ZAGOTAVLJANJE VARNEGA DOSTOPA DO STORITEV

mag. Tomaž Aljaž, univ. dipl. inž; Selim Tolaj, univ. dipl. inž.

Povzetek— **Z nenehnim tekmovanje po konkurenčnosti in ponudbi storitev je postalo nujno, da podjetja ponudijo svoje produkte in storitve preko interneta in klicnih linij. Pri tem pa morajo na enostaven način omogočiti dostop do informacij, ki jih želijo uporabniki.**
Poleg overovitev uporabnika na sami aplikaciji, je ključnega pomena njegova overovitev na samem dostopu do omrežja v katerem se nahajajo storitve.
Pri klicnem dostopu je na razpolago nekaj overovitvenih protokolov, kateri omogočajo bolj ali manj varen način overovitve. Možni so dodatni varnostni mehanizmi in tehnologije, ki dodatno povečajo stopnjo varnosti pred nepooblaščenim dostopom do omrežja in varovanju prenešenih podatkov oz. informacij.
Dostop iz interneta v omrežje, kjer se nahajajo storitve, je običajno najbolj varovan. V sedanjem konkurenčnem boju je nujno za podjetja, da ponudijo svoje storitve tudi prek interneta. Na ta način odprejo lokalne storitve v internet. Tudi tukaj so izredno pomembni varnostni mehanizmi in tehnologije, ki so uporabljene za povezovanje uporabnikov do teh storitev.
V članku bodo opisani varnostni mehanizmi in tehnologije, ki so lahko uporabljeni pri klicnem dostopu ali dostopu iz interneta. Prikazani pa bodo tudi trendi internetnih aplikacij.

***Ključne besede*—Oddaljen dostop, VPN, PPP, varnost.**

I. UVOD

Z nenehnim tekmovanje po konkurenčnosti in ponudbi storitev je postalo nujno, da podjetja ponudijo svoje produkte in storitve preko interneta in klicnih linij. Pri tem pa morajo na enostaven način omogočiti dostop do informacij, ki jih želijo uporabniki (kupci oz. stranke).
Poleg overovitev uporabnika na sami aplikaciji, je ključnega pomena njegova overovitev na samem dostopu do omrežja v katerem se nahajajo storitve. V grobem lahko razdelimo dostop do storitev na dva dela:

- oddaljen dostop prek klicnih linij in
- oddaljen dostop iz interneta.

II. ODDALJEN DOSTOP PREK KLICNIH LINIJ

Oddaljen dostop prek klicnih linij omogoča uporabnikom (oddaljenim uporabnikom), da se povežejo prek javnega telefonskega omrežja na strežnik oddaljenega dostopa (ki se nahaja npr. v podjetju). Na ta način naredijo začasno fizično ali navidezno povezavo do njega. Po uspešni overovitvi na strežniku oddaljenega dostopa postanejo transparentno povezani v omrežje na katerega je strežnik oddaljenega dostopa povezan. Takšna transparentna povezljivost omogoča oddaljenim uporabnikom, da se povežejo iz oddaljenih lokacij in dostopajo do virov kot, da bi bili fizično priključeni v omrežje, vendar je hitrost prenosa (bistveno) manjša kot v lokalnem omrežju.
Protokol, ki omogoča takšen način povezovanja se imenuje Point-to-Point Protocol (PPP).
V nadaljevanju so opisani različni načini overovitve oddaljenih uporabnikov.

A. Overovitveni protokoli

Za overovitev uporabnikov se uporabljajo različni overovitveni protokoli, med kateri sta najbolj poznana Password Authentication Protocol (PAP) [1] in Challenge Handshake Authentication Protocol (CHAP) [2]. Microsoft pa ima svoje izpeljanke kot npr. MS-CHAP [3].

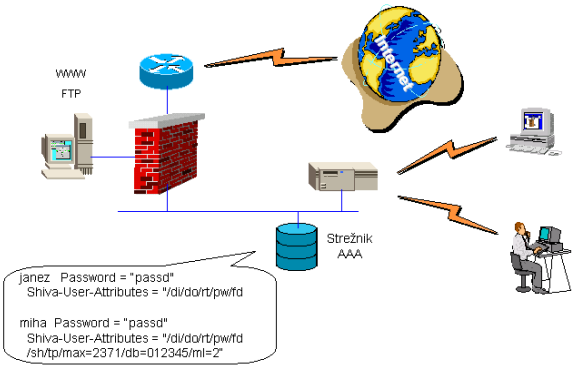
```
PPPPAP: Authenticate Request, ID = 0x 2
    PPPPAP: Code = Authenticate Request
    PPPPAP: ID = 2 (0x2)
    PPPPAP: Length = 17 (0x11)
    PPPPAP: Peer ID Length = 5 (0x5)
    PPPPAP: Peer ID = aljaz
    PPPPAP: Password Length = 6 (0x6)
    PPPPAP: Password = tomtom
```

