Mehanizmi za overjanje dostopa do informacijskega sistema

Sašo Žurga, študent, Fakulteta za varnostne vede, Univerza v Mariboru

Namen prispevka
Ker so podjetja v današnji dobi v tesni povezavi z varnim delovanjem informacijskih sistemov so v samih podjetjih potrebni različni mehanizmi za overjanje, s pomočjo katerih sistem za nadzor dostopa preveri identiteto posameznika. Zaščita podatkov znotraj sistema, kot tudi zagotavljanje varnosti v širšem pomenu besede, se lahko zagotovi s postopkom ugotavljanja identitete. Pa naj v tem pogledu govorimo o šibkem overjanju, močnem overjanju, kombinaciji obeh metod ali o biometričnih metodah. Nadalje prav tako zaposleni s svojim ravnanjem pripomorejo k varovanju podatkov ter informacij s katerimi se srečujejo v okviru svojih službenih dolžnosti.

Metodologija
V prispevku je uporabljena deskriptivna metodo, kjer sem s pomočjo primarnih in sekundarnih virov opisal osnovne pojme. V nadaljevanju sem uporabil razlagalno metodo in kompilacijo.

Ugotovitve
Za opravljanje procesa dela se s pomočjo overjanja omeji možnost zlorabe informacijsko komunikacijskih tehnologij zaposlenim in kakršnekoli manipulacije s podatki, ki bi morda namenoma ali ne namenoma lahko ogrozili ali škodovali informacijski varnosti znotraj podjetja. Overitev uporabnika je običajno izvedena s pomočjo gesel, ki pa na žalost predstavljajo šibek člen v celotni overitveni shemi.

Izvirnost/pomembnost
Prispevek predstavlja različne metode overjanja, ki se uporabljajo za učinkovito zaščito nepooblaščenega dostopa do informacijskega sistema. Ugotovitve prispevka so namenjene uporabnikom informacijskih sistemov v podjetjih za zagotavljanje učinkovite zaščite s pomočjo mehanizmov za overjanje.

Ključne besede: gesla, identiteta, informacije, overjanje, varnost.

1 UVOD

Z elektronskim poslovanjem se povečuje pretok informacij preko omrežja, ki je vsem dostopen. Da bi preprečili dostop in uporabo teh informacij tretjim osebam, je potrebno uvesti določene ukrepe. Ti ukrepi so vse bolj pomembni, saj bodo tudi v prihodnosti podjetja prenašala vedno več podatkov preko omrežij. Posluževanje mehanizmov za overjanje ali s postopkom ugotavljanja identitete se lahko zaščitijo podatki znotraj sistema in posledično s tem zagotavljanje varnosti in neokrnjenosti podatkov.
Ker se uvaja v poslovanje vse več tehnologije, lahko trdimo, da poleg konkurenčnosti in hitrejšega poslovanja, kar predstavlja pozitivno stran tehnološkega napredka, postanemo obenem tudi bolj ranljivi in na ta način izpostavljeni zlorabam naših podatkov. Več podatkov delimo na omrežju, večja je možnost zlorabe. Zato je pomembno pravilo, da znamo zaščititi naše podatke in opremo in na ta način tudi upravičiti zaupanje strank, s katerimi poslujemo.

2 ŠIBKO OVERJANJE

Šibko overjanje je kriptografski način overjanja med predhodno neznanima uporabnikoma brez zanašanja na tretjo osebo, ki ji v celoti zaupata. Pod šibko overjanje bi lahko prištevali :

- - gesla,
- - enkratna gesla.

2.1 Gesla

Gesla so v računalništvu niz znakov, ki se uporabljajo za overitev uporabnikov računalniškega sistema in posledično za preprečevanje nepooblaščenega dostopa. Pod pojmom računalniškega gesla štejemo več dejavnikov: velikost gesel, oblika gesel (velike in male črke, števila, fraze), občasno menjavanje gesel, starost gesla, omejeno število prijav s pomočjo gesla ter zaščita gesel (Buser, 2009).

2.2 Enkratna gesla

Enkratna gesla (one-time password) so gesla, ki so veljavna le za eno sejo ob prijavi. Poglavitna prednost enkratnih gesel je ta, da jih je mogoče uporabiti samo enkrat, saj po uporabi postanejo neveljavna. Napadalec se naknadno ne more prijaviti z enakim geslom. Dodatna lastnost enkratnih gesel je njihova "naključnost". Nemogoče je namreč iz trenutnega enkratnega gesla napovedati ali ugotoviti prihodnja gesla (Holbl, 2007).

