SecureKey - SMS AVTENTIKACIJA

Bojan Sajovic
GenLan d.o.o., Slovenska c. 30, Ljubljana
bojan.sajovic@securekey.si , info@genlan.si

Povzetek

Odprtokodna osnova se je izkazala kot stroškovno in tehnično zelo učinkovita pri razvoju predstavljenega izdelka.

Preverjanje istovetnosti uporabnika oziroma avtentikacija je bistven postopek pri zagotavljanju varnosti podatkov in storitev v informacijskih sistemih. Eden najbolj zanesljivih načinov je enkratno geslo, saj zagotavlja, da gesla za prijavo ni možno prestreči in ponovno uporabiti. Mobilni telefon ima praktično vsak, za kogar želimo preveriti istovetnost. Ti dejstvi sta nas spodbudili, da smo razvili sistem za preverjanje istovetnosti uporabnika s pomočjo enkratnih gesel, posredovanih preko SMS sporočil. Uporabimo ga lahko za preverjanje istovetnosti pri dostopanju do zelo širokega nabora storitev in naprav, saj omogoča povezljivost z vsemi napravami in storitvami, ki znajo uporabljati RADIUS način preverjanja istovetnosti. Je enostaven za uporabo. Zasnovan je na odprtokodnih sistemih. Zmanjšuje število naprav, ki jih je treba nositi s seboj. Je v celoti plod domačega, slovenskega znanja in večmesečnega razvoja naših strokovnjakov, ki so v to vložili svoje bogate večletne izkušnje s področja varnosti in tehnologij informacijskih sistemov. Tudi v praksi se je že izkazal kot povsem konkurenčen tujim rešitvam s tega področja. V marsičem pa jih tudi prekaša, obenem pa je edini tovrstni produkt, ki podpira delo prek slovenskih mobilnih operaterjev.

Abstract

SMS Authentication

Open source has proven to be cost-effective and technically very effective in developing a product presented.

Authentication is a vital process in ensuring the security of data and services in IT systems. One of the most reliable ways of authentication is a unique password, as it ensures that the password can not be intercepted and reused. Mobile phone has virtually anyone for whom we want to verify identity. These facts have guided us to develop a system for verifying the identity of the user through one-time passwords, transmitted via SMS messages. It can be used to authenticate to a wide range of services and devices, as it offers connectivity with all the facilities and services that can use radius means of identification. It is easy to use. It is based on open source systems. It reduces the number of devices that must not be forgotten or lost. It is entirely the result of domestic, Slovenian know-how and several months of development from our experts, during which they used years of their rich experience in security technology and information systems. In practice this system has already proved to be quite competitive with other one-time password solutions. In many ways it even surpasses them.

Ključne besede

Preverjanje istovetnosti, avtentikacija, SMS, mobilna telefonija, radius, enkratno geslo, identiteta

Key words

Authentication, mobile phone, SMS, radius, one-time password, identity

1. AVTENTIKACIJA

Preverjanje istovetnosti uporabnika, za kar večinoma uporabljamo tujko avtentikacija, je eden od temeljnih postopkov pri zagotavljanju varnosti podatkov in storitev v informacijskih sistemih. Obenem je tudi eden od najbolj občutljivih členov pri zagotavljanju varnosti, saj je v veliki meri odvisen od uporabnikov.

V grobem jo delimo na preverjanje s pomočjo tistega kar vemo, tistega kar imamo in tistega, kar smo.

Kaj vemo?

Že v časih pred razvojem informacijskih tehnologij so za preverjanje istovetnosti s pomočjo »tistega kar vemo« uporabljali gesla. V vojski se je ob prihodu na menjavo straže moral novi stražar staremu izkazati z geslom, ki sta ga oba poznala, da ga je ta spustil do stražarskega mesta.

V današnjem svetu – svetu informacijskih tehnologij – je to po navadi povsem enostaven vnos gesla. Pa naj si bo to geslo za dostop do informacijskega omrežja, elektronske pošte ali pa vnos PIN-a (Personal Identification Number) ob odklepanju mobilnega telefona.

