Zahvala

Zahvaljujem se mentorju doc. dr. Tonetu Vidmarju in somentorju doc. dr. Aleksandru Jurišiču za strokovno vodstvo, usmerjanje ter za vse koristne nasvete in ideje.

Svojim staršem sem hvaležen za vsestransko podporo.

Hvala mojima Alenki in Martinu za vse.

Povzetek

Magistrsko delo opisuje model infrastrukture javnega ključa za upravljanje z zaupanjem med interakcijami subjektov iz različnih varnostnih okolij. Pravilna odločitev uporabnika certifikata, ali bo glede na dostopne podatke ter varnostno politiko sistema sprejel izvedbo akcije, je ključnega pomena za ohranjanje zaupnosti in neokrnjenosti virov sistema.

Uporabnik certifikata gradi zaupanje v javni ključ entitete s pomočjo modela zaupanja. Le-ta predstavlja uporabnikovo videnje infrastrukture javnega ključa. Delovanje modela temelji na poenotenem pristopu za zapis in obravnavo varnostnih politik, izjav in razmerij med entitetami. Opira se na že predstavljene pristope za upravljanje z zaupanjem. V ključnih delih jih razširja in posplošuje s ciljem omogočiti uporabo modela v realnih situacijah in obstoječih infrastrukturah javnega ključa.

Vsak uporabnik si sam izdela (formalizira) svojo varnostno politiko ter določa parametre izjav glede na vire, ki jih hoče zaščititi, in vrsto dostopa. Model na podlagi varnostne politike (uporabnikovih zahtev) in zbranih podatkov (izjav) vrne nedvoumen odgovor o primernosti izvedbe akcije glede na dostopne podatke, varnostno politiko sistema in tveganje, ki ga je uporabnik pripravljen sprejeti.

Predlagane so rešitve za poglavitne pomanjkljivosti v organizaciji obstoječih infrastruktur javnega ključa, ki so: odvisnost varnosti sistema od uporabnikovega poznavanja in spoštovanja varnostnih postopkov v infrastrukturi, formalizacija zapisa varnostne politike sistema za vrednotenje zaupanja v javni ključ entitete, ugotavljanje višine nudenega jamstva. Predlogi se nanašajo predvsem na organizacijske in tehnične izboljšave za enostavnejšo, učinkovitejšo in predvsem varnejšo uporabo infrastrukture javnega ključa.

Uporaba modela za upravljanje z zaupanjem je predstavljena na dveh trenutno najbolj pogostih primerih uporabe globalnih omrežij in infrastrukture javnega ključa. Prav tako je podan okviren predlog izvedbe gradnikov modela v infrastrukturi javnega ključa.

VSEBINA

I. UVOD

Z razvojem novih telekomunikacijskih sistemov in računalniških omrežij pospešeno prihaja do uvajanja avtomatiziranih mehanizmov za izvajanje transakcij in izpodrivanja klasičnih papirnatih dokumentov. Tradicionalni varnostni mehanizmi kot so fotografije, papirnati certifikati in prostoročni podpisi, postajajo nezanesljivi in nepraktični. Zahtevajo fizični transport in so z razvojem kopirne tehnike občutljivi za ponarejanje, nedovoljeno kopiranje, krajo, izsiljevanje ali uničenje. Le z zagotovitvijo varnosti komuniciranja digitalnih informacij in izvajanja transakcij lahko v popolnosti izkoristimo možnosti, ki nam jih ponujajo globalna omrežja in telekomunikacijski sistemi. *Varnostne zahteve*, ki jih uporabniki postavljajo, so (Stallings [60]):

- *zaupnost*: potrebno je preprečiti razkrivanje vsebine sporočila nepooblaščenim entitetam,
- *prepoznavanje*: pred začetkom komuniciranja in med njim je potrebno nedvoumno prepoznati entiteto, s katero komuniciramo,
- *neokrnjenost*: sporočila se pri prenosu preko omrežja ne smejo neopazno spreminjati,
- *nadzor dostopa*: dostop do omrežnih virov je dovoljen le pooblaščenim entitetam v skladu s pravili, ki jih določi lastnik (upravljavec) vira,
- *preprečevanje tajenja*: entitete ne smejo imeti možnosti uspešnega zanikanja sodelovanja pri aktivnostih, v katerih so dejansko sodelovale.

Orodja za zagotavljanje naštetih varnostnih zahtev (storitev) so: šifriranje, digitalno podpisovanje, beleženje in nadzor aktivnosti, protokoli za prepoznavanje, nadzor dostopa. Obseg uporabe je odvisen od zahtevane stopnje varnosti in uporabljenih storitev zaščite. Način uporabe orodij je predpisan v varnostnih politikah sistema. Varnostne politike naštevajo vire, grožnje ter določajo pravila za zaščito virov.

Večina zgoraj naštetih orodij temelji na *asimetrični kriptografiji*. V nasprotju s simetrično kriptografijo, kjer uporabljamo isti ključ za šifriranje in dešifriranje, imamo tu dva ključa; za šifriranje in dešifriranje. Ključa sta matematično neločljivo povezana. Kljub poznavanju enega izmed obeh ključev brez dodatnih podatkov ni mogoče na enostaven način določiti drugega. Šifrirni (javni) ključ objavimo, dešifrirnega (zasebni ključ) pa skrbno varujemo. Javni ključ uporabljamo za šifriranje podatkov in preverjanje digitalnega podpisa, zasebnega pa za digitalno podpisovanje in dešifriranje sporočil. V zadnjih letih je asimetrična kriptografija postala vodilna tehnologija za digitalizacijo poslovanja v globalnih omrežjih.

Osnovni problem varnosti v globalnih omrežjih je problem *overjanja javnih ključev*. Slednje je predpogoj za uporabo asimetrične kriptografije, saj brez prepričanja, da javni ključ pripada entiteti, ne moremo biti prepričani o izvoru šifriranega sporočila ali identiteti podpisnika dokumenta. Šifrirni ključ sam po sebi ne vsebuje dodatnih

informacij o entiteti, ki poseduje pripadajoči zasebni ključ in četudi bi, bi težko preprečili kopiranje teh informacij. Prav tako je potrebno vedeti, ali je ključ sploh še veljaven (ali je prišlo do razkritja zasebnega ključa) in v kakšne namene se lahko uporablja.

Problem overjanja rešujemo z digitalno podpisano podatkovno strukturo – *digitalnim certifikatom javnega ključa*. Certifikat povezuje identiteto entitete, njen javni ključ, obdobje veljavnosti, namen uporabe (izdaje) ključa in še množico manj pomembnih atributov. Certifikate izdajajo in z njimi upravljajo *certifikatne agencije*. Z digitalnim podpisom certifikata potrjujejo pripadnost javnega ključa entiteti in veljavnost atributov, zapisanih v certifikatu. Ker so podatki v certifikatu varovani z digitalnim podpisom izdajatelja, ni potrebna dodatna zaščita pri prenašanju po odprtih omrežjih. Uporaba certifikata pretvori problem iskanja javnega ključa entitete v problem pridobivanja pristnega javnega ključa izdajatelja certifikata.

Digitalni certifikati se kažejo kot daleč najbolj obetajoča rešitev za celostno varovanje komunikacij in izvajanja transakcij. Ker so predstavljeni kot podatkovna struktura le iz ničel in enic, jih je enostavno prenašati brez izgub in dragega človeškega posredovanja. Nudijo visoko stopnjo varnosti, saj zahteva izračun zasebnega ključa izdajatelja, ki varuje neokrnjenost certifikata, velikanske računske potenciale. V bodočnosti bodo digitalni certifikati vgrajeni v vsak del programske oziroma strojne opreme, ki bo omogočala varno komuniciranje z drugimi napravami ali posamezniki.

Zaradi velikega števila uporabnikov (interesnih skupin) v globalnih omrežjih se bodo lokalne agencije med seboj povezovale. Certifikatne agencije si lahko vzajemno overjajo ključe (*križni certifikati*) in tako tvorijo hierarhično ali nehierahično infrastrukturo javnega ključa. *Infrastrukturo javnega ključa* predstavljajo okolje in storitve, ki v globalnih omrežjih omogočajo uporabo tehnologij, temelječih na asimetrični kriptografiji. Tako uporabnikom certifikata ni potrebno zaupati eni sami certifikatni agenciji. Infrastruktura javnega ključa je bistven element za omogočanje varnih elektronskih komunikacij v porazdeljenih okoljih.

Preverjanje pristnosti javnega ključa entitete izvedemo s preverjanjem veljavnosti digitalnega podpisa in preostalih atributov v certifikatu, ki vsebuje javni ključ. Če podatki niso spremenjeni, če je certifikat še vedno veljaven ter če javni ključ ni bil preklican, je postopek uspešno končan. To pa zahteva izpolnjevanje dveh pogojev (Ford, Baum [21]):

- imamo pristen javni ključ certifikatne agencije, izdajatelja, s katerim preverimo veljavnost digitalnega podpisa certifikata,

- agenciji zaupamo, da izdaja certifikate le po temeljitem preverjanju identitete entitete in posedovanju para ključev.

Če nimamo ključa izdajatelja certifikata, moramo najprej pridobiti njegov certifikat (pri drugem izdajatelju) in preveriti veljavnost. Postopek rekurzivno nadaljujemo, dokler ne naletimo na veljavni ključ, katerega lastnika poznamo in mu zaupamo. Vsi certifikati, ki jih potrebujemo v postopku preverjanja, sestavljajo *verigo certifikatov*.

Vendar digitalno podpisani certifikat uporabniku certifikata običajno ne zadostuje za odločitev o primernosti entitete za izvedbo akcije oziroma za dostop do vira. Zaupanje v entiteto in primernost ključa lahko določimo šele na podlagi dodatnih informacij o postopkih, ki jih izdajatelj uporablja za preverjanje entitete, posedovanje para ključev, zaščito ključa za podpisovanje (tako podpisnega ključa agencije kot ključa entitete), omejitvah in namenu uporabe ključev, jamstvu... Slednje informacije so običajno zbrane v *politiki certificiranja* agencije in predstavljajo temelj delovanja certifikatnih agencij.

V sedanji organizaciji infrastrukture javnega ključa so vsi postopki v zvezi z overjanjem javnega ključa entitet in preverjanjem certifikatov prepuščeni uporabniku certifikata. Sam mora zbrati in preveriti vse podatke. Skrbnost preverjanja ter dostopnost podatkov je bistvenega pomena pri odločanju za sprejetje akcije in zagotavljanju varnosti sistema. Postopek overjanja in gradnje zaupanja v javni ključ entitete je potrebno avtomatizirati.

1. UPRAVLJANJE Z ZAUPANJEM

Za varno komuniciranje in izvajanje transakcij je mnogokrat premalo, da vemo le, kdo je imetnik javnega ključa oziroma pošiljatelj sporočila. Povezati hočemo kriptografijo, varnostno politiko uporabnika certifikata in njegovo videnje zaupanja v homogeno celoto. Na podlagi zbranih podatkov (izjav), zaupanja v izjave in entitete ter varnostne politike sistema (uporabnika), se želimo odločiti, ali je zahteva entitete po izvedbi akcije skladna z varnostno politiko sistema.

Zasnovali bomo model, ki bo uporabniku certifikata omogočal sprejemanje odločitev z upoštevanjem podatkov, katerim ne zaupa povsem. Prav tako nima zagotovila, da je pridobil vse podatke, ki so bistveni za presojo. Ponujal bo jezik za opis varnostnih politik, relacij zaupanja, izjav o entitetah in bo nudil splošen mehanizem za ovrednotenje skladnosti akcije z varnostno politiko. Model bo na podlagi izjav, zaupanja v izjave in pridobljenih podatkov (domnev) vrnil odgovor o tveganju pri izvedbi akcije in zaupanju v javni ključ entitete. Omogočal bo *upravljanje z zaupanjem* (trust management).

Model zajema vse vidike uporabe infrastrukture javnih ključev, vključno z izjavami o zaupanju, priporočili, mero zaupanja v izjave, obravnava več verig certifikatov, vrednoti tveganja, odvisnosti podatkov. Rezultati modela so neodvisni od vrstnega reda vrednotenja zaupanja (uporabe pravil). Postopki omogočajo učinkovito izvedbo in enostavnost uporabe. Model omogoča modeliranje poljubno velike populacije entitet, enostavno dodajanje entitet in parametrov ter obravnavo kompleksnih varnostnih politik.

Model infrastrukture javnega ključa

Model infrastrukture javnega ključa predstavlja uporabnikovo videnje infrastrukture. Zgrajen je iz entitet, ki tvorijo infrastrukturo, in izjav, ki so jih entitete podale o drugih entitetah. Primeri entitet so certifikatne agencije in imetniki certifikatov. Gradnikom modela uporabnik pripiše stopnjo zaupanja. Okolje modela je

infrastruktura javnega ključa. Omogoča pridobivanje izjav in ustvarjanje novih. Za vsako interakcijo uporabnik zgradi nov model.

Izjave so podatki, ki jih uporabnik pridobi iz infrastrukture javnega ključa, oziroma jih ima varno shranjene. Ločimo več vrst izjav: izjava o pristnosti javnega ključa, izjava o zaupanju entiteti (da skrbno izvaja določene postopke), priporočila in digitalni certifikati javnega ključa. Posamezni izjavi lahko uporabnik doda še parametre, ki natančneje opredeljujejo izjavo. Poleg osnovnih vhodnih podatkov modela uporabnik pri odločanju uporablja še podatke o statusu certifikatov in višini jamstva, ki jih izdajatelj nudi v primeru zlorabe certifikata.

Zaupanje izjavam in entitetam

Izjavam in entitetam uporabnik prireja *stopnjo zaupanja*. Slednja odraža uporabnikovo videnje zaupanja, ki jo pripisuje entiteti oziroma izjavi. Najtežji del postopka pri upravljanju z zaupanjem je odločitev, v kolikšni meri lahko uporabnik zaupa entiteti, ki je izjavo izdala. Določiti stopnjo zaupanja je težak problem. Določamo jo lahko izkustveno oziroma na podlagi posvetovanja z neko relevantno entiteto, ki vodi bazo podatkov o entitetah v infrastrukturi. Prirejanje mere zaupanja naj bi odsevalo dogajanja v infrastrukturi in bi bilo za uporabnika kar se da enostaven in intuitiven proces. Rezultat modela je v veliki meri odvisen od prirejanja zaupanja. V literaturi je slednje ob obravnavi modelov porinjeno vstran. Ali je mera preveč splošna (Reiter, Stubblebine [53]) in jo težko povežemo z nameravano akcijo, ali pa prirejanja zaupanja ob predstavitvi modela sploh ne obravnavajo (Maurer [40]).

V primeru obstoja vrhovne avtoritete, ki bi ji vsi zaupali in bi vodila evidenco o entitetah ter njim prirejenim stopnjam zaupanja za izvajanje določene akcije, bi model z zveznimi vrednostmi verjetno dobro deloval. Model bi nudil natančno vrednotenje zaupanja v izjave in tveganja pri izvajanju transakcij. Ni verjetno, da bo kdaj prišlo do ustanovitve globalne avtoritete, tako iz sociooloških kot tehničnih razlogov. Zato je potrebno uporabniku ponuditi enostavno, a še sprejemljivo rešitev za določanje stopnje zaupanja v izjave oziroma entitete.

Predstavljeni model privzema diskretno metriko za določanje zaupanja izjavam. Za uporabnika je izjava veljavna ali neveljavna. Tako se bistveno poenostavi določanje zaupanja in interpretacija rezultatov modela. Uporabnik se na podlagi podatkov o namenu uporabe ključa, kdo jamči za povezavo javni ključ - entiteta, kako je slednji preveril identiteto entitete in posedovanje para ključev, kako je izvedeno hranjenje ključev, nadalje kakšne so obveznosti vpletenih strank, varnostne zahteve uporabnika certifikata, jamstva, ki jih nudi izdajatelj v primeru zlorabe ali neprimerne uporabe ključev, odloči o zaupanju v izjavo. Ob prirejanju zaupanja lahko izjavo opremi še z dodatnimi parametri, ki natančneje opisujejo pogoje veljavnosti izjave.

Vrednotenje zaupanja

Ideja predlaganega modela je, da uporabnik na podlagi izjav in domnev pride do sklepa o primernosti izvedbe akcije z uporabo izpeljevalnih pravil. Uporabnik s pomočjo i*zpeljevalnih pravil* iz veljavnih izjav in domnev gradi nove veljavne izjave.

Prvi korak k ovrednotenju zaupanja v javni ključ entitete oziroma tveganja je izgradnja *začetnega pogleda na infrastrukturo javnega ključa* (Maurer [40]). Začetni pogled vsebuje izjave, za katere uporabnik meni, da so v njegovem kontekstu in glede na predlagano akcijo veljavne in jim lahko zaupa. Izražajo njegovo začetno prepričanje, na podlagi katerega s pomočjo pravil izpeljuje nove izjave. Dejstvo, da je izjava vsebovana v začetnem pogledu, še ne pomeni, da je veljavna v absolutnem smislu. Pomeni le, da je v uporabnikovem kontekstu taka predpostavka upravičena. Ravno tako izvzetost izjave iz začetnega pogleda še ne pomeni, da je neveljavna, morda se uporabniku le ne zdi pomembna. Začetni pogledi entitet se praviloma razlikujejo. To še posebej velja za izjave zaupanja, ki so pogosto izraz izkušenj ob interakcijah z entitetami, varnostne politike in okolja. Zato mora uporabnik pri gradnji začetnega pogleda upoštevati, koga naj sklep prepriča: ali njega samega ali tudi neodvisnega razsodnika (na primer sodnika).

Uporabnik izjave in parametre za začetni pogled črpa iz varnostne politike sistema. Glede na akcijo, ki jo namerava entiteta izvesti (vrsta dostopa, vir do katerega dostopa), uporabnik določi množico začetnih izjav in parametrov, ki tvorijo začetni pogled. Izjave, ki se navezujejo na vir, ki ga ščitimo, so pripravljene že vnaprej. Začetni pogled gradimo iz statične množice veljavnih izjav. Ostale podatke, ki so potrebni za odločanje o primernosti izvedbe akcije, uporabnik pridobiva iz infrastrukture javnega ključa. Pri tem sam določa vrsto in časovno svežino podatkov.

Model na podlagi zbranih podatkov odloči, ali je zahteva po izvedbi transakcije v skladu z varnostno politiko sistema. Uporabnik podatkom v večini ne zaupa popolnoma, te zadržke o veljavnosti podatkov model vključuje v proces odločanja.

Poudarek predstavljenega modela je na učinkovitosti izvajanja in primernosti uporabe v praksi. Temelji na enostavnem zapisu izjav, varnostne politike sistema in pravilih za izpeljavo novih izjav, ki jim zaupamo.

Kot neločljivi del je vključen problem ugotavljanja statusa certifikata. Na realnih primerih poizkušamo pokazati, da je reševanje problema močno odvisno od okoliščin, v katerih deluje infrastruktura, in varnostnih zahtev entitet. Za povečanje robustnosti modela pri določanju zaupanja je poudarek na iskanju več med seboj neodvisnih verig certifikatov. Pri reševanju problemov poizkušamo vključiti uporabo modernih tehnologij (pametne kartice), saj se izkaže, da se z njihovo pomočjo kompleksnost problemov bistveno zmanjša. Na koncu poizkusimo predlagane rešitve umestiti v okvir standarda X.509 [30], [28].

Razdelitev vsebine po poglavjih

Magistrsko delo je razdeljeno po poglavjih na sledeči način. V drugem poglavju opredelimo osnovne pojme, povezane z infrastrukturo javnega ključa in digitalnimi certifikati ter podamo kritike obstoječe zasnove infrastrukture. Ker je za zagotavljanje varnosti v odprtih (globalnih) najpomembnejša asimetrična kriptografija, v tretjem poglavju predstavimo prevladujoče asimetrične šifrirne postopke, jih primerjamo in nakažemo prednosti posameznega postopka v okviru infrastrukture javnega ključa. Četrto poglavje obravnava uporabo namenskih naprav (pametnih kartic) za hranjenje zasebnega ključa in digitalnih certifikatov. Poudarek je predvsem na poenostavitvi nekaterih mehanizmov infrastrukture. Peto poglavje se v celoti ukvarja s trenutno

najbolj perečim problemom: z ugotavljanjem statusa certifikata. Slednja storitev infrastrukture je najkompleksnejša, saj mora zadostiti tako zahtevam po ažurnosti podatkov kot zahtevam po visoki stopnji razpoložljivosti in varnosti. V šestem poglavju predstavimo problem overjanja pristnosti javnega ključa in predstavimo model infrastrukture javnega ključa. Model je zasnovan z namenom preseganja poglavitnih problemov obstoječih infrastruktur javnega ključa in razbremenitev uporabnika certifikatov. Sledi sklep in pregled uporabljene literature.

II. DIGITALNI CERTIFIKATI IN INFRASTRUKTURA JAVNEGA KLJUČA

V poglavju bomo preučili razloge za razvoj, vlogo in pomen digitalnih certifikatov za komuniciranje in izvajanje transakcij v globalnih omrežjih. Ogledali si bomo trenutni razvoj in izpostavili slabosti na področju organiziranosti, učinkovitosti in varovanju zasebnosti.

1. OD PAPIRJA DO DIGITALNEGA CERTIFIKATA

Posamezniki in organizacije imajo pogosto upravičene potrebe, da preverijo identiteto ali kakšen drug atribut entitete, s katerim komunicirajo ali izvajajo transakcijo. Pri tradicionalnih metodah prepoznavanja oziroma dokazovanja primernosti entiteta predloži enega ali več papirnih certifikatov (osebni dokument, potrdilo, diplomo…). Fotografije, prostoročni podpis so bili v oporo pri preverjanju identitete imetnika certifikata. Vgrajeni varnostni elementi (vodni žigi, poseben papir, posebno črnilo …) so preprečevali ponarejanje.

Z naraščanjem izkoriščanja globalnih omrežij za poslovno in zasebno rabo se postavlja vprašanje, kako doseči zaupanje v dokazila, ki jih predloži entiteta, s katero komuniciramo. Ena izmed rešitev je izposojena iz fizičnega sveta. Entiteta se izkaže s potrdilom, ki ga je izdala ustrezna avtoriteta (državna ustanova, univerza, podjetje...) in povezuje identiteto entitete ter ostale pomembne atribute. Analogija v digitalnem svetu je digitalni certifikat javnega ključa. To je digitalno podpisan elektronski dokument. Izdajatelj - certifikatna agencija z izdajo certifikata izjavlja, da entiteta poseduje par ključev in da so podatki v certifikatu veljavni (resnični). Če je izdajatelj avtoriteta za navedeno področje in mu zaupamo ter je podala izjavo o entiteti, potem entiteti lahko zaupamo. Certifikat postane osnovno sredstvo zaupanja.

Z razvojem računalnikov in telekomunikacijskih omrežij se papirnati transakcijski mehanizmi pospešeno zamenjujejo z avtomatiziranimi. Gonilne sile, ki stojijo za prehodom iz papirnatega v avtomatične mehanizme, so:

- Kraja, izguba ali uničenje papirnatega certifikata sovpada s krajo, izgubo ali uničenjem vsaj dela njegove vrednosti. Prav tako je lahko zelo drago ali celo nemogoče od izdajatelja pridobiti novo kopijo certifikata.

- Papirni certifikati so podvrženi obrabi, so nerodni za avtomatično obdelavo in v mnogih situacijah neučinkoviti. Elektronski certifikati so enostavni za izdelavo, razdeljevanje, kopiranje. Preverjanje in avtomatična obdelava je mnogo bolj učinkovita in zahteva manj stroškov.

- Papirni certifikati niso primerni za predstavljanje negativnih kvalifikacij imetnika. Imetnik lahko certifikat, ki mu ni po volji, uniči. Nekatere negativne atribute lahko priključimo pozitivnim (vožnja v vinjenem stanju v vozniškem dovoljenju), a to ni vedno mogoče.

- Komuniciranje v globalnih omrežjih (elektronska pošta, prenosni telefoni) nudijo mnoge prednosti pred osebno komunikacijo in izvajanjem transakcij v fizičnem svetu. Mnoge prednosti in možnosti ne pridejo do izraza, če uporabljamo papirne certifikate, ker zahtevajo fizični transport.

- Vse bolj dostopne naprave z reprodukcijskimi zmogljivosti povečujejo nevarnost ponarejanja izkazov. Kriptografske tehnike omogoča učinkovito zaščito certifikatov pred ponarejanjem.

V mnogih primerih je uporaba simetrične kriptografije neprimerna. Entitete si morajo s strežnikom sejnih ključev deliti skupni ključ in mu zaupati. Pred začetkom vsake seje mora strežnik zgraditi in razposlati skrivni sejni ključ. Razen tega ne omogoča izvedbe mehanizma za preprečevanje tajenja na enostaven način (brez posredovanja tretje stani). Potreba po deljenju skrivnosti s partnerjem in še z nekom negira osnovno zahtevo kriptografije, ohranjanje popolne zaupnosti komunikacij med entitetami. Kot posledica takega razmišljanja sta Diffie in Hellman v znamenitem članku [15] predstavila kriptografijo javnega ključa. Le-ta omogoča entitetama, da digitalno podpisujeta in šifrirata sporočila brez posredovanja tretje strani, četudi se ne poznata in nista še nikoli komunicirali. Tako odpade potreba po posredniku, ki posreduje ob vsaki transakciji.

V zgoraj omenjenem članku o javni kriptografiji je nakazan problem ugotavljanja pripadnosti ključa entiteti. Predlagano je, da bi ustanovili varen in priključno dostopen javni imenik, ki bi vseboval povezave med imenom entitete in njenim javnim ključem. Rešitev ima številne slabosti. Imenik bi moral zagotavljati neokrnjenost podatkov, visoko stopnjo razpoložljivosti, upravnik imenika bi moral jamčiti za verodostojnost povezave entiteta - javni ključ, uporabniki bi mu morali zaupati.

Leta 1978 je Kohnfelder [38] predlagal, da bi v izogib ozkemu grlu, ki ga predstavlja imenik, uvedli zaupanja vredne entitete, certifikatne agencije. Le-te izdajajo digitalne certifikate javnega ključa. Certifikat je digitalno podpisana izjava, ki veže javni ključ in naziv entitete. S certifikatom entiteta dokazuje, da poseduje javni in njemu pripadajoči zasebni ključ. Izdajatelj - certifikatna agencija s svojim podpisom jamči, da so podatki v certifikatu točni. To omogoča uporabnikom certifikata, da lokalno preverijo veljavnost povezave med javnim ključem in entiteto s preverjanjem digitalnega podpisa certifikata in obdobja veljavnosti. Za preverjanje mora uporabnik imeti javni ključ izdajatelja, ki je certifikat izdala.

Najpomembnejša lastnost digitalnih certifikatov javnega ključa je, da ne potrebujejo dodatnih varnostnih storitev. Certifikat ni zaupen dokument in ga lahko javno objavimo, za njegovo neokrnjenost skrbi digitalni podpis izdajatelja. Nadzor dostopa do izdanih certifikatov je potreben le v primeru, ko bi razkritje podatkov, ki jih vsebuje certifikat, predstavljalo grožnjo za ohranjanje zasebnosti entitete. Več bomo o varovanju zasebnosti entitete in digitalnih certifikatih spregovorili v nadaljevanju.

Certifikati nastopajo v različnih oblikah in se poleg preverjanja identitete entitete uporabljajo tudi za dodeljevanje pravic (avtorizacijo). Za slednje je priporočljivo, da imajo čim krajšo življenjsko dobo. A tudi za identifikacijske certifikate je kar nekaj dilem o dolžini obdobja veljavnosti.

2. IDENTIFIKACIJSKI CERTIFIKATI

Identifikator entitete je vsak niz podatkov, ki ga lahko povežemo z entiteto (ime, prstni odtis, številka kreditne kartice…). *Identifikacijski certifikati* javnega ključa povezujejo javni ključ entitete z njenim identifikatorjem.

Priporočilo X.509 za digitalne certifikate je eden izmed najbolj znanih in uveljavljenih primerov identifikacijskih certifikatov. Prvi različici priporočil za X.509 združljive certifikate (označujemo jih kot X.509v1 oziroma X.509v2) je ITU (International Telecommunications Union) objavil leta 1988 in 1993 [30]. Prve različice so predvidevale certificiranje javnih ključev prosilcev, ki so enolično poimenovani po priporočilu X.500 za priključne podatkovne zbirke globalno unikatnih nazivov [29]. Naziv v imeniku X.500 je lahko karkoli, čemur lahko pripišemo enolično ime. Tretja revizija priporočila X.509v3, objavljena leta 1997 [28], v veliki meri izboljšuje prilagodljivost certifikata, saj predpisuje standardiziran način dodajanja novih polj v certifikat. Prav tako omogoča uporabo lokalnih imen v certifikatu in s tem priznava, da je globalna shema poimenovanja preveč zapletena in omejujoča.

Na podlagi priporočila X.509 so bili narejeni mnogi standardi in programski paketi za certifikatne agencije. Delovna skupina PKIX (Internet Public Key Infrastructure) je izdelala osnutek informativnega standarda v okviru IETF (Internet Engineering Task Force), ki naj bi certifikate po priporočilu X.509v3 prilagodil za uporabo v globalnih omrežjih (internetu) [27]. Kot primere praktičnih (delujočih) izvedb priporočila X.509 lahko navedemo Fortezzo (standard, temelječ na pametnih karticah za varno elektronsko pošto in šifriranje datotek v Ameriškem obrambnem ministrstvu [23]), S/MIME (Secure Multipurpuse Internet Mail Extensions, standard za elektronsko pošto, ki ga je predlagala RSA Data Security Inc. [58]), SET (Secure Electronic Transaction, protokol za varno izvajanje transakcij s kreditnimi karticami brez prisotnosti kreditne kartice na plačilnem mestu, predlagala sta ga MasterCard in Visa [59]).

Identifikacijski certifikati bodo odigrali pomembno vlogo tudi izven globalnih omrežij z migracijo na pametne kartice. Podjetja za javni prevoz, finančne institucije, ponudniki zdravstvenega zavarovanja načrtujejo razdelitev pametnih kartic med svoje uporabnike kot način uporabe njihovih sistemov. Zaradi omejenih zmogljivosti trenutne generacije pametnih kartic (kot bomo spoznali v četrtem poglavju) identifikacijski certifikati še nimajo dominantne vloge v teh načrtih. Vendar je prehod na digitalne certifikate na dolgi rok iz varnostnih razlogov nujen.

Digitalni certifikati javnega ključa po priporočilu X.509 in porazdeljeni globalni imenik X.500

Priporočilo X.509 je bilo namenjeno overjanju javnih ključev entitet, ki so bile enolično imenovane v X.500 imeniku, in nudi okvir za izgradnjo infrastrukture javnega ključa. X.500 je bil zasnovan za nudenje podpore velikim računalniškim omrežjem.

Za razumevanje certifikatov po priporočilu X.509 si najprej oglejmo priporočilo X.500, ki opisuje globalni imenik entitet [29], [20]. Imenik je urejen hierarhično v

obliki drevesa (DIT – Directory Information Tree). Vsak vnos v imeniku vsebuje množico atributov, na primer organizacijo, kjer posameznik dela, elektronski naslov, certifikat javnega ključa… Zapis lahko predstavlja osebo, računalnik, tiskalnik, podjetje, organizacijo. Za lažje iskanje je vsakemu vnosu v imeniku določeno globalno unikaten naziv (DN – distinguished key). Za zagotavljanje unikatnosti se nazivi dodeljujejo na poseben, standardiziran način.

Vsako vozlišče ima natanko enega predhodnika – starša (izjema je koren drevesa) in poljubno število otrok. Vsakemu vozlišču je prirejeno relativno unikatno ime (RDN-relative distinguished name), ki je unikatno glede na nivo. Globalno unikatno ime dobimo tako, da staknemo RDN-je vseh predhodnih vozlišč. Nivoji drevesa označujejo državo, pokrajino, okraj, organizacijo, organizacijsko enoto in splošno ime entitete.

Problem predlaganega zapisa nazivov entitet po priporočilu X.500 je, da v praksi nikoli ni bila predstavljena delujoča shema poimenovanja. Hierarhični modeli poimenovanja ustrezajo entitetam, ki so same organizirane hierarhično. Globalna omrežja sestavlja množica skupin brez trdnih povezav. Pojavljala se je zaskrbljenost pred zaščito zasebnosti in razkrivanja hierarhije podjetij. Certifikati so bili po priporočilu X.509 namenjeni za kontrolo dostopa do vnosov v imeniku in overjanju javnih ključe entitet, zapisanih v imeniku.

Problem unikatnega poimenovanja entitet je bila rešena s poimenovanjem entitete s stikom države, organizacije, poslovne enote in splošnega imena. Certifikati po priporočilu X.509 v tretji verziji omogočajo poleg unikatnega še alternativno ime entitete. Slednje lahko zajema naslov elektronske pošte, omrežni (IP) naslov...

Digitalni certifikat javnega ključa po priporočilu X.509

Pomen najpomembnejših polj , ki jih vsebuje certifikat [28], [21]:

- verzija: označuje verzijo formata po priporočilu X.509,
- serijska številka: unikatni identifikator, ki ga certifikatu dodeli certifikatna agencija,
- podpisni algoritem: označuje algoritem digitalnega podpisa, s katerim je certifikatna agencija podpisala certifikat,
- ime izdajatelja: v formatu X.500 zapisan naziv certifikatne agencije,
- obdobje veljavnosti: označuje začetni in končni datum, med katerima je certifikat veljaven,
- ime imetnika certifikata: v formatu X.500 je zapisano ime imetnika privatnega ključa, ki mu pripada certifikat javnega ključa,
- informacija o javnem ključu: predstavlja vrednost javnega ključa, vključno z oznako algoritma, pri katerem naj se ključ uporabi.

Certifikati po prvotnem standardu ne vsebujejo vseh informacij, ki jih uporabnik certifikata potrebuje za določanje zaupanja v javni ključ entitete in vrednotenje tveganja (Mendes, Huitema [43], Klobučar [33], Ford, Baum [21], Fox, LaMacchia [24]). Polje, ki označuje imetnika certifikata, je premalo opisno in neprimerno za mnoge aplikacije. Uporabnik pri vrednotenju zaupanja potrebuje informacijo o politiki certificiranja, v skladu s katero je bil certifikat izdan. Omogočeno mora biti razločevanje namena uporabe ključev za entiteto, ki ima več certifikatov. Certifikat mora varovati pred zlonamernimi agencijami z opisom omejitev dovoljenih akcij za imetnika certifikata. Prav tako se pojavlja problem z velikostjo in svežino seznama preklicanih certifikatov. Zato so v tretji različici standarda predvideli možnost neobveznih polj, ki dodatno pojasnjujejo zgoraj navedene pomanjkljivosti.

Priporočilo X.509v3 [28] se je razvilo in preseglo svoje korenine v imeniku X.500 [29]. Verzija 3 je vnesla nekaj korenitih sprememb v zapis certifikatov in seznam preklicanih certifikatov. Oboji so sedaj lahko razširljivi. Izdajatelji certifikatov lahko določijo vsebin o certifikata glede na lastne potrebe. Omogočene so standardne razširitve za dodatne informacije o ključu, varnostni politiki, atributih izdajatelja in imetnika certifikata, omejitve v verigi certifikatov ter večji prilagodljivosti seznama preklicanih certifikatov.

V nadaljevanju se bomo osredotočili le na tiste razširitve, ki bistveno vplivajo na izvedbo infrastrukture javnega ključa na podlagi standarda X.509 Razvrstimo jih lahko v tri kategorije (Ford, Baum [21], Stallings [60]):

- Omogočeno je, da izdajatelj v certifikat vključi uporabljeno politiko certificiranja in namen uporabe ključa. Le-te razširitve naj bi uporabniku digitalnega podpisa pomagale pri odločitvi, ali je certifikat primeren za uporabo.

- Certifikat vsebuje še dodatna, alternativna imena za izdajatelja oziroma imetnika certifikata. To omogoča, da certifikat deluje brez imenika X.500. Kot primeri alternativnih imen so elektronski naslov, naslov URL. Alternativno ime se lahko uporabi tudi za identifikacijo izdajatelja seznama preklicanih certifikatov.

- Razširitve za omejevanje poti pri preverjanju certifikatov. Določajo polja, ki v križnih certifikatih omejujejo pristojnosti podrejenih agencij. Agencijam omogoča, da se povežejo na smiseln način. Agencija določi, ali lahko imetnik certifikata tudi sam deluje kot izdajatelj certifikatov in imensko domeno, za katero lahko izdaja certifikate. Odredi lahko, da certifikat vsebuje identifikacijo politike certificiranja, ki je bila uporabljena pri izdaji certifikat. Z definiranjem primerno strogih pogojev se možne poti preverjanja certifikatov čedalje bolj ožijo, dokler ne preostane le še ena sama izbira.

