MIKROPROCESORSKA KARTICA IN KARTIČNI OPERACIJSKI SISTEM

Peter Pehani

Povzetek

Uporaba mikroprocesorskih oz. pametnih kartic (angl. smart cards) se intenzivno širi na mnoga področja človekovega delovanja. Pametna kartica je kartica z mikroračunalnikom, ki ga nadzira kartični operacijski sistem. Kartični operacijski sistem je trajno shranjen v pomnilniku ROM. Njegovi prioriteti sta varno izvajanje ukazov, ki prihajajo v mikroračunalnik od zunaj, ter nadzor dostopa do podatkov, ki so shranjeni v kartičnem pomnilniku EEPROM.
Kartični operacijski sistemi prihodnosti, ki so v povojih, bodo omogočali sožitje več aplikacij na isti kartici, večjo prilagodljivost kartice za kasnejše spremembe, ipd.

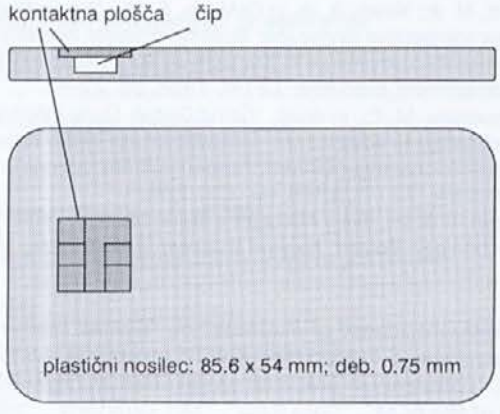
Abstract

Use of microprocessor cards - or smart cards - is spreading intensively on many fields of human activity. Smart card is a card with a microcomputer that is controlled by a card operating system. Card operating system is loaded permamently into ROM. Its priorities are secure execution of commands that enter into the microcomputer from outside world, and control of access to the data that are stored in the EEPROM.
Future card operation systems will enable sharing of more applications on a single card, greater flexibility of the card for possible changes, and so on.

1. UVOD

Kartice so hitro razvijajoča se veja informacijske tehnologije. Medtem, ko so koncem osemdesetih let svoj pohod začele *magnetne kartice*, so jim v devetdesetih sledile najprej *pomnilniške kartice* in nato še *mikroprocesorske kartice*.

Vsaka kartica je sestavljena iz nosilca standardnih dimenzij, na katerega je pritrjen pomnilniški medij. Našteti trije tipi kartic se razlikujejo po tem, kateri medij služi za shranjevanje podatkov: pri magnetnih karticah je to magnetni trak, pri pomnilniških pomnilniški čip, pri mikroprocesorskih pa mikroračunalnik z mikroprocesorjem. Tipični primeri za magnetne kartice so bančne in kreditne kartice, za pomnilniške telefonska kartica, za mikroprocesorske pa kartica zdravstvenega zavarovanja (pri nas v uvajanju). Obstaja še en tip kartic - *optične kartice*, pri katerih se informacija shranjuje na plasti, občutljivi za laserske žarke. Zaradi tehnologije, ki je draga in ki zaenkrat omogoča le enkraten zapis na neko lokacijo, te kartice še niso doživele široke uporabe.



Slika 1: Mikroprocesorsko kartico sestavljajo: nosilec, kontaktna plošča in mikroprocesorski čip.

Uporabljata se tudi imeni *čipne kartice* oz. *kartice z integrirnim vezjem*; to so pomnilniške in mikroprocesorske kartice, ker je v njih vstavljen čip. Glavna razlika med pomnilniškimi in mikroprocesorskimi karticami je v tem, da ima pomnilniška kartica v osnovi le preprosto varnostno logiko s kontrolo dostopa do pomnilnika pri branju in pisanju. V mikroprocesorsko kartico pa je vgrajen mikroračunalnik, ki ga je prek kartičnega operacijskega sistema mogoče programirati. Mikroprocesorska kartica ima visoke zmogljivosti pomnilnika, podatki so varno in dolgotrajno shranjeni, možno je izvajati razne kriptografske funkcije in druge algoritme. Tudi zato mikroprocesorske kartice večkrat imenujemo *pametne kartice* (angl. *smart cards*). Raba imena pa ni dosledna; včasih se uporablja le za mikroprocesorske kartice, včasih pa za mikroprocesorske in pomnilniške kartice skupaj. V članku uporabljamo naziv pametne kartice v ožjem smislu samo za mikroprocesorske kartice.

Čipne kartice se najbolj široko uporabljajo pri telekomunikacijah (80 % vseh v uporabi), kot telefonske in GSM kartice. Uporaba čipnih kartic se širi na področja bančništva, prometa, kontrole dostopa, zdravstva in trgovine. Kartica bo kmalu postala redni spremljevalec osebnega računalnika in bo uporabniku omogočala varen in zanesljiv vstop v informacijska omrežja.