Ta način preverjanja istovetnosti je precej zanesljiv, če so izpolnjeni nekateri pogoji. A žal niso vedno. Izkušnje namreč kažejo, da lahko v večini primerov pridemo do približno desetine gesel tako, da obrnemo tipkovnico ali pa si pobliže ogledamo na ekrane prilepljene listke. Poleg tega so ta gesla marsikdaj tako enostavna, da se jih da zlahka uganiti.

Če je edini način preverjanja istovetnosti geslo, potem je nujno potrebno zagotoviti, da je dovolj »dobro«. Temu pogoju po navadi zadovoljimo tako, da ga izdelamo s pomočjo namenskega programa, ki ustvarja naključne nize znakov.

Da bi se izognili možnosti vdora v sistem s pomočjo uporabe gesla, ki ga je nekdo pridobil z opazovanjem, ugibanjem ali poskušanjem, mora biti geslo pogosto menjano in se, seveda, ob menjavah ne sme ponoviti.

Najboljše geslo je torej geslo, ki ga naključno ustvarimo s pomočjo namenskega programa, je časovno omejeno oziroma pogosto menjano, se ne ponovi in ga uporabimo samo enkrat ter takoj nato zamenjamo. Takega gesla ni mogoče uganiti, niti ponovno uporabiti.

Kaj imamo?

Tudi tisto, kar imamo je lahko dokaz istovetnosti. Vladarji srednjega veka so nosili pečatne prstane, s katerimi so potrjevali, da so res oni podpisali listino.

V svetu informacijskih tehnologij je »tisto, kar imamo« certifikat, shranjen na pametni kartici ali pa namenska naprava za enkratna gesla. Te naprave, v obliki kreditne kartice ali obeska za ključe prikazujejo časovno omejena enkratna gesla, izračunana po istem postopku kot ga uporablja strežnik, ki jih preverja.

Prednost dokazovanja istovetnosti s tem kar imamo je dobra varnost, saj bi nekdo drug zelo težko namesto nas za dokaz istovetnosti uporabil nekaj, česar nima.

Razen če tisto ima. »Tisto« moramo namreč vedno imeti. Tisto »nekaj« lahko izgubimo. Ali pa nam ukradejo. Ker certifikat oziroma generator enkratnih gesel potrebujemo samo ob prijavi, ne bi prav hitro opazili, da jih nimamo.

Kaj pa imamo vedno s seboj ?

Mobilni telefon.

Kaj smo?

Tisto, kar smo, je nedvomen dokaz istovetnosti. Saj ob preverjanju vedno dokazujemo prav to. Da smo, kar smo. Vsakdo je vedno tisto, kar je. Njegov prstni odtis se ne spreminja. Vzorec človeške šarenice ostane vedno enak.

Tistega, »kar smo«, se do nedavnega ni prav pogosto uporabljalo za dokazovanje istovetnosti. Še najbolj uporabljan način preverjanja te vrste je bil lastnoročni podpis. Ta je vedno podoben in značilen za posameznika. Ker pa ni zanesljivega in hitrega postopka za preverjanje, je tudi tega preveč lahko ponarediti, da bi se množično uporabljal.

Zanesljivih in hitrih postopkov preverjanja istovetnosti glede na to »kar smo« dolgo ni bilo. Šele v zadnjem času se je tehnologija dovolj razvila, da lahko hitro in zanesljivo preverimo istovetnost s pomočjo prstnega odtisa ali vzorca šarenice.

Prav zahtevna tehnologija je največja ovira za uporabo tega, sicer najzanesljivejšega načina. Potrebna je namreč namestitev namenskih naprav povsod, kjer želimo preverjati istovetnost. Za vsesplošno uporabo bi morali imeti take naprave na voljo v vseh mobilnih napravah in na javno dostopnih internetnih točkah, pa še kje. Skratka povsod, kjer lahko dostopamo do spleta in preko njega do storitev, ki lahko zahtevajo preverjanje. Zato se ta način ne uporablja prav pogosto.