2.2.1 Pametne kartice

Pametne kartice so nadomestile uporabo magnetnih kartic, ki so sicer cenejše, vendar predstavlja večjo možnost nevarnosti za zlorabo za uporabnika. To potrjuje dejstvo, da je lažje prekopirati zapis iz magnetne kartice s pomočjo posebne naprave. V primerjavi z magnetno kartico, dovoli pametna kartica e-podpisovanje le z vnosom gesla. Prav tako preveri ali je terminal originalen. Tak postopek je vsekakor bolj varen, saj predstavlja pametna kartica brez osebnega gesla neuporabnost kot tako (Buser, 2009).
Obstajajo trije pomembnejši principi delovanja tovrstnih kartic (Jurišić, 2008):

- izziv/odgovor: strežnik pošlje naključno število, uporabnik ga s to kartico zašifrira in vrne rezultat. Na drugi strani strežnik šifrira isto naključno število in primerja rezultata.
- sinhronizacija z uro: vsakih 60 sekund kartica izpiše zašifrirano število. Strežnik, sinhroniziran s kartico, prejeto število dešifrira in preveri rezultat.
- ujemanje z dogodkom: enkratno geslo je odvisno od števila dosedanjih overjanj.

Za razliko od močnega overjanja se lahko poslužujemo šibkega overjanja zaradi dejstva, da določene aplikacije zahtevajo manjšo stopnjo zahtevane varnosti po zaščiti. Seveda, kar pa predstavlja odločilen dejavnik, so pa analize možnosti napada na sistem in finančne zmogljivosti. Če ocenimo, da potrebujemo večjo stopnjo varnosti na področju informacij pa si na tej stopnji zagotovimo močno overjanje.

3 MOČNO OVERJANJE

Ob uporabi močnega overjanja nam ta zagotavlja boljšo zaščito za občutljive podatke, kot nam bi to zagotavljala navadno uporabniško ime in geslo. Močno overjanje, še posebno v kombinaciji z ostalimi metodami overjanja zagotavlja močno zagotovilo po varnosti pri finančnih transakcijah, pri katerih dva subjekta uporabljata tretjo osebo, ki ji v celoti zaupata.

3.1 Simetrična kriptografija

Simetrična kriptografija uporablja isti ključ za šifriranje in dešifriranje med pošiljateljem in prejemnikom, to pa zagotavlja dvojno funkcionalnost. Ključ je pri tej metodi tajen, kar pomeni, da se od vsakega uporabnika pričakuje, da ohrani ključ tajen in primerno zaščiten. Zato v primeru, da ključ pride v roke vsiljivca, lahko le-ta s tem ključem dešifrira kakršnakoli prestrežena sporočila. Torej šifriranje je običajno hitro, težje pa je varno izmenjati ključ. Glavni problemi pri tej metodi so (Alexander, 2006):

- Distribucija ključa,
- Celovitost podatkov,
- Ne zmožnost zatajitve.

Vsak uporabnik mora imeti za vsakega dopisovalca poseben ključ. Tu se na ta način pojavi zmeda, predvsem zaradi dejstva, da s tem število ključev raste v skladu s številom uporabnikov. Ker oba uporabnika uporabljata enak ključ za šifriranje in dešifriranje sporočil, lahko na eni strani simetrični šifrirni sistem zagotovi zaupnost, hkrati pa ne zagotavlja overitve. Namreč ne obstaja način, da bi dokazali, kdo je dejansko poslal sporočilo, ker obe osebi uporabljata enak ključ (Hariss, 2001).
Ključi pri simetrični kriptografiji so drugačni kot pri asimetrični. Simetrična kriptografija se pogosto uporablja v kombinaciji z asimetrično.

3.1.1 Kerberos

Kerberos je omrežni protokol za namen overjanja, ki deluje na podlagi kart. Gre za sistem, ki temelji na simetrični kriptografiji pri kateri subjekta za potrebe overjanja uporabljata tretjo osebo, ki ji v celoti zaupata. Kerberos tako vključuje strežnik za overjanje, kot strežnik za dodeljevanje kart. Pri strežniku za overjanje (Authentication Server – AS), overjanje ob prijavi poteka na podlagi dolgotrajnega ključa. Strežnik za overjanje dodeli subjektu karto TGT (ticket granting ticket) ter kratkotrajni ključ za komunikacijo s strežnikom za dodeljevanje kart. V tem primeru strežnik za overjanje zagotavlja samo overjanje (MIT Kerberos, 2011).
Strežnik za dodeljevanje kart (Ticket Granting Server-TGS) pa služi z overjanjem na podlagi kratkotrajnega ključa in karte TGT (ticket granting ticket). Omenjeni strežnik izdaja subjektu elektronske karte za dostop (tickets), ki mu omogočajo dostop do storitev in drugih računalnikov. Strežnik za dodeljevanje kart nam zagotavlja avtorizacijo oziroma nadzor dostopa (MIT Kerberos, 2011).
Prednosti Kerberosa:

- Gesla niso na voljo prisluškovalcem,
- Gesla vnesemo samo v lokalni računalnik, kar pomeni, da ga strežnik ne pozna,
- Geslo vnesemo samo enkrat (enkratna prijava),
- Lažje je zaščititi manjše število računalnikov.

Slabosti Kerberosa:

- Brez preklica: namreč karte TGT (ticket granting ticket) so veljavne do izteka veljavnosti, običajno 10 ur. Vprašanje na mestu je kaj če pride medtem do zlorabe?
- Upravljanje s ključi znotraj domene (dolgotrajni ključi morajo biti vnaprej določeni med strežnikom za overjanje in strežnikom za dodeljevanje kart, le-tem in strežniki ter med strežnikom za overjanje in odjemalci)
- Razpoložljivost (strežnik za overjanje in strežnik za dodeljevanje kart morata biti na voljo ves čas).

Prednosti in slabosti, ki so naštete zgoraj predstavljajo skupek dobrih in slabih lastnosti Kerberosa, kot rešitve za omrežje, pri katerem se srečujemo z varnostnimi problemi. Če povzamemo te lastnosti je orodje za overjanje z močno kriptografijo, z namenom, da nam omogoča varnost podatkov.

3.2 Asimetrična kriptografija

Asimetrična kriptografija deli ključ v javni in zasebni del. Pri šifriranju sporočila je vedno potreben javni del ključa prejemnika. Za dešifriranje pa zasebni del ključa prejemnika. Javni del ključa si lahko vsak ogleda in zato ga lahko pošiljamo preko nezavarovanih kanalov oziroma preko javnih omrežij. Zasebni del ključa ostane pri lastniku ključa (Vidmar, 2002).
V primeru, da je zaupnost najpomembnejša varnostna storitev pošiljatelju, bi šifrirali datoteko s prejemnikovim javnim ključem. V tem primeru lahko datoteko dešifrira le oseba, ki ima pripadajoči zasebni ključ (Hariss, 2001).
Ko pa je pošiljatelju najpomembnejša varnostna storitev overitev, takrat bi zašifrirali sporočilo z zasebnim ključem. To prejemniku zagotavlja, da je edini osebek, ki je lahko šifriral sporočilo, posameznik, ki poseduje ta zasebni ključ. Če bi sporočilo pošiljatelj šifriral s prejemnikovim javnim ključem, overitev ni zagotovljena, kajti javni ključ je razpoložljiv vsakomur (Hariss, 2001).

3.2.1 Digitalno potrdilo

Digitalno potrdilo javnega ključa (public key certificate) je digitalni dokument, ki potrjuje povezavo med javnim ključem in osebo ali institucijo ali strežnikom. Z njim lahko preverimo, komu pripada javni ključ. Potrdilo vsebuje javni ključ in informacijo o njegovem imetniku, ki ju podpiše oseba ali institucija, ki ji zaupamo. Potrdila so objavljena v splošno dostopnih imenikih ali na spletnih straneh. Uporabljamo jih za identifikacijo v elektronskem poslovanju (Vidmar, 2002).
Oblike potrdil glede na izdajatelja potrdila v Sloveniji (Ministrstvo za visoko šolstvo, znanost in tehnologijo, 2011):

1. HALCOM:
   - standardna kvalificirana digitalna potrdila,
   - napredna kvalificirana digitalna potrdila.
2. MJU SIGEN-CA (Slovenian General Certification Authority) je izdajatelj kvalificiranih digitalnih potrdil overitelja na Ministrstvu za javno upravo (MJU) za fizične osebe in poslovne subjekte. Izdaja:
   - spletna kvalificirana digitalna potrdila in
   - posebna kvalificirana digitalna potrdila.
3. MJU SIGOV-CA (Slovenian Governmental Certification Authority) je izdajatelj kvalificiranih digitalnih potrdil overitelja na Ministrstvu za javno upravo (MJU) za državne organe. Izdaja:
   - spletna kvalificirana potrdila in
   - posebna kvalificirana potrdila.
4. POŠTA SLOVENIJE:
   - standardna kvalificirana digitalna potrdila,
   - napredna kvalificirana digitalna potrdila.
5. AC NLB (Agencija za certificiranje Nove Ljubljanske Banke) izdaja:
   - Kvalificirana potrdila za varen elektronski podpis.
6. MINISTRSTVO ZA OBRAMBO:
   - kvalificirano digitalno potrdilo,
   - nekvalificirano digitalno potrdilo.

