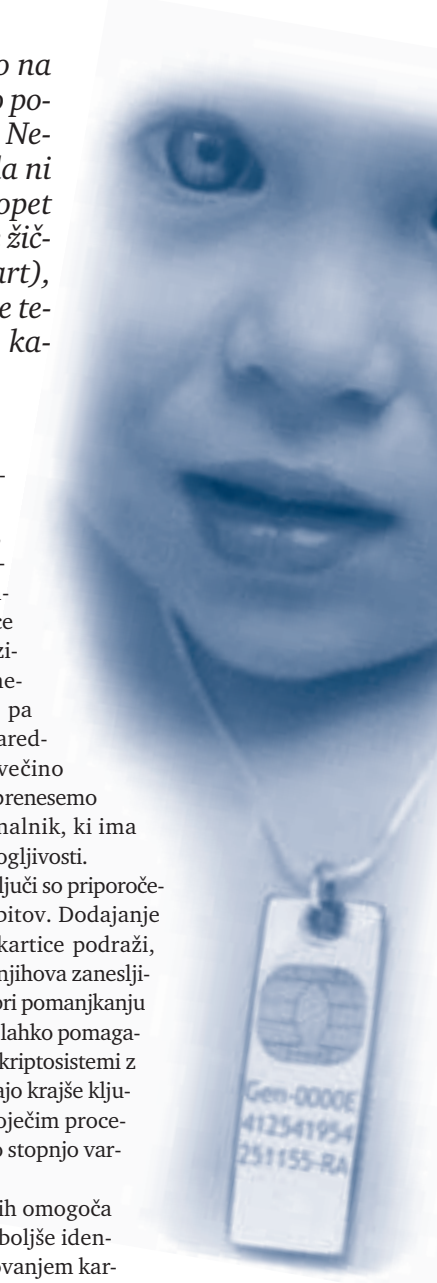
Pametne kartice in varnost

Na naših smučiščih dobimo papirne dnevne karte in jih običajno nosimo na elastični vrvici. Pred vstopom na vlečnico vstavimo kartico v napravo, da jo potegne pod bralnik magnetnega traku ali črtne kode in jo po branju vrne. Nekoč je bil datum veljave kartice odtisnjen kar na kartici s pečatom. Seveda ni bilo težko z radirko in ustreznim pisalom popraviti datuma ter karto zopet uporabiti (posebno, če je bila tedenska). Tehnologija se je na veliko veselje žičničarjev razvila (tako da jim ni več treba stati na mrazu in preverjati kart), varnost pa verjetno še vedno ni idealna. Smučarjem pa bo veliko lepše šele tedaj, ko bomo tudi na naša smučišča dobili brezkontaktne kartice s čipom, kakršne so reklamirali na letošnjem Cebitu.



Predstavljajmo si, kako bi bilo, če bi uporabljali večnamensko brezkontaktno pametno kartico. Zjutraj bi odšli od doma, ne da bi morali vzeti s seboj šop ključev, celo vrat ne bi bilo treba zakleniti. Nakupovanje v trgovini bi se lahko končalo brez postanka pri blagajni. Nato bi se odpeljali na delo z mestnim avtobusom, ne da bi morali skrbeti za drobiž, žetone ali po žepih iskati mesečno karto. Tudi vozniki avtomobilov bi se brezskrbno usedli v avto, ki bi se takoj, ko bi »začutil« našo bližino, samodejno odklenil in po možnosti še vžgal. Na poti ne bi imeli skrbi niti s cestnino niti s parkirnino ali plačevanjem goriva. Izposoja knjig in kopiranje v knjižnici bi potekala brez administrativnih ovir in obračunavanja stroškov. Tudi dostop do interneta, pošte in osebnih zbirk podatkov bi lahko opravili kar na cestnem računalniku brez vnašanja gesel. Lahko bi varno prodajali ali kupovali delnice. Telefonske klice bi sprejemali ali opravljali na bližnjih telefonih. Tudi pri malici in kosilu ne bi bilo treba misliti na denarnico, obisk pri zdravniku pa se ne bi pričel z običajnim: »Najprej morate potrditi kartico.« Ob koncu dneva pa bi se nam doma (ali pa v hotelu) vrata odprla sama, prižgale bi se luči ter stereo z glasbo, ki smo si jo zaželeli na poti domov. Ogledali bi si še kak dober film na televiziji (pay-per-view) ali odšli brez kart v kino, na tekmo ali koncert in si pred spanjem zapisali kak utrinek v svoj dnevnik.

Pričakujemo hiter razvoj uporabe pametnih kartic, vse dokler ne bodo pametne kartice zares postale računalnik v našem žepu.

Da bi bila zgornja zgodba lahko resnična, moramo rešiti problem identifikacije (da ne bomo potrebovali vratarja, ki bi nas moral prepoznati, preden odpre vrata in nam zaželi lep dan), najti način, kako digitalno shraniti vrednost in si pri tem morda zagotoviti še anonimnost. Danes nam to že lahko omogoči računalniška varnost s kriptosistemi z javnimi ključi in pametnimi karticami.

Shraniti je treba številna gesla, ključe za šifriranje, ključe za prepoznavanje, ključe za preprečevanje tajitve ... Prav slednje napravice jih shranijo na enem mestu in pazijo, da nikoli ne zapustijo zaščitenega mesta, kartična tehnologija pa preprečuje uspešno izdelavo ponaredkov. S primerno zasnovo lahko večino računanja in vodenja dnevnikov prenesemo s pametne kartice v osebni računalnik, ki ima večje računske in pomnilniške zmogljivosti.

Za kriptosistem RSA z javnimi ključi so priporočene dolžine ključev tudi do 2000 bitov. Dodajanje komponent (npr. soprocesorja) kartice podraži, hkrati pa se utegne zmanjšati tudi njihova zanesljivost in s tem varnost. Vendar pa si pri pomanjkanju pomnilnika in procesorske moči že lahko pomagamo z novimi tehnologijami (kot so kriptosistemi z eliptičnimi krivuljami), ki omogočajo krajše ključe in hitrejše računanje (že z obstoječim procesorjem), pri tem pa ohranijo enako stopnjo varnosti.

Z digitalnimi podpisi, ki nam jih omogoča javna kriptografija, smo prišli do boljše identifikacije, ki je podprta še s posedovanjem kartice, poznavanjem PIN-a in biometrično kontrolo. PIN ali pa biometrika seveda še ne zadoščata (glej okvir Vohunova dilema). Brez uporabe pametnih kartic je bil običajno prepoznan le računalnik, s katerim se povežemo v omrežje, ne vemo pa za-

logije

stran 66

Pametne kartice in varnost

Pametne kartice so zelo zmogljive napravice in omogočajo celo vrsto dejavnosti in storitev.

stran 76

Prihaja ADSL

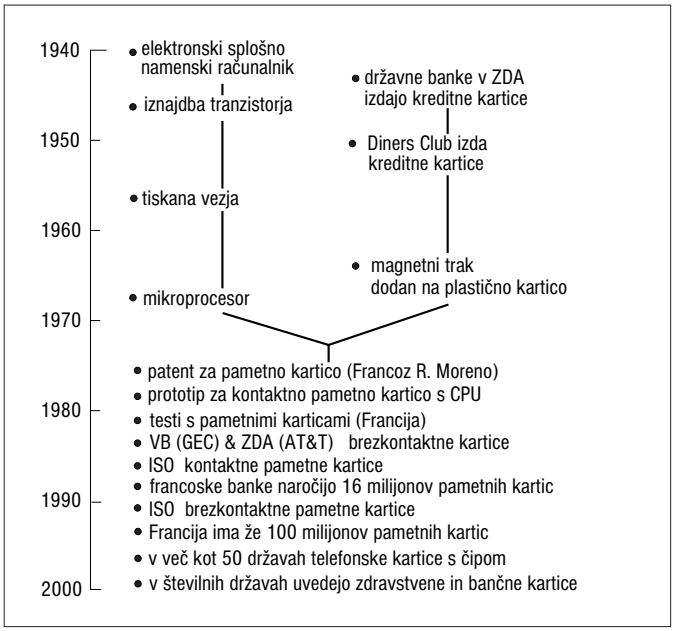
Trenutno najhitrejše telekomunikacijske povezave omogočajo usmerjevalniki ADSL, priključeni na navadno telefonsko omrežje.

gotovo niti tega, komu v omrežju smo se s tem računalnikom predstavili.

