Pametna kartica
(Smart Card)

Aleksandar Jurišić
Department of Combinatorics and Optimization
University of Waterloo, Waterloo, Canada, N2L 3G1
&
Certicom Corp., Mississauga

Alenka Trojar
School of Business and Economics
Wilfrid Laurier University
Waterloo, Canada

20. januar, 1997

Abstract

Smart cards provide the degree of security necessary to make computer networking truly viable. They unify telecommunications and computing. After a brief historical overview of the developement of cards, we survey three basic types of memory cards, in order to better understand the advantages of smart cards. The security aspects of smart cards are illustrated by two examples. Applications of smart cards are surveyed and a view for their future possibilities is given.

Povzetek

Pametne kartice nudijo stopnjo varnosti, ki je potrebna, da računalniške mreže zares zaživijo, ter združijo telekomunikacije in računalnike. Po kratkem zgodovinskem pregledu razvoja kartic sledijo opisi treh spominskih kartic, ki pripomorejo k boljšemu razumevanju prednosti pametnih kartic. Z dvema primeroma so opisani aspekti varnosti in zaščite pametnih kartic. Seznanimo se tudi z osnovnimi komponentami in karakteristikami pametnih kartic. Sledi pregled številnih aplikacij pametnih kartic in njenih možnosti v prihodnosti.

VSEBINA

1 Uvod

Večina ljudi ima danes vsaj eno kreditno kartico. V mnogih deželah uporabljajo tudi telefonske kartice, kartice za avtomate, zdravstvene kartice in še mnoge druge. Današnja tehnologija lahko vse te kartice nadomesti s kartico, ki ima različne funkcije in zagotavlja visoko varnost lastniku ter računalnikom, s katerimi kartica komunicira. Taka kartica se imenuje pametna kartica (*Smart Card*) in se poskusno uporablja po vsem svetu. Ima enako velikost kot običajna kreditna kartica in vsebuje eno ali več tiskanih vezij s funkcijami procesorja, spomina in vhodno/izhodne enote. Pametna kartica nam bo omogočila, da bomo kmalu nosili računalnik kar v žepu. S temi lastnostmi bo pametna kartica postala ključna možnost za varno shranjevanje ter izmenjavo podatkov in bo izboljšala varnost računalniških sistemov.
Osnovne funkcije pametnih kartic so:

- prenašanje podatkov (pametna kartica omogoča varen način shranjevanja in prenašanja podatkov ter varen dostop do informacij),
- identifikacija lastnika kartice (pametna kartica prepozna lastnika in onemogoči, da bi kdo prevzel njegovo identiteto),
- nadomestilo za denar ter varno izvajanje finančnih transakcij.

Po kratkem zgodovinskem pregledu v 2. poglavju sledijo opisi treh spominskih kartic, ki pripomorejo k boljšemu razumevanju prednosti pametnih kartic. V 4. poglavju so opisane prednosti pametne kartice na področju varnosti in zaščite z dvema primeroma. V 5. poglavju pa se seznanimo z osnovnimi komponentami in karakteristikami pametnih kartic. Tehnični del članka je zaključen z opisom sistema pametne kartice. V 7. poglavju je podan pregled številnih aplikacij pametnih kartic, v 8. pa njene možnosti v prihodnosti.

Slika 1: Dimenzije kartice in lega kontaktov so določeni s standardom ISO 7816.

2 Kratka zgodovina

Desetletja so uporabljali papirnate kartice (vizitke) z imenom, priimkom in naslovom za osebno predstavitev in za krajša sporočila. Leta 1930 so se pojavile plastične kartice, ki jih je bančna industrija začela uporabljati kot kreditne kartice. Diner's Club in American Express sta predstavila prve take kartice v 50-ih letih. 1967. leta so začeli plastičnim karticam dodajati magnetni trak. Kasnejši standardi pa so omogočili, da je uporaba magnetne kartice postala mednarodna.

Z razvojem računalnikov in komunikacijskih sistemov v zadnjih 20-ih letih je postala potreba po učinkovitem in varnem komuniciranju vedno nujnejša in pomembnejša. Konec 70-ih let je Francoz Moreno prijavil patent – čip, vgrajen v kreditno kartico. Tako pametno kartico je mogoče programirati za različne funkcije in jo usposobiti za kontrolo dialoga z zunanjo enoto. Sredi 80-ih let so v Angliji in ZDA razvili kontaktne in brezkontaktne pametne kartice in začeli razvijati njihove standarde. V svetu pametnih kartic pa je kritična prav standardizacija. Kartice različnih proizvajalcev morajo imeti usklajeno interakcijo z računalniki. V naslednjih petih, desetih letih pričakujemo nagel razvoj aplikacij za pametne kartice, vse dokler ne bodo pametne kartice zares postale računalnik v našem žepu.