Zavod za zdravstveno zavarovanje Slovenije (ZZZS) bo obstoječo zdravstveno izkaznico zamenjal s *kartico zdravstvenega zavarovanja* (KZZ). Za KZZ je bila izbrana mikroprocesorska kartica, ker nudi od vseh kartic najbolj varno okolje za shranjevanje občutljivih zavarovalniških in medicinskih podatkov.

2. MIKRORAČUNALNIK V MIKROPROCESORSKI KARTICI

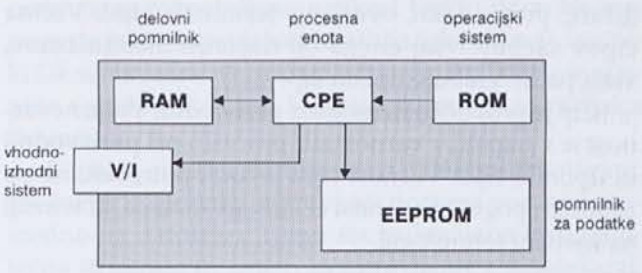
2.1. Mikroračunalniški čip

Čip, ki je vgrajen v mikroprocesorsko kartico, je kot majhen računalnik. Vsebuje naslednje komponente (glej sliko 3) [3, 4, 5, 6]:

- *Centralno mikroprocesorsko enoto* (CPE); CPE večinoma temeljijo na Motoroli 6805 in Intelu 8051; hitrosti do 5 MHz; večinoma so 8-bitne, modernejše pa so 16-bitne.
- Tri vrste pomnilnikov:
  - *RAM - delovni pomnilnik* (angl. Random Access Memory). Shranjuje začasne informacije med delovanjem procesorja. Za svoje delovanje rabi zunanji vir napetosti. Običajne velikosti so med 128 in 512 bajtov. Hitrost pisanja je velikostnega reda 10 ns.
  - *ROM - trajni pomnilnik* (angl. Read Only Memory). Vanj je tovarniško trajno naložen kartični operacijski sistem ali drugo programje za stalne funkcije (angl. *mask*). Ni ga možno naknadno spreminjati.
  - *EEPROM - bralno-pisalni pomnilnik* (angl. Electronically Erasable Programmable Read Only Memory). Služi za shranjevanje uporabnikovih podatkov. Opravlja podobno funkcijo, kot jo ima trdi disk na PC-ju. Navadno zavzema največ prostora v čipu, je največji porabnik energije ter tudi najdražji od vseh pomnilnikov. Prenese med 10.000 in 500.000 ciklov pisanja. Obstojnost podatkov je navadno 10 let. Hitrost pisanja je velikostnega reda 1 ms.
    EEPROM se lahko uporabi tudi za shranitev dopolnilnega kartičnega operacijskega sistema. Začasno se ga lahko uporablja tudi kot dopolnitev RAM-a, z 10^6-krat počasnejšim dostopom.
    Namesto EEPROM-a se lahko uporabita še pomnilnika Flash ali FERAM, ki porabita manj prostora glede na EEPROM in sta precej hitrejša (hitrost pisanja je pribl. 10 ms oz. 100 ns), vendar zaradi različnih vzrokov še nista dosegla tako široke uporabe.

Nobeden od naštetih pomnilnikov ni dostopen neposredno. Vsak zunanji dostop gre preko procesne enote ter varnostne logike.

- *vhodno-izhodni sistem*; dvosmerni serijski vmesnik.



Slika 3: Arhitektura mikroračunalnika v mikroprocesorski kartici.

	magnetna kartica	čipna kartica		optična kartica
		pomnilniška k.	mikroproc. k.	
pomnilniški medij	magnetni trak	pomnilniški čip	mikroračunalnik	optično občutljiva plast
pomnilniška kapaciteta	< 1 kB	0.256 - 2 kB	1 - 64 kB	1000 - 16000 kB
večkratno zapisovanje	DA	DA	DA	NE
varnost proti ponarejanju	majhna	srednja	zelo velika	velika
zaščita proti kopiranju	majhna	srednja	zelo velika	majhna
stopnja standardizacije	do detajlov	delno	delno	v povojih
primer	bančne kartice, kreditne kartice	telefonske kartice	k. zdravstvenega zavarovanja, k. za mobilni telefon	

Slika 2: Primerjava različnih tipov kartic [4].

Čip mikroprocesorske kartice lahko vsebuje dodatne strojne elemente kot so *kontrolne enote* za nadzor napetosti, ure in strojne varnostne logike (dostopanje do pomnilnikov, ipd, *generator naključnih števil* za izvajanje obojestranskega overjanja ter *matematični koprocesor* za izvajanje raznih kriptografskih algoritmov.