V zadnjih dvajsetih letih je kriptografija prišla iz skrivališča na plano, od zapletenega do preprostega, pa tudi pocenila se je. Na delu je veliko vplivov, kot so profesionalizacija kriptografov, nastanek novih učbenikov in organizacije tečajev, neprestana rast računske moči, razvoj algoritmov, kar so prispevali raziskovalci kriptografije in tehnologije (inženiringa), rast e-trgovanja in brezžičnih infrastruktur, ki imajo neomejeno potrebo po kriptografskih storitvah, sodelovanju velikega števila mladih na tem področju ter po olajšanju izvoznih kontrol.

Pričakujemo hiter razvoj uporabe pametnih kartic ter standardov, vse dokler ne bodo pametne kartice zares postale računalnik v našem žepu. Pametna kartica torej omogoča svojemu lastniku ne le priročno shranjevanje informacij, temveč tudi obdelavo le-teh na način, ki zagotavlja varnost. Potreba po varni in prenosni računski platformi daje izjemen zagon razvoju pametnih kartic. Predvidevamo, da bodo v prihodnosti kriptografske operacije tako prodorne, neopazne in poceni, kakor so postale operacije s protokolom IP danes. Do leta 2002 naj bi imeli po ocenah Dataquesta že 4,7 milijarde pametnih kartic (v vrednosti 6,8 milijarde dolarjev).

V nadaljevanju bomo spoznali osnovne vrste pametnih kartic, njihovo uporabo ter trenutno stanje doma in po svetu. Priložen je tudi seznam najbolj uporabnih standardov za pametne kartice. V drugem delu pa bomo spoznali osnovne kriptografske principe in izvedeli več o njihovi varnosti pri pametnih karticah.



▲ Slika 3: Zgodovina razvoja pametnih kartic.

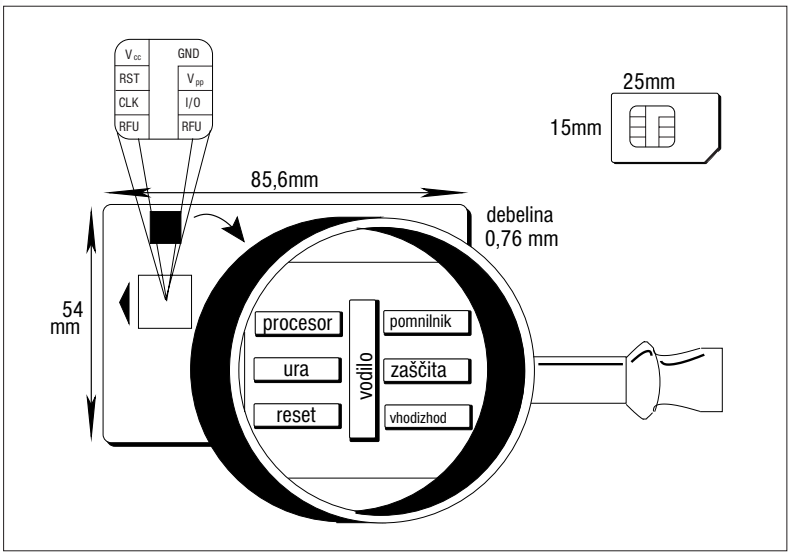
Razvoj in sestava

Kaj je pametna kartica? Gre za pravi pravcati računalnik na kartici (slika 2) seveda brez monitorja in tipkovnice, čeprav imajo nekatere kartice tudi majhen zaslon iz tekočih kristalov in morda celo številčnico za vnos gesla »nadvse pametne kartice« ali »super smart cards«.

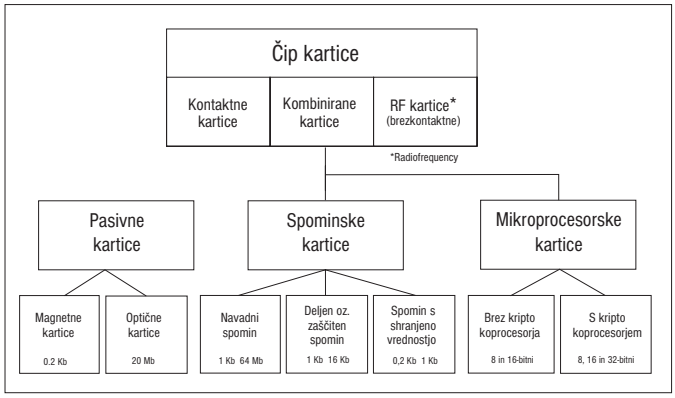
Prve plastične kartice niso bile dosti več od trajnih vizitk, zaradi tiskane informacije jih je bilo teže ponarediti, še vedno pa jih je bral človek, ki je informacijo mehansko prenesel na papir. Magnetni trakovi so avtomatizirali in poenostavili postopek, podpisi in slike pa so omogočili še vedno nepopolno identifikacijo lastnikov kartic. Nekatere današnje izvedbe, npr. zdravstvene kartice in prenosne zbirke podatkov, pa potrebujejo večji pomnilnik in boljši nadzor nad njim, kakor ju omogoča magnetna kartica.

Prava razloga za uporabo pametnih kartic sta vsekakor varnost shranjenih podatkov na kartici in zaščita podatkov drugih računalniških sistemov. Zato je strojna oprema na pametni kartici prirejena in optimalizirana prav za ti nalogi. Seveda ne gre brez uporabe ustreznih kriptosistemov za zaščito podatkov. Varnost pa ni odvisna samo od posebnega mikrokrmilnika in algoritmov, ki jih izvaja operacijski sistem. Treba je zagotoviti varnost celotni uporabi pametne kartice ter dobro poznati (če že ne samostojno izdelati) načela načrtovanja, ki ga uporabljajo izdelovalci pametnih kartic.

Pametne kartice so rezultat vzporednega razvoja mikroprocesorja in magnetne kartice (glej sliko 3). Omogočajo potrebno stopnjo varnosti, da računalniška omrežja



▲ Slika 2: Velikost pametne kartice ustreza standardu ISO 7810 ali ID-000 (npr. SIM), sestavljajo pa jo mikroprocesor, pomnilnik (ROM, RAM, EEPROM), vhodno/izhodna enota (I/O). Oznake na priključkih: Vcc – napajanje, GND – ozemljitev, RST – ponastavljanje (reset), Vpp – napetost za programiranje (uporaba se zmanjšuje), RFU – rezervirano (reserved for future use since 1988).



▲ Slika 4: Delitev kartic s čipom.

zares zaživijo ter združijo telekomunikacije in računalnike.

