertal gånger under diskussioner om integritetskränkning och frågor om säkerhet och risker.

Många svagheter och möjliga angreppmetoder gentemot olika typer av RFID-tekniker har studerats i teorin och även utförts i praktiken. I en artikel av Phillips, Karygiannis och Kuhn [5] beskrivs ett flertal olika RFID-tekniker som används och vilka standarder som finns, de inkluderar även en lista över olika säkerhetsfunktioner som de kan ha. Ari Juels, forskare på RSA laboratories, har skrivit ett flertal rapporter om säkerheten kring RFID. Bland annat har han skrivit en rapport över en studie som han har utfört över användningsområden av RFID och några möjliga angrepp mot dem [6]. Han har även skrivit en artikel tillsammans med D. Molnar och D. Wagner som handlar om integritet och säkerhet

med e-Pass [7]. Några av resultaten från dessa rapporter ingår i den teoretiska delen i denna rapport, då de diskuterar brister och angrepp mot diverse RFID-tekniker.

Mifare Classic, skapat av NXP Semiconductors[1], har fått särskild uppmärksamhet, dels för att det är en av de vanligare typerna av RFID-etiketter, men också för att etiketten har ett flertal brister. NXP Semiconductors har själva utvecklat den kryptografiska algoritm, CRYPTO1, som används och som företaget valt att hålla hemlig. Ett flertal rapporter har dock publicerats om olika angrepp mot etiketter av typen Mifare Classic. På Radbounds Universitet har de analyserat dess kryptosystem samt föreslagit och själva utfört ett flertal angrepp. I den första publicerade rapporten [2] fokuserades angreppen på läsaren. I rapporten avslöjades det kommunikationsprotokoll som används och detaljer över hur CRYPTO1 fungerar upptäcktes. Utöver detta kunde de knäcka krypteringsnycklar som använts genom att avlyssna kommunikation mellan en etikett och en läsare. Samma grupp har därefter arbetat vidare med att utföra mer effektiva angrepp mot Mifare Classic och i [8] presenterar de hur nycklar kan knäckas på fyra olika sätt genom att bara kommunicera med en etikett. Rapporten presenterar ett Brute Force-angrepp och två angrepp som utnyttjar olika brister i Mifare Classic. Det sista angreppet som presenteras är ett angrepp som genom att ha en nyckel kan knäcka fler nycklar på ett mycket effektivt sätt. Angreppet för att hitta fler nycklar efter att en nyckel har hittats används i kloningsexperimentet i denna rapport. Angreppet som används i den praktiska delen för att knäcka en första nyckel har utvecklats av Nicolas T. Courtois på University College London och presenteras i hans rapport ”The Dark Side of Security by Obscurity” [9].

För att läsa av en etikett är även avläsningsavståndet en viktig faktor. Gerard Hancke från University of London har utfört en rad experiment för att finna det maximala avståndet för att utföra skimningsangrepp mot ISO/IEC 14443-etiketter och avlyssning av både ISO/IEC 14443 och ISO/IEC 15693-etiketter. Detta är intressant för detta arbete eftersom Mifare Classic är en ISO/IEC 14443-etikett. För att utföra dessa försök användes utrustning särskilt byggd för att utföra dessa angrepp. Resultaten, som har publicerats i [10], visade att det är möjligt att skimma en ISO 14443-etikett på 15-20 cm avstånd med en antenn som är 15x20 cm stor. Resultaten för avlyssningsangreppet var lyckade upp till 2 m därefter kunde delar av kommunikationen avlyssnas (antingen från eller till etiketten) upp till 4 m, men angreppet var mycket känsligt för bakgrundsbrus.

[1] http://www.nxp.com/

2 Introduktion till RFID

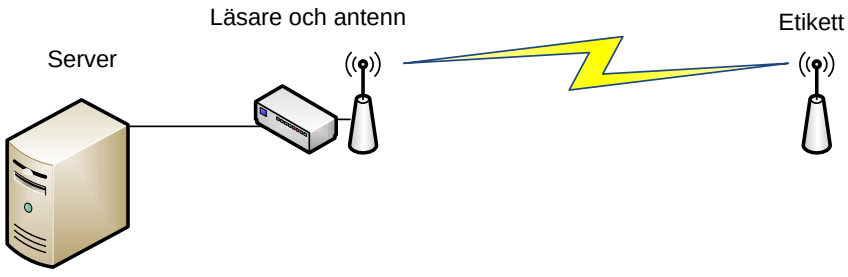
Det var under andra världskriget som föregångaren till RFID uppfanns. Identify friend or foe (IFF) kallades det system som uppfanns av britterna under andra världskriget. En radiomottagare placerades på alla deras plan som började sända en signal när den tog emot radiosignaler från radarsystemet på marken. När signalerna som skickades av planen mottogs kunde systemet identifierade dem som en friend [11]. Inte förrän långt senare började RFID sin riktiga frammarsch, vilket började med identifiering av djur och för inpassering utan en fysisk nyckel. Numera är RFID mer vidspritt och oron för ett ”storebrorssamhälle” blir större med den spårbarhet det medför och de ökade riskerna mot integriteten, som även kan komma att utnyttjas av brottslingar.

I detta avsnitt presenteras hur tekniken RFID fungerar, var RFID används och hur olika RFID-lösningar skulle kunna angripas. Den tekniska bakgrunden är en komprimerad beskrivning av tekniken baserad på information från [12] och läsaren kan referera till denna bok för en djupare teknisk beskrivning.

2.1 Teknisk bakgrund

RFID, radiofrekvensidentifiering, är en teknik som gör det möjligt att kontaktlöst överföra identifieringsinformation. En *RFID-etikett* skickar signaler som tas emot och hanteras av en *RFID-läsare*. Hur dessa signaler skickas varierar mellan olika etiketter, då de kan ha olika egenskaper vilka beror på vad etiketten används för. Hur signalen sedan hanteras av läsaren och det bakomliggande systemet är också beroende av användningsområdet. För att nämna några exempel kan det handla om såväl kontaktlösa inpasseringskort och betalkort som varuidentifieringsetiketter. Fördelen med att använda RFID för identifiering jämfört med andra motsvarande lösningar är att ingen direkt kontakt behövs för att läsa av en etikett, varken fysiskt eller optiskt. Det är även möjligt att läsa av en etikett genom flera olika typer av material och vätskor vilket gör det möjligt att ytterligare öka dess användningsområden.

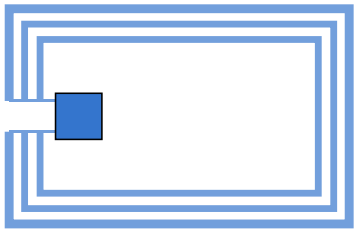
Ett system som använder sig av RFID består alltså av flera olika komponenter, allt beroende av användningsområde. När signaler skickas från en etikett till en läsare, måste de hanteras på något vis för att systemet ska vara komplett och kunna ta ett beslut om identifieringen eller genomföra en åtgärd. Ett bakomliggande system kan sedan hantera det data som mottagits, det kan exempelvis bestå av en databas som innehåller all information om identifiering eller liknande. Figuren nedan visar hur ett RFID-system kan se ut.



Figur 1: Översikt av ett komplett RFID-system, med en etikett som kommunicerar med en läsare, som i sin tur skickar/tar emot data från en server.

RFID-etiketter kan ha väldigt olika utformning och deras funktionalitet och komplexitet kan variera. Hitachi har utvecklats världens minsta RFID-chipp som är mindre än ett dammkorn [13], men vanligare utformning är etiketter som ser ut som kreditkort, nyckelringar eller varuetiketter. Alla

RFID-etiketter har däremot en sak gemensamt, de består åtminstone av en antenn och ett mikrochipp, se Figur 2. En del har bara ett *read-only*-minne och andra har ett minne som är både *läs- och skrivbart*. Utöver skillnaderna på hur minnet fungerar kan signalerna skickas i *klartext* eller *krypterat* vilket beror av mikrochippets egenskaper.



Figur 2: Illustration över en etiketts komponenter, en antenn och mikrochipp.

Mikrochippet i RFID-etiketten kan få ström på ett flertal olika sätt, en uppdelning görs på *passiva*, *aktiva* och *semi-aktiva* etiketter. Strömförsörjningen kan påverka ett flertal egenskaper, så som räckvidden på signalen och den fysiska storleken på etiketten.

Passiva etiketter har ingen egen strömförsörjning, istället får den sin ström från det elektromagnetiska fält som läsarens antenn alstrar genom induktans. En spänning genereras i antennen, som är en spole, och försörjer på så sätt mikrochippet med den ström som behövs. Inte förrän tillräckligt med energi har ackumulerats börjar den utföra olika operationer och skicka signaler. Eftersom den inte behöver några ytterligare komponenter för strömförsörjningen kan de vara mycket små, men detta leder även till att de har en kortare räckvidd jämfört med de andra typerna då de är beroende av läsarens alstrade magnetfält.

Aktiva etiketter har en egen strömkälla, till skillnad från passiva etiketter. De har ett inbyggt batteri och behöver inte vara nära en läsare för att sända signaler, istället sänds signalerna periodvis även om en läsare inte finns i närheten. Det inbyggda batteriet medför att denna typ av etiketter kan vara något större, men fördelarna är att de har en betydligt längre räckvidd då de inte är beroende av läsaren. Aktiva etiketter kan sända signaler genom material som en passiv etikett inte skulle klara av, så som vätskor.

Semi-passiva etiketter är en kombination av de andra två typerna. De har ett inbyggt batteri för att försörja mikrochippet med ström, men är beroende av läsarens elektromagnetiska fält för att skicka signaler, i likhet med passiva etiketter. Semi-passiva etiketter är ett mer strömsnålt alternativ till aktiva etiketter.

Utöver hur etiketter får ström kan etiketter arbeta på olika frekvensband, vilket vidare påverkar räckvidden och storleken på etiketten men även hur mycket data som kan överföras. Uppdelningen av frekvensband görs på lågfrekvensetiketter (100-140 kHz), högfrekvensetiketter (13,56 MHz), ultrahögfrekvensetiketter (868-870 MHz i Europa och 902-928 MHz i Nordamerika) och mindre vanliga frekvensband för etiketter är mikrovåg (2,45 eller 5,8 GHz) och ultrawideband (3,1–10,6 GHz).

Kombinationen av strömförsörjningsmetod, frekvensband och design av etiketten bestämmer i sin tur hur lång räckvidd en etiketts signal har. När en etikett designas är det viktigt att ta hänsyn till dess användningsområde. Ibland designas etiketter för att endast kunna bli avlästa på korta avstånd, så som betalkort, medan andra ska vara möjliga att läsas på långt avstånd väldigt fort, till exempel om

etiketten ligger i ett fordon för att betala tullavgift. Låg- och högfrekventa etiketter är ofta passiva då de inte kräver så mycket ström och kan då skicka signaler på 10-20 cm avstånd, aktiva sådana klarar av någon meter. UHF-etiketter har en mycket bredare räckvidd och de är ofta aktiva, räckvidden för sådana signaler varierar mellan 1-100 m.

2.2 RFID-standarder

De mer avancerade RFID-etiketterna är ofta kallade kontaktlösa smart cards, de kan ha olika säkerhetsmekanismer och ett minne som kan vara modifierbart. Ett flertal standarder definierar olika typer av sådana RFID-etiketter. Enklare RFID-etiketter, de med bara ett ID exempelvis, har inte standardiserats i samma utstreckning. EM4100 är en typ av etikett som inte följer någon standard.

ISO/IEC 14443 är en vanligt förekommande standard för högfrekventa (13,56 MHz) kontaktlösa smart cards av typen ”proximity card” och definierar utformning, radiofrekvensband, initialiseringsprotokoll och antikollisionsprotokoll samt överföringsprotokoll som ska användas för dessa. Standarden är vidare uppdelad i två typer, A och B, där den största skillnaden är i signalens modulering och i initialiseringsprotokollet. Mifare Classic följer ISO/IEC 14443 A-standarden. *ISO/IEC 15693* är också en standard väldigt lik ISO/IEC 14443, men definierar kontaktlösa smart cards av typen “vicinity card”, vilket har ett något längre läsavstånd än “proximity cards”. *ISO/IEC 21481* och *ISO/IEC 180892* är standarder för NFC-teknologin och är baserad på ISO/IEC 14443.

Utöver kontaktlösa smart cards, finns det även ett flertal andra standarder för andra användningsområden av RFID. *ISO/IEC 18000* standardiserar varuidentifiering och är uppdelad i ett flertal delar för olika frekvensområden, dessa förekommer i låg, hög, ultrahög och även i microvågsband. *ISO 18185* är en standard för RFID märkning av fraktgodscontainrar. Slutligen, RFID-märkning av djur är standardiserade i *ISO 11784* och *ISO 11785* och är vidare specificerad i *ISO 14223*.

2.3 Tillämpningsområden

Tillämpningsområdena för RFID är många. Etikettens komplexitet och minneskapacitet i kombination med olika styrkor på signalen medför att användningsområdena de passar till varierar. Detta medför att en angripare måste anpassa sitt angrepp mot ett specifikt tillämpningsområde och teknik.

2.3.1 RFID-implantat hos djur och människor

Ett av de första användningsområdena för RFID var djurmärkning. Husdjur ”chippmärks” med ett ID och information om djuret och dess ägare lagras i en databas. Det kan också användas för att spåra djur i det vilda, för att kunna registrera och kartlägga deras rörelsebeteende. Denna typ av chipp är ungefär lika stora som riskorn och placeras i djurets nacke. Hos boskap är det kanske mer vanligt förekommande att bära en öronmärkning med ett liknande RFID-chipp.

I människor är det inte lika vanligt med implanterade chipp, då det är ett väldigt kontroversiellt ämne. Dagens Nyheter har skrivit om en man som valt att operera in ett chipp i handen för att slippa bära på ett flertal inpasseringskort [14]. Ett annat omtalat användningsområde för implanterade RFID-chipp hos människor är för att kartlägga hälsotillstånd. PositiveID har tillsammans med RECEPTORS LLC patenterat implanterbara RFID-biosensorchipp [15] för att övervaka glukosnivåer i blodet hos diabetiker 2006, men dessa har ännu inte kommit ut på marknaden [16].

Att använda implanterade RFID-chipp istället för vanliga ID-kort är någonting som ibland kan ses i film, men att det faktiskt skulle börja användas i verkligheten är tveksamt. Övervakning och

kartläggning av vad vi gör och var vi är skulle vara möjlig och det skulle vara väldigt integritetskränkande. Fördelar med implanterade identitetshandlingar skulle vara att det är enklare att spåra människor, exempelvis för att förhindra kidnappning och enkelt kunna hitta människor av andra anledningar. Men samma system skulle kunna utnyttjas och anonymitet skulle inte vara möjligt, det kan öka riskerna för identitetsstöld och olovlig spårning skulle kunna göras.

2.3.2 RFID-etiketter på varor

RFID etiketter på varor kan i delas upp i två kategorier, stöldskydd och produktidentifiering.

2.3.2.1 Stöldskydd

Det finns olika typer av stödskydd, dels större återanvändbara etiketter som vanligen används på klädesplagg och andra mer värdefulla varor. Det finns också engångsetiketter som är RFID-etiketter som bland annat kan ses i dagligvaruhandeln. Stöldskyddsetiketterna kan avaktiveras när de passerar en läsare i kassan då den skickar ett ”kill”-kommando till etiketten som avaktiverar den. Avaktiveringen av en etikett kan exempelvis vara resultatet av en stark magnet som gör att etiketten helt enkelt slutar fungera. Dessa kan vara av den typen som bara består av en bit, antingen är den av eller på. Det kan diskuteras om egentligen är RFID men tekniken fungerar på samma sätt trots att det inte är ett ID som sänds. Andra lösningar för detta är att etiketten registreras som betald. Vid butikens utgång finns stora RFID-läsare som larmar i fall en etikett som inte har avaktiverats (eller betalats för) passerar.

Ett sätt att stjäla RFID-skyddade varor är att lägga varor i Faradays bur av något slag, vilket skulle förhindra läsning då radiovågorna stoppas av materialet. Ett alternativt angrepp är att avaktivera stöldskydden på samma sätt som i kassan. Angrepp kan också göras mot läsarna som ska larma om en vara med ett aktivt stöldskydd passerar, genom att förhindra att de fungerar ordentligt genom ett *Denial of Service*-angrepp (läs mer om Denial of Service i 2.4.4). RF jamming är en typ av Denial of Service angrepp vilket kommer leda till att avläsarna larmar hela tiden. Angreppet kan leda till att personalen istället väljer att stänga av larmen, vilket gör det möjligt att stjäla varor obemärkt.

2.3.2.2 Produktidentifiering

Enkla EAN-koder är för korta för att unikt kunna identifiera varor. En EPC, Electronic Product Code, sparas på en RFID-etikett och gör det möjligt att unikt identifiera varor då det har en större minneskapacitet. EPCGlobal är en organisation som har standardiserat EPC och en sådan etikett skulle kunna hålla information om bland annat varans tillverkningsdatum och tillverkare. EPC-etiketter förekommer oftare på pallar än enskilda varor för att underlätta spårning vid leverans [17].

Produktidentifieringsetiketter som använder RFID skulle även kunna användas för att inventera varor i en butik. I butiker kan varor som har etiketter med information om pris och liknande användas för att automatisera betalning. Genom att helt enkelt scanna en varukasse med RFID-märkta varor, kan totalpriset automatiskt beräknas utan att de behöver scannas en och en. Liknande lösningar förekommer även i bibliotek, då de använder RFID-etiketter för att registrera böcker vid utlåning.

Ari Juels diskuterar produktidentifieringsetiketter i sin artikel [6] och beskriver hur ett sådant system skulle kunna exploateras. Dels skulle individer kunna spåras, då vissa varor kanske har RFID etiketter som inte tas bort. Produktidentifieringsetiketterna skulle även kunna utnyttjas av angripare genom att modifiera data på etiketten, kanske för att ändra priset på varan eller för att rapportera felaktig information vid scanning av en pall med varor. Scanningen av pall-etiketten kan då efter ett angrepp

exempelvis informera om att det ligger varor i den när den egentligen står tom (eventuellt efter stöld). Ett annat alternativ är då det handlar om varor i en butik kan dessa, i likhet med stöldskyddade varor, läggas i en väska eller liknande som stoppar signalerna i en kassa som automatiskt skulle beräkna priset för varorna. Varorna skulle inte registreras och en angripare skulle kunna gå ut ur butiken utan att betala för dem.

2.3.3 e-Pass

e-Pass är pass som innehåller ett RFID-chipp. Denna typ av pass har standardiserats av ICAO, International Civil Aviation Organization, i följd av terroristattentaten i USA 2001. Chippet innehåller samma information som passet i övrigt, men även biometrisk information för identifiering av en individ. Den biometriska informationen kan bestå av ansiktsfoto och ibland även fingeravtryck [18].

Eftersom e-Pass innehåller personlig information, kan de jämföras med implanterade RFID-chipp för identifiering, skillnaden är att ett pass inte är någonting som man alltid bär med sig. En kidnappare skulle kunna utnyttja detta system genom att scanna personer med pass med syfte att identifiera betydelserika personer för kidnappning. Innehållet på ett chipp skulle också kunna kopieras i syfte att genomföra en identitetsstöld. Även om passfodralet är av ett material som blockerar signaler (Faradays bur), kan kommunikation mellan en legitim läsare och ett pass avlyssnas som även påpekas i den studie som Juels et al har skrivit om e-Pass [7].

2.3.4 Betalningsmedel

Att sedlar ska innehålla små RFID-chipp för att förhindra förfalskning av sedlar är något som ECB, European Central Bank, gjorde ett uttalande om att de skulle införa till 2005 [19]. Ingenting talar för att det faktiskt har implementeras än idag. Målet med att implementera små RFID-chipp i sedlar var att göra det möjligt att spåra pengar och på så sätt minska risken förfalskning och svarthandel. En risk med RFID-etiketter på sedlar är att det skulle kunna hjälpa en tjuv att identifiera personer med mycket kontanter genom att skanna möjliga mål.

Även för kortbetalningar har RFID gjort en lyckad entré. Bland annat erbjuder Visa [20] och MasterCard [21] kontaklösa kredit- eller kontokort, då endast ”ett svep” över terminalen krävs för att utföra en betalning, utan att behöva ange en kod för mindre summor. För större inköp kan det krävas både PIN-kod och användning av chippet på ett kort.

På ett liknande sätt kan betalningar göras med mobiltelefoner, med den NFC-teknik som finns i dem. Även med NFC erbjuder Visa kontaktlös betalning och ett annat betalmedel med NFC är Google Wallet [22].

Båda kontaktlösa betalkort och betalning med NFC fungerar på liknande sätt som ett betalkort med chipp eller magnetremsa, då en PIN-kod krävs. Visa skriver följande om säkerheten av NFC-betalningar: ”*The SIM card secure element (where the Visa mobile payment application is stored) fulfills the same industry standards as chip and PIN in plastic payment cards.”* [23]

Utöver betalning som är kopplat till ett konto kan även RFID-etiketter “laddas” med pengar. Detta gör det möjligt att använda en sådan etikett för att genomföra mikrobetalningar så som att betala för en kopp kaffe i en kaffeautomat eller för att automatiskt betala trafiktull eller parkeringsavgift. I dessa fall kan det vara möjligt att en summa dras av på etiketten, vilket en angripare skulle kunna se till att återställa efter varje användningstillfälle eller klona etiketter som är sedan kan användas igen, utan att ha laddat dem med pengar. Ett sådant angrepp demonstreras i [24] där ett

cafeteriabetalkort återställs efter varje köp. En annan möjlighet för en angripare är att tömma någon annans ”betalkort” eller göra att det inte fungerar, för att sabotera.

