UNIVERSITATEA TITU MAIORESCU

FACULTATEA: INFORMATICĂ
DEPARTAMENT: INFORMATICĂ
Programa de studii: INFORMATICĂ
DISCIPLINA: INTELIGENȚĂ ARTIFICIALĂ

IA – *Testul de evaluare nr.* 14

Element Securizat SmartCard

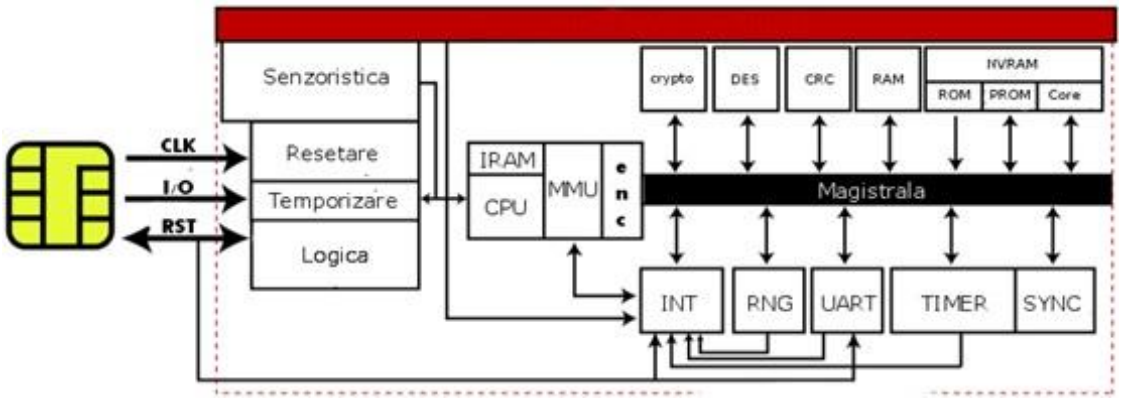
Grupa	Numele și prenumele	Semnătură student	Notă evaluare

Data: ____/____/_____

CS-I dr.ing.
Lucian Ștefăniță GRIGORE

Conf.dr.ing.
Iustin PRIESCU

Ș.L.dr.ing.
Dan-Laurențiu GRECU



Cuprins

1. INTRODUCERE

Elementul securizat este un dispozitiv de tip smartcard, dotat cu capabilități de calcul, control și securitate, care devine din ce în ce mai răspândit în aplicații cu impact economic, precum plățile digitale, logistică de autentificare și acces securizat la resurse.

Denumim „element securizat” un sistem de calcul specializat, sub forma de circuit integrat, prevăzut cu anumite mecanisme de securitate. Un circuit integrat este un circuit electronic miniaturizat, care este fabricat în același substrat. Circuitele integrate poartă mai multe nume: IC, subansamblu, microcip, cip de siliciu, sau pur și simplu chip. La un smartcard, IC oferă capabilități de logică pentru aplicații specifice care vor fi executate de acel card. Aceste IC securizate sunt utilizate în smartcarduri pentru ca o oferă un grad de „siguranță” – ceea ce înseamnă că au fost proiectate și fabricate cu caracteristici care sunt folosite pentru a proteja datele pe care le stochează și pentru a permite efectuarea de transmisii de date care nu pot fi interceptate de răuvoitori. Aplicațiile conținute pe smartcarduri variază în complexitate, dar și în cerințele de memorie și de securitate care sunt necesare pentru a le proteja funcționarea. În funcție de aplicație, se pot folosi memorii flash sau microcontrolere securizate.

1.1 Memorii securizate

Circuitele integrate tip memorie sunt utilizate pentru aplicații de smartcard care doar stochează date, dar cer ca acestea să fie protejate. Prin datele înțelegem informațiile necesare pentru ca aplicația respectivă să își poată desfășura activitatea. De exemplu, următoarele informații trebuie stocate într-o memorie IC pentru a putea face plăți cu cardul:

- emitentul cardului
- card de serie numărul
- alte informații de utilizator (în funcție de aplicația de carte)

Smartcardurile utilizează de obicei memorie non-volatilă (NVM), care permite menținerea datelor chiar și în lipsa unei surse de alimentare. Un card de memorie poate încorpora diferite tipuri de circuite integrate pentru execuția modulului de memorie, dar cele mai populare sunt EPROM și EEPROM. EPROM pot fi modificate o singură dată și sunt folosite la implementarea serviciilor de prepay, cum ar fi cartelele de telefonie mobilă, care dpdv software nu fac altceva decât să scadă un contor de minute până la zero, după care nu mai pot fi reutilizate, pentru că nu există niciun mecanism prin care să le reprogramăm. În schimb, memoriile EEPROM pot fi rescrise de până la 500.000 ori. Mai mult, conține deja capabilitățile aritmetice care sunt necesare pentru a actualiza un contor de servicii preplătite, precum în exemplul de mai devreme.

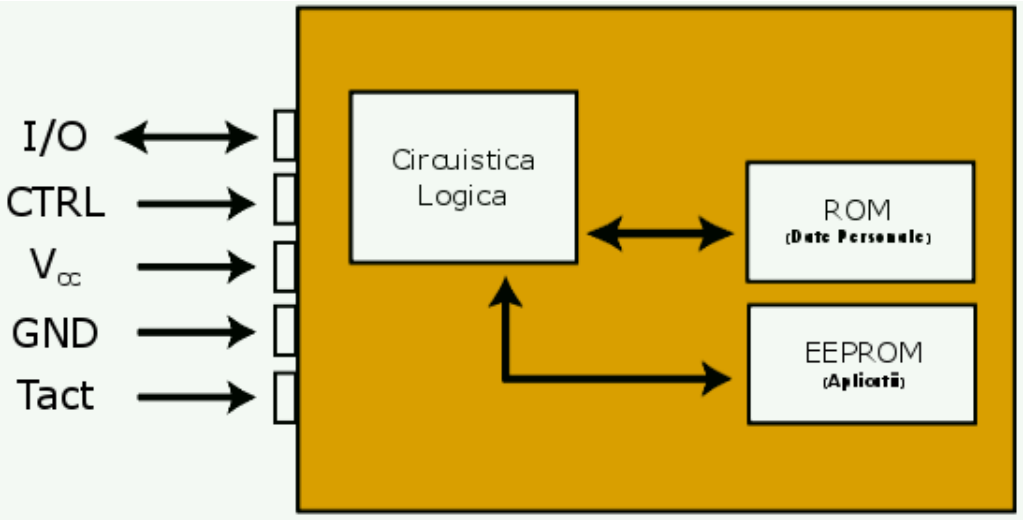


Figura 1. Diagrama bloc a memoriilor IC securizate

Fiecare element securizat este identificat printr-un număr de serie unic. Opționale, memoria IC dispune de logică pentru autentificare, contorizare, eroare și chei de autentificare. Astfel, dezvoltatorii de aplicații pentru smartcard au mai multe opțiuni din care pot alege, ca structură a sistemului de memorie, pentru a satisface cerințele de proiectare. Figura 1 prezintă diagrama bloc a unei memorii IC securizate.

Din cele două tipuri de circuite integrate securizate – memorie și microcontroler – care sunt utilizate în smartcarduri, memoriile sunt mai puțin sigure. De aceea, inclusiv la cele mai simple modele, aceste memorii sunt prevăzute cu o logică de circuit care previne scrierea sau ștergerea datelor. Bineînțeles că și modelele mai complexe limitează și ele accesul la datele stocate în memorie. Pentru a putea asigura mecanisme de securitate, precum execuția unor algoritmi criptografici ce criptează datele stocate pe card cât și interfațarea cu dispozitivul gazdă, cardurile de memorie conțin o logică statică ce implementează aceste lucruri. Acești algoritmi, care folosesc operații aritmetice standard de criptografie, pot lucra într-o aritmetică binară de până la 128 biți.

1.2 Microcontrolere securizate

Microcontrolerele securizate sunt niște circuite integrate mai sofisticate, cu rol de sistem de calcul specializate. Un astfel de microcontroler reprezintă un ansamblu format din memorie non-volatilă (pentru stocarea pe termen lung a datelor), memorie utilizator (pentru execuția de aplicații), RAM, ROM și o interfață I/O. (A se vedea figura 2 la punctul 3.2.1 pentru diagrama bloc a unui microcontroler securizat tip IC.) Sigur microcontroler ICs sunt programate pentru a executa aplicații și funcționalitate poate fi efectuată dinamic. În funcție de ce funcții de securitate microcontroler este necesară pentru a efectua într-o aplicație special, operatorul poate avea un motor criptografice pentru a mai rapid și în siguranță procesul de algoritmi simetrice sau asimetrice.

Programul de cod este scris în memoria ROM a microcontrolerului în timpul procesului de fabricație a circuitului integrat. Codul de program, la care ne referim de multe ori ca sistem de operare (OS) al circuitului integrat, sprijină executarea de aplicații pe care le are de efectuat microcontrolerul. Datele și codul binar sunt stocate în NVM, care poate fi accesată de sistemul de operare al IC. Sistemul de memorie poate fi omogen sau heterogen: EPROM, EEPROM, memorie flash sau memorie cu acces aleator feroelectric (FRAM). Memoria flash este un anumit tip de EEPROM care poate fi șterasă și programată în blocuri mari. FRAM este o tehnologie rapidă și de mică putere, care utilizează materialul prin modificarea polarității, realizând astfel stocarea datelor (peste 100 miliarde de ori accesări).

Securitatea dinamică activă este una din caracteristicile principale ale unui microcontroler securizat. Microcontrolerele au fost incluse în smartcarduri mai ales pentru tranzacțiile sigure de date. Dacă un utilizator sau un sistem nu se pot autentifica față de microcontroler, atunci nu se pot accesa datele stocate pe card. Deci, chiar dacă pierdem un smartcard, datele stocate pe acesta nu vor fi expuse celorlalți. În plus, microcontrolerelor de pe smartcard, deși mici ca dimensiuni, pot prelucra date interne în mod securizat la fel ca un calculator portabil, iar rezultatul calculelor poate fi afișat și acesta la ieșire. Integritatea datelor stocate este protejată de o suită de contramăsuri care intervin atunci când microcontrolerul depistează o tentativă de atac.

Microcontrolerele securizate oferă caracteristici de securitate on-chip, care protejează împotriva atacurilor fizice și logice. Se monitorizează atât frecvența ceasului extern, cât și tensiunile. Drepturile de acces la memorie sunt controlate de unitatea de management și de protecție a memoriei. Un nivel ce constă dintr-un scut activ (active Shield) poate detecta încercări de a sonda sau forța componentele interne sau liniile de semnal. Generarea aleatoare a perturbațiilor de curent pe magistrala inactivă este o tehnică specială care protejează împotriva atacatorilor care analizează semnalele de pe magistrală. Atunci când cineva încearcă să analizeze IC cu diverse tehnici, senzorii încorporați se activează și declanșează o procedură de resetare specială pericolelor de securitate, care suprascrie imediat zona de RAM.