Seznami preklicanih certifikatov

Priporočilo X.509 za certifikate javnega ključa in globalni imenik X.500 so bili zasnovani v sredini osemdesetih let, še pred eksplozivno rastjo globalnih omrežij. Predvideni so bili za uporabo v okoljih brez neposredne omrežne povezave,

uporabniki bi se v omrežje priključevali le občasno. Tako niso posvečali posebne pozornosti seznamu preklicanih certifikatov. Zanemarili so problem velikosti in svežine seznama.

Seznam preklicanih certifikatov je digitalno podpisana podatkovna struktura, ki našteva serijske številke preklicanih certifikatov, ki niso zapadli (Housley et al. [27]). Za vsak preklican certifikat je naveden tudi čas preklica. Seznam je opremljen s časovno znamko, ki priča o času nastanka seznama. Ker je seznam digitalno podpisan, ni potrebe po varnih in zaupanja vrednih strežnikih za razdeljevanje seznama in vzpostavljanje varne seje. Še vedno pa potrebujemo dostop do varnega strežnika točne ure. Uporabnik preveri status certifikata s preverjanjem vsebovanosti serijske številke certifikata v najnovejši izdaji seznama. Kaj je za aplikacijo zadosti svež certifikat, je običajno zapisano v varnostni politiki sistema. Pogostost izdaje seznama je v domeni certifikatne agencije. Slednje je problem, saj vnaša okno negotovosti med preklicem certifikata in objavo. O problemih, povezanimi z ugotavljanjem statusa certifikatov, se bomo posebej ukvarjali v petem poglavju.

V tretji reviziji priporočila so predvideli razširitev seznama preklicanih certifikatov z možnostjo priključnega preverjanja statusa certifikata (Myers et al.[45]). Uporabnik certifikata se poveže s priključnim strežnikom, ki vodi evidenco o statusu certifikatov. Odgovor na poizvedbo označuje status certifikata. Transakcija mora biti varovana, pošiljatelj in čas nastanka odgovora morata biti nedvoumno znana. Storitev mora imeti visoko stopnjo razpoložljivosti. Z rastjo populacije infrastrukture se pojavlja problem z odzivnostjo strežnika.

Tudi seznami preklicanih certifikatov so z revizijo doživeli razširitve (Ford, Baum [21], Stallings [60], Adams, Zuccherato [1]).

- Vsak seznam, ki je izdan za določeno populacijo certifikatov, nosi zaporedno številko seznama. Tako lahko uporabnik ugotovi, ali je zgrešil katerega izmed objavljenih seznamov. Vsak certifikat v seznamu vsebuje tudi razlog preklica.

- *Točke razdeljevanja seznama* preklicanih certifikatov zmanjšujejo količino podatkov, ki jih mora uporabnik pregledati ob preverjanju veljavnosti certifikata. Agencija razbije seznam na več ločenih delov in jih objavlja/razdeljuje iz več različnih lokacij. Razbitje je lahko na podlagi neke prostorske/naslovne lokalnosti ali glede na razlog preklica.

- *Diferenčni seznami preklicanih certifikatov* (delta CLR) so drug način za zmanjševanje velikosti seznama. Namesto objave celotnega seznama, agencija objavi le spremembe, ki so nastale od zadnje objave celotnega seznama. Uporabnik lahko vodi svoj seznam preklicanih certifikatov, ki ga osvežuje s pomočjo diferenčnih seznamov. Tako prihranimo na času, potrebnem za prenos seznama, in zmanjšujemo obremenitev strežnika.

- *Indirektni seznami preklicanih certifikatov*: razširitev predvideva, da sezname izdaja nekdo drug in ne certifikatna agencija, ki je certifikate izdaja. To omogoča izgradnjo centrov, ki bi zbirali sezname iz več agencij in nudili eno samo razdelilno točko.

Ne glede na vse dodatne možnosti še vedno ni razrešen problem ustrezne svežine seznama (time-granularity problem). Čeprav razdelimo seznam in ga pogosto osvežujemo z diferenčnimi seznami, je še vedno časovno okno negotovosti, ko je lahko kljub vsem preverjanjem certifikat neveljaven (ključ razkrit).

Identifikacijski certifikati in podatkovne zbirke

Uporabnika digitalnega certifikata v mnogih primerih ne zanima identiteta entitete, temveč potrditev prejšnjih stikov, pripadnost skupini, preverjanje osebnih podatkov oziroma upravičenost za izvajanje transakcije. Identifikacijski certifikat lahko služi kot kazalec na zapis v podatkovni zbirki, ki vsebuje relevantne podatke. To uporabniku omogoča posodabljanje podatkov in varno hranjenje negativnih označb o entiteti. Ravno tako omogoča izgradnjo profila entitete za potrebe popisa ali trženja.

Uporaba identifikacijskih certifikatov v povezavi s centralno bazo podatkov ima tako za ponudnika storitev kot za uporabnika kar nekaj slabosti (Brands [9]):

- Poizvedbe v podatkovni zbirki dodatno zakasnijo izvajanje transakcij. To lahko predstavlja ozko grlo pri izvajanju storitev.

- Imetniki certifikata ne morejo z gotovostjo vedeti, ali se bo transakcija izvedla, kar vnaša v proces stopnjo negotovosti. Zahteva se lahko zavrne zaradi napačnih, zastarelih podatkov ali zaradi ozkega grla, ker ni bilo mogoče vzpostaviti povezave s strežnikom.

- V primeru geografsko porazdeljene podatkovne zbirke je preverjanje osrednje podatkovne zbirke zahtevno ali celo nemogoče.

- Zaščita na omrežje priključnih podatkovnih zbirk je zahtevna. Vdori v zbirke ogrožajo ugled upravljalca in prinašajo pravne obveznosti.

- Usklajevanje z določili o varovanju zasebnosti uporabnikov prinaša organizacijam znatne stroške.

Preverjanje podatkov v realnem času v centralni podatkovni zbirki s pomočjo identifikacijskih certifikatov je v nasprotju z idejo digitalnih certifikatov, ki naj omogočajo lokalno preverjanje atributov entitete. Uporaba centralne podatkovne zbirke je nezaželena tudi s stališča uporabnika. Vdori in spreminjanje podatkov so podlaga za napačne odločitve. Napačne podatke je pogosto težko izslediti in jim še težje oporekati.

3. ATRIBUTNI CERTIFIKATI

V začetku devetdesetih se je začela porajati ideja o atributnih certifikatih. Slednji povezujejo enega ali več atributov (datum zapadlosti, definicija varnostne politike,

dovoljenja…) z javnim ključem. Atributni certifikati so posplošen primer identifikacijskih certifikatov, saj je naziv entitete le eden izmed množice možnih atributov. Poleg javnega ključa in identifikacije entitete identifikacijski certifikati ne vsebujejo dodatnih osebnih podatkov o imetniku. Namen atributnih certifikatov je predvsem omogočiti uporabniku certifikata, da poleg naziva entitete preveri tudi druge atribute (dovoljenja, pravice dostopa, ustreznost s standardi in predpisi…). Veljavnost atributnega certifikata je omejena z atributom z najkrajšo dobo veljavnosti.

Atributni certifikati imajo nekaj pomembnih prednosti pred identifikacijskimi certifikati (Brands [9]):

- Pri odločanju združujejo vse atribute, pomembne za uporabnika certifikata. Če strani pred transakcijo nista vzpostavili kontakta, je primarni interes uporabnika certifikata pred izvedbo transakcije preverjanje ustreznosti dovoljenj in ostalih bistvenih atributov entitete. Certifikat lahko vsebuje vse atribute, ki bi se sicer morali nahajati v centralni podatkovni zbirki kot vnos za entiteto.

- Mnogim uporabnikom infrastrukture je pred izdajo certifikata nadležno fizično preverjanje v agenciji za registracijo. Atributne certifikate je možno izdati tudi brez prisotnosti prosilca.

- Mnogo težje, dražje in bolj izpostavljeno napakam je ugotoviti identiteto prosilca, kot pa določiti akcije, ki jih sme izvajati. Prav tako je lahko certifikatna agencija izpostavljena večjim poroštvom. Velja, da so le vladne ustanove in velike organizacije (na primer finančne institucije) zmožne zanesljivo ugotavljati identiteto entitete.

- Ideja o izgradnji družbe, kjer bo vsak posameznik odgovoren za svoja dejanja na podlagi identifikacije, je v osnovi zgrešena. Identiteto lahko ugotavljamo le na podlagi papirnatih dokumentov in tako nasledimo vse njihove varnostne pomanjkljivosti.

Pri infrastrukturah javnega ključa, kjer je poleg identifikacije večji poudarek na drugih atributih, lahko ustvarimo znatne prihranke in se izognemo goljufanjem z identiteto.

Standardizacija koncepta atributnih certifikatov predstavlja SPKI (Simple Public Key Infrastructure, Ellison [17], Ellison et al. [18]). Slednja zavrača ne le osredotočenja na identiteto imetnika ključa, ampak tudi uporabo globalnih imen in hierarhično strukturo certifikatnih agencij (modela zaupanja). Leta 1997 se je SPKI združila s SDSI (Simple Distributed Security Infrastructure, Rivest in Lampsonov predlog za infrastrukturo javnega ključa [55]). Temelji na lokalnih imenih ter se osredotoča na javni ključ. SPKI/SDSI 2.0 združuje SDSI lokalna imena in SPKI atributne certifikate [55].

Atributni certifikat ima na podlagi tretje revizije priporočila X.509 [28] enako sintakso kot certifikat X.509v3, le brez navedbe javnega ključa. Vsebuje še kazalec na identifikacijski certifikat za potrebe prepoznavanja. Entiteta ima lahko več atributnih certifikatov, povezanih z identifikacijskim certifikatom. To je prednost, saj atributu ne

povečujejo identifikacijskega certifikata, vrednosti atributov pa se lahko osvežujejo neodvisno od identifikacijskega certifikata.

4. INFRASTRUKTURA JAVNEGA KLJUČA

Infrastruktura javnega ključa omogoča uporabo asimetrične kriptografije v globalnih omrežjih. Je nepogrešljiva za uveljavitev elektronskega poslovanja v globalnem merilu. Sestavljena je iz certifikatnih agencij, imetnikov certifikatov, uporabnikov certifikatov in podpornih storitev za upravljanje s certifikati. Poleg agencij, ki izdajajo certifikate, igrajo pomembno vlogo tudi agencije za registracijo (Ford, Baum [21]). Slednje ne izdajajo certifikatov, marveč v imenu certifikatne agencije registrirajo prosilce za certifikat, preverijo njihovo identiteto in posedovanje para ključev. Agencije za registracijo običajno predstavljajo avtoriteto za vsebino certifikata (poimenovanje, predpisane politike, dovoljeni načini uporabe…). Storitve, ki jih nudi infrastruktura, so poimenovanje naročnika certifikata, registracija, podpisovanje javnega ključa, objava certifikata, podaljšanje veljavnosti ključev, zamenjava ključev, preklic certifikata, seznami preklicanih certifikatov, rekonstrukcija zasebnega ključa.

Pri izgradnji infrastrukture se je potrebno odločiti za strukturo, v katero bodo povezane certifikatne agencije, usklajevanje politik certificiranja, podporne protokole za upravljanje s certifikati. Če hočemo prenesti koncepte upravljanja s certifikati v globalna omrežja, sestavljena iz raznovrstnih organizacij in okolij, zasledimo mnoge probleme, ki niso tehnološkega značaja, a jih je potrebno za zadovoljivo delovanje sistema razrešiti. Tu v prvi vrsti mislimo na pravne vidike elektronskega (digitalnega) podpisa, preprečevanje tajenja in dokazovanja na sodišču. Cela vrsta dodatnih podpornih storitev, tako tehnoloških kot pravnih, je potrebna, da lahko izkoristimo potenciale infrastrukture v celoti.

V svetu trenutno ne obstaja neka prevladujoča infrastruktura javnega ključa. Po predvidevanjih se bo vzpostavilo več med seboj neodvisnih infrastruktur. Med seboj bodo zgradile različne stopnje sodelovanja. Splošno je sprejeta teza, da bodo sobivale mnoge vrhovne certifikatne agencije, čeprav bo morda na lokalnem nivoju ena sama.

Izgradnja infrastrukture mora zadovoljiti vrsto med seboj nasprotujočih si zahtev. Navedimo le najpomembnejše (Ford, Baum [21], MITRE [4]):

a. *Razširljivost* je osnovna zahteva, ki naj jo izpolnjuje infrastruktura javnega ključa. Tako zmanjšujemo stroške postavitve, delovanja, ter omogočimo enostavno in varno uporabo enega kompleta certifikatov za komuniciranje z raznolikimi partnerji.

b. Zaradi enostavnosti uporabe, varnosti in zniževanja stroškov naj skupna infrastruktura *podpira več aplikacij*. Uporabniku, ki je vključen v infrastrukturo, omogočimo izkoriščanje varnostnih storitev pri uporabi elektronske pošte, prenosu datotek, brskanju po svetovnem spletu...

c. S stališča varnosti in upravljanja je nepraktično graditi eno samo globalno infrastrukturo. *Povezljivost ločenih infrastruktur* je pogoj za izpolnitev zahteve v točki a.

d. Vsak uporabnik si v skladu s svojo varnostno politiko izbira pot v modelu zaupanja. Veriga certifikatov, primerna za eno aplikacijo, ni nujno ustrezna za drugo. Za izpolnitev zahtev v točkah a. in b. je potrebno zagotoviti *povezavo politik certificiranja z verigo certifikatov*. S tem zagotovimo izvajanje varnostne politike in omogočimo uporabniku, da sam določa zahteve, primerne za različne aplikacije. Odločitve o zaupanju in tveganju so tako pod kontrolo uporabnika.

e. Vsaka entiteta, ki upravlja ali uporablja infrastrukturo javnega ključa, mora imeti *pregled nad porazdelitvijo tveganja* med stranema, ki komunicirata.

f. Pomemben poseben primer točke e. je *stopnja odgovornosti za nastalo škoda*, ki jo certifikatna agencija krije in je v razmerju s tveganjem, ki ga prevzema pri izdaji certifikata, ter v skladu s politiko certificiranja. MITRE [4] navaja primere, v katerih agencija ni odgovorna za nastalo škodo, ali je odgovorna le v omejenem obsegu. Če navedemo najpomembnejše, so to: izguba ključa ali šibko generiranje ključev s strani uporabnika, ali pa da certifikat ni bil preklican v skladu s politiko certificiranja. Stopnja odgovornosti za nastalo škodo mora biti nedvoumno zapisana v politike delovanja, ki jo izda agencija.

Na trenutni stopnji razvoja infrastruktur javnega ključa sta bistveni pomanjkljivosti odsotnost avtomatskega primerjanja politik certificiranja z varnostno politiko organizacije in ugotavljanje statusa certifikatov. Posledica je oteženo ovrednotenje tveganja in gradnja zaupanja v verigo certifikatov. Sklenemo lahko, da je izpolnjevanje točk e.in d. najšibkejša točka trenutno delujočih infrastruktur javnega ključa.

Povezovanje certifikatnih agencij

Temeljna naloga pri izgradnji velike in razširljive infrastrukture javnega ključa je poenostaviti oziroma pohitriti gradnjo in preverjanje verig certifikatov. Predstavlja najpogostejšo storitev, ki jo uporabnik zahteva od infrastrukture. Storitev vključuje iskanje certifikatov, preverjanje njihovega statusa, primerjavo politik certificiranja ter ovrednotenje stopnje tveganja in zaupanja v različne verige. Avtomatizacija postopkov je za končnega uporabnika nujna.

Odločilno vlogo pri uporabi infrastrukture odigra povezovanje agencij med seboj. Strukturo, ki se pri tem vzpostavi, imenujemo *model zaupanja* in je v veliki meri izraz okolja, za katerega je bila infrastruktura zgrajena, oziroma kdo jo uporablja. Ponazorimo ga lahko z grafom, kjer množica vozlišč predstavlja subjekte infrastrukture (certifikatne agencije, uporabnike), povezave med njimi pa izdane certifikate. Vsaka povezava določa certifikat, ki vsebuje informacijo o javnem ključu in politikah, v skladu s katerimi je bil izdan. Glede na graf lahko razlikujemo sledeče modele zaupanja (Feghhi et al. [20], Ford, Baum [21]).

Splošni hierarhični model

Je najpreprostejša rešitev problema. Drevesna struktura predstavlja sistematično in učinkovito rešitev za povezovanje velikih skupin uporabnikov. Izgradnja certifikatne

verige je preprosta, ne glede na to, katero agencijo je uporabnik pripravljen sprejeti za primarno (ji zaupati). Razširljivost modela s povečevanjem števila uporabnikov in agencij je preprosta. Dolžina verige certifikatov je tudi pri velikem drevesu razmeroma kratka. Uporabnik mora zaupati vsaki agenciji na poti. Problem rešitve je, da mnogo poti zajema vrhovno certifikatno agencijo, kateri morajo posledično zaupati vsi uporabniki certifikatov. V primeru razkritja zasebnega ključa vrhovne agencije je ogrožena celotna infrastruktura, kar predstavlja šibko točko celotnega sistema. Zaradi zadržkov pri vzpostavljanju zaupanja v vrhovno agencijo je model uporaben za specifične primere ali zaprte skupnosti.

Splošni hierarhični model z dodatnimi povezavami

Z dodatnimi povezavami med poljubnimi certifikatnimi agencijami lahko skrajšamo verigo certifikatov in se izognemo striktnemu vključevanju vrhovne agencije v verigo. Povezave niso del osnovne hierarhije. Ni nujno, da so povezave dvosmerne. Kot dodatna možnost omejitve različnih poti je določitev sprejemljivih politik in dopustnih imen, podrejenim certifikatnih agencijam (Ford, Baum [21]).

Hierarhija z odlikovanim vozliščem

Kot različica osnovne strukture je bila razvita hierarhija, kjer podrejene agencije ne overjajo ključev nadrejenih agencij. Vse poti se začnejo pri vrhovni agenciji. Največja dolžina verige je enaka globini drevesa. Uporabniki morajo na varen način pridobiti javni ključ vrhovne agencije. Prednost slednjega pristopa je, da obstaja le ena pot med korenom strukture in imetnikom certifikata, kar odjemalcem omogoča priložiti ustrezno verigo certifikatov. Zaradi sporne zahteve po zaupanju vrhovni agenciji je rešitev v globalnih omrežjih malo verjetna. Uporabna je za okolja, kjer se naravna hierarhija v organizaciji ujema z modelom.

Drevo hierarhičnih modelov

Osnovni problem pri še tako dobro zasnovani arhitekturi je, da uporabnik težko sprejema dejstvo, da mora za vse transakcije zaupati neki točno določeni certifikatni agenciji. Tako pridemo do ideje povezati med seboj ločene hierarhije. Vrhovne certifikatne agencije posameznih infrastruktur se med seboj povežejo, obojestransko certificirajo. Model se izkaže za najlažje prenosljivega v prakso. Posamezne infrastrukture nastajajo kot ločeni otočki, ki bodo s časom sami začutili težnjo po povezovanju. Če model podpira razširljivost neomejenega števila lokalnih infrastruktur, postane omrežje povezav med njimi zelo prepleteno. Le-to odpre mnoga nova vprašanja, na primer iskanje najustreznejše poti (kriteriji odločanja), preverjanje politike certificiranja posamezne lokalne infrastrukture, vrednotenje tveganja.

Veriga certifikatov

Pred vsako uporabo javnega ključa moramo najprej preveriti njegovo pristnost. *Veriga certifikatov* je množica certifikatov, kjer je prvi certifikat samopodpisani certifikat agencije, ki ji zaupamo. Zadnji v verigi je certifikat odjemalca. Eden izmed najpomembnejših storitev, ki naj jo infrastruktura javnega ključa nudi, je gradnja in preverjanje verige certifikatov. Dostopna mora biti vsakemu sistemu, ki uporablja

certifikate. Udobneje je storitev ločiti na dva dela, saj sta izvedbi precej različni. Prvi je s stališča varnosti nekritičen, kar pa za drugega nikakor ne moremo trditi.

Gradnja verige certifikatov

Poiskati moramo pot med certifikatom entitete in certifikatno agencijo, ki ji zaupamo. Zahtevnost gradnje verige je v veliki meri odvisna od modela zaupanja. Pri tem se nam kar sama vsiljuje ideja, da bi podpisnik ob podpisu priložil tudi verigo certifikatov.

Če se problema lotimo v najtrši obliki, imamo na voljo le certifikat entitete in seznam agencij, ki jim zaupamo, oziroma njihove javne ključe. Pot med certifikatom entitete in zaupanja vredno agencijo lahko najdemo, če nam infrastruktura javnega ključa ponuja vsaj eno izmed storitev:

- Ob predložitvi imena agencije nam storitev vrne križne certifikate javnega ključa agencije, ki so jih izdale druge agencije v infrastrukturi.

- Storitev vrne vse križne certifikate, ki jih je izdala certifikatna agencija.

Seveda je to najtežji primer, ko model zaupanja ni strukturiran in je infrastruktura obsežno razvejana. S prisotnostjo hierarhije ali zmerne razvejanosti je postopek hiter in močno poenostavljen. V praktičnih implementacijah je malo verjetno, da bi globina hierarhije presegala štiri nivoje, bila kompleksna in močno razvejana.

Preverjanje verige certifikatov

Po zgraditvi verigo preverimo. Postopek poteka rekurzivno od certifikata agencije, ki ji zaupamo, do certifikata podpisnika (Ford, Baum [21]).

- Preverimo digitalni podpis certifikata in ali je certifikat zapadel. Pomembno je, da imamo dostop do varnega strežnika točne ure.

- Preverimo ujemanje imen v certifikatih z izbrano potjo. Imetnik certifikata je naveden kot izdajatelj sledečega v verigi.

- Ugotovimo status certifikata. Certifikat je bil lahko preklican ali sploh ne obstaja.

- Preverimo skladnost politike certificiranja z varnostno politiko uporabnika.

- Preverimo osnovne omejitev (namen izdaje certifikata, jamstvo...) in imenske omejitev (ali agencija sploh sme izdajati certifikate za imensko domeno...).

Pomembno je, da je celoten postopek preverjanja izveden varno. Če uspe napadalcu spodkopati varnost postopka (zamenja certifikat javnega ključa agencije, ki ji uporabnik zaupa, premakniti referenčno uro...) je rezultat enak, kot če bi podtaknili

lažni javni ključ. Ponareja lahko digitalne podpise in dešifrira sporočila, namenjena drugim entitetam.

Preverjanje digitalnih podpisov in neokrnjenosti potrdil je lažji avtomatski del preverjanja. Težje je odločati, v kolikšni meri lahko zaupamo agenciji. Stopnjo zaupanja lahko določimo šele na podlagi informacij o delovanju certifikatne agencije. Slednji so zapisani v politiki certificiranja.

5. KRITIKE INFRASTRUKTURE JAVNEGA KLJUČA

Pojavljajo se številne kritike organizacije infrastrukture javnega ključa. Nekatere se osredotočijo na tehnološko plat mehanizmov za delo s certifikati (Ellison, Schneier [19], Rivest [56], Brands [9]). Spet druge kritizirajo organizacijske pomanjkljivosti zasnove infrastrukture javnega ključa (Brands[9], Fox, LaMacchia [22], Davis [16], Klobučar [33]). Razdelimo jih lahko na kritike mehanizmov za ugotavljanje statusa certifikatov, porazdelitev bremena hranjenja in upravljanja s ključi, ogrožanje zasebnosti entitet ter odsotnost formalizacije politik certificiranja in upravljanje z zaupanjem. Nekatere izmed naštetih kritik bomo predstavili v tem poglavju, medtem ko bomo drugim namenili samostojna poglavja.

Grožnja za ohranjanje zasebnosti pri uporabi digitalnih certifikatov

Varovanje zasebnosti lahko definiramo kot zahtevo posameznika, skupin ali organizacij, da sami določajo kdaj, kako in v kakšnem obsegu je dovoljeno informacije o njih in njihovih dejavnostih posredovati drugim (Brands [9]). Nadzor definiramo kot dejanje spremljanja in vrednotenja aktivnosti posameznika.

Infrastrukture javnega ključa trenutno omogočajo nadzor vseh komunikacij in transakcij, ki jih entiteta izvaja s pomočjo digitalnega certifikata. Vsak digitalni certifikat enolično določa imetnika para ključev in omogoča avtomatično sledenje gibanja entitete v sistemu. Tudi atributnim certifikatom, ki ne predstavljajo identitete lastnika, lahko sledimo, saj ima vsak digitalni certifikat zaradi varnostnih razlogov (preklic…) unikatno serijsko številko. Digitalni certifikat predstavlja digitalizirano analogijo prstnega odtisa.

S pomočjo serijske številke, ki se v omrežju pojavi, ko imetnik certifikata komunicira ali izvaja transakcije, lahko zgradimo podroben dosje. Gradimo ga brez človeške intervencije, avtomatično in v realnem času. Vsebuje njegovo finančno stanje, navade, zdravstveno stanje, gibanje… Vsak digitalni podpis, ki ga tvori imetnik certifikata, dodamo v dosje in predstavlja izjavo, ki je ni mogoče zanikati.

Digitalne certifikate lahko zlorabimo, da posamezniku onemogočamo dostope do storitev in preprečujemo komuniciranje. V omrežne usmerjevalnike zapišemo seznam certifikatov. Podatke, ki jih partner s ciljnim certifikatom proizvaja, filtriramo za kasnejšo analizo ali takojšno akcijo. Priključno preverjanje veljavnosti certifikatov omogoča agencijam vpogled kdo s kom komunicira v realnem času.

Uporaba pametnih kartic za hranjenje digitalnih certifikatov še poslabša problem varovanja zasebnosti. Praktično je nemogoče preveriti, ali pametna kartica ne prepušča zasebnih podatkov, shranjenih v kartici. Problem je preprečiti dostop več aplikacijam do podatkov na njej brez privoljenja imetnika kartice.
Moč nadzora ni na voljo le uporabnikom certifikata, ampak tudi vohunskim organizacijam, delodajalcem in organizacijam, ki izdajajo certifikate. Kot predstavnike slednjih lahko navedemo finančne in državne ustanove, zavarovalnice, telekomunikacijska podjetja.

Pomanjkljivosti zasnove infrastrukture javnega ključa

Infrastruktura javnega ključa ima v primerjavi s sistemi, ki uporabljajo za varovanje komuniciranja simetrične šifrirne postopke nižje režijske stroške. Prednost je v veliki meri posledica skritih administrativnih stroškov na strani uporabnikov infrastrukture. Varnost sistemov, ki uporabljajo asimetrično kriptografijo, temelji na zaupanju, da bodo uporabniki temeljito preverili javne ključe entitet, s katerimi komunicirajo, in skrbno hranili svoje zasebne ključe (Davis [16]).

Kriptografija javnega ključa je brez dvoma primernejša za globalna omrežja. Upravljanje je preprostejše, nudi dodatne varnostne storitve, manj omejuje uporabnike pri določanju zaupanja v entitete in je primernejše za geografsko razprostranjena omrežja. Velika hiba je pretirana odvisnost od uporabnikovega spoštovanja varnostnih postopkov.

Če primerjamo komponente sistemov, ki uporabljajo simetrično oziroma asimetrično kriptografijo, opazimo:

- Pri uporabi simetrične kriptografije mora strežnik ključev posredovati pred vsako vzpostavitvijo zveze. Entiteti pred začetkom varnega komuniciranja prevzameta kratkoživi sejni ključ. Strežnik za razdeljevanje skrivnih sejnih ključev mora uživati zaupanja uporabnikov in biti vedno na razpolago.

- Strežnik za izdajanje certifikatov (certifikatna agencija) ne potrebuje visoke stopnje razpoložljivosti, saj izdajanje certifikat ni časovno kritična operacija. Med odjemalci mora uživati zaupanje.

- Imenik, ki hrani izdane certifikate, olajša delo uporabniku certifikata, saj mu omogoča enostaven dostop do certifikata entitete. Zagotavljati mora visoko stopnjo razpoložljivosti. Ker ne more neopazno spreminjati certifikatov zaupanje v imenik ni problematičen.

- Strežnik, ki skrbi za objavljanje statusa certifikatov, mora uživati zaupanje, da brez zamude objavlja preklicane certifikate. Glede na izvedbo mehanizma za preklic, na primer za priključno preverjanje, je lahko potrebna visoka stopnja razpoložljivosti.

V primeru uporabe infrastrukture javnega ključa ni nikoli hkrati potrebe po veliki stopnji zaupanja in razpoložljivosti komponent infrastrukture. Prav tako komponente

ne predstavljajo ozko grlo sistema, saj ni potrebe dostop do strežnika za vsako transakcijo. Prednosti so posledica večje obremenitve uporabnikov infrastrukture. Uporaba infrastrukture zahteva pridobivanje in lokalno procesiranja podatkov. Uporabnik mora pogosto preverjati certifikate drugih entitet in varovati ključe pred razkritjem ali zamenjavo. Infrastruktura javnega ključa mu pri tem niti ne pomaga niti nima načina, da bi nadzorovala uveljavljanje ustreznih varnostnih postopkov.

- Praktično vsi protokoli (na primer SSL [60], SET [59]), ki uporabljajo infrastrukturo javnega ključa, ignorirajo problem preverjanja pristnosti javnega ključa korenske certifikatne agencije, ki ji uporabnik zaupa. Pristni javni ključ izdajatelja je ključen za preverjanje digitalnega podpisa certifikatov, ki jih je izdal. Infrastruktura ne nudi avtomatiziranega postopka za preverjanje pristnosti ključa. Tudi ko uporabnik pridobi pristni ključ agencije, mora samopodpisani certifikat varovati pred zamenjavo.

- Preden uporabimo javni ključ entitete, moramo preveriti veljavnost digitalnega podpisa in status certifikata. Preverjanje podpisa je postopek, ki ga opravi uporabnik lokalno na svojem računalniku. Ugotavljanje statusa lahko uporabnik preveri le z dostopom do strežnika, ki hrani statuse izdanih certifikatov. Preprosto pravilo pravi (Davis [16]), da je strošek izdaje ključa in njegovega preklica konstanten. V primeru uporabe infrastrukture javnega ključa je preklic ključa mnogo zahtevnejše opravilo kot izdaja ključa (certifikata) entiteti. Tako je izgubljena bistvena prednost uporabe asimetrične kriptografije pred simetrično, neodvisnost od strežnikov in s tem izogibanje ustvarjanja kritičnih točk sistema (single point-of failure). Dodatno breme, ki ga prinaša preverjanje statusa, sili uporabnika k opustitvi ugotavljanja statusa z vsemi posledicami, ki jih ima za varnost izvajanja transakcij.

- Upravljanje z zasebnim ključem je še en problem, s katerim se mora spopasti uporabnik. Če hoče zasebni ključ uporabljati, ga mora imeti shranjenega v delovnem pomnilniku računalnika. S tem je ključ izpostavljen kraji (Shamir, Someren [62]). Simetrični sistemi z uporabo kratkoživih sejnih ključev omejujejo škodo v primeru razkritja skrivnega ključa. Četudi je ključ shranjen na pametni kartici, je težko kontrolirati dostop različnih aplikacij do kartice. Sklenemo lahko, da je zasebni ključ varen le toliko, kot je varen računalnik, na katerem se nahaja.

Infrastruktura ne vključuje upravljanja s ključi, saj je upravljanje s ključi preneseno na uporabnika. Uporabnik mora temeljito preveriti vse javne ključe entitet, ki jih uporablja, in skrbno varovati svoje zasebne ključe. Nekatere postopke upravljanja s ključi je praktično nemogoče avtomatizirati. To je preverjanje pristnosti ključa agencije, ki ji zaupa, izbira gesla za dostop do zasebnih ključev, izvajanje varnostnih ukrepov v sistemu, ki hrani ključe. Običajni uporabnik infrastrukture ne zna ali ni pripravljen upravljati s ključi na ustrezen način. Tudi v primeru, ko postopke lahko avtomatiziramo (na primer ugotavljanje statusa certifikata), je pričakovati, da bo zaradi zmogljivostnih razlogov delovanja pristajal na kompromise v škodo varnosti. Pravila izvajanja operacij je zaradi odsotnosti centralne avtoritete težko uveljavljati. Vedenje uporabnikov je šibka točka vsakega varnostnega sistema. Infrastruktura javnega ključa nima načina za odpravo vgrajene šibkosti.

Politika certificiranja

Uporabnik ima potrebo ovrednotiti stopnjo zaupanja v javni ključ entitete, oziroma v certifikatno agencijo, ki je certifikat izdala. Običajno stopnjo zaupanja določi glede na politiko certificiranja, ki jo agencija uporablja pri izdajanju certifikatov.

Politika certificiranja je množica pravil, ki določajo uporabnost certifikata v določenem območju in/ali razredu aplikacij s skupnimi varnostnimi zahtevami. Definira se neodvisno od infrastrukture javnega ključa. Regulira odnose med agencijo, imetniki certifikatov, uporabniki certifikatov, ter dejansko definira infrastrukturo. Agencija za certificiranje lahko izdaja certifikate v skladu z različnimi politikami. Poznavanje politike je ključno za vrednotenje povezave med javnim ključem in imetnikom ter za odločitev uporabnika, ali je ključ primeren za uporabo v aplikaciji. Vsaka agencija izda izjavo o postopkih in pravilih delovanja (CPS, certification practice statement, Ford, Baum [21], Chokhani, Ford [13]), ki jih izvaja pri upravljanju s certifikati. V njej opisuje, kako se politike certificiranja uporabljajo v kontekstu sistemske arhitekture postopkov, ki jih izvaja. Uporaba standardne formalizirane strukture zapisa politike certificiranja in izjave o postopkih delovanja bi bile zelo dobrodošle za uporabnike infrastrukture javnega ključa.

Pri tretji različici priporočil za digitalne certifikate [28] je bila sprejeta odločitev, da se v certifikate javnega ključa vključijo tudi politike certificiranja. Vključene so bile z uvedbo enoličnih identifikatorjev. Vključitev informacij o politiki bi nedopustno povečalo velikost certifikata. Žal pa format zapisa in vsebina politike certificiranja nista bili določeni. Kot posledica tega so politike certificiranja še vedno zapisane neformalno. Neenoten in neformaliziran zapis politik povzroča njihovo nejasnost in preobsežnost. Iz njih je težko izluščiti bistvene lastnosti, ki so nujno potrebne pri tehtanju o meri zaupanja v javni ključ entitete, politike so med seboj tudi težko primerljive. Ravno zato vsebina politike ne more biti del mehanizma za preverjanje in graditev zaupanja v javni ključ entitete. Formalni zapis politike bi omogočal naslednje (Klobučar [33]):

- Olajšano bi bilo odločanje uporabnikov, katere politike zadoščajo njihovim zahtevam (varnostni politiki), in kateri certifikati so sprejemljivi za izvajanje posameznih storitev.

- Aplikacije bi lahko same preverjale politike certificiranje ter njihovo skladnost z lokalno varnostno politiko ob preverjanju verige certifikatov, graditvi zaupanja in vrednotenju tveganja.

- Certifikatne agencije bi lažje in hitreje zgradile lastne politike certificiranja z izbiranjem in združevanjem osnovnih gradnikov.

- Lažja bi bila tudi primerjava politik različnih agencij in odločanje o ekvivalentnosti.

- Olajšalo bi odločanje ali so politike podrejenih agencij v skladu z lastno politiko agencije.

III. SIMETRIČNA IN ASIMETRIČNA KRIPTOGRAFIJA

V sledečem poglavju si bomo ogledali kriptografske tehnike, ki tvorijo osnovo za infrastrukturo javnega ključa. Bolj kot šifrirni postopki in matematične osnove nas bo zanimalo, kako specifične lastnosti šifrirnih postopkov učinkovito uporabimo v okviru infrastrukture. Prav tako si bomo ogledali neformalna pravila, ki jim mora posameznik upoštevati pri shranjevanju dokazil za preprečevanje tajenja. Poglobljeno razpravo o matematičnih osnovah in šifrirnih postopkih najdemo v klasičnih delih (Stinson [63], Stallings [60]).

Kriptografija je znanost, ki poizkuša stroške razkritja podatkov povečati nad morebitno dobit v primeru uspešnega napada. Ker se vrednost podatkov s časom zmanjšuje, sta čas in napor, potreben za razkritje šifriranih podatkov, večja kot je vrednost podatkov za napadalca. Kriptografija se ukvarja s postopki, ki pretvarjajo podatke, čistopis v neberljivo obliko, oziroma obratno; s postopkom pretvorbe kriptograma v čistopis. Šifriranje je pretvorba podatkov v obliki, ki jo je skoraj nemogoče razbrati brez poznavanja šifrirnega ključa. Cilj je zagotoviti skrivanje vsebine pred nepoklicanimi, četudi imajo dostop do šifriranih podatkov. Dešifriranje je inverzna pretvorba in pretvori podatke nazaj v berljivo obliko. Tako šifriranje kot dešifriranje potrebujeta za pretvarjanje skrivni podatek, ključ. V primeru simetričnih šifrirnih postopkov sta šifrirni in dešifrirni ključ enaka, pri asimetričnih šifrirnih postopkih sta ključa različna. Kriptografija nudi več kot le varovanje podatkov. Z njeno pomočjo lahko izvajamo prepoznavanja in onemogočamo tajenje.