2.3.5 RFID i inpasseringssystem

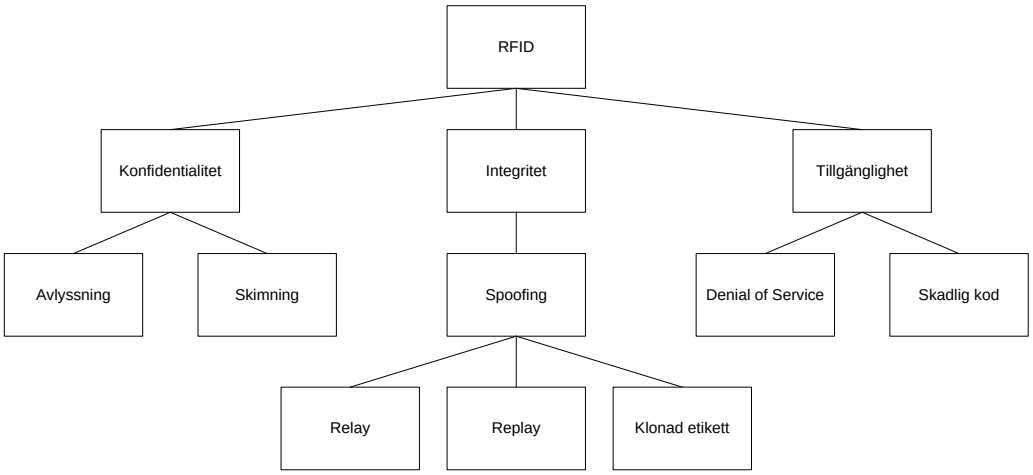
Det finns många typer av inpasseringssystem som använder RFID för identifiering. Det kan handla om tillgång till en dator eller dörrar som kräver upplåsning med RFID-etiketter. Även olika typer av biljetter förekommer (som kan ses som inpasseringssystem) som t.ex. engångsbiljetter till konserter och matcher eller periodbiljetter för resor i kommunaltrafiken. Även elektroniska bilnycklar skulle kunna sägas tillhöra denna kategori.

En RFID-etikett kan ses som en automatiserad inmatning av en PIN-kod. Att komma över en PIN-kod kan alltså liknas med att komma över innehållet på en etikett vilket är det största hotet i ett inpasseringssystem. Utifrån den information som angriparen har tillgänglig kan det vara möjligt att klona en etikett. Ett annat angrepp som kan utföras, baserad på avlyssning av kommunikation, är ett *replay*- eller *relay*-angrepp (läs mer om dessa angrepp i avsnitt 2.4.3). Läsaren skulle inte ana att det inte är den riktiga etiketten den kommunicerar med. Det kan medföra att en person kan erhålla obehörigt tillträde till skyddade områden eller att ett företag lider ekonomisk skada på minskad biljettförsäljning. Ett DoS-angrepp är ett angrepp som kan utföras mot ett inpasseringssystem skulle kunna förhindra inpasseringskontroll hel och hållet då det skulle kunna slå ut hela RFID-systemet.

2.4 Angrepp

Det finns många olika typer av angrepp som är möjliga att utföra på RFID-lösningar. Utöver vanlig stöld då någon kommer över det fysiska objektet, kan det data som finns på etiketten vara det som är av intresse för en angripare. Det kan hända att etiketten i sig innehåller känslig data som någon vill komma åt (t.ex. personlig information) och i andra fall kan denna information användas för att skapa nya etiketter. Dessutom kan angrepp som är intressanta för en typ av RFID-lösning vara mindre intressant för en annan. Till exempel kanske det är mer intressant för en angripare att förstöra en RFID-etikett som är till för stöldskydd än att klona informationen på den.

Vissa angrepp görs mot etiketter, andra mot läsare och ibland är de en kombination av båda. När angrepp utförs mot etiketter handlar det ofta om att ta reda på den information den har medan ett angrepp mot en läsare handlar om att få den att tro att en etikett används eller förhindra att den fungerar som den ska. Angrepp kan vidare delas upp i angrepp mot konfidentialitet, integritet och tillgänglighet (eng. CIA-triaden), se figuren nedan.



Figur 3: Trädstruktur som beskriver uppdelningen av angrepp.

2.4.1 Avlyssning

I nätverkssammanhang innebär avlyssning (eng. eavesdropping) att nätverkstrafiken avlyssnas av en tredje part som är obehörig.

Att trafiken mellan en läsare och etikett avlyssnas kan avslöja väldigt mycket information, beroende på hur och om signalerna har krypterats eller inte, i likhet med fallet för nätverksavlyssning. För etikett som sänder information i klartext, kan en angripare använda den informationen för att utföra ett *spoofing*-angrepp (se avsnitt 2.4.3) mot en läsare i ett senare skede.

Kryptering av data kan göra det svårare för en angripare att utvinna användbar information vid ett avlyssningsangrepp. Men genom att avlyssna en kommunikationssession kan en del information läcka om en osäker kryptering används. Signalerna kan analyseras i efterhand för att eventuellt utvinna information. I fallet Mifare Classic läcker kommunikationen mellan läsare och etikett tillräckligt med information för att kunna knäcka nycklar och eftersom en session har avlyssnats kan informationen som skickats vidare avkrypteras [2].

Avlyssning av kommunikation kan i många fall utföras på ett längre avstånd än direkt kommunikation med en enskild enhet. Detta är sant i de fall det handlar om passiva eller semi-passiva etiketter, eftersom de behöver strömförsörjning från etiketten för direkt kommunikation. Avståndet för avlyssning är också beroende av vilken typ av etikett som används, då signalen kan skickas med olika styrkor. Bakgrundsstrålning från andra system som stör kan också begränsa avståndet för avlyssning då det kan störa signalerna som ska avlyssnas. Kommunikationen från läsare till etikett och etikett till läsare kan variera i styrka eftersom strömförsörjningen varierar och därmed signalstyrkan. Detta bekräftar även Gerhard Hancke under sina försök att utföra avlyssning på ISO 14443 och ISO 15693 etiketter i [10]. Avlyssning av kommunikation i en riktning kunde vara enklare för några typer av etiketter av en viss standard än i den andra riktningen. Han nämner även att ett sådant angrepp skulle kunna förhindras genom ordentlig kryptering av data, då angriparen inte skulle få möjlighet att utvinna någon användbar information.

2.4.2 Skimning

Skimning, kortkapning eller smygavläsning, är ett angrepp som går ut på att en angripare läser av ett kort utan ägarens tillstånd. Normalt talar man om att skimma kreditkort och kortkapning.

När en RFID-etikett skimmas, går angreppet ut på att kommunicera med etiketten med en annan läsare än den genuina för att få ut information som ligger på etiketten. Skimning kan också, i likhet med avlyssning, avslöja information som ligger på etiketten. Det kan bestå av den information som krävs för att få inpassage exempelvis en kod, information om ägaren av kortet eller annat. Informationen som utvinns av ett skimningsangrepp kan göra det möjligt att klona en etikett. Detta innebär att en kopia av en etikett skapas, med eller utan ägarens tillstånd. En kopia kan dels skapas på en emulator eller så kan det skrivas till en ny etikett för att göra en klon.

Att manipulera data på en etikett, utan att ägaren är medveten om detta, är också en typ av skimningsangrepp. Detta kan innebära att innehållet ändras eller raderas. Målet är då inte att kopiera etiketten, utan att ändra informationen på sådant sätt att det eventuellt inte fungerar eller att innehållet har manipulerats för att fungera på ett annat sätt. Om etiketten exempelvis används till betalning kan detta medföra att den innestående summan har minskats (eller ökats).

I de fall etiketten är passiv eller semi-passiv, krävs att läsarens antenn är nära etiketten för att kunna skimmas, då den kräver energiförsörjning från läsaren, jämfört med skimning av aktiva etiketter. Andra svårigheter en angripare kan stöta på är att etiketten kräver autentisering av läsaren för att den ska kommunicera med den.

2.4.3 Spoofing

Spoofing innebär att angriparen lurar en användare eller ett system genom att låtsas vara genuin. Vanligen handlar det om en bluffhemsida som en användare hamnar på istället för den äkta hemsidan, som sedan samlar information om användarna, till exempel kontoinformation. Det kan också handla om falska mail, då en mottagare tar emot ett mail från en förfalskad sändaridentitet.

När det gäller RFID handlar det istället om att antingen lura en läsare till att tro att den kommunicerar med en äkta etikett när det egentligen inte är det, eller lura användare av RFID-etiketter genom att placera en falsk läsare som läser av information från en etikett (skimma). Många andra angrepp faller också under kategorin spoofing, då de går ut på att lura en etikett att tro att den kommunicerar med en legitim läsare eller tvärtom.

Ett spoofingangrepp är ofta beroende av att ett tidigare angrepp har lyckats och nödvändig information har utvunnits för att kunna utföra ett sådant angrepp, exempelvis för att skapa en klon av en etikett eller för att kunna göra en förfalskad läsare. En förfalskad läsare kan användas för att samla ihop data från etiketter som skannas av den. Om den känner till alla nycklar då krypterade etiketter används kan den användas för att samla ihop data från etiketterna, som därefter kan användas för att skapa kopior av etiketter alternativt kan det vara själva informationen på etiketten som är intressant. I andra fall kan en sådan falsk läsare vara till för att kartlägga vilka etiketter som finns i omlopp eller spåra någon.

I det andra fallet, då en läsare spoofas är det användandet av en oäkta etikett (en kopia av något slag) som utgör angreppet. En falsk etikett kan vara en klon av en annan etikett som finns i systemet. Klonen kan vara en etikett i form av ett kort, men det är även möjligt att använda en emulator för att spoofa en läsare. En emulator är en hårdvaruenhet som kan agera en RFID-etikett och har ett minne som är fullt skrivbart. Det finns ett flertal olika emulatorer som kan bete sig som olika typer av RFID etiketter, allt från enkla, lågfrekventa etiketter som bara har ett ID till mer avancerade lösningar, så som smart cards. Proxmark3 [3] är en enhet som använts vid de praktiska experiment som beskrivs i

denna rapport och kan emulera några olika typer av RFID-etiketter och kan programmeras för att emulera fler. OpenPICC [25] är en annan emulator som har stöd för 13,56 MHz etiketter men den är mindre lättillgänglig, för den händige finns ritningar tillgängliga och källkoden är open source. Chameleon [26] är en RFID emulator som bland annat kan emulera som Mifare DESFire EV1 och har hårdvaruaccelererad DES kryptering. Återigen finns inte denna att köpa men implementationen finns i publicerad i rapporten om Chameleon [26].

2.4.3.1 Replay

Genom att spela in kommunikation, helt eller delvis, kan ett replay-angrepp utföras. Angreppet görs därefter genom att spela upp det som har spelats in, inspelningen kan spelas upp som det är eller modifierat, beroende på vad angriparen vill utvinna.

Genom att avlyssna en kommunikationssession mellan en läsare och en etikett kan kommunikationssessionen spelas in och modifieras eller spelas upp som den är för att lura en läsare att tro att den kommunicerar med en etikett. Kommunikation som saknar en handskakningsprocess för autentisering kan enkelt falla offer för ett replayangrepp då sändaren inte verifieras. Det kan också vara möjligt att utföra angreppet genom att försöka autentisera ett flertal gånger tills man hamnar i samma situation som i den inspelade sessionen. Detta kan utnyttjas av en angripare genom att till exempel spela in när en etikett som fungerar som en biljett kommunicerar med en läsare när en resa ska betalas. Om inget skydd som autentisering eller kryptering finns kan angriparen använda samma biljett om och om igen genom att utföra ett replayangrepp.

2.4.3.2 Relay

Ett relay-angrepp går ut på att en angripare skickar vidare ett meddelande till en annan mottagare än den som sändaren väntar sig. Det är i princip en kombination av ett ”man-in-the-middle”-angrepp och ett replay-angrepp.

Genom att en enhet, eller två i detta fall, tar emot och därefter sänder vidare signaler, är det möjligt att få en läsare att tro att den kommunicerar direkt med en genuin RFID-etikett och vice versa. En enhet agerar läsare mot etiketten som sedan skickar signaler till en annan enhet som i sin tur agerar en etikett mot en läsare. Detta innebär att signaler skulle kunna sändas över halva jordklotet.

För att utföra ett relay-angrepp krävs två angripare som bär varsin enhet som kan skicka och ta emot signaler. Dels ska enheten kunna agera en RFID-läsare eller en RFID-etikett och utöver detta ska båda kunna ta emot signaler från den andra enheten. Det krävs nödvändigtvis inte någon särskild utrustning för att utföra angreppet. Smart phones med NFC-stöd kan användas och de kan agera både RFID-läsare och etikett och dessutom kan de skicka data sinsemellan med hjälp av till exempel 3G, Bluetooth eller Wi-Fi. Sträckan mellan de två enheterna kan vara mycket lång beroende av vilken teknik som används för att skicka signalerna. Ett relay-angrepp illustreras i figuren nedan.

Figur 4: Illustration av ett relayangrepp, två enheter skickar en signal på ett längre avstånd och som i sin tur kommunicerar med en RFID etikett respektive läsare.

För att förhindra relay-angrepp finns det mekanismer som kan användas för att upptäcka detta. Mifare Plus X är ett smart card som har ”proximity detection” som ska kunna upptäcka ett relay-angrepp. Ett sätt att upptäcka denna typ av angrepp är genom att kontrollera hur lång tid det tar att få ett svar, då det kan ta längre tid om en signal måste gå via ett flertal enheter [27]. Om det tar för lång tid att få svar på ett kommando kan kommunikationen nekas, då fördröjningen kan vara orsakat av ett relay-angrepp.

2.4.4 Denial of Service

Ett angrepp som förhindrar en server att fungera som den ska kan vara orsakad av en Denial of Service-angrepp (förkortat DoS). Angreppet genomförs genom att ett stort antal sessioner startas mot servern så att den inte hinner svara på alla förfrågningar. Detta förhindrar sedan nya sessioner från andra användare eftersom servern är upptagen.

För RFID gäller samma sak, för att få ett system att sluta fungera som den ska kan ett DoS-angrepp utföras med så kallad ”RF jamming”. Ett DoS-angrepp mot ett RFID-system med RF jamming är likt angreppet som görs mot t.ex. en webserver. Angreppet bombarderar en läsare med ”falsk” kommunikation från ”etiketter”, läsaren kan inte hantera alla mottagna signaler och leder till att angreppet förhindrar en läsare att fungera som den ska. Genom att hindra en etiketts eller läsares funktionalitet kan konsekvenserna vara väldigt olika beroende på tillämpningsområde. För ett inpasseringssystem som slutar fungera kan det medföra att ingen släpps in, manuella kontroller måste utföras vilket tar längre tid eller att man helt struntar i kontrollerna för stunden. En angripare kan vara intresserad av detta angrepp mot ett inpasseringssystem för att stoppa ett möte eller försöka ta sig in obemärkt. Ett annat scenario är att det istället handlar om ett butikslarmsystem, då kan ett DoS-angrepp leda till att larmsystemet stängs av och en angripare kan föra varor ur butiken obemärkt.

2.4.5 Överföring av skadlig kod

Virus, skadlig kod och intrång är olika sätt att bryta sig in i system. I de flesta fall finns skydd och metodik för att hindra den typ av angrepp, särskilt i de fall då de är vanligt förekommande. Det är dock inte lika vanligt att tänka på det vid tillämpningar som använder RFID.

Ibland vill en angripare bara sabotera ett system, vilket i sin tur kan leda till att hela systemet går ner, data går förlorad eller att felaktiga kommandon utförs. Detta skulle även kunna göras med RFID-etiketter som innehåller skadlig kod. När en läsare läser av en etikett förs den skadliga koden in i det bakomliggande systemet.

För att utföra ett sådant angrepp, måste etiketten vara skrivbar och dessutom måste den skadliga koden få plats i minnet. Ett alternativt sätt att införa skadlig kod är att använda en emulator som har ett minne som är fullt modifierbart. Även med ett fåtal tecken kan det vara möjligt att göra skada, genom att injicera någon slags skadlig kod i systemet. Det RFID-baserade viruset som presenteras i [28] är det första av sitt slag och utför en SQL injektion på det bakomliggande systemet. Med en 127 tecken lång sträng som får plats i etikettens minne, utförs angreppet när etiketten som har ”viruset” blir läst. Detta ”virus” sprids sedan vidare till de etiketter som blir avlästa efter att viruset har angripit systemet.

För att utföra ett angrepp som injicerar skadlig kod i det bakomliggande systemet kan en angripare antingen modifiera data på en etikett som används alternativt skriva en ny etikett eller använda en

emulator. Det bakomliggande systemet måste ha skydd för att förhindra intrång och kontrollera vad som har lästs från en etikett innan data hanteras på ett sådant som gör det möjligt för en angripare att sabotera ett system, precis som i andra datorsystem.

3 Kloningsexperiment av RFID

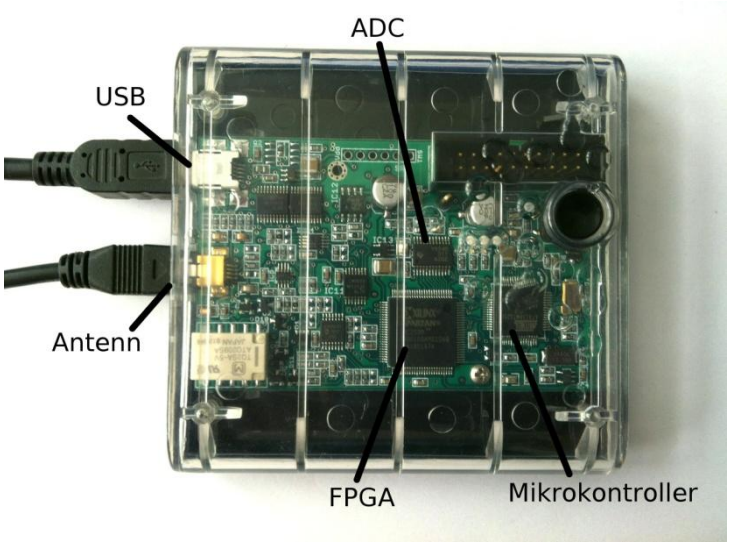
För att verifiera praktisk tillämpning av svagheter i vissa RFID-lösningar presenterar detta avsnitt två kloningsförsök. Det första är en RFID-etikett av modellen EM4100 som används som inpassering till bland annat kontor och hus. EM4100 har endast ett ID i ett read-only-minne och använder ingen kryptering eller handskakning. Den andra etiketten som klonas är av modellen Mifare Classic. Etiketten används i olika inpasseringslösningar men där säkerheten betraktas som viktig. Mifare Classic är en ISO 14443-etikett och har både läs- och skrivbart minne. Innan Mifare Classic börjar kommunicera med en läsare utförs en autentisering mot läsaren och kommunikationen mellan läsare och etikett är krypterad. För att utföra kloningsförsöken har en RFID-skrivare/läsare/emulator som heter Proxmark3 använts.

3.1 Beskrivning av utveckling- och testmiljö

För att klona RFID-etiketter krävs ett par olika verktyg, dels används ett RFID-verktyg som kallas Proxmark3 som kan hantera både in- och utgående signaler i flera olika frekvensband. Utöver Proxmark3 behövs en dator och etiketter som används till kloningsförsöken. Dels används tomma etiketter för skrivning (kloner) och etiketter som klonerna ska baseras på, för läsning.

3.1.1 Proxmark3

För att utföra dessa försök används en Proxmark3 som är ett generellt RFID-verktyg som är ämnad för hobbyentusiaster, utvecklare och forskare. Den är utvecklad av Jonathan Westhues på Cambridge University, för att forska kring RFID. Ritningarna till den finns tillgängliga på Internet[2] för den som är mycket händig och vill bygga en sådan själv. Numera finns den även att köpa färdigmonterad[3]. Figur 5 visar en bild på den Proxmark3 som har använts i detta arbete. Proxmark3 kan skicka och ta emot signaler, vilket gör det möjligt att avlyssna, emulera etiketter och läsa/skriva etiketter, både lågfrekventa (~100 kHz) och högfrekventa (13.56 MHz).