Împotriva analizei puterii funcționează un mecanism de scrambling, împreună cu un generator de numere aleatorii real și capabilități de așteptare aleatoare de stare.

Aceste microcontrolere au început să înlocuiască elementele securizate construite ca memorii semiconductoare, mai ales că tehnologia a evoluat pentru a ne oferi mai multă funcționalitate per mai puțin zona de siliciu (adică, costuri mai mici). Microcontrolerele securizate sunt disponibile cu 8KB sau mai puțină memorie și furnizează capabilități de organizare a sistemului de fișiere de pe spațiul de stocare, sau conform altor structuri de organizare a storajului, precum cele paginate sau bancate. Exemplele anterioare prezintă o imagine a capabilităților de securitate ale microcontrolerelor si nu trebuie confundate cu cele ale memoriilor securizate.

1.3 Protecția datelor

Atunci când concepem o aplicație sau un produs pe bază de smartcard, trebuie să acordăm cea mai mare importanță protecției sistemului informatic, prin acest concept înțelegând inclusiv datele de utilizator. Există o serie de amenințări la care sunt supuse aplicațiile ce folosesc date personale, care pot compromit următoarele caracteristici:

- *confidențialitatea*: toate datele clasificate de către OS și dezvoltatorii de aplicații ca fiind „sensibile” trebuie să fie păstrate confidențiale. Această protecție include, la nivel minim, limitarea accesului altora la memoria IC;
- *integritatea*: datele, codurile, funcțiile de securitate și orice alte componente conexe sensibile trebuie să își păstreze forma originală sau forma în care trebuie să se afle, conform scopului aplicației;
- *disponibilitatea*: pentru ca aplicațiile derulate pe IC să ruleze corect, este necesar ca datele solicitate de IC să fie întotdeauna disponibile, dacă condițiile de securitate sunt îndeplinite, iar funcționarea sistemului în ansamblul său trebuie să fie întotdeauna controlat și accesibil.

Aplicațiile smartcard variază în cerințe dpdv. al stocării, prelucrării și securizării datelor. Aceste cerințe vor dicta alegerea elementului securizat ce va fi folosit cât și tipurile de măsuri de securitate care va fi implementate la cerere.

1.4 Standarde smartcard

Elementele securizate tip smartcard trebuie să se conformeze standardelor pentru realizarea interoperabilității. Standardele ISO/IEC 7816 și ISO/IEC 14443 definesc cadrul general de operare pentru smartcard. IC securizate cu contact trebuie să respecte standardele definite în ISO/IEC 7816 (părțile 1, 2 și 3) pentru smartcard. Partea 1 descrie caracteristicile fizice ale cardurilor pe bază de circuit integrat. Această parte a standardului definește limitele de expunere pentru o serie de fenomene electromagnetice, cum ar fi lumina UV, razele X, câmpurile electromagnetice, câmpurile electrostatice și temperatura ambientală. Partea 2 definește dimensiunile și amplasarea contactelor. De asemenea, include standarde despre numărul, funcția și poziția de contacte electrice. Partea 3 descrie semnale electronice și protocoale de transmisie de carduri de circuit integrat. IC fără contact trebuie concepute în conformitate cu un set suplimentar de standarde definite în ISO/IEC 14443. ISO/IEC 14443 este format din patru părți și descrie două metode de modulare prin care cardurile pot comunica cu dispozitivul de citire. Modulațiile sunt menționate ca tip A și tip B. Partea 1 descrie caracteristicile fizice. Partea 2 specifică puterea de frecvență radio și interfața de semnal. Partea 3 definește inițializarea și mecanismul anti-coliziune. Protocolul de transmisie este descris în partea 4. Protocolul de transmisie specifică schimburile de date și mecanismele de conectare: bloc de date înlănțuite, așteptare-prelungire, și activare multiplă.

2. ATACURI CONTRA ELEMENTELOR SECURIZATE

Microcontrolerele securizate respectă confidențialitatea, accesibilitatea și integritatea datelor stocate în consens cu facilitățile oferite aplicațiilor pentru a-și accesa datele. Majoritatea aplicațiilor care necesită măsuri de siguranță folosesc smartcard cu microcontroler pe post de element securizat, precum aplicații de tip e-Passport, cartele de acces, carduri de credit și portofel electronic.

Trebuie să abordăm problema securității de bază a platformelor cu smartcard. În funcție de cum sunt utilizate, cardurile smart pot fi uneori în situația de a ține secrete chiar față de oamenii care le poartă sau le utilizează. De exemplu, la un smartcard care stochează valoarea monetară într-un registru intern, în cazul în care utilizatorul de card ar beneficia de o modalitate de a modifica această valoare, ar putea fi astfel capabil să falsifice bani.

Deoarece smartcardurile sunt adesea folosite în situații critice de securitate, au fost supuse unei atenții deosebite din partea cercetătorilor și inginerilor. În linii mari, există două categorii de probleme de securitate specifice acestor dispozitive: 1) probleme de terminal și 2) atacuri fizice pe card.

2.1 Problema de terminal

Smartcardurile au nevoie de un mod de a interacționa cu utilizatorii lor (umani sau alte dispozitive). Deoarece majoritatea smartcardurilor nu sunt prevăzute cu capacitate de afișaj, gazda trebuie să ia asupra sa această responsabilitate. Orice afișaj utilizat în timpul tranzacțiilor critice, cum ar fi transferul de bani, trebuie să aibă două proprietăți: afișarea trebuie să fie demnă de încredere și, mai mult, trebuie să fie unspoofable[1]. Asigurarea unui terminal care să prezinte informațiile corespunzătoare și de încredere pentru un utilizator este cunoscută ca „problema de terminal”.

Problema de terminal este o problemă de încredere. Cum poate fi utilizatorul asigurat că aplicația face ceea ce se presupune a face, în timpul unei tranzacții? Cum poate utilizatorul să verifice dacă balanța de contul (de exemplu) a fost corect debitată sau creditată? Problema este că smartcardurile sunt de foarte multe ori ca niște cutii negre.

Multe sisteme aflate acum în faza de proiectare includ utilizarea computerelor personale pe partea de client. Utilizatori vor folosi un PC pentru a interacționa cu smartcardul și pentru a rezolva problema de terminal. Problema este că PC-urile prezintă un grad mic de siguranță, mai ales atunci când sunt utilizate pentru a vehicula o sumedenie de documente și programe, cum fac majoritatea oamenilor.

O consecință directă a slăbiciunilor de securitate ale PC este faptul că nu pot fi folosite drept terminal securizat. În cazul în care PC-ul nu poate fi de încredere, asta se poate transmite și asupra cardului smart. Paradoxal, un motiv excelent pentru utilizarea ubicuă a cardurilor smart este că PC-urile nu pot fi de încredere. Raționamentul spune că este mai bine să stocăm secretele ca PIN-urile, datele personale sensibile și cheile private pe o cartelă inteligentă decât pe un PC. Astfel, în cazul în care PC-ul este compromis, secretele nu pot fi furate atât de ușor.

Cu toate acestea, rămâne problema de terminal. Spre exemplu, următorul scenariu descrie o situație foarte periculoasă. Dacă un atacator a reușit să pună stăpânire pe browser-ul Web al unui alt utilizator, fie prin sistemul de operare, fie prin datele de intrare (HTML) procesate, poate deturna fluxul de acțiuni al acestuia sau poate accesa informațiile sale confidențiale.

De exemplu, orice smartcard necesită un PIN înainte de a utilizare, pentru autentificare. Printr-o interfață de browser, utilizatorul este interogat pentru PIN și îl introduce cu încredere. Browser-ul este însă corupt și când vede codul PIN, îl stochează pentru a fi utilizat mai târziu ilicit. PC-ul este folosit ca un post de ascultare pentru a îndeplini un atac de tip captura și reproducere împotriva smart card. Aceste tipuri de atac adesea merg împotriva protocoalelor criptografice, cu excepția cazului în

[1] https://www.researchgate.net/publication/220335510_Authentication_protocols_based_on_low-bandwidth_unspoofable_channels_A_comparative_survey

care protocoalele sunt concepute special pentru a aborda această problemă. PC-ul fură cheia privată de pe cartela inteligentă și este în măsură să vă reprezinte "legal" cu semnătura digitală.

Ceea ce este necesar în acest caz este un terminal (display) de încredere. Unii cercetători au sugerează că PDA-urile precum 3Com PalmPilots ar putea servi ca afișaj securizat. Ideea este că PDA pot interacționa direct cu utilizatorul în timpul operațiunilor de securitate critice ca introducerea codului PIN. De fapt, PDA poate înlocui smartcard în întregime, deoarece acesta poate efectua cu ușurință toate calculele necesare. PDA-urile sunt, totuși, prea greoaie pentru această aplicație.

Cu toate acestea, în ziua de azi nu există multe argumente pentru a avea mai multă încredere într-un PalmPilot decât într-un PC. PalmPilot versiunile mai noi și alte PDA-uri sunt concepute pentru a lucra în rețea directă cu PC-urile, uneori chiar folosind o stivă TCP/IP. Asta este o veste bună dacă doriți să transferați date la și de la PDA, dar este foarte riscant. La fel ca un PC, un PalmPilot este, probabil, nesigur dacă descărcăm frecvent programe pe el, întrucât au apărut deja viruși pentru PalmPilots.

Problema cu terminalul este foarte greu de rezolvat. Cum tehnologia smartcard devine din ce în ce mai răspândită, cele mai susceptibile la această problemă vor fi interfețele bazate pe PC. Un sistem de operare Windows 95 nesecurizat și un browser web compromis nu ar trebui să fie de încredere pentru a afișa informații critice despre un utilizator de smartcard, așa cum se întâmplă în multe instituții. Un PDA este mai potrivit pentru acest lucru, dar poate avea și el riscuri similare.

2.2 Atacuri fizice

Atacul cel mai evident și mai direct asupra unui smartcard este, bineînțeles, un atac fizic pe card în sine. Pentru un card care stochează valori, acest tip de atac poate fi efectuat chiar de către proprietarul cardului. Atacurile fizice încerca să facă reverse engineering pe card și să determine cheile secrete. Astfel de atacuri s-au demonstrat în practică viabile împotriva chipurilor comerciale securizate, mai ales prin munca a trei grupe de cercetători: Dan Boneh, Richard DeMillo și Richard Lipton de la Bellcore; Ross Anderson din Cambridge și Marcus Kuhn de Purdue; și Paul Kocher și colegii de criptografie de la Research, Inc.