Večfaktorska (dvofaktorska) prijava

Predvsem pri varnostno občutljivih dostopih, kot so dostopi iz spleta v omrežje podjetja oziroma organizacije ali pa dostop do tajnih podatkov, pogosto uporabimo vsaj dve metodi preverjanja hkrati, da tako zagotovimo čim večjo zanesljivost preverjanja istovetnosti. Na ta način močno otežimo, če ne celo povsem preprečimo možnost lažnega predstavljanja pri prijavi v sistem ali storitev.

Kot smo ugotovili, je zapletenost tehnologije največja ovira za uporabo preverjanja preko tega, kar smo. Ostaneta torej samo še ostali dve možnosti – »kaj vemo« in »kaj imamo«.

Pogosto je v uporabi z namensko napravo strojno (geselnikom) generirano enkratno geslo z dodanim PIN-om, saj zagotavlja, da gesla za prijavo ni možno prestreči in ponovno uporabiti. Največkrat uporabljane so SecureID, ActiveIdentity ali podobne »kartice« oziroma »obeski za ključe«.

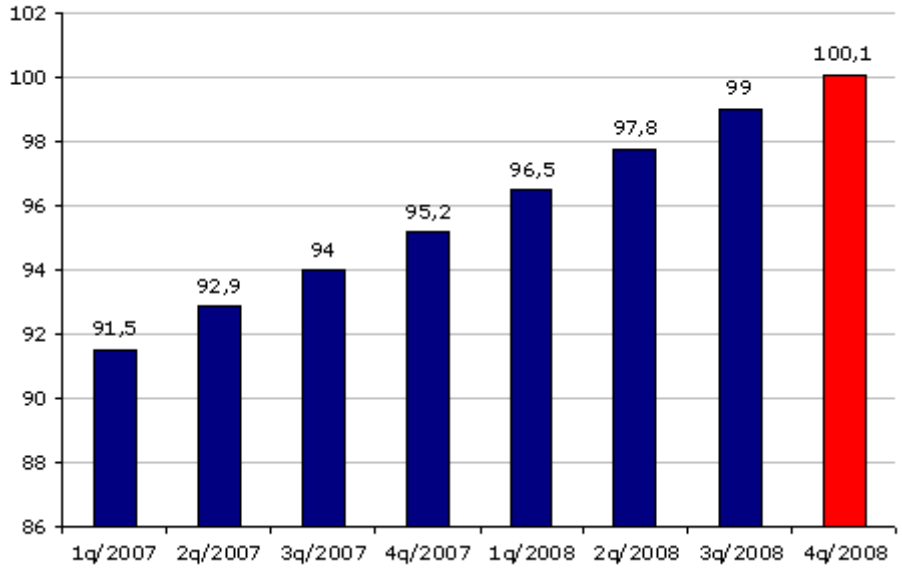
Ta način združuje tisto kar vemo (PIN, ki ga moramo vpisati skupaj z vsakokratnim geslom) ter tisto kar imamo – geselnik. Le-ta je majhen, lahek, enostavno izgubljiv oziroma pozabljiv ter v takem primeru neuporaben. Tega, da smo ga izgubili ne bomo niti opazili, dokler ga ne bomo potrebovali. Pa še ravno poceni ta oprema ni – ne kartica, niti licence in programska oprema, ki je na strežniški strani potrebna za uporabo.

Obstaja pa vsem nam zelo dobro znana naprava, ki jo imamo vedno seboj, poleg tega pa zelo hitro opazimo, če je nimamo. Mobilni telefon.

2. MOBILNA TELEFONIJA

Ker se nam ob razmišljanju o preverjanju istovetnosti vedno znova ponuja mobilni telefon, si zelo na kratko poglejmo stanje mobilne telefonije pri nas.

Penetracija (uporaba na število prebivalcev) mobilne telefonije v Sloveniji je že v zadnjem četrtletju leta 2008 presegla mejo 100% in dosegla 101,7% konec tretjega četrtletja 2009. To pomeni, da ima statistično gledano vsak slovenski državljan več kot en mobilni telefon. »Višek« gre na račun tega, da imajo nekateri en služben in en privatni telefon. Poleg tega se mobilne telefonske številke uporabljajo tudi za nekatere tehnične naprave (javljalniki požara, SMS prehodi telefonskih central in podobno).