Velikosti vseh treh pomnilnikov v čipu mikroprocesorske kartice so relativno majhne v primerjavi z drugimi mikroprocesorji, ker morajo biti izredno majhni. Debelina mikroprocesorske kartice je 0.75 mm. Čipi mikroprocesorskih kartic so redko večji od standardiziranih 25 mm^2, saj pri večjih čipih obstaja nevarnost zloma. V borbi za več pomnilnika gre razvoj v izboljšavanje natančnosti tehnologije, ki je trenutno okoli 0.5 mm in napreduje v skladu z Moorovim zakonom.

Čip je na razne načine zaščiten pred zunanjimi vdori in poskusi analiz od zunaj. Vdori so lahko bolj strojne narave, npr. mikroskopski pregled čipa, ali bolj programsko-procesne narave, npr. analize odzivov na nizke frekvence, odzivnih časov, induciranih napak izven delovnega območja (temperatura, obsevanje). Proti prvim se uporabljajo naslednji obrambni mehanizmi: mešanje vodil, mešanje naslovov pomnilniških celic oz. navidez naključno nelogično razporejanje elementov po plasteh, varnostne prevleke plasti čipa, zavajujoče prazne komponente, ipd. Proti drugim pa: detekcija nizkih in visokih frekvenc, detekcija temperature, prazni takti, overjanje terminala., ipd. Večina čipov vsebuje vsaj enega od naštetih mehanizmov, vseh pa ne vsebuje noben čip.

Čip je praktično nemogoče ponarediti. Večja nevarnost je v napaki v varnostnih procesih pri proizvodnji in uporabi čipa. Varnost čipa je torej potreben, ne pa zadosten pogoj za varnost celotnega sistema, ki temelji na kartični tehnologiji.

2.2. Kontaktne in brezkontaktne mikroprocesorske kartice

Vmesnik med čipom in zunanjim svetom je kontaktna plošča s šest ali osem kontakti, ki prekriva čip. Kontaktna plošča je najbolj izpostavljen del celotnega tokokroga, izpostavljena obrabi, mehanskim poškodbam, pa tudi zlorabi. Komunikacija prek kontaktne plošče je običajen in najbolj razširjen način komunikacije z zunanjim svetom. Mikroprocesorske kartice s kontaktno ploščo imenujemo tudi *kontaktne*.

Mikroprocesorski čip pa lahko komunicira z zunanjim svetom še na en način: prek antene s pomočjo radijskih valov. Take kartice imenujemo *brezkontaktne kartice*. Antena zbira tudi energijo, potrebno za delovanje mikroračunalnika. Razdalja komunikacije je velikostnega reda 1 m in je prvenstveno odvisna od čitalnika (njegove frekvence). Brezkontaktne kartice so zelo primerne za uporabo v transportu in kontroli dostopa, manj pa za prenos zaupnih podatkov. Zaradi kompleksnejše strukture so dražje od kontaktnih, tehnologija še ni tako dognana.

2.3. Standardi

Kartice določajo standardi mednarodnih organizacij za standardizacijo ISO/IEC, CEN, ETSI, ipd, po posameznih industrijskih panogah pa jih dopolnjujejo industrijski standardi, ki jih določajo konzorciji največjih svetovnih proizvajalcev.

Od mednarodnih standardov je za kontaktne mikroprocesorske kartice najvažnejši ISO/IEC 7816 [7]. Gre pravzaprav za množico standardov - do sedaj je sprejetih že 10 delov - ki že več kot 10 let sledi razvoju tehnologije mikroprocesorskih kartic. Standard ISO/IEC 7816 določa fizične karakteristike kartic, dimenzije kartic, lokacije kontaktov, tipe označevanja, protokole komunikacije s svetom, priporočila za kartični operacijski sistem, nabor ukazov kartičnega operacijskega sistema, organizacijo podatkov na karticah, varnostne mehanizme, ipd.

Najpomembnejše industrijske standarde po panogah pripravljajo naslednje skupine:

- EMV (Europay, Mastercard, Visa): specifikacije funkcij kartic v bančništvu;
- ETSI (European Telecommunication Standards Institute): standardi za kartice v navadni in mobilni telefoniji;
- OpenCard Framework: vključitev mikroprocesorskih kartic v omrežja,
- SC/PC (Smart Card Personal Computer): vključitev mikroprocesorskih kartic v osebni računalnik.

3. KARTIČNI OPERACIJSKI SISTEM

Operacijski sistem je nekak posrednik med strojno opremo in aplikacijskim programjem. Gre za skupino sistemskih programov in nanje navezanih ukazov. Z ukazi zunanji svet (uporabnik) komunicira z računalnikom, ne da bi mu bilo treba poznati strojno opremo. *Kartični operacijski sistem* (angl. *COS - card operating system*) se ne more primerjati z obširnimi večopravilnimi sistemi na večjih računalnikih (npr. nima dela z zunanjimi napravami za komunikacijo z uporabnikom, vedno komunicira z računalnikom), kljub temu pa opraviči svoje ime. Prioriteti kartičnega operacijskega sistema sta varno izvajanje programov ter nadzor dostopa do podatkov.