Boneh, DeMillo și Lipton, trei cercetători de la Bellcore, au publicat un document despre importanța protocoalelor criptografice în care au subliniat că un atacator care poate introduce erori de calcul într-un smartcard, poate deduce valorile cheilor criptografice ascunse în smartcard. Un atacator poate face acest lucru chiar și fără să controleze exact natura erorilor sau ordinea în care sunt generate. Prin compararea rezultatului unei criptări eronate cu rezultatul de la o criptare corectă pentru aceleași date, atacatorul poate învăța ceva despre cheia de criptare corectă. Dacă face destul de multe astfel de comparații, atacatorul poate învăța suficiente informații pentru a deduce cheia de criptare întreagă.

Există o mulțime de moduri ca un atacator să introducă erori în sistem. Atacatorul poate supune smartcardul la fluctuații de temperatură, tensiunea de intrare, sau viteza de ceas; iradierea smartcardului cu o sursă de radiație; sau lovit cardul cu un ciocan de cauciuc. Va fi suficient ceva care ar putea face ca tensiunile din interiorul cardului să fluctueze.

Mai târziu, Biham și Shamir au generalizat acest atac cu o tehnică numită Analiza Greșelilor Diferențiale, care funcționează împotriva unei game mai largi de algoritmi criptografici. Punctul de interes este că, în excepția cazului în care un mecanism de criptografie smartcard este proiectat foarte atent, cheile secrete stocate în interiorul cardului ar putea fi extrase de un atacator perseverent.

Într-o altă lucrare, Anderson și Kuhn indică faptul că "smartcardurile sunt rupte în mod obișnuit" și în măsura în care folosirea lor în siguranță necesită protecție fizică, aceste carduri "trebuie tratate cu circumspecție". Lucrarea descrie o serie de atacuri de smartcard, dintre care multe pot fi efectuate de atacatori amatori care dispun de resurse foarte limitate. Atacurile descrise includ manipularea tensiunii, manipulare temperaturii, dezasamblarea chipului eliminare (pentru a sonda mai ușor), atacuri cu lumină UV și micro sondare.

Atacurile mai complexe necesită echipament dedicat și materiale speciale cu care se pot descoperi substraturile circuitului integrat prin decapare, pentru a putea sonda stările prin care trece

elementul securizat, pe bază micro sondelor și ingineriei inverse. O concluzie sumbră ar fi că aceste atacuri vor putea fi mereu încercate de atacatori, iar companiile care proiectează aceste cipuri le pot dota cu mecanisme de securitate care să întârzie atacul, sau să îi crească eventualul cost, dar nu pot oferi 100% securitate. Companiile private care implementează sisteme cu smartcard cunosc acest lucru și fac tot ce pot pentru a gestiona riscurile prudent, iar utilizatorii privați ar trebui să se conformeze acelorași practici.

Merită precizat că aceste tehnici de atac au fost dezvoltate cu unele limitări. Studiul Anderson și Kuhn este oarecum învechit, dar principiile pe care le dezvoltă vor fi mereu de actualitate, pentru a fi implementate pe cele mai noi descoperiri tehnologice. Deși se bazează pe atacuri efectuate împotriva micro-controlerelor convenționale, care sunt, de obicei, mult mai simple decât cele de astăzi pe smart carduri, acestea se aplică și la cele securizate, încât acesta reprezintă doar un palier în modelul de funcționare. Microcontrolerele furnizează acces liber potențialilor atacatori deoarece sunt menite să fie programat interactiv. De exemplu, micro-controlere oferă adesea o interfață pentru memorii; în general vorbind, cartelele inteligente nu au această caracteristică. Astfel, ele oferă mai puține căi de comunicație pentru eventualele atacuri.

2.3 Differential Power Analysis

În 1998, cercetătorii de la Criptography Research, Inc, conduși de Paul Kocher, au anunțat public un nou set de atacuri împotriva smartcardurilor numit analiza diferențială de putere (DPA). DPA poate fi efectuată cu succes împotriva celor mai multe smart carduri aflate în prezent în producție.

DPA este un atac complicat, care se bazează pe concluzii statistice trase pe baza consumului de energie electrică măsurat în timpul calculului. Echipamentul necesar pentru a efectua DPA este simplu: un cititor de cartele inteligente modificat si un PC normal. Algoritmul în sine este destul de complex, dar detaliile au fost publicate pe scară largă.

Cipul la care ne referim are în interiorul său o cartelă inteligentă care folosește cantități diferite de energie electrică pentru a efectua diverse operații. Prin conectarea cardului la un osciloscop, putem măsura un model de consum de energie. Anumite calcule creează modele speciale de comportament în consumul de energie. O analiză atentă a vârfurilor de putere într-un model de consum de putere poate duce la descoperirea de informații despre cheile secrete utilizate în calculele criptografice. Uneori analiza este destul de simplă, întrucât o singură tranzacție oferă date suficiente pentru a fura o cheie. Mai des, mii de tranzacții sunt necesare. Tipuri de informații sensibile care se pot scurge includ codul PIN și cheile criptografice private. Figura 2 este o schema conceptuală a DPA.

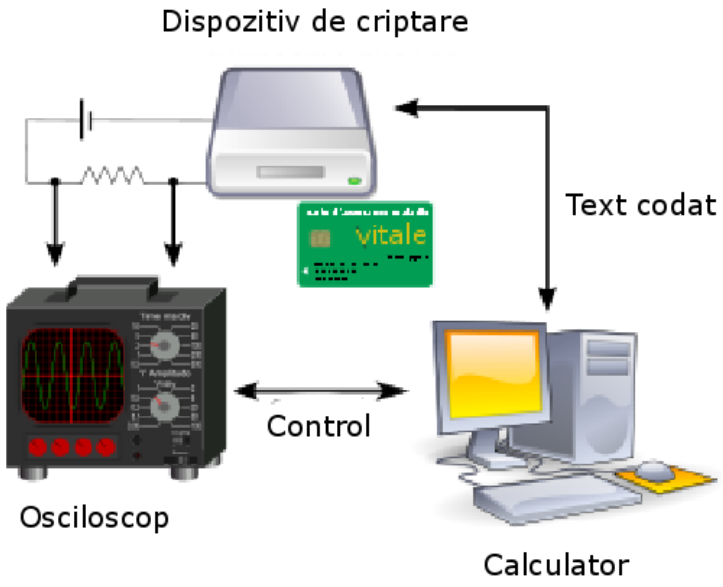


Figura 2. Analiza Diferențială a Puterii.

Soluții posibile contra acestui tip de atac includ mascarea consumului de energie cu zgomot digital sau efectuarea de calcule aleatoare. O altă soluție potențială este ordinea aleatoare în care cardul efectuează secvențe de calcule, astfel încât în cele din urmă, același calcul se efectuează utilizând modele diferite de primitive. Toate aceste potențiale soluții tehnologice sunt moduri de a masca un model care ne-ar da de gol în consumul de energie al cardului.

DPA este de fapt o variantă a atacului dezvoltat de Kocher. Anterioar, atacul exploata faptul că unele operațiuni necesită cantități diferite de timp pentru a termina, în funcție de care valori sunt de calculat. În același mod în care DPA permite unui atacator să adune laolaltă informații cheie bazate pe varianța în consumul de energie, Kocher permite unui atacator să adune laolaltă o cheie bazate pe variante în valoare de timpul necesar pentru a cripta diverse valori de calcul.

Utilizatorii legitimi de smartcarduri nu trebuie să își facă griji prea multe despre DPA sau atacuri programate, deoarece acestea necesită acces fizic la card în sine. Cu excepția cazului în care s-a pierdut cardul sau a fost inserat direct în mașină de un atacator, nu există amenințarea că cardul în sine va fi spart. Principalul risc pe care DPA îl prezintă este pentru companiile care trebuie să se preocupe de fraudă pe scară largă de genul celei efectuate de crima organizată.

Cea mai bună abordare este de a presupune că informațiile se vor scurge de pe cartelele inteligente și sistemele de design în așa fel încât să rămână sigure chiar și în fața scurgeri de informații. O abordare de acest fel pot exclude sisteme smart card concepute pentru a face toată prelucrarea offline, fără un server centralizat.

2.4 Obiective de securitate

O securitate acceptabilă există atunci când costul unui atac de succes este un ordin de mărime mai mare decât potențialul profit. Atingerea stadiului de securitate este o cursă contra-cronometru. Având la dispoziție suficient timp, efort și bani, orice soluție de securitate poate fi până la urmă compromisă.

Nivelul de securitate implementat trebuie să fie echilibrat în mod corespunzător pentru orice tranzacție care folosește date. Valorile datelor sunt protejate, ceea ce determină nivelul măsurilor de securitate care ar trebui să fie dislocate și robustețea de criptografie care ar trebui să fie utilizată. Numărul de aplicații care sunt dezvoltate pentru element securizat cresc, iar atacatorii își concentrează mai mult atenția pe tehnologie.

2.4.1 Tipuri de atacatori

Atacatorii de obicei se încadrează în unul din trei domenii:

- *amator*: amatorii sunt persoane curioase care efectuează atacuri doar pentru „*a vedea dacă se poate face*”;
- *expert*: atac efectuat de experți în domeniu sub auspiciile instituțiilor științifice și universităților care studiază tehnologia;
- *profesional*: cei care execută atacuri pentru recompense financiare sau pentru a obține date sensibile și a compromite un sistem.

IBM propune adoptarea unei taxonomii de atacatori care caracterizează o anumită măsură de comportament și resurse. Această taxonomie este prezentată mai jos:

Clasa 1: Outsideri inteligenți

Sunt de obicei foarte inteligenti, dar pot avea o cunoaștere insuficientă a sistemului. Pot avea acces la echipamente doar moderat sofisticate. Încerca să profite de o slăbiciune existentă în sistem, mai degrabă decât să încerce să creeze una.

Clasa II: Insideri cunoscători

Au formare tehnică specializată de substanță și experiență în domeniu. Au diferite grade de înțelegere a pieselor de sistem, dar nu și acces la cele mai multe dintre ele. Folosesc adesea unelte și instrumente de analiză foarte sofisticate.

Clasa III: Organizații finanțate

Sunt capabili să adune echipe de specialiști cu competențe complementare și conexe susținute de o mulțime de resurse de finanțare. Sunt capabile de a analiza în profunzime sistemul, de a proiecta atacuri sofisticate, și de a folosi cele mai avansate instrumente de analiză. Pot utiliza clasa II ca parte din echipa de atac.

Scopurile atacatorului sunt din cele mai variate, dar în principal pot fi împărțite în următoarele categorii:

i. obținerea cheilor de criptare din RAM sau ROM;
ii. aflarea algoritmului de criptare utilizat;
iii. obținerea altor informații stocate în cip (PINs);
iv. modificarea informațiilor de pe card (balanța de credit).