Slika 1: Penetracija mobilnih uporabnikov v odstotkih (vir:APEK)

Mobilni telefon ima torej praktično vsak, za kogar želimo preveriti istovetnost.

Mobilni telefoni so si med seboj zelo različni. Nekateri podpirajo dostop do spleta ter dostop do elektronske pošte. Drugi spet omogočajo, da lahko gledamo filme in TV oddaje, na tretjih poslušamo ure in ure glasbe. Nekateri pa vseh teh dobrot ne nudijo. Vsem pa je skupno, da lahko, poleg telefoniranja, pošiljamo in sprejemamo SMS sporočila.

3. AVTENTIKACIJA + MOBILNA TELEFONIJA = SMS AVTENTIKACIJA

Med dolgoletnim delom z informacijskimi sistemi in njih uporabniki smo večkrat zaznali potrebo po cenovno dostopni rešitvi za varno preverjanje istovetnosti ob prijavi v čim širši nabor storitev.

Pri nekaterih je bila glavna težava potreba po stalni administraciji, saj uporabniki neprestano pozabljajo, zalagajo ali izgubljajo generatorje enkratnih gesel. Pri drugih, manjših strankah, je nabava namenske strojne opreme in licenc prevelik strošek, čeprav si želijo večje varnosti dostopa. Spet tretji s svojimi storitvami pokrivajo širok nabor uporabnikov, ki niso iz iste organizacije, ob dostopu do storitev pa je vseeno potrebno zagotoviti, da ne prihaja do zlorab ob prijavi. Logistika dostave namenskih naprav je v takem primeru precej velik problem.

Razmislek o zgoraj navedenih potrebah nas je ob upoštevanju dejstev glede penetracije mobilne telefonije vodil do ugotovitve, da lahko za dostavo enkratnega gesla med procesom preverjanja istovetnosti uporabimo kar mobilni telefon.

Očitno pa je tudi, da je uporabnikom pomemben čim manjši strošek implementacije ob zagotavljanju čim večjega nivoja varnosti.

Tako smo se odločili za razvoj sistema za preverjanje istovetnosti uporabnika s pomočjo enkratnih gesel, posredovanih s pomočjo SMS sporočil. Sistem smo imenovali **SecureKey**.

4. PREVERJANJE ISTOVETNOSTI S POMOČJO SISTEMA SecureKey

Izhodišča razvoja

Izhodišča razvoja sistema SecureKey so bila logična posledica zaznanih potreb uporabnikov.

- cenovna dostopnost storitve,
- združljivost s čim širšim naborom obstoječih naprav in storitev,
- enostavna administracija in nadzor,
- povezljivost s slovenskimi ponudniki mobilne telefonije,
- enostavna nadgradljivost z novimi moduli

Cenovna dostopnost

Da bi dosegli cenovno dostopnost storitve rešitev ni smela temeljiti na namenski strojni opremi. Prav tako zahteva po strojni opremi ni smela biti prevelika in ni smela predstavljati skritega stroška za uporabnika. Na najmanjšo možno mero smo želeli zmanjšati potrebo po licencah za operacijski sistem ali drugo potrebno programsko opremo.

Odločili smo se torej za edino smiselno možnost, uporabo odprtokodne programske opreme, na kateri smo gradili našo rešitev.

Združljivost

Pri združljivosti smo bili pozorni na dve področji. Potrebno je bilo zagotoviti, da je sistem uporaben pri preverjanju istovetnosti za čim večji nabor obstoječih storitev in naprav, po možnosti brez dodatnih posegov na njihovi strani. Poleg tega je nujna povezljivost z največkrat uporabljanimi imeniškimi storitvami, ki so vir podatkov o uporabnikih.

Večina naprav na trgu podpira RADIUS protokol za preverjanje istovetnosti, pravic in beleženje dostopov – s tujko AAA (Autenthication, Autorization, Accounting). Kot vir uporabniških podatkov se praktično povsod uporabljajo LDAP imeniki, najpogosteje Microsoft Active Directory ali pa Novell eDirectory.