Količina programske kode je zelo majhna, velikostnega reda 10 kB. Praviloma je koda spravljena v ROM-u. Tja se trajno shrani že med proizvodnjo čipa. Kasnejše spremembe niso možne, verjetnost za načrtno ali nenamerno spremembo vsebine ROM-a je praktično ničelna. Prav zato mora biti operacijski sistem, preden se vloži v ROM, celovit in praktično brez napak. Mnogo časa se posveča testiraju in odpravi napak. Zaradi

majhne procesorske moči in omejenih pomnilniških kapacitet pa mora ustrezati še naslednjim zahtevam: mora biti hiter pri izračunih, optimiziran glede porabe pomnilnika, robusten in zanesljiv, zaupen in vedno na razpolago.

Vsi operacijski sistemi dopuščajo, da se posamezne njegove funcije naložijo v EEPROM, ki sicer služi za shranjevanje podatkov.

Glavne naloge operacijskega sistema so:

- prenos podatkov na kartico in obratno;
- nadzor nad izvajanjem ukazov, časovno usklajevanje, notranja kontrola ukazov;
- ravnanje s podatki oz. z datotekami v EEPROM-u, s poudarkom na varnosti;
- ravnanje s kriptografskimi funkcijami in njihovo izvajanje;
- polnitev kartice z osebnimi podatki in kontrola življenjskega cikla kartice;
- pogosto: izvajanje aplikacijskih funkcij ali aplikacijske kontrolne logike (npr.: zmanjšanje vrednosti v elektronski denarnici, ipd.).

Proizvajalci procesorjev opremijo čip z okleščenim operacijskim sistemom z minimalnim naborom ukazov in funkcij, potrebnih za upravljanje z mikroračunalnikom. Nabor ukazov, ki jih mora kartični operacijski sistem podpirati, sestavljajo: ukazi za delo z aplikacijami in njihovimi podatki (branje, pisanje/obnavljanje, izbiranje), razni varnostni ukazi (izmenjava naključnih števil, preverjanje gesel in ključev, zapiranje dostopa), ipd.

Nabor s standardom predpisanih ukazov v praksi je le osnovni nabor ukazov. Ta nabor proizvajalci kartic razširijo z lastnimi ukazi, ki jih je pogosto še enkrat toliko kot osnovnih. Za množične aplikacije razvijejo proizvajalci kartic svoje kartične operacijske sisteme, ki jih vgradijo v čip ob proizvodnji. Iz enakega čipa tako nastane več različnih kartic, vsaka opremljena z drugačnim operacijskim sistemom. Proizvajalčevi specifični ukazi so dodatni ukazi za zagotavljanje varnosti (preverjanje elektronskega podpisa, obojestranske identitete, ...), ukazi za ravnanje z datotekami (ustvarjanje in brisanje datotek), ipd.

Operacijski sistemi različnih proizvajalcev niso kompatibilni. Razvoj aplikacij za vsak operacijski sistem zato zahteva natančno poznavanje tega sistema. Razloga za nekompatibilnost sta vsaj dva: odprtost standardov za različice in modifikacije operacijskih sistemov (standardi premalo strogi, preveč odprti) ter dodajanje novih funkcionalnosti, ki niso definirane v standardih. Poleg tega tehnologija in raba prehitevata standarde. Večina kartic, ki so sedaj v uporabi, je bila načrtovana pred objavo standardov.

Podrobnosti operacijskih sistemov so skrbno varovane skrivnosti. Opisovanje kartičnega operacijskega sistema je možno le fenomenološko, na splošnem nivoju. Uveljavljeni kartični operacijski sistemi se naslanjajo na standard ISO 7816-4, ki temelji na datotečni organizaciji podatkov v EEPROM-u.

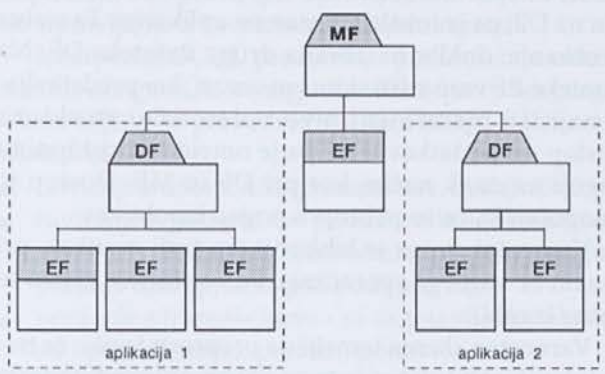
3.1. Datoteke, ki jih podpira kartični operacijski sistem

Strukturo datotek v EEPROM-u, ki jo podpirajo kartični operacijski sistemi, določa standard ISO 7816-4. Struktura je hierarhična, drevesna, povsem podobna DOS-ovi strukturi. Sestavljajo jo naslednji *tipi* datotek:

- *MF* - glavna datoteka oz. glavni imenik (angl. *Master File*): vsebuje vse druge datoteke in imenike. Obsega ves razpoložljivi prostor za datoteke.
- *DF* - namenska datoteka (angl. *Dedicated File*) je datoteka v vlogi imenika; je nekakšna višja organizacijska enota; vanjo so naložene sorodne elementarne datoteke ali imeniki, ki pripadajo skupni aplikaciji.
- *EF* - elementarna datoteka (angl. *Elementary File*) je datoteka s podatki. Postavljena je pod MF ali DF. Datoteka EF ima lahko različno *strukturo*, glede na organizacijo zapisov. Strukture so: trasparentna - EF brez notranje stukture; linearna fiksna - sestavlja jo več enako dolgih nizov; spremenljiva fiksna - sestavljajo jo nizi različnih dolžin; linearna ciklična - enako dolgi nizi, ki se polnijo v cikličnem zaporedju. Izbira strukture EF je pogojena s podatki.

Število nivojev v datototečnem drevesu je poljubno, omejuje ga razpoložljiva velikost EEPROM-a. Najbolj pogosta je trostopenjska hierarhija (glej sliko 4). Imeniki DF so navadno vezani na *aplikacijo*. Aplikacija je skupina sorodnih datotek, ki imajo skupnega upravljalca (lastnika).

Kartični operacijski sistemi so objektno orientirani, pri čemer so podatki o pravicah dostopa vezani neposredno na datoteko. Temu sta prilagojena tudi datotečna struktura in sistem za upravljanje z datotekami. Vsako datoteko sestavljata dva dela: glava (angl. header, file descriptor) in telo (angl. body). Navadno sta fizično na ločenih lokacijah. Glavo datoteke trajno določimo ob vzpostavljanju datoteke. Glava vsebuje



Slika 4: Drevesna struktura datotek v EEPROM-u z vsemi tremi tipi datotek: MF, DF in EF. Struktura predstavlja dvo-aplikacijsko kartico; vsaka aplikacija je na svojem imeniku DF.

lastnosti datoteke: ime, tip, struktura, velikost, lega v drevesu, varnostni atributi (npr.: pristopni pogoji) in drugi atributi. Telo datoteke vsebuje spremenljive uporabnikove podatke, ki jih je mogoče večrat brati in pisati. Izbira datotek poteka na osnovi logičnih naslovov. Te mora poznati terminal, ki pošilja ukaze na kartico.

3.2. Varnostna shema kartičnega operacijskega sistema

Varnostna shema, ki jo podpira kartični operacijski sistem, vsebuje: pristopne mehanizme, pristopne pogoje in varnostni status.

Pristopni mehanizmi so ukazi ali kombinacije ukazov, ki spreminjajo varnostni status in s tem omogočajo delo z datotekami. To so naslednji mehanizmi:

- identifikacija lastnika: preverjanje, ali je kartica v pravih - t.j. lastnikovih - rokah prek poznavanja gesla oz. osebne kode PIN (angl. personal identification number);
- overjanje zunanjega okolja: preverjanje, ali kartico bere pravo okolje; okolje dokaže poznavanje šifrirnega ključa;
- overjanje kartice: obratno - okolje preveri, ali kartica pozna šifrirni ključ.

Pristopni pogoji do posamezne datoteke določajo predpogoje, ki morajo biti izpolnjeni, preden se lahko nad datoteko izvedejo ukazi. Pristopni pogoji se za vsako datoteko v EEPROM-u določijo ob izgradnji datoteke. Zapisani so v glavi datoteke in so trajni. Odvisni so od tipa datoteke ter od zaupnosti podatkov v datoteki. Do datotek dostopamo z različnimi zunanjimi ukazi, ki so bralno-zapisovalni ali administrativni (npr.: branje, pisanje, iskanje, onemogočanje, zaklepanje, brisanje, dodajanje, ...). Pristopni pogoji so definirani za vsak ukaz posebej. Dostop do datoteke s posameznim ukazom je lahko prost, omejen s pristopnim mehanizmom (geslom ali ključem), ali pa prepovedan.

Varnostni status predstavlja stanje po izvedenem pristopnem mehanizmu. Status je vezan na datoteke MF in DF. Status, vezan na MF, je celovit. Status, vezan na DF, pa je lokalen, vezan na aplikacijo. Ta status se ohranja, dokler ni izbrana druga datoteka DF. Na datoteke EF varnostni status ni vezan, ker predstavljajo najnižji hierarhični nivo v datotečni strukturi. Dostop do podatkov v EF pa je omejen s pristopnimi pogoji na enak način, kot pri DF in MF. Dostop je omogočen le, če so pristopni pogoji izpolnjeni.

Varnostni status je lahko vezan tudi na ukaz, pri ukazih t.i. varnega sporočanja. Po končanem ukazu se status izgubi.

Varnostna shema temelji na preprosti logiki: če trenutni varnostni status ustreza zahtevanim pristopnim pogojem, je omogočen dostop do datotek in izvedba nadaljnjih ukazov, kot so branje, pisanje, prehod v nižji hierarhični nivo po datotečnem drevesu. Niže gremo lahko le, ko zadovoljimo pogoje na višjem nivoju.