Slika 2: Pametne kartice so rezultat paralelnega razvoja mikroprocesorja in magnetne kartice.

3 Vrste spominskih kartic in primerjava s pametnimi karticami

Trg kartic je trenutno preplavljen s klasičnimi (magnetnimi) karticami ter različnimi novimi karticami. Da bi lažje razumeli prednosti pametne kartice in njeno potencialno tržišče, bomo najprej opisali značilosti pasivnih (spominskih) kartic, ki so trenutno najbolj v rabi. Pasivne ali spominske kartice se uporabljajo predvsem za shranjevanje podatkov. Delimo jih v tri skupine: magnetne kartice, optične kartice in čip kartice.

(a) Magnetne kartice

Zaradi vse večje potrebe po avtomatizaciji v bančni industriji so dodali plastični kartici magnetni trak. Le-ta deluje podobno kot avdio trak za snemanje; nekateri trakovi imajo tudi "samo-piši" (*read-only*) del, kar pomeni, da lahko informacije samo beremo, ne pa tudi spreminjamo. Kljub temu pa je varnost te kartice pomanjkljiva, saj je magnetni trak izredno lahko posneti in kartico ponarediti. Pomanjkljivost kartice je tudi majhen spomin (manj kot 900 bytov). Vseeno pa je magnetna kartica trenutno najbolj razširjena zaradi nizkih stroškov proizvodnje ter spominske zmogljivosti, ki zadošča za preproste aplikacije.

(b) Optične kartice

Glavna značilnost optične kartice je, da vsebine kartice ne moremo izbrisati. Te kartice delujejo na "piši-enkrat" (*write-once*), "beri-večkrat" (*read-many times*) osnovi. Za branje in pisanje na kartico se uporabljajo laserji, ki izžgejo milijon drobnih luknjic v tanek list optičnega traku (mesto z luknjico ali brez nje predstavlja stanje bita). Optična kartica ima izredno veliko spominsko zmogljivost, saj nanjo lahko spravimo že od 2 do 8MB podatkov. Zaradi te lastnosti se je kartica izkazala predvsem v zdravstvu in netiskanih publikacijah. V primerjavi s pametno kartico ima optična kartica prednost predvsem zaradi velikega spomina in nizke cene.

(c) Čip kartice

Razlikujemo dve vrsti čip kartic, spominske kartice ter pametne kartice. Spominske čip kartice imajo običajno manj spomina kot pametne kartice ter lahko izvajajo manjše logične operacije s pomočjo integriranih vezij. Vendar pa te kartice nimajo inteligence v smislu procesorja in jih zato ne moremo ponovno programirati. Čip kartice se uporabljajo predvsem za telefonske kartice.

Zadnja noviteta na trgu kartic je čip kartica z obsežnim spominom (do 32MB). The Personal Computer Memory Card Industry Association (PCMCIA) je standarizirala izdelke v velikost kreditne kartice, z izjemo debeline. Uporabljajo se predvsem za povečanje spomina v prenosnih računalnikih ter prenos podatkov.

Novi materiali (plastika) in značilnosti (magnetni trak, površina na optičnih karticah, čipi) so izredno povečali trg kartic. Po nekaterih ocenah se uporablja že tri milijarde različnih kartic. Prednost varnega komuniciranja dela kartico vse bolj konkurenčno v finančnih aplikacijah. Pametna kartica stane od manj kot 1 do 20 ameriških dolarjev (USD), medtem ko stanejo optične kartice od 4-8 USD, magnetne kartice pa stanejo 10-50 centov, glede na to, ali vsebujejo sliko, hologram. Čeprav je cena pametnih kartic višja od cen drugih kartic, so jih nekatere dežele (Anglija, Japonska, Francija, Nemčija) pričele uvajati. Uporaba pametnih kartic raste in trend se bo verjetno še povečal, ko se bodo znižali stroški proizvodnje.

4 Zakaj pametne kartice

Ker večina ljudi še vedno uporabja magnetno kartico, bomo podrobneje razložili, zakaj bo pametna kartica nadomestila magnetno kartico. Za razliko od pametnih kartic so magnetne kartice povsem pasivne (uporabljajo se v glavnem za hranjenje podatkov). Magnetna kartica dopušča različne oblike zlorabe, na primer prekoračitev računa, saj večina nakupov ni takoj zapisana v glavnem računalniku (off-line sistemi se vedno bolj uveljavljajo).