Nujno je bilo torej zagotoviti tako LDAP kot tudi RADIUS združljivost.

Že cenovna dostopnost nas je vodila k temu, da smo izbrali odprtokodno osnovo. Tu se je pravilnost izbire osnove le potrdila. FreeRADIUS je odprtokodni AAA strežnik, ki ga je možno nadgrajevati z lastnimi rešitvami in je že v osnovi povezljiv z LDAP imeniki.

Uporabili smo ga kot osnovo in izdelali programske rešitve za ustvarjanje in preverjanje enkratnih gesel ter komunikacijo z mobilnimi ponudniki. Med razvojem smo naredili tudi nekaj knjižnic za povezavo na najpogostejše storitve in naprave. Vse je pripravljeno za

izdelavo dodatnih, če se bo za to pokazala potreba. Sistem je na ta način prilagodljiv potrebam skoraj vseh strank.

Enostavna administracija

Enostavna administracija v današnjih časih pomeni dostop do nastavitev sistema in dnevnikov delovanja preko spletnega vmesnika, saj to administratorju omogoča delo s katerekoli dosegljive delovne postaje. Za lažji nadzor delovanja mora biti omogočen izvoz v vsaj enega od standardnih formatov zapisa. Ker so informatiki dandanes precej obremenjeni, mora biti zagotovljeno, da je potrebno čim manj njihovega dela za učinkovito delovanje storitve. Administracija mora biti enostavna in lahko razumljiva.

V razvoj spletnega vmesnika, preko katerega so možne nastavitve sistema je bilo vloženega precej dela. V osnovi so pripravljene prednastavitve za Microsoft Active Directory in Novell eDirectory. Sistem je enostavno povezljiv tudi z drugimi LDAP imeniki. Enostavna je tudi vključitev novih dostopnih naprav ali storitev v sistem preverjanja istovetnosti.

Da je administratorjevega dela čim manj, je s pomočjo vmesnika, razvitega za končne uporabnike sistema omogočeno, da le-ti za neposredne uporabniške nastavitve poskrbijo kar sami. Uporabniki lahko – seveda samo vsak zase - sami nastavljajo PIN in telefonsko številko, na katero bodo preko SMS sporočil dobivali enkratna gesla.

Ob morebitni izgubi mobilnega telefona oziroma v primerih, da ga uporabnik kje pozabi, je omogočeno, da administrator nastavi časovno omejeno enkratno geslo za dostop za posameznega uporabnika, mu omogoči enkratno prijavo s pomočjo njegovega LDAP gesla, ali pa spremeni telefonsko številko, tako da enkratna gesla začasno dobiva na drug telefon. To je, poleg nadzora delovanja sistema tudi vse delo, ki po opravljeni začetni nastavitvi ostane administratorju.

Povezljivost s slovenskimi ponudniki mobilne telefonije

Pri razvoju SecureKey sistema smo veliko pozornosti posvetili temu, da bo združljiv z vsemi slovenskimi ponudniki mobilne telefonije, ki omogočajo storitev pošiljanja SMS sporočil preko internetne povezave v mobilno omrežje.

SecureKey ni edini sistem, ki omogoča pošiljanje gesel s pomočjo SMS sporočil. Je pa edini, ki to počne na način, ki ga omogočajo slovenski operaterji mobilne telefonije. Tako je njegova postavitev in vključitev pri strankah v Sloveniji možna brez dodatnih stroškov prilagajanja sistema.

Enostavna nadgradljivost z novimi moduli

Celoten razvoj, od začetka naprej je bil zastavljen tako, da je možno enostavno dodajanje novih modulov, v skladu s potrebami uporabnikov. Tako je mogoče SecureKey zgolj z dodatnim razvojem, brez posegov v obstoječi sistem, nadgraditi z rešitvami za pošiljanje gesel po drugih poteh, na primer preko elektronske pošte.