V varnostno shemo sodita še dva varnostna mehanizma, ki ne spreminjata varnostnega statusa, služita pa za varen prenos podatkov. To sta:

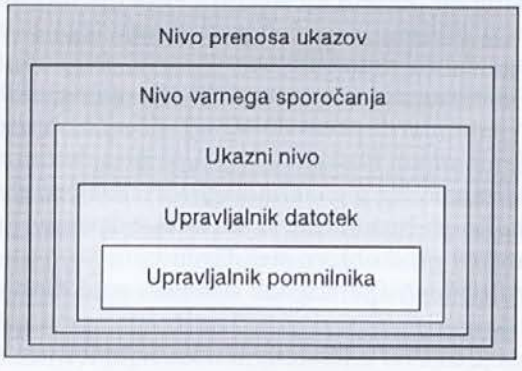
- zagotavljanje celovitosti podatkov: preverjanje, ali se je kak del podatkov pri prenosu izgubil ali je bil "ukraden"; prek šifrirne kode MAC (angl. massage authentication code);
- zagotavljanje zaupnosti podatkov: preprečevanje branja podatkov tretji osebi se zagotovi s šifriranjem s simetričnim ali asimetričnim algoritmom.

3.3. Izvajanje ukazov v kartičnem operacijskem sistemu

Izvajanje ukazov, ki pridejo od zunaj, poteka v več nivojih, ki jih podpira kartični operacijski sistem. To zagotavlja večjo varnost.

Ukaz pride iz zunanjega sveta preko vhodno-izhodnega sistema. Najvišji nivo (angl. transport manager) nadzoruje prenos podatkov s standardnimi protokoli, poleg tega pa nadzira pravilnost prenosa ukazov. Nivo t.i. varnega sporočanja (angl. secure messaging manager) opravi zahtevane kontrole in dešifriranja. Če niso zahtevane, je ta nivo povsem transparenten.

Sledi ukazni nivo (angl. command handling), ki izvaja ukaze in nadzira njihovo izvajanje. Ta nivo prepozna ukaz, opravi kontrolo pravilnosti zaporedja ukazov ter izvede ukaz, če je v trenutnem stanju dovoljen. Zaporedje ukazov se lahko definira vnaprej. Predpisano zaporedje nadzoruje avtomatski nadzor ukazov, ki je postavljen med prepoznavo ukazov in med izvedbo ukazov. Avtomatski nadzor ukazov je paralelna zaščita, ki dopolnjuje zaščito s pravicami dostopa do posameznih datotek. Gre za nekakšno vgrajeno kontrolo izvajanja zaporedja ukazov. Običajno se ta kontrola definira za kratka, a pomembna zaporedja ukazov. Pogost primer so overjanja, kjer morajo ukazi prihajati točno v določenem vrstnem redu. V primeru napačnega vrstnega reda ukazov ali napačnih parametrov overjanje ne uspe in avtomatski nadzor ukazov vzpostavi predhodno stanje.



Slika 5: Nivojska struktura kartičnega operacijskega sistema

Datotečni nivo (angl. file manager) zagotavlja podporo in upravlja z različnimi tipi datotek EF in DF. Če ukaz zahteva dostopanje do datotek, ta nivo prevede logične naslove datotek v fizične. Nadzira tudi pravice dostopa do datotek. Pomnilni nivo (angl. memory manager) skrbi za kontrolo dostopanja do posameznih delov pomnilnika, ureja prosti pomnilnik, izvaja kontrole na nivoju pomnilnika.

Sestavljanje odgovorov je naloga centralnega upravljalnika odgovorov (angl. central return code manager). Upravljalnik pripravlja in razpošilja odgovore tako za notranje nivoje kot za zunanji svet v vseh fazah izvajanja ukaza.

Komunikacija med čitalnikom in kartico poteka po enem samem kanalu, v t.i. polodupleks (angl. half duplex) načinu. Terminal igra vlogo strežnika, ki pošlje ukaz. Kartica pa igra vlogo uporabnika, ki ukaz izvede in vrne odgovor. Vsa komunikacija poteka po sistemu ukaz - odgovor. Nikdar ne pride pobuda s kartične strani.

4. KARTICE PRIHODNOSTI

Daljnoročni cilj razvijalcev mikroprocesorskih kartic je, da bi lastnik z eno kartico lahko opravil več storitev. Poplava vsemogočih kartic za različne namene ta logični razvojni premik že implicitno zahteva: prehod od posamezne kartice za vsako *aplikacijo* na t.i. *večaplikacijsko kartico* (angl. multiapplication card), ki vsebuje več aplikacij in pokriva funkcionalnost več kartic. Pojem "aplikacija" predstavlja skupek funkcij, ki pripadajo istemu poslovnemu subjektu (podjetju, organizaciji, državni službi, javni službi, ...). Večaplikacijska kartica pomeni deljeno lastništvo in odgovornost med več poslovnih subjektov, kar skriva zapleteno shemo poslovnih, organizacijskih, finančnih, tehnoloških in varnostnih vprašanj.