Atacatorii se presupune că au nivele diferite de experiență, resurse și motivație. Motivația de atacator poate include, de asemenea, recompense economice sau de satisfacție și notorietatea învingerii expertului de securitate. Expertiză relevantă poate fi în tehnologia de semiconductoare, inginerie software, hacking tehnic, sau în aplicații specifice smartcard.

2.4.2 Tipuri de atacuri

Atacurile sunt tehnici aplicate pentru a compromite un element securizat și de a descoperi informațiile pe care le deține. Atacurile pot fi clasificate ca atacuri de eroare, atacuri pe canale laterale sau atacuri invazive.

Atacurile de eroare modifică funcționarea internă a IC pentru a induce o eroare în funcționarea acestuia. Operația greșită va dezvălui informații despre cip atunci când se întâmplă.

IC are un set de senzori care controlează funcționarea IC (descrise la punctul 3.2.1), precum și operații logice redundante. În cazul în care IC este manipulat să funcționeze în afara parametrii de stabilizare a senzorilor, va merge în mod alarmă sau îi va fi împiedicată funcționarea completă.

Atacurile pe canale laterale sunt atacuri bazate pe informații obținute din tehnologiile folosite la implementare. De exemplu, calendarul de informații, consumul de energie, scurgerie electromagnetice sau chiar de sunet, toate pot oferi o sursă de informații care să fie exploatate pentru a sparge sistemul. Multe atacuri pe canale laterale necesită cunoștințe tehnice considerabile asupra funcționării interne a sistemului pe care este implementată criptografia.

Anumite contramăsuri în IC o poate descuraja de aceste atacuri, și anume:

- inserarea unei stări de așteptare random;
- confuzii pe magistrală și memorie criptată;
- verificarea continuă a caracteristicii aleatorii;
- curenți de codare sau stabilizare;
- reglarea voltajului;
- magistrală cu șină dublă, în cazul în care transmiterea datelor este trecută de pe o șină pe alta, pentru a induce atacatorul în eroare.

Atacurile invazive, cunoscute și ca atacuri hardware, încearcă să obțină acces neautorizat la informații pe IC. Exemple de atacuri invazive sunt probarea IC cu micro probe sau iradierea cu raze concentrate de ioni (FIB), inginerie inversă, și modificarea de circuit.

Anumite contramăsuri puse în aplicare în IC pot descuraja atacurile invazive:

- suport și criptare definite de utilizator de memorie de utilizator, RAM și ROM;
- utilizarea unei unități de gestiune a memoriei care să interzică cererile de accesare a datelor de către aplicații fără acea permisie;
- scut activ care face ca IC să se oprească atunci când este declanșat;
- geometrie IC de mici dimensiun (0,22 μm ca o dimensiune de maxim caracteristică) pentru a descuraja microprobing;
- confuzie pe magistrală și criptare de date;
- verificarea caracteristicilor aleatoare de IC;
- temporizare și design proprietar.

2.4.3 Modelul potențialelor atacuri

Pentru a evalua securitatea unui smartcard, avem nevoie de un cadru formal și riguros de parametri ca să modelăm matematic atacul și să îi evaluăm dificultatea. Clasificarea vulnerabilităților s-a dovedit dificilă în teorie și practică. În multe cazuri, sunt semnificative detalii precise asupra tipului de vulnerabilitate și metoda potențială de exploatare a acestora. Desigur că această informație nu poate fi cunoscută încă de la momentul evaluării, astfel încât se dovedește a fi dificil să dăm o valoare unică de rating corespunzătoare pentru toate testele de evaluare. Common Criteria (criteriile comune) este un framework ce definește un model de calcul pentru dificultatea unui atac, denumit "atac potențial".

Parametrii de model sunt descriși în ceea ce urmează:

- timpul scurs: acesta este timpul necesar pentru atac. Este puțin probabil ca un atacator să petreacă mai mult de 3 luni pentru a ataca un TOE (țintă de evaluare).
- expertiza: acesta este nivelul de cunoștințe generale și abilitățile pe care atacatorul trebuie să le posede pentru a efectua atacul.
- cunoștințe asupra TOE: acestea reprezintă cunoștințele pe care un atacator trebuie să le știe despre designul, arhitectura sau organizarea internă a cardului țintă (sau cip)
- acces la TOE: acesta este numărul de eșantioane de care are nevoie un atacator pentru a efectua un atac. Mai multe astfel de probe pot fi necesare pentru că unele atacuri presupun distrugerea unor mostre de card pentru a afla informații despre cip înainte de atac. Alte atacuri pot fi predispuse la deteriorarea cardului în timp ce atacul este realizată sau pot activa contramăsuri care vor dezactiva cardul după ce un anumit prag este atins. Numărul de probe se măsoară în praguri de 10, 100, sau mai mult de 100.
- echipamente: acesta este tipul de echipament necesar pentru a realiza atacuri la un smartcard și pot varia foarte mult de la un PC la un cititor de carduri, prin microscoape optice, osciloscoape digitale și lasere, microscoape electronice și stații cu raze concentrate de ioni.
- eșantion deschis: acesta înseamnă utilizarea de probe care sunt în mod deliberat mai slabe (vulnerabile) decât cardurile reale cu care are de-a face atacatorul. Slăbiciunea ar putea fi cunoașterea cheilor de criptare sau a altor valori secrete, capacitatea de a încărca aplicații pe cardul de testare, sau ar putea fi dezactivarea anumitor măsuri de securitate pe mostrele testate.

2.5 Securitatea circuitelor integrate

Securitatea IC are un aspect multi-dimensional. Nu există un mecanism unic de securitate care protejează complet împotriva spectrului larg de atacuri posibile. Prin urmare, designul unui element securizat și utilizarea sa într-un sistem trebuie să includă contramăsuri hardware, software și de sistem pentru protecția datelor și a tranzacțiilor. Securitatea ar trebui să fie parte integrantă în fiecare soluție de smartcard instalat. Este important să se ia în considerare puterea de securitate a platformei de IC selectate pentru orice aplicație de smartcard. Securitatea sistemului în ansamblu ar fi, de asemenea, sporită de alte măsuri puse în aplicare la nivel de sistem.

Microcontrolerele securizate pentru smartcard disponibile în comerț sunt concepute să funcționeze în medii ostile. Aceste circuite integrate sunt fortificate cu mecanisme concepute pentru a rezista la tentativele de a extrage datele confidențiale pe care le protejează elementul securizat IC.

2.5.1 Arhitectura microcontrolerelor securizate

Pentru a se apăra împotriva atacurilor, un IC securizat ar trebui să aibă o arhitectură care îi permite să reziste la toate tipurile de atac cunoscute. Fiecare producător de elemente securizate încorporează propriile sale caracteristici și module de securitate în arhitectura IC. Producătorul poate utiliza propria nomenclatură pentru module, dar acestea trebuie să se comporte identic sau similar în timp ce activează diferitele niveluri de protecție.

Laboratoarele independente de testare a securității pot verifica faptul că fiecare platformă specifică de IC securizate protejează în mod adecvat de la amenințări cunoscute și definite. Mulți producători de IC utilizează rezultatele științifice obținute de aceste părți terțe pentru a îmbunătăți și

a inventa noi contramăsuri, dar apare problema de a împărtăși descoperirile chiar cu concurența. Prin urmare, este mai bine să specificăm pericolele la care IC este capabil să reziste (și în ce măsură) decât de a specifica contracțiunea, așa cum este descris în secțiunea de mai jos. Specificarea contramăsurilor poate restricționa inutil selecția unui element securizat sau poate crește costul în timp ce nu oferă nici un beneficiu practic.

Figura 3 este o diagramă bloc a componentelor unui microcontroler securizat tipic pentru smartcard.

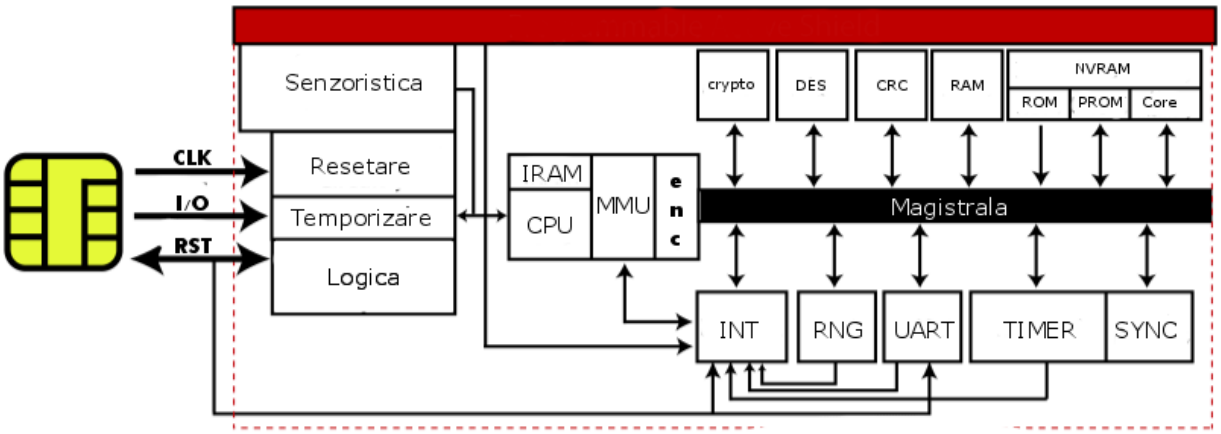


Figura 3. Componentele unui microcontroler securizat pentru smartcard

Toate componentele unui IC contribuie la conferirea aspectelor de protecție a sistemului împotriva atacurilor. În continuare, sunt trecute în revistă modalitățile prin care diferite componente participă la securitatea IC:

- un scut activ (active shield) programabil acoperă întregul IC și este echipat cu straturi de semnal care detectează tentativele de a sonda sau forța modulele interne sau liniile de semnal;
- o serie de senzori sunt înglobați în microcontroler pentru a contracara atacurile invazive sau de eroare, inclusiv:
  - senzori de mică și de înaltă frecvență pentru ceasul intern;
  - senzori și filtre pentru ceasul extern;
  - senzori externi pentru tensiune joasă sau mare;
  - senzori interni de tensiune;
  - senzori de temperatură;
  - senzori de vârf de tensiune;
  - senzori interni de tensiune (glitch);
  - senzori de lumină pe suprafața IC;
- circuitele interne de temporizare sunt folosite pentru criptografie;
- unitatea centrală de prelucrare (CPU) ar trebui să aibă temporizare proprietară pentru a îngreuna misiunea unui atacator de a determina operațiunile pe care le efectuează elementul securizat;
- unitatea de management al memoriei (MMU) este un modul opțional care creează un firewall hardware real pentru IC, îmbunătățind securitatea sistemelor de operare multi-aplicație pentru smartcard. Acest lucru este realizat prin prevenirea appleturilor de a accesa resurse importante ale chipului care trebuie să fie controlate doar de sistemul de operare al cardului smart. În timp ce această trăsătură sporește securitatea pentru platforme smartcard multi-aplicație, acestea nu sunt foarte utile în cazul în care cardurile execută o singură aplicație în mod curent, precum nici pentru sisteme de operare cu structura fixă pentru sistemul de fișiere;
- modulul de criptare pentru magistrala de memorie și procesor (ENCRPT) criptează și decriptează datele stocate folosind chei specifice stocate în ROM, RAM, și NVM și un algoritm simetric proprietar. În plus, magistrala RAM (care conectează RAM la procesor), de

asemenea, poate fi criptate după fiecare resetare a chipului. Aceste măsuri împiedică atacatorul să vadă orice calcule desfășurate pe IC în clar, în cazul în care operațiunile interne din IC sunt expuse atacatorilor. Registrele critice, modulul criptografic și celelalte periferice, de asemenea, sunt criptate;