Tudi ponarejanje in kopiranje magnetnih kartic ni redek pojav. Metode so ponavadi zelo rafinirane. Mogoče je kopirati informacije z magnetnega traku na prazno kartico in vtisniti podatke z originalne kartice.

zaslon
vložišče za kartico
meni
izpisek
vložišče za kuverte
dvig denarja
glavna tipkovnica
odpadki
polog denarja
kuverte

Slika 3: Bankomat

Kadar uporabljamo magnetno kartico v bankomatu, le-ta najprej "vpraša" lastnika kartice za geslo in ga pošlje glavnemu računalniku v banki skupaj z zakodiranim geslom z magnetnega traku. Računalnik zakodira še vtipkano geslo in opravi primerjavo (glej sliko 4).

primerjava

primerjava

Slika 4: Primerjava gesel

Geslo potuje po linijah nezaščiteno in tako lahko nekdo, ki prisluškuje povezavi med bankomatom in računalnikom ali pa ima dostop do gesel na glavnem računalniku v banki, geslo ukrade.

Pametna kartica ima dve značilnosti, ki onemogočata zgoraj omenjene zlorabe in ponarejanje. Ena od teh je non-volatile spomin, tj. spomin, ki se ga ne da spreminjati in se ohrani tudi po prekinitvi napajanja. Ta spomin lahko vsebuje tudi informacije, ki so bile zapisane po tem, ko je bila kartica izdana, in lahko zabeleži vsako transakcijo. S tem prepreči lastniku, da bi prekoračil svoj limit. Druga značilnost pa je, da procesor kartice kontrolira vse interakcije med različnimi zunanjimi enotami, ki berejo kartico in pišejo nanjo, in spominom pametne kartice. Ta je oblikovan tako, da so določeni deli spomina fizično in logično dostopni le izdajatelju kartice.

Naslednja dva primera kažeta, zakaj sta omenjeni značilnosti tako pomembni za zagotovljanje varnosti pri identifikacijskem procesu. Ta je opravljen v dveh delih: najprej mora biti kartica prepričana, da jo uporablja njen lastnik, nato pa komunicira (varno) z glavnim računalnikom.

Oglejmo si bolj podrobno, kako lahko lastnik dokaže svojo identiteto kartici. Recimo, da podjetje hrani svoje informacije v glavnem računalniku, ki je dostopen s pomočjo pametnih kartic. Le-te so izdane zaposlenim, ki imajo dostop do računalniškega sistema. Vsaka kartica je programirana z edinstvenimi informacijami, kot je npr. osebna identifikacijska številka (*personal identification number – PIN*). PIN je zakodiran z enosmerno transformacijo (*hash function*) in shranjen v posebnem delu spomina (tajno področje – *secret zone*), ki ga ni mogoče brati. Ko zaposleni želi imeti dostop do računalniskega sistema, mora vstaviti kartico v vhodno/izhodno enoto in vtipkati PIN. Procesor pametne kartice izvaja enosmerno transformacijo vtipkanega

PIN-a ter ga primerja s shranjenim PIN-om v tajnem področju. Ta primerjava poteka znotraj procesorja kartice. Pomembno je, da PIN ne potuje preko nezanesljivih linij in ni vpisan v delovni spomin glavnega računalnika (ki ga lahko kdo opazuje). Če pametna kartica potrdi, da se PIN-a ujemata, se prične drugi del identifikacije, ko pametna kartica komunicira z glavnim računalnikom in omogoči zaposlenemu dostop do računalniškega sistema.

Čeprav je PIN preverjen lokalno, njegova dolžina (štiri številke) ne zadostuje za varnost. To pomanjkljivost poskušajo odpraviti z omejitvijo števila poskusov vnašanja gesla ali pa z dodatnimi testi, kot so prstni odtisi, geometrija roke, podpis, vzorec zenice, prepoznavanje glasu itd. (glej sliko 5).

prstni odtisi | geometrija roke | odtis noge (otroci) | vzorec ven | prepoznavanje glasu

vzorec zenice | prepoznavanje obraza | zapis zob | DNA | podpis

Slika 5: Biometrični testi

Sedaj pa si oglejmo podrobneje še drugi del identifikacije. Ko smo uspešno opravili prvi del identifikacije in je kartica prepričana, da jo uporablja njen lastnik, prične kartica komunicirati z glavnim računalnikom. To lahko ponazorimo s hipotetično situacijo:

> Temno je kot v rogu in po opravljeni diverziji v sovražnem taboru se vohun vrača v grad. Bližajoč se vratom, zasliši šepetajoč glas:
>
> “Geslo ali streljam!”
>
> *Ali šepeta prijatelj ali sovražnik?*
>
> Kako lahko vohun prepriča stražarja, da pozna geslo, ne da bi ga pri tem izdal morebitnemu sovražniku/prisluškovalcu? McGeoch [17].