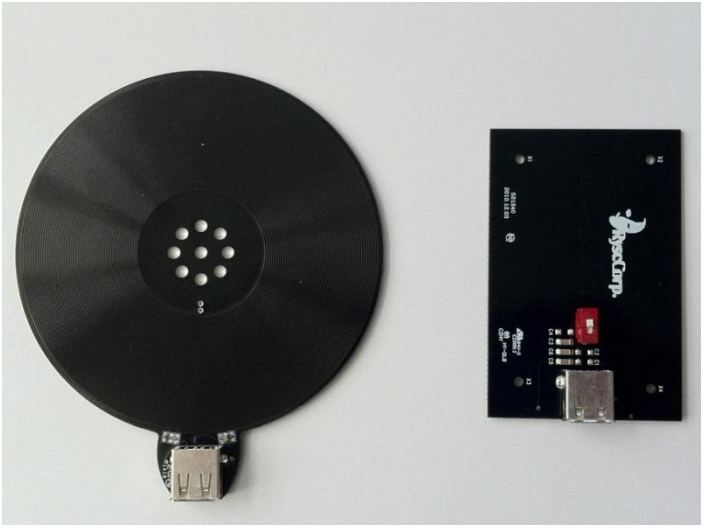
Figur 5: Fotografi av Proxmark3 med ett ytterhölje som skyddar dess komponenter.

Proxmark3 skickar och tar emot signaler med en extern antenn. Signaler digitaliseras till en 8-bitars representation i en ADC (Analog to Digital Converter). Den digitala strömmen bearbetas vidare via en

[2] Information för att bygga Proxmark3 finns tillgänglig på: http://cq.cx/proxmark3.pl
[3] Proxmark3 kan köpas från: http://www.proxmark.org/

FPGA (Field-programmable Gate Array). Dess roll är att hantera de inkommande digitala signalerna och gör dessa signaler tillgängliga till mikrokontrollern, eller tvärtom för utgående signaler; modulera dessa för att sedan skicka dem vidare. Mikrokontrollern är en Atmel AT91SAM7S256 med 256 kb flashminne och en maximal processorhastighet på 55 MHz. Mikrokontrollern hanterar en stor del av de kommandona som datorklienten (mjukvaran) gör tillgänglig för Proxmark3.

Antennen kan antingen byggas själv, då det enda kravet är att den har en Hirose USB kontakt (input till Proxmark3), men det enklare alternativet är att köpa antenner speciellt utvecklade för Proxmark3. Två olika antenner användes för att utföra dessa experiment, en för lågfrekventa etiketter och en för högfrekventa[4], se Figur 6. Avläsningsavståndet beror till stor del på den energi som antennen kan överföra till etiketten. De antenner som använts under verifieringen av angreppen ta emot signaler med ett avstånd på cirka 3 cm.



Figur 6: Antenner till Proxmark3, höger LF antenn, vänster HF antenn.

Proxmark3 ansluts till en dator via USB vilket gör det möjligt att styra mikrokontrollern via ett klientprogram på datorn som skickar kommandon till utrustningen. På så sätt kan beräkningar som kräver mer kapacitet än det som Proxmark3 kan erbjuda utföras på datorn. Utöver kommunikation med datorn används USB-kontakten för att försörja enheten med ström. Proxmark3 kan även användas i stand-alone läge, då den inte använder datorn, ström tillförs via en USB-laddare som exempelvis försörjs av ett batteri. Då Proxmark3 är frikopplad från datorn finns bara ett sätt att ge input till Proxmark3 och det är via den knapp som finns vilket begränsar möjligheterna i det läge en del då det inte är så flexibelt.

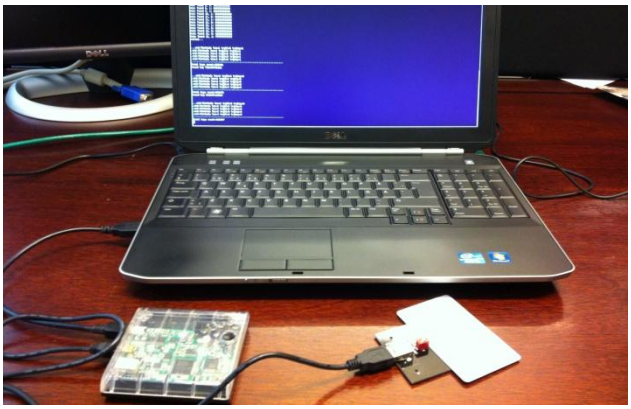
3.1.2 System

För kloningsförsöken har en Dell laptop använts.
Specifikation dator:

```
CPU: Intel Core i5-2430M, Dual Core 2.40GHz
RAM: 4GB
Operativsystem: Ubuntu 11.10 32-bit
```

Källkoden till Proxmark3 finns tillgänglig online på en versionshanteringsserver[5], kallad SVN (Subversion). Följande versioner har använts till grund för detta arbete:

Figur 7: Arbetsplats, visar Proxmark3 inkopplad till dator med tillhörande högfrekvent antenn och en Mifare Classic etikett.



[4] Antenner köpta från: http://www.proxmark.org/
[5] All kod finns online: http://code.google.com/p/proxmark3/

```
Bootrom: SVN version 526
Operativsystem: SVN version 526
Klient: SVN version 526
FPGA image built on 2009/12/8
```

Det fasta program (eng. firmware) som fanns tillgänglig att ladda ner vid utförandet av detta arbete erbjöd en stor del av nödvändig grundfunktionalitet för att kunna utföra verifieringarna i denna rapport. FPGA koden är skriven i Verilog och mikroprocessorns operativsystem och datorklienten främst skriven i C. Tack vare de fasta programmen och Proxmark3s konstruktion är det möjligt att genomföra godtyckliga operationer mot både låg och högfrekventa RFID lösningar. Proxmark3 kan på så sätt agera både läsare och etikett samt avlyssna trafik mellan en etikett och en läsare. En stor del av funktionaliteten för att kunna använda Proxmark3 med ISO 15693-, ISO 14443A och ISO 14443B-kompatibla enheter finns redan implementerad i källkoden för Proxmark3.

Proxmark3 ska dock ses som en utvecklingsplattform. Den största delen av arbetet att verifiera angreppen beskrivna i denna rapport har gått ut på att vidareutveckla mikroprocessorns operativsystem för att sedan både kunna emulera etiketter och klona etiketter samt att utöka klientens funktionalitet för att stödja dessa nya funktioner.

3.2 Fallstudie 1: Kloning av EM4100

EM Microelectonics är tillverkare för EM4100 (tidigare benämning H4100). EM4100 är en passiv 125 kHz RFID-etikett som vanligt förekommer som inpasseringstoken till hus och kontor. Det är en etikett som har ett read-only-minne som innehåller dess ID. Minnet programmeras under tillverkningen med laser och det är inte möjligt att ändra minnesstrukturen efter detta.

3.2.1 EM4100 – Teknisk bakgrund

3.2.1.1 Minnesstruktur

Minnesstrukturen i EM4100 är enkel, som består av en 64-bitar lång minnesarray. De 64 bitarna utgörs av ett 40-bitar långt ID (10 HEX) och 24 kontrollbitar. I Figur 8 visas hur minnet är strukturerat. Minnesblocket inleds med nio startbitar, därefter delas identifikationsnumret (D_{00}-D_{93}) upp i tio 4-bitars block som var och ett efterföljs av en paritetsbit (P_0-P_9). Blocket avslutas med paritetsbitar för varje kolumn (P_{C0}-P_{C3}). Den sista biten i minnet är en stopp-bit (0). En fullständig beskrivning finns i databladet för EM4100 [29].

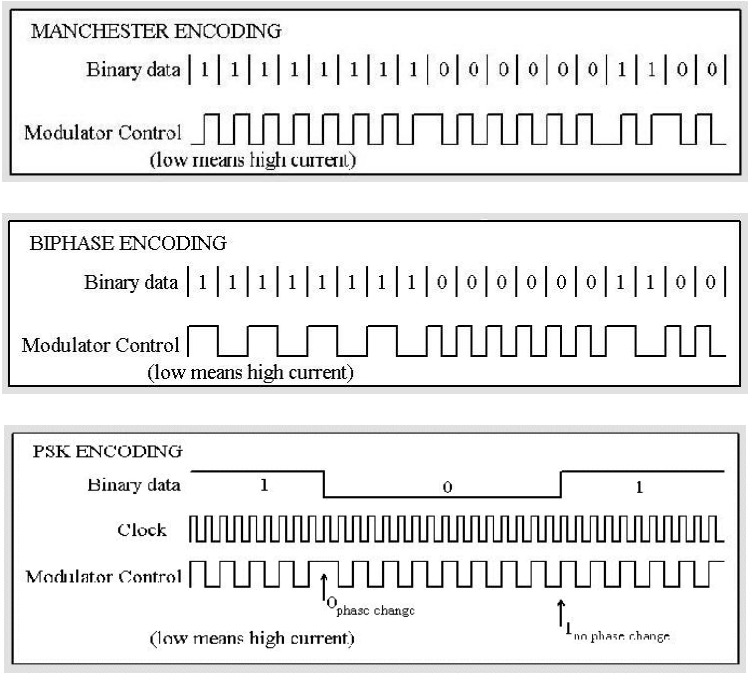
1	1	1	1	1	1	1	1	1
				D_{00}	D_{01}	D_{02}	D_{03}	P_0
				D_{10}	D_{11}	D_{12}	D_{13}	P_1
				D_{20}	D_{21}	D_{22}	D_{23}	P_2
				D_{30}	D_{31}	D_{32}	D_{33}	P_3
				D_{40}	D_{41}	D_{42}	D_{43}	P_4
				D_{50}	D_{51}	D_{52}	D_{53}	P_5
				D_{60}	D_{61}	D_{62}	D_{63}	P_6
				D_{70}	D_{71}	D_{72}	D_{73}	P_7
				D_{80}	D_{81}	D_{82}	D_{83}	P_8
				D_{90}	D_{91}	D_{92}	D_{93}	P_9
				P_{C0}	P_{C1}	P_{C2}	P_{C3}	0

Figur 8: Minnesstruktur EM4100.

3.2.1.2 Dataöverföring

När etiketten befinner sig i det elektromagnetiska fältet som alstras av en läsare, börjar etiketten sända allt det data som finns i minnet om och om igen. Så fort etiketten tas bort från läsarens elektromagnetiska fält, och därmed inte får någon energi, slutar etiketten att sända signaler. Signalerna skickas i den sekvens som data är representerat och strukturerat i etikettens minne. Startsekvensen, paritetsbitarna och stoppbiten gör det möjligt för en läsare att identifiera en etikett. Om paritetsbitarna inte stämmer, ignoreras det som tagits emot.

EM4100-etiketten finns i några olika varianter enligt dess datablad [29]. Varje bit representeras antingen av 16, 32 eller 64 perioder av bärvågen och datamoduleringen är valbar mellan manchester, bifas eller PSK modulering.

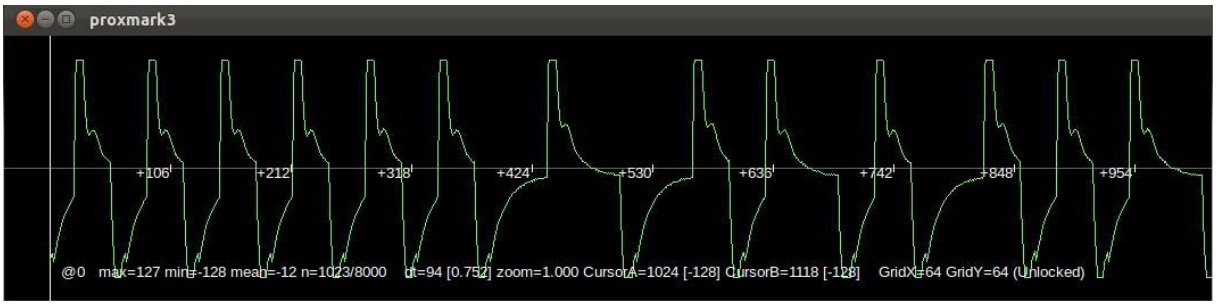


Figur 9: Beskrivning av de olika valen av datamodulering. Bilder från http://www.priority1design.com.au/em4100_protocol.html

3.2.2 Genomförande

För att klona en EM4100-etikett krävs att det ID som etiketten har är känt. Detta kan fås genom att använda en RFID-läsare som kan läsa etiketten. Istället för en kommersiell EM4100 läsare har Proxmark3 använts i detta arbete, som programmerats för att kunna ta emot den typen av signal som EM4100 använder sig av. Alla etiketter av typen EM4100 som stötts på under arbetet har varit manchestermodulerade och skickar en bit på 64 perioder av bärvågen.

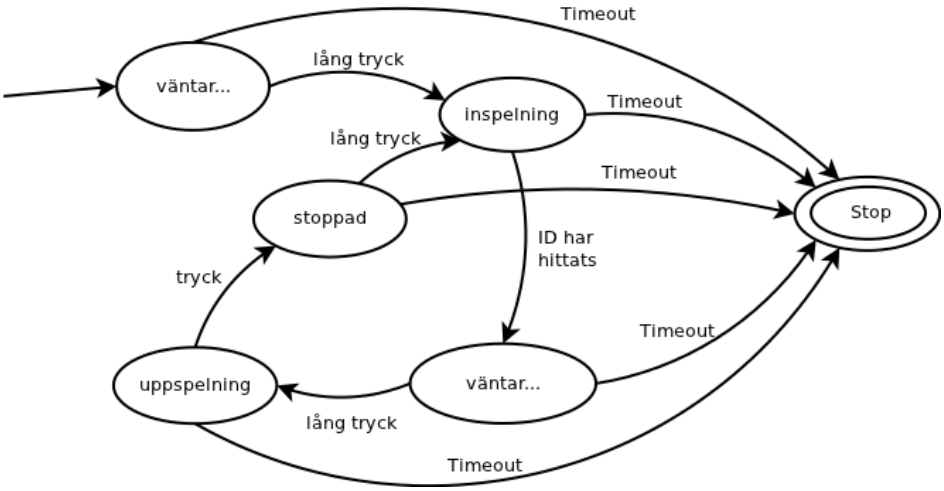
När Proxmark3 används som en läsare, lagras samplade värden (plottade i Figur 10) av signalen i en buffert i minnet och sedan demoduleras den manchestermodulerade signalen (som signalen antas vara under dessa experiment). Proxmark3 gör därefter en sökning i bufferten för att hitta startsekvensen 111111111. Efter att startsekvensen identifierats förväntas att ett ID och korrekta paritetsbitar följer och att meddelandet ska avslutas med stopp-biten 0. Om informationen är felaktig någonstans, inkorrekta paritetsbitar eller att en stopp-bit inte förekommer, fortsätter sökningen efter ett ID vidare.



Figur 10: Skärmdump av det diagram som Proxmark3 datorklient kan rita av de samplade värden som tagits emot vid läsning av EM4100-etikett.

Ett enklare sätt att läsa ett ID är genom att använda en kommersiell EM4100-läsare, denna kan hantera de olika typerna av etiketter och hanterar dem på ett smidigare sätt. De fungerar oftast som ett tangentbord då den är kopplad till en dator via USB. När en etikett kommer in i dess elektromagnetiska fält och börjar skicka sitt identifieringsnummer. Läsaren tar emot denna signal och skickar denna information vidare till den dator som den är kopplad till. Läsaren kan till exempel programmeras för att skicka signaler som tecken och i fall en texteditor eller liknande är aktiv på datorn skrivs de mottagna tecknen i klartext där.

Förutom att läsa EM4100-etiketter kan Proxmark3 även användas för att emulera sådana, vilket är en funktionalitet som finns sedan tidigare. Under emuleringen skickar Proxmark3 kontinuerligt signaler i likhet med en EM4100-etikett, utifrån det ID som ska emuleras. Signalerna skickas manchestermodulerade med en bit som skickas på 64 perioder av bärvågen, som de EM4100-etiketter som används för arbetet. Den befintliga källkoden kan läsa och emulera EM4100-etiketter genom att använda datorklienten. Eftersom det inte krävs mycket beräkningskraft för att utföra operationer för att läsa och emulera EM4100, är det möjligt att utöka funktionaliteten för att klara läsning och emulering i stand-alone läge, d.v.s. utan en dator. All beräkning utförs på samma sätt som på en dator, men istället sker det i mikroprocessorn på Proxmark3. För emulera en etikett i stand-alone läge måste den etikett som ska emuleras skannas under samma session, eftersom strömförsörjningen inte får gå förlorad då informationen (etikettens ID) är skriven i det flyktiga minnet. Genom att trycka på knappen på Proxmark3 under 2 sekunder startas stand-alone läget. Diagrammet nedan visar hur enheten fungerar därefter.

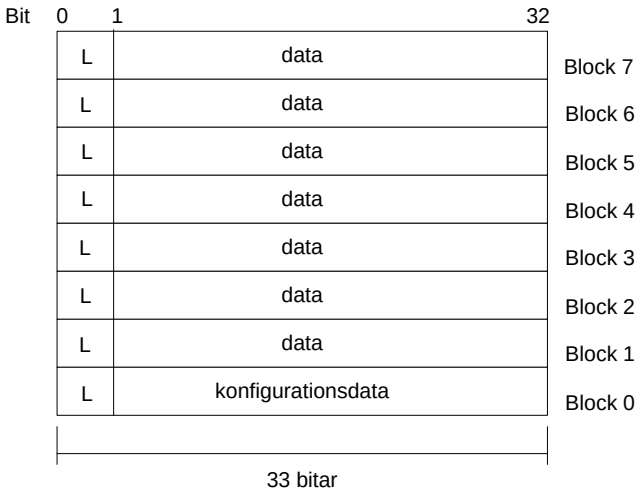


Figur 11: Stand-alone läge för emulering av EM4100 med Proxmark3.

Att klona en EM4100-etikett kräver en annan typ av RFID etikett att skriva till, eftersom EM4100s minne inte är skrivbart. Istället används en annan typ av etikett som är både läs och skrivbar och som kan skicka signaler i samma format som en EM4100-etikett. Det finns etiketter som är omprogrammerbara till att skicka signaler i ett flertal valbara bit-rates och modulering av data. De kan därmed programmeras på ett sådant sätt att de beter sig som en EM4100-etikett. En läsare skulle inte detektera någon skillnad på signalen från en EM4100-etikett och en etikett som programmerats för att bete sig som EM4100. T5555 (eller Q5) [30] och T5567 [31] från Atmel/Temic är två sådana programmerbara etiketter. I likhet med EM4100 börjar de skicka ut all data som finns lagrat i minnet när etiketten kommer in i läsarens elektromagnetiska fält.

Proxmark3 har redan funktioner för att skriva data till denna typ av programmerbar etikett. Det enda som behövdes var att programmera om etiketten med rätt konfiguration för att likna en EM4100-etikett. Den angivna konfigurationen beskriver hur mycket data som ska skickas samt hur många perioder av bärvågsfrekvensen en bit ska skickas på och vilken typ av datamodulering.

I Figur 12 nedan illustrerar den del av minnet i T5555/T5567 som används för EM4100-kloning och ser likadan ut mellan dessa (de har även andra block som inte används för att klona EM4100) [30] [31]. Givet ett ID beräknas det som ska skrivas till etikettens minne, även paritetsbitar, startsekvensen och stoppbiten läggs till för att bygga upp samma minnesstruktur som visas i Figur 8. På T5555/T5567-etiketten används block 1 och 2 för att lagra 64-bitar data, som EM4100-etiketten skulle innehålla. Block 0 innehåller konfigurationsdata, som är något olika för T5555 och T5567, se respektive datablad för detaljer [30] [31]. Vid kloningsförsöket användes T5555-etiketter och Proxmark3 programmerades för att skriva konfigurationen till etiketten. Etiketten konfigurerades för att skicka data från block 1 och 2 manchestermodulerat och med en bit data på 64 perioder av bärfrekvensen, på samma sätt som EM4100-etiketter.

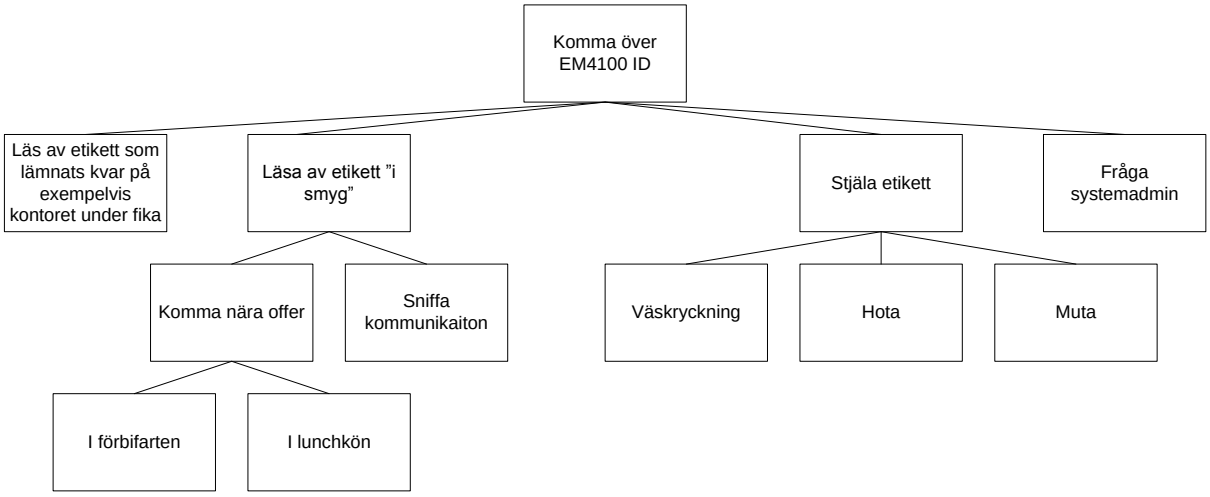


Figur 12: Gemensam minnesstruktur av T5556 och T5567 som används för att klona EM4100 etiketter, den första biten (L) är en låsbit och anger om fältet är omprogrammerbart.

