Pametne kartice – 3. del

Napadi in obrambe: velike skrivnosti malih kartic

Tajni ključ običajno varuje pametna kartica s svojimi neprepustnimi lastnostmi (angl. tamper-resistance). Banke spravijo zasebne ključe strank na njihove pametne kartice, s katerimi se lastniki nato digitalno podpisujejo in s tem zagotavljajo transakcijo. Pametno kartico naj bi uporabljal in se z njo tudi digitalno podpisoval le njen lastnik. Toda kaj, če obstaja napad, ki z nekaj tisoč dolarji standardne opreme omogoči, da pridemo do tajnega ključa v nekaj urah? Nato pametno kartico kloniramo in izvedemo transakcije, ki izpraznijo račun. V nekaterih sistemih lahko kloniranje omogoči, da ustvarimo »zimzeleno« kartico, ki se po vsaki uporabi vrne v začetno stanje, tj. se napolni z denarjem. Kaj, če nobena pametna kartica ni odporna proti takemu napadu?

V zadnjem času se povečuje zanimanje za majhne naprave, kot so pametne kartice, ki preprečujejo, da bi zlahka prišli do njihove vsebine in ključev, ki so na njih shranjeni. Take naprave sicer lahko preučimo s posebno opremo, vendar pa tak laboratorij stane milijone dolarjev. Bolj pomembno je odpraviti najmanjše možnosti za cenejše napade in ravno na tem področju se nadaljuje večna igra mačke z miško ali, če želite, ravbarjev in žandarjev. Pravzaprav gre za pravo oboroževalno tekmo in napadalci postajajo nevarnejši iz dneva v dan.

Pametne kartice imajo največjo prednost pred konkurenco prav zaradi varnosti. Kot smo omenili že v drugem delu, žal niti v računalniški varnosti ne poznamo 100 % zaščite. Celo v primeru pametnih kartic, ki veljajo za »čarobne izstrelke« računalniške varnosti, ni mogoče narediti idealnega sistema za kontrolo dostopa, e-trgovanje, overjanje, zaščito zasebnosti in drugo, ki bi bil popolnoma varen pred vsem in vsakomer. Toda vsak potencialni napadalec analizira koristnost svojega napada, da bi ugotovil, ali je uspešen napad vreden truda, časa in investicij. Ne glede na to, ali gre za denar ali prestiž, se napadalec ne bo lotil pametne kartice, če se mu to ne izplača. V sistemu z več milijoni kartic je potrebno vsaj pol leta za njihovo zamenjavo, stroški so veliki, škoda pa nepopravljiva. Izdelovalci strojne in programske opreme za pametne kartice se zato nenehno sistematično ukvarjajo s tem, kako izboljšati njihovo varnost, ki je že tako izjemno skrbno načrtovana. O tem bi lahko napisali obsežno knjigo. Tu se bomo omejili le na kratek pregled s poudarkom na informacijsko-tehnološkem področju pametnih kartic. Še prej pa se malo bolje seznanimo z digitalnim podpisom, certifikati in ovrednotenjem varnosti kriptosistemov.

Digitalni podpisi

Predstavljajmo si internet kot Divji zahod, seveda brez prahu, kjer pa ne manjka barskih pretepov in žaljivega vedenja. In prav tako kakor se je Divji zahod prelevil v urbano Kalifornijo, postaja internet družbeno

Generiranje ključa in podpisovanje sporočila m		Preverjanje podpisa (r, s) sporočila m osebe A	
DSA	ECDSA	DSA	ECDSA
Izberi naključen $x \in \{2,\ldots,q\text{-}2\}$, t.j. **zasebni ključ**	Izberi naključen $d \in \{2,\ldots,n\text{-}2\}$, t.j. **zasebni ključ**	Priskrbi si avtentično kopijo javnega ključa osebe A:	
Izračunaj $y = g^x \bmod p$, **javni ključ** je (p,q,g,y).	Izračunaj $Q = dP$, **javni ključ** je (E,n,q,Q).	(p,q,g,y)	(E,n,q,Q)
Izberi naključen $k \in \{2,\ldots,q\text{-}2\}$	Izberi naključen $k \in \{2,\ldots,n\text{-}2\}$	Izračunaj $u1 = h(m)(s^{-1} \bmod p) \bmod q$,	Izračunaj $u_1 = h(m)s^{-1} \bmod n$
Izračunaj $r = (g^k \bmod p) \bmod q$ $0 \neq s = k^{-1}(h(m) + x\,r) \bmod q$.	Izračunaj $r = (kP)x \bmod n$ $0 \neq s = k\text{-}1(h(m) + d\,r) \bmod n$.	u2 = r(s -1 mod p) mod q, v = (gu1yu2 mod p) mod q.	$u_2 = r\,s^{-1} \bmod n$ $v = (u_1P + u_2Q)_x \bmod n$.
Podpis je par (r, s).		**Sprejmi** podpis če in samo če je $v = r$.	

Tabela 1. Pri DSA izberemo taki praštevili $p \in \{2^{1023}, \ldots, 2^{1024}\}$ in $q \in \{2^{159}, \ldots, 2^{160}\}$, da je število $p - 1$ deljivo s številom q, pri ECDSA pa tako eliptično krivuljo nad Z_q, da bo število njenih točk deljivo s 160-bitnim praštevilom n. Namesto množenja v množici števil $\{1,2, \ldots, p - 1\}$ po modulu p, na eliptični krivulji seštevamo točke (kot smo predstavili v drugem delu). Sledi izbira elementa g reda q, pri eliptični krivulji pa izbira točke P reda n.

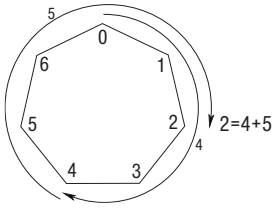
logije

stran 54 Pametne kartice

Popolne zaščite ni in nikoli ne bo mogoča, tehnologija pametnih kartic pa omogoča visoko stopnjo varnosti.

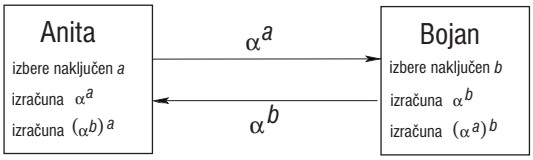
Kripto računalo

Če računamo z realnimi števili, jih moramo zaradi omejene natančnosti računalnikov nenehno zaokrožati (še posebno, ko postajajo števila vse večja in večja). V kriptografiji pa približki ne zadoščajo, zato si raje omislimo končne računske obsege kakor pri številčnici na uri. Tak zgled so praštevilski obsegi (oznaka Z_p), v katerih računamo po modulu velikega praštevila. To pomeni, da seštejemo ali zmnožimo dve števili tako, da pravi rezultat nadomestimo z njegovim ostankom pri deljenju z modulom p (npr. za $p = 7$ velja $4 + 5 = 2$ in $5 \times 4 = 6$, saj ima vsota 9 ostanek 2 pri deljenju s 7, produkt 20 pa ostanek 6). V takih obsegih je vedno možno tudi deljenje, ker smo si izbrali praštevilski modul.



▲ Slika 1: Računanje po modulu 7.

Končni obsegi so zanimivi tudi zato, ker je računanje potenc učinkovito, ne poznamo pa učinkovitih algoritmov za računanje logaritma (za razliko od realnih števil). To sta uporabila Diffie in Hellman za dogovor o ključu (glej sliko 2), pozneje pa še ElGamal za digitalni podpis.