Kriptografski postopki temeljijo na težko rešljivih problemih. Problem je težko rešljiv, če algoritem, ki bi imel polinomsko časovno odvisnost reševanja problema v odvisnosti od vhodnih podatkov, ni znan.

1. NAPADI IN VARNOSTNE STORITVE

Za pregled možnih napadov si računalniški sistem predstavljamo kot vir, ki nudi storitve drugim entitetam. *Napad* je vsaka akcija, ki ogroža varnost podatkov ali sistema. Cilj napada je onemogočati razpoložljivost virov, razkritje zaupnih podatkov, spreminjanje podatkov, ponarejanje podatkov. Napade lahko razvrstimo na pasivne in aktivne.

Pasivni napadi vključujejo prisluškovanje komunikaciji ter spremljanje in analizo prometa med entitetami. Cilj prisluškovanja je vpogled v zaupno vsebino sporočila. Analiza prometa omogoča napadalcu razkritje lokacije in identitete entitet ter pogostost in dolžino sporočil, ki si jih izmenjujeta. Težko jih je odkriti, saj ne spreminjajo sporočil. Poudarek pri zaščiti je bolj na preprečevanju kot na odkrivanju.

Aktivni napadi vključujejo spreminjanje pristnih podatkov (sporočil) oziroma podtikanje lažnih. Razdelimo jih na pretvarjanje, podtikanje starih sporočil, spreminjanje sporočil in preprečevanje strežbe. Pretvarjanje je napad, ko napadalec hlini drugo entiteto. Preprečevanje teh napadov je težko, zato se omejimo na njihovo zaznavanje in odstranjevanje posledic, kar lahko prispeva k preprečevanju.

Varnostne storitve povečujejo varnost računalniških sistemov in podatkov med prenosom po omrežjih. Storitve, ki jih nudijo kriptografski sistemi, so prepoznavanje, zagotavljanje neokrnjenosti podatkov, ohranjanje zaupnosti podatkov, preprečevanje tajenja izvedenih akcij in kontrola dostopa za zagotavljanje razpoložljivosti virov (Stallings [60]). Podrobneje si poglejmo posamezne storitve.

- *Prepoznavanje* zagotavlja pristnost komunikacije. Prejemnik sporočila je prepričan, da je izvor sporočila res entiteta, ki se izdaja za pošiljatelja. Ob vzpostavljanju povezave storitev zagotavlja, da sta entiteti pristni. Med komuniciranjem varuje pred napadalcem, ki se pretvarja kot pošiljatelj oziroma sprejemnik s ciljem pošiljanja ali sprejemanja sporočil.

- *Neokrnjenost podatkov* varuje podatke pred aktivnimi napadi v omrežju. Storitev bolj kot preprečevanje nudi odkritje napada. V primeru povezavno orientirane zveze skrbi, da se sporočila med prenosom po omrežju ne spreminjajo, podvajajo, vstavljajo nova, podtikajo stara, ali da se vrstni red sporočil ne spreminja. Prav tako varuje pred brisanjem sporočil. V primeru nepovezavno orientirane zveze storitev nudi le zaščito pred spreminjanjem sporočil, saj varuje le posamezna sporočila brez ozira na širši kontekst.

- *Zaupnost* je zaščita podatkov pred pasivnimi napadi med prenosom. Stopnja zaščite lahko variira od zaščite vseh podatkov, ki si jih izmenjujeta entiteti, do zaščite posameznih sporočil. Prav tako lahko storitev zaupanja omogoča zaščito prometa podatkov pred analiziranjem. Napadalcu onemogočimo spremljanje pošiljatelja in prejemnika sporočil, frekvenco pošiljanja, dolžino sporočil in ostalih lastnosti prometa med entitetami.

- *Preprečevanje tajenja* onemogoča pošiljatelju zanikanje poslanega sporočila. Prejemnik lahko dokaže, da je sporočilo poslal navedeni pošiljatelj.

- *Kontrola dostopa* omogoča omejevanje in kontrolo dostopa do virov. Vsako entiteto, ki želi dostop do vira, je potrebno najprej prepoznati in ji na podlagi tega določiti pravice.

- *Razpoložljivost* omogoča uporabo sistema overjenim entitetam. Storitev razpoložljivosti omogoča dostopnost in uporabo virov z naslednjimi protiukrepi: prepoznavanjem, šifriranjem in fizičnim varovanja.

2. ŠIFRIRNI POSTOPKI

Simetrični šifrirni postopki

Simetrični šifrirni postopek je klasična oblika šifriranja, znana že iz antičnih časov. Čistopis in šifrirano sporočilo sta običajno enake velikosti. Uporabniki simetričnega kriptografskega sistema si delijo skupni *skrivni ključ*. Ključ se uporablja tako za šifriranje kot dešifriranje sporočil. Sporazumevanje in izmenjava skrivnega ključa pred prenosom sporočil zahtevata vzpostavitev varnega kanala.

Obstajajo sistemi, ki omogočajo varno komuniciranje v globalnih omrežjih le z uporabo simetrične kriptografije. Temeljijo na strežniku za razdeljevanje ključev. Strežnik mora uživati zaupanje entitet in nuditi visoko stopnjo razpoložljivosti storitve. Hkrati predstavlja kritično točko sistema v primeru odpovedi ali napada. Kratkoživi sejni ključi so shranjeni v varnem centralnem strežniku. Entitete si s strežnikom delijo skupni skrivni ključ. Za varno komuniciranje jima strežnik za čas trajanja seje dodeli sejni ključ. Med najbolj znanimi sistemi je Kerberos [36]. Vzdrževanje in varovanje strežnika zahteva precejšna sredstva, prav tako je problem z odzivnostjo pri naraščanju števila uporabnikov.

Običajno se za zagotavljanje varnosti uporablja kombinacija asimetrične in simetrične kriptografije. Z uporabo asimetrične kriptografije si entiteti varno izmenjata skrivni sejni ključ in nato sporočila šifrirata z uporabo simetričnih šifrirnih postopkov (na primer SSL [60]). Prednost simetričnih pred asimetričnimi šifrirnimi postopki je večja hitrost šifriranja. Zato se običajno uporabljajo za šifriranje vsebine sporočil.

Sistemi, temelječi na simetrični kriptografiji, so primerni za overjanje sporočil, ki si jih izmenjuje majhna skupina entitet, katere si med seboj zaupajo. Uporabne so le za prepričevanje prejemnika, da je informacijo poslal legitimni pošiljatelj. Ne morejo pa prepričati tretje strani (razsodnika), da je bila informacija poslana s strani pošiljatelja, saj je zmožnost preverjanja podpisa tesno povezana z zmožnostjo izdelave podpisa.

Asimetrični šifrirni postopki

V nasprotju s simetričnimi postopki je slednja zvrst šifriranja relativno nova. Začetnika sta bila leta 1976 Diffie in Hellman, ki sta v svojem članku predvidela razvoj popolnoma nove vrste kriptografije [15]. Leta 1977 so Rivest, Shamir in Adelman iznašli RSA, prvi asimetrični šifrirni postopek [54]. Med tem časom so se pojavili tudi drugi. Za nas najbolj zanimiv je asimetrični šifrirni postopek na osnovi eliptičnih krivulj (Jurišič [32], Certicom [11], [12]). Najpogostejši primeri uporabe asimetričnih šifrirnih postopkov so protokoli za prepoznavanje, izmenjavo skrivnega ključa in izdelavo digitalnega podpisa.

Vsak asimetrični šifrirni postopek ima svoje tehnične značilnosti, skupno vsem pa je, da imamo par povezanih ključev; šifrirnega (E) in dešifrirnega (D). Povezava med ključema je matematična in s poznavanjem E je zelo težko (ali računsko neizvedljivo) določiti ključ D. To omogoča entiteti, da javno objavi svoj javni ključ E. Vsak lahko uporabi ključ za šifriranje sporočil, namenjenih entiteti. Samo imetnik zasebnega ključa lahko izlušči čistopis sporočila.

Asimetrični šifrirni postopek je *obrnljiv*, če ga lahko uporabljamo za šifriranje in za digitalno podpisovanje (na primer RSA). Pri neobrnljivih asimetričnih postopkih lahko z zasebnim ključem samo šifriramo, ne pa tudi dešifriramo sporočila. Uporabni so le za tvorbo digitalnega podpisa (Stallings, [60]). Ločimo še tretjo vrsto, kjer ne moremo niti šifrirati niti digitalno podpisovati, in jih uporabljamo za izmenjavo ključev. Primer je Diffie-Hellmanov postopek za izmenjavo ključev (Stallings [60]).

Primerjava asimetričnih in simetričnih šifrirnih postopkov:

- Osnovna prednost asimetričnih postopkov je preprostost uporabe in večja varnost, saj zasebnega ključa ni potrebno pošiljati ali deliti s komerkoli. Skrivni ključ si morata partnerja na varen način izmenjati oziroma se zanj dogovoriti. Slabost asimetrične kriptografije je občutljivost za napad s pretvarjanjem, četudi napadalcu zasebni ključ ni znan.

- Asimetrični šifrirni sistemi zagotavljajo digitalni podpis, ki ga ni mogoče zanikati. Prepoznavanje partnerja z uporabo simetrične kriptografije zahteva delitev skupne skrivnosti ali udeležbo zaupanja vredne tretje strani. Pošiljatelj lahko zaradi razkritja skupne skrivnosti oporeka že poslanemu sporočilu. Pri asimetrični kriptografiji je vsak partner sam odgovoren za varovanje zasebnega ključa.

- Kot smo že omenili, so hitrosti šifriranja simetričnih šifrirnih postopkov bistveno večje od asimetričnih. Izkazalo se je, da so asimetrični šifrirni postopki inherentno počasnejši od simetričnih, saj je na primer RSA v povprečju 1000 krat počasnejši od DES šifrirnega sistema (Certicom [11], RSA [57]). Zato se je uveljavil način, da sporočilo šifriramo s simetričnim postopkom, skrivni ključ pa z asimetričnim. Ker je skrivni ključ običajno mnogo krajši kot sporočilo, je postopek precej hitrejši če uporabljamo oba sistema. Tako se običajno uporabljata obe vrsti šifriranja. Asimetrični šifrirni postopki ne zamenjujejo simetričnih, marveč jih za dosego večje varnosti, enostavnosti uporabe in hitrosti šifriranja, le nadgrajujejo.

- V okoljih, kjer lahko brez večjih težav izvajamo varno razdeljevanje skrivnega ključa, ali v enouporabniškem okolju, je asimetrična kriptografija običajno odveč.

Šifrirni sistem RSA

RSA asimetrični šifrirni postopek nudi tako možnost šifriranja kot digitalnega podpisovanja. Varnost postopka temelji na težavnosti faktorizacije velikih števil. Hitrost šifriranja in dešifiranja je pogojena z učinkovitostjo izvedbe modularnega potenciranja.

Z izboljševanjem postopkov za faktorizacijo se bo za enako stopnjo varnosti morala dolžina ključa povečevati. Napredek pri povečevanju hitrosti faktorizacije s pomočjo strojne opreme bolj kot napadalcu pomaga uporabniku šifrirnega postopka, saj lahko učinkoviteje generira in uporablja daljše ključe. V prihodnosti se bo pojavil problem, saj bo z napredkom hitrosti računalnikov in postopkov za faktorizacijo možno napadati šifrirne ključe (digitalne podpise), ki so bili generirani v preteklosti.

Šifrirni sistemi na osnovi eliptičnih krivulj

Kot vsi asimetrični šifrirni postopki tudi slednji temelji na težavnosti reševanja matematičnega problema in sicer diskretnega logaritma nad eliptičnimi krivuljami. Trenutno je reševanje diskretnega logaritma nad eliptičnimi krivuljami manj

učinkovito kot reševanje problema nad celimi števili. To omogoča, da enako stopnjo varnosti zagotavljamo s krajšimi ključi v primerjavi z drugimi asimetričnimi šifrirnimi postopki. Izvedba asimetričnega šifrirnega sistema z eliptičnimi krivuljami omogoča manjšo porabo pomnilnika in večjo hitrost šifriranja. Učinkovitost izvedbe temelji na hitrosti izvedbe množenja števila in točke na eliptični krivulji. Ker je lahko modul pri eliptičnih krivuljah krajši kot v primeru RSA, nam to nudi dodatne možnosti za pohitritev postopka.

Eliptične krivulje so v zadnjih letih doživele razmah. Posebno so primerne za področja, kjer se soočamo z omejitvami v količini pomnilnika, hitrosti prenosa podatkov ali procesorski moči (npr. pametne kartice). Za te vrste sistemov je pričakovati, da se bo uporaba z leti povečevala.

Primerjava eliptičnih krivulj in RSA asimetričnih kriptografskih sistemov.

Velika večina produktov in standardov, ki uporabljajo asimetrično kriptografijo za šifriranje in digitalno podpisovanje, temelji na RSA. Z izboljševanjem postopkov za faktorizacijo celih števil in naraščanjem procesorske moči se bo dolžina ključev povečevala. To bo povzročilo večjo obremenitev sistemov. Strežniki, ki izvajajo veliko število varovanih/šifriranih transakcij (na primer elektronsko poslovanje), bodo še posebej čutili dodatno breme.

- Prednost eliptičnih krivulj je, da pri krajših ključih nudijo enako stopnjo varnosti. Šifrirni sistem, temelječ na eliptičnih krivuljah, lahko pri dolžni ključev 160 bitov nudi enako stopnjo varnosti kot RSA sistem z 1024 bitno dolžino. Iz tabele razberemo, da se bo dolžina ključev hitreje povečevala pri sistemih, temelječih na RSA. Manjši ključi omogočajo krajše certifikate, hitrejše izvajanje operacij ter uporabo manj zmogljivih procesorjev.

MIPS let potrebno za razbitje sistema	RSA dolžina ključa (v bitih)	ECC dolžina ključa (v bitih)	razmerje dolžin
10^{4}	512	106	5 : 1
10^{8}	768	132	6 : 1
10^{11}	1,024	160	7 : 1
10^{20}	2,048	210	10 : 1
10^{78}	21,000	600	35 : 1

Tabela 3.1: primerjava asimetričnih šifrirnih sistemov (Certicom [12]).

- Pri določanju hitrosti šifriranja je zaradi različnih načinov optimizacije težje podati kvantitativno oceno. Velja, da so sistemi, temelječi na eliptičnih krivuljah, v primerjavi s tistimi, ki temeljijo na RSA, hitrejši pri podpisovanju in dešifriranju, a počasnejši pri preverjanju digitalnih podpisov in šifriranju.

- V primeru, ko je potrebno upoštevati še majhne hitrosti prenosa, na primer pri pametnih karticah, je pomembna tudi dolžina digitalnega podpisa. Ponovno se izkaže, da je digitalni podpis z eliptičnimi krivuljami približno trikrat krajši v primerjavi z RSA podpisom pri isti dolžini zasebnega ključa (Certicom [12]). Prednost RSA šifrirnega sistema pred eliptičnimi krivuljami je, da poleg ključa ne potrebuje dodatnih parametrov. A še tu je skupna dolžina podatkov le četrtina podatkov, potrebnih za RSA postopek.

3. DIGITALNI PODPIS

Digitalni podpis je gotovo najpomembnejša pridobitev razvoja asimetrične kriptografije. Predstavlja elektronsko ekvivalentnco prostoročnemu podpisu. *Digitalni podpis* je kriptografski povzetek sporočila, šifriran z zasebnim ključem podpisnika. Je dodatek k sporočilu, lahko tudi nešifriranemu, v primeru, ko si partnerja ne zaupata popolnoma. Zagotavlja neokrnjenost sporočila med prenosom, priča o izvoru sporočila (pošiljatelju) in preprečuje tajenje. Vendar je potrebno digitalni podpis razširiti še z dodatnimi podatki, da bo učinkovito opravljal svojo funkcijo. Več o dodatnih podatkih bomo spregovorili v poglavju o preverjanju digitalnega podpisa.

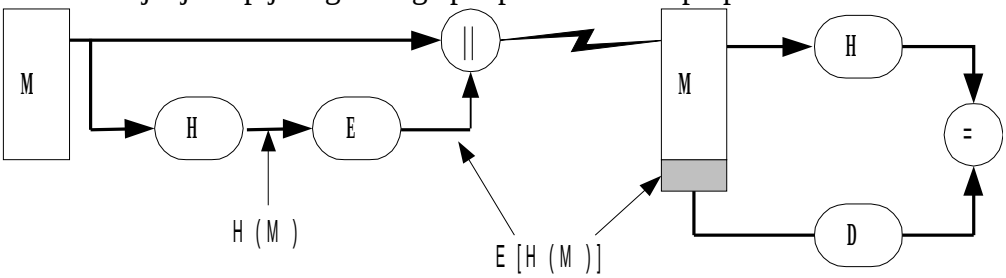
Osnovne lastnosti digitalnega podpisa, so:

- Vsebovati mora informacijo, ki je edinstvena in povezljiva s podpisnikom. Le podpisnik lahko zgradi svoj digitalni podpis, ki priča tudi o času nastanka.

- Digitalni podpis mora biti odvisen od sporočila, ki ga podpisuje. Podpisanega sporočila ni mogoče spremeniti in hkrati ohraniti isti digitalni podpis.

- Digitalnega podpisa na sporočilu se ne da zanikati. Na podlagi podpisa, ki je priložen sporočilu, ima prejemnik sporočila možnost, da tretjo stran (razsodnika) prepriča o identiteti pošiljatelja in neokrnjenosti sporočila.

- Hranjenje kopije digitalnega podpisa mora biti preprosto.



Običajno se digitalni podpis izvede s pomočjo zgoščevalnih funkcij in asimetričnega šifriranja. *Zgoščevalna funkcija* kot vhodni podatek sprejme sporočilo poljubne dolžine in vrne povzetek sporočila fiksne dolžine (Stallings [60]). Slabost vseh uporabljenih postopkov za tvorbo digitalnega podpisa je, da sta varnost in verodostojnost podpisa odvisni od varnosti zasebnega ključa pošiljatelja.

Ločimo *neposredne digitalne podpise*, kjer mora prejemnik poznati le javni ključ pošiljatelja (certifikat), in *digitalni podpis z razsodnikom* (Stallings [60]). Pri slednjem je rešen problem, ki obremenjuje neposredni digitalni podpis, a vključuje razsodnika v celoten proces podpisovanja sporočila. Obe strani morata seveda zaupati izbranemu razsodniku.

Upravljanje s ključi

Upravljanje s ključi je najtežji del kriptografije. Varnost vseh postopkov sloni na primernem hranjenju ključev in preprečevanju razkritja ali izgube ključev. Ločimo dve vrst ključev: *kratkožive* in dolgožive. Kratkoživi se običajno generirajo avtomatično. Uporabljajo se za varovanje seje in se potem zavržejo (uničijo). *Dolgožive* ključe generira izključno uporabnik (lastnik). Uporablja jih za prepoznavanje (pri kontroli dostopa, ohranjanju neokrnjenosti sporočil in preprečevanju tajenja) ter zagotavljanje zaupnosti (pri sporazumevanju in izmenjavi sejnih ključev, varovanju shranjenih podatkov).

Javni ključi, ki jih uporabljamo za prepoznavanje, imajo lahko zelo dolgo življenjsko dobo (tudi nekaj let). Njihovi zasebni pari in simetrični skrivni ključi imajo običajno mnogo krajšo življenjsko dobo (leto ali dve). Za ključe, ki jih uporabljamo za zagotavljane tajnosti podatkov, je dobro, da imajo kar se da kratko življenjsko dobo.

V primeru razkritja skrivnega/zasebnega ključa je potrebno ključ preklicati. Če se je ključ uporabljal za prepoznavanje, so vsa podpisana sporočila, ki niso bila opremljena s časovno znamko, neveljavna. V primeru, da smo ključ uporabljali za varovanje tajnosti podatkov, lahko vse podatke štejemo za razkrite. Poseben problem se pojavi v primeru asimetrične kriptografije in digitalnih certifikatov javnega ključa, saj so certifikati porazdeljeni po omrežju, kar preklic para ključev močno oteži.

Pri nekaterih asimetričnih šifrirnih postopkih tako javni kot zasebni ključ omogočata šifriranje podatkov. Par ključev se lahko uporablja za šifriranje in za digitalno podpisovanje. V praksi se to izkaže za dvorezni meč. Nikoli ne smemo narediti rezervne kopije zasebnega ključa, ki ga uporabljamo za digitalno podpisovanje. Ob koncu življenjske dobe je potrebno zasebni ključ za podpisovanje uničiti. Če pride do razkritja ključa (celo dolgo časa po preteku veljavnosti), lahko napadalec ponareja digitalni podpis na dozdevno starih dokumentih.

Ključi (certifikati) pretečejo po določenem času. Redno obnavljanje ključev omogoča ohranjanje želene stopnje varnosti. Pri obnavljanju ključev je potrebno upoštevati napredek v kriptoanalizi in ustrezno povečevati dolžino ključev. Potrebno je poudariti, da s tem ne preprečimo napade na podatke, ki smo jih šifrirali s krajšimi ključi. Pomembno je, da dolžino ključev določamo glede na življenjsko dobo podatkov in ne glede na trenutno še varno spodnjo mejo za dolžino ključev.

Pare ključev, ki jih uporabljamo za šifriranje, je dobro hraniti kar se da dolgo. Z izgubo zasebnega ključa nam je onemogočen dostop do podatkov, ki so bili šifrirani z javnim ključem. Iz tega je razvidno, da je modro imeti par ključev za šifriranje in par ključev za digitalno podpisovanje sporočil.

Kdo hrani javne ključe in certifikate, ko niso več veljavni, in kako je določena dolžina ključa, so v večini odprta vprašanja, povezana z digitalnim podpisom in organizacijo infrastrukture javnega ključa.

4. PREVERJANJE DIGITALNEGA PODPISA

Preverjanje digitalnega podpisa je ena izmed osnovnih nalog, ki jih omogoča infrastruktura javnega ključa. Digitalni podpis lahko uporabimo za prepoznavanje entitete, s katero komuniciramo, preverjanje neokrnjenosti in izvora podatkov, ali za preprečevanje tajenja. Preverjanje digitalnega podpisa lahko razdelimo glede na čas, ki je pretekel od njegovega nastanka.

Podrobneje si bomo ogledali uporabo digitalnega podpisa za preprečevanje tajenja (Nilson, Pinkas [46]). Glede na čas, ko podpis preverjamo, ločimo tri obdobja: kratkoročno preverjanje podpisa, dolgoročno preverjanje in preprečevanje tajenja, ter arhiviranje digitalno podpisanih dokumentov.

Kratkoročno preverjanje digitalnega podpisa

Preverjanje digitalnega podpisa izvedemo kmalu po njegovem nastanku, ko so certifikati javnega ključa in seznami preklicanih certifikatov še veljavni in na voljo. Uporabnik certifikata mora dobiti vse podatke, ki jih bo potreboval za dolgoročno preverjanje podpisa in preprečevanje tajenja. Če podatkov ne priskrbi podpisnik, jih mora pred preverjanjem pridobiti sam. Kdo priskrbi podatke, je stvar dogovora in okoliščin, v katerih poteka preverjanje.

Identifikacija podpisnikovega certifikata

Certifikatna agencija mora nuditi vse podatke, potrebne za preverjanje digitalnih podpisov, ustvarjenih z javnimi ključi, ki jih je overila. To vključuje podatke o vseh veljavnih in preklicanih certifikatih.

Entiteta ima običajno možnost pridobiti več različnih certifikatov za isti javni ključ. Pridobi jih lahko pri isti ali pri različnih certifikatnih agencijah. Prednost več certifikatov je možnost uporabe enega samega zasebnega ključa za vse javne ključe, kar je ugodno, če za hranjenje zasebnega ključa uporabljamo pametne kartice. V primeru več agencij lahko vsak certifikat vsebuje različno identiteto. Če so certifikati izdani pri eni sami agenciji, lahko certifikati vsebujejo še dodatne atribute (namen uporabe ključa, pravice imetnika…). Ključno za uporabnika je, določiti certifikat, ki je bil uporabljen za izdelavo digitalnega podpisa. Za nedvoumno identifikacijo morata biti serijska številka certifikata in izdajatelj vsebovana kot del podpisanega sporočila.

Mnogo shem za digitalno podpisovanje le doda uporabljeni certifikat, kar je občutljivo za napade, kjer napadalec zamenja certifikat. Dodatna prednost vključitve serijske številke certifikata in izdajatelja je varovanje pred zlonamernimi certifikatnimi agencijami. Slednje izdajajo certifikate entitetam, ki uporabljajo javne ključe drugih entitet. Če je certifikat le priložen in ni zavarovan z digitalnim podpisom, lahko napadalec ustvari vtis, da je sporočilo podpisal nekdo drug.

Alternativna rešitev problema je, da agencija pred izdajo certifikata preveri, ali entiteta poseduje par ključev. Na žalost pa ne nudi jamstva ob preverjanju digitalnega podpisa. Izdajatelj mora voditi dnevnik preverjanja posedovanja para ključev, ga arhivirati in dati na voljo v primeru potrebe.

Razmišljanje velja tudi za primer, ko je certifikat preklican, oziroma je prišlo do razkritja zasebnega ključa agencije, ki je podpisniku certifikat izdala. Podpisnik bi oporekal svojemu podpisu na podlagi sledečega scenarija:

> *Prejemnik sporočila je vnaprej pripravil in podpisal sporočilo s svojim zasebnim ključem ter ga opremil z časovno znamko v upanju, da bo prišlo do razkritja zasebnega ključa agencije.*
>
> *Ko se je to zgodilo, je prejemnik sporočila z uporabo razkritega zasebnega ključa agencije ponaredil certifikat v imenu podpisnika s parom ključev prejemnika.*

Prejemnik oporeka takemu toku dogodkov in predloži certifikat podpisnika, ki je naveden v podpisanem sporočilu, ter s tem dokaže, da je certifikat v danem trenutku obstajal in je bil ob nastanku podpisa veljaven.

Politika certificiranja

Prejemnik digitalno podpisanega sporočila lahko iz certifikata podpisnika izve za naziv entitete. Za preverjanje veljavnosti podpisnikovega certifikata mora na varen način pridobiti samopodpisani certifikat agencije, ki je par ključev overila. Običajno imajo agencije več certifikatov glede na različne imenske domene in politike certificiranja, ki jih uporabljajo. Nedvoumno je potrebno ugotoviti, katera politika je bila uporabljena, njen identifikator mora biti del podpisanega sporočila. Prav tako mora biti v politiki certificiranja navedena serijska številka samopodpisanega certifikata, ki se uporablja za podpisovanje uporabniških certifikatov.

Časovne znamke

Pri preprečevanju tajenja je pomembno zagotoviti, da digitalni podpis, ki je bil preverjen, ostane tak tudi vnaprej. Za preverjanje digitalnega podpisa mora uporabnik pridobiti javni ključ podpisnika ter preveriti njegovo pristnost in veljavnost ob času podpisa. V primeru, da je bil certifikat veljaven v času preverjanja digitalnega podpisa, a je bil kasneje preklican, mora uporabnik certifikata hraniti dokaz o veljavnosti javnega ključa ob podpisu sporočila.

Uporaba *časovnih znamk* lahko priskrbi tovrstne dokaze. Časovno znamko tvori *časovni strežnik točne ure*, ki ob predložitvi kriptografskega povzetka sporočila vrne odgovor. Slednji vsebuje digitalno podpisan kriptografski povzetek sporočila, identiteto strežnika in točen čas. To dokazuje, da so podatki obstajali pred zapisanim časom. Če kriptografski povzetek digitalnega podpisa pošljemo strežniku in ga le-ta opremi s časovno znamko pred preklicem certifikata podpisnika, je to dokaz o veljavnosti digitalnega podpisa ob času preverjanja.

Če hoče prejemnik ohraniti preverjen in veljaven digitalni podpis kot način za preprečevanje tajenja, mora čim prej pridobiti časovno znamko. To mora storiti še

preden pride do razveljavitve podpisnikovega ključa ali kateregakoli izmed verige ključev, ki so bili uporabljeni za preverjanje podpisa. S časovno znamko ga lahko opremi podpisnik ali prejemnik podpisa. V primeru, ko prejemnik sporočila ne opremi digitalnega podpisa s časovno znamko, lahko podpisnik uspešno oporeka po sledečem scenariju:

> *Podpisnik prekliče certifikat, kakor hitro se premisli. Certifikat se vnese v seznam preklicanih certifikatov. Nato trdi, da je nekdo drug sestavil sporočilo in ga digitalno podpisal potem, ko je bil certifikat že preklican. Prejemnik sporočila ni preveril najnovejšega seznama preklicanih certifikatov. Prejemnika lahko obtoži, da se je dokopal njegovega zasebnega ključa in ponaredil digitalni podpis.*

Časovna znamka mora zajemati sporočilo in digitalni podpis, sicer je odprta pot za napad:

> *Napadalec izbere žrtev in zgradi sporočilo, ki se nanaša nanjo. Sporočilo opremi s časovno znamko. Ko se čez nekaj časa dokoplje do zasebnega ključa žrtve, sporočilo podpiše. Podpisano sporočilo je videti, kot bi nastalo še pred razkritjem zasebnega ključa žrtve.*

Čas nastanka digitalnega podpisa

Časovne znamke, kot so bile uporabljene zgoraj, služijo le kot dokaz prejemnika, da je digitalni podpis nastal pred preklicem ali zapadlostjo podpisnikovega certifikata. Ničesar ne povedo o času nastanka digitalnega podpisa. Za določene namene je pomemben čas, ko podpisnik digitalno podpiše sporočilo.

Podpisnik v digitalni podpis vključi čas T_1 kot čas nastanka podpisa. Prejemnik digitalnega podpisa naj v njegovo dobro ponovno podpiše vse podatke z vključitvijo časa T_2 (čas prejetja podpisa) čim prej je mogoče. Obe časovni znamki zagotovi strežnik točne ure. Če je strežnik vreden zaupanja, lahko z gotovostjo trdimo, da je bil podpis kreiran po T_1 in pred T_2.

Uporabnik mora v primeru tajenja s strani podpisnika imeti sledeče dokaze:

- opis politike certificiranja,
- podpisano sporočilo, ki vključuje čas podpisa, serijsko številko certifikata podpisnika, identifikacijo politike certificiranja,
- certifikat javnega ključa podpisnika,
- časovno znamko za celotno sporočilo, ki jo izda zaupanja vreden strežnik točne ure,
- seznam preklicanih certifikatov ali odgovor na poizvedbo o statusu certifikata,

- veljavno verigo certifikatov ob času podpisa, ki se začne z certifikatom agencije, ki ji zaupa, vsebuje certifikat izdajatelja, navedenega v politiki certificiranja, in se končuje s certifikatom uporabnika.

Vse podatke mora uporabnik certifikata zbrati in shraniti ob prejetju in preverjanju podpisa. Vse to ne zadostuje v primeru, če pride do razkritja ključev, ki se nahajajo v verigi certifikatov.

Dolgoročno preverjanje digitalnega podpisa

Preverjanje izvajamo po preteku veljavnosti certifikata, ki je overjal javni ključ podpisnika sporočila. Hkrati je lahko prišlo do spremembe in sicer:

- Spremenjen je bil ključ, ki je bil uporabljen za preverjanje digitalnega podpisa certifikata podpisnika.
- Zapadel je certifikat korenske certifikatne agencije.
- Spremenjeni so bili ključi iz križnih certifikatov, ki so bili uporabljeni za preverjanje podpisa.

Za izvedbo preverjanja moramo uporabiti verigo certifikatov, ki je obstajala ob času nastanka podpisa. Vsi zbrani podatki o certifikatih v verigi (križni certifikati, seznami preklicanih certifikatov, odgovori na poizvedbo o statusu certifikatov) morajo biti opremljeni s časovno znamko. Vsak podatek lahko posebej opremimo s časovno znamko, saj je tako uporaben za preverjanje več digitalnih podpisov.

Tako bo podpisano sporočilo veljavno dlje časa in zaščiteno pred težavami, ki bi nastale z razkritjem katerega izmed ključev v verigi certifikatov.

Hranjenje digitalnega podpisa v arhivske namene

Shranjevanje dokumentov v arhivske namene se lahko zavleče še daleč v čas, ko kriptografski postopki, ki so bili uporabljeni za tvorbo digitalnega podpisa, niso več varni. Razvoj kriptoanalize in večanje računske moči lahko privede do izračunavanja zasebnega ključa s poznavanjem javnega ključa.

V primeru razbitja šifrirnega sistema lahko z nizom časovnih znamk izvedemo zaščito pred ponarejanjem. Časovno znamko je potrebno dodati dokazu, še preden pride do razkritja zasebnega ključa ali razbitja postopka digitalnega podpisa. Časovni strežnik mora uporabljati čim daljše ključe. Z obvezno uporabo časovnih znamk zaščitimo dokaze tako pred razkritjem zasebnega ključa kot pred razbitjem postopka digitalnega podpisa. Lepljenje znamk izvede podpisnik ob tvorbi podpisa oziroma uporabnik ob zbiranju podatkov in preverjanju podpisa. Ni potrebno, da je ključ podpisnika dolg, saj mora varovati pred razbitjem postopka le za čas veljavnosti certifikata.

V primeru napada s kolizijo zgoščevalne funkcije je potrebno celoten podpisan dokument, seznam preklicanih certifikatov in odgovor na poizvedbo o statusu certifikata opremiti s časovno znamko z uporabo zgoščevalne funkcije, ki je bolj robustna pred razbitjem kakor funkcija, uporabljena za tvorbo digitalnega podpisa.

Sklenemo lahko, da je nemogoče ponarediti digitalni podpis, če je bil ob podpisu dokumenta le-ta opremljen s časovno znamko, ki jo je izdal zaupanja vreden časovni strežnik, in je bil podpis veljaven, ter smo preverili veljavnost digitalnih certifikatov. Če je prejemnik podpisal arhivirane dokumente brez uporabe časovnega strežnika, lahko dokumente uporablja le za namene prepoznavanja, ne pa tudi kot dokaz za preprečevanje tajenja.

5. NEKONSISTENTNI CERTIFIKATI

Naravno je pričakovati, da se bo pri podpisovanju sporočil uveljavilo več postopkov za digitalni podpis. Različne skupine se bodo odločale za različne postopke. Relativno preprosto je izvajati preverjanje digitalnih podpisov, ki temeljijo na različnih postopkih. Bistveno zahtevnejše je digitalno podpisovati sporočila z različnimi postopki, saj to veleva zahtevno upravljanje z več zasebnimi ključi in certifikati. Imetniki certifikatov si zagotovo želijo upravljanja s čim manj ključi in podpisovanje z enim samim postopkom. Javni ključ in digitalni podpis certifikata uporabljata pri *konsistentnem certifikatu* isti šifrirni postopek. Entiteti, ki posedujeta enakovrstna konsistentna certifikata običajno ne potrebujeta poznavanja drugih postopkov za preverjanje veljavnosti digitalnega podpisa oziroma certifikata.

Splošno uporabna in učinkovita infrastruktura javnega ključa mora podpirati več postopkov za digitalni podpis, a le eno samo zgoščevalno funkcijo. Veriga certifikatov lahko vsebuje *nekonsistentne* certifikate, prav tako je lahko seznam preklicanih certifikatov (odgovor na poizvedbo o statusu certifikata) podpisan z drugim postopkom, kot so podpisani certifikati.

Nekateri postopki za digitalni podpis zahtevajo še dodatne parametre. Le-ti so lahko enaki za vse certifikate, ki jih izdaja agencija oziroma za celotno infrastrukturo javnega ključa. Edino varno mesto za hranjenje parametrov je v certifikatu javnega ključa. Ker so parametri običajno velika števila (velikostnega reda ključa), je zaželeno, da so skupni vsaj določeni skupini certifikatov. S tem omejimo velikost certifikatov. Burr in Polk [10] predstavljata priporočila za dedovanje parametrov. Povzamemo jih lahko v sledečih točkah:

- Parametre moramo pridobiti iz istega varnega in preverjenega vira kot javni ključ podpisnika.
- Če parametri niso vsebovani v certifikatu, se njihove vrednosti privzamejo iz nadrejenega certifikata v verigi certifikatov.
- Dedovanje parametrov ne velja za nekonsistentne certifikate, slednji morajo vsebovati vrednosti parametrov.

Postavlja se vprašanje, ali sploh potrebujemo nekonsistentne certifikate. Če jih ne, je edina rešitev postavitev več neodvisnih infrastruktur javnega ključa, kjer vsaka skrbi za svoj asimetrični šifrirni postopek. Uporabnik mora za vsak postopek imeti svoj certifikat ter odjemalca, ki je sposoben preverjati in podpisovati z izbranim postopkom. Vprašanje je, kateri postopek uporabiti za tvorbo digitalnega podpisa v primeru, ko partner nima posebnih preferenc? Ali naj sporočila podpisuje z vsemi postopki, ki so na voljo? Poleg tega bi bile potrebne vzporedne certifikatne poti. Zaradi vsega naštetega bi se stroški upravljanja bistveno povečali tako za infrastrukturo javnega ključa kot za uporabnike.