Vrste kartic s čipom

Da bi bolje razumeli vlogo in pomen pametnih kartic, si oglejmo nekoliko širšo skupino – kartice s čipom. Razdelimo jih lahko na tri skupine glede na način dostopa do podatkov na kartici: na kontaktne, brezkontaktne in kombinirane. Vsako od teh skupin lahko nadalje razdelimo glede na velikost in tip pomnilnika ter prisotnost procesorja; glej sliko 4. Procesor pa da kartici pravo »pamet«. Pomnilniške kartice torej strogo gledano niso pametne kartice, a se ime pametna kartica pogosto uporablja za vse kartice s čipom.

Oglejmo si posamezne vrste kartic nekoliko podrobneje.

Pasivne kartice

Čeprav te kartice ne vsebujejo čipa, jih iz zgodovinskih razlogov prištevamo v to skupino – so namreč predhodnice sodobnih pametnih kartic. Trenutno so najbolj razširjene magnetne kartice – to so kartice z magnetnim trakom na hrbtni strani. Uporabljajo jih v bančništvu, za omejevanje dostopa ... Magnetni trak na hrbtni strani lahko shrani le okrog 200 bajtov podatkov. Optične kartice niso tako razširjene, kakšne so, pa prikazuje slika 5.

Pomnilniške kartice

Pomnilniške kartice nimajo lastnega procesorja in zato ne morejo dinamično obdelovati podatkov. Glede na vrsto pomnilnika ločimo tri tipe pomnilniških pametnih kartic.

Kartice z navadnim pomnilnikom so namenjene zgolj shranjevanju podatkov. Imajo najnižjo ceno na bit shranjene informacije. Pojavljajo se kot kartice s čipom in pomnilnikom EEPROM ali pa kot kartice s pomnilnikom flash.

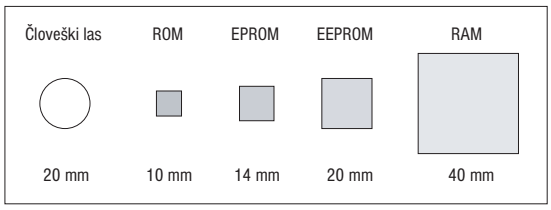
Kartice z zaščitenim ali deljenim pomnilnikom imajo vgrajena preprosta logična vezja, s katerimi nadzorujejo dostop do podatkov. Pri teh karticah lahko določene dele pomnilnika zaščitimo pred pisanjem ali branjem, kar navadno dosežemo z gesli ali sistemskimi ključi. Uporabne so predvsem tam, kjer ni potrebna visoka varnost podatkov, na primer za kontrolo dostopa s PIN-om ali kot kartica za razne ugodnosti.

Kartice s shranjeno vrednostjo so namenjene shranjevanju vrednosti ali žetonov, za enkratno ali večkratno uporabo. Tipičen primer takih kartic so telefonske kartice.

Mikroprocesorske kartice

Tem karticam pravimo pametne kartice. Sposobne so dinamično obdelovati podatke. Ponavadi vsebujejo procesor, vhodno-izhodno enoto ter več vrst pomnilnika. Trenutno se uporabljajo 8-, 16- in 32-bitni procesorji, v povprečju imajo 64 Kb ROM-a, 16 do 32 Kb EEPROM-a ter 3 Kb RAM-a, vhodno-izhodna enota pa dosega prenose 9,6–115 Kbitov na sekundo (pri čemer je možen samo polovični-dupleksni način). Po računski moči so primerljive s prvotnim računalnikom IBM-XT, kartice s kripto-soprocesorjem pa v nekaterih opravilih prekašajo celo 50 MHz računalnik 486.

To danes sicer ni veliko, toda vedeti moramo, da je velikost čipa na kartici omejena na 25 mm^2 (sicer bi se utegnil čip zaradi upogibanja kartice poškodovati). Pri tem si mora procesor deliti prostor še s pomnilnikom, vodilom, vhodno/izhodno enoto ter največkrat še z generatorjem naključnih števil. Slika 7 prikazuje velikost posameznih celic pomnilnika, ki lahko shranijo 1 bit informacije.



▲ Slika 7: Velikost posameznih pomnilniških celic, ki lahko shranijo 1 bit informacije. Velikosti so približne in se nanašajo na 0,8-mm tehnologijo.

Čas vpisovanja enega bita informacije v posamezno celico znaša za RAM 70 ns, za EEPROM pa 3–10 ms. Celice ROM lahko samo beremo.

Večina proizvajalcev zagotavlja shranjevanje podatkov v EEPROM-u do 10 let. Po tem času se zaradi zgradbe EEPROM celice lahko zgodi, da le-ta ne shrani več vrednosti, ki je bila vanjo vpisana. Zato moramo podatke obnavljati, če jih potrebujemo več kakor 10 let.

Mnogo današnjih mikroprocesorskih kartic ima krip-

PROCESORJI ZA PAMETNE KARTICE

Čip	mPD78-9828	mPD70-3903	SLE66C-X160S	SLE66C-X320P	SLE66C-X640P	ST19KF-16	ST19XL-34	P83W8-532	H8/3113
izdelovalec	NEC	NEC	Infineon	Infineon	Infineon	SGS-Thomson	SGS-Thomson	Philips	Hitachi
tip procesorja	8-bitni	32-bitni	16-bitni	16-bitni	16-bitni	8-bitni	8-bitni	8-bitni	8-bitni
frekvenca	40 MHz	40 MHz	5 MHz	15 MHz	15 MHz	10 MHz	10 MHz	8 MHz	10 MHz
tehnologija	0,35 mm	0,35 mm	0,6 mm	0,25 mm	0,25 mm	0,6 mm	0,35 mm	0,6 mm	0,5 mm
napetost	1,8V – 5,5V	2,7V – 5,5V	2,7V – 5,5V	2,7V – 5,5V	2,7V – 5,5V	3V, 5V	3V, 5V	2,7V – 5,5V	3V, 5V
RAM	1 Kb	3 Kb	1 Kb	3 Kb	5 Kb	1 Kb	4 Kb	2 Kb	1,5 Kb
ROM	24 Kb	128 Kb	32 Kb	64 Kb	136 Kb	32 Kb	96 Kb	32 Kb	32 Kb
EEPROM	8 Kb	32 Kb	16 Kb	32 Kb	64 Kb	16 Kb	34 Kb	32 Kb	16 Kb
W/E EEPROM	100.000	100.000	500.000	700.000	500.000	100.000	100.000	/	/
DES	4 ms	4 ms	3.7 ms	7 ms	7 ms	/	19 ms	10 ms	/
SHA	< 2ms	<2 ms	5,6 ms	5,6 ms	5,6 ms	8,2 ms	8,2 ms	5 ms	/
MD5	/	/	9 ms	9 ms	9 ms	/	/	/	/
RSA 512 sign	16 ms	16 ms	37 ms	37 ms	37 ms	20 ms	20 ms	37 ms	68 ms
RSA 512 ver	2 ms	2 ms	10,3 ms	20,3 ms	20,3 ms	2 ms	2 ms	10 ms	/
RSA 1024 sign	100 ms	100 ms	230 ms	83 ms	83 ms	110 ms	110 ms	160 ms	480 ms
RSA 1024 ver	7 ms	7 ms	24 ms	7 ms	7 ms	5 ms	7 ms	25 ms	/
DSA 512 sign	31 ms	31 ms	50 ms	48 ms	48 ms	25 ms	25 ms	58 ms	/
DSA 512 ver	70 ms	70 ms	90 ms	43 ms	43 ms	40 ms	40 ms	82 ms	/

▲ V tabeli ni podatkov za podpisovanje z eliptičnimi krivuljami, saj zanje ni potreben soprocesor, tako da so časi odvisni predvsem od izvedbe. Praviloma so krajši od ustreznih časov za podpisovanje s kriptosistemom RSA za javne ključe. Podatki so povzeti po članku H. Handschuh in P. Paillier, *Smart Card Crypto-Coprocessors for Public-Key Cryptography: third international conference, CARDIS'98, Louvain-la-Neuve, Belgium, September 14-16, 1998; proceedings*, ter dopolnjeni s podatki iz interneta.