- coprocesorul criptografic este un procesor suplimentare care executa algoritmi aritmetici, fie simetrici, fie asimetrici, precum 3DES, AES, RSA și criptografie de curbă eliptică (ECC). Aceste motoare de calcul descarcă operațiunile de prelucrare criptografică mai intensă de la CPU, și cresc securitatea prin aplicarea unor contramăsuri hardware. Astfel, aceste contramăsuri permite elementului securizat să funcționeze mai eficient și mai sigur;
- modulul de criptare Data Encryption Standard (DES) efectuează calcule specifice algoritmilor DES și Triplu DES;
- modulul de verificare a redundanței ciclice (CRC) verifică integritatea datelor pentru a vedea dacă a apărut o eroare în timpul transmisiei, la citire sau la scriere. Calculele CRC sunt standardizate în stratul de protocol; ISO/IEC 7816 pentru smartcarduri de contact, și ISO/IEC 14443 pentru smartcarduri fără contact (cu exemple de cod care arată cum sistemele gazdă trebuie să le implementeze);
- modulul de memorie non-volatilă (Memorie ROM, PROM și de utilizator) se asigură că datele sunt criptate pentru a împiedica atacatorul de a vedea datele în text clar, în cazul în care datele sunt extrase din IC;
- magistrala de date este criptată adică datele care sunt transmise de-a lungul ei sunt criptate, ceea ce face dificil pentru un atacator să determine ce este vehiculat. Toate datele transmise către și de la registrele de securitate relevante cu funcționalitate specială ar trebui să fie transmise prin această magistrală. Aceasta poate face scrambling și la adresele datelor transportate și transmise, ceea ce face schema de adresare mai obscură pentru atacator;
- generator real (și de calitate) de numere aleatoare (RNG) care este baza multor protocoale criptografice și care este, de asemenea, utilizat în conjuncție cu software-ul să întărească criptografia împotriva analizei diferențiale de putere (DPA) și analizei simple de putere (SPA);
- RNG poate fi folosit pentru a crea în mod arbitrar diferite stări de așteptare false care să încurce atacatorul atunci când încearcă să analizeze consumul de energie de pe cip. Cel mai important este ca numerele aleatoare să fie de calitate, pentru a proteja cheile de criptare atunci când sunt utilizate la operațiuni mutuale de autentificare și criptare. În aceste aplicații, numerele aleatoare sunt criptate, schimbate și apoi în cele din urmă folosite ca bază pentru cheile de sesiune care securizează tranzacțiile. Atacatorii nu pot ghici numerele aleatoare reale și, prin urmare, folosirea lor maximizează siguranța criptografiei;
- un dispozitiv care maschează curentul perturbă consumul de curent efectuând operațiuni extra de acces în memorie (ROM, XRAM și NVM). Ca urmare a acestei perturbări, consumul de curent al programului în execuție este ascuns. Atunci când este utilizat împreună cu RNG-ul și stările aleatoare de așteptare, această caracteristică este o contramăsură puternică împotriva analizei de putere.

2.5.2 Sisteme de operare pentru microcontrolere securizate

Microcontrolerele securizate au nevoie de un sistem de operare, pentru a permite execuția aplicațiilor care le populează. Sistemul de operare este încorporat pe IC în ROM în timpul procesului de fabricație. OS nu numai definește operațiunile de program pentru aplicații IC, dar de asemenea, include caracteristici de securitate software pentru a contracara atacurile de securitate și de a spori caracteristicile de securitate hardware. Aproape 50 la sută din codul OS într-un smartcard poate fi destinat pentru a sprijini caracteristicile de securitate. Dezvoltatorul software trebuie să fie bine informat despre arhitectura IC astfel încât sistemul de operare pot fi proiectate pentru a optimiza IC în mod de operare.

Viteza și performanța unui anumit procesor comparativ cu altul la rularea unei aplicații specifice ar trebui să fie întotdeauna judecat în cadrul unui OS securizat și a unor aplicații/appleturi

securizate (verificate independent de un laborator de încredere) pentru a ne asigura ca niciuna nu beneficiază de avantajul computațional conferit de lipsa de securitate.

2.5.3 Metode de testare a securității IC

În continuare prezentăm două platforme de testare ce pot fi folosite la gestionarea riscurilor de securitate generate de potențiale atacuri asupra smartcardului. Aceste platforme constau în teste de securitate pentru smartcard care pot fi aplicate, compuse din metode și instrumente software adecvate:

a. **JACARTA** este o platformă de evaluare a securității cardurilor smart pe bază de Java, dezvoltată de compania Brightsight. Are un instrument software care facilitează testarea, analiza si validarea de securitate și funcționalitate a produselor scrise în Java pentru smartcard. Aceasta va permite validarea diferite componente puse în aplicare pe un Java card prin standardele deschise care reglementează funcționarea acestor smartcarduri. Suita de testare este formată de metode de testare bazate pe specificațiile mediului de execuție care includ API-ul de smartcard, card de platformă globală și teste pentru programele Java într-o mașină virtuală. Acestea se aplică în mod iterativ, în următoarea ordine. În primul rând, instrumentul de testare este autentificat la smartcard printr-un protocol corespunzător. În al doilea rând, applet-ul de testare este încărcat pe smartcard și se demarează procedura de testare a funcționalității aplicației. Applet-ul apoi va răspunde la procesele de încărcare, instalare și eliminare, ce vor fi specificate de către Java smartcard. După finalizarea întregului test, instrumentul va genera un raport pentru rezultatul testelor. În cele din urmă, applet-ul se elimină de pe card. Prin urmare, instrumentul JACARTA nu doar se ocupă cu smartcarduri de standard unificat, dar, de asemenea, poate fi utilizat cu unele modificări de cod de program indicate de furnizorul aplicației.

b. **JCAT** este dezvoltat de LaBRI (Bordelais Laboratoire de Recherche) și poate rula în diferite medii de execuție. Acest instrument nu doar simulează atacuri hardware, dar și software. Cu JCAT se poate simula și radiație electromagnetică capabilă de a modifica conținutul celulelor de memorie de pe circuitul integrat, pentru a modifica în fapt anumite componente ale sistemului țintă. Simulatorul poate testa și executa programe pe smartcard și să verifice după atacuri intenționate. Este caracterizat prin completarea pas cu pas a acestei metodologii de testare, pentru a observa memoria, bufferele și stiva de execuție. Starea de analiză este furnizată în timpul procesului de implementare și vor include atacurile laser. Convertorul de JCAT convertește formatul de fișier CAP într-o altă formă, iar subcomponentele acestui sistem pot fi folosite pentru a modifica codul binar

3. INTERFAȚAREA ELEMENTELOR SECURIZATE

Nevoia de protecție a datelor într-un element securizat (IC, smart card) trebuie să fie balansată cu nevoia de a comunica cu IC și de accesul la date. În general, smartcardurile actuale nu pot afișa informații sau accepta direct intrări de la utilizator.

Pentru ca utilizator să acceseze informațiile conținute pe un smart card, are nevoie de o interfață pentru a comunica cu un cititor sau un terminal personal, un terminal de comerciant la punctul de vânzare, o bancă ATM sau un cititor de smartcard atașat la calculator.

Trei elemente sunt necesare pentru o cartelă inteligentă pentru a comunica cu lumea exterioară:

- sursă de alimentare;
- semnal de temporizare (ceas);
- transfer de date securizat către și dinspre smartcard

Datele pot fi transferate prin contact fizic, utilizând conexiunile electrice cu tampoane de contact de la suprafață smartcardului, sau fără contact (contactless), folosind transmisie prin radiofrecvență (RF). Transmisia de date fără contact este folosită des prin smartcarduri emise pentru aplicații cum ar fi bilete de transport în comun, carduri de acces și carduri de plată de debit si credit.

Cele două metode de transfer de date dau naștere la trei tipuri de cartele inteligente: carduri de contact cu o interfață de contact fizică, carduri contactless cu o interfață radio și carduri cu – interfață dual, care au atât o interfață de contact cât și o interfață contactless. Alegerea acestei interfețe depinde de cerere și de cerințele de afaceri, care trebuie să includă, de asemenea, considerente de securitate. Smartcardurile pot folosi fie module securizate de memorie sau microcontroler securizate, pe bază de circuit integrat.

3.1 Element securizat cu contact

Interfața de protocol a unui element securizat tip smartcard este standardizată prin ISO/IEC 7816-3, în timp ce legăturile sale fizice sunt standardizate prin ISO/IEC 7816-2. Un smartcard tipic este asamblat cu un IC livrate ca o plăcuță cu semiconductor, ambalate într-un singur modul și încorporate într-un card din plastic. Elementele componente sunt prezentate în figura 4.

Interfațarea cu exteriorul se realizează prin inserarea cardului într-un cititor de smartcard sau terminal astfel că modulul face o conexiune fizică cu tampoanele de contact ale dispozitivului de citire.