Za uporabo nekonsistentnih certifikatov je pametno vse breme izvedbe preložiti na končne uporabnike. Za dosego združljivosti mora uporabnik znati preverjati digitalne podpise po vseh podprtih postopkih. Ker uporabnik običajno potrebuje le en postopek za digitalni podpis, mora skrbno varovati samo en zasebni ključ.

S prenosom bremena na uporabnika in uporabo nekonsistentnih certifikatov se postavlja vprašanje, kam umestiti nekonsistentne certifikate za zagotavljanje združljivosti. Ponujajo se naslednje možne rešitve:

1. Certifikatna agencija podpisuje le z enim postopkom za digitalno podpisovanje, a izdaja certifikate javnega ključa tudi za druge postopke (nekonsistentni certifikati za končne uporabnike). To lahko omogoči učinkovitejšo uporabo certifikatov. Agencija podpisuje certifikate z digitalnim podpisom, ki ga je zamudno generirati, a enostavno preveriti. Asimetrični šifrirni postopek entitete omogoča hitro podpisovanje, a zahteva večje procesorske zmogljivosti za preverjanje. Za končnega uporabnika je celoten proces uporabe certifikata enostavnejši in hitrejši. Ker certifikat podpišemo le enkrat, preverjamo pa ga mnogokrat, je taka rešitev smiselna. Slednje je zelo koristno za naprave, ki ne premorejo velikih procesorskih zmogljivosti (na primer pametne kartice).

   Taka nedoslednost ni praktična. Vsako preverjanje digitalnega podpisa zahteva od entitete zmožnost preverjati digitalne podpise po obeh postopkih in pripravljenost oba postopka tudi sprejeti. Varnost uporabe certifikatov je enaka varnosti šibkejšega postopka. Entiteti, ki uporabljata enak postopek digitalnega podpisa, morata poznati oba postopka, čeprav je certifikat za isti šifrirni postopek obema izdala ista agencija. Dodaten argument proti tej rešitvi so parametri za digitalni podpis, ki morajo biti eksplicitno vsebovani v certifikatu entitete. Rešitev je uporabna le za okolja, kjer smo omejeni s procesorskimi zmogljivostnimi končnih uporabnikov. Še vedno obstaja problem s pomnilniškimi in komunikacijskimi zmogljivostmi, saj je potrebno prenašati tudi parametre.

2. Agencija izdaja konsistentne certifikate za več postopkov. S tem se izognemo nekonsistentnim certifikatnim verigam. Agencija navzkrižno certificira vse svoje podpisne ključe z nekonsistentnimi certifikati. S tem zagotovi obstoj poti med entitetami, ki uporabljajo različne postopke za podpisovanje. Certifikatna agencija izdaja entitetam konsistentne certifikate in jim priporoča, da so sposobne preverjati digitalne podpise na podlagi vseh postopkov, ki jih agencija podpira.

Pojavi se problem, kateri algoritem uporabiti za podpisovanje seznama preklicanih certifikatov. Verjetno bi bilo potrebno razdeljevati verzije, podpisane z vsemi podprtimi postopki.

3. Certifikatna agencija vedno podpisuje z enim postopkom in izdaja konsistentne certifikate končnim uporabnikom. Lahko izdaja tudi nekonsistentne certifikate drugim agencijam za zagotavljanje združljivosti. V primeru, ko je potrebno entiteti izdati certifikat za drug algoritem digitalnega podpisa, to opravi ustrezna agencija. Agencija je lahko ena sama, le da je logično razdeljena na več agencij, kjer vsaka skrbi za določen šifrirni postopek (ločujemo jih po imenih). Seznam preklicanih certifikatov se izdaja za vsak postopek posebej.

Izvedba ločenih infrastruktur javnega ključa s konsistentnimi certifikati je nepraktična, saj je predraga za vzdrževanje in zahteva upravljanje več certifikatov ter odločitev, kateri ključ uporabiti za podpisovanje dokumentov. Nekonsistentni certifikati entitet so uporabni le za specifična okolja. Če agencija podpisuje z več postopki digitalnega podpisa, zaplete mehanizem za ugotavljanje statusa certifikatov. Rešitev z logično ločenimi agencijami je najbolj primeren za splošno namenske infrastrukture. Glede na vse povedano, lahko sklenemo:

- Certifikati entitet naj bodo konsistentni.
- Agencija naj podpisuje certifikate le z enim postopkom za digitalno podpisovanje.
- Če se pojavi potreba po več postopkih za digitalno podpisovanje, uporabimo več različnih agencij (z različnimi imeni) za izdajanje certifikatov. To omogoča, da so seznami preklicanih certifikatov podpisani le z enim postopkom.
- Kjer z več agencijami upravlja le ena entiteta, naj jih poveže z nekonsistentnimi križnimi certifikati.
- Vsi samopodpisani certifikati agencij naj vključujejo parametre, potrebne za izvedbo digitalnega podpisa.
- Ostali certifikati naj vsebujejo parametre le, če so nekonsistentni, oziroma uporabljajo parametre, ki so različni od parametrov agencije, ki je certifikat izdala.

IV. HRANJENJE DIGITALNIH CERTIFIKATOV JAVNEGA KLJUČA

V pričujočem poglavju si bomo pogledali prednosti uporabe namenskih naprav za hranjenje zaupnih podatkov, namreč zasebnega ključa in certifikata javnega ključa. Predstavili bomo prednosti uporabe v infrastrukturah javnega ključa za preprečevanje razkritja zaupnih podatkov kot vir točne ure, hranjenje certifikatov korenskih certifikatnih agencij in poenostavitev mehanizmov infrastrukture (še posebej mehanizma za ugotavljanje statusa certifikata).

Običajno se zasebni ključ in certifikat javnega ključa hranita v osebnem računalniku oziroma napravi, kjer je zaščita dostopa izvedena programsko. Prednosti so predvsem hitra in poceni izdelava programske opreme, ki omogoča upravljanje s ključem oziroma certifikatom, enostavnost razpošiljanja programske opreme preko omrežja (ni potrebe po fizičnem transportu). Prav tako je prednost, da vsak posameznik lahko izdaja digitalne certifikate in da je pravilnost delovanja programske opreme relativno enostavno preveriti.

Ne glede na vse naštete prednosti so v infrastrukturi javnega ključa programske izvedbe sistema za upravljanje in varovanje zasebnega ključa z vidika varnosti nezaželene. Osnovni problem (grožnja) je kraja zasebnega ključa in zamenjava certifikata korenske agencije, ki ji entiteta zaupa. Če je generiranje in hranjenje zasebnega ključa izvedeno na osebnem računalniku, je praktično nemogoče preprečiti razkritje, izgubo, spreminjanje ali nedovoljeno uporabo le-tega. Shamir in Someren [62] prikažeta način, kako lahko s pomočjo programa, ki ga poženemo na pomnilniškem mediju, odkrivamo šifrirne ključe. Postopek temelji na iskanju podatkov, ki izkazujejo neobičajno visoko stopnjo entropije. Četudi ključe ščitimo s šifriranjem in uporabo gesla, lahko zaščito še vedno napademo s pomočjo grobe sile, preizkusimo vsa verjetna (možna) gesla. Če hočemo ključ uporabljati za šifriranje, moramo v določenem trenutku imeti šifrirni ključ shranjen v čistopisu v delovnem pomnilniku, kjer je edina zaščita izvedena na ravni operacijskega sistema.

Prav tako v mnogih izvedbah infrastrukture javnega ključa imetnikom certifikata le-tega ni dovoljeno posojati, kopirati ali imeti v souporabi z drugimi entitetami. Primeri *osebnih certifikatov* so certifikati, ki predstavljajo naročniško izkaznico, izkaz zaposlitve v podjetju, diplomo. Vsem je skupno, da je potrebno izdajatelju certifikata za izdajo in uporabo plačevati uporabnino ali pa posedovanje certifikata prinaša določene ugodnosti. Čeprav lahko v certifikat vključimo podatke, ki nam pomagajo določiti izvor - domicil certifikata (na primer IP številko) oziroma informacijo, ki omogoča sledenje, sta rešitvi neuporabni tako z vidika zagotavljanja varnosti kot z vidika ohranjanja zasebnosti uporabnikov certifikata. Posojanje certifikatov je v literaturi malo obravnavan problem in rešitve za preprečevanje le-tega še niso na voljo (Brands [9]).

Pripraven način za izogibanje zgoraj naštetih problemov je hranjenje zasebnega ključa na pametni kartici.

1. PAMETNE KARTICE

Pametna kartica je plastična kartica, ki vsebuje procesor in pomnilno enoto (Petri [49]). Nekatere poleg teh osnovnih komponent vsebujejo še čitalec prstnih odtisov, zaslon, tipkovnico in celo brezkontaktni komunikacijski vmesnik. Pametna kartica je majhen računalnik s svojim operacijskim sistemom, programi in podatki. Glede na zmogljivost procesorja in količino pomnilnika ločimo pomnilniške (sinhrone) in procesorske (asinhrone) kartice. Prve so relativno preproste in vsebujejo le pomnilnik in vezja za kontrolno dostopa (na primer telefonske kartice). Pomnilniške kartice premorejo samo osnovne zaščitne mehanizme (preprečevanje ponovnega polnjenja števila impulzov...).

Procesorske kartice nudijo mnoge dodatne funkcije in izpopolnjene načine zaščite vsebine. Pomnilne zmogljivosti procesorske kartice so mnogo večje. Tipična procesorska kartica vsebuje od 128 do 1024 zlogov delovnega pomnilnika (RAM), od 1 do 16 tisoč zlogov pomnilnika za zaupne podatke (EEPROM) in od 1 do 16 tisoč zlogov bralnega pomnilnika (ROM). V delovnem pomnilniku hranimo vmesne rezultate izračunov, bralni pomnilnik hrani operacijski sistem kartice. Zanimivo je dejstvo, da zahteva delovni pomnilnik štirikrat toliko prostora na silicijevi ploščici kot EEPROM, slednji pa je prav tako štirikrat bolj potraten s prostorom kot bralni pomnilnik. Vse to nam v veliki meri omejuje možnosti kompromisa med časovno in prostorsko potratnostjo izvedb algoritmov. Vsebina pomnilnika je zaščitena pred nepooblaščenim dostopom in spreminjanjem. Branje, pisanje in brisanje je pod strojno in programsko kontrolo ter je možno le z izpolnitvijo vnaprej določenih pogojev. Če sistem zazna poizkus vdora, avtomatično prepiše zaupne podatke (zeroization).

Običajno imajo procesorske kartice le zelo preprost osem bitni procesor s hitrostjo ure, ki ne presega 5MHz. Tako bi se operacije asimetrične kriptografije (dešifriranje) z dolžino ključa 1024 bitov (na primer RSA) in le omejenim delovnim pomnilnikom izvajale kar nekaj minut. Zato nekatere izvedbe poleg procesorja vsebujejo še kriptografski koprocesor. Slednji vsebuje dodatno aritmetično enoto, prirejeno za računanje z velikimi števili (v primer RSA za hitro potenciranje). Tako se trajanje operacij z zasebnim ključem skrajša na nekaj sto milisekund. Vsako povečanje pomnilnih ali procesorskih zmogljivosti bistveno poveča ceno kartice. V primeru uporabe asimetričnega šifrirnega sistema, temelječega na eliptičnih krivuljah, ni potrebe po dodatnem procesorju.

Prav tako je tudi hitrost komuniciranja kartice z zunanjim svetom zelo omejena. Kartica komunicira s terminalom preko serijskega vmesnika, katerega hitrost ne presega 9600 baudov na sekundo. Prenos je izmenično enosmeren. Komunikacijo vedno začne terminal (čitalec pametnih kartic). Slednji izvaja bralne in pisalne operacije, oskrbuje vezja na kartici s potrebno energijo in uro. Dimenzije, električne lastnosti, komunikacijski protokoli in sporočila so standardizirani po ISO standardih (ISO 7816-1 do ISO7816-4, Husemann [25]).

Pametne kartice in kriptografski postopki

Pri izvedbi kriptografskih postopkov s pomočjo pametnih kartic je potrebno poleg prednosti upoštevati še mnoge omejitve, ki jih tehnologija postavlja. Pametne kartice

imajo zelo omejene pomnilne zmogljivosti za shranjevanje podatkov, programa in programskih spremenljivk. Procesorska moč pametnih kartic je relativno majhna. Pri tem ne upoštevamo posebnih kriptografskih koprocesorjev, ki precej povečajo ceno kartice. Ne nazadnje in za izvedbo prav tako kritični faktor je majhna hitrost komuniciranja z okolico. Tipične operacije so šifriranje, dešifriranje, preverjanje in tvorba digitalnega podpisa.

Pametna kartica ne dovoli, da bi vsebina pomnilnika za zaupne podatke (zasebni ključ, certifikat) zapustila kartico. Tudi lastnik kartice nima neposrednega dostopa do ključa. Uporaba zasebnega ključa je zavarovana s prepoznavanjem entitete (običajno z osebno številko PIN) tako, da samo posedovanje kartice še ne omogoča podpisovanje z zasebnim ključem na kartici.

DES in triple-DES so primeri simetričnih šifrirnih postopkov, ki se nahajajo na pametnih karticah. Pogosto so uporabljeni za izdelavo kriptografskih povzetkov. Ker pametna kartica omogoča le majhne hitrosti prenosa podatkov, je šifriranje velike količine podatkov počasno. SHA-1 in MD-5 so zgoščevalne funkcije, ki se običajno nahajajo na pametnih karticah (Stinson [63]).

Kartice omogočajo generiranje pare ključev za asimetrične šifrirne postopke. Postopek je običajno dolgotrajen (v primeru RSA od 8 sekund do 3 minut, Certicom [12]). Prav tako kvaliteta ključev ni dobra, saj skromne procesorske zmogljivosti omejujejo kvaliteto generatorja psevdo-naključnih števil in postopka za izbiro velikih praštevil.

Izvedba psevdo-naključnega generatorja se med posameznimi izdelovalci razlikujejo. Ločimo dva primera. V prvem ima vsaka kartica svoje unikatno začetno seme in postopek za generiranje psevdo-naključnih števil. Nekatere izvedbe izkoriščajo fizikalne lastnosti silicija za pridobivanje naključne vrednosti. Zaradi izoliranega okolja na kartici je težko narediti dober vir naključnosti.

Šifrirni sistemi, ki temeljijo na eliptičnih krivuljah, nudijo pri izvedbi s pametnimi karticami precejšne prednosti, še posebej na področjih (Certicom [12]):

- *Manjše pomnilniške zahteve*. Težavnost matematičnega problema, na katerem temeljijo šifrirni sistemi z eliptičnimi krivuljami, omogoča, da so šifrirni ključi in posledično certifikati kratki. Potreba po pomnilniku je manjša in čas, potreben za prenos podatkov (digitalnega podpisa, certifikata) v ali iz kartice, je krajši.

- S povečevanjem procesorske hitrosti in z izboljšavami algoritmov za reševanje diskretnega logaritma (faktorizacije) bo potrebno za zagotavljanje enake stopnje varnosti povečevati dolžino ključev. Pri šifrirnih postopkih, temelječih na eliptičnih krivuljah, se *dolžina ključev v primerjavi z ostalimi šifrirnimi postopki najpočasneje povečuje*.

- Narava postopka za šifriranje z eliptičnimi krivuljami v nasprotju z ostalimi asimetričnimi postopki *ne zahteva dodatnega kriptografskega koprocesorja*. Za izvedbo zadostuje vgrajeni procesor, kar prinese znaten prihranek pri ceni.

- Uporaba pametnih kartic za tvorbo digitalnega podpisa zahteva, *da zasebni ključ nikoli ne zapusti kartice* in je nedostopen vsem ostalim entitetam. Ostali asimetrični šifrirni sistemi zadovoljujejo slednje zahteve s prenosom ključa na kartico v varnem okolju, saj je generiranje ključev na kartici računsko prezahtevno in nepraktično. Ključe za eliptične šifrirne sisteme lahko generiramo tudi z napravami, ki imajo skromne procesorske zmogljivosti, če je na voljo dober psevdo-naključni generator.

Napadi na pametne kartice

Čeprav so pametne kartice zasnovane tako, da so odporne proti vdiranju v sistem kartice in razkritju zaupne vsebine še vedno obstaja cela paleta uspešnih napadov. Vrsta napada je pogojena z znanjem, denarnimi zmožnostmi napadalca in privlačnostjo vsebine za napadalca. Razvrstimo jih lahko v sledeče kategorije (Petri [49], Kocher [34], [35], Schneier, Shostack [61]):

- Napadi na *logično delovanje*. Kartica deluje v normalnih pogojih. Z opazovanjem komunikacije in pretoka podatkov med terminalom in kartico lahko zajemamo podatke o vsebini kartice. Tovrstni napad (timing attack) je prvi opisal Kocher [34]. Kartici pošiljamo različne nize podatkov za podpisovanje z zasebnim ključem. Z beleženjem časa izvedbe operacije in številom ničel in enic v rezultatu se lahko dokopljemo do zasebnega ključa. Napad zahteva poznavanje dostopnega gesla (PIN). Ker kartica ne premore svojega vira energije, lahko z opazovanjem porabe energije med izvajanjem operacij določimo zasebni ključ, shranjen na kartici (Kocher [35]).

- *Fizični napadi*. Izvajamo jih s spreminjanjem napetosti, temperature, frekvence ure s ciljem priti do zaupnih podatkov. Prav tako lahko z razkritjem silicijevega substrata in spreminjanjem delovanja logičnih vezij poizkušamo obiti programske in fizične mehanizme varovanja (Anderson, Kuhn [2]).

- Napadi *s trojanskim konjem*. Trojanskega konja namestimo na računalnik žrtve in počakamo, da uporabnik vnese PIN. Tako lahko uporabljamo zasebni ključ uporabnika brez vednosti lastnika. Z vnosom PIN-a za vsako uporabo ključa lahko tovrstne napade onemogočimo. Taka rešitev je za uporabnika kartice precej moteča.

Prednosti pametnih kartic kot so večja varnost podatkov, aktivna zaščita pred vdiranjem, prilagodljivost, večnamenskost, možnost izvajanja transakcij brez potrebe po priključevanju na strežnik za prepoznavanje, so poglavitni prispevki pri povečevanju varnosti računalniških sistemov. Rešitve z uporabo pametnih kartic so smiselne, če je vrednost tistega, kar ščitimo, velika. Pametne kartice si lahko predstavljamo kot agenta, ki nas zastopa in sodeluje v našem imenu z aplikacijo. Digitalni podpis in sheme za prepoznavanje so naravna uporaba pametnih kartic. Kartice ščitijo tako zasebnost podatkov pred nedovoljenim dostopom kot tudi podatke izdajatelja oziroma ponudnika storitve. Omogočeno je vzpostavljanje shem z deljenjem skrivnosti in hkrati preprečevanje manipulacije podatkov, shranjenih na pametni kartici.

2. PREDNOSTI UPORABE PAMETNIH KARTIC

Izvedba infrastrukture javnega ključa s hranjenjem zasebnih ključev in certifikatov na pametni kartici prinaša mnoge prednosti. Z uporabo pametnih kartic kot nosilcev in upravljavcev certifikatov in zasebnih ključev se mnogi mehanizmi v infrastrukturi javnega ključa poenostavijo ali postanejo celo nepotrebni (Brands [9], Petri [49]).

- Preprosto je izvesti *varovanje pametnih kartic pred napadi virusov in trojanskih konj*, ki se hočejo dokopati do zasebnega ključa, saj operacijski sistem kartice ne dopušča, da bi zasebni ključ zapustil kartico. Vsa šifriranja opravi interni procesor na kartici na podlagi vhodnih podatkov in zasebnega ključa. Kartica vrne le rezultat.

- Sistemi, ki temeljijo na prepoznavanju na podlagi digitalnih certifikatov, so mnogo bolj varni pred napadi kot sistemi, kjer ima vsak uporabnik svoje geslo, saj *ni potrebe po skupni skrivnosti*. Zasebni ključ je shranjen le na enem mestu in nikoli ne zapusti pametne kartice. Kartica omogoča uporabo ključa, ne da bi ga bilo potrebno prenašati preko omrežja ali hraniti na računalniku, priključenem v omrežje. Tudi z vdorom v računalnik se napadalec ne more polastiti ključa.

- Sistemi s pametnimi karticami nudijo *večkratno prepoznavanje*, saj poleg poznavanja gesla zahtevajo tudi posedovanje kartice. Če kartica podpira biometrično kontrolo dostopa (Jain, Hong [31]), je možno še dodatno prepoznavanje glede na značilne fiziološke oziroma vedenjske lastnosti (danosti) posameznika. Če prepoznavanje temelji na glasu ali prostoročnem podpisu, je omogočeno prepoznavanje po določenem dejanju, ki ga zmore le lastnik para ključev. Ker prepoznavanje ne temelji na znanju oziroma posedovanju nečesa, je preprečeno, da bi entiteta svoj certifikat posojala

- S hranjenem zasebnega ključa in certifikata na računalniku oziroma v spletnem brskalniku je pri prepoznavanju v nekem smislu prepoznan računalnik in ne imetnik certifikata. Uporaba kartice za hranjenje ključa in certifikata omogoča *resnično prepoznavanje entitete*, prav tako je certifikat enostavno prenosljiv.

- Če ima kartica vgrajeno zaščito dostopa (PIN kodo, geslo, prepoznavanje na podlagi biometričnih podatkov), je nepoklicanim *onemogočena uporaba in dostop do vsebine odtujene kartice*. Če je zasebni ključ shranjen na disku, lahko napadalec s poizkušanjem vseh možnih gesel pride do ključa, saj so gesla običajno enostavna in predvidljiva. Pametna kartica lahko po določenem številu napačnih vnosov PIN-a zaklene kartico in prepreči napad z grobo silo.

- Zaščitni mehanizmi, ki varujejo pred poseganjem v delovanje in kopiranje vsebine pametne kartice, *preprečujejo entitetam izdelavo kopij osebnih certifikatov*. Pri programski izvedbi hranjenja digitalnih certifikatov je preprečevanje izdelave kopij mogoče le s priključnim preverjanjem vsake posamezne transakcije.

- Če ima pametna kartica vgrajeno zanesljivo (natančno) notranjo uro, lahko *preverjanje zapadlosti certifikata* namesto uporabnika digitalnega certifikata opravlja pametna kartica, ki prepreči uporabo certifikata, če je le-ta pretečen. Certifikati, ki jim je potekla veljavnost, se lahko sami onemogočijo za uporabo. Pametna kartica le spremlja datum zapadlosti in se po zapadlosti samodejno blokira. Tako lahko prejemnik digitalnega podpisa opusti vzdrževanje varnega strežnika točne ure.

- Z uporabo zanesljive notranje ure lahko kartica *omejuje število uporab* certifikatov v določenem časovnem obdobju. To pride v poštev pri določenih tipih certifikatov ali poroštvih, ki jih nudi certifikatna agencija.

- Pametna kartica sama presodi, ali lahko imetnik certifikata izvede transakcijo. Tako v kali preprečimo zle namene posameznikov.

- Certifikat lahko *vsebuje tudi negativne atribute* (na primer prepoved vožnje osebnega avtomobila). Imetnik prepreči objavljanje zanj neugodnih atributov le s poseganjem v vsebino pametne kartice. Slednja z blokiranjem delovanja onemogoči uporabo vseh certifikatov na kartici.

- Kartica lahko prepreči lastniku certifikata, da bi drugemu uporabniku pomagal k dostopu, za katerega ne poseduje ustreznega certifikata.

- Onemogočeno je izsiljevanje imetnika certifikata, da bi izsiljevalcem predal par ključev, saj ne more/zna zlomiti zaščite za dostop do zasebnega ključa.

- Pametna kartica lahko *interno vodi dnevnik*, ki omogoča izdajatelju globlji vpogled v poslovanje imetnika certifikata (npr. seznam vseh transakcij, znesek elektronske denarnice...). Če ima kartica vgrajeno notranjo uro, lahko kartica dodaja časovno znamko k digitalnemu podpisu. Pri tem je potrebno poudariti, da je smiselno voditi dnevnik dogodkov le, če je škoda z uničenjem kartice večja kot pa dobit, ki je rezultat vdora v kartico.

- Ranljivost zasebnega ključa otežuje zanesljivo povezavo digitalnega podpisa z entiteto, kar zapleta pravni status digitalnega podpisa, kot elektronskega ekvivalent prostoročnemu podpisu. Zato so naprave, ki so dobro zaščitene pred poseganjem v njihovo vsebino, ključnega pomena za *zagotavljanje pravnih temeljev elektronskega poslovanja*.

- Pomemben prispevek bi pametne kartice v infrastrukturo javnega ključa prinesle tudi na področju *mehanizmov za preverjanje preklica certifikatov*. Ker je tveganje za razkritje zasebnega ključa bistveno zmanjšano in je izluščevanje ključa iz pametne kartice dolgotrajen proces, je problem svežine in razširjanja seznama preklicanih certifikatov v veliki meri odpravljen. Le poredkoma se bo pojavila potreba po priključnem preverjanju veljavnosti certifikatov. Preverjanje transakcij se po pravilu lahko opravi brez neposrednega dostopa do strežnika, ki hrani seznam preklicanih certifikatov. Z robustno izvedbo zaščite pametne kartice je predvidena velikost seznama preklicanih certifikatov, ki jih uporabljamo za prepoznavanje, zanemarljive velikosti.

- Pametne kartice omogočajo enostavno prenosljivost certifikata.
- Izvedbe infrastrukture javnega ključa s pametnimi karticami imajo psihološko prednost pred programsko izvedbo upravljanja s certifikati.

Seveda je vsaka naprava, ki je odporna pred vdiranjem in zlorabo vsebine, primerna za hranjenje zaupnih podatkov (na primer iButton [26]). Drugačne izvedbe nudijo lažje varovanja z uporabo vira napajanja ali bolj dovršeno kontrolo dostopa. Mi bomo v okviru dela za vse možne izvedbe uporabljali izraz pametna kartica.

Glede na vse povedano je naravno, da so se tudi v praksi pojavile implementacije infrastrukture javnega ključa na osnovi pametnih kartic. Najbolj uspešna implementacija te vrste je Fortezza [23]. Ostale omembe vredne so SET [59]. Eden izmed redkih infrastruktur javnega ključa, ki so bile namensko zasnovane na osnovi pametnih kartic, je Tokenner (Brands [9]).

3. OMEJITVE PRI UPORABI PAMETNIH KARTIC

Seveda hranjenje digitalnega certifikata in zasebnega ključa na pametnih karticah ne prinaša samo dobrih stvari. Posebno kritične so pomnilne zmogljivosti pametnih kartic, saj moramo poleg para ključev hraniti vsaj še digitalni podpis certifikata. Slednji lahko pri uporabi 1024 bitnega RSA digitalnega podpisa doseže 128 zlogov. Zapis certifikata po standardu X.509 lahko preseže tisoč zlogov, certifikat agencije pa zaradi daljših ključev tudi do dva tisoč zlogov. Ker imajo mnoge naprave precej omejeno hitrost pošiljanja ali sprejemanja podatkov (9600 baud/sekundo), je lahko velikost certifikata nezanemarljiv problem. V skladu z varnostnimi zahtevami in zakoni o digitalnem podpisu se čedalje pogosteje pojavlja zahteva, da ima vsak uporabnik tri različne pare ključev: za šifriranje, prepoznavanje in preprečevanje tajenja. Z uveljavljanjem varnega komuniciranja in elektronskega poslovanja v svetu brezžičnih naprav (digitalni telefoni...) in pametnih kartic se pojavlja potreba po bolj zgoščeni predstavitvi podatkov v certifikatih javnega ključa.

Cilj zgoščenega zapisa certifikatov je zadostiti omejenim zmožnostim za procesiranje, hranjenje in hitrostjo prenosa. Pri tem ne sme trpeti varnost ali združljivost z obstoječimi storitvami, temelječimi na digitalnih certifikatih. Učinkovitost je prav tako pomembna postavka, še posebej če uporabljamo certifikate s kratko življenjsko dobo. Obstaja kar nekaj predlogov, kako prihraniti prostor. Pristop, kjer s povečanjem časa izvajanja sprostimo pomnilniške zmogljivosti, ni uporaben, saj imajo naprave omejene tako procesorske kot pomnilniške zmogljivosti. Prav tako bi lahko zahteve po dodatnem procesiranju povzročale probleme za aplikacijske strežnike, ki komunicirajo z napravami. Čeprav imajo strežniki običajno na voljo zadosti procesorskih in pomnilnih zmogljivosti, morajo postreči velikemu številu odjemalcev v kratkem času. Znatno povečanje časa, potrebnega za obdelavo certifikata, lahko ogrozi zmožnost strežnika, da obdela transakcije z zahtevano intenzivnostjo.

Certifikati javnega ključa zagotavljajo povezavo med entiteto in njenim javnim ključem. Vsako spreminjanje naj vsaj ohrani nivo varnostni. Zato zgoščevanje

certifikatov s krajšanjem dolžine ključa ne pride v poštev. Razmisleka vredna je uporaba šifrirnih postopkov, katerih dolžine ključev so inherentno krajše kot pa v primeru splošno uveljavljenega RSA postopka. Kot očiten kandidat se kažejo šifrirni postopki na osnovi eliptičnih krivulj. Tu za zagotavljanje iste stopnje varnosti potrebujemo dolžino ključa, ki je za osemkrat manjša kot pri RSA.

Pristope za zgoščevanje certifikatov lahko strnemo v štiri skupine: s priporočilom X.509 združljive rešitve okrnjenih certifikatov, s priporočilom X.509 nezdružljive rešitve, ki jih je mogoče pretvoriti v standarden zapis, certifikati, ki niso združljivi s standardom in jih ni mogoče pretvoriti, in nove smeri v zapisovanju certifikatov. Pregled pristopov za zgoščevanje zapisa certifikata lahko bralec najde v Nystr□m [48].

Računske, komunikacijske in pomnilne zmogljivosti pametnih kartic so pogosto navedene kot glavni razlogi za počasno uveljavljanje infrastruktur javnega ključa na podlagi pametnih kartic. Trenutno vsi predlogi implementacije predvidevajo pametne kartice z velikimi pomnilniki (EEPROM-i) in zmogljivimi kriptografskimi koprocesorji. Učinkovitost izvedbe je poglavitnega pomena pri implementacijah certifikatov s pametnimi karticami za kratkožive certifikate. Dodajanje kompleksnih komponent in programske opreme v kartice je zahteven in drag postopek, kar lahko vodi v oslabitev zaščite. Dodajanje novih elektronskih komponent vpliva tudi na zanesljivost delovanja pametne kartice.

Slabosti hranjenja certifikatov na pametnih karticah

Izvedba mehanizmov infrastrukture javnega ključa le s pametnimi karticami nam lahko prinese precej prednosti pred programsko izvedbo. Vendar mnoge prednosti ne pridejo do izraza, če izvedemo hranjenje certifikatov le s pomočjo pametnih kartic. Poglavitne slabosti so:

- *Ogrožanje zasebnosti uporabnika* pametne kartice. S pravilno zasnovo in uporabo lahko pametne kartice v veliki meri izboljšajo nadzor nad ohranjanjem zasebnosti informacij pri komuniciranju v globalnih omrežjih. Vendar sistemi pametnih kartic trenutno ne omogočajo preprečevanja sledenja transakcijam, ki jih posameznik izvaja s pomočjo kartice. Zaradi varnostnih razlogov kartica ob vsaki transakciji pošlje unikatno številko kartice, ki je lahko ključ za zbiranje informacij o dejavnostih posameznika. Brands [9] predlaga možne rešitve problema varovanja zasebnosti.

- Nad samim *delovanjem pametne kartice uporabnik nima nadzora*, kaj šele vpogleda. Brez velikih težav jih lahko programiramo, da delujejo kot trojanski konj, ki hkrati z nudenjem storitev entiteti skrivaj pošiljajo tudi zasebne podatke. Dejstvo, da vladne organizacije naročajo izdelovalcem elektronske opreme vgradnjo stranskih vrat ,dvom še krepi Brands [9].

Naprava lahko skrivoma pošilja ali sprejema podatke z uporabo van Eck-ovega efekta (Brands [9]) s pošiljanjem ali sprejemanjem radijskih signalov. To še posebej velja pri brezkontaktnih karticah. Podoben skrivni kanal za prenos podatkov je pri komuniciranju z drugo napravo. Poleg podatkov, ki so določeni s protokolom, lahko

naprava oddaja še dodatne podatke. Več o tem lahko bralec najde v (Brands [9]) in tam navedenih referencah.

Pametne kartice se ne bodo mogle uveljaviti, če jim uporabniki ne bodo zaupali. Če bo nevarnost sledenja karticam pretehtala udobnost in enostavnost uporabe, se na tržišču ne bodo uveljavile.

Poleg skrbi za izgubo zasebnosti pri uporabi pametnih kartic lahko navedemo še druge pomisleke. Za večino kaj hitro vsaj teoretično in na papirju najdemo ustrezne rešitve.

- Pri dodajanju novih komponent in programiranju je potrebna previdnost, da ne ogrozimo varnostnih mehanizmov, ki preprečujejo poseganje v samo delovanje kartice in v njej shranjene skrivne podatke. Pri napravah, ki morajo zagotavljati odpornost pred zlonamernim vplivanjem na njihovo delovanje (tamper-resistance), je dodajanje novih komponent in spreminjanje programske opreme mnogo zahtevnejše.

- Dodajanje novih elektronskih komponent na že tako omejen prostor še dodatno ogroža *zanesljivost delovanja sistema*. Nedelujoča kartica je lahko zelo neprijetna, če ne že dramatična novica za uporabnika. Če je kartica namenjena za uporabo v več aplikacijah, se uporabnik nenadoma znajde pred nezmožnostjo uporabe več storitev.

- Zaradi prostorske omejitve bo vedno zelo *omejen nabor funkcionalnosti*, ki ga lahko shranimo na kartico. Količina pomnilnika, potrebna za vodenje dnevnika dogodkov, je znatna. Zaslon in tipkovnica najbolj zmogljivih pametnih kartic omogočata izmenjavo le zelo osnovnih podatkov.

- Pametnim karticam je potrebno zaupati, da bodo ščitile varnostne interese imetnika. Ker bodo le redke pametne kartice vsebovale svoj zaslon in tipkovnico, bo vnos identifikacije uporabnika običajno izveden s pomočjo terminala, ki bo komuniciral s kartico. Potrebna bo določena *stopnja zaupanja, da terminal ne bo zajemal imetnikovih zaupnih podatkov*. Prav tako bodo vsi rezultati, ki jih bo hotela kartica sporočiti imetniku, prikazani uporabniku preko terminala. Odpirajo se možnosti za ogrozitev varnosti imetnika s pomočjo lažnih terminalov. Uporabnik terminala ne more preveriti, da so podatki, ki jih je vnesel oziroma so mu bili prikazani, pristni.

  Če ima imetnikov računalnik tipkovnico, lahko preko nje vnaša zaupne podatke in spremlja informacije o izvedbi transakcij. Ni potrebe, da uporablja posebno napravo.

- Če se tvorba ključev izvaja v sami kartici, ne moremo preveriti, ali je bil postopek generiranja tak, da ključev ni mogoče uganiti. Težko je postaviti jamstvo, da na primer *certifikatna agencija ne more rekonstruirati vseh skrivnih ključev*. To precej omaja pravni status digitalnega podpisa.

- Zaradi varnosti bodo izdajatelji kartic prisiljeni vsakih nekaj let izdajati nove verzije pametnih kartic. V vmesnem času bodo uporabniki soočeni s problemi prehoda na novo tehnologijo.

Povezava pametnih kartic in programskih rešitev

V večini primerov pametna kartica ne more opravljati svoje funkcije sama zase, saj po svoji naravi lahko deluje le v povezavi z drugo napravo (mnogo pametnih kartic sploh ne vsebuje svojega vira napajanja). Tako se v mnogo primerih pametne kartice uporabljajo v povezavi z osebnimi računalnikom (ali v splošnem s programsko vodeno napravo pod kontrolo uporabnika). Pri integraciji pametnih kartic in programsko vodenih naprav (osebnih računalnikov) je bilo že precej narejenega na področju standardizacije, na primer PC/SC delovna skupina ali pa OpenCard (Husemann [25], [26], [3]) .

Kombinacija pametnih kartic in osebnega računalnika nudi več očitnih prednosti. Navedimo le nekaj najbolj očitnih. Daljši seznam lahko bralec najde v (Brands [9]).

- Preprečimo lahko napade z lažnimi terminali. S pomočjo tipkovnice lahko vnašamo gesla, kode PIN ali biometrične podatke ter odčitavamo informacije o poteku transakcije preko zaslona. Ni potrebe po posebni napravi, ki bo sprejemala vhodne in izhodne podatke s pametne kartice.