4 BIOMETRIJA

Biometrično pomeni, merjenje nezamenljivih in nespremenljivih telesnih značilnosti, na podlagi katerih lahko človeka identificiramo. K nezamenljivim značilnostim ljudi spadajo obraz, prstni odtis, geometrija roke, glas in oči. V informacijski tehnologiji povezujemo biometrijo s tehnologijo za merjenje in analizo človekovih lastnosti z namenom overjanja.
Značilnosti, ki ustrezajo za potrebe biometrije so (Abts in Mulder, 2009):

- Biometrična značilnost mora biti prisotna pri vsakem uporabniku,
- Značilnost mora biti pri vsakem uporabniku drugačna,
- Značilnost naj se ne bi skozi en časovni razpon spreminjala ali pa le malo,
- Značilnost se mora s tehnologijo zaznati.

Biometrične metode se delijo na statične in dinamične. Pri statičnih ali fizioloških gre za preverjanje na podlagi lastnosti posameznika, ki so vedno prisotne (prstni odtis, mrežnica, šarenica, oblika dlani).
Pri dinamičnih pa se preverja na podlagi določenih vzorcev obnašanja (podpis, govor) (Abts in Mulder, 2009).
Dejstvo je, da so te vrste oziroma sistemi overjanja precej draga naložba, kot tudi kasnejše vzdrževanje. Kot rezultat tega pa je, da tovrstni sistemi služijo varovanju občutljivih in zaupnih informacij.
Niso pa biometrične metode overjanja nezmotljive, niti niso nedostopne s strani napadalca. Lažje je namreč izvesti napad na shranjeno bazo primerjalnih vzorcev na napravi, kot pa je kopirati edinstvene telesne značilnosti. In ravno na tem področju se kaže slabost sistemov overjanja, ki delujejo na podlagi biometrije (RSA Security, 2011).

4.1 Primer gumijastih prstov

Naslednji primer pa nazorno prikazuje nasprotje pravila, da je lažje izvesti napad na shranjeno bazo, kot pa kopirati telesne značilnosti. Japonski kriptograf iz Yokohama University je leta 2002 uspel dokazati zmotljivost senzorjev za prepoznavo prstnih odtisov. Proizvajalci tovrstne opreme so seveda trdili, da je ta oprema zelo zanesljiva, in je odporna na razne poskuse preslepitve senzorjev (Schneier, 2002).
Eksperimenta se na začudenje javnosti in tudi podjetij, ki proizvajajo tovrstne senzorje za prepoznavo prstnih odtisov, ni lotil z dragimi sestavinami ali izdelave v specializiranih laboratorijih. Uporabil je namreč enostavno želatino, katero je vliv v pripravljen plastičen model lastnega odtisa prsta. S tem načinom je pretental vseh 11 senzorjev, ki so takrat veljali za najboljše na področju komercialne uporabe (Schneier, 2002).

4.2 Zakonski pogoji za dopustnost biometrije v zasebnem sektorju

Izvajanje biometrijskih ukrepov se delodajalci največkrat poslužujejo za potrebe oziroma namen evidentiranja prisotnosti na delovnem mestu in za namene opravljanja dejavnosti in varovanja premoženja oziroma poslovnih skrivnosti. Delodajalec lahko uvede biometrijo le nad svojimi zaposlenimi, pred uvedbo biometrije pa mora delodajalec pridobiti tudi odločbo informacijskega pooblaščenca, če izvajanje določenih biometrijskih ukrepov v zasebnem sektorju ni urejeno z zakonom. Dokler odločbe ne pridobi, biometrije ne sme izvajati (Pirc Muser 2006).
Biometrijo se dovoljuje (Informacijski pooblaščenec, 2008):
Za javni sektor je to dovoljeno kadar tako določa zakon (npr. Zakon o potnih listinah državljanov Republike Slovenije), izjemoma na podlagi posebnih zakonskih določil tudi za vstop v stavbo ali dele stavb in evidentiranje zaposlenih na delu.
Za zasebni sektor pa velja, da se lahko tovrstne ukrepe uporablja le, če so nujno potrebni za:

- opravljanje dejavnosti,
- varnost ljudi ali premoženja,
- varovanje tajnih podatkov ali
- varovanje poslovne skrivnosti.