Slika 1: Sledenje overovitve PAP

S stališča varnosti je najmanj primeren protokol PAP, ki prenaša uporabniško ime in geslo v berljivi obliki (slika 1).
Dosti primernejši način overovitve je na osnovi protokola CHAP, ki prenaša prek omrežja samo kodo, ki je nastala kot posledica zgoščevalne funkcije nad uporabniškim imenom, geslom in še nekaterih drugih parametrov.

B. Klasični oddaljen dostop

Oddaljeni uporabniki uporabljajo protokol PPP za vzpostavitev/vzdrževanje komunikacije in zgoraj omenjene protokole za overovitev. Overovitev uporabnika se izvede na osnovi statičnega uporabniškega imena in gesla, ki je preverjena v lokalni ali oddaljeni bazi (varnostni strežnik).
Statična gesla, brez dodatnih mehanizmov varovanja, niso primerna za dostop do nekega podjetniškega omrežja oz. dostopa do storitev v omrežju.

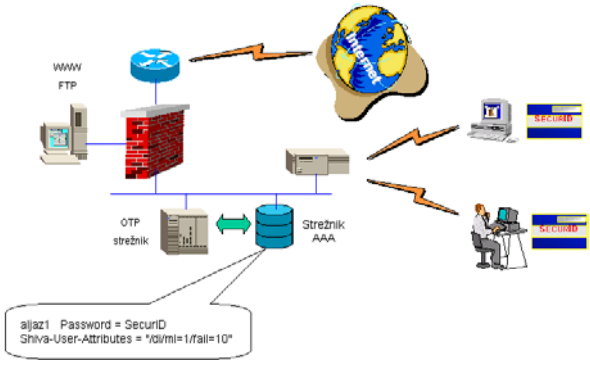


Slika 2: Klicni dostop

Pomanjkljivost statičnih gesel je ta, da si morajo uporabniki zapomniti celo vrsto le-teh. Rezultat tega je, da si izmislijo enostavno uganljiva gesla ali jih celo hranijo na mesta, kjer jih lahko hitro najdejo.
Dodatno stopnjo varnosti lahko dosežemo za uporabnike, ki se povezujejo iz vnaprej znanih lokacij (poznamo telefonske številke). V teh primerih lahko za njihovo overovitev, poleg uporabniškega imena in gesla, uporabimo še dodatne overovitvene mehanizme kot sta overovitev na osnovi identifikacije klicne številke in povratni poziv.
Vsi moderni telefonski sistemi podpirajo storitev identifikacije kličoče številke. Če je izbrana overovitev na osnovi identifikacije kličoče številke, se poleg uporabniškega imena in gesla, preveri še kličoča številka. Kombinacija vseh treh parametrov overovi uporabnika.
Povratni poziv deluje na naslednji način. Uporabnik pokliče na strežnik oddaljenega dostopa, se uspešno overovi na osnovi uporabniškega imena in gesla. Po uspešni overovitvi strežnik oddaljenega dostopa prekine zvezo in ga v nekaj sekundah pokliče nazaj. Tukaj se vidijo dve prednosti. Prva je za podjetje, ki nudi takšno storitev, saj je nepooblaščen dostop do storitev na ta način zelo zmanjšan, saj mora nepooblaščena oseba poznati uporabniško ime in geslo ter uporabljati uporabnikov telefon. Druga prednost je za same uporabnike, saj na ta način plačajo samo en impulz , vse druge pa krije podjetje.
Oba predstavljena mehanizma sta lahko uporabljena tudi skupaj in se načeloma ne izključujeta.

C. *Sistem enkratnih gesel*

Overovitev uporabnikov na osnovi statičnih gesel ne predstavlja zadostno zaščito za uporabnike, ki ne kličejo iz v naprej znanih telefonskih številk.
V okolju, kjer je potrebno zagotovit dostop iz lokacij, ki niso v naprej znane, je potrebno zagotoviti večjo stopnjo overovitve uporabnikov.
Večjo stopnjo overovitve se lahko zagotovi z sistemom enkratnih gesel (slika 3). V ta namen se mora v omrežje postaviti dodaten strežnik, strežnik sistema enkratnih gesel. Vsi omrežni elementi, ki izvajajo overovitev na osnovi enkratnih gesel, se povezujejo nanj.