Vohunova dilema je vsakdanji problem v telekomunikacijah. Kadar kartica v bankomatu komunicira z banko, morata biti oba prepričana o avtentičnosti (pristnosti) drug drugega. Iz tega sledi, da morajo biti elektronska gesla taka, da jih ni mogoče ponarediti in da ne koristijo prisluškovalcu. Ena od metod za varno izmenjavo gesel v tem kontekstu se imenuje *dokaz brez znanja* (*zero-knowledge proof*), kar pomeni, da dokažeš (z odgovori na serijo vprašanj), da poznaš svoje geslo, a pri tem ne izdaš niti en sam bit gesla. Glej [17], [13] in [20].

Glede na pomembnost podatkov, ki jih varujemo, se odločimo za ustrezno obliko zaščite. Geslo oziroma PIN predstavlja osnovno zaščito, DES (*Data Encryption Standard*) [5], [25] nudi srednji, shema javnih ključev (*Public Key Scheme – PKS*) [12], [8], [9, Ch.13,14], [15] pa visok nivo zaščite.

Slika 6: Pametna kartica proizvede slučajno število, ter ga pošlje čitalcu. Ta ga zakodira s pomočjo svojega privatnega ključa in rezultat pošlje pametni kartici. Če pametna kartica uspešno odkodira slučajno število z javnim ključem, potem je prepričana o avtentičnosti čitalca. Enak proces poteka v nasprotni smeri. Čitalec pošlje novo slučajno število kartici, ki ga le-ta zakodira s svojim privatnim ključem. Če ga čitalec uspešno odkodira, potem se lahko začne komunikacijski proces.

5 Deli in vrste pametnih kartic

Mikroračunalnik pametne kartice je majhen računalnik, ki vsebuje vse tri osnovne mikroračunalniške komponente: procesor, spomin in vhodno/izhodno enoto (ne vsebuje pa vseh integriranih vezij kot osebni računalnik).

Slika 7: Mikročunalnik pametne kartice

(a) Procesor

Procesor naredi pametno kartico "pametno", različno od drugih kartic. Ima dve osnovni funkciji: manipulira in interpretira podatke. Trenutno so v rabi 8-bitni procesorji, pojavljajo pa se tudi že 16-bitni. Operacijski sistem odloča, kje bodo shranjeni podatki in v kakšnih okoliščinah bo izveden prenos informacij preko vhodne/izhodne enote. Kartica poskrbi za samouničenje pri vsakem nenormalnem stanju (segrevanje ali fizično poseganje v notranjost kartice zaznanavajo varnostna stikala – *temper resistent switches*). Aplikacijski programi pa omogočajo identifikacijo, varne finančne transakcije itd.

Nekatere vrste pametnih kartic vsebujejo tudi kripto-koprocesorje za hitro enkripcijo/dekripcijo oziroma za generiranje digitalnih podpisov (*digital signatures*), ki overovijo poslovne informacije ali pa potrdijo identiteto. Več o tem si lahko preberete v [2] in [4].

(b) Spomin

Spomin je lahko trajen (*non-volatile*) ali začasen (*volatile*), glede na to, ali se podatki ohranijo ali izgubijo po prekinitvi napajanja, oziroma ko računalnik ugasnemo. Pametna kartica mora imeti trajen (*non-volatile*) spomin, ki hrani podatke, kot so ime nosilca kartice, aplikacijske programe itd. Imeti mora tudi spomin, kamor se vpisujejo sprotne informacije, npr. stanje po pravkar opravljeni transakciji.

Na splošno ima pametna kartica tri vrste spomina:

- Read Only Memory (ROM) – za shranitev operacijskega sistema,
- Random Access Memory (RAM) – za začasno shranjevanje podatkov,
- Programmable Read Only Memory (PROM), ki ga lahko delimo v Eraseble Programmeable ROM (EPROM) ali Electrically Eraseable Programmable ROM (EEPROM).

Slika 8: Vrste spomina v pametni kartici

EPROM se lahko uporablja v pametni kartici za permanentno shranjevanje zapisov transakcij skozi njeno življenjsko dobo. EPROM ji omogoča večjo spominsko kapaciteto kot drugi spomini, vendar pa je podatke mogoče le zapisovati in ne brisati, tako se spomin po določenem času napolni in kartici se izteče življenjska doba. Prve pametne kartice so imele NMOS EPROM, sedanji trend pa je CMOS EEPROM s kapaciteto od 100 bytov do 64KB. EEPROM se uporablja za shranjevanje programov in podatkov, ki se periodično spreminjanjo. Ker se EEPROM lahko zbriše z elektronskim signalom, kartica ne zapade, ko je spomin poln. EEPROM ima manjšo spominsko kapaciteto in je dražji kot drugi tipi spomina ter potrebuje več integriranega vezja. Zaradi tega ni ustrezen za shranjevanje zapisov transakcij.