▲ Slika 2: Diffie-Hellmanov protokol. Anita in Bojan ne smeta nikomur izdati svoja zasebna ključa in čeprav njuna javna ključa lahko prestreže katerikoli prisluškovalec, znata le onadva izračunati skupno skrivnost.

vse bolj sprejemljiv, morda tudi po zaslugi nečesa tako preprostega, kot je podpis. Deloma je bil problem interneta, da nihče ni bil prepričan o identiteti drugih. Medtem ko je anonimnost lahko zelo koristna, je tako poslovanje skoraj nemogoče. Podpisi pa ne omogočajo le identifikacije, pač pa tudi celostnost, ob tem pa preprečujejo tajenje.

Oglejmo si primerjavo digitalnih podpisov v grupi Z_p z digitalnim podpisom v grupi na eliptični krivulji oziroma čisto konkretni ameriški Digital Signature Algorithm (DSA), ki je enakovreden kriptosistemu RSA, z njegovim eliptičnim analogom ECDSA (tabela 1).

Certifikati so se pojavili kot garancija javnih ključev. Seveda pa zmorejo veliko več, saj vsak certifikat sestavlja razširljiva množica polj. Nekatera polja so vnaprej določena, toda dodamo jih toliko, kolikor jih potrebujemo. Velika podjetja lahko ustvarijo močne strukture certifikatov, ki nosijo dodatne informacije o privilegijih lastnikov in njihovih omejitvah. Certifikat lahko na primer določa limit vrednosti pogodbe, ki jo posamezni uslužbenec lahko podpiše, ali dostop do finančnih dokumentov, ki jih lahko vidi.

Pomembnejše vprašanje pri certifikatih je, koliko garancije v resnici zagotavljajo. Nekateri certifikati prve stopnje (npr. VeriSign) so dodeljeni vsakomur, ki izpolni obrazec na ustrezni domači strani. Le-ti so uporabni zgolj za konsistentnost prisotnosti, ne zagotavljajo pa, da je lastnik prava oseba. Certifikati druge stopnje pa so izdani šele po preverjanju kakšne podatkovne zbirke določenih strank. Če ste kreditno sposobni, potem lahko dobite tak certifikat. Vseeno pa ni jasno, kdo zagotavlja, da ni mogoče ukrasti identitete osebe, o kateri imamo dovolj podatkov. (Nekomu je npr. uspelo dobiti kreditno kartico za psa – ko bi ga le znal prisiliti, da mu še poravnava račune vsak mesec.) VeriSign ponuja tudi certifikate tretje stopnje, za katere mora uradni notar preveriti prijavo in opraviti identifikacijo. S tem seveda certifikat pridobi dodaten nivo zaupanja. Vendar pa bi bilo zaupanje še večje, če bi agencija za certifikate sama opravila identifikacijo in nato finančno zagotavljala pravilnost le-te.

Certifikate moramo znati preklicati, ko na primer zaposleni zapusti podjetje ali če pride do kraje. Takšen mehanizem pa je lahko precej neprijeten. Čez čas se nabere preveč preklicanih certifikatov, ki zahtevajo več prostora in upočasnijo preverjanje. Zato X.509 standard (ki ga uporabljajo tako rekoč vsi) predpisuje le certifikate z določenim rokom trajanja, tako da lahko stare certifikate odstranimo iz obtoka. Certifikati za šifriranje so običajno veljavni veliko manj časa od certifikatov za podpisovanje dokumentov.

Kolikor javnih ključev shranimo na pametni kartici, toliko sogovornikov bomo znali prepoznati. Če pa je slednjih več kakor prostora za ključe, potem je najbolje shraniti na kartico javni ključ neke agencije za certifikate (CA), s katerim bomo lahko preverjali od CA podpisane javne ključe naših sogovornikov.

Stopnje varnosti kriptosistemov

M. Blaze, W. Diffie, R. Rivest, B. Schneier, T. Shimomura, E. Thompson in M. Wiener so leta 1996 (http://theory.lcs.mit.edu/rivest/publications.html) predlagali minimalne dolžine ključev, potrebnih za varen simetrični sistem (npr. DES ali IDEA):

- Da bi zagotovili ustrezno zaščito pred najbolj resnimi grožnjami

dolžina ključa (v bitih)	posamični napadalec ❶	majhne skupine ❷	raziskovalna omrežja ❸	velika podjetja ❹	vojaške obveščevalne službe ❺
40	dnevi	ure	minute	milisekunde	mikrosekunde
56	leta	tedni	dnevi	minute	milisekunde
64	tisočletja	stoletja	desetletja	ure	sekunde
80	∞	∞	tisočletja	stoletja	dnevi
128	∞	∞	∞	∞	∞

▲ Tabela 2: Povprečen čas za napad z grobo silo (angl. Brute Force Attack) – ocene glede na tehnologijo iz leta 2000.

❶ posameznik ima en PC in programsko opremo (2^{20}–2^{28} ključev/s),
❷ majhna skupina, 16 PC-jev (2^{24}–2^{32} ključev/s),
❸ raziskovalna omrežja, 256 PC-jev (2^{28}–2^{36} ključev/s),
❹ veliko podjetje z 1.000.000 dolarjev za strojno opremo (2^{48} ključev/s),
❺ vojaška obveščevalna organizacija z 1.000.000.000 dolarjev za strojno opremo in napredno tehnologijo (2^{60} ključev/s).

SLOVAR

AES (angl. *Advanced Encryption Standard*) Ime za nov *Federal Information Processing Standard (FIPS)* za simetrični kriptosistem, ki bo nadomestil DES; leta 2000 je zanj *National Institute of Standards and Technology (NIST)* izbral belgijsko bločno šifro **Rijndael**; dolžina ključev oziroma blokov je 128, 196 ali 256.

Ameriška vohunska organizacija (angl. (American) National Security Agency – NSA) Vladna organizacija ZDA, ki skrbi za komunikacijsko varnost in odgovarja ministrstvu za obrambo (angl. Department of Defence – DoD); nadzoruje tuje komuniciranje in razbija šifre; razvija nove kriptografske algoritme in omejuje uporabo znanih algoritmov.

agencija za certifikate (angl. *certification authority* – CA, nem. *die Zertifizierungsinstanz*) Organizacija, ki izdaja, objavlja in vzdržuje listo izdanih certifikatov za javne ključe z datumi veljave (preklicani certifikati imajo zapadli datum ter morda še razlog preklica, glej črna lista) in jamči, da so pristni; je del PKI.

asimetrični kriptosistem Šifrirni algoritem z uporabo dveh ključev, javnega (ki ga pozna kdorkoli) in zasebnega (ki ga pozna samo ena oseba); vsak par ključev je povezan, vendar iz javnega ni mogoče učinkovito pridobiti zasebnega; npr. javni ključ uporabimo za šifriranje, zasebni pa za odšifriranje; glej tudi overjanje.

avtentičen (gr. *authentikos*) Pristen, izviren, pravi, verodostojen, izvira od avtorja ali lastnika, overjen.

avtentikacija Glej overjanje.

avtorizacija Preizkušanje za izdajo dovoljenja za izvajanje določene akcije, npr. plačilo s kreditno kartico avtorizira izdajatelj kartice, če sta kartica in plačilno mesto prepoznana za pravo, če je vrednost nakupa manjša od limita; avtorizacijo dosežemo z overjanjem.