Večaplikacijske kartice ne gre mešati z *večfunkcionalno kartico*. Večfunkcionalna kartica je opremljena z aplikacijo, katere lastnik in izdajatelj je en sam poslovni subjekt. Aplikacija na njej lahko opravlja različne *funkcije*, vendar vse v službi istega lastnika, zato je njen razvoj razmeroma preprost. Primer je večfunkcionalna kartica večjega podjetja, opremljena z aplikacijo, ki opravlja naslednje funkcije: kontrola prihodov-odhodov, kontrola dostopa do varovanih objektov, mesečna karta za mestni avtobus, plačevanje malice v menzi.

Večaplikacijske kartice bi potrebovale operacijski sistem, podoben klasičnim operacijskim sistemom, z naslednjimi zahtevami:

- Podpora več-aplikativnosti: uporabnik ima le eno kartico, ki gosti aplikacije različnih lastnikov z različnih področij življenja (plačilni promet, zdravstveno in socialno varstvo, transport, vladni in splošni dokumenti, elektronsko poslovanje, telekomunikacije).
- Varnost: soobstoj več aplikacij, pogosti prenosi podatkov ter izguba kartice so veliki riziki. Nujni so dodatni mehanizmi, ki omogočajo souporabo delov podatkov in programja med aplikacijami, po drugi strani pa varnostni mehanizmi pri razmejevanju dostopov med zaupnimi podatki posameznih aplikacij. Druge nujne dopolnitve: kompleksen sistem upravljanja s ključi; poostrene sheme overjanja terminala, kartice in aplikacije.
- Interoperabilnost kartice na vseh dostopnih točkah, ki se doseže s skladnostjo z vsemi mogočimi standardi ter obsega kompatibilnost med posameznimi tipi kartic, operacijskimi sistemi in spremljevalnimi orodji (čitalniki kartic).
- Prilagodljivost in odprtost: operacijski sistem naj omogoča dinamično dopolnjevanje funkcionalnosti; standardizirano nalaganje novih aplikacij na kartice v obtoku na varen in zanesljiv način; sistem upravljanja z aplikacijami, ki ji kartica vsebuje, in njihovimi verzijami.

Narejenih je bilo že nekaj poskusov, približati se takemu odprtemu operacijskemu sistemu:

- operacijski sistem za podporo bazam podatkov po standardu ISO 7816-7
- modularni interpreterji, npr. Java
- večaplikacijski operacijski sistemi, npr. MULTOS

4.1 Kartice s podporo bazam podatkov

Kartice s podporo bazam podatkov slonijo na že sprejetem standardu ISO 7816-7. Standard predpisuje objekte baze podatkov na kartici, uporabniške profile ter ukaze jezika SCQL (angl. smart card query language), ki služi kot interpreter za običajni jezik SQL.

Objekti baze SCQL so podobni objektom v običajnih bazah podatkov: tabele, pogledi (podmnožice tabel), sistemske tabele (objekti, uporabniki, dostopne pravice). Uporabniški profili so hierarhično strukturirani v tri razrede: lastnik baze podatkov, lastnik posameznega objekta v bazi, uporabnik. Uporabniški razredi določajo pravice uporabnikov. Višji razredi dopuščajo več pravic pri upravljanju z objekti tabele, ter upravljanje z hierarhično nižjimi razredi.

Interpreter SCQL predstavlja podmnožico ukazov standardnega SQL-a (angl. standard query language). Ukazi SQL-a se prevedejo v ukaze SCQL-a. Ukazi so naslednji:

- ravnanje z uporabniki (predstavitev, dodaj/odvzemi),
- ravnanje s podatki oz. podatkovnimi objekti (ustvari bazo, dodaj/odvzemi tabelo, pogled, omogoči/prekliči dostop, briši/piši podatek, ...),
- ravnanje s transakcijami - za zagotavljanje celovitosti operacij (začni, prekini, ponovi).

V nasprotju z uveljavljenimi operacijskimi sistemi, ki temeljijo na standardu ISO 7816-4, je baza podatkov SCQL precej bolj fleksibilna in omogoča:

- enostavno spreminjanje dostopnih pravic;
- dinamično ravnanje s pomnilnikom (glede na zasedenost in dolžino podatkov);
- različna overjanja, ki jih je možno kombinirati v poljubni kombinaciji;
- kontrolo celovitosti procesov pri transakcijah;
- iskanje po bazi.

4.2. Java kartice, MULTOS kartice

Java je programski jezik, ki teče na številnih mikroprocesorskih platformah. Je popolnoma objekten jezik z dobrimi varnostnimi mehanizmi, zato je primeren tudi za uporabo na mikroprocesorskih karticah.