Biometrijo je vsekakor smiselno uporabiti pogosto v kombinaciji z močnim overjanjem, kjer je dejansko poleg dokaza o edinstvenih telesnih značilnostih, potrebno uporabiti tudi geslo za dostop.

5 ZAKLJUČEK

Gesla v celotni shemi varnega postopka overjanja, predstavljajo šibek člen, vendar so v praksi največkrat uporabljena metoda za preverjanje identitete.
Tako kot pri klasičnem poslovanju je pri elektronskem poslovanju prav tako pomembna informacija o osebah, ki v elektronskem poslovanju sodelujejo. To nam zagotavljajo digitalno potrdilo, ki ga izdaja kvalificirani overitelj, ki nam pomaga pri identifikaciji »pravega« subjekta, obenem pa nam na ta način s pomočjo asimetričnega kodiranja zagotavlja, da bo informacija dostopna le tistemu, ki je namenjena.
Biometrične metode v kombinaciji z identifikacijskimi karticami predstavljajo velik tehnološki napredek pri samem procesu overjanja. Namreč nezamenljive lastnosti, ki jih ima vsak posameznik različne se lahko merijo s pomočjo čitalcev ali podobnih naprav, ki pa morajo prav tako ugotoviti, da gre pri poskusu identifikacije za živo biometrično lastnost primera. Namreč možnost je tudi, da lahko pride do zlorabe poskusa identifikacije s pomočjo npr. Prstnega odtisa »gumijaste roke«, kot smo zasledili v primeru japonskega kriptografa. Dejstvo je, da so te vrste oziroma sistemi overjanja precej draga naložba, kot tudi kasnejše vzdrževanje. Kot rezultat tega pa je, da tovrstni sistemi služijo varovanju občutljivih in zaupnih informacij.
Kljub temu pa biometrične metode, kljub pozitivnemu napredku na tehnološkem nivoju, nazadujejo na področju vdora v posameznikovo integriteto.

VIRI

Abts D. in Mulder W. (2009). Grundkurs Wirtschaftsinformatik. Weisbaden: Vieweg+teubner

Alexander, M. (2006). Netzwerke und Netzwerksicherheit: Das Lehrbuch. Heidelberg: Huthig

Buser, L. (2009). Varnost elektronskih plačilnih sistemov. Diplomsko delo. Maribor. Ekonomsko-poslovna fakulteta

Ministrstvo za visoko šolstvo, znanost in tehnologijo. Register overiteljev v Republiki Sloveniji. Pridobljeno 2.1. 2012 na http://www.mvzt.gov.si/fileadmin/mvzt.gov.si/pageuploads/pdf/informacijska_druzba/signed-REGISTER_OVERITELJEV_V_RS_ver27__05.12.2011m.pdf

Hariss, S. (2001). CISSP All-in-One Exam Guide, Chapter 8 Cryptography. Pridobljeno 2.12 2011 na http://www.cccure.org/Documents/Cryptography/cisspallinone.pdf

Holbl, M. (2007). Enkratna gesla - večja varnost. Pridobljeno 2.1. 2012 na http://www.monitor.si/clanek/enkratna-gesla-vecja-varnost/

Informacijski pooblaščenec. (2008). Smernice glede uvedbe biometrijski ukrepov. Pridobljeno 27.12. 2011 na https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Biometrija_-_smernice.pdf

Jurišić, A. (2008). Kriptografija in teorija kodiranja. Pridobljeno 27.12. 2011 na http://lkrv.fri.uni-lj.si/~ajurisic/kitk2-08/folije/p01.pdf

MIT Kerberos (2011). Kerberos: The Network Authentication Protocol. Pridobljeno 29.11. 2011 na http://web.mit.edu/kerberos/

Pirc M., N. (2006). Neodvisni nadzor in varstvo osebnih podatkov. Pravna praksa, 25(35), 6-10.

RSA Security. (2011). Information Security Glossary. Pridobljeno 28.12. 2011 na http://www.rsa.com/glossary/

Schneier, B. (2002). Crypto-Gram Newsletter. Pridobljeno 27.12. 2011 na http://www.schneier.com/crypto-gram-0205.html

Vidmar, T. (2002). Informacijsko komunikacijski sistem. Ljubljana: Pasadena.