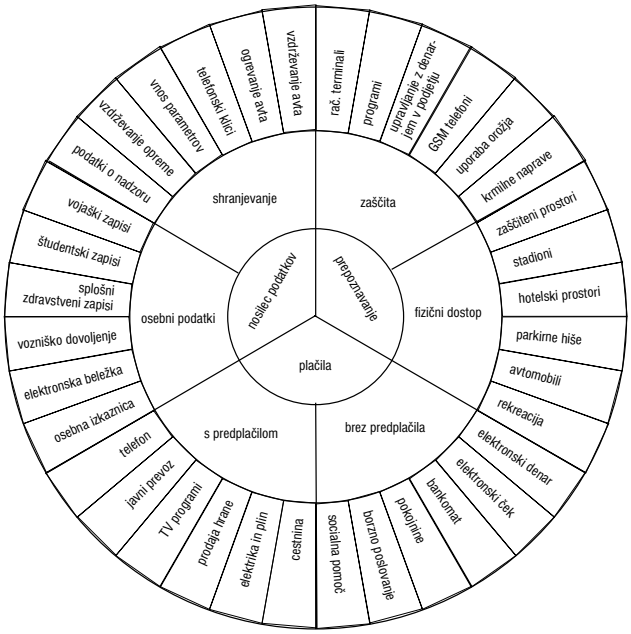
to-soprocesor. Zmožne so generiranja in preverjanja digitalnih podpisov ter šifriranja podatkov s simetričnim ključem. Podatki so organizirani v datotečnem sistemu, do katerega ima procesor dostop s kartičnim operacijskim sistemom (COS). Uporabljajo se v telefonih GSM (kartica SIM), za avtentikacijo, shranjevanje občutljivih podatkov (npr. zasebnih ključev, certifikatov).

Najnovejši podatki o zmogljivejših procesorjih, ki so na voljo za pametne kartice, so zbrani v tabeli.

Pojasnimo še nekatere oznake iz tabele. *Frekvenca* označuje notranjo frekvenco delovanja procesorja, zunanja frekvenca, ki jo dovajamo kartici, pa je vedno 5 MHz. *Tehnologija* označuje velikost, v kateri so izdelani tranzistorji in povezave v čipu. *Napetost* pomeni napajalno napetost , medtem ko napetost za programiranje znaša okrog 20 V in ni navedena v tabeli. *RAM*, *ROM* in *EEPROM* označujejo velikost posamezne vrste pomnilnika. Oznaka *W/E EEPROM* označuje število pisanj/brisanj celice EEPROM, preden ta postane neuporabna. Oznaka *DES* označuje čas, potreben za šifriranje 64 bitov podatkov s 56-bitnim ključem z algoritmom DES. *SHA* in *MD5* označujeta čas, potreben za izračun SHA-1 ali MD5 povzetka enega bloka izbranih podatkov (160 bitov za SHA-1 in 512 za MD5). V preostalih vrsticah se oznaki *sign* in *ver* nanašata na podpisovanje ali preverjanje digitalnega podpisa, številke pa pomenijo dolžino ključa v bitih.

Uporaba

Manj kakor trideset let po prvem patentu za pametne kartice smo lahko priče bliskovitemu razvoju uporabe na mnogih področjih. Nekatera področja uporabe prikazuje slika 8.



▲ Slika 8: Področja uporabe pametnih kartic.

Daleč največje število kartic se še vedno uporablja v telekomunikacijah, zadnja leta pa lahko opazimo porast uporabe tudi v zdravstvu in financah. Podrobneje si oglejmo uporabo na teh področjih, z identifikacijo pa se bomo ukvarjali pozneje.

Telekomunikacije

V javni telefoniji so pametne kartice tako rekoč izpodrinile vse druge sisteme. Še pred petimi leti so bili pri nas najpogostejši javni telefoni na žetone, dandanes pa takih ne najdemo več. Razlogov je več. Telefoni na žetone so dražji za izdelavo, saj morajo biti trpežni, da zaščitijo žetone pred krajo, in so dragi za upravljanje, saj mora nekdo pobirati žetone. Po drugi strani pa telefoni na pametne kartice ne vsebujejo ničesar, kar bi koristilo morebitnemu napadalcu, in jih ni treba vsakodnevno vzdrževati.

STANDARDI

Tako kakor na drugih tehničnih področjih tudi za pametne kartice obstajajo standardi, ki opisujejo njihove lastnosti. Pomanjkanje standardov v prvih letih razvoja se odraža predvsem v nezdružljivosti kartic posameznih proizvajalcev, vendar se stanje zadnja leta izboljšuje. Najpomembnejši standardi, ki so povezani s pametnimi karticami, so navedeni spodaj.

ANSI X9 Skupina standardov, ki opisujejo kriptografijo z javnimi ključi v finančni industriji. Izdal jih je American National Standard Institute, najpomembnejši med njimi pa so X9.30-2 opis zgoščevalne funkcije SHA-1 (Secure Hash Algorithm), X9.62 The Elliptic Curve Digital Signature Algorithm (ECDSA) in X9.63 Elliptic Curve Key Agreement and Transport Protocols. Dostopni so na http://www.ansi.org.

EMV Skupina standardov, ki so jih razvili Europay, MasterCard in Visa, opisuje pametne kartice za uporabo v plačniških sistemih. Napisani so tako, da omogočajo uporabo kartic različnih bank na istem bankomatu, ne da bi pri tem banka morala razkriti interni sistem plačevanja.

EN 726 Opisuje telekomunikacijske kartice s čipom. Razvil ga je European Telecommunications Standards Institute (ETSI). Dostopen je na http://www.etsi.fr.

EN 1546 Najpomembnejši mednarodni standard za elektronske denarnice, osnova za večino sistemov elektronskih denarnic.

GSM 11.11 Global System for mobile communications, vsebuje popoln opis vmesnika med pametno kartico in mobilnim aparatom. Vključuje tudi opis velikosti pametne kartice ter položaj kontaktov, podatkovne strukture in električne karakteristike pametne kartice. Standard je dostopen samo članom združenja GSM.

IEEE P1363 Najpomembnejši standard za javno kriptografijo. Dosegljiv je na http://www.ieee.com.

ISO 7810 Opisuje najpomembnejše fizične lastnosti identifikacijskih kartic brez čipa, med drugim tudi velikost kartice. Standard je na http://www.iso.ch.

ISO 7811 Opisuje postopke zapisovanja podatkov na magnetne kartice.

ISO 7816 Najpomembnejši standard za kontaktne pametne kartice. V standardu je določen položaj čipa in kontaktov ter opis protokolov in ukazov.

ISO 9798 Opisuje kriptografske postopke za avtentikacijo.