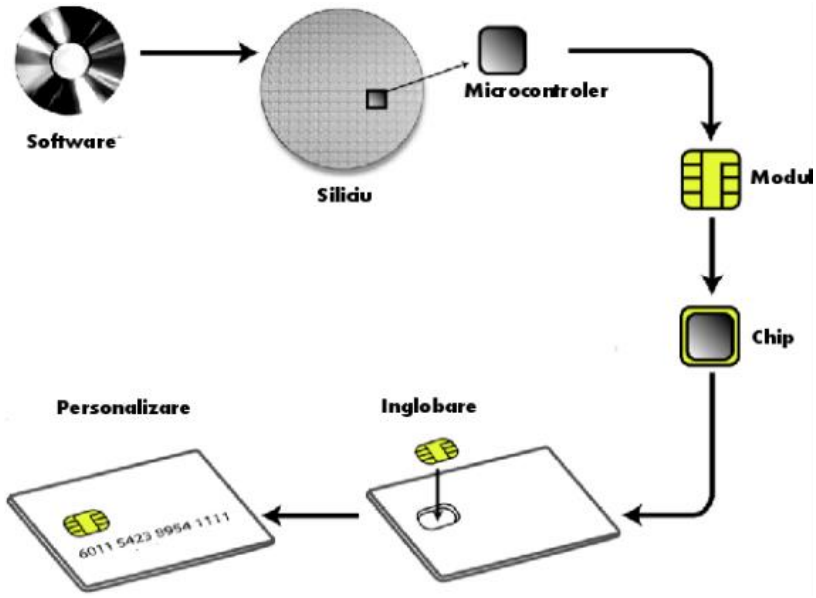


Figure 4. Elementele componente ale unui smartcard cu contact

În ultima vreme au început să apară smartcarduri cu display LED numeric care pot afișa (de exemplu) un cod de autorizare generat intern sau dotate cu un buton de activare care controlează dacă o anumită funcție este activă sau nu. Astfel de smartcarduri sunt în prezent complexe și costisitoare și nu au ajuns încă să fie comercializate în masă. De obicei, acestea conțin circuite suplimentare, cum ar fi circuite integrate și necesită o baterie ca sursă de putere pentru afișaj.

Dispozitivele securizate pe bază de IC (de exemplu, smartcard) pot veni într-o varietate de factori de formă, inclusiv carduri de plastic, brelocuri, manșete, ceasuri de mână, PDA-uri și telefoane mobile.

3.2 Elemente securizate fără contact fizic

Există două principalele diferențe dintre un smartcard cu contact și unul fără contact. În primul rând, nu există nicio conexiune fizică între cele contactless și dispozitivul de citire. În al doilea rând, alimentarea unui element securizat contactless este asigurată cu energie transferată de la cititor prin câmpul de RF și induce un curent electric în bobina de antenă a IC atunci când intră în raza de acțiune a câmpului RF produs de dispozitivul de citire (figura).

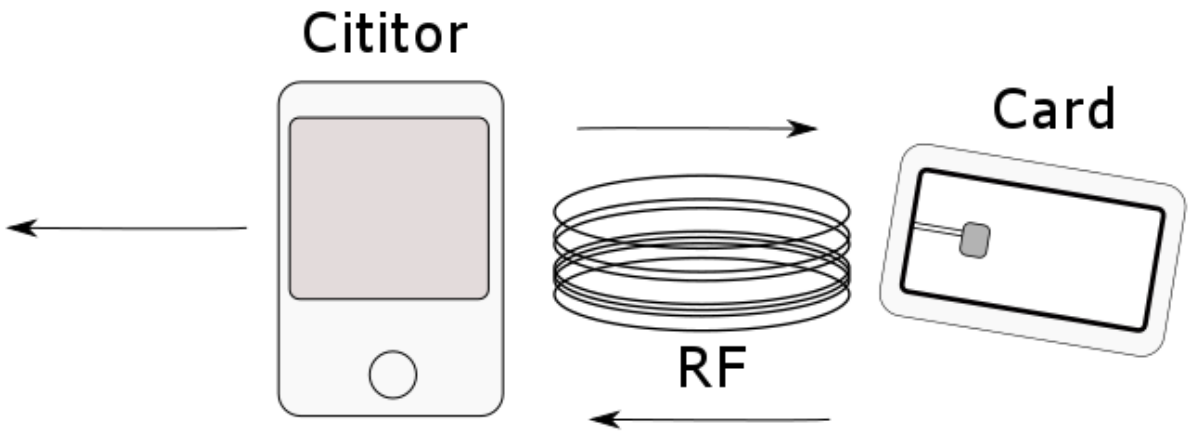


Figura 5. Carduri contactless în domeniu de RF

Modulul cu circuit integrat securizat este încorporat în card fără a fi expus la suprafața cardului gazdă. Acest modul are doar două contacte externe, spre diferență de cele cinci pe care le are un smartcard cu contact fizic, care se conectează la o bobină de antenă, încorporată și aceasta în card (figura 6).

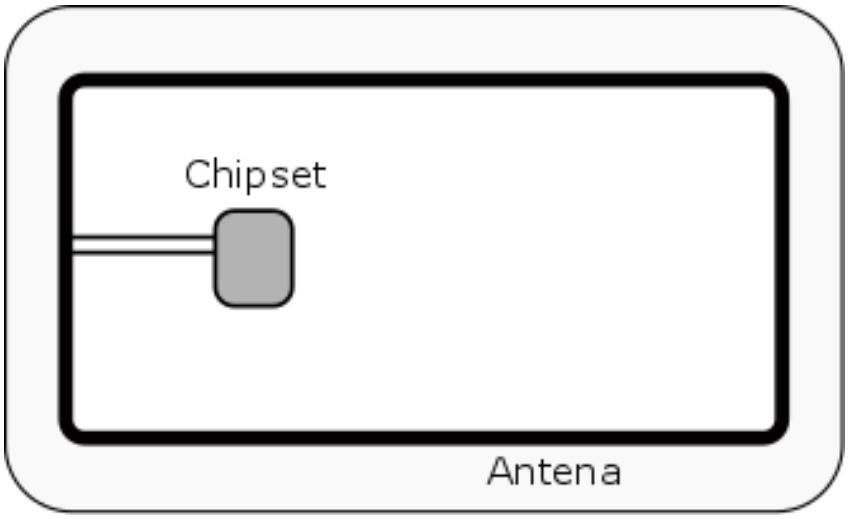


Figura 6. Elementele componente ale unui smartcard fără contact

Transferul de date cu un smartcard contactless este gestionat prin protocoale speciale, conform ISO/IEC 14443; cu toate acestea, caracteristicile de securitate și caracteristicile de protecție a datelor (pentru a proteja conținutul memoriei) sunt exact aceleași ca și în cazul smartcard cu contact. Singura diferență este modul în care datele sunt vehiculate cu exteriorul.

Un punct cheie de notat este că energia generată de câmpul RF al cititorului scade semnificativ odată cu distanța. Cu cât cardul este mai departe de cititor, cu atât mai mică este puterea disponibilă pentru a pentru a pune în mișcare IC-ul. Limita pentru alimentarea și comunicarea cu microcontrolerele securizate este undeva în intervalul de 5-10 cm față de cititorul de smartcard.

Recent s-a trecut la implementarea aplicațiilor contactless pentru plăți mobile folosind tehnologia de comunicare la apropiere (NFC), care respectă standardele universale ale ISO, ECMA International și Institutul European de Standarde în Telecomunicații (ETSI), în conformitate cu ISO/IEC 14443.

3.3 Element securizat cu interfață dual

Un smartcard cu interfață dual are atât o interfață de contact, cât și una fără contact. Din punct de vedere fizic, arată ca un card cu contact, dar modulul IC are și două puncte de contact suplimentare pentru bobina de antenă. Acest IC utilizează protocoalele ISO/IEC 7816 și ISO/IEC 14443 ca să comunice cu un dispozitiv de citire. Figura 7 ilustrează un astfel de smartcard.

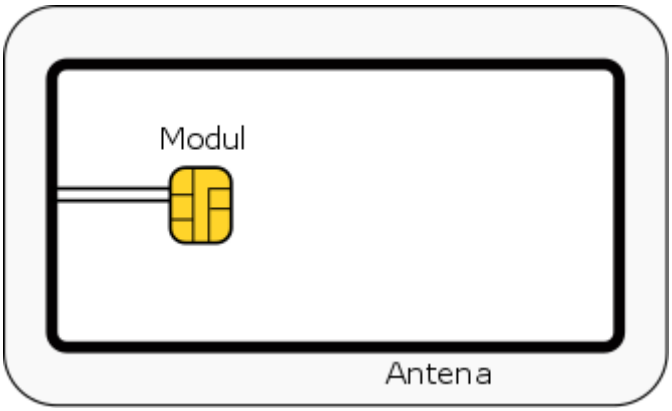


Figura 7. Smartcard cu interfață dual

Un card cu interfață dual poate fi necesară, de exemplu, pentru un card de tranzit, care necesită modul contactless pentru tranzacții rapide si trecere prin turnicheți, dar și modul de contact pentru a permite reîncărcarea fondurilor la un ATM sau terminal POS.

Putem considera un tip de smartcard cu interfață dual și un card hibrid. Acestea funcționează atât în mod contact cât și fără contact prin utilizarea circuitelor securizate separat pentru fiecare mod. Cardurile hibrid, deși se află încă în folosință, nu reprezintă o tehnologie de actualitate; au fost o soluție anterioară pentru a permite cardurile inteligente să opereze în mod contact și fără contact, care se poate realiza acum cu cele de interfață dual.

3.4 Securizarea sistemelor heterogene de smartcard

De ceva timp, percepția generală a fost că smartcardurile contactless sunt mai puțin sigure decât cele cu contact. Cu toate acestea, acest lucru nu este neapărat adevărat. Un card contactless este în mod inerent la fel de sigură ca un card de contact, întrucât sunt proiectate aceleași caracteristici de securitate într-un microcontroler securizat contactless ca într-un dispozitiv de contact. Tehnologia contactless nu prezintă mai multe vulnerabilități fundamentale decât tehnologie pe contact, dar constrângerile specifice și amenințările de securitate trebuie să fie luate în considerare și rezolvate la nivel de aplicație. Aceeași poziție oficială o are și Eurosmart, care folosesc elemente securizate cu

microcontroler cu caracteristici fizice de securitate destinate a proteja de manipulare și de clonare. Circuitele integrate securizate cu interfață dual trebuie să fie proiectate astfel încât operare nu prezintă riscuri de securitate, cum ar fi scurgeri de informații către persoane neautorizate. Din acest motiv, unele aplicații sunt concepute astfel încât ambele moduri pot nu fi operaționale în același timp. Cu toate acestea, au apărut cerințe recente care necesită funcționarea simultană, astfel încât, de exemplu, un telefon mobil poate continua cu comunicații de voce în timp ce este folosit și pentru a te autentifica printr-un punct de acces. Operațiunile duale nu reprezintă neapărat o amenințare de securitate. Cu toate acestea, cerințele trebuie să fie specificate în etapa de proiectare.

Există numeroase articole în mass-media care induc panică în populație referitor la interceptarea dispozitivelor RFID și a cardurilor de plată contactless. Cele mai multe astfel de articole confundă tehnologia RFID și tehnologia cardurilor contactless cu element securizat. În timp ce ambele folosesc RF, primul este conceput cu capacitate limitată de securitate și poate fi citit de la o distanță lungă, iar al doilea este conceput pentru a fi sigur și poate fi citit doar pe distanțe foarte scurte (maxim 10 cm).