För att klona ett ID till en etikett placeras en T5555-etikett nära antennen och ett kommando ges med önskat ID, vilket sedan skrivs till etiketten. T5555-etiketten fungerar sedan som en EM4100-etikett.

3.2.3 Analys och diskussion

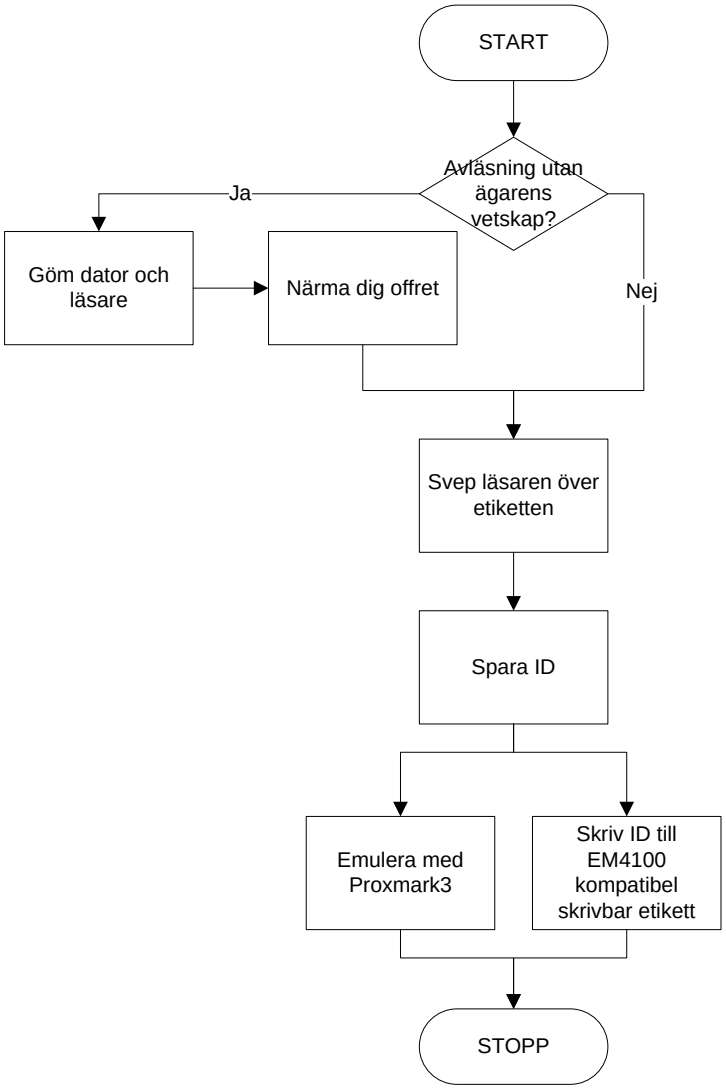
Trots att EM4100 endast är en read-only-etikett är det fullt möjligt att skapa en klon. Dels är det möjligt att använda en emulator för att emulera etiketten och dels är det möjligt att skriva informationen till en etikett som fungerar på samma sätt som EM4100.



Figur 13: Attackträd för att komma över ett EM4100 ID.

Att skapa en klon kräver endast att en etiketts ID är känt. Etikettens ID kan hittas på flera olika sätt, se Figur 13. För att läsa ut ett ID från en etikett kan ett flertal olika verktyg användas, där en kommersiell läsare eller ett verktyg likt Proxmark3 kan anges som exempel. Att använda Proxmark3 är inte det bästa valet i det fall det är viktigt att utföra en snabb avläsning, exempelvis mot ett ovetande offer, då den är mer känslig för variationer i signaler än andra läsare. Avläsningen måste

ske under rätt tillfälle, då den inte läser inkommande signaler och hanterar dem samtidigt för att hitta ett ID. Som tidigare nämnts i avsnitt 3.2.2, sparas samplade signal-värden i en buffert som programmet söker i för att hitta en sekvens som innehåller ett etikett-ID. Om inte ett ID har identifierats i bufferten, börjar Proxmark3 ta emot signaler som en läsare igen för att fylla bufferten med nya värden. En ny sökning utförs för att hitta sekvensen som motsvarar ett ID från en EM4100 etikett och denna process upprepas tills ett ID hittas eller programmet avslutas. En kommersiell läsare är i detta fall mer pålitlig för att läsa av ett ID. Dessutom är en kommersiell läsare en betydligt billigare lösning för detta syfte och en sådan kan läsa av ett ID av en etikett som bara sveps förbi. Läsaravståndet beror till stor del av antennen (i kombination med etiketten). Den antenn som finns att köpa till Proxmark3 kräver att etiketten mer eller mindre har kontakt med antennen för att signalerna ska registreras medan den kommersiella läsaren som använts för dessa försök kan läsa en EM4100 etikett på ca 3-10 cm avstånd. Det finns även läsare som har antenner som kan läsa på 1m avstånd, men de är då relativt stora.



Figur 14: Flödesdiagram som presenterar vilka steg som måste utföras för kloning av EM4100.

Nästa steg är att använda det ID som lästs av från etiketten för att spoofa en läsare. Proxmark3 har den fördelen att den även kan användas för att emulera en etikett, vilket kan göras på en gång efter att ett ID lästs in. Proxmark3 kan sedan spela upp ID, båda när den är inkopplad till en dator eller i stand-alone läge. Det senare gäller bara om etiketten kan läsas under samma ”session”. Det är även möjligt att skapa en ny etikett med samma ID, så länge en kompatibel etikett används som beskrivits tidigare. Till detta finns ett flertal alternativ, exempelvis T5555- eller T5567-etiketter. För att skriva till en kompatibel etikett kan antingen Proxmark3 användas eller en annan typ av läsare som klarar av skrivning till den typ av etiketter. Det finns även så kallade ”kloningsmaskiner” som är en kommersiell produkt som är ämnad för låssmeder. Keymaster Pro av RMXlabs kan klona några olika typer av RFID-etiketter, bland annat EM4100 [32]. Vid användning av en kloningsmaskin, till skillnad från en vanlig läsare, måste en knapp hållas intryckt vid läsning av en etikett och etikettens ID lagras i kloningsmaskinens minne. Kloningsmaskinen kan lagra hundratals olika ID för att senare kunna kopieras till en RFID etikett.

För någon som vill klona en EM4100-etikett och samtidigt har tillgång till rätt verktyg är det alltså kloningen en väldigt enkelt uppgift. Någon särskild kunskap behövs egentligen inte för att utföra ett kloningsangrepp mot EM4100-etiketter. Proxmark3 är inte det bästa valet för kloning av EM4100, dels på grund av det höga priset men även dels för att Proxmark3 är långsam vid läsning, se Tabell 1. Fördelen med Proxmark3 är att antennen kan bytas ut för att få något längre läsavstånd, men det kan kräva en hel del arbete för att lyckas konfigurera antennen rätt för att fungera bra. Billigare alternativ är de kloningsmaskiner som finns tillgängliga, som inte kräver någon dator för att utföra kopieringen. Det billigaste alternativet är dock en EM4100-läsare som även kan skriva till etiketter som är kompatibla med EM4100, men dessa kräver i många fall att de är kopplade till en dator. Vid läsning skrivs det lästa ID:t till en texteditor och detta kan sedan i ett senare skede användas för att använda ett program (tillhörande läsaren) för att skriva till en etikett som är kompatibel med EM4100. Läsningen av en etikett är så pass snabb att en läsning skulle kunna göra väldigt diskret, trots att angriparen måste komma nära för att utföra avläsningen. I det fall avläsningen måste vara möjlig på ett längre avstånd, kan en lång-avståndsläsare användas för att utläsa etikettens ID som fungerar på upp till 1m. Därefter, vid ett annat tillfälle, kan detta ID användas för att skriva till en ny etikett med en skrivare. En kommersiell läsare är dessutom enklare och snabbare att använda än Proxmark3 som är långsam eller en kloningsmaskin som kräver att en knapp hålls intryckt under inläsning. Figur 14 visar hur ett angrepp skulle kunna utföras för att skapa en klon av en EM4100-etikett, då etiketten först måste läsas av för att kunna ta reda på ett ID. För en jämförelse av olika verktyg som kan användas för att utföra en kloning av EM4100, se Bilaga B: Prisexempel för RFID-utrustning.

Tabell 1: Genomsnittlig tid för kontakt med etikett för att utföra en operation med Proxmark3.

	Genomsnittlig tid Proxmark3
Läsning av EM4100	4 sekunder
Skrivning till T5555	4 sekunder

Tabellen nedan sammanfattar kloningen av EM4100 med Proxmark3. Implementeringstiden inkluderar orientering av källkoden till Proxmark3, implementering av stand-alone läge och kloning av EM4100 till en T5555-etikett. För att en angripare ska kunna implementera detta krävs också viss

förkunskap. Tiden för förberedelser inkluderar hämtning av generell kunskap om RFID och detaljer kring EM4100 och T5555. Utöver detta inkluderas även tid för uppsättning av utvecklingsmiljöer och uppgradering av Proxmark3s operativsystem och firmware. Under utförandet av de förberedande stegen inför implementeringen är det mycket möjligt att stöta på diverse problem, så som inkompatibla drivrutiner eller fel version av källkod i Proxmark3.

Tabell 2

Implementeringstid	40 timmar + 40 timmar förberedelser	
Pris för utrustning	Proxmark3 LF antenn Klonetikett	$229 $59 $2
	Totalt	$290 (ca 2000 sek)
Begränsningar för att utföra kloningsangreppet med Proxmark3	Etikett inom 4cm från läsaren under 4 sekunder Inga andra störande RFID-etiketter inom läsavstånd	

3.3 Fallstudie 2: Kloning av Mifare Classic

Mifare Classic, ibland även kallad Mifare Standard, är en typ av kontaktlös smart card tillverkat av NXP Semiconductors. Mifare Classic är ett smart card av typen ISO 14443A och är därmed ett passivt och högfrekvent (13,56 MHz).

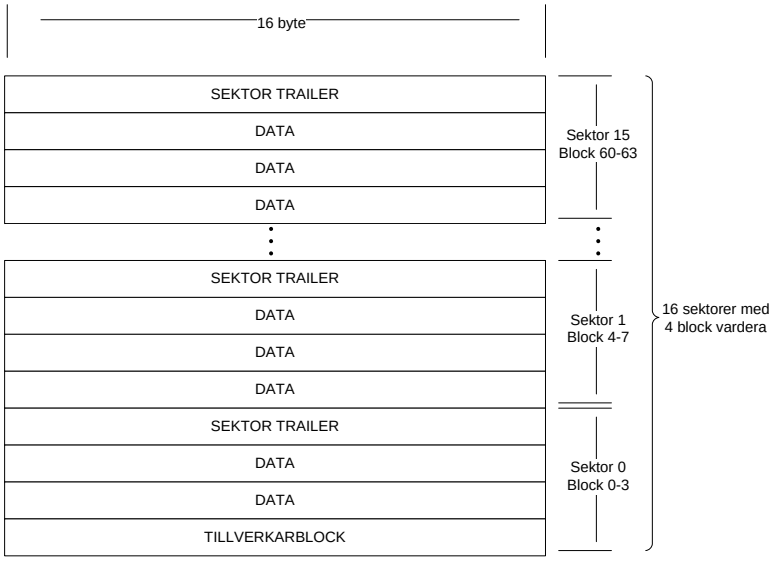
Mifare Classic används i ett flertal olika sammanhang, i inpasseringssystem, betalsystem och för biljetter för att nämna några. I Sverige finns resekortet AB (tidigare Resekortföreningen) som har skrivit RFK-specifikationen som har som mål att kunna använda samma resekort för att resa i hela Sverige. Resekort som följer RFK-specifikationen är baserade på Mifare Classic och flera av landets resekort idag är av denna typ.

3.3.1 Mifare Classic – Teknisk bakgrund

3.3.1.1 Minnesstruktur

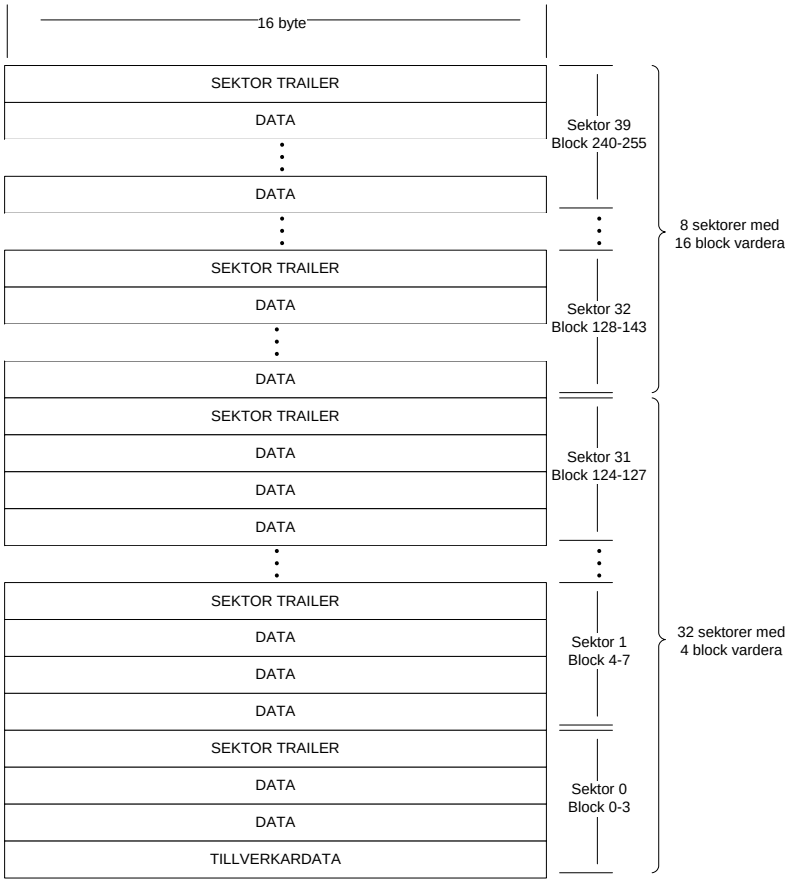
Mifare Classic finns i två versioner som har olika minneskapacitet, 1K och 4K, men deras funktionalitet är i övrigt densamma. Mifare Classic har ett EEPROM minne, vilket innebär att minnet är icke-flyktigt och modifierbart. Minnet är uppdelat i sektorer, som i sin tur är uppdelade i block. Varje sektor kan ha olika åtkomstvillkor och begränsningar för vilka operationer som är tillåtna att utföras på dess sektor-block.

Mifare Classic 1K har ett minne som består av totalt 1024 byte. Detta är uppdelat i 16 sektorer om 4 block, där varje block är 16 byte, se Figur 15.



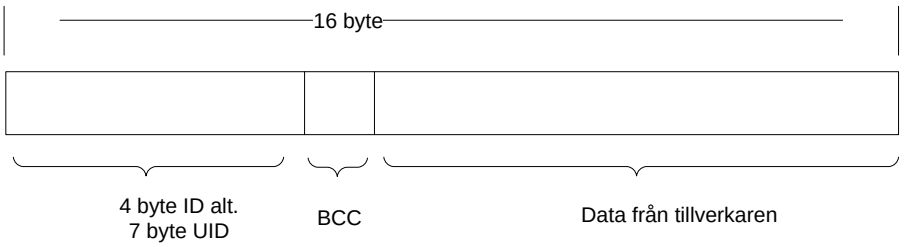
Figur 15: Mifare Classic 1K minnesstruktur.

Mifare Classic 4K har en större minneskapacitet, 4096 byte. Uppdelningen av minnet är något annorlunda, se Figur 16. Det är uppdelat i totalt 40 sektorer, varav de 32 lägsta sektorerna består av 4 block och de sista 8 sektorerna har 16 block vardera. Blocken är lika stora som i 1K versionen d.v.s. 16 byte.



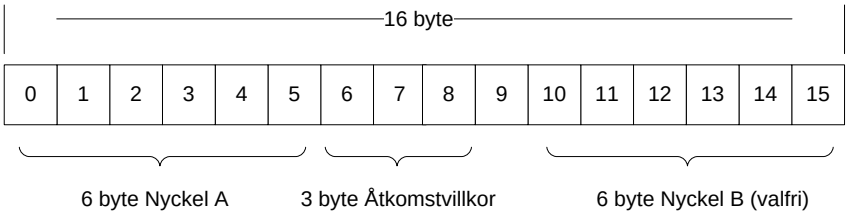
Figur 16: Mifare Classic 4K minnesstruktur.

Det finns tre typer av block: tillverkarblock, sektor trailer-block och datablock. Varje etikett har ett tillverkarblock i block 0, sektor 0, som består av data som skrivits av kretstillverkaren. Tillverkarblocket innehåller dels etikettens ID, vilket kan vara ett 4-byte långt ID eller ett 7-byte långt unikt ID, därefter följer en BCC (Bit Count Check, kontrollbit för ID) och resten är data om kretstillverkaren. Detta block är skrivskyddad och blir låst under tillverkningsproceduren, vilket innebär att det inte är möjligt att ändra en etiketts ID.



Figur 17: Tillverkarblocket i block 0, sektor 0.

Varje sektor har ett sektor trailer-block, som illustreras i Figur 18, det innehåller information som styr åtkomsten till sektorns datablock. Dels består den av minst en krypteringsnyckel (A) i byte 0-5 och eventuellt ytterligare en nyckel B i byte 10-15. Alternativt kan utrymmet för nyckel B användas för att lagra data. Byte 9 är oanvänd och kan användas för att lagra valfri data. Åtkomstvillkoren för sektorn definieras i byte 6, 7 och 8. Vid leverans är alla nycklar `ffffffffffff`.



Figur 18: Översikt av sektor trailer blocket, bestående av nycklar och åtkomstvillkor.

Åtkomstvillkoren beskriver vilka operationer som är tillåtna för varje block i sektorn som sektortrailerblocket tillhör och de anger även vilken nyckel (A eller B) som krävs för att utföra en viss operation. Möjliga operationer är läsning, skrivning, ökning, minskning, överför och återställ (namnen från operationerna anges i databladet för Mifare Classic [33]). Block kan även låsas genom att inte tillåta varken nyckel A eller B att utföra en eller flera operationer. Läsningen av åtkomstvillkor-blocket kan också ställas in och det kan inte läsas om inte rätt nyckel används för läsning, vilket förhindrar läsning av nycklarna för obehöriga. Inställningarna för sektorer med 4 block sätts blockvis, sektorer med 16 block är uppdelad i 4 grupper där varje grupp delar åtkomstvillkor. Se Bilaga A: Mifare Classic åtkomstvillkor för ytterligare detaljer om åtkomstvillkoren.

Datablocken kan förekomma i två varianter, antingen som läs- och skrivblock eller värdeblock. Vilken typ av block ett visst block är konfigureras i åtkomstvillkoren då de definieras av vilka operationer som är tillåtna på ett block. Läs och skrivblock är precis vad det låter som, block vars data kan läsas och skrivas (såvida det inte är låst). Värdeblock används då etiketten exempelvis ska användas som en elektronisk börs. Denna typ av block har en särskild struktur för att upptäcka eventuella fel som

kan ske under en transaktion genom att bl.a. använda olika kontrollbitar. Utöver detta används särskilda operationer som ser till att operationerna på blocken utförs säkrare genom att använda ett temporärt block. Operationerna öka värde i ett block, minska värde i ett block, återställ som flyttar värdet från ett block till ett temporärt dataregister och överför som flyttar innehållet i ett temporärt dataregister till ett block. Se Mifare Classic datablad för vidare information om dess minnesstruktur [33] [34].

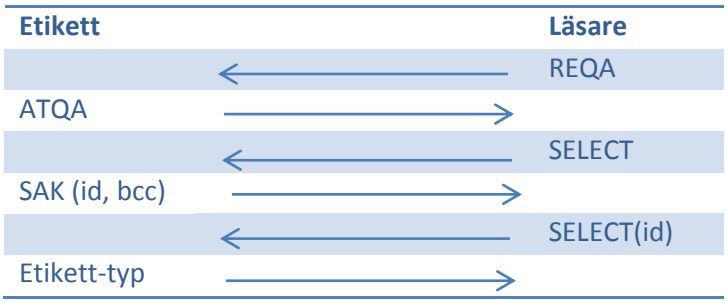
3.3.1.2 Dataöverföringsprotokoll

Mifare Classic följer standarden ISO 14443A för kontaktlösa kort. Standarden beskriver etikettens utformning, arbetsfrekvens, modulering och kodning av data, anti-kollisionsrutiner och kommunikationsprotokoll. Mifare Classic följer dock inte denna standard till fullo, då det finns vissa variationer i det kommunikationsprotokoll som används jämfört med standarden. Dessa små skillnader medför att systemet har brister som gör det möjligt att knäcka den kryptering som används.