Prav tako je dokaj enostavno dodati preverjanje podatkov uporabnikov iz drugih virov, ne samo LDAP imenikov.

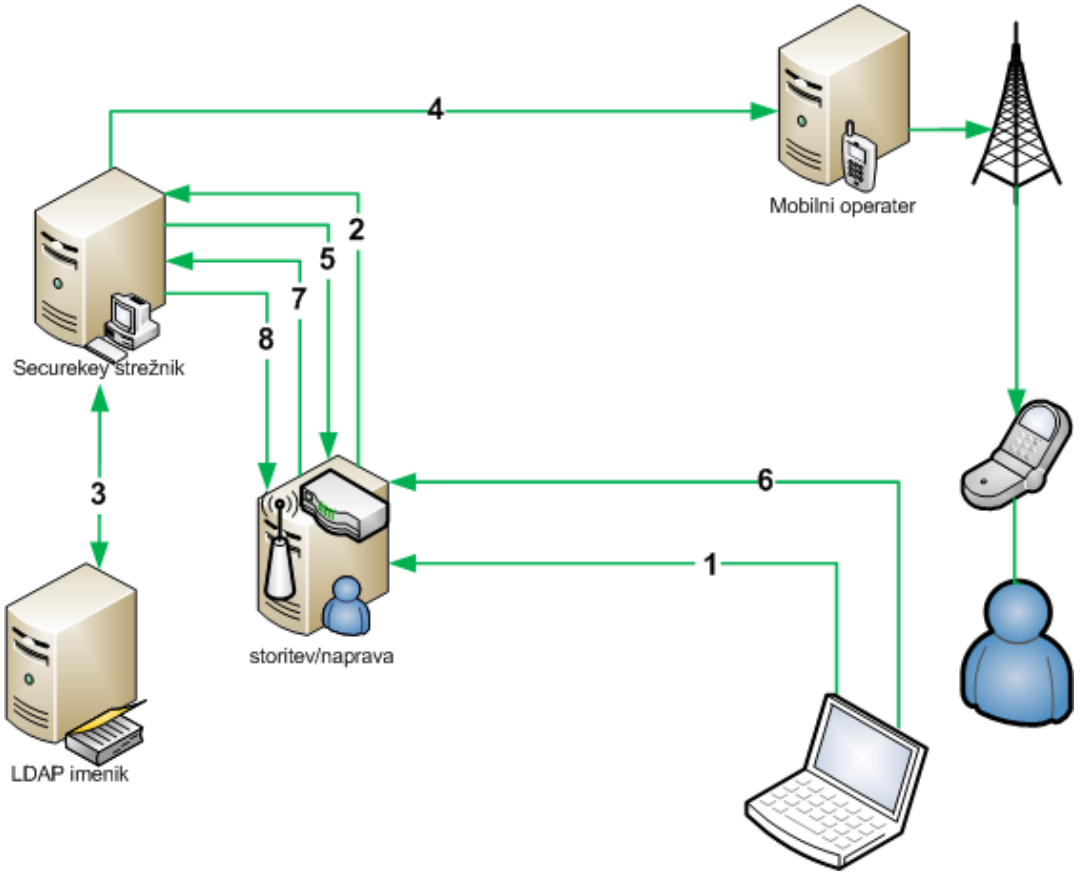
5. DELOVANJE SECUREKEY REŠITVE

Kako SecureKey deluje ? Delovanje je v osnovi zelo enostavno.

Uporabnik se sistemu predstavi s svojim uporabniškim imenom in PIN-om (tistim, kar ve). Sistem mu preko ponudnika mobilne telefonije pošlje SMS z enkratnim geslom (na mobilni telefon - tisto kar ima), nakar prijavo dokonča z vnosom dobljenega gesla.

Poglejmo si celoten potek še malo podrobneje.