ISO 10373 Opisuje metode za preizkušanje magnetnih, optičnih, kontaktnih in brezkontaktnih kartic.

ISO 13491 Standard opisuje koncepte, potrebe in ocenjevalne metode za varne kriptografske naprave v bančništvu.

ISO 10536 Standard za brezkontaktne pametne kartice z dometom do 10 cm.

ISO 14443 Standard za brezkontaktne pametne kartice z dometom več kakor 10 cm.

ITU X.509 Določa strukturo in zapis certifikatov, mednarodno najpogosteje uporabljena osnova za strukture certifikatov. Dostopen je na http://www.itu.ch.

PKCS11 To je mednarodni standard za API, ki uporablja kriptografske funkcije. API se imenuje Cryptoki, vsebuje pa funkcije, kot so RC2, RC4, RC5, MD5, SHA-1, DES, trojni DES, IDEA, RSA, DSA.

Javacard To je industrijski standard, ki je osnova za javo v pametnih karticah. Objavil ga je Sun.

SET Secure Electronic Transactions – Skupina standardov za plačila s kreditnimi karticami prek omrežja s številko kartice. SET so skupno razvili CyberCash, GTE, IBM, MasterCard, Microsoft, Netscape in Visa. Dosegljiv je na http://www.setco.org.

V uporabi so večinoma predplačniški sistemi kartic za enkratno uporabo. Ob nakupu vsebuje kartica določeno količino denarja ali kredit, ki se med uporabo zmanjšuje. Ko znesek na kartici doseže vrednost nič, postane kartica neuporabna. Obstajajo tudi kartice, ki jih lahko vnovič napolnimo, vendar niso tako pogoste.

V digitalni mobilni telefoniji so pametne kartice prisotne od vsega začetka. Prvotno smo jih uporabljali zgolj za identifikacijo telefona, ker pa je prihajalo do čedalje pogostejših zlorab (prisluškovanje ter klicanje na tuj račun), je bil pri uvajanju evropskega standarda mobilne telefonije (GSM) poudarek predvsem na varnosti. Specifikacija GSM zahteva overitev uporabnika, zagotavlja celovitost podatkov ter zaupnost klicev. Pametne kartice, ki to troje zagotavljajo, so znane kot moduli SIM in so v vsakem telefonu GSM. Prva faza specifikacije GSM je zahtevala uporabo 4 Kb EEPROM, druga faza, ki je trenutno v uporabi, pa zahteva 8 Kb EEPROM za shranjevanje ključev, podatkov o uporabniku in telefonskih številk. V pripravi je že naslednja faza, ki predvideva uporabo eliptičnih krivulj za overitev uporabnika in izmenjavo sejnega ključa. Kartice GSM tudi preverjajo PIN (Personal Identification Number).

Pametne kartice se uporabljajo tudi za zaščito plačanih televizijskih programov. V tem primeru se na kartici samo shrani ključ za odšifriranje signala, dešifriranje pa opravi posebna naprava, ki jo priključimo med TV sprejemnik in anteno ali kabelski sistem. Kartico lahko uporabimo tudi v druge namene, na primer za usmerjeno oglaševanje. V tem primeru kartica odloča, katere reklame bodo predvajane in katere ne. Ravno tako lahko kartica omogoča predvajanje samo tistih programov, ki so primerni za otroke.

Omenimo še uporabo pametnih kartic v računalniških omrežjih. Do večine računalnikov pristopamo z uporabniškim imenom in geslom. Varnostni problemi nastanejo predvsem zaradi šibkih gesel, ki jih bomo podrobneje obravnavali v drugem delu članka. Ker si je zapletena gesla teže zapomniti, lahko problem rešimo preprosto tako, da geslo shranimo na pametni kartici. Ob prijavljanju v računalnik se kartica in računalnik medsebojno overita, kartica pa nato overi uporabnika. Kartica lahko tudi shrani uporabniški profil in druge podatke, na primer članstvo v določeni skupini, s katerimi so določene pravice uporabnika. Če kartico odstranimo, računalnik odjavi uporabnika. Pametne kartice pa lahko uporabimo tudi za shranjevanje certifikatov.

Pametne kartice so rezultat vzporednega razvoja mikroprocesorja in magnetne kartice.

Zdravstvo

Glavni motiv za uvajanje pametnih kartic v zdravstvu je nadzor stroškov. Uporabljajo se za dokazovanje zdravstvenega zavarovanja bolnika, ki zahteva zdravstvene storitve. Kartice zdravstvenega zavarovanja ponavadi ne vsebujejo zdravstvenih podatkov o lastniku, zato kartici ni treba preverjati uporabnika. Lastništvo se namreč v teh primerih dokazuje z drugimi metodami, na primer z osebnim poznanstvom med zdravnikom in bolnikom ali z osebno izkaznico. Če so na kartici shranjeni tudi zdravstveni podatki bolnika, mora biti zagotovljena zasebnost teh podatkov in dostop do njih omejen. Največkrat se to doseže s hkratno uporabo profesionalnih zdravstvenih kartic, ki jih lahko imajo samo usposobljeni zdravstveni delavci. Obe kartici morata biti vstavljeni v terminal, preden lahko pridemo do podatkov o bolniku. Ravno tako so določene različne ravni dostopa do podatkov, s čimer dodatno zagotovimo zasebnost. Na kartici so lahko shranjeni tudi podatki o dializi, krvni skupini, darovanju organov ali kroničnih boleznih, ki jih je treba zdraviti (srčne bolezni, sladkorna bolezen ...) Če pride do nesreče, lahko zdravstvena ekipa takoj ugotovi ključne medicinske podatke, kar lahko tudi reši življenje.

Bančništvo

V bančništvu se v glavnem uporabljajo magnetne kartice v obliki bankomatnih in kreditnih kartic. S pojavom pametnih kartic pa so se banke začele nagibati k novim načinom uporabe – k elektronskim denarnicam. Medtem ko se bankomatne kartice uporabljajo za takojšnje plačilo, kreditne pa za odloženo plačilo, so elektronske denarnice predplačniške. To pomeni, da ob izdaji kartica vsebuje določen znesek, ki se ob vsakem plačilu zmanjša. V večini primerov so uporabljeni mehanizmi, podobni tistim na telefonskih karticah. Te kartice so največkrat uporabne zgolj na napravah izdajatelja, na primer za plačevanje parkirnine. O pravih elektronskih denarnicah pa govorimo, kadar s karticami lahko plačujemo na raznih plačilnih mestih, predvsem manjše zneske, in ko ni potrebe po preverjanju vsake transakcije. Elektronske denarnice so tesno povezane s pravim denarjem. Če namreč ponaredimo denarnico ali uspemo spremeniti znesek na njej, je to ekvivalentno ponarejanju pravega denarja. Zato morajo elektronske denarnice uporabljati daljše ključe (npr. 2048 bitov za RSA ali 192 za kriptosisteme z eliptičnimi krivuljami).

Slovenija in svet

Trenutno predstavlja Evropa okrog 80 % tržišča pametnih kartic, 15 % predstavlja Azija in samo 5 % Severna Amerika. Vendar se delež neevropskih držav povečuje. Največ je predplačniških telefonskih kartic, ki predstavljajo več kakor polovico vseh izdanih kartic. Sledijo jim kartice GSM in bančne kartice. Zadnja leta smo priča množičnemu pojavljanju mobilnih telefonov tudi v Sloveniji. Zanimivo je, da tak razcvet opažajo v ZDA šele zdaj. Tudi sicer so pametne kartice v Ameriki precej manj razširjene kakor v Evropi. Razlog je nizka cena telefonskih pogovorov, zaradi česar ni bilo potrebe po predplačniških telefonskih karticah, pozneje pa je bilo pametne kartice težje uvajati.