3.3.1.3 Anti-kollision och autentiseringsprotokoll

Anti-kollisionsprotokollet som definieras i ISO 14443A förhindrar att en läsare kommunicerar med flera etiketter samtidigt när flera etiketter befinner sig i dess elektromagnetiska fält. Om det finns flera etiketter väljer läsaren ett utav dem, autentiserar sig och utför en operation på ett eller flera block. Därefter väljer läsaren nästa etikett i turordningen.

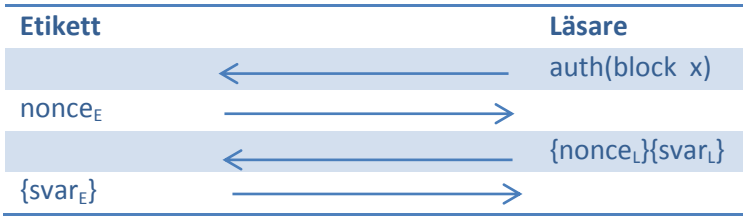
När en etikett kommer in i en läsares fält, hamnar den i ett väntande tillstånd när den blir strömsatt. Läsaren är den som initialiserar kommunikation mot en etikett och ser till att anti-kollisionsprotokollet följs. Detta förhindrar att två eller flera etiketter i läsarens fält stör varandra. Läsaren kommunicerar istället mot etiketterna en åt gången. Läsaren börjar kommunikationen genom att sända ett REQA (Request type A) eller ett WUPA (WakeUp type A) kommando för att kontrollera vilka etiketter som finns i området. Alla etiketter i området svarar på detta med ett ATQA (Answer To Request type A). Läsaren sänder därefter ett SELECT kommando och etiketterna svarar med (id, bcc), där bcc är en kontrollsumma. Efter att ha utfört anti-kollisionsalgoritmen väljer läsaren ett ID (en etikett) för att kommunicera med och skickar SELECT(id). Etiketten med det motsvarande ID avslutar anti-kollisionsfasen med att svara med en kod som beskriver vilken typ av etikett det är.



Figur 19: Anti-kollisionsprotokoll mellan etikett och läsare.

När en etikett har valts måste läsaren autentiseras för det block den vill utföra en operation på. Detta görs genom att utföra ett Challenge-Response-autentisering i en trestegshandskakning för att verifiera läsare och etikett. Det första steget är att läsaren sänder en förfrågan för att autentisera till ett visst block för att utföra en operation. Etiketten svarar med en *nonce,* en engångssiffra (nonce kommer från engelskans ”number used once”) som genererats av dess slumptalsgenerator som är en *challenge*. Under nästa fas i handskakningen skickar läsaren tillbaka ett svar till etikettens *challenge*

tillsammans med en nonce genererad av läsaren, som är krypterad med återkopplat strömchiffer CRYPTO1 (se avsnitt 3.3.1.3.1 för vidare beskrivning av CRYPTO1). För krypteringen används den nyckeln som krävs för åtkomst för den efterfrågade operationen på det block som angivits. Etiketten avslutar handskakningen genom att skicka sitt svar på läsarens *challenge nonce* krypterat med CRYPTO1 till läsaren. Figur 19 illustrerar denna autentiseringsprocess mellan en etikett och läsare.



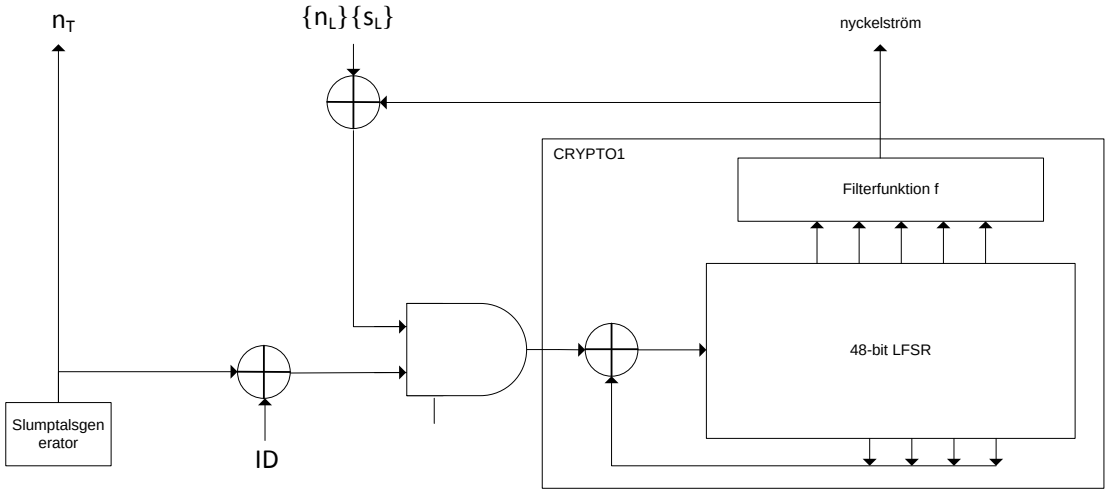
Figur 20: Autentisering för ett block, {} betyder att meddelandet är krypterat. L anger att läsaren har valt värdet och E anger att etiketten har valt värdet.

När autentiseringen är klar, kan läsaren utföra en önskad operation på etiketten och kommunikationen är krypterad. Om läsaren därefter vill autentisera till ett annat block för att utföra fler operationer, utförs denna autentiseringsprocess ytterligare en gång, men all kommunikation är krypterad.

3.3.1.3.1 Kryptering med CRYPTO1

Krypteringen som används av Mifare Classic är utvecklad av NXP Semiconductors och har fått namnet CRYPTO1. All kommunikation mellan en läsare och etikett är krypterad efter den första fasen i trevägshandskakningen under autentiseringen, som beskrivs i föregående avsnitt 3.3.1.3.

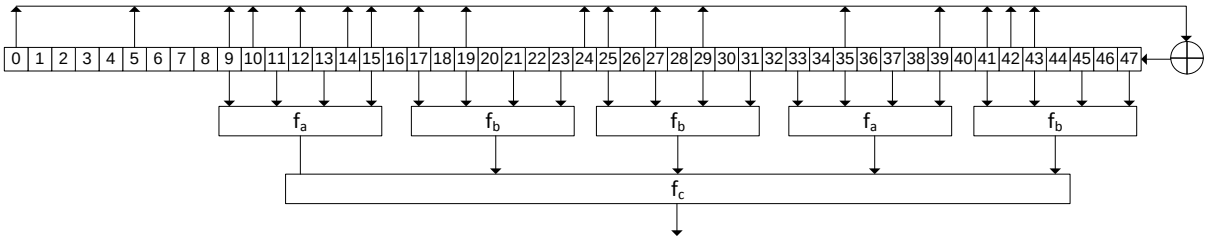
Den slumptalsgenerator som finns i Mifare Classic är en 16-bitars linjärt återkopplat skiftregister (eng. Linear Feedback Shift Register, förkortat LFSR) och producerar ett 32-bitar långt tal (nonce), som vid strömsättning initieras med samma initiala vektor (IV) varje gång. Vid varje klockpuls ändras innehållet i skiftregistret, genom att en bit skjuts ut och en bit skjuts in, som baseras på innehållet i skiftregistret. Totalt producerar slumptalsgeneratorn 65535 tal innan den börjar om efter 0,6 sekunder [35].



Figur 21: Överblick av CRYPTO1 och dess initiala tillstånd, figur baserad på illustration från [1]. ⊕ är en XOR operation som utförs för att kombinera två bitar.

CRYPTO1 är ett strömchiffer baserat på en 48-bitars linjärt återkopplat skiftregister och en filterfunktion *f*. I [8] beskrivs hur strömchiffret ser ut i sitt initiala skede vilket illustreras i Figur 21. Sektornyckeln för det block och den operation som efterfrågas av läsaren är den som finns inmatat i skiftregistret vid initialiseringen. Därefter kombineras det slumptal som genererats av etikettens slumptalsgenerator tillsammans med etikettens ID in i skiftregistret, under de första 32 klockpulserna. Sist matas läsarens nonce in i skiftregistret och därefter används den feedback-bit som beräknas vid varje klockpuls.

För att producera nyckelströmmen, matas 20 bitar av skiftregistret in i filterfunktionen *f* vid varje klockpuls och producerar en bit av nyckelströmmen. Denna bit används för att kryptera en bit av meddelandet: meddelandebit XOR nyckelströmbit. Innehållet i skiftregistret skjuts sedan en bit åt sidan och en ny bit läggs till som baseras på några av de bitar som finns där (återkopplingen), se Figur 22 nedan, vidare detaljer om filterfunktionen finns beskrivna i [8].



Figur 22: Bilden illustrerar CRYPTO1. En 48-bitars återkopplat skiftregister i kombination med filterfunktionen f producerar vid varje klockpuls en bit av nyckelströmmen. Varje bit i skiftregistret flyttas ett steg och återkopplingen producerar en ny bit som placeras i registret. Baserad på illustration från [8].

Vidare detaljer om hur CRYPTO1 fungerar och detaljer om orsaken till bristerna kan läsas om i [2] [8] [1], eftersom dessa inte är detaljer som har varit direkt nödvändiga att ta hänsyn till i detta arbete.

3.3.1.3.2 Brister i Mifare Classic

Mifare Classic har ett flertal brister som gör det möjligt att knäcka de nycklar som används för att kryptera data. Dels följer inte kommunikationsprotokollet ISO 14443A då vissa delar inte krypteras på korrekt sätt, dessutom är slumptalsgeneratorn som etiketterna använder förutsägbar.

Slumptalsgeneratorn, ett 16-bitars LFSR som producerar ett 32-bitar långt tal (nonce), initialiseras med samma initiala vektor varje gång när etiketten får ström. Därefter ändras innehållet i skiftregistret i ett förutsägbart mönster vid varje klockpuls och efter ett visst antal klockpulser börjar den om och producerar samma sekvens av slumptal. Detta leder till att varje gång etiketten får ström produceras samma sekvens av ”slumptal” och det är möjligt att få etiketten att skicka samma nonce genom att vänta samma tid t efter varje strömåterställning. Ett alternativt sätt att få samma slumptal gång på gång är att vänta exakt 0,6 sekunder och slumptalsgeneratorn producerar samma tal igen. Denna brist i slumptalsgeneratorn utnyttjas för att utföra ett angrepp. Detta var en av de första bristerna som upptäcktes och beskrivs i [35].

Utöver en svag slumptalsgenerator, finns det brister i kommunikationsprotokollet. Kryptering av paritetsbitar görs med samma del av nyckel som nästkommande databit i meddelandet, vilket alltså läcker information om krypteringsnyckeln som använts. Dessutom, när etiketten tar emot ett meddelande under autentiseringen som innehåller en eller flera inkorrekta paritetsbitar svarar den

inte. Däremot om alla paritetsbitar är korrekta, men svaret är fel, svarar etiketten med ett krypterat NACK, som i klartext är 0x05 och på så sätt kan man utföra ett known-plaintext-angrepp [8].

Bristerna i slumptalsgeneratorn och kommunikationsprotokollet i kombination med detaljerad kunskap om CRYPTO1 gör det möjligt att knäcka alla nycklar för en Mifare Classic etikett. CRYPTO1 är också uppbyggt på ett sådant sätt att det är möjligt att med viss information beräkna innehållet i skiftregistret vid en tidigare tidpunkt. Ett flertal card-only angrepp har presenterats som utnyttjar bristerna på olika sätt. I [8] presenteras fyra olika angrepp. Det första angreppet som presenteras i rapporten är ett Brute Force-angrepp som använder sig av den information som paritetsbitarna läcker. Två angrepp fixerar slumptalen, det vill säga flera anrop utförs med samma nonce. Det första håller etikettens nonce fixerad genom att stänga av och på läsarens magnetfält så att etiketten producerar samma nonce och en annan då läsarens skickar samma nonce vid varje autentiseringsförsök, som helt kontrolleras av angriparen. Det sista angreppet, som används i detta arbete, kallas ett ”nästlat” angrepp. Detta angrepp knäcker fler nycklar efter att en nyckel har hittats och utnyttjar bristerna i slumptalsgeneratorn. I korthet beräknas skillnaden av två nonce som etiketten skickar under två autentiseringsförsök efter varandra. Tillsammans med information som paritetsbitarna i etikettens nonce läcker, är det möjligt att beräkna den krypteringsnyckel som har använts. Angreppet för att hitta en nyckel har sedan förbättrats och förfinats. Angreppet som publicerats i [9] är snabbare och kräver mindre minne och är det angrepp som används i detta arbete för att hitta en första nyckel. Detta angrepp utförs genom att utföra ett flertal autentiseringsförsök, där etikettens nonce hålls fixerad (etiketten skickar samma nonce varje gång). I autentiseringsprocessens andra fas, när läsaren skickar ett krypterat svar, varieras paritetsbitarna som läsaren skickar för att etiketten ska svara med ett krypterat NACK. Då är paritetsbitarna i svaret korrekt, men svaret är fel. När tillräckligt mycket information har samlats ihop från de krypterade NACK-svaren är det möjligt att beräkna den nyckel som har använts till krypteringen.

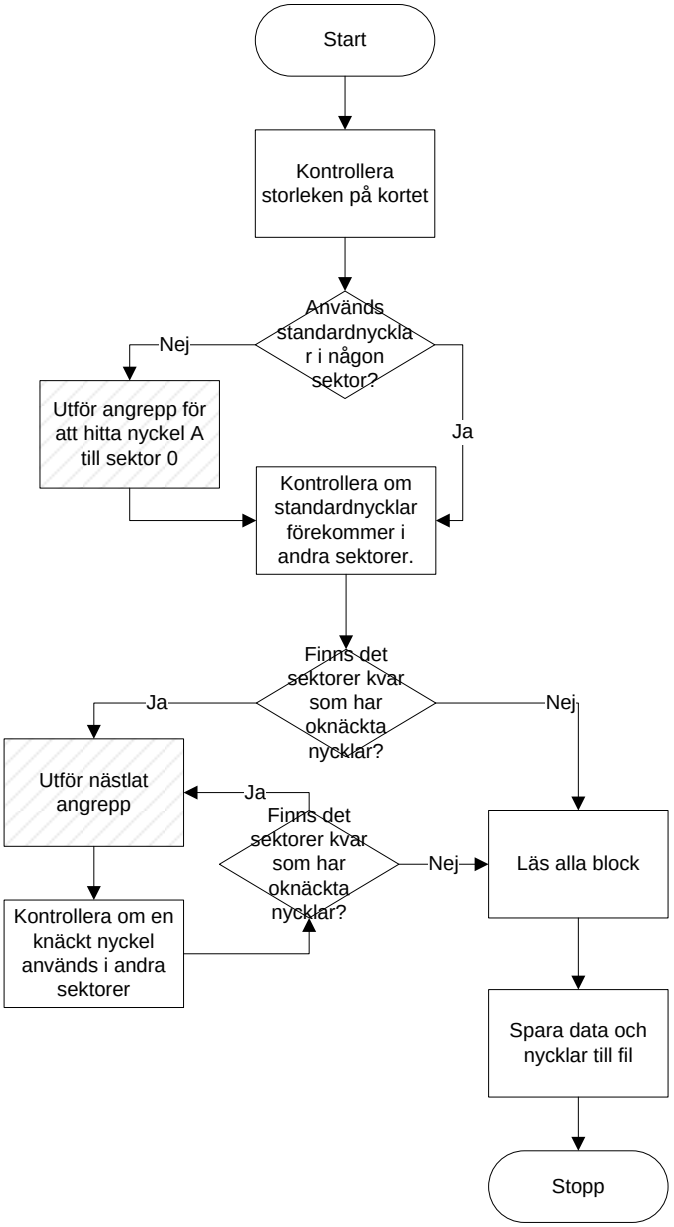
3.3.2 Genomförande

Att klona en etikett går ut på att kopiera allt innehåll, både inställningar och data, från en etikett till en annan. För att kunna klona en etikett måste det vara möjligt att läsa allt innehåll på den etikett som ska klonas. Om nycklarna är kända är detta en enkel uppgift då det endast kräver en läsning, men annars måste nycklarna knäckas. Bristerna som beskrivits i tidigare avsnitt finns implementerade i några olika toolkits och kodbibliotek som kan användas för knäckning av Mifare Classic nycklar[6]. Ett av dessa kodbibliotek, CRAPTO1[7], finns implementerad i Proxmark3s källkod.

Det finns två möjliga sätt att utvinna nycklar, det första är att lyssna på en kommunikationssession och sedan i efterhand knäcka nycklar. Genom avlyssning avslöjas inte all information på etiketten, utan bara det som har skickats under kommunikationen och inte allt data på etiketten. För att få ut allt måste en etikett skimmas för att utvinna all data på etiketten, vilket inkluderar samtliga nycklar (både nyckel A och B i varje sektor!) och innehållet i alla block (tillverkarblocket, datablock och sektor trailer-block). De angrepp som verifieras i detta arbete utför därför ett card-only angrepp som utvinner all information på en etikett för att skapa en klon.

[6] MFCUK: http://code.google.com/p/mfcuk/, CRAPTO: http://code.google.com/p/crapto1/, LIBNFC: http://www.libnfc.org/
[7] CRAPTO1 - http://code.google.com/p/crapto1/

Sedan tidigare har klienten och operativsystemet till Proxmark3 stöd för att utföra angrepp för att knäcka nycklar som används på en Mifare Classic-etikett. Angreppet är uppdelat i två delar, den första för att knäcka en första nyckel och sedan ett angrepp för att knäcka resterande nycklar. Implementationen för att knäcka en nyckel baseras på det angrepp som Nicolas T. Courtous presenterar i sin artikel ”The Dark Side of Security by Obscurity” [9]. Denna implementation försöker knäcka nyckel A till sektor 0 genom att hålla etikettens nonce fixerad, som är möjlig då slumptalsgeneratorn på etiketten är förutsägbar (se avsnitt 3.3.1.3.2). Angreppet utförs genom att samla information från de krypterade NACK-svar som etiketten skickar då läsaren skickar ett krypterat svar där alla paritetsbitar är korrekta under den andra fasen i autentiseringen (se avsnitt 3.3.1.3). Genom att samla data från etikettens svar ett visst antal gånger har tillräckligt med data samlats ihop för att kunna beräkna den hemliga nyckeln för en sektor, den nyckel som räknas ut stämmer dock inte varje gång. Om den nyckeln som räknas ut inte är korrekt upprepas angreppet igen, tills en korrekt nyckel har hittats. För att hålla den timing som krävs för att etiketten ska sända samma nonce under flera autentiseringsförsök, stängs läsarens antenn av och på för att nollställa etikettens slumptalsgenerator, sedan skickas autentiseringskommandot. Med Proxmark3 är inte tiden mellan påslagning av antennen och kommandots utskick precis vid varje försök, vilket leder till att etikettens nonce inte är samma vid varje anrop. Proxmark3 lyckas fixera etikettens nonce vid i genomsnitt vid var tredje försök. Nästa steg är att hitta alla andra nycklar som används på etiketten, detta görs med det nästlade angreppet som presenteras som det fjärde angreppet i ”Wirelessly Pickpocketing a Mifare Classic Card” [8]. Det nästlade angreppet är också implementerad i Proxmark3 sedan tidigare, för detaljer om hur angreppet utförs, se [8]. I korthet utnyttjar angreppet det faktum att slumptalsgeneratorn är förutsägbar och information som paritetsbitar läcker. Först autentiseras läsaren till en sektor, där nyckeln är känd, och därefter till en annan sektor, med krypterat autentiseringskommando (som beskrivs i 3.3.1.3 Anti-kollision och autentiseringsprotokoll). Genom att autentisera till två sektorer i följd är det, utifrån den nonce som etiketten skickar, möjligt att beräkna vilken nyckel som har använts för kryptering. Implementationen av angreppen är baserade på de vetenskapliga artiklar som nämnts. För en angripare kan några små ändringar göras för att effektivisera angreppen och förhindra att utföra onödiga operationer. Dessa har implementerats i detta arbete och presenteras nedan.