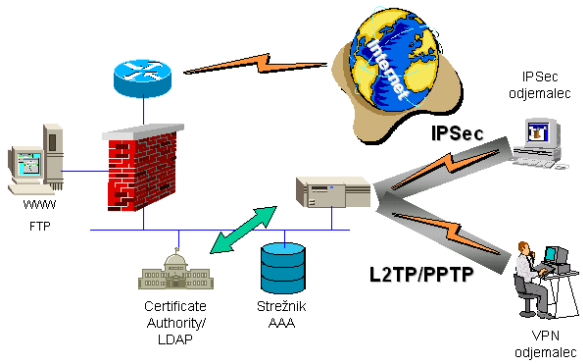
Slika 3: Overovitev s pomočjo sistema enkratnih gesel

Uporabnik mora, poleg uporabniškega imena in skrivnosti (gesla), imeti (pametno) kartico ali na svojem računalniku nameščeno posebno programsko opremo, ki simulira kartico. Kartica časovno generira naključne kode, ki so veljavne v danem časovnem oknu. Kombinacija uporabniškega imena, skrivnosti (PIN) in naključne kode uspešno overovi končnega uporabnika. Tudi, da pride do nepooblaščenega pregledovanja komunikacije (snifanja) in se na nepooblaščen način pridobi navedena informacija, si nepooblaščena oseba z njo nima kaj dosti pomagati. Sistem je namreč zasnovan tako, da je samo ena koda veljavna v danem časovnem oknu.

D. *Tunelske tehnologije*

Na razpolago je kar nekaj tehnologij, ki omogočajo tuneliranje uporabniških podatkov. Nekatere izmed njih ponujajo tudi varovanje le-teh, s pomočjo šifriranja, ali samo zagotovijo, da so podatki prišli do cilja nespremenjeni. Najbolj poznane so naslednje tehnologije: Layer 2 Tunneling Protocol (L2TP) [4], IP Security (IPSec) [5], Point-to-Point Tunneling Protocol (PPTP) [6] in Layer 2 Forwarding (L2F) [7].
IPSec in L2TP sta odprta protokola oz. tehnologije, medtem ko so ostali navedeni protokoli rešitve posameznih proizvajalcev. PPTP je Microsoftova, L2F pa Cisco Systems rešitev.
Da se lahko vzpostavi tunel od uporabnika do strežnika oddaljenega dostopa, po eni izmed navedenih tehnologij, jo morata podpirati oba. Na uporabnikovem računalniku mora biti nameščena posebna programska oprema, ki takšno komunikacijo omogoča.
IPSec je odprt standard, ki omogoča šifriranje, overovitev in zaščito pred ponavljanjem podatkov. Varuje vse podatke, ki se nahajajo nad IP nivojem. Tunel na osnovi IPSec protokola se lahko vzpostavi s pomočjo v naprej definiranih gesel ali s pomočjo arhitekture javnih ključev (PKI). Uporaba IPSec tunelov na osnovi statično definiranih gesel je smiselna le v laboratorijih, nikakor pa za produkcijsko omrežje (problem razširljivosti sistema in sama

varnost gesel). Arhitektura javnih ključev zahteva postavitev certifikatnega urada ali se zanašati na »zunanji« certifikatni urad, kateremu podjetje zaupa. Uporabnik mora pridobiti od (zaupanja vrednega) certifikatnega urada digitalni certifikat, katerega uporablja za vzpostavitev IPSec tunela do strežnika oddaljenega dostopa. Strežnik oddaljenega dostopa preveri digitalni certifikat na certifikatnem uradu.

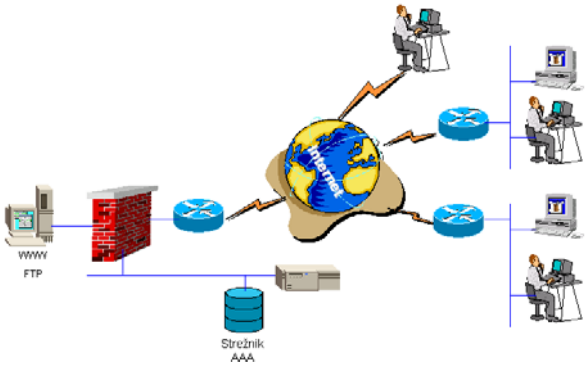


Slika 4: Tunelske tehnologije

Za vzpostavitev tunelov od uporabnikov do strežnika oddaljenega dostopa je smiselna še uporaba protokola PPTP, saj omogoča šifriranje podatkov.
Uporaba drugih dveh navedenih tehnologij, L2TP in L2F, ni smiselna v tem okolju, saj se skoraj nič oz. zelo malo pridobi na varnosti podatkov, ki se prenašajo prek omrežja.