Čedalje več držav uvaja tudi zdravstvene kartice. Tako je Nemčija že leta 1994 uvedla zdravstvene kartice (približno 65 milijonov), vendar pa je predvidena zgolj administrativna raba brez shranjevanja zdravstvenih podatkov. V Franciji so uvedli zdravstvene kartice leta 1998, v Sloveniji pa leta 1999. Trenutno potekajo v Evropi številni pilotski projekti, najbližje uvedbi pa so Španija, Belgija, Grčija in Italija. Belgija je za vojsko leta 2000 uvedla optične kartice, na katerih so shranjeni zdravstveni podatki.

V uporabi mobilnih aparatov prednjačijo prebivalci skandinavskih držav, Slovenci pa smo po številu aparatov na prebivalca v Evropi na zelo visokem mestu.

V transportu do zdaj še ni pravega razcveta, v Nemčiji potekajo razni pilotski projekti, v Sloveniji pa je bil uveden ABC. Za parkiranje v parkirnih hišah in na označenih parkiriščih se uporabljajo kartice z magnetnim trakom, z uvedbo enotne predplačniške pametne kartice pa bi se način plačevanja precej poenostavil.

V bančništvu se po svetu pojavljajo predvsem elektronske denarnice, najbolj znana je shema Mondex. Razvila jo je National Westminster Bank iz Velike Britanije, trenutno pa jo uporabljajo banke po vsem svetu. Mondex je edina večja shema na svetu, ki omogoča prenos denarja med dvema karticama Mondex. Najdlje obstoječa shema elektronskih denarnic je Danmont na Danskem, uvedena leta 1995, s poizkusnim uvajanjem v letu 1992. Znana je tudi belgijska shema Proton, ki podpira vnovično polnjenje kartic, njena posebnost pa je varen plačilni modul, nameščen na vseh prodajnih mestih. Visa je vpeljala več shem z blagovno znamko Visa Cash, mednarodni standard Visa Cash pa je bil objavljen leta 1997. Pri nas se pametne kartice uporabljajo zgolj kot možnost pri elektronskem poslovanju, kjer so namenjene shranjevanju certifikatov. To med drugimi omogočajo Nova ljubljanska banka, SKB banka, Nova kreditna banka Maribor, Poštna banka Slovenije, Gorenjska banka, Hypo banka ter Slovenska zadružna kmetijska banka. Glavni proizvajalci pametnih kartic so Gemplus, Schlumberger, Siemens, Hitachi, Thomson, NEC in Philips.

Da bi bile elektronske denarnice povsem ekvivalentne denarju, morajo omogočati transakcije med karticami. S tem je lastnikom omogočeno nakazovanje denarja sorodnikom, prijateljem in ponudnikom storitev, ki niso vključeni v mrežo trgovcev, katerim je kartica primarno namenjena, na primer hišnim pomočnicam in raznim serviserjem.

Najpreprostejše elektronske denarnice so za enkratno uporabo, modernejše oblike pa omogočajo vnovično polnjenje denarnice, pogosto kar na bankomatih ali na posebnih napravah v bankah. Kartice za enkratno uporabo so praviloma anonimne, medtem ko tiste za večkratno uporabo nosijo podatke, s katerimi se uporabnik lahko identificira.

Potreba po pametnih karticah se kaže tudi pri varnih elektronskih transakcijah. Skupina proizvajalcev, ki vključuje tudi Viso in MasterCard, je razvila standard SET (Secure Electronic Transactions), ki omogoča avtentikacijo in celovitost transakcije s kreditnimi karticami; SET uporablja številko računa, serijsko številko in datum poteka veljave, zato se lahko uporablja s katerokoli kreditno kartico. Čeprav SET ščiti podatke, ne more preprečiti goljufom in tatovom, da ne bi uporabljali ukradenih številk kartic, saj SET ne zahteva, da je kartica prisotna med transakcijo. Rešitev tega problema so pametne kartice in SET nameravajo dopolniti tako, da bo omogočal avtentikacijo kartice same – s tem bodo učinkovito onemogočene zgoraj opisane goljufije.

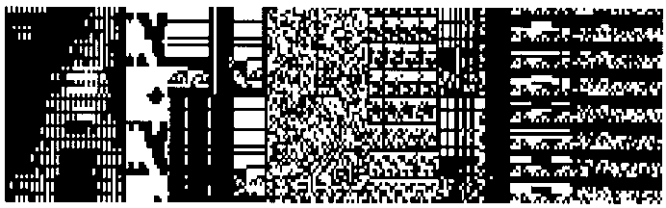
Zadnje čase se pojavljajo pametne kartice tudi v e-bančništvu za shranjevanje certifikatov, potrebnih za varno povezavo med uporabnikom in banko.

Transport

Zaradi čedalje večjih potreb po mobilnosti se mora vsak večji sistem prilagajati potrebam mobilnih uporabnikov. Pri izboljšanju mobilnosti pa nam lahko pomagajo pametne kartice. V transportu so primerne predvsem brezkontaktne kartice. V javnih prevoznih sredstvih lahko učinkovito nadomestijo klasične vozovnice, predvsem sezonske in mesečne, ki morajo biti bolje zaščitene pred poneverjanjem. Možne so tudi povezave med različnimi ponudniki, tako bi na primer uporabljali isto kartico za vlak in avtobus. Z razvojem razvedrilnih sistemov na letalih in vlakih pa se odpirajo nove možnosti uporabe. Pametne kartice lahko uporabimo tudi za cestninjenje, s čimer močno povečamo pretok vozil, saj se vozilu ni treba ustaviti, le hitrost mora zmanjšati, nekateri sistemi pa dopuščajo tudi večje hitrosti, tako da je cestninjenje lahko povsem neopazno.

Ključi in protokoli

Moderne kriptografske sisteme kontroliramo s ključi, ki določijo preoblikovanje podatkov. Seveda imajo tudi ključi elektronsko obliko (binarno zaporedje: 01001101010101...). Pretvorba podatkov pa ni edina naloga informacijske in računalniške varnosti. Lastnik ključa mora varno shraniti svoj ključ. Neprestano si moramo prizadevati za varnost ključev in za odgovornost zanje. Shamir in Someren (*Playing hide and seek with stored keys*, Financial Cryptography, LNCS 1648, 1999, str. 118-124) opozarjata, da je mogoče ključe, za katere mislimo, da so varno spravljeni na disku, učinkovito poiskati. Na sliki 9 vidimo, da je osrednji del pomnilnika, kjer se nahaja ključ, videti bolj naključen od drugih delov (črna točka predstavlja vrednost bita 1, bela pa vrednost 0).



▲ Slika 9: Namesto vizualnega iskanja si lahko pomagamo s približnim merjenjem naključnosti (npr. koliko različnih vrednosti bajtov se pojavi v vsakem kosu s 64 bajti – običajno 30, s standardno deviacijo 10, pri ključih pa 60, z odstopanjem od povprečja za največ 3).

Iz vsega zgoraj naštetega je očitno, da je smiselno shranjevati kriptografske ključe na ločenih napravah, kot so pametne kartice ali pa druge naprave, z vgrajenim sistemom, ki preprečuje njegovo odpiranje. Če se to vseeno zgodi, se samouniči celotni pomnilnik.