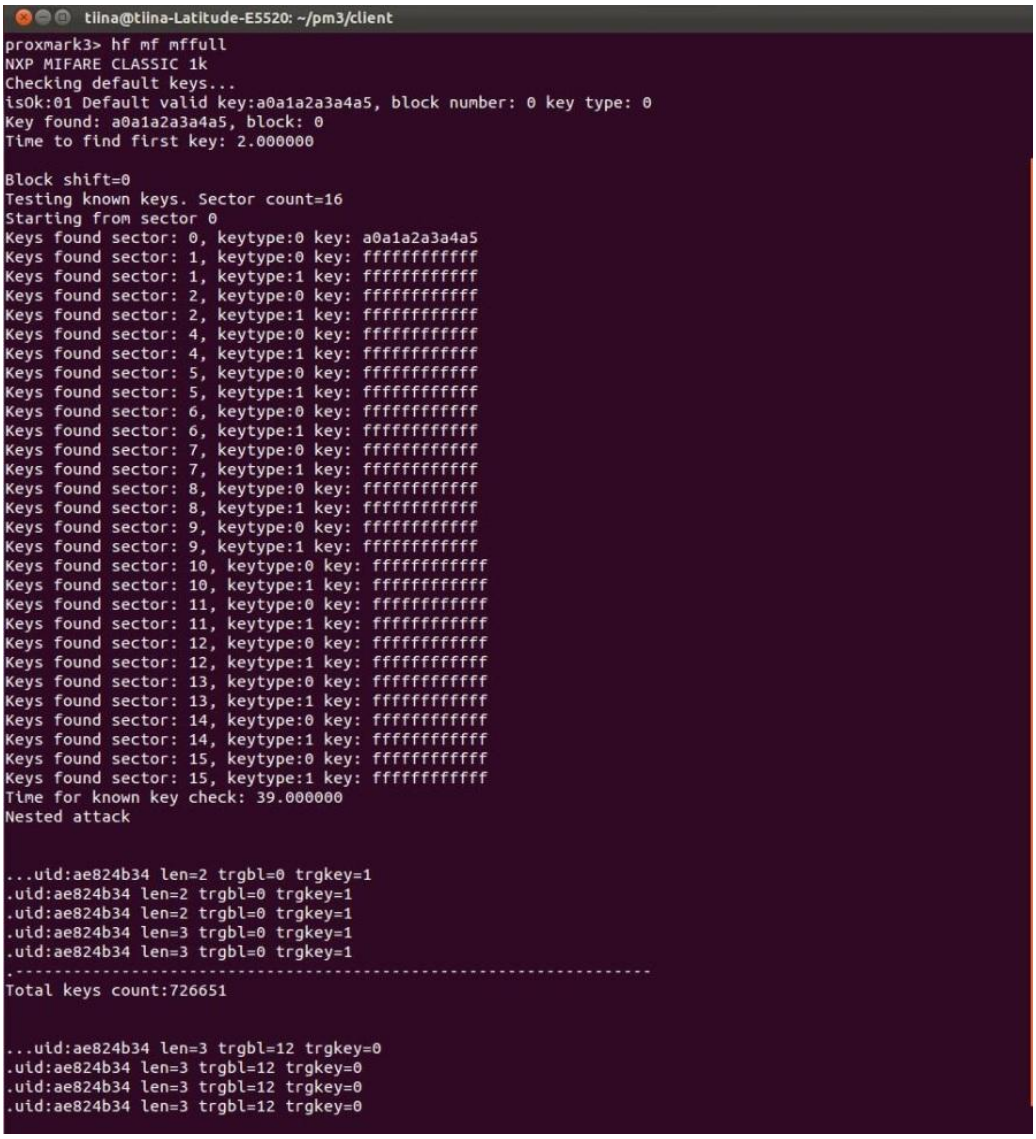


Figur 23: Flödesdiagram som visar implementationen av angreppet, de markerade rutorna är angrepps-funktioner som fanns i Proxmark3 sedan tidigare.

Det första steget för att utföra ett fullständigt kloningsangrepp är att detektera om etiketten är av typen 1K eller 4K. Detta är viktigt för att rätt antal nycklar blir knäckta och att alla block sedan blir lästa för att få ut all data på en etikett. Standardnycklar är nycklar som ges som exempel i datablad som NXP tillhandahåller[8] . Försök i detta arbete, och andras, har visat att standardnycklar många gånger är i bruk på etiketter, särskilt i sektorer som inte innehåller något data. Angreppet för att hitta en första nyckel som finns implementerad är eventuellt inte nödvändig att genomföra om en standardnyckel används i någon sektor. Inte förrän efter en kontroll av standardnycklar misslyckas utförs angreppet för att hitta en första nyckel. Den nyckel som har hittats, antingen genom kontrollen av standardnycklar eller som resultat av angreppet, används sedan till att utföra det nästlade angreppet. Innan det nästlade angreppet utförs kontrolleras om det finns några sektorer

[8] Dessa är inte tillgängliga för allmänheten, men information om nycklarna har sammanställts online: http://code.google.com/p/mfcuk/wiki/MifareClassicDefaultKeys

som fortfarande har nycklar som är okända efter kontrollen av standardnycklar. Om det finns okända nycklar kvar, utförs det nästlade angreppet, tills alla nycklar har hittats. Varje gång en ny nyckel knäcks kontrolleras om nyckeln används i andra sektorer också, för att eventuellt minska antalet angrepp som utförs.



Figur 24: Skärmdump av programmet som utför angrepp för kloning. Här ser vi att kortet är Mifare Classic 1K och den första nyckeln (block 0, key type 0 (A)) är `a0a1a2a3a4a5`. Sedan fortsätter kontrollen av standardnycklar och många nycklar är `ffffffffffff`, därefter börjar det nästlade angreppet att utföras.

När alla nycklar är kända måste all data på etiketten läsas för att sedan kunna göra en klon. För att kunna använda informationen i ett senare skede skrivs innehållet från alla block på en fil, även sektorblock med ifyllda nycklar. Normalt skrivs dessa inte ut när sektor trailer-blocket läses från en etikett (de visas då som nollor). Det som har sparats till en fil kan i ett senare skede användas för att skrivas till en ny etikett eller användas för att emulera en etikett med Proxmark3 för att skapa en klon. Den största utmaningen vid kloning här är att skriva till en ny etikett. Att skapa en klon innebär att det inte är någon skillnad på två etiketter. Detta är inte möjligt att göra med original Mifare Classic-etiketter eftersom tillverkarblocket (block 0) inte går att skriva till för att två etiketter inte skall kunna få samma ID. Det kan finnas en mycket, mycket liten möjlighet att hitta en etikett som

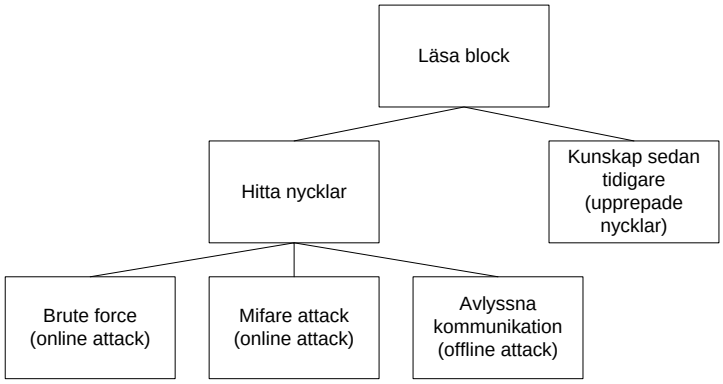
har samma 4-byte ID, då dessa inte är garanterat unika [36]. Men att använda en original Mifare Classic-etikett är inte den enda möjligheten för att skapa en klon, det finns etiketter som liknar Mifare Classic till beteende och utformning tillgängliga på marknaden. Dessa etiketter har dessutom ett skrivbart tillverkarblock, vilket gör det möjligt att göra en exakt klon. Under detta arbete har bara etiketter hittats i 1K format. Etiketternas kvalitet varierar mellan olika tillverkare. Vissa av dessa etiketter saknar slumptalsgenerator alls, vilket innebär att samma nonce genereras hela tiden. De ”klonetiketter” (hädanefter kallas en sådan etikett för klonetikett för att separera från original Mifare Classic-etiketter) som har använts under dessa försök är inte helt felfria, se jämförelse av klonetikett och en original Mifare Classic-etikett i 7.3Bilaga C: Avlyssning av kommunikation - jämförelse av Mifare Classic Originaletikett och Klonetikett.

3.3.3 Analys och diskussion

Fyra steg krävs för att göra en klon av en etikett:

1. Hitta en första nyckel
2. Utifrån den första nyckeln hitta resterande nycklar
3. Läsa av allt blockinnehåll och spara tillsammans med nycklar till varje sektor
4. Skriva allt innehåll till en ny etikett

Att komma åt all data som en etikett innehåller är det viktigaste för att göra en klon. Figur 25 visar alternativa sätt att hitta en nyckel för att läsa ett block. De data som lästs kan sedan användas med en emulator, skrivas till en annan etikett eller en klonetikett. De olika typerna av ”kloner” har sina fördelar och nackdelar. En emulator kan vara svår att gömma och lura någon att tro att det är en äkta etikett medan en annan Mifare Classic-etikett inte kan ha samma ID. En klonetikett kan ha vissa variationer i hur den fungerar, jämfört med en original Mifare Classic etikett. Den typen av klonetikett som använts i detta arbete har svarat på ett kommando som original-etiketten inte svarade på (se Bilaga C: Avlyssning av kommunikation - jämförelse av Mifare Classic Originaletikett och Klonetikett). Dessutom är tillgången av klonetiketter begränsad, de finns bara i 1K versionen som har kort-format i skrivande stund.



Figur 25: Attackträd för att läsa ett block på en etikett.

För att utföra ett angrepp är tiden som det tar att klona ett kort en viktig faktor för angriparen. Med en optimerad hårdvarukonfiguration, dator och kod i likhet med den som har använts av forskarna på Radbounds Universitet i [8] skulle angreppen kunna utföras mycket snabbt. Att hitta en första nyckel med angreppet i [9] som finns implementerad i Proxmark3 skulle det ta ungefär 10 sekunder. Att finna resten skulle ta ungefär 1 sekund per sektor under det nästlade angreppet. Det bör noteras att

denna optimerade implementation är utvecklad av fyra forskare inom området som ytterligare har fått hjälp av andra specialister. De beskriver inte i rapporten vad de har för systemspecifikation på den dator som utför angreppet eller andra detaljer, men de nämner att de har använt Proxmark3. Den implementation av angreppen som finns öppet tillgänglig till Proxmark3 är inte samma version som använts under deras försök [8] och för att någon skulle lyckas konfigurera verktyget på ett liknande sätt och uppnå denna hastighet och effektivitet behövs någon med stor kunskap inom inbyggda system och signalhantering för att skriva om koden.

Tiden för att utföra de olika delarna av angreppet under detta arbetes försök med Proxmark3 har varit betydligt längre än de som Radbounds forskare uppnådde. Som tidigare nämnts, lyckas Proxmark3 inte med att utföra den precisa kontrollen av timingen för att producera samma nonce vid varje försök. Fixeringen av noncen krävs för att utföra angreppet för att hitta en första nyckel och samma nonce produceras i genomsnitt vid var tredje försök med Proxmark3. Eftersom denna timing är samma vid varje försök (tiden mellan påslagning av det elektromagnetiska fältet och kommandon som skickas) blir samma nonce fixerad vid upprepade försök med samma etikett. Ibland händer det att det är en annan nonce som fixeras då anropet fördröjdes något och leder sedan till att försök att återupprepa noncen igen blir svårare. Detta medför att det krävs fler autentiseringsförsök innan samma nonce produceras igen. Dessutom klarar Proxmark3 bara ungefär fyra autentiseringsförsök per sekund. Så länge Proxmark3 inte hamnar i ”ofas” lyckas den oftast hitta den första nyckeln efter ca 30-60 sekunder, annars är det väldigt svårt att förutse hur lång tid det tar. 50 försök visade att i det snabbaste fallet hittades en nyckel på 14 sekunder, men den långsammaste tog hela 427 sekunder, den genomsnittliga tiden blev 86 sekunder. Detta angrepp är endast nödvändigt då det inte finns någon standardnyckel. Genom att först kontrollera efter standardnycklar så kan angreppstiden förkortas. I det fall ingen sektor använder standardnycklar, innebär dock kontrollen av standardnycklar att angreppet tar längre tid. Eftersom dessa många gånger används i praktiska tillämpningar är det dock värt att kontrollera dem först.

För att hitta resten av nycklarna används det nästlade angreppet, som enligt rapporten [8] kan knäcka en nyckel på under en sekund. Den rapporterade tiden skiljer sig stort från det som Proxmark3 lyckas med. Här är förutsägbarheten av slumptalsgeneratorn en viktig del av angreppet, men slumptalet fixeras inte på det sättet som i angreppet för att hitta en nyckel. Istället är skillnaden mellan de två kort-nonce som läsaren tar emot från två olika autentiseringsförsök en viktig del. Det första steget är att samla ihop tillräckligt med information och därefter ska olika tabeller byggas baserat på den informationen som har utvunnits. Att samla ihop tillräckligt med information tar flera sekunder och att bygga tabellerna som behövs tar också några sekunder. Dessutom hittas inte en nyckel vid varje försök av det nästlade angreppet. Ibland måste angreppet upprepas för samma sektorer flera gången för att hitta en nyckel.

Tabell 3 presenterar genomsnittlig tid för olika delar av angreppet för den implementation av Proxmark3 som har använts i detta arbete och visar en jämförelse mot tiderna som rapporterats i [8] och [9]. Det är bristerna i slumptalsgeneratorn som utnyttjas i båda angreppen. Tidsskillnaden beror till stor del på hur väl Proxmark3 lyckas fixera kortets nonce men även hur många anrop till kortet den kan göra under en viss tid. Det är värt att uppmärksamma att Proxmark3 klarar 4 transaktioner (t.ex. autentiseringsförsök) per sekund med den konfiguration som använts i dessa försök. Detta kan sedan jämföras med cirka 30 transaktioner per sekund med den konfiguration av Proxmark3 som använts i [8].

Tabell 3: Genomsnittlig tid under försök för några olika operationer som används under kloningsangreppet och jämförelse med tider som har presenterats i rapporter.

	Tid under försök	Tid enligt rapporter
Knäcka en första nyckel	86 sekunder	10 sekunder
Knäcka en nyckel (nästlad)	51 sekunder	<1 sekund
Kontroll 5 standardnycklar	2 sekunder/sektor (a och b)	-
Läsa ett block	0,5 sekunder	-

Med informationen som samlats ihop för hur lång tid olika operationer tar är det möjligt att beräkna ungefärlig tid för ett angrepp, i bästa och värsta fall då angriparen inte har tidigare kunskap om etikettens nycklar. Tiderna presenteras som ett genomsnitt, då ett värsta fall är väldigt svårt att resonera kring då Proxmark3 kan har svårt att lyckas få en nonce att upprepas och det inte finns någon maxtid för det. Angriparen saknar också kunskap om etikettens storlek, men båda 1K och 4K versionerna presenteras i tabellen nedan, då tiderna för att utföra ett angrepp kan variera stort mellan dem. I det bästa fallet är alla nycklar standardnycklar vilket kontrasterar det värsta fallet, där inga standardnycklar används och alla måste knäckas. Se Tabell 4 för en jämförelse av tidsåtgången för att knäcka nycklar i de olika fallen och en jämförelse mot den tid som rapporteras i [9] [8].

Tabell 4: Jämförelse av tidsåtgång av angrepp för att hitta nycklar för Mifare Classic 1K- respektive 4K-etiketter. Observera att värsta fall innebär använder genomsnittlig tid för att knäcka en nyckel och att alla nycklar är satta.

	Bästa fall		Värsta fall		Tid enligt rapporter	
	1K	4K	1K	4K	1K	4K
Kontrollera	16 * 2s	40 * 2s	16 * 2s	40 * 2s	-	
Första nyckeln	-	-	86s	86s	10s	10s
Resten av nycklarna	-	-	31 * 51s	79 * 51s	31 * 1s	79 * 1s
Totalt	= 32s	= 80s	≈ 28 min	≈ 70 min	= 41s	= 89s

När alla nycklar har hittats är nästa steg att läsa alla block. Proxmark3 är inte snabb på att utföra läsoperationen, vilket tar runt 32 sekunder att läsa alla block på en 1K etikett och 128 sekunder att läsa alla block om det är en 4K etikett. Fram till och med detta steg måste angriparen ha tillgång till etiketten och inte förrän efter läsningen är genomförd är det möjligt att skapa en klon.

När all data från en etikett är sparad, behövs bara en bärare dit informationen kan skrivas till för att skapa en klon. Som tidigare nämnts, kan bäraren vara en emulator, en original Mifare Classic-etikett eller en klonetikett. Vad som passar bäst beror på det bakomliggande systemet, om det kontrollerar att etikettens ID stämmer, kan bara en emulator eller en klonetikett användas, annars kan en vanlig Mifare Classic-etikett användas.

Ett stort problem för att utföra ett angrepp om någon har etiketten i exempelvis fickan, är att lyckas hålla läsarantennen tillräckligt nära. Angreppet är inte pålitligt när läsaren inte kan nå etiketten under hela angreppets gång. När angreppet utförs med Proxmark3 måste antennen vara mindre än 4 cm från etiketten för att kunna kommunicera med det. Om etiketten inte svarar på läsarens samlas inte tillräckligt med data ihop för angreppet. Det kan leda till att en del i angreppet misslyckas och hela angreppet tar längre tid att slutföra. Detta medför att en mycket viktig del i analysen är på hur långt avstånd som angreppet kan genomföras. Avläsningsavståndet är ingenting som har undersökts

närmare praktiskt i detta arbete. Däremot har just detta undersökts i en annan rapport, där har skimningsangrepp utförts mot ISO 14443A etiketter, den standard som Mifare Classic tillhör. Resultaten som presenteras i denna rapport, ”Practical Eavesdropping and Skimming Attacks on High-Frequency RFID tokens” [10], visar att med en antenn som är 14,8x21cm stor kan strömsätta, skicka och ta emot signaler från en ISO 14443A etikett på 15-20 cm avstånd. Skillnaden är inte stor från det maximala avståndet som beskrivs i Mifare Classics datablad [33] [34], som är 10 cm. Avståndet kan dock anses vara tillräckligt för att ha all utrustning i en väska för att kunna utföra ett angrepp utan att någon märker det.

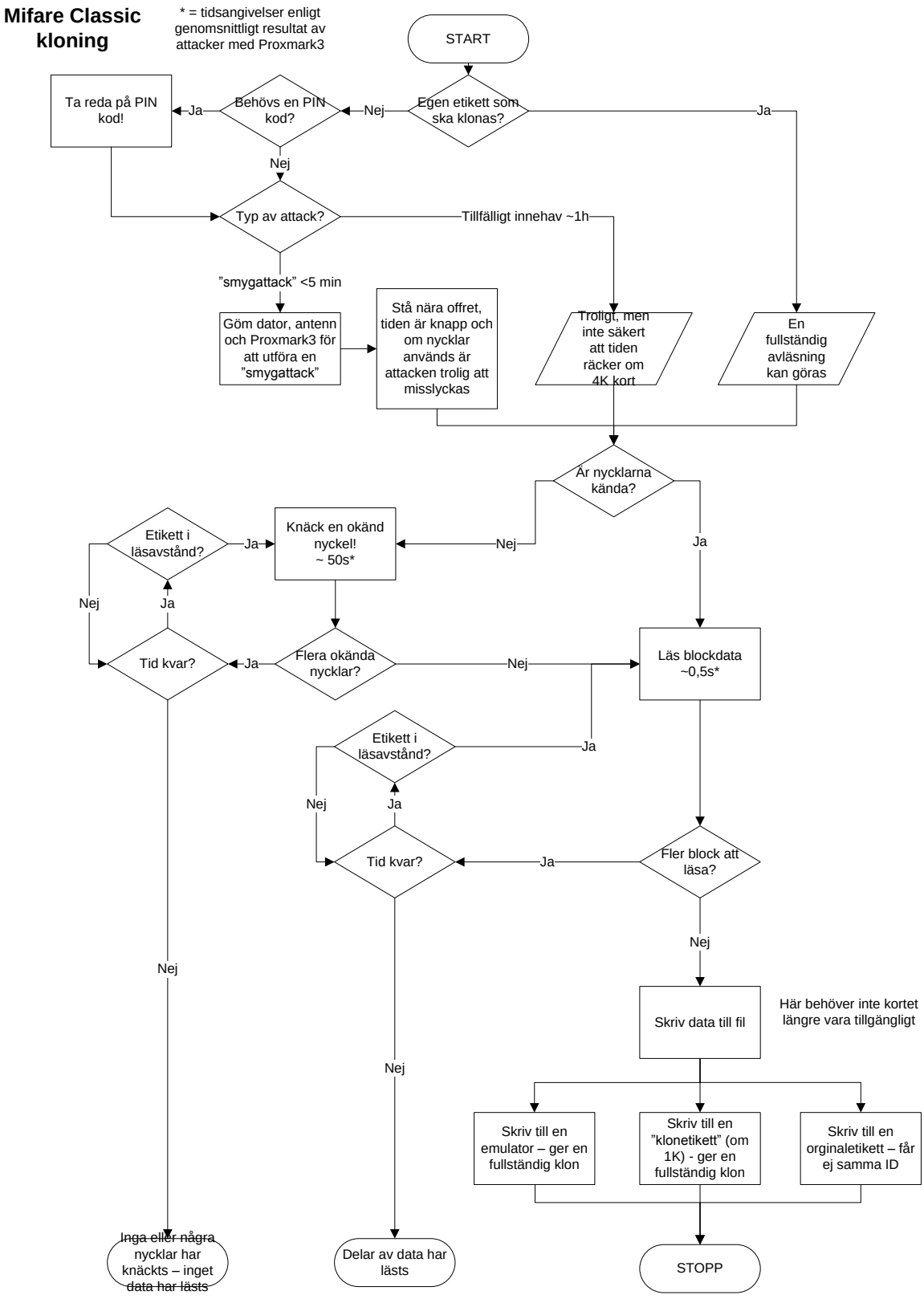
Ett kloningsangrepp kan utföras på ett flertal sätt, beroende av *vems* etikett som ska klonas och vilka andra säkerhetsmekanismer dess bakomliggande system innehar. En angripare kan tänkas utföra ett angrepp medan offret står på tunnelbanan, då är tiden för angreppet mycket begränsad, dessutom kan det vara svårt att skimma etiketten på ett diskret sätt och samtidigt hålla sig tillräckligt nära. Ett annat scenario är då ägaren av etiketten har gått på lunch och lämnat sin Mifare Classic-etikett på kontoret och en angripare har något längre tid att utföra angreppet och detta behövs inte göras lika diskret. Det tredje scenariot är att det är en etikett som angriparen själv innehar som ska klonas, då finns ingen tidsbegränsning eller diskretionskrav. En angripare kan också ha tidigare kunskap om systemet, till exempel om alla etiketter har samma nycklar, då finns förkunskap om systemet och ett angrepp kan göras väldigt fort. Andra skyddsmekanismer för ett system kan vara är exempelvis en PIN-kod eller att etikettens ID används av systemet för identifiering. Dessa exempel på skyddsmekanismer begränsar möjligheterna för en lyckad kloning ytterligare. Figur 26 visar hur ett kloningsangrepp skulle kunna tänkas gå till väga och vilka begränsningar som kan finnas vid utförandet.