biometrika Preizkus pristnosti osebe na podlagi neponovljivih ali težko ponovljivih bioloških lastnosti, kot so prstni odtis, geometrija roke, struktura ožilja na očesnem ozadju ali pa šarenice, zapis zob, DNK, glas, lastnoročni podpis, ipd.

bločna šifra (angl. *block cipher*) Simetrična šifra, ki procesira čistopis v bitnih skupinah, imenovanih bloki; za njeno alternativo glej tokovna šifra.

celovitost (tudi celostnost) Neokrnjenost sporočila (angl. *message integrity*), preneseno sporočilo je celovito, neokrnjeno, nedotaknjeno; na poti do prejemnika ni bilo spremenjeno; zagotovljena je z uporabo MAC ali zgoščevalne funkcije.

certifikat Elektronski dokument, ki je podpisan javni ključ, izdan od pooblaščene agencije in dopušča preizkus pristnosti javnega ključa; najbolj razširjena in znana je specifikacija strukture in kodiranja certifikatov po standardu X.509; prednost tega je, da samo CA (in ne nujno vsak uporabnik) opravi prepričljivo identifikacijo.

časovna znamka ali žig (angl. *timestamp*) Za nekatere namenske programe je pomemben točen čas, kdaj so neki podatki obstajali; v ta namen pripnemo (in podpišemo) ustreznim podatkom časovno znamko.

čistopis (angl. *clear text*) Besedilo, ki ga še nismo šifrirali.

črna lista (angl. *black/hot/red list, certification revocation list*) Seznam v zbirki podatkov, ki označuje vse pametne kartice ali certifikate, ki so bili verjetno kompromitirani in ne morejo biti avtorizirani.

delitev skrivnosti (angl. *secret sharing*) Kriptografski protokol, ki razdeli skrivni ključ na dele in da po enega vsakemu od njih, tako da lahko iz svojih delov izračunajo ključ samo pooblaščene (izbrane) skupine, poljubna skupina, ki ne vsebuje nobene pooblaščene skupine, pa ne more ugotoviti niti enega samega bita ključa.

DES (Data Encryption Standard) Najbolj znan in sploh prvi komercialni simetrični (bločni) kriptosistem; dolžina ključev je 64 bitov, vsak osmi je parity check bit, deluje na 64-bitnih blokih; zasnovan v 60-ih letih pri IBM-u; za široko rabo raje uporabimo trojni-DES, IDEA ter DES-ovega naslednika AES.

DH-protokol (Diffie in Hellman) Najbolj popularen kriptografski protokol, njegov cilj je dogovor o ključu prek javnega kanala; predstavitev tega koncepta leta 1976 je upoštevan kot rojstvo kriptografije z javnimi ključi; varnost temelji na DLP.

DSA (Digital Signature Algorithm) Algoritem za digitalni podpis, ki uporablja DLP in ga je predlagala ter standardizirala vlada ZDA; trenutno se uporabljajo 1024-bitni parametri (tako kakor pri algoritmu RSA).

digitalni podpis (angl. *digital signature*) Uporabljamo ga za ugotavljanje pristnosti elektronskega sporočila, dokumenta ali entitete (druge funkcije so npr. še zagotavljanje celovitosti ali preprečevanje tajenja); digitalni

(npr. velike komercialne ustanove ali vladne agencije), mora biti ključ dolg vsaj 75 bitov.

- Da bi zagotovili ustrezno zaščito za naslednjih 20 let, morajo biti ključi dolgi vsaj 90 bitov (pri tem upoštevamo pričakovano rast računske moči).

IBM-ovi napotki ustvarjalcem varnostnih sistemov, ki se do neke mere zanašajo na neprepustnost naprav, delijo napadalce v naslednje skupine:

1. razred (pametni »outsiderji«): Običajno so zelo inteligentni, a imajo premalo informacij o sistemu in omejen dostop do napredne opreme, zato pogosto poskušajo izkoristiti obstoječe šibkosti sistema (kot pa da bi jih sami ustvarili).

2. razred (»insiderji«): Imajo precejšnjo specializirano tehnično izobrazbo in izkušnje. Čeprav morda ne poznajo vseh komponent sistema, utegnejo prej ali slej priti do informacij, do zelo naprednih orodij in instrumentov za analizo.

3. razred (močnejše organizacije): Sposobne so sestaviti ekipe specialistov ter pridobiti zavidljiva sredstva in opremo zanje. Tako lahko opravijo temeljite analize sistemov, iznajdejo zapletene napade in uporabljajo vrhunsko opremo.

dolžina ključev v bitih	število možnih ključev	potreben čas pri hitrosti eno šifriranje na mikrosekundo	potreben čas pri hitrosti 10^6 šifriranj na mikrosekundo
32	$2^{32} = 4.3 \times 10^9$	≈ 36 minut	≈ 2 milisekundi
56	$2^{56} = 7.2 \times 10^{16}$	≈ 1142 let	≈ 10 ur
128	$2^{128} = 3.4 \times 10^{38}$	≈ 5×10^{24} let	≈ 5×10^{18} let

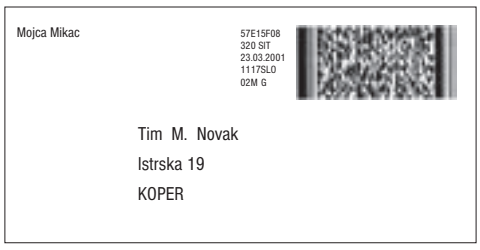
▲ Tabela 3: Povprečen čas za napad z grobo silo.

simetrične šifre (AES)	asimetrične (RSA, DSA)	eliptične krivulje (ECDSA)
40 bitov	274 bitov	80 bitov
56 bitov	384 bitov	106 bitov
64 bitov	512 bitov	132 bitov
80 bitov	1024 bitov	160 bitov
112 bitov	2048 bitov	237 bitov
128 bitov	3072 bitov	283 bitov
192 bitov	8192 bitov	409 bitov
256 bitov	16384 bitov	540 bitov

▲ Tabela 4: Dolžina ključev z enakovredno varnostjo.

Če posplošimo sklepe zgornje skupine kriptografov na kriptosisteme z javnimi ključi, dobimo tabelo 4. Konkretno pa za »eliptične« kriptosisteme velja, da morajo biti ključi, ki zagotavljajo kratkoročno varnost, dolgi vsaj 150 bitov, za srednjeročno varnost pa vsaj 180 bitov.

Hitrost podpisovanja in preverjanja podpisov ima neposreden vpliv na to, koliko časa moramo čakati, da je odobrena neka (trans)akcija. Na eni strani imamo naprave, kot so pametne kartice, ki imajo na razpolago zelo malo energije ter omejeno računsko in prostorsko moč, na drugi pa strežnike, ki so običajno močnejši računalniki (tudi z več procesorji). Vendar pa mora zato strežnik obdelati (npr. za banko ali kakšno drugo podjetje) tudi po 1000 in več podpisov ali preverjanj podpisov na sekundo. Zato želimo imeti čim učinkovitejše kriptografske algoritme tako na enem kakor na drugem koncu (npr. sheme za digitalne podpise). Dodaten razlog za to je tudi, da zmogljivosti procesorjev na pamet-



◀ Slika 3: Digitalna poštna znamka, predstavljena s črtno kodo formata PDF417 na pisemski ovojnici.