Unele atacuri au ca scop specific interfața de date contactless:

- Eavesdropping: în care un atacator încearcă să intercepteze un card contactless valabil folosind un cititor alternativ;
- Activarea nedorită: care este similar cu interceptarea, în care atacatorul încearcă să activeze un card contactless autentic fără cunoștința proprietarului cardului;
- Denial of Service: în care atacatorul încearcă să interfereze transmisia RF, astfel încât sistemul nu funcționează și tranzacțiile nu pot fi completate corect;
- Man-in-the-middle: în care un dispozitiv de citire fals capturează date prin interceptarea transmisiilor și redirecționează informațiile către un card contactless fals conectat la un canal de comunicare alternativ, precum o legătură de frecvență ultra înaltă (UHF), care apoi comunică cu un cititor alternativ.

Astfel de atacuri pot fi împiedicate printr-un design bun al sistemului care utilizează autentificarea hard și criptografia dinamică. Utilizarea tehnologiei smartcard fără contact permite gestionarea sigură a datelor stocate și transmise folosind criptare puternică, provocări aleatoare, controlul la acces prin autentificare și, prin urmare, oferă contramăsuri împotriva atacurilor descrise.

Un design bun de securitate ține seama de cerințele de securitate și limitările unei aplicații încă de la început și identifică riscurile care sunt acceptabile. Așa cum este valabil pentru toate atacurile și amenințări, contramăsurile pot fi implementate, dintre care unele pot induce costuri suplimentare sau pot fi mai convenabile pentru utilizatori. De exemplu, un card contactless pot fi protejate prin includerea într-un manșon de protecție din metal, dar apoi cardul trebuie să fie extras de acolo pentru utilizare. Multe contramăsuri implică, în cele din urmă, realizarea unui compromis.

Atât în mediile de contact cât și în cele fără, smartcardul este doar o parte a întregului sistemului. Cum software-ul instalat pe card poate compensa limitările hardware și invers, măsurile de securitate externe cardului pot întări securitatea globală aplicației.

4. SECURIZARE HARDWARE vs SOFTWARE

În lumea digitală de astăzi, accesul la voce, video și date importante prin conexiuni tip cablu sau wireless devine ceva obișnuit. Portofelele electronice, aplicațiile de telefonie mobilă, și gestionarea drepturilor digitale (DRM) în legătură cu datele audio-video, precum și serviciile de streaming online sunt exemple pentru această tendință, care introduce un nou set de probleme de securitate. Astăzi, o arhitectura de securitate concepută în mod corespunzător creează o soluție de fiabilitate în care securitatea este executată atât hardware cât și software. Companiile trebuie să înțeleagă amenințările la adresa sistemelor specifice pe care le administrează, astfel încât acestea să poată dezvolta soluții care oferă dreptul la un nivel acceptabil de securitate. Este vorba nu doar de bazele de date ale băncilor și instituțiilor publice care sunt la risc; multe entități necomerciale stochează informații sensibile, care pot fi vândute sau încorporate în produse competitive, producătoare de venituri, iar acestea sunt de asemenea afectate. Compromiterea procedurii de autentificare poate permite accesul ilegal la rețelele și datele private de acest tip.

Sisteme de securitate software și hardware utilizează criptografia și cheile de criptare. Cheile private sunt folosite în software-ul care rulează pe platforme deschise (cum ar fi PC-uri sau servere) dar le lasă descoperite în fața atacurilor de inginerie reversibilă. Acestea pot fi apoi folosite pentru a compromite sistemul. Adăugarea unor componente hardware securizate, cum ar fi un microcontroler securizat, la un sistem de securitate software oferă un mijloc de a implementa, proteja și aplica aceste cheile într-un mediu securizat. Memoria protejată de utilizator deține cheile de criptare și este parte din același hardware ca nucleul principal, care include coprocesoarele aritmetice pentru criptografie, care și ele sunt protejate de atacurile de inginerie inversă descrise anterior. Cheile de sistem protejate în termenii microcontrolerelor securizate pot fi folosite pentru a obține chei de sesiune temporar dislocate din sistemele deschise gazdă, care au o capacitatea de procesare mult mai mare. În acest fel, un lanț de încredere este construit pe cheile de bază păzite de microcontrolere securizate, dar în cele din urmă sunt puse în aplicare de viteza de procesare a platformelor de calcul de ultimă oră.

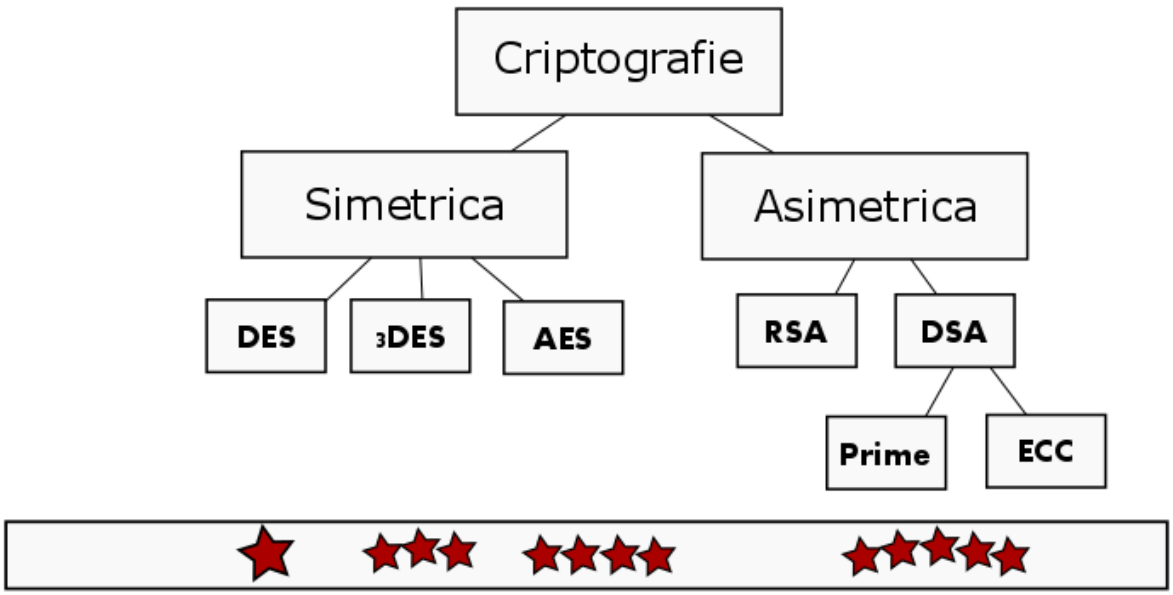


Figura 8. Cerințele unui algoritm criptografic

Combinația de securitate hardware și software trebuie să se soldeze cu o comunicare rapidă pe magistrală, capacitate de prelucrare semnificativă și utilizarea cheilor și aplicațiilor pentru atingerea scopurilor. De exemplu, dislocarea financiară la punctul de vânzare (POS) se face cu un sistem de chei și criptografie ca modul de acces securizat (SAM) și funcționează bine pentru a procesa rapid și sigur tranzacții folosind cantități diferite de date. În acest caz, SAM procesează toate

criptografia pe partea de tranzacție, precum autentificarea datelor statice (SDA) sau autentificarea datelor dinamice (DDA) folosind coprocesoarele DES/RSA înglobate. Un alt exemplu bun este utilizarea de către industria de cablu și satelit TV a smartcardurilor pentru a gestiona accesul clientului la programe plătite (pay-per-view). În acest caz, cartela inteligentă nu procesează în masă criptarea și decriptarea datelor audio și video, ci mai degrabă acționează ca deținător al cheilor de autentificare care permit securizarea execuției software-ului pe dispozitivul gazdă (received). Cartelele inteligente nu doar simplifică implementarea cheilor care să permită aceste aplicații foarte diferite, dar face acest lucru în timp cu gestionarea costurilor. Microcontrolerul securizat asigură securitate la nivel de sistem în circuitele integrate mai puțin costisitoare, care nu necesită magistrale de viteză mare (precum interfața serială periferice (SPI) și magistrală serială universală (USB)) și înlocuiește măsuri software/hardware de securitate costisitoare de altfel necesare pentru a securiza funcționarea sistemelor și dispozitivelor electronice.

Utilizatorii acestor controlere determină ce rutine de criptografie trebuie folosite, pe baza cerințelor aplicației și vor pune în aplicare elementele de securitate folosind propriul lor sistem de operare și software-ul de aplicație. Figura 8 ilustrează modul în care poate fi realizată securitatea la o gamă largă de opțiuni pentru criptografia simetrică și asimetrică.

5. NIVELURI de SECURITATE

Un smartcard este doar una din componentele care contribuie la punerea în aplicare un sistem de calcul. Mecanismele de securitate pot fi implementate în card și în OS, la nivel software și la nivel de sistem.

Trebuie o viziune holistică asupra securității unei aplicații întrucât nici un mecanism unic nu oferă securitate completă. În schimb, obiectivul devine ca timpul și efortul necesare pentru a compromite un sistem să nu ofere vreun câștig atacatorului. Riscul la care e supus sistemul trebuie să fi egalat cu contramăsuri de securitate pentru a reduce expunerea la un nivel unde considerăm că riscul poate fi tolerat. Când dezvoltăm un sistem bazat pe smartcard, contramăsurile menite să protejeze datele trebuie să includă caracteristici hardware, software, și de sistem. Această combinație de mecanisme de securitate este denumită „*niveluri de securitate*”

Deciziile asupra nivelurilor de securitate pe care trebuie să le ia un emitent și tipul de măsuri de securitate care ar trebui să fie implementate într-o aplicație ce rulează pe un sistem bazat pe smartcard trebuie să echilibreze riscurile sau amenințările pe care emitentul se așteaptă să le întâlnească față de costurile de implementare a elementele de securitate, dar și impactul pe care aceste caracteristici le pot avea la utilizarea smartcardului. Nu toate aplicațiile necesită același nivel de securitate. Cerințele de securitate ale aplicației trebuie să fie definite atunci când un sistem este proiectat astfel încât emitentul să selecteze tehnologia și abordarea corespunzătoare pentru punerea în aplicare.

5.1 Noțiuni generale de securitate

Mecanismele de securitate sunt implementate în întregul sistem. Progresele tehnologiei IC permite ca multe caracteristici de securitate să fie implementate la nivelul IC. Aceste caracteristici sunt concepute pentru a proteja conținutul memoriei IC și pentru a preveni sau contracara orice atacuri. Sunt de asemenea disponibile și contramăsuri suplimentare care sunt proprietare producătorilor individuali, deci tehnologia pe care sunt construite rămâne confidențială.