PROM je razdeljen v tri področja (glej sliko 9). V *tajnem področju* (*secret zone*) so lahko shranjeni podatki, ki jih uporablja samo procesor, na primer lastnikovo geslo, kreditni limit itd. Drugi podatki, na primer priimek in ime lastnika, naslov, so shranjeni v *odprtem področju* (*open zone*), in jih lahko preberemo z različnimi čitalci, a jih ne moremo spreminjati. *Delovno področje* (*working zone*) vsebuje zapis podatkov, ki se nanašajo na funkcijo kartice in jih je potrebno spreminjati (npr. zapisi nakupov). V delovnem področju se lahko piše (in bere) samo ob določenih pogojih, na primer če je kartica v čitalcu oziroma blagajni pri pooblaščenem prodajalcu.

Slika 9: Področja PROM-a

(c) Vhodno/izhodna enota

Vmesnike pametne kartice delimo na kontaktne in brezkontaktne. Kontaktna kartica se napaja in komunicira preko kovinskih kontaktov. Brezkontaktna kartica pa nima neposrednega kontakta in je ni potrebno nikamor vložiti. Podatke in energijo prenaša na več načinov, kot so induktivni, optični capacitive caupling, microvawe coupling itd., in glede na to deluje na razdalji 1mm ali pa nekaj metrov (na primer na avtocesti čitalec zazna brezkontaktno kartico v avtu, ki vozi do 100km na uro). Brezkontaktna kartica ima številne prednosti pred kontaktno kartico, saj je zanesljivejša, njena življenjska doba je daljša ter omogoča hitrejšo in enostavnejšo uporabo. Čitalna enota nima reže, tako je manj možnosti za vandalizem (npr. lepilo, žvečilni gumi v reži).

Slika 10: Primera brezkontaktne kartice

6 Sistem pametne kartice

Sistem pametne kartice lahko vsebuje pisalno-čitalno enoto (*writer-reader unit* – *WRU*), tiskalnik in osebni računalnik.

Slika 11: Sistem pametne kartice

Oglejmo si primer, ko je pametna kartica uporabljena kot kreditna kartica (potovalni ček) in komunicira s čitalcem v trenutku prodaje (glej sliko 12). Kaj se dogaja v čitalcu kartice? Lastnik vloži svojo pametno kartico v čitalec, vtipka PIN, kartica in čitalec pa preverita avtentičnost drug drugega. Kupec potrdi vrednost nakupa, čitalec pa sporoči kartici, da zabeleži nakup in zmanjša svojo vrednost za ceno prodanega blaga. Ko je transakcija zaključena, čitalec izvrže kartico.

Slika 12: Pametna kartica v vlogi potovalnega čeka

Čitalci v trgovinah se občasno povežejo z glavnim računalnikom v banki, da mu sporočijo nastale transakcije in obnovijo seznam ukradenih kartic. Čitalec pametne kartice imamo lahko tudi doma, kjer ga povežemo z računalnikom, tiskalnikom ali televizorjem, da si ogledamo tekoče podatke o opravljenih nakupih in stanje našega računa v banki (glej sliko 13). Sistem pametne kartice poveča fleksibilnost in varnost v mnogih aplikacijah, ker ima sposobnost opravljati zapletene računske operacije in ščititi spravljene podatke.

Slika 13: Uporaba pametne kartice doma

7 Aplikacije

Pametne kartice lahko v širšem smislu delimo na kartice s finančnimi aplikacijami in na kartice z nefinančnimi aplikacijami. Trenutno so predvsem v rabi kartice z nefinančnimi aplikacijami v telekomunikacijah, zdravstvu, šolstvu in vojski. Precejšnje investicije v bankomate in že vpeljana uporaba magnetnih kartic v plačilne namene sta vsekakor vzroka za trenutno neenakomerno porazdeljeno tržišče (v ZDA imajo sedaj 13.000 čitalcev pametnih kartic in kar 5 milijonov naprav za magnetne kartice). Porast zlorab magnetne kartice v zadnjih letih pa bo prav gotovo nagnil tehtnico v prid pametni kartici.

Slika 14: Področja uporabe pametnih kartic

(a) Finančne aplikacije

Mnoge finančne aplikacije temeljijo na vnaprej plačani kartici (*prepaid card*). S tako kartico lahko plačamo toliko zneskov, kolikor denarja smo položili nanjo in je zlasti uporabna za indirektne sisteme (*off-line*). Vnaprej plačano kartico uporabljamo predvsem za plačevanje avtomatov (običajno na kovance), kot so javni telefon, fotokopirni in pralni stroj, parkirna ura, prodaja hrane in pijače. Raje uporabljamo indirektne sisteme, saj so hitri in poceni. Čeprav so zneski plačila majhni, je pretok denarja velik, plačevanje pa izredno poenostavljeno. Predstavniki državnih bank pa opozarjajo, da gre za novo metodo tiskanja denarja brez ustaljenih določil, kdo garantira za izdano vrednost.