Java kartica temelji na modularnem sistemu. Interpreter je naravna rešitev, saj je pri kartici včasih težko ločiti strojni del od programskega; sta zelo prepletena. Ideja je naslednja: aplikacijo napišemo na PC-ju z Javo. Na kartici je poseben interpreter te Java kode JVM (angl. Java Virtual Machine), ki razume programsko kodo. Funkcionalnost JVM je neodvisna od procesorja. Kot vmesnik med procesorjem in JVM delujejo programske knjižnice Java API, ki komunicirajo s poljubnim kartičnim operacijskim sistemom. Trenutno so kartični procesorji prešibki za celotno prevajanje Java kode. Zato je JVM dvodelna: en del je na PC-ju in z njim se opravi predprevajanje. Drugi del pa je na kartici in prevaja to predpripravljeno kodo.

Slika 6: Arhitektura Java kartice.

Java kartica bo zaživela ob zmogljivejših kartičnih mikroprocesorjih. Že zdaj napoveduje lažji razvoj novih aplikacij in možnost elegantne večaplikativne kartice. Prvi primerki Java kartic so že na testiranjih.

MULTOS kartica (angl. Multiapplication Operating system): MULTOS predstavlja prvi poizkus za izdelavo pravega večaplikacijskega operacijskega sistema. Arhitektura aplikacije z MULTOS-om je večnivojska, podobna kot pri Java kartici: aplikacijo se napiše v C-ju, prek C-prevajalnika prevede v interpretativni jezik MEL (angl. MULTOS Executable Language). Tako prevedena koda prek API-jev komunicira z operacijskim sistemom MULTOS.

5. ZAKLJUČEK

Čipne kartice se širijo na mnoga področja našega življenja. Z nekaterimi modernimi produkti, kot npr. mobilni telefon, so praktično zrasle skupaj. Zaenkrat ni videti meja razvoja. Letna proizvodnja čipnih kartic že presega 1000 milj. in nezadržno raste. Od tega odpade večina (80 %) na pomnilniške kartice, slabih 20 % pa na mikroprocesorske, ki se uporabljajo za aplikacije, zahtevne s tehnološkega vidika ali zaščite podatkov. Zaenkrat je uporaba bolj domena Evrope (90 %). Potencialno tržišče bo v letu 2000 blizu 3000 milj. čipnih kartic, od tega okoli 50 % telefonskih.

Že od nastanka je spremljalo mikroprocesorske kartice pomanjkanje široko sprejetih standardov, predvsem za operacijske sisteme. Proizvajalci so razvijali svoje rešitve, standardi pa so capljali za njimi. Problem postaja z željami po večaplikacijski kartici vedno bolj pereč. V boj za operacijski sistem, ki bo prevladal nad ostalimi in postal de-facto standard, se je z letošnjim letom vključil tudi Microsoft. To pa pomeni velik pritisk na vse ostale proizvajalce. Ni nujno, da bo zmagala kvaliteta, lahko da bo tržna prodornost.

6. REFERENCE

[1] ADAMS, Jane: "*More Brain Power for Smart Cards*", Card Technology, January 1999, pp. 54-57
[2] BALABAN, Dan: "*Stepping into the spotlight*", Card Technology, January 1999, pp 20-24
[3] HENDRY, Mark: *Smart Cards - Security and Applications*, Artech House, Norwood 1997
[4] LENDER, Friedwart: *Hybrid cards*, Tutorial at the International Health Card Conference, Heidelberg 1995
[5] RANKL, Wolfgang, in EFFING, Wolfgang: *Smart Card Handbook*, John Wiley & Sons, Chichester 1997
[6] VEDDER, Klaus, in WEIKMANN, Franz: *Smart Cards - Requirements, Properties and Applications*, Giesecke & Devrient, 1998
[7] ISO/IEC 7816, *Information technology - Identification cards - Integrated circuit(s) cards with contacts.*
Part 1: 1987, Physical characteristics
Part 2: 1988, Dimensions and location of the contacts
Part 3: 1989, Electronic signals and transmission protocols
Part 4: 1993-95, Interindustry commands for interchange
Part 5: 1994, Numbering system and registration procedure for application identifiers
Part 6: 1994, Interindustry data elements
Part 7: 1997, Interindustry commands for Structured Card Query Language (SCQL)
Part 8: 1998, Security related interindustry commands
Part 9: v branju, Enhanced interindustry commands
Part 11: v branju, Security architecturedržavljane Slovenije.

◆

Peter Pehani je diplomiral na Fakulteti za fiziko in matematiko, Oddelku za fiziko. Zaposlen je na Zavodu za zdravstveno zavarovanje Slovenije, *za tehnično podporo projektu "Kartice zdravstvenega zavarovanja" področje: kartica in kartična tehnologija, personalizacija, čitalniki. Projekt je v zaključni fazi - pred uvedbo sistema kartice zdravstvenega zavarovanja, z 2 milijona karticami za vse državljane Slovenije.*