- S primerno zasnovo lahko večino računsko intenzivnega dela in vodenja dnevnika dogodkov prenesemo s pametne kartice v osebni računalnik. Le-ta poseduje mnogo večje računske in pomnilniške zmogljivosti. Tako postanejo postopki z zelo dolgimi ključi izvedljivi tudi s cenenimi pametnimi karticami brez dodatnega kriptografskega koprocesorja.

- Računalnik uporabniku lahko prepreči skrivni odliv podatkov s preverjanjem pretakanja sporočil med pametno kartico in računalnikom. Preverja, ali so podatki v predpisanih območjih in v skladu s protokolom.

Integracija pametnih kartic in uporabnikovega računalnika ponuja ustrezno okolje za odkrivanje odliva podatkov na enostavno izvedljiv način.

V. MEHANIZMI ZA UGOTAVLJANJE STATUSA CERTIFIKATOV

Eden izmed najbolj perečih problemov pri postavljanju in vzdrževanju infrastrukture javnega ključa je pomanjkanje mehanizmov za učinkovito upravljanje s certifikati. Poglavitna ovira je odsotnost učinkovite izvedbe mehanizma za ugotavljanje statusa certifikatov. Izvedba mehanizma za preklic je težak problem in težko je hkrati zadostiti zahtevam po ažurnosti in zmogljivosti za različne aplikacije in okolja.

Certifikat javnega ključa povezuje identiteto entitete in njen javni ključ. Certifikat ima svoje *obdobje veljavnosti*, ki traja tipično od nekaj mesecev do nekaj let. Obdobje je določeno glede na namen uporabe ključa (za digitalno podpisovanje sporočil, izdanih certifikatov, seznamov preklicanih certifikatov, šifriranje podatkov, izmenjavo ključev…), predvideno količino podatkov, ki jih s ključem nameravamo šifrirati, in pomembnost podatkov, ki jih varujemo. Običajno so obdobja veljavnosti glede na namen uporabe ključev predpisana v varnostni politiki sistema. V tem obdobju lahko uporabniki certifikatov zaupajo, da je povezava javni ključ - entiteta veljavna.

V predvidenem obdobju veljavnosti certifikata izdajatelj vodi evidenco o statusu certifikata in o slednjem obvešča uporabnike. Po preteku obdobja izdajatelj certifikata ne jamči več za veljavnost povezave javni ključ - entiteta in atributov, vsebovanih v certifikatu. Še vedno pa se lahko certifikati s pretečenim obdobjem veljavnosti uporabljajo za preverjanje digitalnih podpisov, ki so bila ustvarjeni v času veljavnosti certifikata (večinoma za arhivske namene).

Certifikat je veljaven, dokler ne zapade ali dokler ga ne prekličemo. *Preklic certifikata* je dejanje, s katerim izdajatelj razdre povezavo med javnim ključem in atributi v certifikatu. Pomeni, da je veljavnost certifikata potekla pred datumom zapadlosti, ki je naveden v certifikatu in da se na veljavnost vsebino certifikata ne moremo zanesti. Status certifikata je najpomembnejša informacija, ki jo izdajatelj (ali pooblaščena agencija) vodi o posameznem certifikatu. Z možnostjo preklica certifikata je omogočena daljša življenjska doba certifikatov in zmanjšanje možnosti, da uporabniki prihajajo v stik z neveljavnimi certifikati.

Preklic certifikata lahko povzroči več dogodkov. Med najpogostejšimi so sum ali dejansko razkritje zasebnega ključa entitete, izguba ali uničenja zasebnega ključa oziroma nosilca ključa, eden izmed atributov certifikata je postal neveljaven ali ga je potrebno spremeniti. Nadalje da certifikat ni več potreben za namen, zaradi katerega je bil izdan, ali da je prišlo do spremembe statusa entitete oziroma razmerja med izdajateljem in imetnikom certifikata. Odločitev o preklicu certifikata je v domeni izdajatelja. Običajno pride do preklica na zahtevo pooblaščene osebe. Izdajatelj ob prejetju zahteve preveri izvor zahteve po preklicu.

Kdo so pooblaščene osebe, ki certifikat lahko prekličejo, je zapisano v pravilih delovanja certifikatne agencije. V splošnem imetnik certifikata ni edini, ki lahko zahteva preklic. Na primer podjetje, ki odpusti zaposlenega, prekliče njegov certifikat in s tem pravice do dostopa do določenih storitev. Zanimivo je vprašanje, kdo vse sme, poleg imetnika para ključev, razglasiti razkritje zasebnega ključ oziroma njegovo izgubo.

Pripomnimo, da ni potrebe po preklicu certifikata, če pride do uničenja zasebnega ključa ali pa imetnik para ključev prostovoljno preneha z dejavnostjo, zaradi katere je certifikat pridobil. Pri slednjem predvidevamo, da je certifikat služil le za prepoznavanje. Javni ključ pa je potrebno preklicati, če je bil par uporabljen za šifriranje v primeru, da je prišlo od izgube zasebnega ključa. Postavlja se vprašanje, kako to varno storiti. Običajno je potrebno pridobiti nov skrivni ključ za varno komunikacijo z agencijo.

1. VPLIV PREKLICA CERTIFIKATA NA VERIGE CERTIFIKATOV

Literatura in tudi obstoječe izvedbe infrastrukture javnega ključa dajejo le malo poudarka na pomenu preklica certifikata. Tudi standardi ne posvečajo velike pozornosti semantiki preklica. Tako je pomen preklica v celoti prepuščen uporabniku in posamezni implementaciji preverjanja veljavnosti verige certifikatov.

Namen certifikata ali verige certifikatov je prejemniku priskrbeti podatke, bistvene za odločitev, ali bo digitalni podpis sprejel kot zadostno zagotovilo za veljavno izvedbo transakcije. Certifikat predstavlja le dejstvo, ki naj uporabniku pomaga do pravilne odločitve. Njegova naloga je vzpostavitev *prehodnega zaupanja*.

Proces preverjanja veljavnosti verige certifikatov od certifikata entitete do certifikata agencije, ki ji uporabnik zaupa, je algoritmična graditev (vzpostavljanje) zaupanja v podpisnikov javni ključ. Veriga certifikatov je zaporedje certifikatov, kjer velja tranzitivna lastnost razširjanja zaupanja. Preverjanje, ali je bil certifikat preklican, je le ena izmed funkcij algoritma.

Za učinkovito uporabo ključev in s tem varnostnih storitev je zaželeno, da veriga certifikatov vedno obstaja in jo je enostavno zgraditi. Privzemamo, da sta entiteti del iste infrastrukture javnega ključa oziroma so njune infrastrukture povezane s križnim certifikatom. Pomembno vlogo igra dolžina verige, saj se z njeno dolžino veča nevarnost zlorab, zmanjšuje zaupanje v javni ključ ter otežuje primerjanje posameznih politik certificiranja. Model zaupanja v veliki meri določa način in težavnost graditve verige certifikatov.

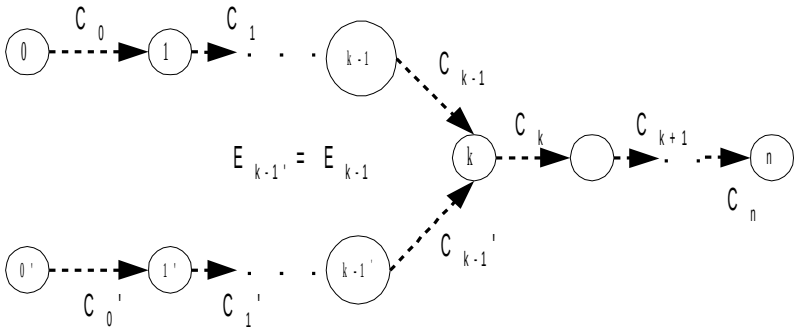
Predlagani standardi za infrastrukturo javnega ključa IETF PXIX (Housley, Ford [27]) natančno določajo postopke za ugotavljanje veljavnosti verige certifikatov. Nič pa ne povedo, kako jo zgradimo. Semantika preklica certifikata je nedefinirana, kar prenese določanje pomena preklica na posamezno implementacijo oziroma uporabnika. V vsakem primeru je dolžnost izdajatelja certifikata, da ga prekliče, četudi na zahtevo imetnika. Certifikatna agencija v končni fazi utrpi največ škode, če so v obtoku neveljavni certifikati, ki jih je izdala.

Za globlje razumevanje pomena preklica si podrobneje oglejmo proces preverjanja verige certifikatov od certifikata podpisnika do certifikata agencije, ki ji uporabnik zaupa. Cilj je preveriti veljavnost certifikata, ki je bil priložen podpisu, ter ugotoviti, ali se veriga certifikatov sklada z varnostnimi zahtevami, zapisanimi v varnostni politiki uporabnika. Uporabnik poizkuša zgraditi zaupanje v javni ključ entitete.

Ugotavljanje statusa certifikata je sestavni in nepogrešljivi del postopka. V nadaljevanju se bomo oprli na delo Foxa in LaMacchie [24].

Pomen preklica certifikatov

Predstavimo verigo certifikatov s $C = c_o, c_1, c_2, \ldots c_n$, kjer je c_n certifikat podpisnika in c_0 samopodpisani certifikat agencije, ki ji uporabnik zaupa. Certifikat c_k je podpisala agencija, katere javni ključ najdemo v certifikatu c_{k-1}, za k=1...n. Po definiciji je *veriga certifikatov neveljavna*, če je vsaj eden izmed certifikatov v verigi preklican. Privzemimo, da so vsi certifikati v verigi veljavni. Izberimo neko drugo verigo $C' = c'_0, c'_1,\ldots, c'_{k-1}, c_k, \ldots c_n$, kjer je c_n certifikat podpisnika in c'_0 certifikat agencije, ki ji uporabnik zaupa. c_i in c'_i so različni za i = 0, …, k-1. Certifikata c_{k-1} in c'_{k-1} imata enak javni ključ. Grafično predstavitev verig najdemo na spodnji sliki.



Slika 5.1: Interakcija verig certifikatov

Ker se mehanizem za preklic certifikatov nanaša na točno določen certifikat, lahko prekličemo certifikata c'_{k-1}, vendar pri tem c_{k-1} še vedno ostane veljaven. Veriga certifikatov C' postane neveljavna, C pa še vedno omogoča zgraditev zaupanja v javni ključ podpisnika. Ali je tako stanje dopustno, je odvisno od razloga preklica certifikata. Certifikat c'_{k-1} je izjava, s katero izdajatelj $I_{Ck-1'}$ poveže ime nosilca certifikata in njegov javni ključ. Certifikat lahko preberemo kot izjavo: Izdajatelj certifikata c'_{k-1} potrjuje povezavo med javnim ključem in identiteto entitete.

Preklic certifikata c'_{k-1} lahko pomeni:

1. Certifikat je bil preklican, ker je prišlo od *razkritja zasebnega ključa* entitete. V tem primeru bi moral preklic c_{k-1}' povzročiti neveljavnost vseh verig certifikatov, kjer se pojavlja javni ključ entitete k-1. Torej je tudi veriga C neveljavna. Idealna rešitev je, da se ob preklicu certifikata zaradi razkritja zasebnega ključa vsi certifikati z istim javnim ključem razveljavijo, saj sta ključa entitet enaka in se uporabljata za preverjanje digitalnega podpisa certifikata c_k. Prejemnik certifikata bi moral preveriti status vseh certifikatov, kateri imajo enak javni ključ kot certifikat, ki ga preverja, četudi jih ne uporablja pri gradnji verige certifikatov.

2. Zaradi neveljavnosti je *preklicana povezava med javnim ključem in nazivom* entitete. Ločimo dva primera:

   a) Če sta naziva entitet v certifikatih c_{k-1}', c_{k-1} različna, potem preklic certifikata c_{k-1}' ne vpliva verigo certifikatov C, slednja je še vedno veljavna ne glede na razveljavitev verige C'.

   b) Naziva sta enaka. Prejemnik lahko po lastni presoji zavrne (ali vsaj zahteva dodatna zagotovila) veljavnost verige C, če je naziv imetnika certifikata pomemben za varno in pravilno izvedbo transakcije.

3. Izdajatelj certifikata je *prekinil poslovno razmerje z imetnikom certifikata*. Ni več pripravljen jamčiti za povezavo med javnim ključem in nazivom entitete, čeprav je povezava še vedno lahko veljavna. V slednjem primeru gre za prekinitev pogodbenih odnosov in preklic c_{k-1}' nima vpliva na verigo certifikatov C.

Dejstvo, da je dejanje preklica certifikata potrebno še dodatno pojasniti z razlogom za preklic, so spoznali tudi avtorji standarda X.509. V drugi različici standarda (Housley et al. [27]) so predvideli, da lahko seznam preklicanih certifikatov vsebuje tudi razlog preklica certifikata. Uporabniku je omogočeno ovrednotenje posledice preklica certifikata. Možni razlogi preklica so: razkritja zasebnega ključa, kompromitacija certifikatne agencije, spremembe v atributih certifikata (tudi sprememba imena entitete), zamenjava certifikata, nepotrebnost certifikata za namen, za katerega je bil izdan, začasna razveljavitev certifikata (suspend).

A četudi bi bili razlogi preklica vedno na voljo in bi se enolično preslikali v eno izmed zgoraj navedenih točk (na primer začasnega preklica certifikata ne moremo z gotovostjo uvrstiti v nobeno izmed zgornjih točk), bi se še vedno pojavljal problem v primeru, ko bi prišlo do razkritja zasebnega ključa. Slednji primer lahko vpliva tudi na druge verige certifikatov, ki preklicanega ne vsebujejo. Sklenemo lahko, da četudi imamo možnost poizvedovati o statusu certifikata in razlogih za njegov preklic, nam uporaba informacije o preklicanih certifikatih še vedno vnaša znatno mero negotovosti v proces gradnje zaupanja.

2. IZVEDBA MEHANIZMOV ZA RAZŠIRJANJE STATUSA CERTIFIKATOV

V nadaljevanju se bomo ukvarjali z mehanizmi, ki se uporabljajo za ugotavljanje statusa certifikata. Eksplozivna rast elektronskega poslovanja v globalnih omrežjih je povzročila zaskrbljenost zaradi pomanjkanja učinkovitega upravljanja s certifikati. Ena izmed osnovnih zaprek pri vzpostavitvi le-teh storitev je odsotnost učinkovite izvedbe mehanizma za preklic certifikatov. Če je preklic certifikata izjemen dogodek, preverjanja statusa certifikata, zapadlosti oziroma preklica, zagotovo ni. Uporaba certifikata, ki je bil preklican in njegov status objavljen, razreši agencijo vse odgovornosti za nastalo škodo.

Izvedbe lahko razdelimo na tiste, ki zahtevajo priključni dostop do strežnika, kateri hrani status certifikatov, in na tiste, kjer je potrebno v rednih intervalih pridobiti nov seznam preklicanih certifikatov. Časovna svežina podatkov in obremenitev infrastrukture je v obeh primerih ključna in kritična za varnost izvajanja transakcij. MITRE [4] je ocenila, da bo večina stroškov upravljanja infrastrukture javnega ključa odpadla na oznanjanje statusa certifikatov. Za vodenje statusa certifikatov skrbi izdajatelj oziroma njemu podrejena entiteta. Seznam preklicanih certifikatov in odgovor na poizvedbo o statusu certifikata morata vsebovati podatke, ki omogočajo preverjanje neokrnjenosti sporočila in identitete pošiljatelja. Prav tako je potrebno informacijo o statusu certifikatov opremiti s časovno znamko in tako preprečiti napad s ponavljanjem. Vse izvedbe slonijo na dobri omrežni povezljivosti za priključno preverjanje oziroma redno osveževanje seznama preklicanih certifikatov.

Težko je izdelati shemo, ki bi zadostila kriterijem ažurnosti in enakomerne porazdelitve bremena med sodelujoče v vseh okoljih. Zaenkrat še ni bilo predstavljene rešitve, ki bi zadostila zahtevam svežine informacije, enakomerno porazdelila breme med vse strani in bila univerzalno primerna za vsa okolja. Bolj podrobno bi mehanizem za razširjanje statusa certifikatov razdelili na tri izvedbe. Razvrstimo jih lahko kot sezname preklicanih certifikatov, priključne dostope, kratkožive certifikate.

- Najbolj razširjen način izvedbe je *seznam preklicanih certifikatov* (Adams, Zuccherato [1], Cooper [14], McDaniels, Rubin [41]). Seznam preklicanih certifikatov je digitalno podpisana podatkovna struktura z označenim datumom nastanka, ki našteva vse preklicane certifikate v dani administrativni domeni. Status kateregakoli certifikata v domeni lahko razberemo v zadnji izdaji seznama. Pogostost objavljanja seznama certifikatov je odvisna od certifikatne agencije. Večja pogostost zmanjšuje verjetnost uporabe preklicanega certifikata, a bolj obremenjuje infrastrukturo pri razdeljevanju seznama med uporabnike. Večinoma je pogostost objavljanja certifikatov znana vnaprej. Obstaja kar nekaj predlogov izboljšav osnovne ideje, ki omogočajo zmanjšanje stroškov hranjenja in prevzemanja seznama preklicanih certifikatov.

- Pri *priključnem preverjanju* (Myers et al. [45]) status certifikata preverimo v realnem času. Vsako preverjanje se obravnava ločeno in neodvisno od ostalih. Tako se uporabnik izogne postopkom upravljanja s seznami preklicanih certifikatov in se osredotoči le na certifikate, katerih status ga zanima. Slednja rešitev vnaša zakasnitev in negotovost v izvajanje transakcije. Strežnik predstavlja ranljivo točko infrastrukture. Prav tako je problem v odzivnosti strežnika z rastjo populacije uporabnikov. Vrsta avtorjev (Micali [44], Nora, Nassim [47]) je podala predloge za izboljšave.

- V večini obstoječih infrastruktur je življenjska doba certifikata dolga (nekaj mesecev ali celo let). Uporaba dolgoživih identifikatorjev ima zgodovinske korenine še iz časov, ko so bili le-ti v papirni obliki. Izdelava je bila zapletena in dolgotrajna. V času računalnikov in digitalnih certifikatov pa je razlika med izdajo enega ali sto certifikatov zanemarljiva. *Izdajanje certifikatov s kratko življenjsko dobo* je v mnogih primerih zadosten ukrep, da se izognemo problemu preklicanih certifikatov, ker je čas izpostavljenosti neveljavnemu certifikatu majhen. Če jih opremimo še z dokazom o svežini izdaje (časovne

znamke), se izognemo problemu preklica v celoti (McDaniels, Rubin [41], Rivest [56]).

Poudariti je potrebno, da vsi mehanizmi za ugotavljanje statusa certifikata zahtevajo varen časovni strežnik, saj lahko napadalec v nasprotnem primeru ponaredi čas nastanka digitalnega podpisa in uporablja že preklican ključ.

Vsi mehanizmi lahko z vnaprej znanim (ocenjenim) časovnim zamikom posredujejo entiteti status certifikata. Nobeden od zgoraj naštetih mehanizmov se ne ukvarja s pomenom preklica certifikata. Le-tega lahko uporabnik certifikata na podlagi razloga za preklic obravnava v skladu s svojo varnostno politiko.

Preklic certifikata je proces, ki za izvedbo zahteva določen čas. Osnovna dilema uporabe certifikatov za izvajanje transakcij je *časovni interval* med izjavo, da je certifikat veljaven, in njegovo uporabo. Slednji določa še dopustno izpostavljanje neveljavnemu, morda še nepreklicanemu certifikatu, ki ga je uporabnik pripravljen sprejeti. Čas je lahko zapisan v varnostne politike sistema. Kot dominantne faktorje, ki določajo širino intervala, so vrsta transakcije, način, kako je bil certifikat pridobljen, zaupanje, ki ga uporabnik goji do imetnika certifikata in agencije, ki je certifikat izdala. V praktični izvedbi je interval vedno kompromis med še sprejemljivo svežino informacije in odzivnostjo aplikacije (strežbe).

Večina obstoječih mehanizmov za oznanjanje statusa certifikata je realizirana ali s seznamom preklicanih certifikatov ali s priključnim preverjanjem. Prav na račun seznama preklicanih certifikatov je v literaturi mnogo argumentov proti taki izvedbi mehanizma za preklic. Ker mnogi izmed njih nudijo globlji vpogled v problem preklica certifikatov in nam bodo v pomoč pri gradnji modela, si oglejmo kritike.

3. KRITIKE SEZNAMA PREKLICANIH CERTIFIKATOV

Uporaba seznama preklicanih certifikatov za objavljanje predčasno zapadlih certifikatov odpira vrsto vprašanj tako s področja učinkovitosti delovanja in organiziranosti infrastrukture javnega ključa kot s stališča varnosti in stopnje tveganja, ki mu je uporabnik certifikata izpostavljen. Večina kritik se nanaša na omejenost izvedbe z vidika storitev, ki jih ponuja in stroškov.

Rivest [56] podaja obširen seznam pripomb in predlogov za izboljšanje. Oglejmo si jih in zgradimo mehanizem za preverjanje veljavnosti certifikatov brez seznama preklicanih certifikatov.

- Prejemnik digitalnega podpisa naj postavlja zahteve o svežini predloženih dokazil.

Poleg digitalno podpisanega sporočila entiteta običajno predloži tudi svoj certifikat javnega ključa, lahko pa še certifikat agencije, ki ga je izdala. Svežino predloženih dokazil določa agencija. Slednje ne bi smelo biti v domeni izdajatelja certifikata, saj uporabnik trpi posledice v primeru, če je njegova odločitev glede na podatke, ki jih

ima na voljo, napačna. Tako je periodično izdajanje certifikatov in seznama preklicanih certifikatov napačno, saj uporabniku certifikata ne omogoča določanja svežine podatkov.

Kot dodatno pripombo glede seznama preklicanih certifikatov omenimo dejstvo, da je sestavljen le iz negativnih izjav. Če certifikata ni v seznamu, še ne pomeni, da je z njim vse v redu. Preklic certifikata je proces, ki zahteva svoj čas.

- Podpisnik dokumenta mora priskrbeti vsa relevantna dokazila, ki jih uporabnik potrebuje za preverjanje digitalnega podpisa, vključno z informacijo o svežini atributov v certifikatu.

Sledeči princip se tiče bolj učinkovitosti delovanja infrastrukture javnega ključa kot same varnosti. Argumenti za tako izvedbo so:

- Tako podpisnik kot uporabnik lahko poizvedujeta o stanju certifikatov.
- Informacija o svežini certifikata je za podpisnika uporabna še nekaj časa.
- Breme iskanja podatkov preložimo na podpisnika (odjemalca) in ne na morebiti preobremenjenega uporabnika (strežnik).
- Omogočimo izvedbo strežnika brez stanj. Strežnik brez stanj je odpornejši za napade, ki onemogočajo strežbo (denial-of-service-attack).

Možna izjema, da podpisnik priloži dokaz o veljavnosti certifikata, je primer, ko želi prejemnik brezpogojno preverjanje svežine informacije, zapisane v certifikatu, kar izvede s priključnim dostopom do ustreznega certifikatnega strežnika.

- Najpreprostejši način za dokaz časovne svežine podatkov v certifikatu je predložitev certifikata, ki je bil izdan pred kratkim.

Čeprav se zdi, da potrebujemo priključni dostop do certifikatnega strežnika, se lahko z uporabo metode, ki jo je predlagal Micali [44], temu izognemo. Z uporabo vedno dostopnega strežnika ponovno preverimo izdani certifikat, katerega je predhodno izdala certifikatna agencija.

Poseben problem predstavlja interval veljavnosti certifikata. Le-ta trdi (na primer pri certifikatih po standardu X.509), da je certifikat veljaven do točno določenega datuma, razen če ni bil pred tem datumom preklican. S stališča uporabnika certifikata to ni zelo koristen podatek, saj mora vselej preveriti, ali je bil certifikat preklican. Tudi v primeru certifikatov po priporočilih SPKI/SDSI 2.0 (Rivest, Lampson [55], Ellison et al. [17], [18]) ni stanje nič boljše. Iz vsebine slednjega lahko razberemo le, da je veljaven do datuma izteka, kar razreši uporabnika poizvedovanja o statusu certifikata. Način se obnese pri relativno kratkih intervalih veljavnosti. Pri slabo odmerjenih (prevelikih) intervalih bi se uporabnik po nepotrebnem izpostavljal

tveganju. Prav tako bi lahko tudi izdajatelj postavljal omejitve glede pogostosti izdajanja certifikatov.

- Izdajatelj certifikata lahko poskrbi za bolj splošna (uporabna) zagotovila glede veljavnosti certifikata javnega ključa. Življenjsko dobo bi bilo primerneje razdeliti na tri obdobja:

  I. Vsebina certifikata je zagotovo veljavna.
  II. Vsebina certifikata je verjetno veljavna.
  III. Certifikat je neveljaven.

Certifikati po priporočilu X.509 prehodijo le faze II in III; SPKI/SDSI pa le fazo I in III. S tem omogočimo uporabniku, da se na podlagi lastne presoje glede na stopnjo tveganja in zahtevano akcijo odloči, ali bo za certifikat, ki je v drugem intervalu, zahteval od podpisnika dokazilo o veljavnosti.

Z razdelitvijo obdobja veljavnosti na predlagane intervale uporabnik lažje definira sprejemljivo stopnjo tveganja v varnostni politiki. Izdajatelj certifikata z določitvijo časa gotove veljavnosti vsebine zmanjša število poizvedb in obremenitev strežnikov. Transakcije z nizko stopnjo tveganja oziroma majhnih vrednosti se lahko izvedejo brez dodatnega preverjanja.

Razbitje intervala veljavnosti je bistvena izboljšava v primerjavi s seznamom preklicanih certifikatov, kjer ne obstaja čas gotove veljavnosti vsebine certifikatov.

- Podpisnik naj uporabniku certifikata priloži dokaz, da ni prišlo do razkritja njegovega zasebnega ključa.

Razkritje zasebnega ključa obravnavamo kot poseben primer. Eden izmed pogostih povodov za preklic certifikata je izguba ali razkritje zasebnega ključa. Ker imamo v tem primeru dokaz, da ključ ni bil razkrit ločeno od certifikata, ni potrebe po eksplicitnem preklicu. Z ločitvijo razkritja ključa od ostalih razlogov za preklic certifikata in ker je potrebno ob predložitvi certifikata še potrdilo o neokrnjenosti zasebnega ključa, smo certifikatno agencijo razbremenili opravil v zvezi z razkritjem zasebnega ključa.

Ob razkritju zasebnega ključa imetnik certifikata (ali kdorkoli drug) podpiše sporočilo, v katerem oznani, da je prišlo do razkritja njegovega zasebnega ključa. Za primer izgube zasebnega ključa si sporočilo pripravi vnaprej. Z vzpostavitvijo posebnega strežnika, ki prisluškuje objavam o razkritju ključa in izdaja potrdila, da v omrežju niso zaznali objave o razkritju ključa imetnika certifikata, je rešen tudi problem dokazovanja o ohranitvi integritete zasebnega ključa.

Tako so certifikatne agencije popolnoma razrešene opravil v zvezi s preklici certifikatov in seznami preklicanih certifikatov postanejo nepotrebni. Podpisnik sporočila lahko predloži dokaze samo na podlagi različnih vrst certifikatov. Obe strani se lahko dogovorita o zahtevani stopnji svežine informacije v certifikatih, podpisnik lahko po potrebi priskrbi ustrezno sveže certifikate. Predlog skriva problem

oblikovanja globalnega mehanizma, ki mu mora uporabnik zaupati. Bogatejši za izkušnjo imenika X.500 smo lahko precej skeptični o praktični vrednosti slednjega predloga.

4. UPORABA MEHANIZMOV V RAZLIČNIH OKOLJIH

V nadaljevanju si bomo ogledali mehanizem preklica s seznamom preklicanih certifikatov v treh različnih okoljih. Hkrati bomo pretehtali kritike o realizacije mehanizma za ugotavljanje statusa certifikatov s seznamom. Še prej pa bomo povzeli argumente proti uporabi seznamov preklicanih certifikatov.

1. Ker uporabnik certifikata tvega, mora imeti nadzor nad svežino zagotovil o pristnosti javnega ključa. Pri realizaciji s seznamom preklicanih certifikatov je ažurnost statusa certifikatov podana s pogostostjo osveževanja seznama. Torej je uporabnik podrejen agenciji oziroma entiteti, ki seznam generira.

2. Zaradi učinkovitosti delovanja infrastrukture naj podpisnik priskrbi vsa potrebna zagotovila o veljavnosti. Za vsako transakcijo mora podpisnik pridobiti in predložiti dokaze o statusu certifikata.

3. Za transakcije velikih vrednosti je potrebno imeti na voljo mehanizme za priključni dostop za preverjanje statusa certifikata v realnem času. Čeprav se slednje ne tiče izvedbe preklica s seznamom, implicira še dodatne mehanizme. Argument temelji na predpostavkah, da je zakasnitev inherentna pri izvedbi mehanizma s seznamom in da so transakcije visokih vrednosti pogoste.

4. Stroški upravljanja in razdeljevanja seznama so visoki. Velikost seznama je sorazmerna z domeno, katero seznam pokriva, življenjsko dobo certifikatov in verjetnostjo predčasnega preklica.

5. Seznam preklicanih certifikatov je neprimerna rešitev za transakcije, ki zahtevajo odgovor v realnem času. Stroški tvorbe in razdeljevanja seznama onemogočajo priključno generiranje seznama.

6. Seznam preklicanih certifikatov ne nudi pozitivnega odgovora. Ker seznam vsebuje le preklicane certifikate, obstoja veljavnih ne moremo ugotoviti le na podlagi seznama (informacije o veljavnosti).

7. Nov certifikat je najboljše zagotovilo o svežini informacije. Če je na voljo certifikat z zagotovljeno dobo veljavnosti, se proces preverjanja skrči na preverjanje digitalnega podpisa certifikata. Ker je status certifikata z njegovim obstojem znan, preverjanje v seznamu preklicanih certifikatov ni potrebno.

8. Certifikati v tradicionalnih sistemih s seznamom preklicanih certifikatov ne vsebujejo dodatnih zagotovil o svežini atributov poleg njihove življenjske dobe. Ob vsaki uporabi mora prejemnik pridobiti in preveriti ustrezno svež seznam preklicanih certifikatov. Skupaj s prejšnjo ta točka predstavlja močan argument za priključni mehanizem za preverjanje statusa certifikatov.

Če povzamemo, seznami preklicanih certifikatov ne morejo nuditi storitev, ki jih zahteva uporabnik. Storitev, ki jo nudi, je predraga. Ne smemo pozabiti, da je storitev določena z aplikacijo in zahtevami okolja. Poglejmo si veljavnost zgoraj naštetih argumentov na treh tipičnih okoljih uporabe infrastrukture javnega ključa.

Elektronsko poslovanje in spletna trgovina

Pri elektronskem poslovanju infrastruktura javnega ključa omogoča izvedbo transakcij med trgovcem (strežnik) in kupci (odjemalci). Kupec v vlogi uporabnika certifikata začne s transakcijo ter preveri identiteto strežnika (običajno s protokolom tipa izziv - odgovor). Kupčeva identiteta običajno ni preverjena, trgovcu zadošča številka kreditne kartice kot jamstvo o identiteti. Certifikatna agencija jamči za veljavnost certifikata z digitalnim podpisom in mehanizmom za preverjanje preklicanih certifikatov. Kupec je odvisen od veljavnosti strežnikovega certifikata (neokrnjenost zasebnega ključa) za zagotavljanje varnosti plačila (transakcije). Kupec tvega v primeru razkritja plačilnega kanala. Strežnik tvega svoj sloves za varno izvajanje plačil, a čeprav je tveganje mnogo manj določljivo, so izgube lahko mnogo večje.

> V tem primeru stopnja tveganja ni bistveno večja za uporabnika certifikata javnega ključa. Torej argument pod točko 1 ne pride v poštev.

Trenutno je v globalnih omrežjih okoli 40 certifikatnih agencij (spletni brkljalniki so opremljeni s certifikati certifikatnih agencij). Število strežnikov je mnogo večje, a še vedno mnogo manjše od števila odjemalcev. Hipotetično bi moralo teh nekaj agencij razdeljevati status za milijon certifikatov več milijonom kupcem. V tem modelu so agencije močno obremenjene. V slednjem slutimo razlog za odsotnost mehanizma za preverjanje statusa certifikatov v globalnih omrežjih. Podpora obstoječih mehanizmov v globalnih omrežjih je odločno predraga (kar izniči argument pod točko 2).

Strežniki so običajno močno obremenjeni. Zahteva, da pridobivajo in razpošiljajo status certifikat, le še poslabša problem odzivnosti. Mnogo verjetneje je, da ima kupec na voljo proste vire za pridobitev statusa certifikata.

Obstajajo tehnik, ki zmanjšujejo ali porazdelijo breme vodenja evidence o preklicanih certifikatih. Certifikatna agencija lahko dodeli dejavnosti, povezane s preklici certifikatov, drugi entiteti. Tako ni potrebno uporabljati istega ključa za podpisovanje certifikatov in podpisovanje informacije o preklicanih certifikatih. To je precejšna prednost, saj zasebnega ključa agencije (ki ga uporablja za podpisovanje certifikatov) ni na računalniku, ki je priključen v omrežje.

Priključna izvedba preverjanja statusa zahteva od strežnika, da vsak odgovor na poizvedbo digitalno podpiše. To lahko že pri zmerni stopnji obremenitve pripelje do računsko intenzivne vrste strežbe. Slednje implicira porazdelitev storitve med več strežnikov.

Izvedba s seznamom se izogne večini stroškov, povezanih z izračunavanjem digitalnega podpisa, a ob velikih seznamih rešitev zahteva znaten del omrežnih

zmogljivosti strežnika. Soočeni smo s klasičnim kompromisom med priključno rešitvijo in seznamom oziroma med procesorsko zmogljivostjo in omrežno prepustnostjo.

Izvedba z varnim imenikom se izogne zahtevam po veliki procesorski moči in veliki omrežni prepustnosti. Prednosti v odzivnosti in zagotavljanju svežih informacij, ki jih ponuja rešitev, so pripeljale do izvedbe dreves preklicanih certifikatov (Nora, Nassim [47], Micali [44]).

Glede na trenutne zahteve pri trgovskih transakcijah v globalnih omrežjih ni čutiti potrebe po mehanizmih, ki bi nudili informacijo o statusu certifikata v realnem času. Velika večina transakcij ne spada v skupino transakcij velikih vrednosti. Tako trgovci kot kupci so pripravljeni sprejeti ažurnost informacij o preklicu, ki jo diktirajo drugi.

Na koncu še omenimo, da strežniki, ki razdeljujejo informacije o preklicu, predstavljajo ozko grlo in kritično mesto v primeru odpovedi. Za povečanje zanesljivosti je modro nuditi več neodvisnih virov informacij o stanju certifikatov.

Intranet

Certifikate lahko uporabljamo kot način za prepoznavanje odjemalca v informacijskih storitvah intraneta. V modelu, ki ga bomo analizirali, strežnik nudi zanimive podatke internemu omrežju podjetja. Odjemalec se mora pred uporabo storitve strežniku predstaviti. Strežnik je v vlogi uporabnika certifikata. Ker so vsi odjemalci v isti administrativni domeni, lahko storitve, povezane s certifikati, opravlja majhno število certifikatnih agencij.

Število intranetnih strežnikov je majhno. Zato zajemanje in preverjanje seznamov preklicanih certifikatov ne bi smelo predstavljati prevelike obremenitve za lokalno omrežje. Seznami imajo lastnost referenčne lokalnosti. Ker je malo agencij, si lahko strežniki priskrbijo status certifikata za mnogo certifikatov hkrati. Dobljene informacije bodo uporabne za mnoge transakcije.

Storitev, ki jo strežnik ponuja, določa stopnjo tveganja tako za strežnik kot za odjemalca. To omogoča nivo zaščite, ki je skladen s tveganjem oziroma škodo, ki nastane ob nepooblaščenem vstopu (vdoru) v strežnik. Strežnik je najbolj obremenjen člen v celotni verigi, saj mora preveriti identiteto odjemalca, veljavnost certifikata in nuditi storitev. Ker so dostopi do strežnika običajno pogosti, je smiselno zmanjšati latenco preverjanja certifikata na najmanjšo možno mero.

V modelu obvelja prvi argument: tisti, ki preverja, lahko najbolje oceni stopnjo tveganja, zato naj ima kontrolo nad ažurnostjo podatkov. Stopnja tveganja ni enaka za vse storitve.

McDaniels in Rubin [41] sta predlagala sledečo rešitev z uporabo seznama preklicanih certifikatov. Vsak strežnik se pri strežniku za objavo informacij o preklicanih certifikatih naroči na pošiljanje seznama. Pogostost pošiljanja določi intranetni strežnik. Največja pogostost je določena s hitrostjo, s katero lahko zgradimo seznam preklicanih certifikatov. Zaradi konstantnih stroškov digitalnega podpisa,

hitrosti omrežja in majhnega števila intranetnih strežnikov lahko ta način nudi skoraj enakovredno storitev, kot je priključni dostop do strežnika za informacije o preklicanih certifikatih.