SLOVAR

podpis je dodan čitljivemu besedilu na tak način, da prestane preizkus le, če vsebina sporočila ostane nespremenjena; običajno je izveden z asimetričnim kriptosistemom (npr. RSA, ElGamal): z zasebnim ključem se generira informacija, ki jo tretja oseba uporabi zato, da z javnim ključem preveri veljavnost; pravna veljava digitalnega podpisa je ponavadi določena z zakonom; digitalnim podpisom včasih pravimo tudi elektronski podpisi, vendar vsekakor pri tem ne smemo misliti na digitalni ali elektronski zapis običajnega podpisa.

dogovor o ključu (angl. *key agreement/exchange*) Postopek, pri katerem si dve strani z asimetričnim kriptosistemom izbereta skupni skrivni ključ; najbolj popularen je DH-protokol (pri simetričnih kriptosistemih se morata strani, ki želita komunicirati, najprej dogovoriti za skupni ključ, pri tem pa je težava, da običajno nimata na voljo varnega kanala za ta namen).

dokaz brez razkritja znanja (angl. *zero-knowledge-proof*) Protokol, katerega cilj je prenesti en sam bit; prejemnik želi biti prepričan, da pošiljatelj poseduje določeno informacijo, vendar ne sme zvedeti same informacije.

e-trgovina (angl. *e-commerce*) Obsega vsa poslovna delovanja, ki jih izvajamo elektronsko.

ElGamalovi kriptosistemi Kriptosistemi z javnimi ključi, ki jih je leta 1985 predlagal Taher ElGamal za šifriranje z javnimi ključi in digitalne podpise; njihova varnost temelji na težavnosti problema diskretnega logaritma.

enkratni ščit (angl. *one time pad*) Edini dokazano varen simetrični kriptosistem; šifriranje in odšifriranje potekata tako, da sporočilu ali tajnopisu z »ekskluzivnim ali« (XOR) prištejemo enako dolgo naključno zaporedje; (čeprav se ta sistem uporablja v praksi še danes, pa je njegova slaba stran dolžina ključa in dejstvo, da ni varen, če isti ključ uporabimo večkrat, ali če imajo podatki znano strukturo).

enkripcija Glej šifriranje.

enosmerna funkcija (angl. *one way function*) Matematična funkcija, ki jo je moč učinkovito izračunati, njenega inverza pa v doglednem času ne moremo poiskati (npr. zgoščevalna funkcija, glej tudi DLP).

generator naključnih števil Naprava ali algoritem, ki proizvaja člene zaporedja naključnih in med seboj neodvisnih bitov.

geslo Skrivna beseda, skupina znakov ali stavek (angl. *password, pass phrase*), ki se uporablja kot nadomestilo za avtorizacijo uporabnika ali kot dostopni mehanizem v računalniški sistem, program, do podatkov ipd.

IDEA Simetrični (bločni) kriptosistem, ki deluje na blokih dolžine 64 bitov, uporablja pa 128-bitni ključ; na začetku 1990-ih sta ga razvila X. Lai in J. Massay; zelo je popularen v Evropi (patentiralo ga je podjetje Ascom iz Švice).

identifikacija Postopek za preverjanje identitete osebe ali naprave, običajno s primerjavo predstavljenega gesla in ustreznega shranjenega gesla ali z digitalnim podpisom.

izziv-odgovor (angl. *challenge-response*) Protokol, s katerim preverimo pristnost osebe, s katero komuniciramo; ena stran pošlje izziv (običajno je to neko naključno število), na katerega naj bi druga stran pravilno odgovorila (glej dokaz brez razkritja znanja).

javni ključ (angl. *public key*) Eden od dveh šifrirnih ključev v asimetričnem kriptosistemu; lastnik objavi ali pošlje javni ključ, tako da ga lahko uporabijo vsi; sporočilo, ki je zašifrirano z javnim (ali podpisano z zasebnim) ključem, je mogoče razkriti (ali preveriti podpis) le z ustreznim zasebnim (ali javnim) ključem.

Kerckhoffov princip Pomembno merilo za ocenjevanje kriptografskih algoritmov: napadalec pozna kriptosistem ali algoritme, ki jih uporabljamo, ne pa tudi ključev, ki nam zagotavljajo varnost.

ključ (angl. *key*) Parameter, s katerim določamo preoblikovanje podatkov in tako nadzorujemo kriptografske sisteme, npr. šifriranje in odšifriranje (skriti ključ), digitalno podpisovanje (zasebni ključ), preverjanje podpisov (javni ključ); danes imajo v kriptografiji ključi večinoma elektronsko obliko, predstavljeno z binarnim zaporedjem ničel in enic; ključ običajno naključno izberemo iz neke vnaprej poznane dovolj velike množice, ki jo imenujemo **prostor ključev**.

kodiranje Ni nujno šifriranje, uporablja se predvsem za pretvarjanje podatkov v obliko, primerno za prenos ali shranjevanje.

kriptoanaliza Razbijanje kriptosistemov in napadi nanje; npr. iskanje vsebine sporočil brez vednosti ključa ter iskanje zasebnih ključev iz javnih.

kriptografija (tajnopisje, skritopisje, skrivnopisje) V klasičnem smislu je to teorija o zakrivanju vsebine sporočil, danes pa je to obsežno področje, ki zajema probleme, kot so pristnost, avtorizacija in digitalni podpis.

kriptologija Veda, ki se ukvarja s kriptoanalizo in kriptografijo.

nih karticah ne naraščajo tako hitro kakor potrebe po varnosti.

Kriptosistemi z eliptičnimi krivuljami (ECC) so iz dneva v dan bolje sprejeti kot izbrana metoda za varovanje podatkov v omejenih okoljih, glej IEEE P1363, ANSI X9 (1. del).

Nazoren primer za uporabo krajšega ključa v praksi je digitalna znamka, ki predstavlja digitalni podpis naslova, podatkov o pošiljatelju itd. ter jo uvajajo v ZDA in Nemčiji. Za znamko na sliki 3 smo uporabili digitalni podpis z eliptičnimi krivuljami, sicer bi znamka zavzela precej več prostora.

Varnost pametnih kartic

Varnost pametne kartice je zagotovljena s štirimi komponentami, to so kartica, čip, operacijski sistem in namenski program. Zadnje tri ščitijo podatke in programe na procesorju pametne kartice ter so, čeprav neodvisne od kartice, nujne za fizično in logično varnost pametne kartice. Če ena od teh komponent odpove ali ne izpolnjuje ustreznih zahtev, pametna kartica ni več varna. To je primerljivo z verigo, v kateri najšibkejši člen določa odpornost celotnega sistema. Resen problem pri vseh informacijskih sistemih je, da enemu uspešnemu napadu sledi plaz enakih napadov. Medtem ko zaradi uspešno ponarejenega denarja v praksi ne pride do inflacije, saj ponarejevalci ne morejo narediti dovolj velike količine denarja ali pa vsega spraviti v promet, je pri digitalnem denarju čisto drugače, kajti ponaredka ne moremo razlikovati od originala. Pa vendar je z ustreznim kriptografskim protokolom možno poskrbeti, da številke, ki predstavlja vrednost, ne moremo porabiti dvakrat.