Proxmark3 är inte det enda verktyget som kan utföra angrepp för att knäcka nycklar till Mifare Classic-etiketter. Det finns andra Mifare Classic kompatibla läsare som kan användas så länge det är möjligt att kontrollera vilka paritetsbitar som skickas och en del kan kontrollera timingen för att upprepa noncen ännu bättre. Angreppen finns implementerade i open source bibliotek[9], och två enheter som kan användas för att utföra dessa angrepp är Touchatag[10] som är en NFC läsare, och OpenPCD[11] som är en RFID verktyg, i likhet med Proxmark3. Ytterligare information om dessa finns i 7.2 Bilaga B: Prisexempel för RFID-utrustning.

Sammanfattningsvis, för ett angrepp med Proxmark3 då angriparen inte har förkunskap om nycklarna, krävs minst en minut för att läsa allt data i det bästa fallet vilket förutsätter att det är en Mifare Classic 1K etikett som endast använder standardnycklar. I det värsta fallet, för en angripare, är att etiketten är en Mifare Classic 4K där alla nycklar är olika. Då tar angreppet i genomsnitt runt en timme. Källkoden som finns att ladda ner till Proxmark3 (SVN version 526) är inte optimerad för att utföra dessa angrepp i kloningssyfte utan kan betraktas mer som ett ”proof of concept”. Dessutom utförs inte angreppen mot 4K etiketter på ett bra sätt, dels saknas en funktionalitet för att skriva till 4K kort och ingen hänsyn tas till att minnesstrukturen är annorlunda när angreppet utförs. Skillnaden mellan 1K och 4K etiketter är hur många sektorer som finns och hur många block av data de innehåller, men utöver detta så är angreppsmetoderna likvärdiga. Med några förbättringar kan angreppet utföras på det vis som har beskrivits i denna rapport, som med ett kommando i Proxmark3

[9] Libnfc: http://www.libnfc.org
[10] Touchatag: http://www.touchatag.com/
[11] OpenPCD: http://www.openpcd.org/

klienten kan utföra ett kloningsangrepp på det sätt som visas i Figur 23: Flödesdiagram som visar implementationen av angreppet.



Figur 26: Flödesdiagram över ett kloningsangrepp mot Mifare Classic.

Implementeringstiden för att utöka Proxmark3 till att kunna utföra ett fullständigt kloningsangrepp mot Mifare Classic 1K och 4K tog ungefär 80 timmar effektiv tid. Innan en angripare kan implementera och utföra ett angrepp krävs en hel del förberedande arbete och förkunskap, som tar ungefär lika lång tid att samla ihop som att utföra implementeringen. Dels behövs generell kunskap om RFID för att förstå angreppets grundläggande principer men även vilka verktyg som kan användas för att utföra ett kloningsangrepp mot Mifare Classic. Även kunskap om hur Mifare Classic 1K och 4K fungerar och vilka skillnader de har, information om klonetiketter och även antennens funktionalitet är viktiga för en angripare. Förutom att samla ihop förkunskap, kan man stöta på en del bekymmer vid uppsättning av arbetsmiljöer och uppgradering av Proxmark3s operativsystem och firmware. Tabellen nedan sammanfattar arbetet av kloningsförsök, det visar vilka resurser som skulle krävas för att återskapa det som har gjorts i denna rapport. Implementeringstiden innefattar orientering i den befintliga koden, utökning för kloning av 4K etiketter samt implementation av ett kommando i klienten för att knäcka alla nycklar, läsa alla block och skriva allt data som har lästs till en fil. Ett stort problem som implementationen av det kompletta angreppet har är att den försöker knäcka samtliga nycklar, både A och B, för varje sektor. Det innebär att om utrymmet i sektor trailer-blocket för nyckel B bara används för data kommer inte angreppet att lyckas, då den försöker knäcka den nyckeln. För att fixa detta skulle en ytterligare kontroll vara nödvändig som varje gång en nyckel A knäcks kontrollerar om nyckel B används genom att läsa sektor trailer-blocket. Ur sektor trailer-blocket kan man sedan utläsa om nyckel B används för någon åtkomstoperation för något av blocken i sektorn. Om nyckel B inte används innebär det att det utrymmet istället bara används för data.

Tabell 5

Implementeringstid	80 timmar + 80 timmar förberedelser	
Pris för utrustning	Proxmark3 HF antenn Klonetikett	$229 $59 $25
	Totalt	$313 (ca 2200 sek)
Begränsningar för att utföra kloningsangreppet med Proxmark3	Etikett inom 4cm från läsaren Inga andra störande RFID-etiketter inom läsavstånd Lång tid för att utföra angrepp	

Att uppnå den effektivitet och precision som beskrivs i den konfiguration av Proxmark3 som har använts i samband med utvecklingen av dessa angrepp i [8] kräver troligen stora ändringar i Proxmark3s FPGA-kod (hårdvarukoden). Den implementation av angreppet som finns tillgänglig för Proxmark3 är inte att betrakta som optimal då det tar lång tid att skapa de tabeller som behövs för det nästlade angreppet, jämfört med det som har presenterats i [8].

Att knäcka nycklar är inte alltid nödvändigtvis ett steg som måste göras för att klona en etikett. För ett angrepp då nycklarna redan är kända kan vilken läsare som helst användas. Till exempel om nycklar för en viss utgivare av etiketter visar sig alltid vara de samma, kan information om dessa spridas och vem som helst kan klona en etikett genom att använda en enkel läsare. Det är inte möjligt att göra ett system som använder Mifare Classic helt säkert, men det är möjligt att säkra systemet till en hög nivå. Genom att göra det svårare för en angripare kan riskerna minskas,

exempelvis genom att alltid använda olika nycklar i alla sektorer och undvika standardnycklar även om alla block inte används. Att ha en databas och uppdatera information på etiketterna vid användning kan också göra det möjligt att upptäcka ifall en etikett har klonats, då information på etiketten inte matchar det som står i databasen. I slutändan handlar det om att ha ett säkert bakomliggande system och att göra det så svårt som möjligt för en angripare att utföra en kloning.

4 Resultat och diskussion

RFID kan vara en sårbar teknik om inte hänsyn har tagits vid införandet av ett RFID-system om vilka risker och möjliga hot som finns. Kloning av en RFID-etikett kan leda till identitetsstöld, förfalskning av varor (etiketten säger att innehållet är någonting annat än vad det är) och utfärdandet av ”falska” biljetter. Hur enkelt eller svårt det är att angripa ett RFID-system beror på vilka skyddsmekanismer som finns, både på etiketten och i det bakomliggande systemet.

I vissa fall, i likhet med EM4100-etiketten, räcker det med att lyssna av kommunikationen mellan en RFID-etikett och en läsare eller att enkelt läsa av informationen på etiketten för att få den information som behövs för att göra en kopia av den. Andra funktioner som en RFID-etikett kan inneha kan göra angreppet för att kunna klona en etikett svårare. Exempel på säkerhetsfunktioner kan vara autentisering och kryptering. Mifare Classic skickar data krypterat och kräver autentisering men har flera svagheter som gör det möjligt att knäcka dess krypteringsnycklar. Det kan dock ta ”relativt” lång tid att utföra angreppet. Det är inte möjligt att förutse hur lång tid ett angrepp tar för att knäcka alla krypteringsnycklar med den implementation som har använts i detta arbete, eftersom det inte finns någon garanti om att Proxmark3 lyckas få samma nonce från kortet flera gånger i följd (se avsnitt 3.3.3). Det värsta fallet under försöken var 429 sekunder för en nyckel. Detta förutsätter att angriparen inte har någon tidigare kunskap om etikettens utformning, såklart.

Att utföra ett angrepp för att skapa en klonad etikett är möjlig på några olika sätt, som har beskrivits i respektive analysavsnitt och det finns ett flertal alternativa verktyg för att klona RFID-etiketter. Proxmark3 som främst har använts till kloningsförsöken i denna rapport är inte det enda alternativet. För kloning av EM4100 är Proxmark3 kanske det sämsta valet och ett bättre val för en angripare är en kommersiell EM4100/T5555/T5567 läsare/skrivare. Om en kommersiell läsare/skrivare används krävs ingen programmeringskunskap för att genomföra kloningen. Programvara finns redan tillgängliga som kan utföra allt som behövs för att skapa en klon. För att utföra ett kloningsangrepp på en Mifare Classic-etikett krävs i dagsläget mer teknisk kunskap och modifiering behöver utföras av de verktyg som finns tillgängliga. Klientprogrammet till Proxmark3 kan i sitt grundutförande utföra alla angrepp som krävs för att göra en klon för Mifare Classic 1K, men varje steg i angreppet kräver interaktion med användaren. Om angriparen har programmeringsvana är modifieringarna att betrakta som enkla för att automatisera angreppet på det sätt som har gjorts i denna rapport. Se Tabell 5 på sidan 39 för en sammanställning av kloningsangreppet av Mifare Classic. All information för att klona EM4100 eller Mifare Classic finns tillgänglig på Internet. För en angripare är diskussionsforum och bloggar värdefulla källor för att få information om kloning och andra angrepp mot RFID.

Oavsett hur systemet ser ut är kloning av EM4100- och Mifare Classic-etiketter möjlig, vilket har verifierats i denna rapport. Klonen av en EM4100-etikett kan skrivas till en kompatibel etikett eller en emulator. Mifare Classic har ett ID som inte går att skriva och gör det omöjligt att skapa en fullständig klon på ett annan Mifare Classic-etikett. För att få en klonad etikett med samma ID måste en emulator användas. Men en 1K etikett kan faktiskt klonas till en klonetikett som har ett skrivbart tillverkarblock (ID kan skrivas). För en angripare är en emulator det sämre valet - den inte ser ut som en etikett och användningen av en emulator istället för en etikett skulle se misstänkt ut.

Att utföra ett angrepp för att utvinna den information som krävs för att skapa en klon från ett ovetande offer är inte nödvändigtvis en enkel uppgift. Det finns många möjliga störningsmoment för angriparen som försvårar utförandet av ett angrepp:

1. Angriparen måste kunna vara tillräckligt nära etiketten som ska klonas under den tiden som angreppet utförs. För EM4100 är läsavståndet inget större hinder, då endast ett svep nära etiketten av en läsare är nödvändig (4-10 cm). För att utföra ett angrepp mot Mifare Classic måste etiketten vara nära (<5 cm) under en viss tid, som inte är förutsägbar, dock max 70 min (i genomsnitt). Att lyckas vara så pass nära så pass länge ett ovetande offer kan vara väldigt svårt.
2. RFID-etikettens typ måste vara känd innan angreppet alternativt måste angreppet utföras med ett system som kan identifiera etikettens typ. Att automatisera identifieringen av etikettens typ är ett svårt moment för angriparen och det begränsar vilka verktyg som kan användas för att utföra ett angrepp. Proxmark3 är ett verktyg som eventuellt skulle kunna göra detta, eftersom den inte har begränsningar till en viss typ av etikett eller frekvensband. Identifiering av frekvensbandet kan vara svårt eftersom olika antenner måste användas för olika frekvensband. När frekvensbandet har identifierats är etikettens typ fortfarande okänd. Typ av etikett kan eventuellt identifieras genom att studera vad etiketten skickar för signaler, förutsatt att den skickar signaler innan läsaren initialiserar kommunikation.
3. Störande signaler från andra etiketter eller mycket bakgrundsbrus kan försvåra läsning. Störande signaler kan komma från andra etiketter som offret har i fickan. Angriparen kanske inte vet vilken etikett som har blivit avläst, då denne inte har förkunskap om vilken etikett som tillhör vilket system. Om angriparen har viss förkunskap om systemet ser situationen annorlunda ut, men det hindrar inte läsning av fel etikett. För att läsa av rätt etikett krävs kunskap om etikettens typ och kanske även dess ID för att särskilja två etiketter av samma typ.

Ett kloningsangrepp kan också ske under ett annat scenario, då angriparen är ägaren av etiketten. Det leder till att de moment som kan försvåra eller hindra ett lyckat angrepp vid läsning av en etikett som inte är i angriparens ägo, inte medför några problem. Detta angrepp kanske är mindre intressant för EM4100, men fullt möjligt. Angreppet är dock mer intressant för Mifare Classic då det ofta används som resekort och liknande lösningar och angriparen kan tjäna pengar på att utföra kloningen. Den klonade etiketten kan sedan säljas vidare, billigare än vad de skulle kosta att köpa eller ”tanka” etiketten. Företag som tillhandahåller denna typ av etiketter skulle lida ekonomiskt om deras etiketter blev klonade och sålda på en svart marknad, men om det handlar om en anställd som klonar inpasseringsnycklar skulle detta innebära en stor risk för verksamheten.

För etiketter som har skrivbart minne kan de utsättas för andra angrepp som kan ses som en sidoeffekt av kloning. I Mifare Classics fall, när nycklarna är kända, är det möjligt att ändra det data som finns på etiketten. Det kan leda till ett annat angrepp, exempelvis kan data på etiketten modifieras för att agera som ”virusbärare” (avsnitt 2.4.5) eller ett skimningsangrepp (avsnitt 2.4.2) kan utföras. Om etiketten innehåller personlig information kan angriparen komma över detta genom läsning. Ibland kan ett angrepp mot etiketten helt enkelt utnyttjas till ens egen vinning, genom att exempelvis återställa informationen på en etikett efter ett köp eller öka värdet på etiketten. I Appendix D visas två flödesdiagram som exemplifierar hur modifiering och återställning kan göras på Mifare Classic-etiketter.

Eftersom RFID kan användas i så många olika typer av system är det svårt att generalisera användandet av RFID-etiketter. Om man däremot tänker på vad RFID står för, radiofrekvensidentifiering, kan ett antagande göras om att det åtminstone används för identifiering av något slag. Om det förekommer kloner av etiketter är det inte möjligt att skilja på vilken som är den äkta genom att läsa av dem, men de kan ha olika fysisk utformning. För att detektera kloner kan det bakomliggande systemet vara uppbyggt på ett sätt att den eventuellt upptäcker förekomster av dem. För enkla etiketter, de med bara ett ID, kan avläsningar registreras i en databas. Genom att sedan kontrollera registreringen av ID nummer kan eventuellt kloner upptäckas om ett ovanligt beteende förekommer. I ett inpasseringssystem där in- och utpassering registreras kan kloner upptäckas om samma ID försöker passera in när den redan har registrerats som inpasserad. Ett liknande system för läs- och skrivbara etiketter kan förenkla upptäckten av klonade etiketter ytterligare och registrering av utpassering är inte nödvändig. Genom att skriva viss information om inpassering på etiketten, kan en jämförelse göras av den information som finns skriven på etiketten mot vad som står i databasen. Om informationen på etiketten och i databasen inte överensstämmer har etiketten modifierats på något vis, då den ena etiketten (klonen eller originalet) inte har uppdaterats med den senaste informationen. Med andra ord är det viktigt att samtliga komponenter i ett RFID-system, det bakomliggande systemet och etiketten, är utformade för att upptäcka eller förhindra användning av klonade eller modifierade etiketter.

För någon som ska implementera ett RFID-baserat system är det viktigt att tänka på vilka tillgångar som ska skyddas, hur kritiska eventuella sårbarheter är och sannolikheten av angrepp. Det kan vara bra att jämföra ett RFID-system med ett annat motsvarande system och utföra en avvägning av fördelarna och nackdelarna av respektive lösning. Motsvarigheten till RFID-baserade inpasseringssystem kan vara nycklar eller dörrvakter, RFID-etiketten måste vara korrekt och systemet som hanterar avläsningen tar beslut om inpassering godkänns eller inte. Jämförelsen kan även göras på angrepp som är möjliga, att stjäla en nyckel eller att stjäla en RFID-etikett och att lura dörrvakten för att få inpassering eller att klona en etikett för att nå samma mål. Fördelen med RFID-etiketter kan vara den enkelhet som de medför, båda genom att automatisera identifiering och den kontaktlöshet som det bidrar med. Men detta medför inte alltid en tillräcklig nivå av säkerhet som visats i detta examensarbete, då kloning kan vara en risk. För att göra ett RFID-system säkrare kan man använda flerfaktorautentisering, då en kombination av avläsning av en etikett och exempelvis inmatning av en PIN-kod används, alternativt avläsning av fingeravtryck eller liknande. Detta ger en ytterligare nivå skydd och systemet blir säkrare men samtidigt går många av de största fördelarna med RFID-system förlorad: automatisering av identifiering och smidigheten.

5 Slutsats

Ju vanligare RFID-lösningar blir, desto fler angripare kommer få upp ögonen för dess svagheter. Idag kanske det inte är så vanligt att det utförs angrepp mot RFID-baserade system, då det inte räcker med att utföra detta hemma i vid sin dator som en hacker eller vara på plats och slita sönder systemet som en inbrottstjuv för att komma förbi det. Det är här hackarna och inbrottstjuvarna får samarbeta, det krävs både någon som knäcker systemet och någon som utför angreppen på plats. Exempelvis kan ”hackaren” vara den som bygger systemet för att klona ett kort och ”tjuven” är den som ser till att få tillgång till en RFID-etikett som ska klonas. De som väljer att implementera en RFID-lösning måste ta till hänsyn vilka hot som kan finnas och hur systemet skulle kunna utnyttjas för att förhindra eventuella angrepp. Om säkerheten är viktig – använd en RFID-lösning som har tillräcklig bra säkerhetsmekanismer.

Utifrån experiment som utförts verkar många utgivare av etiketter vara omedvetna om svagheter och problem med den typen av etiketter de använder. Bakomliggande system saknar ofta kontroller som hindrar användning av klonade etiketter. Särskilt i Mifare Classics fall är det viktigt att utnyttja alla sektornycklar för att göra det så svårt som möjligt för en angripare att klona etiketter. Dessutom är ”klonetiketter” någonting som inte har rapporterats om tidigare och medför att en etiketts ID inte är någonting som kan användas för att göra ett Mifare Classic-baserat system säkrare. Däremot har tidsåtgången av kloningsangrepp som utförts mot Mifare Classic varit långt över de som rapporterats i vetenskapliga artiklar. Resultaten i detta arbete visade att risken för smyg-angrepp är osannolik, på grund av tiden ett angrepp tar och hur nära en angripare måste befinna sig. Däremot är det mer sannolikt att kloning genomförs av en egen etikett eller en etikett som har stulits tillfälligt, därför bör Mifare Classic inte användas som någon typ av värdehandling. Inte heller bör Mifare Classic användas om det finns risk för insider-hot om kontroll av spridning av etiketter är viktig.

Vad som är tillräckligt bra är individuellt för varje system och användningsområde vilket kräver att en grundlig riskanalys bör genomföras i varje fall. Denna rapport kan vara en bra grund för att utföra en riskanalys för system som använder EM4100-etiketter (eller likande) eller Mifare Classic. Kloning av EM4100-etiketter kan betraktas som enkel. Men kloning av Mifare Classic kan vara svår att utföra på någon som är ovetande om angreppet, men om angriparen äger etiketten eller har förkunskap om nycklar kan kloner skapas utan större hinder. Om säkerheten är viktig bör åtgärder vidtas för att göra ett system säkert. Däribland ingår användandet av RFID-etiketter med fler och bättre säkerhetsmekanismer, så som autentisering och säker kryptering, men det är även viktigt att det bakomliggande systemet är utformat för att hantera eventuella angrepp.

5.1 Förslag på fortsatta arbeten

Utifrån detta arbete kan ett flertal mindre områden undersökas vidare, dels teoretiskt men också praktiskt.

- Hur skulle angreppen mot Mifare Classic kunna snabbas upp för att uppnå liknande resultat som presenterats av forskare?
- Utveckla ett program som kan utföra ett angrepp som kan detektera etikettens typ. Proxmark3 skulle vara ett bra verktyg för att använda till den typen av vidare arbete.
- Vidare studier under vilka omständigheter kloningsangrepp kan utföras genom att studera vilka andra hinder som kan finnas, till exempel flera etiketter i en plånbok eller störande signaler från omgivningen.