Z izvedbo avtomatične dostave seznama preklicanih certifikatov se strežnik izogne čakanju na odgovor na poizvedbo o statusu certifikata. Mnoge transakcije se lahko izvedejo brez posredovanja certifikatne agencije.

Slabost predlagane rešitve je konstantna zasedenost omrežja za pošiljanje seznamov. Slednjo lahko omilimo z uporabo diferenčnih seznamov preklicanih certifikatov (Housley et al. [27]). Seznam vsebuje le tiste certifikate, ki so bili preklicani od zadnjega popolnega seznama. Uporaba razdeljevalnih točk (strežnikov) lahko razbremeni strežnik, ki skrbi za seznam preklicanih certifikatov.

Z varnostnega vidika je sporno hraniti zasebni ključ certifikatne agencije na strežniku, ki je priključen v omrežje. Zaradi zahtev po svežih informacijah o preklicu se mora ključ nahajati na visoko razpoložljivem strežniku. Modro je ločiti ključ, ki ga uporabljamo za podpisovanje certifikatov, in ključ za podpisovanje seznamov preklicanih certifikatov.

Da bi seznam preklicanih certifikatov objavljal tudi informacije o obstoju certifikata, je potrebno spremeniti le specifikacijo seznama, da vsebuje tudi intervale evidenčnih številk že izdanih certifikatov. Tako ustvarimo mehanizem za razdeljevanje pozitivnih izjav o statusu certifikatov.

Elektronska pošta

Elektronska pošta je postala dominanten medij, s pomočjo katerega uporabniki komunicirajo v globalnih omrežjih. Naloga infrastrukture javnega ključa je omogočiti prepoznavanje med poljubnimi sogovorniki. Tisti, ki preverja identiteto partnerja, običajno ne ve ničesar o sogovorniku niti o agenciji, ki je certifikat izdala.

Poizkusi, da bi vzpostavili globalen okvir za prepoznavanje, so propadli kot posledica netranzitivnosti zaupanja, težav pri iskanju entitet, katerim bi vsi zaupali in množice tehničnih, političnih in sociooloških razlogov.

Posledično so nastajale infrastrukture javnega ključa v neodvisnih skupnostih. Za uspeh mora okvir za prepoznavanje tesno slediti socialnem okolju, v katerem bo deloval. Zaradi pomanjkanja globalnega zaupanja ni verjetno, da bo kdaj obstajala globalna infrastruktura javnega ključa.

Zaradi različnosti skupin, ki uporabljajo elektronsko pošto, je malo verjetno, da bo uporabljena enotna infrastruktura (ali mehanizem za preklic certifikatov). Neodvisne skupine se bodo povezovale s pomočjo prehodov. Vzpostavitev mehanizmov za preklic certifikatov bo zaživel le v okoljih, kjer se bo pojavila potreba.

5. O KRATKOŽIVIH CERTIFIKATIH

Kot je ugotovil Rivest [56], je pogosto izdajanje certifikatov najboljši dokaz o veljavnosti certifikata. Zagotavlja tako prepoznavanje kot veljavnost. Zmanjšuje možnost napačne interpretacije ali ponarejanja serijskih številk certifikata in njegovega statusa. Izdajanje certifikatov je računsko zelo intenziven postopek. V primeru ko je agencija močno obremenjena, je rešitev s kratkoživimi certifikati neprimerna. Ustrezna je le za okolja, kjer si lahko privoščimo računsko intenzivno obremenitev strežnika za izdajo certifikatov.

Če povežemo kratkožive certifikate in obdobje zagotovljene veljavnosti, bistveno zmanjšamo stroške za upravljanje s certifikati. Ker je razkritje zasebnega ključa edini razlog preklica certifikata, se izognemo stroškom, povezanim z upravljanjem s preklicanimi certifikati. Obdobje, v katerem je potrebno prijaviti neveljavnost certifikata, je zelo omejeno.

VI. MODELIRANJE INFRASTRUKTURE JAVNEGA KLJUČA

Poiskati javni ključ entitete oziroma ugotoviti pristnost javnega ključa je osnovni gradnik za varno izvajanje transakcij v vsakem večjem porazdeljenem sistemu. Zaradi odsotnosti osrednje agencije, ki bi nudila tovrstne informacije, se postopki prepoznavanja oziroma ugotavljanja pristnosti javnega ključa entitete izvajajo z gradnjo ter preverjanjem verige certifikatov in so v celoti prepuščeni uporabniku certifikata. Uporabnik zgradi verigo certifikatov entitet, tako da:

- zaupa agenciji na začetku verige in poseduje njen pristni javni ključ,
- vsaka agencija v verigi jamči za certifikat, izdan sledeči entiteti v verigi,
- je zadnji člen verige entiteta, katere javni ključ zanima uporabnika.

Pristop h graditvi povezave javni ključ - entiteta z verigo certifikatov je z varnostnega vidika ranljiv. Sloni na uporabnikovem zaupanju, da je vsaka agencija temeljito preverila naslednjo v verigi, preden je izdala križni certifikat. Če so vse agencije skrbno izvajale postopke, zapisane v politikah certificiranja, lahko uporabnik zaupa v povezavo med javnim ključem in identiteto entitete. Sicer je lahko uporabnik v svojem zaupanju zaveden za vsa naslednja vozlišča in posledično tudi glede pristnosti javnega ključa entitete.

Za povečanje zaupanja v javni ključ entitete in odpornosti na napade je smiselno vrednotiti zaupanja v več verigah. Čeprav je uporaba odvečnih (redundantnih) informacij za gradnjo zaupanja privlačna, ni brez skritih pasti. Certifikatne verige so lahko med seboj v korelaciji, ki jih je težko ugotoviti in še težje zajeti v odločanje. Če k temu dodamo še uporabnikovo nezaupanje v izjave, ki jih dajejo agencije, je še toliko težje ugotoviti veljavnost povezave javni ključ - entiteta.

Opisan pristop nadgradimo. Zaupanje gradimo s pomočjo *modela infrastrukture javnega ključa*. Cilj postavitve modela infrastrukture je pripraviti osnovo za analizo scenarija (primernosti akcije) ter sklepanje o zaupanju v javni ključ entitete in ovrednotenje tveganja ob sprejetju akcije. Model zgradimo iz podatkov (izjav), ki jih hranimo ali jih pridobimo iz infrastrukture. Predstavljen je v obliki usmerjenega grafa. Povezave predstavljajo relacije zaupanja med vozlišči (entitetami) infrastrukture, izdanimi priporočili, certifikati, izjavami o zaupanju, izjavami o pristnosti javnega ključa entitete. Glede na uporabljeno metriko zaupanja povezavam (izjavam) predpišemo stopnjo zaupanja.

Entiteta pridobiva podatke iz infrastrukture javnega ključa. Podatki, ki jih infrastruktura nudi, so lahko nepopolni oziroma nedostopni. Uporabnik certifikata niti podatkom niti entitetam ne zaupa popolnoma. Glede na stopnjo zaupanja, ki jo uporabnik certifikata pripisuje podatkom in entitetam, želi ovrednotiti zaupanje v javni ključ izbrane entitete in stopnjo tveganja v primeru sprejetja odločitve o izvedbi transakcije na podlagi podatkov, ki so na voljo. Postopek zbiranja podatkov, postavitve modela infrastrukture in gradnje zaupanja imenujemo *upravljanje z zaupanjem*. *Gradnja zaupanja* je algoritmični postopek, ki na podlagi zbranih

podatkov in njim prirejenim stopnjam zaupanja ter varnostne politike sistema vrne jedrnat odgovor o zaupanju v povezavo javni ključ - entiteta in tveganju v primeru izvedbe zahtevane akcije.

Pri gradnji modela si želimo izpolnitev sledečih lastnosti. Model infrastrukture naj bo splošen in naj ima veliko izrazno moč. Zajema naj vse vidike uporabe infrastrukture javnih ključev, vključno z izjavami o zaupanju, priporočili, stopnjo zaupanja v izjave, obravnavanjem več verig certifikatov, vrednotenjem tveganja, odvisnosti verig. Rezultati modela naj bodo neodvisni od vrstnega reda vrednotenja zaupanja (uporabe pravil). Postopki modeliranja naj omogočajo učinkovito izvedbo vrednotenja zaupanja v povezavo javni ključ - entiteta in enostavno uporabo. Omogoča naj modeliranje poljubno velike populacije entitet, enostavno dodajanje entitet in parametrov ter obravnavo kompleksnih varnostnih politik. Dodatne zahteve glede metrike zaupanja bomo podrobneje podali v drugem podpoglavju.

Gradnja zaupanja ni vključena v nobeno trenutno delujočo infrastrukturo javnega ključa. Še najbližje je PGP (Pretty Good Privacy, Zimmermann [65]) in njegova dopolnitev s spletnim strežnikom ‘PathServer’ za overjanje PGP ključev, avtorjev Stubblebina in Reiterja [52]. Pri slednjem uporabnik določi komu in v kolikšni meri lahko zaupa, a sistem na podlagi prirejene stopnje zaupanja ne sprejema ustreznih sklepov. Odločitve so prepuščene uporabniku, gradnja zaupanja ni sestavni del infrastrukture.

1. PREGLED OBSTOJEČIH PREDLOGOV REŠITEV

S problemom graditve zaupanja v verigo so se začeli ukvarjati kmalu po začetku vzpostavljanja prvih globalnih infrastruktur. Predstavljenih je bilo več predlogov za upravljanje z zaupanjem na podlagi podane verige certifikatov (poti v grafu). Tako sta na primer avtorja Mendes in Huitema [43] predlagala razširitev certifikatov po standardu X.509, ki bi podpiral metriko zaupanja. Stubblebina in Reiterja [52] predlagata podporo overjanja javnega ključa entitete v infrastrukturi, temelječi na PGP certifikatih [65] s pomočjo spletnega strežnika. Predloge za metriko zaupanja, ki se ne opirajo na določeno predstavitev certifikatov, so predstavili Beth et al. [5] in Maurer [40].

Kot vhodne podatke za izračun zaupanja v javni ključ entitete model iz infrastrukture sprejme certifikate entitet, priporočila in izjave zaupanja v entitete. Vhodni podatki služijo pri graditvi usmerjenega grafa zaupanja. Vozlišča grafa predstavljajo entitete, povezave pa izjave, ki so jih entitete v infrastrukturi dale o drugih entitetah. Avtorji predlagajo različne načine določanja metrike zaupanja, prirejanja stopnje zaupanje dobljenim izjavam. V večini primerov povezavam priredijo število iz intervala [0,1], ki predstavlja stopnjo zaupanja v izjavo (Beth et al. [5], Mauer [40]). Stubblebin in Reiter [52], [53] povezavam ne prirejata dodatnih parametrov. Vozlišča grafa predstavljajo ključi, povezave med njimi pa certifikate. Metrika se osredotoči na dolžino poti in število disjunktnih poti v grafu zaupanja.

Gradnja zaupanja se izvaja na podlagi usmerjenega grafa. Maurerjev [40] oziroma Bethov model [5] vrne številsko vrednost v intervalu [0,1], kar naj bi pomenilo stopnjo zaupanja v pristnost javnega ključa. Stubblebinov in Reiterjev model [53]

vrne število ločenih poti, krajših od neke vnaprej določene vrednosti med zaupanja vrednimi ključi in ključem, ki ga preverjamo. Vsi modeli poizkušajo ovrednotiti zaupanje z upoštevanjem več poti. S tem poizkušajo narediti model, odpornejši na napade. Z odpornostjo modela na napade sta se ukvarjata Kohlas in Maurer [37] ter Levien in Aiken [39].

Nobeden od navedenih modelov ne zajema ugotavljanja statusa certifikatov, iskanja verig certifikatov in preverjanja njihove neodvisnosti. Prav tako je izpuščen opis, kako naj uporabnik prireja stopnje zaupanja izjavam. Pri vseh je opaziti kompromis med učinkovitostjo (uporabnostjo) izvedbe modela in izrazno močjo ter natančnostjo semantike na drugi strani.

Podobne modele za upravljanje z zaupanjem, temelječe na atributnih certifikatih, najdemo v delih Blaze-a et al. [6], [7], [8]. Modeli uporabniku certifikata na podlagi atributov certifikata entitete in zahtevane akcije omogočajo odločanje o dopustnosti izvedbe transakcije. V nadaljevanju se z njimi ne bomo ukvarjali, saj bomo razvijali model za upravljanje z zaupanjem na podlagi identifikacijskih certifikatov.

2. KRITERIJI ZA DOLOČANJE METRIKE ZAUPANJA

Metrika zaupanja definira način prirejanja stopnje zaupanja podatkom (izjavam), ki jih dobimo iz infrastrukture. Reiter in Stubblebine [51] sta podala kriterije za določanje primerne metrike zaupanja. Menimo, da si je dobro ogledati kriterije za določanje metrike, še preden razgrnemo naš predlog modeliranja infrastrukture javnega ključa in vrednotenja zaupanja. Mnoge do sedaj predlagane metrike so izpolnile le nekaj ciljev na račun zanemarjanja ostalih.

Osnovna zahteva za model je očitno vrniti rezultat, ki ga je mogoče enostavno osmisliti. Osnovni faktor, ki pripomore k temu, je natančnost modela. Ustreznost metrike zaupanja lahko analiziramo glede na tri kriterije:

- *pomen*, ki ga lahko pripišemo vrednosti, katero model vrne;

I. *obseg uporabnikove presoje* pridobljenih podatkov:
Določanje metrike pri gradnji modela od uporabnika ne sme zahtevati, da določa povezave med ključi in njihovimi lastniki. V tehničnem smislu certifikate podpiše ključ in ne entiteta. Smisel priporočila je dejstvo, da je težko določiti povezavo javni ključ - entiteta. Vendar se je pri postavitvi modela potrebno odločiti za kompromis med samostojnim delovanjem modela in vključevanjem uporabnika v proces graditve zaupanja.

II. *nedvoumnost*:
Pomen parametrov modela naj bo nedvoumen. To še posebej velja za mero zaupanja oziroma verjetnost veljavnosti izjave. Način prirejanja mere zaupanja izjavam mora biti algoritmično določen.

III. *zajemanje vseh informacij na voljo*:
Metrika naj upošteva vse relevantne informacije za odločitev o veljavnosti povezave med javnim ključem in entiteto. To vključuje tudi izjave o

zaupanju in priporočila. Če model vrne rezultat, ki je posledica omejenih (pomanjkljivih) vhodnih podatkov, bo v splošnem potrebno vložiti več truda v interpretacijo rezultata.

IV. *enostavno tolmačenje sklepa*:
Rezultat modela naj bo intuitiven. Pomen naj bo mogoče zapisati v naravnem jeziku. Za uporabnika je uporaben le rezultat, ki mu lahko pripiše pomen.

- *občutljivost modela* na napade zlonamernih posameznikov ali agencij;

V. *odpornost metrike na napade*:
Metrika naj bo robustna. Odporna naj bo na manipulacije sovražnih entitet. Občutljivost na različne vrste napadov naj bodo podrobno opisane. Če lahko napadalec z napadom rezultat vrednotenja zaupanja spremeni v svoj prid, metrika ne opravlja svoje vloge.

- *uporabnost metrike* pri praktičnem vrednotenju zaupanja;

VI. *upoštevanje vseh pomembnih podatkov*:
Uporabnost metrike ne sme biti odvisna od skrivanja za določanje zaupanja pomembnih odločitev od uporabnika. Izjema so le odločitve, ki jih lahko avtomatiziramo z determinističnimi in intuitivnimi pravili.

VII. *učinkovitost*:
Izračun metrike mora biti učinkovit.

VIII. *smiselno obnašanje pri pomanjkljivih podatkih*:
Rezultat modela pri nepopolnih vhodnih podatkih mora biti smiseln. Običajno bo težko ali celo nemogoče pridobiti vse podatke, ki so pomembni za gradnjo zaupanja. Gradnja zaupanja se bo skoraj zagotovo izvajala le nad podmnožici podatkov, ki so v določenem času na voljo.

IX. *monotonost*:
Pomembna dodatna lastnost je *monotonost* modela. Z dodajanjem podatkov naj se zaupanje ne zmanjšuje. Za popolnost definicije je potrebno upoštevati še preklicane certifikate in certifikate, ki vsebujejo nasprotujoče si informacije.

3. MODEL INFRASTRUKTURE JAVNEGA KLJUČA

Gradniki modela

V predstavljenem modelu je infrastruktura javnega ključa sestavljena iz heterogenih delov, ki lahko izdajajo, shranjujejo in razdeljujejo podatke, povezane z entitetami. Videti je kot porazdeljena baza podatkov o certifikatih in podatkih, ki certifikate dopolnjujejo (na primer seznami preklicanih certifikatov, priporočila). Infrastruktura

omogoča uporabniku, da pride do podatkov, oziroma da dodaja podatke v infrastrukturo (izdaja priporočila, certifikate). Dodane informacije so koristne le za entitete, ki izdajatelju zaupajo, oziroma lahko v izjave zgradijo zaupanje. Za ostale nimajo uporabne vrednosti.

Priporočila, izjave o zaupanju in pristnosti javnega ključa

Kot smo omenili, model poleg certifikatov predvideva še obstoj izjav, ki jih v obstoječih infrastrukturah javnega ključa ne zasledimo. Pojem *priporočila* je prenesen iz realnega sveta. Nemogoče je poznati vse ljudi, s katerimi se srečujemo in jim moramo zaupati. Tedaj se zanašamo na priporočila. Lahko so implicitna ali eksplicitna. Uporabnik infrastrukture natančno določi uporabo priporočil pri gradnji zaupanja v javni ključ entitete. V našem primeru si priporočilo predstavljamo kot podpisano izjavo izdajatelja o zaupanju v entiteto, da je primerna za izvajanje določene akcije. Podobna je certifikatu. Od certifikata javnega ključa se razlikuje v tem, da je vsebina lahko zaupne narave in jo moramo ustrezno varovati. Priporočila so tudi kompleksnejša kot certifikati. V okviru modela infrastrukture javnega ključa definiramo več stopenj priporočil:

I. *Priporočilo prvega reda* priporoča entiteto, ki je vredna zaupanja za overjanje javnih ključev.

II. *Priporočila drugega reda* naštevajo entitete, ki jim lahko zaupamo pri priporočanju drugih entitet za overjanje javnih ključev.

III. *Priporočilo i-tega reda* govori o entiteti, ki je vredna zaupanja za izdajanje priporočil reda i-1.

V takem pojmovanju certifikat javnega ključa predstavlja priporočilo ničtega reda. Ker zaupanje zelo hitro plahni po nivojih priporočil, je smiselno uporabljati le majhno število nivojev. V našem modelu bomo privzeli, da priporočilo i-tega reda obsega tudi vsa priporočila nižjega reda.

Podobno definiramo *izjavo o zaupanju*. Predstavlja prepričanje uporabnika, da je entiteta primerna (merodajna) za izvajanje določenega tipa akcij.

I. *Zaupanje prvega reda* v entiteto pomeni prepričanje uporabnika, da agencija vestno izvaja predpisane postopke pri overjanju javnih ključev entitet.

II. *Zaupanje drugega reda* predstavlja prepričanje, da je entiteta preudarna pri priporočanju drugih entitet za izvajanje dejavnosti certifikatne agencije.

Tudi tu je umestno opozorilo, da zaupanje plahni zelo hitro, zato naj dober model uporablja le majhno število nivojev.

Razlika med priporočilom in izjavo o zaupanju je, da je slednja največkrat določena že v varnostni politiki sistema, priporočilo pa uporabnik dobi iz infrastrukture. Za zaščito pred napadi na model, kot bomo spoznali v šestem razdelku tega poglavja,

mora biti izjava o zaupanju dobro varovana skrivnost. Priporočila pomagajo le pri gradnji zaupanja, uporabnik jih ni obvezen upoštevati. Pri formalni definiciji modela (v četrtem razdelku poglavja) bomo prikazali pretvorbo priporočila v izjavo o zaupanju.

Izjava o pristnosti javnega ključa predstavlja prepričanje uporabnika, da javni ključ resnično pripada entiteti. Pravimo, da je kopija javnega ključa entitete *pristna*. Kako uporabnik pridobi pristni javni ključ, ne bo predmet obravnave. Običajno je to zapisano v lokalni varnostni politiki sistema.

Izjave lahko ločujemo tudi glede na način pridobivanja. Uporabnik glede na akcijo, ki jo entiteta želi izvesti, določi začetne izjave o zaupanju in pristne javne ključe. Običajno so slednje že določene v varnostni politiki za nameravano akcijo oziroma vir, do katerega entiteta dostopa. Način pridobitve pristnih kopij javnih ključev entitet (agencij) ne bo predmet obravnave in je običajno določen v lokalni varnostni politiki sistema. To množico izjav imenujemo *začetni pogled* uporabnika na infrastrukturo. Vse ostale izjave skuša uporabnik pridobiti ali sam ali s pomočjo entitete iz infrastrukture. O tem, kdo naj pridobiva podatke, bomo podrobneje spregovorili v nadaljevanju.

Enostaven model infrastrukture javnega ključa

Predpogoj za varno komuniciranje je prepoznavanje entitete in izmenjava šifrirnih ključev. Postopek prepoznavanja in preverjanja pristnosti javnega ključa entitete razdelimo na naslednje korake:

I. zbiranje dokazil o identiteti entitete,

II. analiziranje zbranih podatkov,

III. sprejetje sklepa.

Prva in druga faza nista nujno neodvisni. Uporabnik certifikata lahko ob spoznanju, da za odločitev nima zadosti podatkov, začne podatke ponovno zbirati. Zbiranje podatkov je lahko izvedeno z dostopanjem do strežnikov, ki hranijo certifikate in z njimi povezane informacije, ali na osnovi avtomatičnega dogovarjanja, kjer entiteta (imetnik certifikata, odjemalec) zbira potrebne podatke. Razlog slednjega pristopa je predpostavka, da bo entiteta zbrane podatke lahko uporabljale tudi v bodočih transakcijah, zato je smiselno, da jih sama zbira in arhivira. Uporabnik certifikata (strežnik) je lahko močno obremenjen in bi z zbiranjem dokazil v procesu vrednotenja zaupanja le po nepotrebnem obremenjeval lastne vire, saj so zanj zbrana dokazila le trenutnega pomena. Uporabnik zbira/shranjuje dokazila le v primeru potrebe po preprečevanju tajenja izvedbe akcije s strani entitete.

Ali so zbrani podatki zadostno zagotovilo o identiteti entitete, pristnosti javnega ključa in ali je entiteta primerna za izvajanje zahtevane akcije, je odvisno od cele vrste parametrov. Določi jih uporabnik glede na varnostno politiko sistema in vrsto akcije, ki jo namerava entiteta izvesti.

Preverjanje identitete in pripadnosti javnega ključa entiteti, ki je pogoj za izvedbo akcije, lahko izvedemo s pomočjo infrastrukture javnega ključa. Kot smo že omenili, je digitalni certifikat javnega ključa digitalno podpisana podatkovna struktura, ki jo izda certifikatna agencija in z njo potrjuje pripadnost para ključev entiteti. Za uporabnika je certifikat uporaben le, če so izpolnjene naslednje zahteve:

I. Uporabnik pozna javni ključ agencije in je prepričan o njegovi pristnosti (slednje je potrebno za preverjanje digitalnega podpisa).

II. Uporabnik zaupa agenciji, da je pred izdajo certifikata temeljito preverila entiteto; tako identiteto kot posedovanje para ključev.

III. Certifikat je veljaven (ni bil preklican ali mu ni preteklo obdobje veljavnosti) in je bil izdan za namen, ustrezen akciji, ki jo namerava entiteta izvesti.

Če ne poznamo javnega ključa agencije, ki je certifikat izdala, je prvi korak za izpolnitev prvega pogoja, pridobitev certifikata, ki overja javni ključ certifikatne agencije. Postopek ponavljamo in tako gradimo verigo certifikatov, dokler ne pridemo do agencije, ki ji zaupamo in imamo njen pristni javni ključ. Veriga certifikatov je za uporabnika certifikata uporabna le, če zaupamo vsaki entiteti v verigi in so vsi certifikati v verigi veljavni.

V preprostem modelu je graditev zaupanja v javni ključ entitete izveden z verigo certifikatov. Prvemu členu (agenciji) v verigi zaupamo in imamo njegov pristni javni ključ. Vsak sledeč člen verige je overjen s strani predhodnika in ima uporabnik zaupanje vanj. Zadnji člen v verigi je entiteta, katere javni ključ preverjamo. Zaupanje je v enostavnem modelu tranzitivno, če le zaupamo prvemu členu v verigi.

Kompleksnejši model

Preverjanje pristnosti javnih ključev z uporabo certifikatov je relativno preprosto. Pogosto pa nas ne zanima samo pristnost javnega ključa in identiteta entitete. Noben proces prepoznavanja ni brez napak in nikomur ne zaupamo popolnoma. Zato želimo izjavam in entitetam prirediti *stopnjo zaupanja*. Stopnja zaupanja opisuje uporabnikovo videnje veljavnosti izjave oziroma vestnega izvajanja varnostnih postopkov entitete pri izdajanju izjav. Glede na stopnje zaupanja, ki jih pripišemo izjavam in entitetam, želimo ovrednotiti zaupanje v povezavo javni ključ - entiteta oziroma tveganje, kateremu smo izpostavljeni pri izvedbi akcije. Za uporabo modela v poslovnem svetu je zelo koristno zaupanje razširiti s podatkom o višini jamstva, ki ga nudi izdajatelj certifikata v primeru zlorabe našega zaupanja v certifikat.

Precej bolj prikrito je, kako naj vzpostavimo in razširjamo zaupanje, oziroma kako iz znanih podatkov zgradimo zaupanje v izjave ter ovrednotimo tveganje pri izvedbi akcije. Model je potrebno razširiti. Za doseganje večje natančnosti in realnosti modela vanj poleg certifikatov vključimo še priporočila, izjave o zaupanju in izjave o pristnosti javnega ključa entitete. Izjavam priredimo stopnje zaupanja. Z združevanjem več izjav povečujemo zaupanje v izjavo/entiteto.

Naravno je, da poizkušamo povečati stopnjo zaupanja v pristnost javnega ključa s preverjanjem več verig certifikatov. Več izjav združimo, da dobimo izjavo, ki ji bolj zaupamo. Združevati stopnje zaupanja izjav in verig certifikatov za doseganje večjega zaupanja je na videz preprosto, a v splošnem izjave/verige certifikatov niso neodvisne, kot smo spoznali v prvem podpoglavju petega poglavja.

Problem pri sprejemanju sklepov na podlagi zbranih podatkov je ugotavljanje odvisnosti med vhodnimi podatki. Razdelimo jih lahko na strukturne in korelacijske odvisnosti. Primer *strukturne odvisnosti* je prepletanje verig (kot smo spoznali v petem poglavju), kjer lahko preklic enega certifikata povzroči neveljavnost drugih verig. Kot primer *korelacijske odvisnosti* lahko navedemo entiteti, ki sta del iste organizacije (interesne skupine), tako njuna mera zaupanja ne more biti neodvisna. Število možnih odvisnosti eksponentno narašča s številom entitet. Korelacijsko odvisnost je zelo težko ugotoviti in obravnavati v modelu. Na splošno je odvisnosti težko ugotavljati in še težje izmeriti.

Varnostne politike

Varnostna politika predpisuje obnašanje entitet in ščitenje virov pri interakcijah z entitetami, ki ne pripadajo sistemu. Sestavljena je iz množice pravil, ki opisujejo grožnje, vire, ki jih je potrebno ščititi, in načinov zaščite. Viri v sistemu so običajno zaščiteni z mehanizmi za kontrolo dostopa. Mehanizmi določajo dostop do virov v sistemu in kontrolirajo načine dostopa. Osnovni elementi mehanizma za kontrolo dostopa so viri, entitete in pravice dostopa. Pravice dostopa predpisujejo dovoljene akcije entitete, pogoje, pod katerimi lahko entiteta dostopa do virov, in vrste operacij, ki jih lahko izvaja. Dodatno so lahko določeni tudi šifrirni postopki. Dober mehanizem za kontrolo dostopa mora podpirati preklic dovoljenj in izrecno prepoved dostopa entitete.

V porazdeljenih sistemih ločimo vsaj dve vrsti varnostnih politik, ki se pojavljajo pri varovanju porazdeljenih sistemov. Prva je politika, ki določa prirejanje stopnje zaupanja podatkom in entitetam iz infrastrukture. Druga je varnostna politika uporabnika, ki določa minimalno zahtevano mero zaupanja za izvedbo akcije ter maksimalno mero zaupanja, ki jo lahko določena izjava/entiteta dobi.

4. DETERMINISTIČNI MODEL INFRASTRUKTURE

V nadaljevanju bomo predstavili deterministični model infrastrukture javnega ključa. Mero zaupanja v izjave/entiteto bomo diskretizirali. Zavzemala bo le vrednosti 0 in 1 (ali uporabnik izjavi zaupa ali ne). Motiv za odločitev je dejstvo, da je težko določiti postopek, ki bi na smiseln in učinkovit način izjavam prirejal zvezne mere zaupanja. V prid slednji ugotovitvi govori tudi dejstvo, da se večina predlaganih modelov, ki uporabljajo zvezno mero za zaupanje, (Maurer [40], Beth et al. [5]) izogne obravnavi, kako izjavam določati stopnjo zaupanja, oziroma so predlagani postopki zapleteni. Za uporabnika so dobljene stopnje zaupanja preveč abstraktne, rezultati pa brez dodatne interpretacije neuporabni. Tako smo bistveno poenostavili odločanje o zaupanju. Menimo, da je tako model enostavnejši in preglednejši za uporabo. Izognili smo se

zapletenemu izračunu zaupanja in ranljivosti za napade, ki so jim podvrženi ostali modeli (Reiter, Stubblebine [51], [50], Maurer [40]).

Dodatno smo v model uvedli *parametre izjav*. Slednje natančneje opredeljujejo okoliščine, v katerih uporabnik sprejema izjavo kot veljavno oziroma primernost entitete za izvedbo akcije. Uporabniku je omogočena natančnejša kontrola tveganja in gradnja zaupanja. Parameter lahko določa, do katere vrednosti transakcije smo pripravljeni zaupati agenciji oziroma za kakšen namen uporabe zaupamo certifikatom, ki jih agencija izdaja. Prav tako lahko certifikatom priredimo parameter, ki opisuje vrednost, do katere izdajatelj jamči za pravilnost atributov v certifikatu, in primerno obnašanje imetnika certifikata. Menimo, da je parametrizacija problema bolj naravna in enostavneje določljiva, saj nudi uporabniku globlji vpogled v posledice odločitev v primeru sprejetja akcije.

S tako zasnovo modela nameravamo doseči enostavnost in učinkovitost izračuna. Model za izračun uporablja le preprosta izpeljevalna pravila, za določitev minimalne višine jamstva pa algoritem maksimalnega pretoka v grafu (Ford, Fulkerson [22]). Rezultati modela so uporabni brez dodatnih interpretacij. Model sprejme javni ključ entitete kot pristen in primeren za izvedbo transakcije ali pa izvedbo transakcije (pristnost ključa) zavrne. Kot dodatno informacijo model vrne še minimalno višino zavarovanja transakcije. Slednja je v primeru uporabe modela v poslovnem svetu gotovo najustreznejša metrika.

Model kot elemente, s pomočjo katerih poizkuša zgraditi zaupanje, uporablja izjave o pristnosti javnega ključa, izjave o zaupanju entitetam, priporočila in certifikate. Predpostavimo lahko, da bo entiteta ob vstopu v infrastrukturo javnega ključa dobila začetno množico izjav, katerim bo brezpogojno zaupala. Tak primer je javni ključ agencije, ki je overila njen javni ključ, izjave o zaupanju korenske agencije drugim agencijam... Ostale bo določila v skladu s svojo varnostno politiko (glede na zaupanje agencijam, da skrbno preverjajo entitete pred izdajo certifikatov). Ob interakciji z ostalimi entitetami v infrastrukturi se bo množica dinamično povečevala (pridobivamo nova priporočila, zgradimo zaupanje v entiteto) oziroma zmanjševala (izjave zapadejo, so preklicane, pride do prekinitve pogodbenih odnosov, z entiteto imamo slabe izkušnje).

Eden izmed temeljnih predpogojev za upravljanje z zaupanjem je koncizen zapis varnostne politike sistema. Da je slednja uporabna, mora biti zapisana jasno, enostavno in zgoščeno. Čeprav se zdijo zahteve med seboj nasprotujoče, bomo prikazali način, ki bi na optimalen način zadostil vsem kriterijem. Cilj je omogočiti vsakemu uporabniku, da si na podlagi svoje predstave, katere dejavnosti so z njegovega stališča varne in dopustne, določi varnostno politiko pri interakcijah z entitetami v sistemu. Zapisu bo omogočal avtomatično gradnjo začetnega pogleda uporabnika.

Poseben problem pri gradnji zaupanja v javni ključ podpisnika je vprašanje, kdo zbira potrebne podatke. Menimo, da na to vprašanje ni mogoče enostavno odgovoriti. Potrebno je upoštevati okolje, v katerem potekajo transakcije, varnostne zahteve, upoštevati, ali imajo entitete na voljo proste zmogljivosti za pridobivanje podatkov ter potrebo entitet, da arhivirajo informacije za preprečevanje tajenja izvedenih akcij.

Pri gradnji modela se bomo soočili s problemom gradnje verig certifikatov in ugotavljanja statusa certifikatov. Osrednji problem obstoječih infrastruktur javnega ključa predstavlja mehanizem za ugotavljanje statusa certifikata (kot smo spoznali v petem poglavju). Trenutno še ni rešitve, ki bi zadostila tako zahtevam po ažurnosti in svežini informacij o statusu certifikata. Po predvidevanjih MITRE [4] bo ob globalizaciji infrastruktur javnega ključa večina stroškov upravljanja posledica vzdrževanja mehanizmov za preklic certifikatov. Pozornost bomo namenili tudi pomenu preklica certifikata, saj se nobeden izmed trenutno predlaganih standardov temu ne posveča v zadostni meri. V povezavi s pomenom preklica bomo obravnavali gradnjo vzporednih verig certifikatov. Podali bomo predlog, kako nedvoumno odkrivati vzporedne verige in v njih skrite pasti (prvi razdelek petega poglavja).

Pri reševanju problemov si bomo bolj kot z dovršenimi postopki pomagali s tehnologijo, ki je na voljo, in organizacijo infrastrukture. Poudarek bo na uporabi pametnih kartic kot potencialno zelo obetajoče in še premalo izkoriščene tehnologije v infrastrukturah javnega ključa. V četrtem poglavju smo spoznali vse potencialne prednosti uporabe pametnih kartic za hranjenje certifikatov in zasebnih ključev uporabnika. V okviru predlaganega modela bomo ocenili, katere izmed potencialnih prednosti pridejo resnično do izraza.

Ker smo prepričani, da ni univerzalnega modela, ki bi zadostil vsem kriterijem, si bomo predlagani model ogledali v okoljih, ki po našem mnenju trenutno prevladujejo; to je spletna trgovina, intranet. Za posamezna okolja bomo predlagali, kako najbolj učinkovito razrešiti zgoraj naštete dileme za varno uporabo infrastrukture javnega ključa.

Ko bo model zgrajen in bodo odgovori na odprta vprašanja, ki smo jih našteli, znana, bomo poizkusili model prenesti v realno okolje. Pri tem se bomo oprli na certifikate po priporočilu X.509 [28]. Vodila nas bo želja, da bi v čim večji meri ostali znotraj priporočila in rešitve implementirali z mehanizmi, ki so na voljo.

Formalna definicija modela

Preden model formalno opišemo, na hitro očrtajmo osnovne ideje in predstavimo terminologijo. Osnova za razširitev modela je Maurer-jev [40] predlog. Sintaksa je preprosta. *Izjave* so preprosti izrazi in se pojavljajo v eni od štirih oblik: pristnost javnega ključa entitete, izjava zaupanja v entiteto, digitalni certifikat javnega ključa in priporočilo. Sintaksa ne vsebuje niti Boolovih operatorjev niti eksistenčnih oziroma univerzalnih kvantifikatorjev. Semantika temelji na dveh *pravilih izpeljave*: pravilo za določanje pristnosti javnega ključa in pravilo za izpeljavo zaupanja. S pomočjo pravil izpeljujemo nove izjave na podlagi že obstoječe množice izjav, za katere verjamemo, da so pravilne.

Izjave *vrednotimo* z merama veljavno ali neveljavno. Izjava je veljavna, če in samo če jo lahko izpeljemo iz aksiomov. Neveljavna izjava ni nujno napačna (lažna), a četudi je resnična, nimamo dokazov za to.

Množico aksiomov modela sestavljajo izjave (o pristnosti javnega ključa, o zaupanju v entiteto), za katere menimo, da so resnične. Množico aksiomov imenujemo *začetni*

pogled. Izpeljani pogled je množica izjav, ki smo jih izpeljali iz aksiomov z uporabo izpeljevalnih pravil.