Laže se je zaščititi pred znanimi tipi napadov kakor pred neznanimi, a žal nikoli ne bomo poznali vseh napadov ali imeli na voljo dokaze, da drugačni napadi ne obstajajo. Sledili bomo standardu ISO 13491-1, ki opisuje koncepte, zahteve in ocene za kriptografsko varno opremo v bančnem sektorju. Pa se podajmo v ping-pong igro ukrepov in protiukrepov za napade in obrambo pred njimi. Napade delimo na *družbene*, *fizične* in *logične*.

Družbeni napadi

Ta skupia zajema vse vrste napadov, povezanih z ljudmi, ki proizvajajo ali uporabljajo pametne kartice. Da se izognemo tem napadom,za izdelovanje pametnih kartic in programske opreme uporabljamo javne postopke, izdelano kodo pa pregleda in preizkusi neodvisna skupina v okviru ocenjevanja programske opreme.

S tem se približamo idealu, ko je varnost odvisna od ključev, znanje programerjev pa ne koristi napadalcem. V svetu pametnih kartic naj bi bil torej uveljavljen princip, da ni nedokumentiranih mehanizmov ali funkcij (ne gre za pomanjkljivost pač pa za odliko), saj se vse prepogosto dogaja, da takšne posebnosti običajno niso dobro preizkušene in preverjene. Razvojni računalniki zahtevajo popolnoma izolirano omrežje (zunanji dostop mora biti prepovedan). Programerji nikoli ne delajo sami (princip štirih oči) in nihče ne pozna vseh razvojnih delov (delitev skrivnosti).

> ***Napadalci postajajo iz dneva v dan nevarnejši, 100 % zaščite ni.***

Vsak čip je označen z edinstveno številko, iz katere se izpeljejo ključi, ki jih nato uporabljamo za overjanje po principu izziv-odgovor. Prenos kode na kartico je specifičen za čip in overjanje je obvezno za vsak dostop v zaključnih fazah, sicer bi bilo možno podtakniti lažne (dummy) pametne kartice, ki bi se ves čas vede enako kot originalne, pri tem pa bi npr. vsake toliko časa napadalcu izpisale celotno vsebino pomnilnika.

Za uspešno obrambo moramo imeti vsaj grobo sliko o potencialnih napadalcih in njihovih motivih, kot so pohlep, slava in status, pa naj si gre za kriminalne nagibe ali znanstveno raziskovanje.

SLOVAR

kriptosistem Kriptografski algoritem, ki poda pravila za preoblikovanje podatkov in se uporabi npr. za šifriranje ali odšifriranje; običajno so odvisni od vsaj enega (skrivnega) parametra (ključa); delimo jih na simetrične in asimetrične kriptosisteme.

kriptosistem z eliptičnimi krivuljami (angl. *Elliptic Curve Cryptosystem - ECC*) Asimetrični kriptosistem, ki uporablja skupino točk na eliptični krivulji; **ECDSA** je različica DSA s skupino na eliptični krivulji; ta razred kriptosistemov je privlačna alternativa RSA, saj so njegova glavna prednost krajši ključi (npr. 160 bitov za isto varnost kakor 1024-bitni RSA); posebej učinkovit, ko ga uporabimo v prostorsko, računsko ali časovno omejenih okoljih, kot so pametne kartice.

kriptosistem z javnimi ključi (angl. *public key cryptosystem*) Glej asimetrični kriptosistem.

m-trgovanje (angl. *mobile-commerce*) Možnost mobilnega izvajanja poslovanja (npr. e-poslovanje z mobilnim telefonom ali kakšno drugo majhno napravo).

MAC (angl. *Message Authentication Code*) Dodatek sporočilu, ki ga izračunamo s skrivnim ključem in s tem zagotovimo celovitost sporočila.

MQV Protokol za dogovor o ključu so leta 1995 predlagali Menezes, Qu in Vanstone; temelji na DH-protokolu (kot večina dogovorov o ključu), vendar ima to prednost, da se ob dogovoru o ključu overi obe strani.

naključna števila Mnogi kriptosistemi potrebujejo naključne elemente, večinoma v obliki naključnih števil, ki jih generiramo vedno znova (v teh primerih je varnost postopka odvisna tudi od ustreznosti teh naključnih števil); generiranje naključnih števil ostaja problem (izvor pravih naključnih dogodkov je v resnici možen z natančnim opazovanjem naravnih dogodkov, kar pa ni lahko realizirati s programsko opremo) zato uporabljamo namesto tega psevdo naključna števila.

napad z grobo silo (angl. *brute force attack*) Napad na kriptografski sistem s sistematičnim preizkušanjem vseh možnih ključev.

NR Digitalni podpis, ki sta ga iznašla Nyberg in Rueppel; njegova varnost temelji na DLP in omogoča povračilo sporočila iz podpisa.

odšifriranje (dekripcija) Postopek, s katerim iz tajnopisa povrnemo vsebino sporočila (glej šifriranje).

overjanje Šifrirni postopek, ki potrdi pristnost sporočila ali podpisa (in s tem osebe ali naprave, s katero poteka komunikacija) ter zagotovi, da sporočilo izvira od pravega (pričakovanega, dopustnega, zakonitega) pošiljatelja; v primeru asimetričnega kriptosistema uporabimo zasebni ključ za podpis, javni pa za preverjanje pristnost podpisa.

pametna kartica (angl. *smart card*) Alternativno ime za mikroprocesorsko kartico in se nanaša na procesor, ki je »pameten« (in samostojno računa); skoraj nemogoče je manipulirati notranje procese in pomnilnik; uporablja se za kriptografske namenske programe, katerih funkcionalnost obsega en sam čip (za razliko od čip kartic, ki vsebujejo več medsebojno povezanih čipov); pomnilniške kartice torej strogo gledano niso pametne kartice, a se ime pametna kartica »zlorablja« za vse čip kartice.

patent Dokument, ki da izumitelju izključno pravico do izkoriščanja njegovega izuma za omejen čas v eni ali več državah (običajno za maksimalno dobo 20 let).

povračilo sporočila (angl. *message-recovery*) Možnost pridobitve sporočila iz podpisa v protokolu *digitalnega podpisa*; v tem primeru ni treba pošiljati sporočila ob podpisu – za *RSA* je to očitna izbira, ustrezni protokoli pa obstajajo tudi, če varnost temelji na *DLP* (npr. NR).

preprečevanje tajenja (angl. *non-repudation*) Preprečitev, da nekdo zanika dano obljubo ali storjeno dejanje; dosežemo ga lahko z ustreznim digitalnim podpisom in zakoni.

preverjanje podpisa (angl. *signature verification*) Postopek, s katerim se z uporabo javnega ključa prepričamo, ali je digitalni podpis ustreznega dokumenta veljaven in preverimo pristnost podpisa.