Pravila, ki določajo, kako uporabljamo kriptografske elemente, opisujejo protokoli. Na primer ko želimo stopiti k nekomu v pisarno, najprej potrkamo, počakamo na povabilo (Naprej!), nato odpremo vrata, pozdravimo in običajno še zapremo vrata. (Tudi če ne dobimo vabila, marsikoga zamika, da bi vseeno pritisnil na kljuko, pa čeprav to ni dovoljeno.) Tak je protokol za vstop v pisarno, če smo že prej dogovorjeni za sestanek, in če poteka v varnem okolju (v nasprotnem primeru bi bil protokol seveda precej drugačen).

Protokole seveda izvaja program, ki ga poganjamo v nekem operacijskem sistemu. Vendar pa se prav lahko zgodi, da je nekomu uspelo v naš računalnik vstaviti **trojanskega konja**, program, ki izvede običajno funkcijo, poleg tega pa naredi v ozadju (brez vednosti uporabnika) še nekaj nepričakovanega (za razliko od virusa se trojanski konj ne razmnožuje). M. Trampuš je za seminarsko nalogo na podiplomskem tečaju iz *Kriptografije in računalniške varnosti* na Fakulteti za računalništvo in informatiko (glej http://valjhun.fmf.uni-lj.si/~ajurisic) izdelal program, s katerim je prestregel klic podprograma v dinamični knjiž-

Kriptografske ključe je smiselno shraniti na ločenih napravah, kot so pametne kartice.

nici. Na ta način je izvedel napad na spletni brskalnik (Internet Explorer), ki uporablja SSL (angl. Secure Socket Layer) za zaščiten prenos podatkov, in napad na program za elektronsko pošto, ki omogoča podpisovanje sporočil (Outlook Express za kriptografske funkcije uporablja CryptoAPI). Tovrstne napade preprečimo tako, da otežimo zapis programa v pomnilnik za poznejše izvajanje in hkrati zaščitimo programsko kodo z MAC ali digitalnimi podpisi. Razvijalci modernejših pametnih kartic so se posvetili tudi tem problemom.

Da bi lažje razumeli potrebo po varnem načinu sporazumevanja, je v okvirju *vohunova dilema* predstavljen primer problema, ki lahko nastopi, če za varnost ni dovolj poskrbljeno ali če je protokol pomanjkljiv.

S takim problemom se srečamo tudi, ko želimo dvigniti denar na bankomatu, saj ne moremo biti prepričani, ali nas po geslu sprašuje banka ali pa je vmes kakšen posrednik ali lažni bankomat.

Vohunova dilema

Bilo je temno ko v rogu, ko se je vohun vračal v grad po opravljeni diverziji v sovražnem taboru. Ko se je približal vratom, je zaslišal šepetajoč glas:

Kako lahko vohun prepriča »stražarja«, da pozna geslo, ne da bi ga pri tem izdal morebitnemu vsiljivcu/prisluškovalcu?

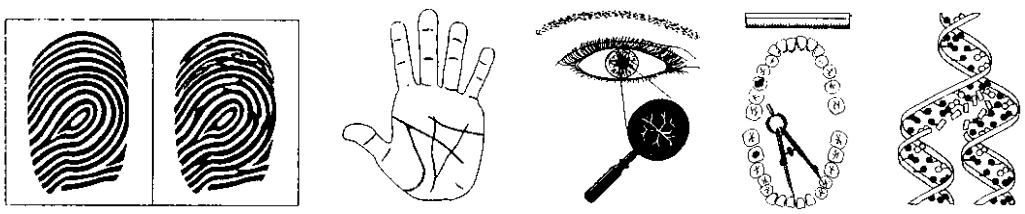
Identifikacija in delitev oblasti

Problem, ki se pojavi pri vohunovi dilemi, nastopi zato, ker nimamo učinkovite metode overjanja in identifikacije oseb, ki sodelujejo v protokolu. Pri tem izraz overjanje (avtentifikacija) pojmujemo kot potrditev pristnosti. Potrebne metode za rešitev problema lahko razvijemo s kriptografijo, pri tem pa si dodatno pomagamo s pametnimi karticami. Konkretne kriptografske metode bomo podrobneje opisali v drugem delu članka, tukaj pa si oglejmo samo vlogo, ki jo odigrajo pametne kartice.

V večini primerov je identifikacija le ena od funkcij pametne kartice. Pri tem lahko kartico uporabljamo na veliko načinov, npr. v velikem podjetju, kjer jo lahko uporabljamo za nadzor dostopa, zapisovanje števila fotokopij in časa telefoniranja, za plačilo obrokov v menzi, za knjižnico ... Če je treba, lahko v povezavi s centralnim sistemom večino računskih in pomnilniških operacij prepustimo sistemu.

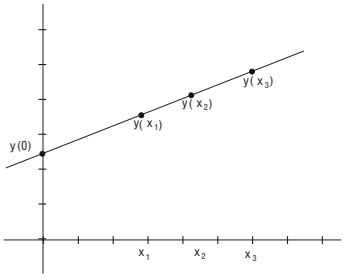
Evropa predstavlja 80 % tržišča pametnih kartic, Severna Amerika pa samo 5 %.

Kartice v velikosti modulov SIM lahko uporabljamo tudi za označevanje živali. Kartico jim preprosto vpnemo v uho ali ovratnico ali jo vstavimo pod kožo. V ta namen so uporabne predvsem brezkontaktne pametne kartice. Ta način označevanja precej poenostavi ugotavljanje izvora bolnih živali, kar je ob epidemijah, ki se zadnje čase pojavljajo, precej pomembno. Kartico lahko opremimo tudi z ustreznimi senzorji, tako da nas lahko ob kakršnikoli spremembi zdravja živali obvesti, mi pa lahko pravočasno ukrepamo. Tak način nadzora je tudi precej cenejši od klasičnih oblik, predvsem zato, ker lahko tukaj učinkovito izvedemo pogost nadzor (npr. brezžični terminal namestimo v vrata hleva in živali nadziramo ob vstopanju v hlev, pri tem bolne živali samodejno ločimo od zdravih, s čimer preprečimo širjenje bolezni).

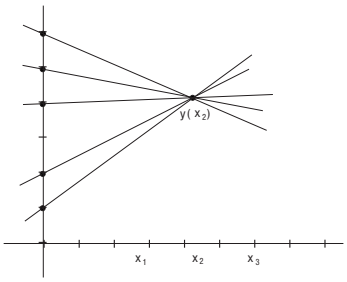


▲ Slika 10: Biometrični preizkus je preizkus za avtentičnost osebe na podlagi neponovljivih ali težko ponovljivih bioloških lastnosti, kot so prstni odtis, oblika roke, struktura ožilja na očesnem ozadju ali pa šarenice, zapis zob, DNK, glas, lastnoročni podpis ipd.

Če kartica ni namenjena interni uporabi (torej znotraj enega podjetja), potem mora omogočati tako overjanje uporabnika kakor overjanje podjetja, ki je kartico izdalo. Posebno pozornost je treba nameniti varnosti. Pri karticah, namenjenih širši javnosti, je pomembna tudi odgovornost izdajatelja, na primer pri osebnih izkaznicah, vozniških dovoljenjih in potnih listih. V vseh treh primerih mora kartica zagotavljati največjo možno stopnjo zaščite, saj so posledice zlorabe v teh primerih najhujše. Dodatni problemi nastopijo, če kartico uporabljamo tudi v avtomatiziranem okolju – brez prisotnosti ljudi. V teh primerih mora kartica zagotoviti avtentičnost uporabnika, za kar se največkrat uporabljajo biometrični preizkusi (glej sliko 10) in koda PIN.