- I rapporten har även andra läsare och antenner för att utföra angreppen nämnts men inte testats, och att undersöka detta vidare vore ytterligare ett intressant område att fördjupas.
- En studie över RFID-etiketter som ska vara säkrare, så som Mifare DESFire (EV1) och HID iClass. Finns det svagheter som skulle kunna utnyttjas av angripare vid användning av andra RFID-etiketter?
- Hur påverkar NFC-enheter ett skimningsangrepp? Vilka skillnader finns det med vanliga Mifare Classic-etiketter och en NFC-enhet som används som en Mifare Classic-etikett?

En annan vinkling av arbetet är att istället för att fundera på hur en angripare skulle kunna utnyttja ett RFID-system är att fundera på hur någon som ska implementera ett system ska kunna göra det bättre. Detta kan göras genom att kartlägga hur det bakomliggande systemet ska fungera för att på bästa möjliga sätt detektera eller förhindra angrepp.

6 Litteraturförteckning

[1] K. Nohl, ”Cryptanalysis of Crypto-1,” 8 Mars 2008. [Online]. Available: http://www.cs.virginia.edu/~kn5f/Mifare.Cryptanalysis.htm. [Använd 6 Augusti 2012].

[2] F. D. Garcia, G. de Koning Gans, R. Muijrers, P. van Rossum, R. Verdult, R. Wichers Schreur och B. Jacobs, ”Dismantling MIFARE Classic,” i *Proceedings of the 13th European Symposium on Research in Computer Security, ESORICS 2008*, 2008.

[3] ”Get Your Proxmark3,” [Online]. Available: http://proxmark3.com/. [Använd 6 Augusti 2012].

[4] NXP, ”http://www.nxp.com/documents/leaflet/75015782.pdf,” 19 November 2010. [Online]. Available: http://www.nxp.com/documents/leaflet/75015782.pdf. [Använd 6 Augusti 2012].

[5] T. Phillips, T. Karygiannis och R. Kuhn, ”Security Standards for the RFID Market,” *IEEE Security & Privacy,* vol. 3, nr 6, pp. 85-89, 12 December 2005.

[6] A. Juels, ”RFID Security and Privacy: A Research Survey,” *IEEE Journal on Selected Areas in Communications,* vol. 24, nr 2, pp. 381-395, 2006.

[7] J. Ari, D. Molnar och D. Wagner, ”Security and Privacy Issues in E-passports,” i *SECURECOMM '05 Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, Washington, DC, USA, 2005.

[8] F. D. Garcia, P. van Rossum, R. Verdult och R. Wichers Schreur, ”Wirelessly Pickpocketing a Mifare Classic Card,” i *Oakland IEEE Symposium on Security and Privacy*, 2009.

[9] N. T. Courtois, ”THE DARK SIDE OF SECURITY BY OBSCURITY and Cloning MiFare Classic Rail and Building Passes, Anywhere, Anytime,” Cryptology ePrint Archive: Report 2009/137, 2009.

[10] G. P. Hancke, ”Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens,” *Journal of Computer Security,* vol. 19, nr 2, pp. 259-288, Mars 2011.

[11] M. Roberti, ”The History of RFID Technology - RFID Journal,” [Online]. Available: http://www.rfidjournal.com/article/view/1338. [Använd 6 Augusti 2012].

[12] K. Finkenzeller, RFID handbook: fundamentals and applications in contactless smart cards and identification, 2:a red., Chichester: Wiley, 2003.

[13] ”HITACHI GLOBAL : News Release : Operation verified on world's smallest 0.05 mm x 0.05 mm "contactless powder IC chip" One-ninth the size of previous prototype, enabling insertion in paper,” 13 Februari 2007. [Online]. Available: http://www.hitachi.com/New/cnews/070213c.html. [Använd 6 Augusti 2012].

[14] U. By, ”Han har ett chip under huden - DN.SE,” 5 April 2011. [Online]. Available:

http://www.dn.se/livsstil/reportage/han-har-ett-chip-under-huden. [Använd 6 Augusti 2012].

[15] P. Zhou, D. Pang och W. Li, ”Embedded Bio-Sensor System”. USA Patent 7297112, 18 Oktober 2006.

[16] PositiveID Corporation, ”PositiveID Corporation™ - Products - HealthID and MicroFluidic Systems,” 2012. [Online]. Available: http://www.positiveidcorp.com/products.html. [Använd 6 Augusti 2012].

[17] EPCglobal, ”Frequently Asked Questions,” [Online]. Available: http://www.gs1.org/docs/epcglobal/Frequently_Asked_Questions.pdf. [Använd 6 Augusti 2012].

[18] International Civil Avation Organization, ”ePassports and biometrics,” 29 Juli 2011. [Online]. Available: http://legacy.icao.int/icao/en/atb/meetings/2011/TagMrtd-20/Docs/TagMrtd-20_IP002-rev_en.pdf. [Använd 6 Augusti 2012].

[19] J. Yoshida, ”Euro bank notes to embed RFID chips by 2005,” EEtimes, 19 December 2001. [Online]. Available: http://www.eetimes.com/electronics-news/4164053/Euro-bank-notes-to-embed-RFID-chips-by-2005. [Använd 6 Augusti 2012].

[20] Visa Europe, ”Visa payWave,” [Online]. Available: http://www.visaeurope.com/en/cardholders/visa_paywave.aspx. [Använd 6 Augusti 2012].

[21] MasterCard, ”MasterCard PayPass Home,” [Online]. Available: http://www.paypass.com/. [Använd 6 Augusti 2012].

[22] Google, ”Google Wallet - a smart, virtual wallet for in-store and online shopping,” [Online]. Available: http://www.google.com/wallet/. [Använd 6 Augusti 2012].

[23] Visa, ”Barcelona - wave and pay with mobile phones - case study.pdf,” 2010. [Online]. Available: http://www.visaeurope.com/en/making_money_flow/video_popup/idoc.ashx?docid=7c65cb27-53fb-40f5-921d-6404c938495b&version=-1. [Använd 6 Augusti 2012].

[24] T. Kasper, M. Silbermann och C. Paar, ”All You Can Eat or Breaking a Real-World Contactless Payment System,” i *Financial Cryptography*, 2010, pp. 343-350.

[25] OpenPCD, ”OpenPICC RFID Emulator Project - OpenPCD,” [Online]. Available: http://www.openpcd.org/OpenPICC_RFID_Emulator_Project. [Använd 6 Augusti 2012].

[26] T. Kasper, I. von Maurich, D. Oswald och C. Paar, ”Chameleon: A Versatile Emulator for Contactless Smartcards,” i *ICISC 2010*, Springer Berlin / Heidelberg, 2011, pp. 189-206.

[27] J. Reid, J. M. Gonzalez Nieto, T. Tang och B. Senadji, ”Detecting relay attacks with timing-based protocols,” i *ASIACCS '07 Proceedings of the 2nd ACM symposium on Information, computer and communications security*, 2007.

[28] M. R. Rieback, B. Crispo och A. S. Tanenbaum, ”Is Your Cat Infected with a Computer Virus?,” i *PERCOM '06 Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, Washington, DC, USA, 2006.

[29] EM MICROELECTRONIC, *EM4100 Read Only Contactless Identification Device, EM4100 Datablad,* 2002.

[30] Sokymat Identification, ”Q5 datasheet,” [Online]. Available: http://rfid.wz.cz/LFcipy/Q5_doc.pdf. [Använd 6 Augusti 2012].

[31] Atmel, ”Multifunctional 330-bit Read/Write RF Identification IC ATA5567,” [Online]. Available: http://www.atmel.com/Images/doc4874.pdf. [Använd 6 Augusti 2012].

[32] RMXLABS, ”RMXLABS — Дубликатор электронных ключей KeyMaster 4 RF,” [Online]. Available: http://www.rmxlabs.ru/products/keymaster_pro_4_rf/. [Använd 6 Augusti 2012].

[33] NXP Semiconductors, *MIFARE Classic 1K - Mainstream contactless smart card IC, MF1S503x Datablad,* 3.1 red., 2011.

[34] NXP Semiconductors, *MIFARE Classic 4K - Mainstream contactless smart card IC, MF1S703x Datablad,* 3.0 red., 2010.

[35] K. Nohl, H. Plötz, D. Evans och Starbug, ”Reverse-Engineering a Cryptographic RFID Tag,” i *SS'08 Proceedings of the 17th conference on Security symposium*, Berkeley, CA, USA, 2008.

[36] NXP Semiconductors, ”mifare.net :: 4-7Byte UID,” NXP Semiconductors, [Online]. Available: http://mifare.net/technology/4-7byte-uid/. [Använd 6 Augusti 2012].

[37] P. Lindstrom och F. Thornton, RFID Security, Rockland, MA, USA: Syngress Publishing, 2005.

[38] H. Knospe och H. Pohl, ”RFID Security,” *Information security technical report,* vol. 9, nr 4, pp. 39 - 50 , 2004.

[39] S. A. Weis, ”RFID (Radio Frequency Identification): Principles and Applications,” MIT CSAIL, 2007.

7 Bilagor

7.1 Bilaga A: Mifare Classic åtkomstvillkor

Informationen nedan baseras på information från Mifare Classic 1K och Mifare Classic 4K datablad [33] [34]. Vid leverans är samtliga nycklar `ffffffffffff` och åtkomstvillkoren är satta till `C1 = 0, C2 = 0, C3 = 1` (kursivt markerad i tabellen ” Åtkomstvillkor för sektor trailer”), nyckel A används för alla operationer.

Åtkomstvillkoren för en sektor beskrivs med tre bytes i sektor trailern, byte 6, 7 och 8.

	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Byte 6	$\overline{C2_3}$	$\overline{C2_2}$	$\overline{C2_1}$	$\overline{C2_0}$	$\overline{C1_3}$	$\overline{C1_2}$	$\overline{C1_1}$	$\overline{C1_0}$
Byte 7	$C1_3$	$C1_2$	$C1_1$	$C1_0$	$\overline{C3_3}$	$\overline{C3_2}$	$\overline{C3_1}$	$\overline{C3_0}$
Byte 8	$C3_3$	$C3_2$	$C3_1$	$C3_0$	$C2_3$	$C2_2$	$C2_1$	$C2_0$

kontrollbitar	Sektorblock MC 1k	Sektorblock MC 4k	
		Sektor 0-31	Sektor 32-39
$C1_0, C2_0, C3_0$	0	0	0-5
$C1_1, C2_1, C3_1$	1	1	5-9
$C1_2, C2_2, C3_2$	2	2	10-14
$C1_3, C2_3, C3_3$	3	3	15

Åtkomstvillkor för sektor trailer:

Åtkomstbitar			Åtkomstkontroll för					
			Nyckel A		Åtkomstbitar		Nyckel B	
$C1$	$C2$	$C3$	Läsa	Skriva	Läsa	Skriva	Läsa	Skriva
0	0	0	Aldrig	Nyckel A	Nyckel A	Aldrig	Nyckel A	Nyckel A
0	1	0	Aldrig	Aldrig	Nyckel A	Aldrig	Nyckel A	Aldrig
1	0	0	Aldrig	Nyckel B	Nyckel A|B	Aldrig	Aldrig	Nyckel B
1	1	0	Aldrig	Aldrig	Nyckel A|B	Aldrig	Aldrig	Aldrig
0	*0*	*1*	*Aldrig*	*Nyckel A*	*Nyckel A*	*Nyckel A*	*Nyckel A*	*Nyckel A*
0	1	1	Aldrig	Nyckel B	Nyckel A|B	Nyckel B	Aldrig	Nyckel B
1	0	1	Aldrig	Aldrig	Nyckel A|B	Nyckel B	Aldrig	Aldrig
1	1	1	Aldrig	Aldrig	Nyckel A|B	Aldrig	Aldrig	Aldrig

Åtkomstvillkor för block:

Åtkomstbitar						
$C1$	$C2$	$C3$	Läsa	Skriva	Öka	Minska, Flytta, Återställa
0	0	0	Nyckel A|B	Nyckel A|B	Nyckel A|B	Nyckel A|B
0	1	0	Nyckel A|B	Aldrig	Aldrig	Aldrig

1	0	0	Nyckel A|B	Nyckel B	Aldrig	Aldrig
1	1	0	Nyckel A|B	Nyckel B	Nyckel B	Nyckel A|B
0	0	1	Nyckel A|B	Aldrig	Aldrig	Nyckel A|B
0	1	1	Nyckel B	Nyckel B	Aldrig	Aldrig
1	0	1	Nyckel B	Aldrig	Aldrig	Aldrig
1	1	1	Aldrig	Aldrig	Aldrig	Aldrig

7.2 Bilaga B: Prisexempel för RFID-utrustning

Priserna nedan är ungefärliga

Mifare Classic

Proxmark3 $229 + HF antenn $59

Touchatag (ACR122) NFC läsare $39.95

Klonetikett $25/styck

Mifare Classic 1K/4K (S50/S70) $2/styck

EM4100

Proxmark3 $229 + LF antenn $59

Keymaster Pro 4 RF "kloningsmaskin" 275€

Proxy Key T5 "kloningsmaskin" 110€

125 KHz RFID Card Copier/Duplicator 125K-ID-P-D3 $79

Vanlig EM4100 läsare 125K-R-USB-D1 $49

EM4100 läsare/T5567 skrivare T5-RW-USB-D1 $69

EM4100 läsare 80-90 cm 125K-R-LR-232 (RS232 kontakt) $129

EM4100 kompatibel skrivbar etikett $2/styck

7.3 Bilaga C: Avlyssning av kommunikation - jämförelse av Mifare Classic Originaletikett och Klonetikett

Kommunikation mellan en Mifare Classic läsare har avlyssnats med hjälp av Proxmark3 för att demonstrera skillnaden i beteendet vid autentisering till block 01. Den första visar originaletiketten som är en äkta Mifare Classic, det andra visar dess klon som inte har ett äkta Mifare Classic-chipp. Dessa är något redigerade då anti-kollisionsprocessen är lång innan en etikett faktiskt blir vald för autentisering (markerat med ”SNIP” nedan). Värt att notera att kommandot `30 00 02 a8` som används för att läsa block 0 av läsaren utan autentisering är möjlig på klonetiketten, medan originaletiketten svarar med `04`, vilket betyder att operationen inte är tillåten. Denna avlyssning är avklippt efter autentiseringen, då kommunikationen är krypterad därefter och fungerar på samma sätt på båda etiketterna.

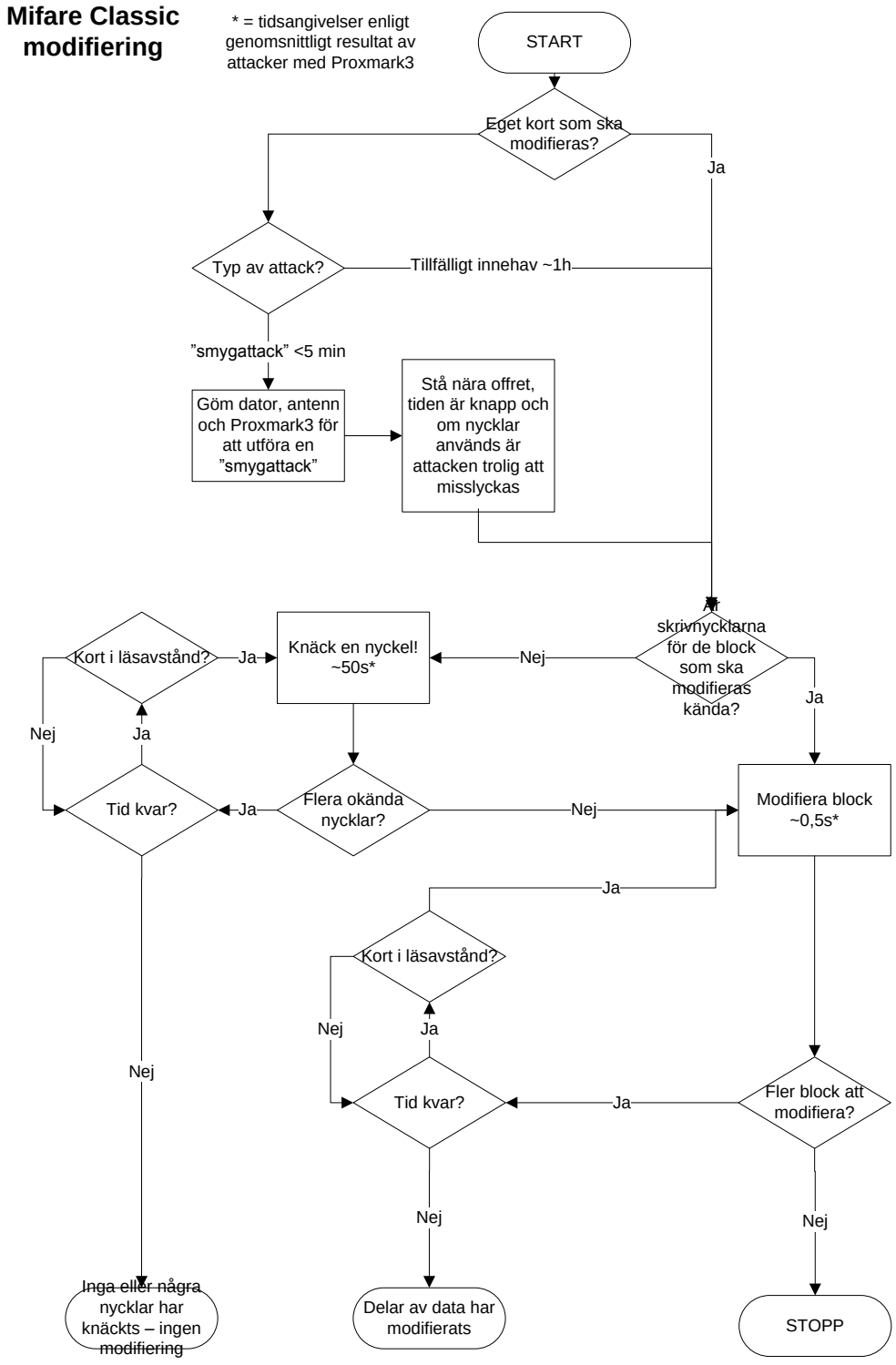
```
recorded activity ORIGINAL:
 ETU     :rssi: who bytes
---------+----+----+-----------
 +      0:    0: TAG 04
 +   1928:     :     50  00  57  cd
 +   4239:     :     52
 +    197:     :     00
 +   3227:     :     93  20
 +     64:    0: TAG ae  82  4b  34  01
 +   5071:     :     93  70  ae  82  4b  34  53  f4  d8
 +     64:    0: TAG 08
 +    120:    0: TAG ea  07
 +  95413:     :     30  00  02  a8       // Läs block 00 (ej autentiserad)
 +     72:    0: TAG 04
 +   1920:     :     50  00  57  cd
 +   4087:     :     52
 … SNIP …
 +     66:    0: TAG 04  00
 +   3094:     :     93  20
 +     66:    0: TAG ae  82  4b  34  53
 +   5086:     :     93  70  ae  82  4b  34  53  f4  d8
 +     64:    0: TAG 08  b6  dd
 +  57520:     :     60  01  7c  6a          // Autentisera till block 01
 +    114:    0: TAG f3  0f  8e  3d          // nonce från etikett
 +   3854:     :     ca  15  2e  4c  8b  4f  e8  ca     !crc       // svar
från läsare
 +     66:    0: TAG c8! e9! d9! 05!             // svar från etikett
…

recorded activity KLON:
 ETU     :rssi: who bytes
---------+----+----+-----------
 +      0:    0: TAG 04  00
 +   3176:     :     93  20
 +     64:    0: TAG ae  82  4b  34  53
 +   5416:     :     93  70  ae  82  4b  34  53  f4  d8
 +     63:    0: TAG 08  b6  dd
```

```
 +  95453:    :     30  00  02  a8
 + 166036:    :     26
 +     64:   0: TAG 04  00
 +   3088:    :     93  20
 +     64:   0: TAG ae  82  4b  34  53
 +   5207:    :     93  70  ae  82  4b  34  53  f4  d8
 +     64:   0: TAG 08  b6  dd
 +    248:   0: TAG 30  63  63
 +  95061:    :     30  00  02  a8      // Läs block 00 (ej autentiserad)
 +    464:   0: TAG ae  82  4b  34  53  88  04  00  47  c1  35  14  c9  00
24  08  8f  0f
… SNIP …
 +  95980:    :     30  00  02  a8
 +    464:   0: TAG ae  82  4b  34  53  88  04  00  47  c1  35  14  c9  00
24  08  8f  0f
 +  83070:    :     60  01  7c  6a         // Autentisera till block 01
 +    312:   0: TAG c3  2e  dd  29       // nonce från etikett
 +   3368:    :     e8  9e  a2  b2  15  de  85  6a     !crc     // svar
från läsare
 +     80:   0: TAG 5e! 8a! fa! 65     // svar från etikett
…
```

7.4 Bilaga D: Flödesdiagram för modifiering och återställning av data på Mifare Classic

Flödesschemat nedan illustrerar hur ett angrepp skulle kunna utföras för att modifiera data på en Mifare Classic-etikett.



Flödesdiagrammet nedan illustrerar hur ett kort skulle kunna återställas till ett tidigare stadie, det vill säga, kortet har lästs av tidigare och därefter skrivs samma data tillbaka på kortet. Det innebär att exempelvis ett kort som används som ett resekort ”laddas på” vid en återställning.