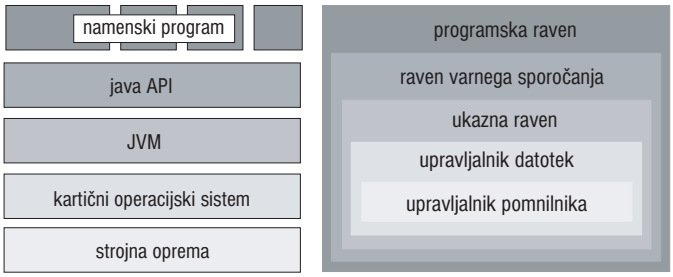
problem diskretnega logaritma (angl. *Discrete Logarithm Problem – DLP*) Za dano število b iščemo število x za katerega je $a^x = b$; čeprav znamo obratni problem, t.j. potenciranje, izvesti učinkovito, se DLP izkaže za veliko težji problem; to spoznanje potrebujemo pri protokolih za dogovor o ključu (npr. DH-protokol), pri šifriranju in digitalnih podpisih; za današnje potrebe varnosti izberemo v primeru skupine Z_p^* običajno praštevilo p velikosti 1024 bitov, v primeru grupe na eliptični krivulji pa je njena moč običajno velikosti 160 bitov.

problem faktorizacije naravnih števil (angl. *Integer Factorization Problem - IFP*) Problem iskanja faktorjev danega števila n; zahtevnost tega problema raste z velikostjo števila n, ki je za današnje potrebe varnosti običajno velikosti 1024 bitov ali 300 mest.

Napadi na logično delovanje

Namenski program mora biti načrtovan tako, da varnost celotnega sistema ni ogrožena, če napadalcu uspe zlomiti varnost ene kartice. Kriptosistemi in njihova izvedba naj bodo preprosti. Značilnost zanesljivih kartičnih operacijskih sistemov (COS) je delitev na nivoje z jasno določenimi pravili za komunikacijo med njimi. Privilegiji dostopa k posameznim datotekam in ukazom morajo biti dodeljeni karseda konzervativno. Dostop mora biti po pravilu prepovedan in dopuščen le, ko je zares nujno potreben.

Vsak ključ za overjanje mora imeti svoj števec, ki ga lahko le povečujemo, ne pa tudi zmanjšujemo. Paziti moramo, da so procesi nedeljivi (v ta namen jim običajno določimo tudi minimalno dopustno frekvenco) in da števec povečamo, preden izvedemo primerjavo ključev, sicer bi bilo v načelu možno preizkusiti vse možnosti. Velika prednost pametnih kartic je, da izdelujejo dnevniške datoteke (angl. log-file) za vsak namenski program posebej.

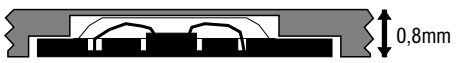


Slika 4: Delitev na ravni pri pametni kartici z javo (levo) in ustrezna delitev pri navadnih pametnih karticah.

Pred nekaj leti je bilo skoraj nemogoče dobiti pametne kartice ali mikrokrmilnike, ki so jih uporabljali za njihovo izdelavo, danes pa je že možno dobiti pametne kartice in konfiguracijske programe številnih podjetij. Lahko uporabimo tudi javansko tehnologijo za pametne kartice, s katero je veliko laže narediti programe in jih naložiti na prazno pametno kartico. Moderne pametne kartice imajo mehanizme, ki omogočijo nalaganje programov na pametno kartico tudi potem, ko je že bila izdana lastniku kartice. Tu je treba poskrbeti, da ne naložimo še trojanskega konja ali virusa. Če operacijski sistem odkrije napako v strojni opremi, pošlje pametna kartica sporočilo o napaki in se izključi ali vstopi v neskončno zanko.

Fizični napadi

Pri tej vrsti napadov napadalec poskuša kartici spremeniti delovno napetost, temperaturo, frekvenco itd. in tako zmesti njeno normalno delovanje, delovanje generatorja naključnih števil ali pa spremeniti kak števec. Kartico na primer hladimo s tekočim dušikom in s tem upočasnimo njeno delovanje do te mere, da lahko natančno opazujemo, kaj se dogaja v procesorju. Napad z lasersko (ali rentgensko ali ultravijolično) svetlobo bi v načelu lahko prisilil generator naključnih števil, da vsakič izbere isto število ali pa spremeni DES tako, da se vede kot linearna transformacija. Vendar pa imajo vsi novejši procesorji za pametne kartice senzorje, ki zaznajo nenormalne delovne pogoje; v večini primerov se čip ob neustreznih pogojih samodejno uniči. Drugi možen napad je »odpiranje« čipa; z ustrezno nanotehnologijo ugotoviti njegovo notranjo zgradbo.



Slika 5: Prerez pametne kartice. Čipa ni težko odstraniti s kartice z nožem, veliko teže pa ga je odpreti.

Ker nanotehnologija neprestano napreduje, se da kartice, starejše od dveh let, z novo tehnologijo že odpirati, vendar pa so stroški takih napadov precejšnji. Zato ti napadi največkrat niso upravičeni, saj moramo

SLOVAR

PIN (angl. *personal identification number*) Osebna identifikacijska številka, skrivno geslo, izraženo s številkami; uporablja se zlasti za identifikacijo lastnika pametne kartice sami kartici.

PKI (Public Key Infrastructure) Kombinacija strojnih in programskih komponent, pravil in postopkov, ki zagotavljajo pristnost javnih ključev s certifikati.

psevdo naključno zaporedje števil Zaporedje števil, generirano z algoritmom, ki pa ga ni moč učinkovito ločiti od zaporedja naključnih števil, npr. ne da se učinkoviti napovedati naslednji člen zaporedja na osnovi prejšnjih.

RSA Kriptosistem z javnimi ključi (predstavljen leta 1978), poimenovan po njegovih izumiteljih Rivestu, Shamirju in Adlemanu; varnost temelji na problemu faktorizacije celih števil.

seme (angl. *seed*) Vrednost, s katero inicializiramo psevdo naključni generator, tako da z njim dobljenega zaporedja napadalec ne more predvideti.

simetrični kriptosistem (tudi **simetrična šifra**) Kriptografski algoritem, ki uporablja isti ključ za šifriranje in za odšifriranje; delimo jih na bločne in tokovne.

skriti vhod (angl. *trap door*) Mehanizem v programski opremi ali algoritem, ki je namenoma vključen, da bi lahko tisti, ki ve zanj, zaobšel varnostne funkcije ali zaščitne mehanizme.

standard Dokument, ki vsebuje tehnične opise in natančna merila za pravila ter definicije lastnosti ali možnosti, da bi s tem zagotovili, da so materiali, izdelki, postopki in usluge lahko uporabljeni za to, za kar so bili namenjeni, in da so medsebojno združljivi; izdajo ga nacionalne ali pa mednarodne organizacije, medtem ko specifikacije izdajo podjetja ali pa združenja podjetij.

steganografija Področje kriptografije, ki se ukvarja s skrivanjem obstoja sporočila (običajno zašifriranega) v digitalnih podatkih, kot so slike, z namenom, da bi tajno prenesli sporočilo.

šifriranje (**enkripcija**) Postopek, s katerim skrijemo vsebino sporočila; glej šifra, ključ.