▲ Slika 11: Pri delitvi skrivnosti dobi vsak le koordinato *y* svoje točke, ki jo ima shranjeno na pametni kartici. Program v trezorju ima še ustrezne od 0 različne koordinate *x*, zato lahko izračuna *y(0)*. Vsaki dve točki natanko določata premico in s tem ključ.



▲ Slika 12: Če imamo eno samo točko, ne moremo ugotoviti, kateri ključ je pravi, saj so vsi videti enako dobri.

Oglejmo si zdaj primer, ki je dokaj pogost v praksi: v neki banki morajo trije direktorji odpreti trezor vsak dan, vendar pa ne želijo zaupati kombinacije posamezniku. Zato bi radi imeli sistem, po katerem lahko odpreta trezor dva od njih. Ta problem lahko rešimo z (2,3)-stopenjsko shemo za deljenje skrivnosti, ki sta jo leta 1979 neodvisno odkrila Blakley in Shamir. Za njen opis zadošča, da se spomnimo osnovnošolskega znanja matematike, t.j. da premico določata dve točki. Ideja je prikazana na slikah 11 in 12. Posamezne dele skrivnosti seveda shranimo na pametnih karticah, ki ustrezno zagotavljajo avtentičnost lastnika, tako da kraja ali izguba kartice ne ogrozi varnosti sistema. V Rusiji uporabljajo (2,3)-stopenjsko shemo za nadzor jedrskega orožja (predsednik, obrambni minister, vrhovni vojaški poveljnik).

V splošnem je *(t,n)*-stopenjska shema metoda za delitev skrivnosti *K* med *n* oseb, 2 *?* *t* *?* *n*, za katero velja:

- poljubnih *t* oseb lahko izračuna vrednost *K*,
- katerakoli skupina z manj kot *t* osebami ne more izračunati prav nobene informacije o vrednosti *K*.

Za to shemo je dovolj, da v prejšnji rešitvi nadomestimo premico s polinomom stopnje *(t-1)* (iz srednje šole se spomnimo, da je tak polinom natanko določen s točkami *t*). Varnost te sheme je celo brezpogojna in neodvisna od računsko zahtevnega problema, kot je na primer faktorizacija v primeru RSA. Možne so seveda tudi razne posplošitve, kot je dodelitev različnih prioritet različnim osebam (na primer za dostop do vojaške skrivnosti sta potrebna dva generala ali pet majorjev) ... Sheme za delitev skrivnosti so vsestransko uporabne, saj jih lahko uporabimo povsod, kjer do podatkov dostopamo hierarhično. Tak način dostopa je dokaj pogost v velikih podjetjih, bankah in vojski. Za podrobnosti glej članek P.S. Gemmell, An Introduction to Threshold Cryptography, CryptoBytes 2/3 (1997), 7-12, ki je dosegljiv na naslovu http://www.rsasecurity.com/rsalabs/cryptobytes/..

»Varno« shranjeni ključi

Za ilustrativni primer si predstavljajmo finančno institucijo, ki uporablja managerjev PC za digitalni podpis finančnih transakcij. V času odmora (malica, kosilo, sestanek) se za nekaj minut pritihotapi v pisarno napadalec (tajnica, tehnik ali stranka). Recimo, da PC trenutno ni v omrežju in ga ne moremo uporabljati neposredno za digitalni podpis nepooblaščene finančne transakcije. Cilj napadalca je kar se da hitro preiskati gigabite podatkov na disku in najti tajni ključ za podpisovanje. Ta ključ je lahko zapisan v posebni datoteki (prekomerno zaupanje v varnost PC-ja) ali pa je vgrajen v kriptografski namenski program (slab design). Še slabše je, če je ključ shranjen v računalniku brez vednosti varnostno zavednega uporabnika (na primer v izmenjalni datoteki Windows, ki vsebuje vmesno stanje pri prejšnjem podpisovanju; v datoteki z varnostno kopijo, ki jo je naredil sistem samodejno v rednih časovnih intervalih; ali v poškodovanem sektorju, ki ga datotečni sistem ne upošteva več kot svojega). Napad je možen tudi, če ima napadalec le disketo s kratkim programom, nima pa na voljo dovolj velikega pomnilnika, kamor bi shranil celotno vsebino diska, in ne dovolj časa, da bi za podpis preizkusil vsako podzaporedje bitov z diska (npr. 10^{19} modularnih potenciranj za **napad z grobo silo**).

Pri uvajanju identifikacijskih kartic na nacionalni ravni se pojavi več problemov, eden od njih je tudi nadzor ljudi. Če ima državna organizacija dostop do vseh podatkov na karticah, lahko to močno ogrozi svobodo

▲ Slika 13: Nova slovenska osebna izkaznica

posameznika. Za primer vzemimo osebno izkaznico. Vsakič, ko se moramo identificirati, predložimo osebno izkaznico. Čip na kartici si vsako tako identifikacijo zapomni, ob prvem naslednjem stiku s centralnim sistemom pa zbrane podatke posreduje naprej. Tako lahko policija (ali pa celo vojska) izdela natančen profil vsakega državljana, ki poseduje osebno izkaznico. Nadzor nad problematičnimi osebami bi bil tako precej poenostavljen. Še huje bi bilo, če bi bile kartice brezkontaktne. V tem primeru se sploh ne bi zavedali, kdaj kartica komunicira. Policija bi na skrita mesta postavila terminale in nato samo zapisovala, katere osebe so na določenem mestu. Anonimnost in zasebnost bi povsem izginili iz našega življenja, nadzor bi bil popoln. Takšne in podobne črne scenarije je seveda treba in možno preprečiti, toda za to je potrebna velika mera usklajevanja, predvsem pa urejenost zakonov na tem področju.

Osebnih izkaznic v obliki pametnih kartic v Evropi in po svetu še ni. Razlog je predvsem pomanjkanje ustreznih zakonov. Pri uvajanju nove osebne izkaznice v Sloveniji (slika 13) se je sicer možnost pametne kartice pojavila, vendar ni bila sprejeta. Tako je nova osebna izkaznica samo plastična, ne pa tudi pametna.

Pametni kartici na pot

Do kakšne mere lahko postane pametna kartica v povezavi z obstoječimi računalniki in zbirkami podatkov v bližnji prihodnosti neke vrste osebna izkaznica in instrument v rokah sistema (ali birokracije)?

»Osebna izkaznica je najbolj premetena oblika terorja.«
E. v. Salomon

Pametna kartica – quo vadis?* Ali predstavlja, v tem ne ravno pogumnem novem svetu novo stopnjo kontrole posameznikov in s tem še večji nadzor? Ali pa pomeni ukrotitev potenciala pametnih kartic način, s katerim si bomo povrnili pravice do samoodločbe in zasebnega življenja ali vsaj zagotovilo za status quo?

Že danes je jasno, da je pametna kartica močno orodje, in ki bo prej ali slej postala pomembnejša od osebnih računalnikov. Et respice finem!** Pametna kartica z ustrezno programsko opremo lahko predstavlja osnovo za številne sisteme. Ko jo prilagodimo posamezniku, odpre nove možnosti. Izberimo si pravo pot, pot neodvisnosti!

Aleksandar Jurišić
Jernej Tonejc

* Kam greš? ** Ozri se na konec!