1. Uporabnik se preko vmesnika storitve oziroma naprave prijavi s svojim uporabniškim imenom in PIN-om.
2. Storitev/naprava posreduje zahtevo po odobritvi dostopa SecureKey strežniku.
3. SecureKey strežnik preveri PIN uporabnika v LDAP imeniku. Če ni pravilen zavrne dostop.
4. Če je bil PIN pravilen, generira enkratno geslo, ga časovno označi in omeji ter pošlje preko internetne povezave mobilnemu operaterju v dostavo na uporabnikov mobilni telefon.
5. Strežnik zahteva od storitve/naprave dodatne podatke, z obvestilom, da naj uporabnik vnese po SMS-u posredovano enkratno geslo
6. Uporabnik vnese v SMS sporočilu prejeto geslo.
7. Storitev/naprava preveri dodatne informacije, torej vneseno geslo pri SecureKey strežniku.
8. Strežnik preveri pravilnost vnesenega gesla in sporoči napravi oziroma storitvi ali je prijava odobrena, ali ne.



Slika 2: delovanje SecureKey storitve

6. KAJ POTREBUJEMO ZA POSTAVITEV?

Edini finančni strošek, poleg licenc SecureKey rešitve, je mesečna naročnina v okviru pogodbe za vzpostavitev posredovanja SMS sporočil, sklenjene z mobilnim operaterjem.

Zahteve po strojni opremi, potrebni za postavitev SecureKey strežnika so majhne. Na strojni opremi z 1 GHz Pentium procesorjem in 1 GB delovnega spomina ter 20 GB velikim diskom lahko SecureKey preskušeno opravi vsaj 80 avtentikacij na sekundo (288000 na uro). To je povsem dovolj tudi za podjetja ali organizacije z večjim številom uporabnikov.

Strojna oprema take vrste so štiri do pet let stare delovne postaje, torej prav tiste, ki jih počasi odpisujemo. V vsaki organizaciji se da najti strojno opremo, ki jo lahko usposobimo v ta namen.

Če ima stranka na voljo virtualizacijsko okolje (VMware, XEN, Hyper-V), potem SecureKey sistem brez težav postavimo kot virtualni strežnik, saj za svoje delovanje potrebuje samo omrežno povezavo in dostop do interneta preko http/https protokola za dostavo SMS sporočil ponudniku mobilne telefonije. Sistem ne potrebuje nobene dodatne namenske strojne opreme. Nabava licenc za operacijski sistem ali drugo programsko opremo ni potrebna.

7. PREDNOSTI …

Kot vse rešitve ima tudi SecureKey svoje prednosti in slabosti. Ker smo izhajali iz želja in potreb strank, je prednosti veliko več.

Nedvomna prednost je ta, da je SecureKey osnovan na odprtokodnih tehnologijah. Zato je lahko finančno precej ugodnejši od drugih podobnih rešitev. Sistem ne potrebuje namenskih naprav, ne na strežniški strani, niti za izdelavo ali dostavo gesel.

Kaj pa varnost?

Poglejmo si najpogostejši način prijave z uporabo enkratnih gesel - v službeni sistem, od doma. Ugotovimo lahko, da se približno 10% uporabnikov prijavi enkrat na dan, ker zvečer še kaj postorijo od doma. 20% jih dela preko vikenda in se torej prijavijo enkrat ali dvakrat na teden. Skoraj vsi ostali pa le med prazniki ali počitnicami, torej enkrat na dva ali tri mesece. Že skupina, ki namenske naprave največ uporablja, bi izgubo le-te ugotovila šele čez kak dan.

Prva prednost sistema SecureKey je ta, da namenske naprave ne moremo izgubiti. Ne morejo nam je niti ukrasti. Saj je nimamo. V primeru izgube naprave je posledica ta, da se v želene sisteme ne moremo prijaviti, dokler je ne nadomestimo z drugo. V primeru izgube mobilnega telefona in uporabe SecureKey-a pa lahko administrator preusmeri gesla na drug telefon (ženin, otrokov, …).

Izginotje telefona zaznamo kmalu. Izgube ali kraje naprave za enkratna gesla, kot smo lahko videli, vsaj 70% uporabnikov ne bi prav kmalu ugotovilo. S tem ima morebitni napadalec ali tat tudi ustrezno več časa za poskus vdora v sistem s pomočjo ukradene naprave.