šifra (angl. *cipher*) Algoritem ali postopek za šifriranje in odšifriranje podatkov; šifre delimo na asimetrične in simetrične, slednje delimo naprej še na bločne in tokovne.

tajnopis (angl. *ciphertext*) Zašifrirano sporočilo (glej tudi čistopis).

terminal Naprava, ki napaja pametno kartico z električno energijo in prek katere kartica prejema in pošilja podatke; nekateri terminali imajo tudi zaslon in tipkovnico ali številčnico.

tokovna šifra (angl. *stream cipher*) Simetrična šifra, ki obdela sporočilo bit po bit; glej bločna šifra.

trčenje (pri zgoščevalni funkciji) Dve različni sporočili se zgostita v isto vrednost; če pri funkciji nikoli ne pride do trčenj ali če takih trčenj ni moč učinkovito poiskati, pravimo, da je brez trčenj (angl. *collision-resistant*).

trojanski konj Program, ki izvede običajno funkcijo, poleg tega pa naredi v ozadju (brez vednosti uporabnika) še nekaj nepričakovanega; za razliko od virusa se le-ta ne razmnožuje.

trojni-DES Da bi rešili problem prekratkega ključa simetričnega kriptosistema DES, uporabimo DES trikrat, vendar vsakič z drugim ključem; obstaja več variant trojnega-DESa, ki se razlikujejo npr. glede na število uporabljenih ključev; najbolj pogosta metoda (standardizirana pri American National Standard Institute) uporabi prvi ključ za šifriranje, drugi za odšifriranje, in nato zopet prvi za šifriranje (v tem primeru je dejanska dolžina ključa 112 bitov – obstajajo pa tudi variante s tremi različnimi ključi, t.j. s 168-bitnim ključem).

zasebni (privatni) ključ (angl. *private key*) Eden od dveh šifrirnih ključev v asimetričnem kriptosistemu; zasebni ključ je znan samo njegovemu lastniku, javni ključ pa se objavi in po možnosti ga še podpiše CA; uporablja se za šifriranje in generiranje digitalnega podpisa.

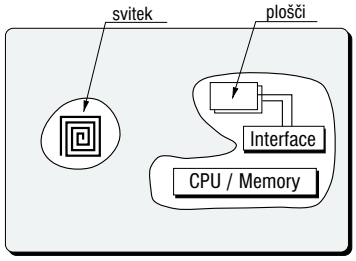
zasebnost (angl. *privacy*) Sporočila, ki ga ena stran pošlje drugi, ne more prebrati nihče drug.

zaupnost (angl. *confidentiality*) Eden od ciljev šifriranja; le pooblaščene osebe naj bi dobile določene dele informacij.

zgoščevalna funkcija (angl. *hash function*) Postopek za stiskanje podatkov z enosmerno funkcijo, tako da iz rezultata ni moč izračunati originalnih podatkov ali najti trčenj (rezultat je fiksne dolžine ne glede na količino vhodnih podatkov) vsako spreminjanje podatkov z zelo veliko verjetnostjo spremeni tudi rezultat zgoščevalne funkcije; rezultat imenujemo **zgostitev**, **prstni odtis** ali **izvleček** (angl. *hash* ali *digital fingerprint*); tipična predstavnika sta SHA-1 in RIPEMD-160 (s 160-bitnimi zgostitvami).

napadati vsako kartico posebej in v dobro načrtovanem sistemu kartic to ni posebna grožnja.

DFA-napad (angl. *Differential Fault Analysis*) namenoma povzroči izolirane napake pri kriptografskem računanju in so ga predlagali proti asimetričnim kriptosistemom leta 1996 D. Boneh, R.A. DeMillo in R.J. Lipton, Anderson pa ga je še istega leta prilagodil vsem kriptosistemom, če seveda ne uporabimo preventivnih ukrepov. Napad DFA na DES potrebuje le 200 blokov tajnopisa, da izračuna vrednost tajnega ključa. Za trojni DES (s 168-bitnim ključem) se število blokov tajnopisa ne poveča bistveno.

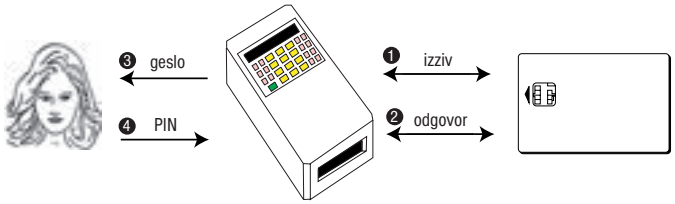


◀ Slika 6: Brezkontaktna pametna kartica.

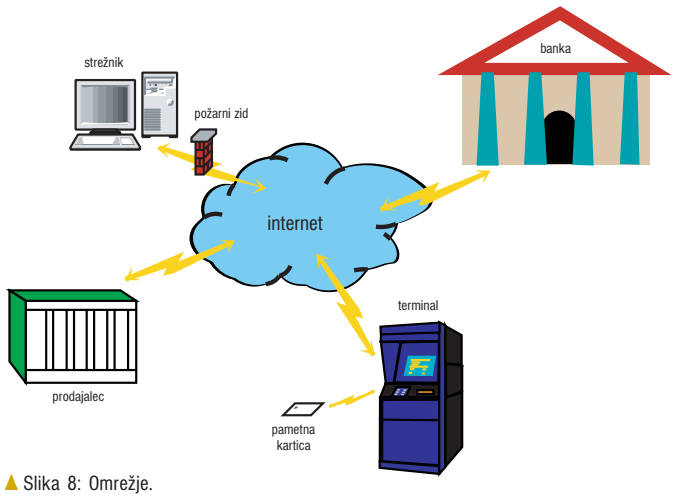
Obstajajo pa tudi napadi, ki ne posegajo v neposredno delovanje kartice. Med te sodijo časovni napad in analiza porabe moči. Pri prvem merimo čas, ki ga kartica porabi za izvajanje nekega ukaza in na podlagi izmerjenega časa sklepamo o podatkih, ki jih je kartica obdelovala, ali pa o določenih bitih ključa. Pri napadu z analizo porabe moči pa merimo tok, ki ga procesor potrebuje, da izvrši določen ukaz. Na ta način lahko napademo večino kriptosistemov, ki niso ustrezno zaščiteni, med njimi pa so tako simetrični kakor asimetrični. Zato je ključnega pomena, da poznamo te napade in se pred njimi zaščitimo. Poraba elektrike mora biti zelo podobna za vse strojne ukaze in ne sme biti odvisna od podatkov, ki jih obdeluje vodilo, sicer bi bilo možno ugotoviti določeno količino tajnih informacij. Lep primer je kriptosistem DES, ki se na pametnih karticah uporablja še dokaj pogosto. Če je nepravilno izveden, lahko s preprostim merjenjem odkrijemo 48 bitov tajnega ključa, tako da moramo odkriti samo še preostalih 16 bitov, za katere pa lahko uporabimo napad z grobo silo. Podobni napadi obstajajo tudi pri asimetričnih kriptosistemih. Zato uporabljamo razne zaslepljevalne metode (angl. blinding), s katerimi poskušamo prikriti, katero operacijo izvajamo. Več o teh napadih in obrambah pred njimi lahko zainteresiran bralec prebere v Timing attack for RSA and DSA, P. Kocher, Differential Power Analysis, P. Kocher, J. Jaffe in B. Jun (http://www.cryptography.com/dpa/index.html).

Čitalniki pametnih kartic

Pametne kartice uporabljamo za komunikacijo z drugimi računalniki (oddaljenimi ali bližnjimi). Ta poteka prek čitalnikov pametnih kartic ali terminalov, saj te naprave lahko tudi pišejo na pametne kartice, ne pa samo berejo z njih. Vsak terminal z več kakor samo enoto s kontakti, pretvornikom in uro, ima tudi procesor (8- ali 16-bitni) in pomnilnik (RAM na baterijsko napajanje ter kakšen megabajt EEPROM-a). Delimo jih na prenosne in fiksne. Prvi za razliko od drugih običajno niso ves čas povezani v omrežje in imajo lahko tudi preprostejše tipkovnice in zaslone. Tipični predstavniki prvih so mobilni telefoni in terminali POS. Medtem ko lastnik zaupa svoji napravi in mu ni treba vnašati PIN-a v nepoznan terminal, pa z uporabnikom ni tako (glej sliko 7).