Začetni pogled zgradimo iz izjav, ki so pomembne v kontekstu preverjanja pristnosti javnega ključa entitete in gradnje zaupanja pred izvedbo akcije. Najdemo jih v varnostni politiki in so določene z varnostnimi mehanizmi za akcijo oziroma vir, do katerega entiteta dostopa. Če nimamo na voljo drugih izjav, pogled na infrastrukturo javnega ključa razširjamo le na podlagi začetnega pogleda. To so izjave, za katere menimo, da so veljavne (pristnost javnih ključev, izjave zaupanje v entitete, ki smo jih dobili iz varnostne politike). Izjave, ki smo jih dobili od drugih entitet (certifikate javnega ključa, priporočila) imenujemo *domneve* oziroma *trditve.*

Grafično bomo pogled predstavili v obliki usmerjenega grafa. Izjave oziroma domneve bomo predstavili kot usmerjene povezave v grafu, kjer vozlišča predstavljajo entitete. Graf predstavlja mrežo certifikatov, zaupanja, pristnih javnih ključev in priporočil, ki so nam na voljo pri odločanju.

Zaupanje v pristnost javnega ključa in izjavo o zaupanju za izvajanje posamezne akcije bomo predstavili s polno usmerjeno povezavo od uporabnika certifikata do podpisnika. Črtkasta usmerjena povezava povezuje izdajatelja priporočila (certifikata) in entiteto. Ker predvidevamo nekaj stopenj zaupanja in priporočil, bomo povezave ustrezno označili z rimskimi številkami.

V nadaljevanju bomo privzeli sledečo notacijo. Uporabnika certifikata bomo označevali z A, podpisnika, entiteto, ki je inicirala akcijo, z B, certifikatne agencije pa z X, Y, Z, W.

Strnimo vse do sedaj povedano. Za lažje opis delovanje modela na začetku ne bomo vključili parametrov izjav.

> **Definicija I.** *Pogled* je množica izjav, za katere uporabnik verjame, da so veljavne. *Začetni pogled* odraža uporabnikovo začetno prepričanje o veljavnih izjavah in je običajno določeno z varnostno politiko sistema. Vsebuje izjave o pristnosti javnih ključev in izjave o zaupanju. Je osnova, iz katere lahko z uporabo izpeljevalnih pravil zgradimo zaupanje v nove izjave.

Začetni pogled vsebuje izjave, za katere uporabnik meni, da so v njegovem kontekstu in glede na predlagano akcijo veljavne in jim lahko zaupa. Dejstvo, da je izjava vsebovana v začetnem pogledu, še ne pomeni, da je veljavna v absolutnem smislu. Pomeni le, da je v uporabnikovem kontekstu taka predpostavka upravičena. Ravno tako izvzetost izjave iz začetnega pogleda še ne pomeni, da je neveljavna, morda se uporabniku le ne zdi pomembna.

Množico izjav, ki sestavljajo začetni pogled, bomo označevali z zavitimi oklepaji in z oznako $View_A$. Domneve, pridobljene iz infrastrukture, bodo v okroglih oklepajih. Izjave, ki jih podtakne napadalec, pa v lomljenih oklepajih.

Definicija II. Imamo sledeče vrste izjav:

- *Pristnost javnega ključa* ($Auth_{A,X}$) označuje naše **prepričanje**, da je določen javni ključ E_x pristen (pripada entiteti X). Grafično ga prikažemo kot povezavo od A do X: A ⟶ X.

- *Zaupanje* ($Trust_{A,X,1}$) označuje naše **prepričanje**, da je določena entiteta X vredna zaupanja za izdajanje certifikatov. Podobno je naše prepričanje, da je entiteta X vredna zaupanja za izdajanje priporočil reda i, označeno kot $Trust_{A,X,i}$. Simbolično to prikažemo z A $\xrightarrow{i}$ X.

- *Certifikati* ($Cert_{X,Y}$) označujejo dejstvo, da imamo certifikat javnega ključa entitete Y, ki ga je **domnevno** izdala in podpisala agencija X. Prislov 'domnevno' izraža dejstvo, da brez dodatnega preverjanja ne zaupamo, da je certifikat dejansko izdala entiteta X. Grafično prikaz je X ⇢ Y.

- *Priporočila* ($Rec_{X,Y,i}$) označuje dejstvo, da imamo priporočilo i-tega reda za entiteto Y, ki ga je **domnevno** izdala in podpisala entiteta X. Označba je X $\overset{i}{\dashrightarrow}$ Y.

Omeniti velja, da lahko pristnost ključa tolmačimo kot poseben primer certifikata, na primer kot certifikat, podpisan z našim zasebni ključem (ki mu neomajno zaupamo). Podobno lahko izjavo zaupanja tolmačimo kot poseben tip priporočila, ki ga sami izdamo.

Zapišimo sedaj pravila za izpeljavo novih izjav iz že obstoječih. Izpeljane izjave/sklepi govorijo o pristnosti javnega ključa ali o zaupanju entiteti za izvajanje določenih akcij. Cilj modela je izpeljati izjavo, ki označuje zaupanje v pristnost javnega ključa podpisnika sporočila, pobudnika akcije.

Definicija III. Izjava je veljavna, če in samo če je vsebovana v začetnem pogledu $View_A$, oziroma jo lahko izpeljemo iz začetnega pogleda z uporabo spodnjih pravil.

$$\forall X, Y : Auth_{A,X}, Trust_{A,X,1}, Cert_{X,Y} \Rightarrow Auth_{A,Y} \qquad (1)$$

in

$$\forall X, Y, i \geq 1 : Auth_{A,X}, \mathrm{Trust}_{A,X,i+1}, \mathrm{Rec}_{X,Y,i} \Rightarrow Trust_{A,Y,i} \qquad (2)$$

Z $View_A$' označimo *zaprtje množice* $View_A$ za pravila (1), (2). To je množica izjav, izpeljanih z uporabo pravil iz $View_A$. Izjava S je *veljavna* le, če pripada množici $View_A$'.

Prvo izpeljevalno pravilo govori o izpeljevanju zaupanja v pristnost javnih ključev. Trdi, da A lahko izpelje pristnost javnega ključa Y (ga vključi v razširjen pogled, zaprtje), če ima pristni javni ključ entitete X, izdajatelja certifikata, izjavo o zaupanju prvega reda v entiteto X in certifikat javnega ključa Y, ki ga je izdal X.

Drugo pravilo izpeljuje izjave, ki se nanašajo na zaupanje. Če ima A zaupanje reda i+1 v X in pristno kopijo javnega ključa X-a ter priporočilo X-a reda i za entiteto Y, potem lahko sklepa o zaupanju (mu zaupa) reda i v entiteto Y.

Zaupanje v pristnost javnega ključa entitete B je vzpostavljeno, ko se izjava $Auth_{A,B}$ nahaja med izjavami v razširjenem pogled $View_A'$, ki smo ga izpeljali iz začetnega pogleda na infrastrukturo s pomočjo izpeljevalnih pravil (zaprtje začetnega pogleda).

Privzeli bomo, da zaupanje oziroma priporočilo reda i obsega tudi zaupanja (priporočila) nižjih redov. Pravilo ni del modela, je intuitivne narave in za sam model ni bistveno. Po kratkem premisleku uvidimo, da nima pomena entiteti določati reda zaupanja I in III, ne pa tudi reda II. Formalno bi to izrazili kot:

$$\forall X, Y; 1 \le k < i : Trust_{A,X,i} \Rightarrow Trust_{A,X,k} \qquad (3)$$

in

$$\forall X, Y; 1 \le k < i : \mathrm{Re}c_{A,X,i} \Rightarrow \mathrm{Re}c_{A,X,k} \qquad (4)$$

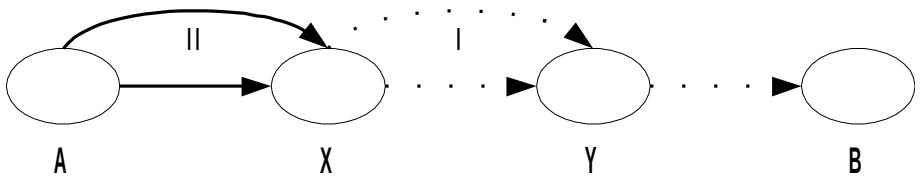
Oglejmo si število korakov, ki so potrebni, da model vrne odgovor. Brez izgube splošnosti privzemimo, da obstaja ena sama pot med A in B. Hitro uvidimo, da v končno mnogo korakih pridemo do izjave o zaupanju v javni ključ entitete ali pa da ne moremo več uporabiti izpeljevalnih pravil. Za vsak korak po poti potrebujemo eno ali dve uporabi izpeljevalnih pravil. Slednje velja v primeru, ko moramo najprej zgraditi zaupanje v entiteto in nato še zaupanje v pristnost njenega javnega ključa. Za vsako uporabo pravila potrebujemo tri ustrezne izjave. Ko naredimo po poti korak naprej (imamo zaupanje v sledeče vozlišče in njen pristni ključ), postanejo vse povezave, ki se končujejo v predhodnem vozlišču, nepomembne. Enako velja za povezavi (priporočilo in certifikat), kateri imata ponor v novem vozlišču. Torej smo pridobili dve novi izjavi in hkrati črtali štiri izjave. Razmišljanje se na naslednjem koraku ponovi. Naravno je, da je množica začetnih izjav končna.

Kot zanimivost si poglejmo primer, ko infrastruktura javnega ključa ne vsebuje priporočil (na primer certifikati po priporočilu X.509 [28]). Tedaj je uporabno le pravilo za izpeljavo (1). Postavljeni model dobro deluje tudi v obstoječih infrastrukturah javnega ključa. Uporabnik mora zaupati vsaki entiteti na poti in imeti pristni javni ključ prve agencije v verigi ter certifikate vseh ostalih entitet na poti.

Zgledi uporabe modela

V nadaljevanju si poglejmo dva primera uporabe modela. Služila nam bosta za prikaz delovanja modela in v oporo pri razširitvi funkcionalnosti in pri ocenjevanju ranljivosti modela v nadaljevanju.

Primer 1:



Slika 6.1: Model infrastrukture javnega ključa za primer 1.

Zgradili smo si graf zaupanja, prikazano na sliki 6.1, skupaj z dodatnimi priporočili in izjavami o zaupanju. Naš začetni pogled na infrastrukturo javnega ključa je:

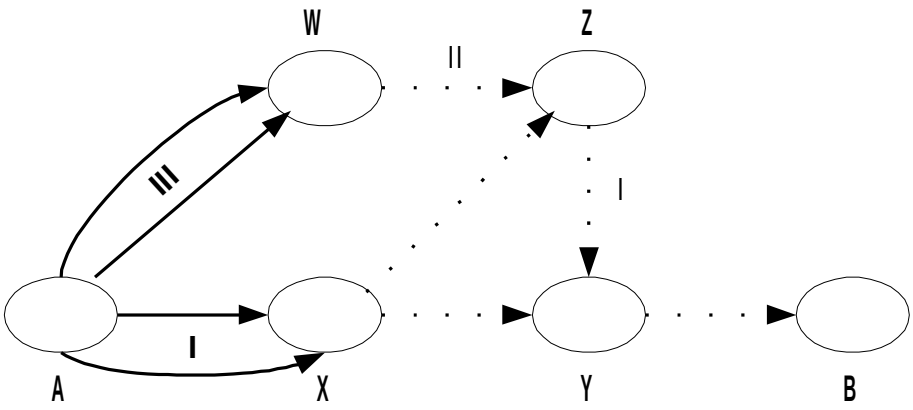
$$View_A = \{Auth_{A,X}, Trust_{A,X,2}\};\ (\mathrm{Re}c_{X,Y,1}, Cert_{X,Y}, Cert_{Y,B})$$

Začetni pogled vsebuje pristni javni ključ certifikatne agencije X in zaupanje, da X izdaja zaupanja vredna priporočila entitetam, ki izdajajo certifikate. Poleg tega imamo na voljo še par certifikatov, katera sta domnevno izdali certifikatni agenciji X oziroma Y, in priporočilo prvega reda, ki ga je X izdala entiteti Y. Zaupanje v pristnost javnega ključa entitete B lahko izpeljemo s pomočjo sledečih korakov:

$$Auht_{A.X}, Trust_{A,X,2}, \mathrm{Re}c_{X,Y,1} \Rightarrow Trust_{A,Y,1}$$
$$Auth_{A,X}, Trust_{A,X,1}, Cert_{X,Y} \Rightarrow Auth_{A,Y}$$
$$Auth_{A,Y}, Trust_{A,Y,1}, Cert_{Y,B} \Rightarrow Auth_{A,B}$$

Primer 2: Začetni pogled na model je sledeč:

$$View_A = \{Auth_{A,X}, Auth_{A,W}, Trust_{A,X,1}, Trust_{A,W,3}\};\ (\mathrm{Re}c_{W,Z,2}, \mathrm{Re}c$$



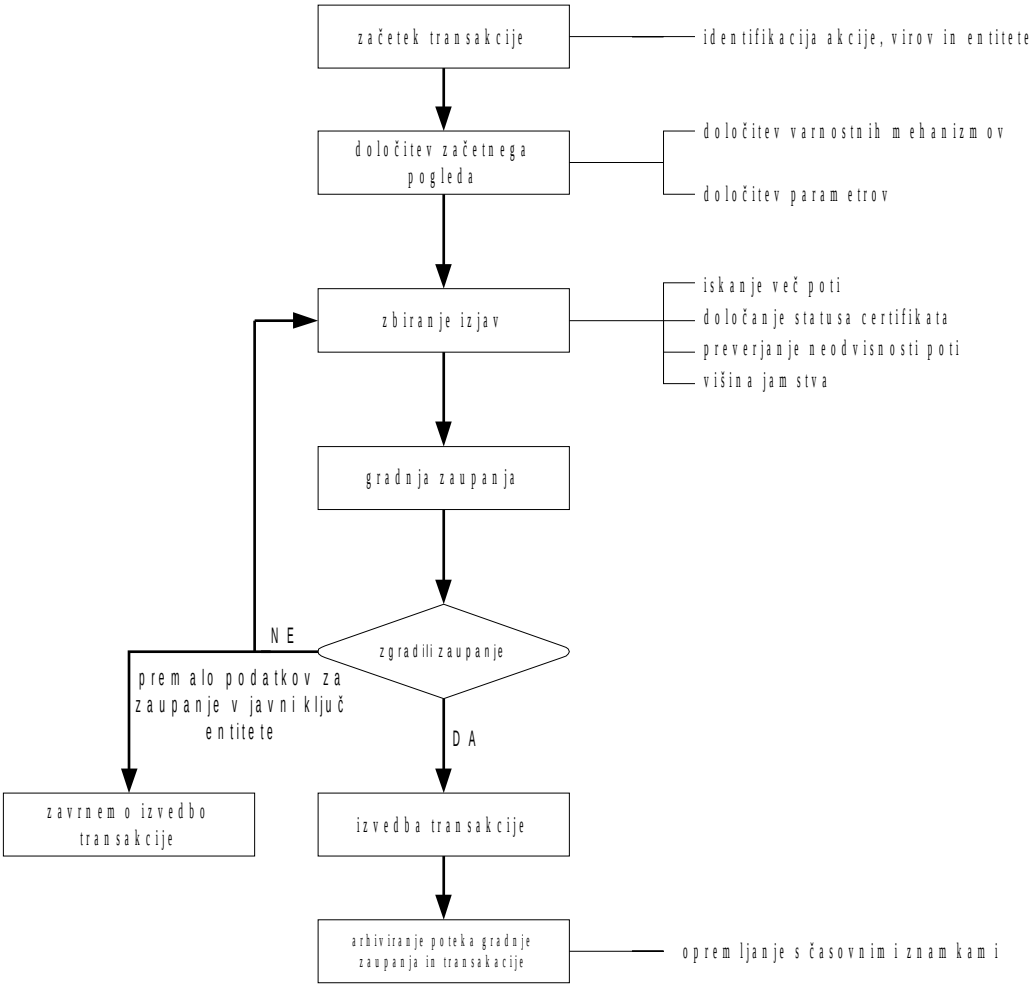
Slika 6.2: Model infrastrukture za primer 2.

$$Auth_{A,X}, Trust_{A,X,1}, Cert_{X,Z} \Rightarrow Auth_{A,Z}$$
$$Auth_{A,X}, Trust_{A,X,1}, Cert_{X,Y} \Rightarrow Auth_{A,Y}$$
$$Auth_{A,W}, Trust_{A,W,3}, \mathrm{Re}\, c_{W,Z,2} \Rightarrow Trust_{A,Z,2}$$
$$Auth_{A,Z}, Trust_{A,Z,2}, \mathrm{Re}\, c_{Z,Y,1} \Rightarrow Trust_{A,Y,1}$$
$$Auth_{A,Y}, Trust_{A,Y,1}, Cert_{Y,B} \Rightarrow Auth_{A,B}$$

Na splošno *View*$_A$' vsebuje več izjav kot je potrebno, da pridemo do ustreznega sklepa. Primer ilustrira, da lahko priporočila in certifikate izdajamo neodvisno. Entiteta lahko priporoča drugo entiteto, katere javnega ključa sploh ne pozna. Izdaja certifikata zahteva preverjanje pristnosti javnega ključa, ki ga certificiramo. Nasprotno pa izdaja priporočila ne zahteva izmenjave podatkov z entiteto.

V primeru, ko ne moremo izpeljati *Auth*$_{A,B}$, lahko z razširitvijo pogleda s pridobivanjem novih certifikatov, priporočil, z določanjem novih zaupanja vrednih entitet in z overjanjem javnih ključev poizkušamo izpeljati zaupanje v javni ključ entitete.

Predstavljeni primeri prikazujejo delovanje modela ter gradnjo zaupanja. Model še zdaleč ni popoln in uporaben za resnično gradnjo zaupanja v javni ključ entitete. Predstavljeno orodje bomo v nadaljevanju razširili. Ogledali si bomo korake gradnje grafa, določanja začetnega pogleda, zbiranja domnev, ki naj v končni fazi omogočijo ovrednotenje zaupanja. Za pomoč pri gradnji si postavimo diagram poteka:



Slika 6.3: Diagram poteka za izgradnjo zaupanja v javni ključ entitete.

5. POSTOPEK GRADNJE ZAUPANJA

Določitev začetnega pogleda

Uporabnik zgradi začetni pogled, ko identificira odjemalca, njegov certifikat (javni ključ), vir, do katerega dostopa, ter vrsto akcije, ki jo kani izvesti. Glede na vir in vrsto dostopa je v varnostni politiki opredeljeno, kdo in pod katerimi pogoji ima dostop do vira, ter vrste akcije, ki jih sme izvajati.

Zapis varnostne politike

Ker so v večini primerov varnostne politike sistema zapisane v naravnem jeziku, so za uporabnika nejasne in pogosto preobsežne. Iz njih je težko razbrati varnostne ukrepe in zahtevano stopnjo zaupanja za izvedbo akcije.

Zato bomo v našem model formalizirali zapis varnostne politike na način, ki omogoča avtomatičen način gradnje začetnega pogleda. Politika je predstavljena v obliki tabele. Za vsak vir, ki ga varujemo in vsako možno akcijo nad virom, imamo v preseku

stolpca in vrstice določeno vsebino začetnega pogleda. Varnostno politiko oziroma tabelo si zgradi vsak uporabnik sam. Le on pozna vire, dovoljene vrste dostopa, varnostne zahteve, potrebne za ohranjanje neokrnjenosti sistema, tveganje, ki ga je pripravljen sprejeti, in jamstva, ki jih zahteva. V primeru neukega uporabnika lahko tabelo zgradi strokovnjak na podlagi uporabnikovih zahtev o še sprejemljivem tveganju in stopnji varnosti, ki jo zahteva. Tabela naj bo varovana skrivnost, saj lahko iz nje napadalec razbere zaupanja uporabnika, oziroma podtika, briše ali spreminja izjave in parametre.

vir \ vrsta dostopa				
	...	...	$Auth_{A,X}(P\_purp)$	...
	...	$Auth_{A,X}, Trust_{A,X}$ $P\_trans\$, P\_level$	$P\_insur\$, P\_\#path$	$Auth_{A,X}, Trust_{A,X}(Px)$
	...	...	$No\_Trust_{A,X}$	...

Tabela 6.1: Formalni zapis varnostne politike.

Vsebina je različna glede na vrsto vira, nameravane akcije in način varovanja. Običajno vsebuje seznam pristnih javnih ključev in izjave o zaupanju entitetam. Poudarek je na *pozitivnih izjavah*. Izjava mora jasno povedati, kaj kdo sme in pod kakšnimi pogoji. Dodatne izjave, ki jih hranimo, so negativna potrdila (Not_Trust). Slednje izrecno prepovedujejo dostop entitetam, katerim na podlagi preteklih izkušenj ne zaupamo. Trenutno nobena obstoječa infrastruktura javnega ključa ne podpira negativnih certifikatov, ki bi pričali o prepovedih. Malo verjetno je, da bi entiteta predložila tovrstni certifikat, čeprav je s pomočjo pametnih kartic to mogoče izvesti (četrto poglavje, drugi razdelek).

Poleg izjav tabela vsebuje tudi *parametre*. Parametri podrobneje določajo zahteve, ki jih mora entiteta izpolnjevati. Omogočajo natančnejše določanje tveganja, ki ga je uporabnik pripravljen sprejeti, in jamstva, ki jih uporabnik zahteva za izvedbo akcije. Razdelimo jih na *parametre izjav* in *samostojne parametre* (parametre vira). Primeri možnih parametrov izjav so višina jamstva, ki ga jamči agencija ob zlorabi certifikata, namen uporabe pristnega javnega ključa (digitalni podpis, šifriranje, prepoznavanje...), primeri samostojnih parametrov pa maksimalna vrednost transakcije, maksimalni red zaupanja, ki ga lahko uporabimo pri graditvi zaupanja, število ločenih poti. Dodatno lahko parameter zahteva, da entiteta predloži potrdilo o nerazkritju javnega ključa ali pred kratkim izdan certifikat. Množica parametrov je močno odvisna od vira in vrste zaščite.

Predstavitev izjav

Izjave in parametri v varnostni politiki morajo biti za učinkovito uporabo in zaščito primerno predstavljeni. Zaupanje v entiteto predstavimo kot poseben certifikat, podpisan z uporabnikovim zasebnim ključem. Vsebuje naziv entitete, obdobje veljavnosti in parametre, ki jih določi uporabnik. Ker smo privzeli, da izjava zaupanja implicira tudi zaupanja nižjih redov, lahko vsebuje tudi javni ključ entitet. Izjavo o pristnosti javnega ključa predstavimo kot zaupanje ničtega reda. Poleg ostalih polj mora vsebovati vsaj še javni ključ entitete, predviden namen uporabe in obdobje veljavnosti. Tudi predstavitev priporočila je podobna. Predstavljena je kot certifikat, ki ga izda entiteta in poleg vseh običajnih polj vsebuje še vrsto in red priporočila ter parametre izjave. Uporabnik jim glede na izdajatelja priredi še dodatne parametre.

Kot smo že omenili, je potrebno varovati zaupnost in neokrnjenost izjav med prenosom in hranjenjem v računalniku. Izjave zaupanja in pristnosti javnega ključa so varovane z zasebnim ključem uporabnika. Če ni prišlo do razkritja ključa, jih je potrebno varovati le pred izbrisom iz tabele in vpogledom drugih entitet. Ker zaupanje ni absolutno, je potrebno pred uporabo preveriti obdobje veljavnosti izjav o zaupanju in pristnosti javnega ključa. Priporočila so z varnostnega vidika zelo podobna certifikatom, njihovo neokrnjenost varuje digitalni podpis izdajatelja. Potrebno je varovati njihovo zaupnost med prenosom. Pred uporabo priporočila je potrebno preveriti, ali so bila preklicana, so zapadla, oziroma ali je bil razkrit zasebni ključ izdajatelja. Zaupnost in neokrnjenost parametrov vira prav tako varujemo z zasebnim ključem uporabnika.

Po izgradnji začetnega pogleda, ki se lahko izvede popolnoma avtomatsko, začnemo z zbiranjem podatkov in gradnjo zaupanja v javni ključ entitete. Ponovno je potrebno poudariti, da lahko uporabnik z določanjem vsebine tabele sam določa stopnjo tveganja, ki ga je pripravljen prevzeti.

Zbiranje podatkov

Ko je začetni pogled določen, lahko začnemo z gradnjo zaupanja v javni ključ entitete. Malo verjetno je, da bomo zaupanje tudi zgradili. Potrebno je pridobiti še dodatne izjave, ki nam bodo izgradnjo omogočile. Tako se postavljajo vprašanja, kdo naj zbira podatke in katere.

Odgovor o zbiralcu podatkov je zelo odvisen od okolja, kjer se izvajajo aktivnosti. Kot bomo na koncu poglavja prikazali na primeru dveh okoljih uporabe infrastrukture javnega ključa, je odločitev pogojena z obremenjenostjo entitet. Pomembno je tudi ali so podatki za entiteto uporabni le v okviru tekoče transakcije ali pa jih bodo lahko uporabile tudi v drugih transakcijah. Prav tako je potrebno upoštevati zahteve po arhiviranju podatkov. Podrobneje smo se s temi vprašanji ukvarjali v tretjem in petem poglavju.

Tudi pri določanju, katere podatke zbirati, ni enostavnega odgovora. Zagotovo je potrebno za uspešno gradnjo zaupanja zbrati križne certifikate agencij in priporočila. Ne smemo zanemariti primera, ko ima entiteta več certifikatov/priporočil za različne namene, izdane pri različnih agencijah. Natančno moramo določiti

certifikat/priporočilo, izdajatelja ter predviden namen uporabe. Zgraditi je potrebno verigo križnih certifikatov od agencije (lahko jih je tudi več), ki jim uporabnik certifikata zaupa in so navedene v začetnem pogledu, pa do agencije, ki je overila javni ključ entitete. Za večjo odpornost modela na napade je dobro, da zbrani certifikati tvorijo več ločenih poti. Prav tako je potrebno za vse zbrane izjave preveriti status in višino jamstva, ki ga izdajatelj nudi. Torej moramo hkrati zbirati še sezname preklicanih certifikatov oziroma opravljati poizvedbe o statusu certifikatov in priporočil. Ne nazadnje moramo upoštevati tudi interakcijo verig certifikatov, kot smo to spoznali v petem poglavju.

Graditev verige certifikatov

Vsi algoritmi za preverjanje pristnosti javnih ključev, tako tisti v priporočilu X.509 kot v informativnem standardu IETF-a [27], privzemajo, da je veriga certifikatov že zgrajena. V nam dostopni literaturi še nihče ni predlagal načina, kako učinkovito izvesti iskanje poti med dvema poljubnima certifikatnima agencijama. Glede na trende v razvoju infrastrukture javnega ključa globina modela zaupanja verjetno nikoli ne bo presegla tri do štiri nivoje (na primer globalni, državni, podjetje, izpostava podjetja). Kaže, da bo model zaupanja grafično najbolj podoben gozdu dreves z odlikovanimi vozlišči. Mnoge aplikacije in varnostni protokoli (na primer standard za varno uporabo elektronske pošte S/MIME, SSL [60], [58], certifikate že priložijo) nudijo uporabniku dodatno pomoč pri gradnji verige. Videti je, da zgraditev verige sama po sebi ne bi smela predstavljati nepremostljivega problema. A še vedno si lahko v najneugodnejšem primeru splošnega modela zaupanja predstavljamo situacijo, ko uporabnik pozna le certifikat entitete in zaupanja vrednih agencij.

Preverjanje statusa certifikata

Poleg certifikata potrebujemo še zagotovilo, da certifikat ni bil preklican pred iztekom njegove dobe veljavnosti. Mehanizem za ugotavljanje statusa certifikata je eden izmed najbolj perečih problemov pri gradnji in obratovanju infrastrukture. Zagotoviti mora ažurnost informacij in ustrezno kvaliteto storitve. Tudi tu se postavlja vprašanje, kdo naj priskrbi potrdilo o veljavnosti certifikata. Podobno kot zgoraj lahko ugotovimo, da je slednje odvisno od okolja. Informacije naj pridobiva tisti, ki ima proste zmogljivosti in potrebuje podatke za arhiviranje v primeru tajenja izvedbe akcije.

Trenutno so v okviru organizacije IETF, delovne skupine PKIX, predlagana dva mehanizma za ugotavljanja statusa certifikata: mehanizem s seznamom preklicanih certifikatov (Housley et al. [27]) in priključno preverjanje (Myers et al. [45]). Obe rešitvi imata svoje slabosti in smo jih že obravnavali v petem poglavju.

Če ponovimo poglavitne pripombe glede seznama preklicanih certifikatov, so to nezmožnost uporabnika, da določa svežino informacije, visoki stroški upravljanja in razdeljevanja seznama, nezmožnost dajanja odgovora o statusu določenega certifikata (seznam našteva le preklicane certifikate). Čeprav obstajajo predlogi, ki deloma rešujejo opisane probleme (Nora, Nissim [47], Micali [44], McDaniels [42], Copper [14]), še vedno ni na voljo primerne rešitve za vsa okolja uporabe kriptografije javnega ključa.

Preverjanje statusa certifikata s priključnim dostopom do strežnika naj bi omogočalo pridobivanje informacije o statusu v realnem času. Na podlagi opisa protokola OCSP (Myers et al. [45]) lahko navedemo pomanjkljivosti. Agencija sme uporablja isti ključ za podpisovanje odgovorov in izdanih certifikatov. To pomeni, da se zasebni ključ nahaja na računalniku, ki je priključen v omrežje, kar omogoča široko paleto napadov z namenom razkritja ključa (Shamir, Someren [62]). Pozitiven odgovor brez dodatnih pojasnil (ki niso obvezna) ne pove dosti o certifikatu, niti ali je bil certifikat sploh izdan in ali je bil odgovor generiran še v obdobju veljavnosti certifikata. Odgovor strežnika v primeru nerazumljive ali napačne poizvedbe ni digitalno podpisan s strani strežnika. Slednje omogoča, da napadalec prestreže odgovor in podtakne svojega. S tem onemogoča strežbo in preprečuje izgradnjo zaupanja v ključ entitete. Strežnik tako predstavlja privlačno tarčo za napadalca, saj s tem onemogoča delovanje celotne infrastrukture. Sestavljanje odgovorov in digitalno podpisovanje je računsko intenzivna operacija in prav lahko bo strežnik močno obremenjen ter neprivlačen za uporabo, če poizvedbe ne bodo obdelane v realnem času.

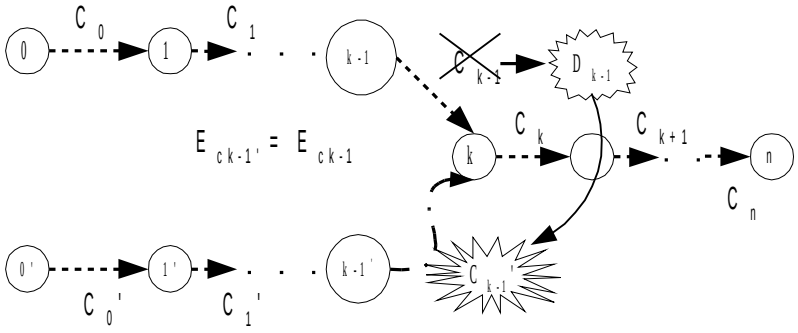
Kot rešitev problema ugotavljanja statusa certifikata predlagamo uporabo pametnih kartic za hranjenje zasebnega ključa entitete. Certifikat lahko vsebuje negativne kvalifikacije. Pri hranjenju ključev in certifikatov na pametni kartici je verjetnost razkritja ključa oziroma zamenjave korenskega certifikata zanemarljiva. Potreba po preverjanju statusa certifikata se pojavi le redko. Seznam preklicanih certifikatov bo praviloma majhen. Za certifikate, ki se uporabljajo za prepoznavanje, bo ob robustni izvedbi zaščite pametnih kartic velikost seznama praktično enaka nič.

Zgornjo rešitev razširimo z uporabo kratkoživih certifikatov. Slednji so najboljši dokaz o svežini atributov, zapisanih v certifikatu. Rešitev je učinkovita, saj nudi tako garancijo veljavnosti kot pristnosti povezave javni ključ - entiteta. Ponovna izdaja certifikatov ima tudi slabo stran, saj je računsko zelo intenzivna operacija. V primeru ko je strežnik za izdajo certifikatov zelo obremenjen, je taka rešitev preveč potratna. Z uporabo obdobja, ko je certifikat zanesljivo veljaven (Rivest [56]), lahko močno zmanjšamo stroške upravljanja mehanizma za ugotavljanje statusa certifikata. Slednje predstavlja pogodbo med uporabnikom in izdajateljem certifikata, v kateri se izdajatelj zaveže, da certifikata ne bo preklical. Čas gotove veljavnosti je lahko zaobjet v parametru izjave.

Tako smo v veliki meri znižali stroške ugotavljanja statusa certifikata, saj je pri kratkoživih certifikatih obdobje, v katerem je potrebno preklicati certifikat, omejeno.

Preverjanje interakcije med verigami certifikatov

Ob iskanju več neodvisnih verig se pojavi problem interakcije verig. Ker so lahko interakcije zelo kompleksne in jih je težko zajeti v model, se bomo omejili le na že predstavljeni primer. Kot smo opozorili v prvem razdelku petega poglavja, lahko preklic križnega certifikata vpliva tudi na veljavnost drugih verig. Zato bomo v nadaljevanju oblikovali predlog, kako se izogniti skritim pastem medsebojnega vpliva navidezno neodvisnih verig certifikatov.



Slika 6.4: Vpliv preklica certifikata na certifikatne verige.

Če obnovimo, se v primeru, ko imata verigi certifikatov končni del verige enak in imata zadnja še različna člena enak javni ključ, lahko ob razkritju zasebnega ključa (agencije I_{k-1} oziroma I_{k-1}') pride do interakcije in napada. Potrebujemo nadgradnjo mehanizma za ugotavljanje statusa certifikata. Zasnovati je potrebno storitev, ki bi na poizvedbo o javnem ključu vrnila vse preklicane križne certifikate z navedenim javnim ključem in razlogom za preklic. Za vsako verigo, ki jo zgradimo, bi morali zbrati javne ključe križnih certifikatov in preveriti, ali je bil preklican križni certifikat in je bil ključ izdajatelja enak enemu izmed ključev iz naše množice.

Odgovornost agencij

Poleg zbiranja certifikatov in njihovega statusa se za določene aplikacije izkaže primerno, da zbiramo tudi informacije o višini poroštva. Le-te izdajatelj nudi v primeru razkritja zasebnega ključa entitete in njegove zlorabe ali v primeru neprimernega obnašanja entitete, lastnice certifikata.

Višina poroštva

Model še dodatno izpopolnimo in približamo zahtevam uporabnika. Kot bomo videli kasneje pri analiziranju odpornosti modela na napade, lahko ena sama entiteta zavede uporabnika v njegovem prepričanju o pristnosti javnega ključa entitete. Vsakemu certifikatu priredimo vrednost (Reiter, Stubblebine [50], [51]). Vrednost predstavlja denarni znesek, s katerim izdajatelj jamči za primerno obnašanje entitete, ki ji certifikat pripada. Izdajatelj se obveže, da povrne škodo v primeru, če so atributi certifikata neresnični ali če se zasebni ključ entitete uporabi za zavajanje uporabnika bodisi namerno ali nenamerno. Slednje velja v primeru razkritja zasebnega ključa. Tako izdajatelj zavaruje uporabnika certifikata. Uporabnik mora višina zneska jamstva na varen način pridobiti od izdajatelja. Naravno mesto za slednji parameter je v certifikatu entitete.

V primeru, da je prišlo do razkritja zasebnega ključa izdajatelja, ali da se izdajatelj ne obnaša v s skladu predpisano politiko certificiranja, nosi odgovornost za njegova dejanja agencija, ki ga je overila, oziroma pooblastila za izvajanje dejavnosti. Podobno razmišljanje lahko uporabimo za celotno verigo; od agencije, ki ji zaupamo, do entitete, katere ključ preverjamo. Tako bi vsaka pot od zaupanja vrednih agencij do

entitete imela svojo agencijo, ki bi odgovarjala za škodo v primeru neupravičenega zaupanja v povezavo javni ključ entitete.

Primerna metrika za odločanje, ali zaupamo v javni ključ entitete, bi bila minimalna odškodnina, ki jo dobimo v primeru zavajanja. Za izračun uporabimo postopek določanja maksimalnega pretoka skozi graf, ki je v tem primeru sestavljen le iz certifikatov in priporočil (Ford, Fulkerson [22]). Tako lahko uporabnik dodatno odloča o tveganju, ki je zanj še sprejemljivo.