Unele atacuri sunt concepute pentru a exploata caracteristicile fizice ale siliciului circuitului integrat, bazându-se pe limitările sale fizice. Un exemplu de un astfel de atac este atacul de analiza a puterii (DPA sau SPA). Producătorii IC au pus în aplicare funcții speciale pentru a încurca atacatorii și a-i împiedica să obțină datele critice. Mai mult, prin adăugarea unui strat de securitate software în sistemul de operare, operațiunile fizice (electronice) pot fi mascate chiar și mai departe, întărind semnificativ aceste contramăsuri de securitate.

Lucrând împreună, dezvoltatorii de hardware și software pot crea straturi suplimentare de securitate, care ar putea consolida datele pe orice element securizat. Software-ul întărește hardware-ul și vice-versa, astfel încât rezultatul final este un produs mult mai sigur.

Pentru a proiecta un sistem securizat cu smartcard, proiectantul trebuie să privească dincolo de elementele securizate ca și circuite integrate. În cazul în care un card este compromis, proiectantul sistemului trebuie să se asigure că securitatea întregului sistem nu este pusă în pericol. De exemplu, accesarea conținutului unei zone de memorie securizate nu ar trebui să dezvăluie orice cheie de criptare sau master, care sunt utilizate în întregul sistem. Spargerea unui card nu ar trebui să ofere posibilitatea de a sparge și altele. Mai multe mecanisme pot fi încorporate în cadrul sistemului care vor permite îmbunătățiri suplimentare de securitate în timp ce cardurile circulă cu sau fără voia proprietarului. Un exemplu de astfel de metodologie este de a popula firmware-ul IC cu mai multe chei criptografice. Cheile ar putea fi schimbate la întâmplare sau la intervale definite pe baza unui număr de tranzacții sau un criteriu de interval de timp. O altă modalitate de îmbunătățire a securității sistemului este de a permite sistemului de operare să accepte downloaduri securizate care ar permite ca noi rutine de securitate să fie adăugate la IC, după necesități. Sistemul ar putea avea, de asemenea, o suită de caracteristici de securitate care sunt controlate de sistemul de back-office al emitentului.

Un exemplu relevant pentru a construi niveluri suplimentare de securitate într-un astfel de sistem pot fi găsite în sistemele globale de plată implementat de industria financiară.

5.2 Industria plăților financiare

Industria plăților financiare a proiectat mai multe straturi de securitate în tradiționalele cărți de credit și la sistemele de plată în debit pentru a proteja toate părțile implicate într-o tranzacție de plată. Cele mai multe dintre aceste măsuri de protecție sunt independente de tehnologia folosită pentru a transfera informațiile de cont de plata la cardul de plată sau la dispozitivul de la comerciantul POS terminal și sunt utilizate atât pentru benzi magnetice, cât și pentru tranzacții contactless. De exemplu, autorizarea online, managementul riscului și sistemele de detectare a fraudei sunt folosite pentru a detecta activitatea potențial frauduloasă de tranzacții de plată. În plus, firmele de plăți au răspundere legală, ceea ce protejează consumatorii folosind tradiționalele conturi de consum.

5.2.1 Securizarea plăților contactless

Industria financiară a adăugat tehnologie de securizare a sistemelor de plată pentru a preveni frauda la plăți fără date de contact; aceste măsuri de securitate sunt puse în aplicare atât pe dispozitivul contactless, cât și în rețeaua de procesare și în sistem.

În timp ce implementările diferă de la emitent la emitent, cele mai populare măsuri de securitate care sunt utilizate sunt:

- *la nivel de card*, fiecare card contactless poate avea propriile sale "chei secrete" unice built-in care utilizează tehnologie standard de criptare pe 128-biți pentru a genera o valoare de verificare unică a cardului (de exemplu, CVV sau CVC) sau o criptogramă care identifică exclusiv fiecare tranzacție. Două cărți nu împărtășesc aceeași cheie, iar cheia nu este transmisă niciodată;
- *la nivel de sistem*, rețelele de plată au capacitatea de a detecta și respinge automat orice încercare de a utiliza aceleași informații de tranzacție de mai multe ori. Astfel, chiar dacă cineva ar putea "citi" informații dintr-o tranzacție contactless sau chiar mai multe tranzacții din aceeași carte, informațiile ar fi inutile pentru reutilizare;
- *plățile contactless* nu au nevoie ca numele deținătorului cardului să fie schimbat între card și terminal. De fapt, cele mai bune practici în cadrul industriei nu includ stocarea numele deținătorului cardului în elementul securizat;
- *unele carduri și dispozitive contactless de plată* nu includ numărul de cont al deținătorului de card, dar utilizează un număr alternativ, care este asociat cu un cont de plată de sistemul de prelucrare back-end al emitentului. Acest număr alternativ nu poate fi utilizat la alte tranzacții de plată (de exemplu, cu un card de bandă magnetică sau pe Internet).

5.2.2 Securizarea plăților EMV

Când discutăm despre securitatea smartcardurilor la plățile financiare, este necesar să luăm în considerare impactul pe care l-a avut introducerea de carduri de plată EMV în lume. EMV cu smartcard a fost introdus în Europa, Asia, America Latină, Canada, cu obiectivul de a reduce frauda. Microcontrolerele securizate folosite în cărțile EMV de credit și debit a permis industriei de plată să pună în aplicare caracteristici de securitate în afara celor disponibile pe carduri cu bandă magnetică, cum ar fi următoarele:

- *card de autentificare*, care permite unui POS terminal să utilizeze criptografia ca să determine dacă un card este autentic. Sunt folosite trei tehnici: autentificarea datelor statice (SDA),
- *autentificare dinamică de date (*ADD), și generarea combinată a criptogramei pentru datele de autentificare/execuție (CDA)
- *verificarea cardului*, care permite titularului cardului să utilizeze un număr personal de identificare (PIN) (în cazul în care nu este compromis) pentru a confirma faptul că titularul cardului valabil este prezent.

Caracteristicile microcontrolerului securizat de pe cardurile EMV poate îmbunătăți, de asemenea, controlul pe care îl avem asupra tranzacției autorizare bazate pe comportamentul de cheltuieli al utilizatorului cardului. Microcontroler poate susține tranzacții offline și să decidă singur când să treacă online, în loc să se bazează strict pe limitele impuse de comerciant. Mai mult:

- circuitele integrate pot fi blocate împotriva utilizării printr-un mesaj online de la emitent;
- contoare 1-N pot decide cât de multe tranzacții pot apărea fără autorizare online. Această caracteristică poate limita numărul de tranzacții care apar mai jos de limita de credit a deținătorului de card;
- un contor de valoare poate urmări valoarea cumulată cheltuită între autorizațiile online, și poate declanșa o autorizația online sau poate preda controlul emitentului

Dacă microcontrolerul securizat de cardul EMV este folosit pentru a verifica titularul cardului și cardul în sine, cele mai multe fraude personale pot fi eliminate, inclusiv fraudă referitoare la pierdutul sau furatul cardurilor, carduri care nu au fost niciodată primite prin poștă și carduri contrafăcute. Cardul pot fi autentificat prin verificarea faptului că acesta nu a fost modificat folosind un algoritm de criptare programat de emitent în IC. Acest proces poate fi efectuat offline între card și terminal.

Identitatea titularului cardului poate fi, de asemenea, validată prin utilizarea unui cod PIN sau a altor metode care sunt definite în specificația EMV. Pentru validarea PIN, procesul verifică că PIN-ul introdus de titularul cardului se potrivește cu PIN-ul criptat de pe elementul securizat al cardului EMV. Contoarele pot preveni încercări repetate de a ghici un PIN și folosirea cardului pe blocuri.

Utilizând microcontrolere securizate, smartcardurile EMV previn fraudele cauzate de criminali care încearcă să șterpelească informații de pe banda magnetică a cardurilor de credit sau debit sau prin stamparea de numere pe cardurile contrafăcute.

Disponibilitatea certificatelor de tranzacție și semnăturilor digitale pentru carduri de plată EMV poate reduce frauda la comerciant prin utilizarea criptografiei pentru tranzacții non-repudiere și certificate. EMV, de asemenea, permite emitentului să utilizeze script-uri pentru a modifica elementele de date (cum ar fi parametrii de risc sau PIN-ul) pe o cartelă inteligentă EMV în timpul tranzacțiile online.

Pentru a sprijini tranzacțiile online, emitenții sunt obligați să primească date suplimentare referitoare la IC în mesajul online și să răspundă achizitorului, deci, prin urmare, aparatului, cu date suplimentare ca răspuns. Aceasta include autentificarea folosind criptogramei pentru cerere de autorizare (ARQC) și criptogramă cu răspuns de autorizare (ARPC) într-un proces cunoscut ca autentificare reciprocă online (OMA).

5.2.3 Alte implementări

În plus față de plățile de credit și de debit, smartcardurile securizate sunt utilizate pentru alte aplicații de plată (de exemplu, tranzit) și pentru implementarea accesului pe bază de identitate. Pentru orice implementare de sistem smartcard, straturile de securitate trebuie să fie puse în aplicare și abordările pentru punerea în aplicare trebuie definite de către emitent sau de la nivelul industriei:

- e-Passports sunt IC smartcard contactless cu microcontroler securizat. Organizația Aviației Civile Internaționale (OACI) definește specificațiile pentru documentele de călătorie, ce poate fi interpretată electronic (MRTDs), inclusiv e-Passport, cu țări emitente care implementează diferite niveluri de securitate adecvate pentru cetățenii lor;
- industria de tranzit folosește elemente securizate contactless la nivel mondial ca mijloc de plată a tarifului în sisteme de colectare automată. Practicile de securitate de obicei folosite în sistemele de plăți de tranzit sunt determinate de către autoritatea emitentă de tranzit;
- guvernul american emite carduri smart de identificare tuturor angajaților și contractorilor, care se bazează pe standardele Institutului Național de Standarde și Tehnologie (NIST): Standardul de Prelucrare a Informațiilor Federale 201 (FIPS 201), Verificare Identității Personale a Angajaților și Contractorilor Federali (PIV) și FIPS 140-2 despre cerințele de securitate pentru modulele criptografice.

Aplicațiile cu smartcard pot implementa, de asemenea, factori de autentificare suplimentară (ex., un cod PIN sau biometrice) pentru a lega și mai bine proprietarul cu cardul și pentru a asigura că numai titularul autorizat al cardului îl poate utiliza.

O altă organizație importantă din industrie este GlobalPlatform. Obiectivul principal al GlobalPlatform este stabilirea, menținerea și adoptarea specificațiilor pentru a permite o

infrastructură deschisă și interoperabilă pentru carduri inteligente, aparate și sisteme, pentru a simplifica și accelera dezvoltarea, implementarea și gestionarea de aplicații pe mapamond.

GlobalPlatform dezvoltă modele și convenții necesare pentru a facilita aplicarea Eco-industriei de încărcare și management, precum sistemele de back-end pentru carduri, securitate, chei de management și implementarea aplicațiilor.