III. DOSTOP IZ INTERNETA

A. »Običajno« okolje

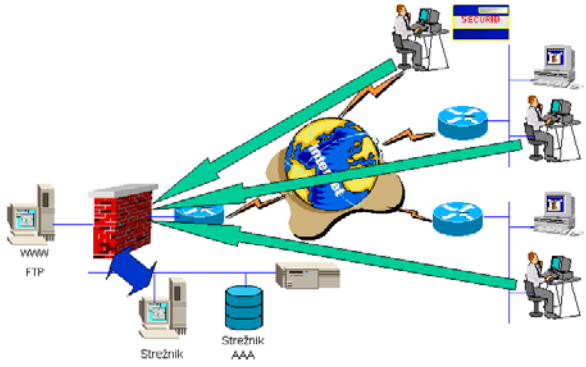


Slika 5: Običajno okolje povezovanja v internet

Podjetja imajo eno ali več povezav do interneta. Nepooblaščen dostop do notranjega omrežja iz interneta varuje požarna pregrada. Postavljeno je posebno omrežje, t.i. demilitarizirano omrežje (DMZ), ki ima kontroliran dostop po samo določenih protokolih (npr. FTP, HTTP). V to omrežje je običajno postavljen spletni strežnik, ki oglašuje podjetje v internetu; in strežnik za prenos datotek – FTP.
Posledica tega je, da uporabniki storitev podjetja ne morajo dostopati do notranjih virov ne da bi se ustvarila velika varnostna luknja.

B. Sistem enkratnih gesel

Za dostop do notranjih virov se lahko uporabi sistem enkratnih gesel. V ta namen se mora požarna pregrada administrirat tako, da zna izvesti overovitev na osnovi enkratnih gesel. Uporabniki storitev podjetja imajo pri sebi (pametne) kartice ali posebno programsko opremo s pomočjo katere se lahko overovijo, preden dostopajo do notranjih virov (razpoložljivost odvisna od politike varnosti).



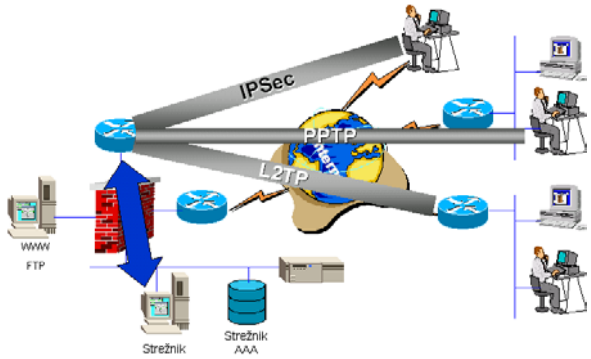
Slika 6: Uporaba sistema enkratnih gesel

Uporabnik vzpostavi povezavo do notranjega vira, požarna pregrada prestreže to zahtevo in zahteva overovitev uporabnika. Uporabnik se overovi na zgoraj opisan način. Požarna pregrada pošlje sprejete informacije strežniku sistema enkratnih gesel, ki preveri uporabnika. Po uspešni overovitvi požarna pregrada »spusti« uporabnika do želene storitve.

C. Navidezna privatna omrežja

Podjetje je povezano v internet kot je opisano v razdelku A. Želja podjetja pa je omogočitev oddaljenim uporabnikom dostop do notranjih storitev, pri tem pa uporabiti internet kot prenosni medij. Glede na željo in možnost uporabe posamezne tehnologije se odloči katero bo podprl (običajno omejitev naprave katero ima nameščeno pri sebi). Veliko vlogo na izbiro tehnologija pa ima vsebina prenešenih podatkov (ali jih je potrebno varovati).
Zaključitev tunelov se lahko izvede na isti napravi, ki služi za povezavo v internet, vendar takšen način ni priporočljiv. Tuneliranja pobere kar nekaj procesorske moči in če je takšnih tunelov veliko, lahko trpijo notranji uporabniki. Druga slabost pa je sam nadzor podatkov, ki se nahajajo znotraj tunelov. Dosti primernejša rešitev je postavitev ločene naprave za zaključitev tunelov. Ta naprava se postavi v ločeno,

t.i. demilitarizirano omrežje. S tem ko smo postavili napravo v ločeno omrežje imamo dosti večji nadzor nad vsebino tunela (kdo in kam želi komunicirat).
Če želi varovati podatke, se lahko odloči za uporabo IPSec tehnologije, ki je odprt standard. Izgradnja navideznih privatnih omrežij uporablja tunelske tehnologije, ki so zgoraj opisane.