Pametne kartice se bodo kmalu uporabljale kot nadomestilo za denar in čeke, se pravi, da bomo namesto gotovine uporabljali elektronsko gotovino, namesto papirnatega čeka pa elektronski ček ali elektronski potovalni ček (vnaprej položen denar je mogoče porabiti v katerikoli valuti). Pametna kartica bo v resnici postala elektronska denarnica in bo zagotavljala tudi kreditno sposobnost.

Slika 15: Vnaprej plačane, kreditne in večnamenske kartice, ki se uporabljajo na področju finančništva.

(b) Aplikacije v zdravstvu

V zdravstvu nudijo pametne kartice kompletno paleto uslug, na primer identifikacijo, vodenje administracije, kot so zapisi o izdanih receptih, boleznih, cepljenjih, pregledih, plačevanju, skratka vse zdravstvene informacije o lastniku kartice, njegovih zdravnikih (v urgentnih primerih) ter komunikacijo med zdravniki, pri tem pa ohranijo zasebnost podatkov. Poenostavljajo administracijo in omogočajo geografsko mobilnost (na primer bolnikom, ki potrebujejo dializo). Problem povzroča samo nezadosten spomin, ki pa se ga da bolje izkoristiti z uporabo mednarodno uveljavljenih kratic za diagnoze, zdravila in podobno.

Slika 16: Področja v zdravstvu, kjer se uporabljajo pametne kartice

(c) Aplikacije v šolstvu - na univerzah

Zapis na pametni kartici vsebuje informacije o študentu, tako akademske kot administrativne. Hkrati pa kartica omogoča identifikacijo in vstop v knjižnice, laboratorije, športne ter druge objekte. Ker je univerza svet v malem, se je študentska pametna kartica prva približala večnamenski kartici, s tremi glavnimi funkcijami, te pa so podatkovna baza, kontrola dostopa in elektronska denarnica.

Slika 17: Aplikacije pametnih kartic v šolah

(d) Aplikacije v telekomunikacijah

Aplikacije za javne telefone so daleč največji uporabnik čip kartic. Večina telefonskih kartic so vnaprej plačane kartice (prepaid cards) in zaenkrat nimajo procesorja, marveč le nekaj logike v obliki integriranega vezja, z ne več kot 100 bytov spomina. So izredno zanesljive in poceni. Lahko hranijo tudi izbrane telefonske številke in omogočajo hitro klicanje teh številk (*speed dialing*). Nekatera telefonska podjetja pa že nudijo telefone s pametnimi karticami.

Danes je mogoče dobiti številke, ki niso vezane na telefonski priključek, marveč na pametno kartico, že v 85-ih državah. V tem primeru je pametna kartica v bistvu *sledi-me telefon* (*follow-me phone*), kar pomeni, da kjerkoli vložimo pametno kartico v telefon in vtikamo PIN, lahko sprejmemo telefonski klic ali pa kličemo sami. Telefon je lahko osebna last ali pa je na razpolago v taksijih, letalih, ladjah, v rent-a-car-ih, javnih govorilnicah itd.

Slika 18: Philiphsov GSM telefon ter nekaj GSM telefonskih kartic

Ta sistem se je začel razvijati 1987. leta in se imenuje GSM (*Global System for Mobile Communications*). Gre za mednarodni mobilni telefonski sistem, ki temelji na digitalnem prenosu in značilostih pametne kartice. Ima že preko 10 milijonov naročnikov in se bo kmalu razširil po vsem svetu. Uporabnikova kartica potrjuje njegovo identiteto (*SIM - Subscriber Identity Module*). Ko je kartica vložena v GSM telefon, GSM uporabi podatke na kartici in PIN za preverjanje naročnikove identitete, klic pa je obračunan v matični državi. Hkrati pa lahko pametna kartica omogoči tudi šifriran prenos in s tem prepreči prisluškovanje.

Slika 19: GSM (Global System for Mobile Communications)

(e) Varovanje podatkov in računalniškega sitema

Pametne kartice se lahko uporabljajo kot varnostna ključavnica za računalnike in diske. Če ne vtipkamo pravilnega gesla ali če pametna kartica ni prisotna, se tipkovnica oziroma sistem zaklene. Informacije na disku ali pa kakšnem drugem podatkovnem mediju je moč zakodirati s pomočjo lastniku avtentičnega ključa, spravljenega v pametni kartici. Podobno je lahko zaščitena tudi komunikacija med različnimi računalniki.