Dejstvo je, da so gesla, poslana preko SMS sporočila zelo varna rešitev, saj so izdelana s pomočjo generatorja naključnih števil in se jih v omejenem času njihove veljavnosti ne da ugotoviti s poskušanjem. Gesla na namenskih napravah so izračunana na podlagi določenega matematičnega algoritma, saj se mora enak postopek izvajati tudi na strežniku, da jih le-ta lahko preverja. Kodo, ustvarjeno s predpisanim in nespremenljivim postopkom je laže ugotoviti, kot naključno kodo v omejenem času.

SecureKey način preverjanja istovetnosti prinaša še dodatno prednost glede varnosti dostopa. V primeru poskusa vdora z ugibanjem PIN-a in gesel je uporabnik takoj opozorjen, saj prične na svoj telefon dobivati sporočila. Poskus vdora v SecureKey sistem na ta način torej nima smisla. Poleg tega sistem omogoča tako imenovani »Intruder lockout« - zaklepanje uporabniškega računa v primeru zaporednih neuspelih poskusov prijave.

Sistem lahko uporabimo za preverjanje istovetnosti pri dostopanju do zelo širokega nabora storitev in naprav, saj omogoča povezljivost z vsemi napravami in storitvami, ki znajo uporabljati radius način preverjanja istovetnosti. In to so skoraj vse naprave – od velikih strežnikov do majhnih dostopnih točk za brezžična omrežja, ki jih lahko kupimo v bližnji veleblagovnici.

8. … IN SLABOSTI

Bistvena prednost storitve SecureKey je hkrati tudi njena glavna potencialna slabost.

SecureKey je odvisen od delovanja mobilnega operaterja. Bolje rečeno od delovanja njegove storitve pošiljanja SMS sporočil. A slabost je bolj teoretična kot praktična, saj v več kot pol leta testiranj in redne uporabe sistema nismo zaznali nobenih tovrstnih težav.

Da bi tudi to slabost čim bolj omejili smo v SecureKey vgradili možnost uporabe redundančnih operaterjev. Uporabimo lahko torej oba slovenska mobilna operaterja, ki omogočata storitev pošiljanja SMS, tako da v primeru težav pri enem od operaterjev sistem samodejno dostavi geslo preko drugega.

Kot morebitna slabost ostane torej samo še možnost nedostave SMS sporočila zaradi nedosegljivosti signala mobilnega operaterja. Vendar pa v takem primeru tudi ni pričakovati, da bi se lahko povezali v svetovni splet in potrebovali preverjanje istovetnosti.

9. ZAKLJUČEK

SecureKey je sistem preverjanja istovetnosti s pomočjo enkratnih gesel, posredovanih preko SMS sporočil. Je enostavnejši in primernejši za uporabo v primerjavi z drugimi rešitvami preverjanja istovetnosti z metodo enkratnega gesla, saj zmanjšuje število naprav, ki jih je treba nositi s seboj, hkrati pa prinaša večjo varnost in manj administracije.

Je plod domačega, slovenskega znanja in večmesečnega razvoja naših strokovnjakov, ki so v to vložili svoje bogate večletne izkušnje s področja varnosti in tehnologij informacijskih sistemov.

Sistem je tudi operativno v uporabi in se je tudi v praksi že izkazal kot povsem konkurenčen tujim rešitvam s tega področja. V marsičem pa jih tudi prekaša.

VIRI IN LITERATURA

[1] WIKIPEDIA: Two factor authentication. [URL: http://en.wikipedia.org/wiki/Two-factor_authentication], 29.2.2010

[2] SiOL : Penetracija mobilne telefonije porasla na 101,7 odstotka. [URL: http://www.siol.net/tehnologija/telekomunikacije/2009/12/penetracija_mobilne_telefonije_porasla_na_1017_odstotka.aspx] , 15.2.2010

[3] RIS : Penetracija mobilnih uporabnikov v Sloveniji presegla 100 odstotkov. [URL:http://www.ris.org/index.php?fl=2&lact=1&bid=10495&db=34&parent=27], 2.3.2010