Izhod take metrike za gradnjo zaupanja je uporaben za celo vrsto poslovnih transakcij, kjer je vrednost transakcije pomembna. Hkrati je koristen, saj nalaga odgovornost vsakemu izdajatelju certifikatov, da pretehta koristi in tveganja za certifikate, ki jih izdaja. V končni fazi bo tržišče odločilo, ali je metrika ekonomsko upravičena. Menimo, da bi morala že visoko-nivojska tehnologija omogočati uporabo tovrstne metrike.

Pri tem se zavedamo, da so mnoge podrobnosti trenutno še odprt problem. Večina niso tehničnega značaja in so bolj v domeni pravne in organizacijske ureditve infrastrukture javnega ključa. Najočitnejši sta plačevanje zavarovalnih premij in določanje agencij, ki nosijo poroštvo. Model s predlagano metriko vsekakor vrača zelo uporaben rezultat za uporabnika.

Gradnja zaupanja

Ko je uporabnik certifikata zbral zadosti podatkov, lahko začne z gradnjo zaupanja v javni ključ entitete (pobudnika akcije). Gradnja zaupanja se izvaja avtomatično, brez posredovanja uporabnika certifikata, s procesiranjem grafa zaupanja za nameravano akcijo. Če uspemo zgraditi zaprtje, ki vsebuje izjavo $Auth_{A,B}$, je postopek gradnje zaupanja končan in se imetniku certifikata omogoči izvedba akcije. Preostane le še shranjevanje vseh uporabljenih dokazil.

Omenimo še delovanje modela v primeru, ko izjava oziroma začetni pogled vsebuje parametre, ki dodatno pojasnjujejo zahteve, ki jih mora entiteta izpolnjevati. Izpeljana izjava mora vsebovati vse parametre, ki so jih vsebovale vhodne izjave. Vrednost vsakega parametra, prirejenega novi izjavi, je maksimalna vrednost vseh istovrstnih parametrov. Parametri vira še dodatno dopolnjujejo zahteve uporabnika certifikata. Izjava o pristnosti javnega ključa entitete se vključi v pogled, le če ustreza vsem zahtevam (parametrom) vira, sicer se privzame, da je ni mogoče izpeljati.

Ob procesiranju grafa zaupanja in uporabi izpeljevalnih pravil dobivamo nove veljavne izjave. Postavlja se vprašanje, ali jih smemo vključiti v tabelo varnostne politike. Tabela je zgrajena vnaprej in je statična. Izjave bi dinamično lahko dodajali, le če bi iz verige pobirali parametre in jih dodajali izpeljanim izjavam “Auth” oziroma “Trust” (minimalen čas veljavnosti, minimalni znesek jamstva, maksimalni red uporabljenega priporočila/zaupanja). Razrešiti je potrebno primer, ko parameter ne predstavlja številčne vrednosti. Vrednosti, ki jih zavzema, bi bilo potrebno urediti po velikosti. Vendar ni nujno, da je tako dodana izjava (veriga) ob naslednji uporabi sploh še veljavna. Ob razkritju zasebnega ključa (neveljavnosti izjave “Auth”),

preklicu certifikata ali umiku priporočila bi prenehalo veljati tudi jamstvo. Menimo, da dinamično dodajanje izjav v tabelo prinese preveč problemov in je vsakokratno izpeljevanje izjav iz majhne množice veljavnih izjav enostavnejše.

Arhiviranje

Ko smo zbrali vse potrebne podatke in zgradili zaupanje v javni ključ entitete ter izvedli transakcijo, je celoten postopek za uporabnika in entiteto končan. Preostane še shranjevanje vseh podatkov, na podlagi katerih smo prišli do odločitve. Vse podatke opremimo s časovnimi znamkami za primer, da je potrebno v kasnejšem času dokazovati izvedbo transakcije, kot smo to spoznali v četrtem razdelku tretjega poglavja. V primeru, da je hranjenje certifikatov izvedeno s pametnimi karticami in imajo le-te vgrajene točno uro, opremimo vse digitalne podpise s časovno znamko. Če entiteta hrani podatke le za lastno evidenco, zadostuje, da jih podpiše z lastnim zasebnim ključem in doda časovne znamke (s pomočjo pametne kartice). V primeru, da hoče podatke uporabiti za preprečevanje tajenja in dokazovanje izvedbe tretji strani (razsodniku), je nujna uporaba strežnika točne ure, ki opremi vse bistvene podatke s časovnimi znamkami. Kot smo omenili, lahko tudi za to nalogo uporabimo pametne kartice kot priročni strežnik točne ure.

6. VRSTE NAPADOV IN ROBUSTNOST MODELA

V sledečem razdelku bomo analizirali robustnost modela na napade. Definirajmo možne napadov v jeziku modela. Napadalec se dokoplje do zasebnega (podpisnega) ključa entitete. S tem je napadalcu omogočeno, da dodaja lažne povezave (izjave) v model. Napad bomo imenovali *napad na vozlišče*. Znatno bolj omejen je *napad na povezave*. Pri slednjem je napadalec sposoben preslepiti entiteto (certifikatno agencijo), da overi para ključev, ki jih ne poseduje, oziroma da mu izda priporočilo (Levien, Aiken [39]).

Posebne vrste napad je, ko napadalec onemogoča pridobitev podatkov (certifikatov, priporočil) z napadom na strežnik, ki skrbi za razdeljevanje certifikatov in informacij, povezanih z njimi. To je klasičen *napad onemogočanja strežbe* (denial of service attack).

Privzeli bomo, da je napadalec sposoben izdati poljuben certifikat ali priporočilo, podpisano z njegovim parom ključev. Izvzeli bomo napad na šifrirne postopke in digitalne podpise, saj bi v primeru njihovega razbitja napadalec lahko bistveno hitreje in z manj truda prišel do zastavljenega cilja. Prav tako ne bomo obravnavali primera, ko lahko napadalec vnese svoje izjave v varnostno politiko sistema, saj mu je s tem verjetno že uspelo prodreti v sistem uporabnika in so mu odprta vsa vrata.

Cilj napadalca je, da poizkuša uporabniku podtakniti nepristen javni ključ oziroma preprečiti zgraditev zaupanja v ključ entitete. Slednji napad lahko uvrstimo med napade onemogočanja strežbe in je izven okvira obravnave modela. V nadaljevanju razdelka se bomo posvetili le napadom, kjer napadalec poizkuša prevarati uporabnika glede pristnosti javnega ključa entitete.

Napadalec poizkuša preslepiti uporabnika z izdajanjem lažnih certifikatov, priporočil in onemogočanjem graditve več neodvisnih poti. Tako prisili uporabnika, da zgradi pot, ki nudi napadalcu največ možnosti za uspeh. Ponovno se pojavi vprašanje, kdo naj zbira podatke, ki uporabniku pomagajo graditi model infrastrukture. Zlonamerna entiteta lahko skrbno filtrira podatke, ki jih dostavlja uporabniku certifikata in tako pripravlja teren za uspešno izvedbo napada. Pri sestavljanju varnostne politike sistema moramo skrbno pretehtati posledice gradnje zaupanja le na podlagi delnih podatkov.

Analiza napadov na model

Ker smo izbrali diskretno metriko, smo se v veliki meri izognili občutljivosti, kateri so podvrženi mnogi drugi modeli za upravljanje z zaupanjem (Reiter, Stubblebine [51]). Pomemben ukrep pri povečevanju robustnosti modela je varovanje izjav zaupanja in seznama pristnih javnih ključev (tabele varnostne politike). Kajti če napadalec ne pozna začetnega pogleda, le s težavo ugotovi topologijo grafa zaupanja modela, s pomočjo katerega uporabnik gradi zaupanje. Prav tako je res, da s spremljanjem dostopa do certifikatnih strežnikov, poznavanjem topologije infrastrukture javnega ključa, vzajemnih overjanj agencij, lahko napadalec v dobršni meri zgradi uporabnikov model infrastrukture. Z določitvijo več zaupanja vrednih agencij uporabnik poveča možnost, da bo obstajalo več neodvisnih poti ter bo napadalec moral napasti več vozlišč in dodati več lažnih povezav.

Čeprav je robustnost na napad močno odvisna od topologije infrastrukture javnega ključa in njene povezanosti z drugimi infrastrukturami, lahko podamo nekaj splošnih smernic, ki koristijo tako napadalcu pri načrtovanju napada kot uporabniku pri obrambi.

- Za načrtovanje napada je zelo ugodno, da poznamo začetni pogled uporabnika. Omogoča nam, da identificiramo *odlikovana vozlišča*. Iz izpeljevalnih pravil je hitro jasno, da nima smisla napasti vozlišč, ki jim uporabnik ne zaupa, oziroma jih odlikovana vozlišča ne priporočajo. Med odlikovana vozlišča štejemo tista iz začetnega pogleda in tista, ki se med gradnjo zaupanja vanj uvrstijo.

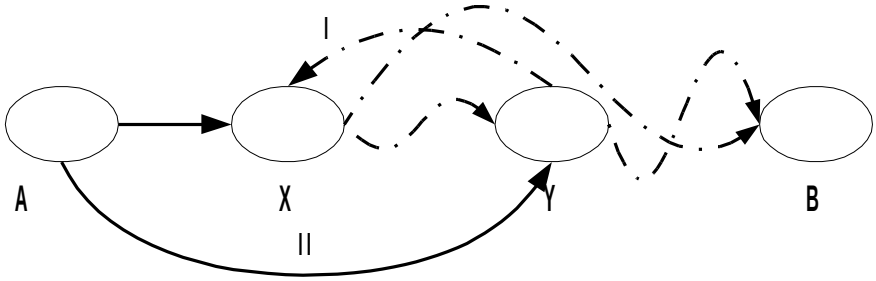
- Napad na odlikovano vozlišče je močno orodje v rokah napadalca, saj omogoča uporabniku podtikanje lažnih podatkov (certifikatov, priporočil). Pri tem lahko za zavajanje metrike uporabnika (ki jo domnevno ne pozna) napadalec določi več navidezno neodvisnih poti. Tovrstni napad je v praksi pogosto neizvedljiv, saj so zasebni ključi za podpisovanje dobro varovana skrivnost agencij za certificiranje. Toda če agencija uporablja isti ključ za podpisovanje certifikatov in seznamov preklicanih certifikatov, se lahko pojavi problem v primeru vdora v sistem. Računalnik za razdeljevanje statusa certifikatov je običajno zaradi potrebe po veliki stopnji razpoložljivosti priključen v omrežje (Shamir, Someren [62]).

- Če napadalcu uspe ukaniti odlikovano vozlišče, da mu izda priporočilo s primernimi vrednostmi parametrov, je na dobri poti, da zavede uporabnika v njegovem zaupanju.

Sklenemo lahko, da mora biti varnostna politika dobro varovana skrivnost, saj s tem napadalcu otežimo izbiro vozlišč, ki jih mora napasti. Uporaba diskretne metrike se izkaže za mnogo bolj robustno, saj ne omogoča enostavne manipulacije z metriko (Reiter, Stubblebine [51]).

Primer 3: Oglejmo si primer, ko model ne omogoča zgraditve zaupanja v javni ključ entitete, saj obstaja možnost, da pride do zavajanja in prevare uporabnika. Vijugaste črtkane povezave pomenijo podtaknjene lažne podatke.

$$View_A = \{Auth_{A,X}, Trust_{A,Y,2}\};\ (\mathrm{Re}c_{Y,X,2});\ \langle Cert_{X,B}, Cert_{X,Y}, Cert_Y$$



Slika 6.5: Primer robustnosti modela za gradnjo zaupanja.

Izpeljava pristnosti javnega ključa $Auth_{A,B}$ je nemogoča, kar je popolnoma v skladu s pogledom uporabnika. V primeru, da je X nepošten, lahko ponaredi $Cert_{X,B}, Cert_{X,Y}$ in celo $Cert_{Y,B}$ brez vednosti in vpletenosti Y. Slednje velja v primeru, ko mu uspe razkriti skrivni (podpisni) ključ Y. Začetni pogled za zahtevano akcijo ne vsebuje $Auth_{A,Y}$, v skladu z modelom pa lahko izjave o pristnosti javnega ključa uporabnik črpa le iz varnostne politike, oziroma jih izpelje iz začetnega (razširjenega) pogleda. V pričujočem primeru ima uporabnik na voljo premalo podatkov za tako izpeljavo.

7. PRIMERI UPORABE MODELA ZAUPANJA

Elektronsko poslovanje in spletna trgovina

Infrastruktura javnega ključa omogoča izvajanje transakcij med spletnimi prodajalci in kupci. Kupci so v tem primeru uporabniki digitalnih certifikatov in pričnejo transakcijo z razpoznavanjem strežnika (običajno s pomočjo protokola vrste izziv - odgovor, na primer SSL [64]). Največkrat je preverjena le identiteta strežnika, saj se prodajalec zadovolji s številko plačilne kartice. Glede na svojo varnostno politiko ima entiteta interes zavarovati številko kartice. Grožnja je razkritje številke plačilne kartice in nepooblaščena uporabe kartica na škodo imetnika. Zaščita je običajno izvedena s šifriranjem seje med kupcem in prodajalcem.

Začetni pogled

Začetni pogled vsebuje javne ključe certifikatnih agencij, ki jim uporabnik zaupa, in izjave o zaupanju za izdajanje certifikatov. Strežnik pošlje tudi svoj certifikat ali kar celotno verigo certifikatov.

Kot parameter izjav je zelo primeren znesek nakupa. Glede na velikost zneska nakupa je uporabnik pripravljen zaupati le določenim certifikatnim agencijam oziroma razredom certifikatov, ki jih le-te izdajajo in zanje jamčijo z zadostno odškodnino v primeru zlorabe certifikata ali izgube zasebnega ključa entitete. Seveda pa je potrebno podatke pridobiti iz politike certificiranja agencije, ki certifikate izdaja. Žal v večini primerov politike certificiranja niso zapisane formalno. Potrebno je vnaprejšnje zbiranje in hranjenje podatkov o razredih certifikatov in višini nudenega jamstva. Ker je trenutno na svetu okoli štirideset agencij, ki se ukvarjajo z overjanjem javnih ključev spletnim strežnikom, to ne bi smel biti prevelik problem.

Zaradi velike obremenjenosti strežnika je nerealno pričakovati, da bo za vsakega kupca priskrbel še podatke o statusu certifikata in sodeloval pri gradnji verige. Prav tako je vprašljivo, ali je ekonomsko upravičeno za vsakega kupca generirati tako veliko količino prometa za pridobivanje informacij o statusu certifikatov v verigi. Podatki, ki bi jih zbiral, so prehodnega značaja in bi bili v veliki večini primerov uporabni le za eno samo transakcijo.

V interesu kupca je zbiranje in hranjenje podatkov o preverjanju certifikatne verige in graditvi zaupanja. Kajti le s pomočjo podatkov, ki jih bo opremil s časovno znamko in arhiviral, bo lahko izpodbijal transakcije, izvedene z njegovo plačilno kartico, katera je bila odtujena med komuniciranjem s strežnikom zaradi razkritja zasebnega ključa strežnika.

Intranet

Strežnik nudi zanimive podatke in storitve uporabnikom v sistemu. Nekatere izmed storitev oziroma podatkov so zaupne narave. Potrebno je izvajati kontrolo dostopa ter vodenje dnevnika o izvedenih storitvah. V tem primeru se certifikati uporabljajo kot sredstvo za identifikacijo entitet, ki komunicirata. Preveri se identiteta tako strežnika kot odjemalca. Vendar je odjemalec v ugodnejšem položaju. Ker ima odjemalec običajno že certifikat strežnika ima in tudi pristen javni ključ agencije, ki je overila ključe strežnika, je njegova naloga v protokolu za preverjanje identitete strežnika lahka.

Nasprotno se mora strežnik v identiteto odjemalca na podlagi zbranih podatkov šele prepričati. Čeprav je pričakovati, da so v tem modelu entitete v isti administrativni domeni (vsaj v primeru intraneta je tako), pa je preveč optimistična domneva o obstoju ene same certifikatne agencije. V skrajnem primeru so lahko agencije prostorsko ločene (različne izpostave podjetja po svetu). Zato je upravičeno pričakovati veliko število uporabnikov in hierarhično zgradbo modela zaupanja (drevo z odlikovanim vozliščem).

Začetni pogled

V tem primeru je začetni pogled močno pogojen z vrsto storitve (transakcije), ki jo odjemalec pričakuje. Zahteva po strežbi je lahko enostaven dostop do podatkov za pregledovanje ali pa naročilo za prenos sredstev. Varnostna politika in mehanizmi za kontrolo dostopa so bistveno drugačni za ti dve skrajni možnosti.

Začetni pogled vsebuje javne ključe vseh ali vsaj za potrebe strežnika najpomembnejših agencij. Prav tako so v začetnem pogledu vsebovane izjave o zaupanju posameznim agencijam za izdajanje certifikatov.

Dodani parametri se običajno nanašajo na znesek transakcije, ki jo lahko izvede entiteta, ki ima ključ, overjen s strani določene agencije, višina jamstva, namen izdaje certifikata odjemalcu... Dodaten parameter(izjava) je, ali strežnik sploh zaupa certifikatom ki jih določena agencija izdaja odjemalcem (No_Trust).

Realno je pričakovati, da bo strežnik močno obremenjen. Odjemalec bo skoraj zagotovo imel na voljo zadosti prostih zmogljivosti za pridobivanje podatkov, ki bodo uporabni za gradnjo verige certifikatov. Obe strani imata interes arhivirati zbrane podatke za primer preprečevanja tajenja (odjemalca) oziroma analizi vdora v sistem in ocenjevanju škode.

Hranjenje zasebnega ključa odjemalca na pametnih karticah lahko prinese bistvene izboljšave v mehanizem za ugotavljanje statusa certifikata uporabnika. Pametne kartice nudijo močno zaščito pred izgubo, krajo, posojanjem, kopiranjem ali izsiljevanjem. Prav tako je mogoče onemogočiti nezaželeno obnašanje imetnika pametne kartice. Če ima kartica vgrajeno točno uro, lahko točen čas vključimo v digitalni podpis. To v veliki meri ali skoraj v celoti odpravi potrebo po priključnem preverjanju statusa certifikata oziroma rednem pošiljanju seznama preklicanih certifikatov.

8. PREDLOG IMPLEMENTACIJE MODELA V OKOLJU CERTIFIKATOV X.509

Ker smo hoteli model zasnovati tako, da je z minimalnimi spremembami uporaben tudi v obstoječih infrastrukturah javnega ključa, si v nadaljevanju oglejmo predlog izvedbe. Povzeli bomo le ključne elemente modela, saj je zavedamo, da zahteva praktična izvedba mnogo dodatnih podrobnosti.

Predstavitev izjav

Varnostno politiko gradi uporabnik sam, saj pozna vire, možne vrste dostopa, varnostne zahteve, entitete, ki jim zaupa, tveganje, ki ga je pripravljen sprejeti in jamstva, ki jih zahteva. V primeru, da uporabnik ni seznanjen z osnovami

računalniške varnosti, lahko tipizirano politiko zgradi administrator sistema in jo razdeli med uporabnike.

Zaščito določa vir, ki ga ščitimo. Tabela vsebuje le pozitivne izjave (kaj kdo sme, pod katerimi pogoji). Izjema so lahko izjave, ki govorijo o slabih izkušnjah uporabnika z drugimi entitetami (Not_Trust), neke vrste negativni certifikat. Sicer sestavljajo tako formalizirane varnostne politike izjave tipa “Auth” in “Trust”. Predstavljena je v obliki tabele in je varovana skrivnost, saj lahko napadalec iz nje razbere naše zaupanja (kar olajša napad) ali lahko celo podtakne oziroma zamenja izjave. Politike certificiranja so vključene v tabelo s pomočjo izjav zaupanja. Politike trenutno v veliki večini niso formalizirane. V primeru formalizacije lahko identifikator politike vključimo kot parameter vira, vse pridobljene izjave morajo biti izdane na podlagi predpisane ali celo ostrejše politike (namerno puščamo ob strani problem primerljivosti različnih politik certificiranja, Klobučar [33]).

Kako poimenujemo entitete, je odvisno od infrastrukture in ne igra pomembne vloge, dokler lahko uporabnik certifikata nedvoumno določi, kdo je entiteta, s katero komunicira. Naziv je lahko po priporočilu X.500 ali naslov elektronski pošte entitete ali URL naslov. Skladno s poimenovanjem v infrastrukturi morajo biti poimenovane tudi entitete v tabeli.

Vse izjave so predstavljene kot certifikati. Izjave tipa “Trust” so predstavljene kot certifikat, ki ga podpiše uporabnik s svojim podpisnim (zasebnim) ključem. Poleg naziva entitete in vrste izjave certifikat vsebuje še red zaupanja. Kot smo že omenili, lahko izjavo “Auth” predstavimo kot “Trust” reda nič. Ker zaupanje ni absolutno, izjave zaupanja običajno vsebujejo še dodatne parametre, ki pogojujejo zaupanje v entiteto.

Priporočila predstavimo kot certifikat, ki ga izdajatelj opremi s svojim nazivom, nazivom tistega, ki ga priporoča (nosilca), redom priporočila ter parametri (pogoji za veljavnost priporočila). Ni potrebno, da izdajatelj priporočila pozna javni ključ entitete. Običajno je časovno omejen (plačljivost izdaje) in ga izdajatelj lahko tudi prekliče. V interesu entitete je, da pridobiva priporočila. Priporočilo reda nič predstavlja certifikat javnega ključa.

Izjave imajo poleg osnovnih podatkov lahko še dodatne parametre, ki dodatno določajo veljavnost izjav in postavljajo zahteve, ki jih mora imetnik certifikata izpolnjevati. Za najočitnejše primere lahko navedemo čas veljavnosti izjave, višino jamstva izdajatelja, namen uporabe (varovanje elektronske pošte, podpis dokumentov...). Tudi vir ima lahko na zahtevano akcijo predpisane parametre (višina jamstva, ki ga pot nudi, maksimalni red priporočila, število neodvisnih poti, maksimalna starost izjav, način varovanja zasebnega ključa...). Parametri so lahko vključeni v certifikat kot nekritične razširitve [28].

Izdajatelj lahko priporočila tudi prekliče, zato je potrebno preverjati status zbranih priporočil. Koristno je, da imajo vse izjave parameter, ki govori o dobi (gotove) veljavnosti. Prav tako je potrebno preverjati tudi izjave o pristnosti javnega ključa, saj lahko pride do razkritja zasebnega ključa.

Organizacija infrastrukture

Z uporabo preprostih prijemov v organizaciji delovanja infrastrukture lahko izboljšamo učinkovitost uporabe in zmanjšamo obremenitev strežnikov.

Pametne kartice bistveno zmanjšajo obremenitev infrastrukture z razdeljevanjem statusa certifikatov. S stiskanje velikosti certifikatov, kot smo to spoznali v tretjem razdelku četrtega poglavja, lahko ena sama pametna kartica nosi vse zasebne ključe, uporabnika in vse negative izjave o njem. Če presodimo, da akcija ni kritična, lahko v primeru hranjenja certifikatov na kartici preskočimo preverjanje statusa certifikata. Z razvojem kartic (notranji vir napajanja), jih lahko uporabniki uporabljajo kot varen strežnik točne ure. To nam omogoča ločevanje dogodka izgube ključa od ostalih razlogov za preklic certifikata.

Z uvedbo nove storitve, ki vrne vse certifikate, ki so bili preklicani v infrastrukturi in imajo določeno vrednost javnega ključa, se lahko izognemo nevarni interakciji certifikatnih verig (prvi razdelek petega poglavja). Pri tem se zavedamo, da je verjetnost izdaje dveh enakih javnih ključev majhna.

Hitrost preverjanja neokrnjenosti certifikata in izdaje kratkoživih certifikatov lahko izboljšamo z uporabo nekonsistentnih certifikatov (peti razdelek tretjega poglavja oziroma peti razdelek petega poglavja). Tako razbremenimo strežnik za izdajo certifikatov in postopek gradnje zaupanja, saj je preverjanje/kreiranje digitalnega podpisa računsko zelo intenzivna operacija. Seveda je potrebno pred uvedbo nekonsistentnih certifikatov analizirati razmerje med preverjanjem in kreiranjem digitalnega podpisa. Kot dodatno pohitritev in razbremenitev infrastrukture bi uvedli dobo gotove veljavnosti certifikata (tretji razdelek petega poglavja).

Za resnično samostojno delovanje modela bi bilo potrebno dodati postopek, ki bi subjektoma omogočal dogovor, kdo zbira podatke in zahteve o svežini zbranih podatkov, potrebne za zgraditev zaupanja.

VII. SKLEP

Upravljanje z zaupanjem je v obstoječih infrastrukturah javnega ključa prepogosto nesistematično. Pojavlja se potreba po formalnem zapisu in obravnavi vseh dejavnikov, ki so pomembni pri gradnji zaupanja v entiteto in njen javni ključ.

V magistrskem delu so predstavljene poglavitne organizacijske ter tehnične pomanjkljivosti obstoječih infrastruktur, in podani predlogi za njihovo odpravo. Na podlagi obstoječih predlogov za upravljanje z zaupanjem je zasnovan nov model zaupanja. Le-ta predstavlja uporabnikov pogled na infrastrukturo javnega ključa. Predstavljen model ponuja razširitev in posplošitev obstoječih predlogov. Omogoča formalen zapis varnostne politike sistema, izjav entitet, povezav med entitetami ter določitev vseh pomembnih dejavnikov izjav in virov, ki so ključni pri vrednotenju zaupanja v entiteto in njen javni ključ, ter oceni tveganja v primeru sprejetja akcije. Poudarek modela je na uporabnikovem določanju vseh pomembnih dejavnikov za ohranjanje zaupnosti in neokrnjenosti virov.

Predstavljeni model je zasnovan dovolj splošno, da ga lahko brez problemov vključimo v že obstoječe infrastrukture. Za svoje delovanje ne potrebuje večjih razširitev obstoječih standardov za digitalne certifikate javnega ključa, ali večjih sprememb organizacije infrastrukture. Bolj kot na dovršenih postopkih in vpeljavi novih formalizmov je poudarek na uporabi obstoječih mehanizmov infrastrukture in tehnoloških zmožnosti. V zgledih je bilo predstavljeno delovanje modela in njegova odpornost na napade. Na primerih trenutno najpogostejše uporabe globalnih omrežij v povezavi z infrastrukturo javnega ključa sta bila izdelana predloga organizacije infrastrukture in gradnikov modela za vrednotenje zaupanja, tveganja ter učinkovito uporabo infrastrukture.

Smer nadaljnjih raziskav in razvoja modela vidimo predvsem v izvedbi modela v delujoči infrastrukturi javnega ključa. Menimo, da se bo s čedalje intenzivnejšo uporabo storitev, ki jih nudijo globalna omrežja, in z napadi nanje, pokazala potreba po formalni in preprosti metodi za varovanje podatkov in zasebnosti vsakega uporabnika. Zavestno sprejemanje tveganja in opuščanje osnovnih varnostnih ukrepov (preverjanje statusa certifikatov, hranjenje zasebnih ključev...) je dolgoročno po našem mnenju nesprejemljivo. Tehnološko so orodja pripravljena, potrebno je le še doreči odprta pravna in organizacijska vprašanja.

VIII. VIRI IN LITERATURA

[1] C. Adams, R. Zuccherato, A General, Flexible Approach to Certificate revocation, June 1998, http//:www.entrust.com/resources/whitepapers.htm

[2] R. Anderson, M. Kuhn, Tamper Resistance – A Cautionary Note, Second USENIX Workshop on Electronic Commerce Proceedings USENIX, str. 1-11, November 1996.

[3] M. Baentsch, P. Buhler, T. Eirich, F. H□ring, M. Oestreicher: JavaCard – From Hype to Reality, IEEE Concurrency, Vol. 7, No. 4, str. 36-42, October-December 1999.

[4] S. Berkovits, S. Chokhani, J. A. Furlong, J. A. Geiter, J. C. Guild, Public Key Infrastructure Study: Final Report. Produced by the MITRE Corporation for NIST, April 1994.

[5] T. Beth, M. Borcherding, B. Klein, Valuation of trust in open systems, Computer Security – ESORICS '94, D. Gollmann (Ed.), Lecture Notes in Computer Science, Berlin: Springer-Verlag, Vol. 875, str. 3-18, 1994.

[6] M. Blaze, J. Feigenbaum, J. Lacey, Decentralized trust management, Proceedings of the 17th IEEE Symposium on Security and Privacy, str. 164-173, IEEE Computer Society Press, 1996.

[7] M. Blaze, J. Feigenbaum, J. Ioannidis, A. Keromytis, The KeyNote Trust-Management System Version 2, IETF, RFC 2704, September 1999.

[8] M. Blaze, J. Feigenbaum, J. Ioannidis, A. Keromytis, The role of trust management in distributed systems security, Vitek (Ed.), Jensen (Ed.), Secure Internet Programming: Security issue for mobile and distributed objects, Springer-Verlag, 1999.

[9] S. Brands, Rethinking Public Key Infrastructure and Digital Certificates, Brands Technologies, ISBN: 9090130594, 1999.

[10] W. E. Burr, W. T. Polk, A Federal PKI with Multiple Digital Signature Algorithms, Federal PKI Technical Working Group, Draft, September 1997.

[11] Current Public-Key Cryptographic Systems, Certicom, Published: April 1997, Updated: July 2000, http//:www.certicom.com.

[12] The Elliptic Curve Cryptosystems for Smart Cards, Certicom, Published: May 1998, http//:www.certicom.com.

[13] S. Chokhani, W. Ford, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, IETF, RFC 2527, 1999.

[14] D. A. Cooper, A Model of Certificate Revocation, Proceedings of the 15th Annual Computer Security Applications Conference, str. 256-264, December 1999.

[15] W. Diffie, M. E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. 22, str. 644-654, 1976.

[16] D. Davis, Compliance Defects in Public-Key Cryptography, Proceedings 6th USENIX Security Symposium, str 171-178, Marec 1997.

[17] C. Ellison, SPKI Requirements, Internet Draft, IETF SPKI Working group, RFC 2692, September 1999.

[18] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, T. Ylonen, SPKI Certificate Theory, Internet Draft, IETF SPKI Working group, RFC 2693, September 1999.

[19] C. Ellison, B. Schneier, Ten Risks of PKI: What You’re not Being Told about Public Key Infrastructure, Computer Security Jurnal, Vol. XVI, No. 1, http://www.counterpane.com, 2000.

[20] J. Feghhi, J. Feghhi, P. Williams, Digital certificates: Applied Internet Security, Addison-Wesley, ISBN: 0-201-30980-7, 1998.

[21] W. Ford, M.S. Baum, Secure electronic commerce: building the infrastructure for digital Signature and Encryption, Prentice-Hall, ISBN: 0-13-476342-4, 1997.

[22] L. Ford, D. Fulkerson, Maximal flow through a network, Canadian Journal of Mathematics, str. 399-404, 1956.

[23] Fortezza, http://www.armadillo.huntsville.al.us/Fortezza_docs/

[24] B. Fox, B. LaMacchia, Certificate Revocation: Mechanics and Meaning, Proceedings of the Financial Cryptography FC '98, Vol. 1465, str. 178-183, Februar 1998.

[25] D. Husemann, The Smart Card: Don’t Leave Home Without It, IEEE Concurrency, Vol. 7, No. 2, str. 24-27, April-Junij 1999.

[26] D. Husemann, R. Hermann, OpenCard: Talking to Your Smart Card, IEEE Concurrency, Vol. 7, No. 3, str. 53-57, Julij-September 1999.

[27] R. Housley, W. Ford, W. Polk, D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, IETF RFC 2459, Januar 1999.

[28] ISO/IEC, Draft Amendment DAM 1 to ISO/IEC 9594-8 on Certificate Extension, 1997.

[29] ITU-T Recommendation X.500 - ISO/IEC 9594-8, Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services,1994.

[30] ITU-T Recommendation X.509 - ISO/IEC 9594-8, Information technology – Open Systems Interconnection – The Directory: Authentication framework,1994.

[31] A. Jain, L. Hong, S. Pankanti: Biometric identification, Communications of the ACM, Vol. 43, No. 2, str. 91-98, Februar 2000.

[32] A. Jurišič, A. Menezes, Elliptic Curves and Cryptography, Dr. Dobb's Journal, str. 26-35, April 1997.

[33] T. Klobučar, Formalni modeli varnostnih politik v globalnih računalniških omrežjih, doktorska disertacija, Univerza v Ljubljani, 2000.

[34] P. Kocher, Timing Attacks on Implementation of Diffie-Hellman, RSA, DSS and Other Systems, Advances in Cryptology CRYPTO '96, Proceedings, Springer-Verlag, str 104-112, 1996.

[35] P. Kocher, Differential Power Analysis, Proceedings of Advances in Cryptology – CRYPTO '99, str. 388-397, August 1999.

[36] J. Kohl, B. C. Neuman, The Kerberos Network Authentication Service (Version 5), IETF, RFC 1510, September 1993.

[37] R. Kohlas, U. Maurer, Reasoning about Public-Key Certification: On Bindings Between Entities and Public Keys, Proceedings of Financial Cryptography FC '99, 1999.

[38] L. M. Kohnfelder, Towards a Practical Public-Key Cryptosystem, MIT S.B. Thesis, 1978.

[39] R. Levien, A. Aiken, Attack resistant trust metrics for public key certification, Proceedings of the 7th on USENIX Security Symposium, str. 229-241, Januar 1998.

[40] U. Maurer, Modeling a Public-Key Infrastructure, Proceedings of 1996 European Symposium on Research in Computer Security (ESORICS' 96), E. Bertino (Ed.), Lecture Notes on Computer Science, Springer-Verlag, str 325-350, 1996.

[41] P.D. McDaniels, A. Rubin, A Response to 'Can We Eliminate Certificate Revocation Lists?', Proceedings of Financial Cryptography 2000, Februar 2000.

[42] P.D. McDaniels, S. Jamin, Windowed Certificate Revocation, Proceedings of IEEE Infocom 2000, str. 1406-1414, March 2000.

[43] S. Mendes, C. Huitema, A new approach to the X.509 framework: Allownig a global authentication without a global trust model, Proceedings of the 1996 Internet Society Symposium on Network and Distributed System Security, str. 172-189, 1996.

[44] S. Micali, Efficient Certificate revocation, Technical Report TM-542b, MIT Laboratory for Computer Science, Marec 1996.

[45] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, IETF, RFC 2560, Junij 1999.

[46] H. Nilsson, D. Pinkas, Validation of Electronic Signature, White Paper, http//:www.iD2tech.com.

[47] M.Nora, K. Nassim, Certificate Revocation and Certificate Update, Proceedings of the 7th USENIX Security Symposium, str. 217-228, Januar 1998.

[48] M. Nystr□m, J. Brainard: An X.509-Compatible Syntax form Compact Certificates, Secure networking – CQRE (secure) '99, R. Baumgart (Ed.), Lecture Notes on Computer Science, Springer-Verlag, str. 76-93, 1999.

[49] S. Petri, An Introduction to Smartcards, Litronic, 1998, http//:www.litronic.com/whitepaper.

[50] M. Reiter, S. Stubblebine, Authentication metric analysis and design. ACM Transactions on Information and System Security, Vol. 2, No. 2, Maj, 1999.

[51] M. Reiter, S. Stubblebine, Toward acceptable metrics of authentication, Proceedings of the 1997 IEEE Symposium on Security and Privacy, str. 10-20, Maj 1997.

[52] M. Reiter, S. Stubblebine, Path indenpendence for authentication in large-scale systems, Proceedings of the 4th ACM Conference on Computer and Communication Security, str. 57-66, April 1997.

[53] M. Reiter, S. Stubblebine, Resilient authentication using path independence, IEEE Transaction Computing, Vol. 47, str. 1351-1362, December, 1998.

[54] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM, Vol. 21, št. 2, str. 120-126, 1978.

[55] R. Rivest, B. Lampson, SDSI - A Simple Distributed Security Infrastructure, April 1996, http//:theory.lcs.mit.edu/~rivest/sdsi10.ps.

[56] R. Rivest, Can We Eliminate Certificate Revocation Lists?, R. Hirschfeld (Ed.), Financial Cryptography FC '98, Vol. 1465, str. 178-183, Februar 1998.

[57] RSA Laboratories, RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1, RSA Security Inc., May 2000.

[58] S/MIME, http://www.rsasecurity.com/standards/smime/ .

[59] SET, http://www.visa.com, http://www.mastercard.com .

[60] W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, 2nd Edition, ISBN: 0-13-869017-0, 1998.

[61] B. Schneier, A. Shostack, Breaking Up Is Hard To Do: Modeling Security Threats for Smart Cards, October 1999, http://www.counterpane.com.

[62] A. Shamir, N. Someren, Playing hide and seek with stored keys, http://www.ncipher.com/products/files/papers/anguilla/keyhide2.pdf.

[63] D. R. Stinson, Cryptography: Theory and Practice, CRC Press, Boca Raton Florida, ISBN: 0-8493-8521-0, 1995.

[64] D. Wagner, B. Schneier, Analysis of the SSL 3.0 protocol, November 1996, http://www.counterpane.com.

[65] P.R. Zimmermann, The Official PGP User's Guide, MIT Press, Cambridge, MA, 1995