(f) Plačani televizijski programi

spredaj zadaj

Slika 20: Za plačane TV programe (*pay-TV*) se običajno uporablja pametna kartica v obliki ključa.

Določene televizijske programe je treba posebej plačati in so zakodirani. Če jih hočemo gledati, moramo pri ustrezni televizijski hiši plačati naročnino ter dobiti posebno enoto, ki zna program odkodirati. Da pa ne bi prišlo do ponarejanja teh enot (predvsem kadar je na voljo samo enosmerna komunikacija od televizijske hiše do gledalca), je dobro uvesti gesla in jih pogosto zamenjevati, same enote pa avtentizirati. Ta problem se da enostavno rešiti s pametno kartico, saj je veliko lažje zamenjati geslo na kartici ali pa kartico kot pa samo kodirano enoto.

Slika 21: Aplikacije (d)-(f), pametne kartice v telekomunikacijah in uporabniški elektroniki

(g) Aplikacije v vojski

Pametna kartica ima izredno pomembno vlogo v vojski, saj med drugim omogoča kontrolo gibanja, dostop do raznih objektov, uporabo orožja ter zagotavlja tajnost komunikacij.

(h) Druge aplikacije

Pametne kartice lahko uporabljamo na različnih področjih, tudi v transportu, hotelih, športu, na razstaviščih, črpalkah in še marsikje. Kartica lahko vsebuje zapis podatkov ali rezultatov, na primer na borzi. V Angliji so nadomestili vstavljanje kovancev v posebne merilce za uporabo kurjave in elektrike z vnaprej plačano pametno kartico. Pametne kartice postajajo vse bolj popularne na vseh koncih sveta, tudi na olimpijskih igrah v Atlanti 1996. leta. Vsak športnik je dobil svojo pametno kartico, ki jo je uporabljal za identifikacijo, kot elektronsko denarnico in za dostop v razne objekte. Več kot milijon vnaprej plačanih kartic so uporabljali v tisočih trgovinah.

Slika 22: Pametna kartica, ki so jo uporabljali na olimpijskih igrah v Atlanti.

Obstajajo tudi druge možnosti uporabe pametne kartice, ki pa zaenkrat se niso tako razširjene, na primer za dostop v zabavišče, kino, gledališče, kot potni list itd.

8 Zaključek

Danes si ne moremo predstavljati osebnega in poslovnega življenja brez kartic. Papirnato kartico, s katero smo se nekoč predstavljali, je z razvojem novih materialov zamenjala plastična kartica s funkcijo kreditne kartice. Bančna industrija je zaradi potrebe po avtomatizaciji dodala plastični kartici magnetni trak. Premajhen spomin in nezadostna varnost sta glavni pomanjkljivosti magnetne kartice. Precej večjo spominsko zmogljivost ima optična kartica, največjo zaščito pa nam nudi pametna kartica. Pametna kartica nam omogoča predplačila, poslovanje brez gotovine, dostop do objektov, bazo osebnih in drugih podatkov ter zaščito le-teh, predvsem pa onemogoča zlorabo in nepoštenje ter poenostavlja administracijo. Nadomestila bo kovance, bančne izpiske, čeke, identifikacijske dokumente, transportne karte, zdravstvene recepte, kreditne kartice, ključe itd, glej sliko 23.

Pametna kartica je računalnik v žepu, njen razvoj in možnosti pa še zdaleč niso zaključene. Na Japonskem in v ZDA so izoblikovali pametno kartico s tipkovnico in majhnim zaslonom (super pametna kartica – *Super Smart Card*), razvita pa je tudi že tako imenovana kombinirana kartica (*Combi Card* ali *Hybrid Card*), ki ima lastnosti kontaktne in brezkontaktne kartice.

Slika 23: Področja uporabe pametnih kartic

Pred kratkim so se Europay, Mastercard in Visa (EMV) dogovorili za skupno specifikacijo pametne kartice, ki določa osnovne protokole za komunikacijo med kartico in čitalcem. Ta je analogna RS-232 standardu za komunikacijo med osebnim računalnikom in modemom. Specifikacija je dovolj splošna, da lahko izmenjamo katero koli informacijo med hardwarom in softwarom. To pa je osnova za večnamensko pametno kartico (*Multipurpose Smart Card*).

Glavni prozvajalci pametne kartice (Gemplus,Thompson – Francija, Philips–Nizozemska, Motorola–ZDA, Mondex–Anglija, Siemens–Nemčija) so dosegli prvo stopnjo njene tehnične zrelosti. Spominska kapaciteta ni več ovirajoč faktor, pojavljajo pa se nove dileme, kot so izbira med nivojem zaščite ter ceno kartice, katere informacije zaščititi in komu omogočiti dostop do njih. Prihodnost pametne kartice je odvisna tudi od potreb po zasebnosti, od gospodarskih in političnih razmer, programskih možnosti in drugih vplivov. Pametna kartica je tu in njene možnosti je treba izrabiti.