▲ Slika 7. Kako preprečiti, da nam lažni terminal ne ukrade gesla? Tako, da PIN vnesemo v terminal šele, ko se terminal in kartica medsebojno overita. Kako vemo, da sta se kartica in terminal overila? Kartica preko terminala pokaže geslo, ki ga lahko spreminjamo neodvisno od terminala.



Slika 8: Omrežje.

Le v čisto omrežnih terminalih, katerih edina funkcija je pretvoriti električne signale in jih prenašati med računalnikom in pametno kartico, običajno ni dodatno vgrajenih varnostnih mehanizmov. Takoj ko terminal deluje neodvisno od višjega sistema, pa naj si bo le začasno ali stalno, mora vsebovati tudi glavne (master) ključe za kriptografske algoritme. Ti so zelo občutljivi in jih moramo ves čas skrbno varovati. Ne morejo biti shranjeni v običajnem elektronskem vezju, pač pa v posebnem varnostnem modulu terminala (običajno velikosti škatlice za vžigalice), ki ima posebno mehansko in električno zaščito za odkrivanje napadov. Tako kakor pri pametnih karticah ključi nikoli ne zapustijo modula, pač pa so uporabljeni le znotraj njega za računanje. Zaradi visoke cene varnostnih modulov jih v zadnjih letih nadomeščajo pametne kartice formata ID-000 (kartice SIM).

Seveda pa terminali niso edini del omrežja, pri katerih mora biti za varnost dobro poskrbljeno. Ker danes večina komunikacije poteka prek interneta, je možnih točk za napade precej. Slika 8 prikazuje tipično omrežje, v katerega so vključeni trgovci, banke, terminali in strežniki, ki na primer obdelujejo zahtevke posameznih kupcev in jih nato ustrezno usmerijo naprej. Razsežnost interneta ne omogoča fizično varnost podatkov, varno komunikacijo pa zagotavlja kriptografija. Zaradi večje varnosti mora biti vsa komunikacija med deli omrežja zašifrirana, posamezni elementi pa se morajo ob vsaki komunikaciji medsebojno overiti.

Nadzor

V proračunu ugotovimo, da nam zmanjkuje denarja, pa čeprav zadnje čase nismo kupili nič večjega, prihodki pa so redno prihajali. Kaj je prvi ukrep? Preštejemo denar, ocenimo varnost poslopja, zamenjamo ključavnice, namestimo boljša vrata in rešetke na okna in podobno? Verjetno ne. Za začetek je najbolje na blagajno namestiti alarm in morda še kamero. Z opazovalnim sistemom pridobimo čas. Sedaj lahko v miru pregledamo vse vrednostne papirje, analiziramo okolje ter izboljšamo varnost. Brez nadzora ni mogoče govoriti o popolni varnosti, z njim pa je občutek takoj boljši.

> ***Nadzor je prvi in najpomembnejši korak na poti do varnosti.***

Pri omrežni varnosti je ponavadi ravno nasprotno. Večina podjetij misli, da je za nadzor treba poskrbeti šele takrat, ko so vsi drugi varnostni ukrepi že izvedeni. Vendar pa je takšno razmišljanje zgrešeno. Nadzor bi moral biti prvi korak v vsakem načrtu varnosti. Omrežni skrbnik lahko začne nadzor izvajati takoj. Za oceno varnosti in odkrivanje možnih vstopnih točk potrebujemo čas, varnost pa se ne izboljša, dokler dejansko ne odpravimo pomanjkljivosti. Nameščanje varnostnih programov izboljša varnost le, če je izvedeno na pravem mestu in na pravilen način. Toda kako lahko omrežni skrbnik ve, katere programe namestiti in ali ti programi res delujejo? Edini način je, da nadzoruje omrežje.

Tak način razmišljanja je še posebej pomemben v dinamičnih omrežjih, kot so na primer omrežja v podjetjih. Le-ta se dnevno spreminjajo: novi programi, novi strežniki, nove šibke točke. Omrežni skrbnik misli, da je njegovo omrežje varno, že naslednji dan pa v časopisu prebere o novih pomanjkljivostih programov, ki jih uporablja. Naenkrat njegovo omrežje ni več varno, čeprav se ni nič spremenilo. Seveda lahko skrbnik namesti nove programe, spremeni nastavitve omrežja, postavi dodatni požarni zid ... Toda kako lahko ve, ali vsi ti ukrepi zares delujejo? Tako, da nadzoruje omrežje.

> ***Razsežnost interneta onemogoča fizično varnost podatkov, zato nam varno komunikacijo zagotavlja kriptografija.***

Nadzor je edini način, s katerim dobimo resnične podatke o varnosti celotnega sistema, o tem, ali vse naprave delujejo pravilno in ali so vsi varnostni mehanizmi pravilno nastavljeni. Šele ko te podatke imamo, lahko začnemo delati spremembe. Spreminjanje nastavitev brez nadzora je golo ugibanje. Zato je nadzor prvi in najpomembnejši korak na poti do varnosti.

Sklepne misli

Tako kot so osebni računalniki postali del vsakdana, so tudi pametne kartice postale nekaj samo po sebi umevnega in nam omogočile, da smo aktivno prisotni v digitalnem svetu. Nekatere napovedi za bodočnost postajajo vse bolj razvidne. Kriptografske operacije bodo izginile v infrastrukturo, kompleksnost kriptografskih upravljanj s ključi bo skrita pred uporabniki. Novi protokoli bodo postali praktični, omogočeni bodo novi načini poslovanja. S primerno zasnovo lahko večino računanja in vodenja dnevnikov prenesemo s pametne kartice na osebni računalnik, ki ima večje računske in pomnilniške zmogljivosti. Manj očitna pa je prihodnost z nekaterih drugih vidikov, kot so na primer družbeni, ekonomski in politični. Predstavljajte si samo, da se kmalu ne bomo mogli več usesti v avto in voziti, ne da bi nas pri tem ves čas nadzorovala pametna kartica (radarske kontrole sploh ne bodo več potrebne).

Od PC-ja do pametne kartice.

Zaradi novih napadov bodo izdajatelji prisiljeni vsakih nekaj let izdelati nove različice pametnih kartic. Pri tem pa bodo naročniki sistemov pametnih kartic morali imeti aktivnejšo vlogo kot doslej, kajti le izobražen naročnik bo vedel, kaj lahko zahteva in kaj lahko za svoj denar dobi.

Zainteresiranemu bralcu, ki se želi podrobneje seznaniti s pametnimi karticami, priporočamo knjigo W. Rankl, Smart Card Handbook, Wiley, 2000, več o kriptografiji pa lahko najdete v knjigi Handbook of Applied Cryptography, A. Menezes, P. van Oorschot in S. Vanstone, CRC Press, 1997, ki je dostopna tudi prek interneta na naslovu: http://www.cacr.math.uwaterloo.ca/hac/.

Aleksandar Jurišić
Jernej Tonejc