Kartica za uporabo telefona na ulici in v javnih prostorih je nujno potrebna dinamičnemu človeku.

Plačevanje s kartico odpravlja potrebo po gotovini. Pametna kartica je bolj odporna proti goljufijam in začenja nadomeščati magnetno kartico.

Vnaprej plačana kartica olajšuje uporabo igralnih avtomatov, obisk teniških igrišč, kinomatografov, rekreacijskih parkov itd.

S SIM-kartico ima GSM naročnik možnost uporabljati prenosne telefone po vsem svetu, kot bi bili njegovi.

Pametna kartica je zanesljiv medij za identifikacijo in poenostavi administracijo v zdravstvu itd.

Pametna kartica za mestni prevoz, parkirno uro, knjižnico, športno opremo itd.

Pametna kartica omogoča varne transakcije v bančnem in borznem poslovanju ter finančništvu.

Pametna kartica kot študentska kartica nadomešča kovance, bone in indekse.

Slika 24: Siemensove kartice

References

[1] S. Bassein, A Sampler of Randomness, *Scientific American*, *American Math. Monthly*, June-July (1996), pp. 483-490.

[2] T. Beth, Confidental Communication on the Internet, *Scientific American*, December 1995, pp. 87-91.

[3] G. J. Chaitin, Randomness in Arithmetic, *Scientific American*, July 1988, pp. 52-57.

[4] D. Chaum, Achieving Electronic Privacy, *Scientific American*, August 1992, pp. 96-101.

[5] A. K. Dewdney, On making and breaking codes, Part I,II (in Computer Recreations) *Scientific American*, October, November 1988, pp. 120-123, 104-107.

[6] Finance and Economics: Going for Olympic gold cards *Economist*, March (1996), 67-68.

[7] C. H. Fancher, Smart Cards, *Scientific American*, August 1996, pp. 40-45.

[8] M. Gardner, A new kind of cipher that would take millions of years to break, (in Mathematical games), *Scientific American*, August 1977, pp. 120-124.

[9] M. Gardner, *Penrose tiles to trapdoor Ciphers.* W.H. Freeman and Company 1989.

[10] M.E. Haykin and R.B.J. Warnar, *Smart Card Technology: New Methods for Computer Access Control*, NIST, Special publication 500-157, 1988.

[11] P.L. Hawkes, D.W. Davies and W.L. Price (eds.), *Integrated Circuit Cards Tags and Tokens*, BSP Professional Books, 1990.

[12] M. E. Hellman The Mathematics of Public-Key Cryptography, *Scientific American*, August 1979, pp. 146-158.

[13] Jean-Jacques, Myriam, Maurier and Michaël Quisquater, Louis, Marie-Annick, Gaïd, Anna, Gwenolé, and Soazig Guillou (in collaboration with T. Berson, for the English version), How to Explain Zero-Knowledge Protocols to Your Children, *Advances in Cryptology - Crypto' 89, Lecture Notes in Computer Science* **435**, Springer-Verlag Berlin, New York (1990), pp. 628-631.

[14] D. Kahn, Modern Cryptology, *Scientific American*, July 1966, pp. 38-46.

[15] B. Magajna, O tajnopisih, *Obzornik mat. fiz.*, **38** (1991), 9-18.

[16] J. McCrindle, *Smart Cards.* IFS Publications/Springer-Verlag, 1990.

[17] C.C. McGeoch, Zero-knowledge proofs, *American Math. Monthly*, Aug.-Sep. (1993), pp. 682-685.

[18] R. McIvor, Smart Cards, *Scientific American*, November 1985, pp. 152-159.

[19] D. Naccache, D. M'Raïhi, Gemplus, Cryptographic Smart Cards, *IEEE Micro*, Vol. 16, No. 3, June 1996, pp. 14-24.

[20] I. Steward, Proof of Purchase on the Internet (in Mathematical Recreations), *Scientific American*, October? 1995, two pages.

[21] G. Stix, Dr. Big Brother (in Science and Business), *Scientific American*, February 1994, pp. 108-110.

[22] J. Svigals, *Smart Cards, The Ultimate Personal Computer.* Macmillan Publishing Company, 1985.

[23] P. Wallich, Wire Pirates (in Trends in Communication) *Scientific American*, March 1994, pp. 90-101.

[24] J.L. Zoreda and J.M. Oton, *Smart Cards.* Artech house, 1994.

[25] J. Zupan, Nekaj o kriptografskih metodah, *Obzornik mat. fiz.*, **25** (1978), 129-136.