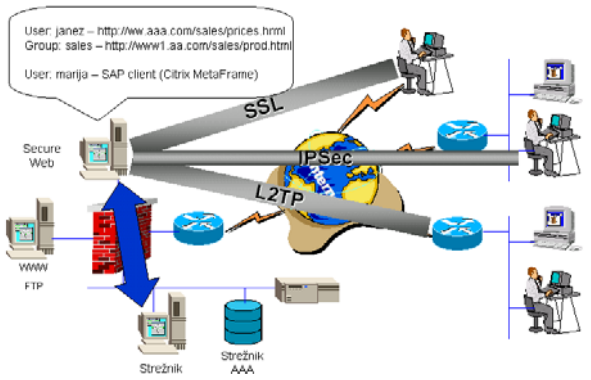


Slika 7: Navidezna privatna omrežja

Zelo pogosto se uporablja kombinacija L2TP in IPSec tehnologije.

D. Trendi

V zadnjem času se vse več pozornosti namenja ne samo varnosti dostopa ampak tudi varnosti aplikacij in storitev, ki v večini bazirajo na spletnih tehnologijah. Zaradi e-poslovanja in zapletenih poslovnih ter finančnih postopkov, aplikacije potekajo po celotnem informacijskem sistemu podjetja in ne samo na demilitariziranem omrežju.



Slika 8: Trendi

Zaradi te kompleksnosti je potrebno definirati in postaviti celotno varnostno ogrodje, ki omogoča centralizirano upravljanje z uporabniki, enotno prijavo za vse aplikacije ter nenehno spremljanje in beleženje vseh aktivnosti. Za ta namen se pred požarno pregrado ali v demilitariziranem omrežju postavi strežnik s specifično programsko opremo, ki deluje kot nadgradnja požarne pregrade na aplikativnem nivoju in omogoča zgoraj omenjeno funkcionalnost. Požarna pregrada zagotavlja samo varen dostop do tega strežnika, poganjanje vseh drugih internih aplikacij pa poteka izključno s strani tega varnega strežnika. Od spletnega odjemalca do tega strežnika se vzpostavi SSL seja.
Varni strežnik mora podpreti vse mehanizme overovitve (sistem enkratnih gesel, digitalni certifikati – PKI, itn.,) ter povezljivost z globalnim imenskim sistemom (LDAP strežnik). Prav tako aplikativna oprema mora vsebovati API knjižnice zaradi popolnejše integracije s internimi aplikacijami.

LITERATURA

[1] B. Lloyd, W. Simpson: RFC 1334, PPP Authentication Protocols, oktober 1992
[2] W. Simpson: RFC 1994, PPP Challenge Handshake Authentication Protocol (CHAP), avgust 1996
[3] G. Zorn, S. Cobb: RFC 2433, Microsoft PPP CHAP Extensions, oktober 1998
[4] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter: RFC 2661, Layer Two Tunneling Protocol "L2TP", avgust 1999
[5] S. Kent, R. Atkinson: RFC 2401, Security Architecture for the Internet Protocol, november 1998
[6] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn: RFC Point-to-Point Tunneling Protocol (PPTP), julij 1999
[7] A. Valencia, M. Littlewood, T. Kolar: RFC 2341, Cisco Layer Two Forwarding (Protocol) "L2F", maj 1998
[8] K. Reeks: E-Security for E-Business, oktober 2000
[9] E. Greenberg, Carmin McLaughlin: Real-World Security, september 2000

BIOGRAFIJA

Tomaž Aljaž (aljaz@iskratel.si) je magistriral leta 1999 na Fakulteti za elektrotehniko, računalništvo in informatiko v Mariboru. Rezultate njegovega strokovnega, znanstvenega in raziskovalnega dela najdemo na delu dveh področij. V zadnjem obdobju daje prednost sožitja telekomunikacijskih in podatkovnih omrežij, uvajanju novih storitev, ki so s tem omogočene in upravljanja ter zagotavljanja varnosti v teh modernih integriranih informacijskih sistemih. Drugo pokriva področje analize različnih protokolov, ki prevladujejo v navedenih primerih.
Je avtor in soavtor več referatov na strokovnih konferencah v Sloveniji.
Zaposlen je v podjetju ISKRATEL d.o.o., kjer je produktni vodja za IP in konvergečne produkte. Prav tako je soavtor večjih pilotskih projektov podjetja ISKRATEL. Aktivno sodeluje pri izobraževanju uporabnikov iz področja računalnikih komunikacij.

Selim Tolaj (tolaj@iskratel.si) je diplomiral leta 1988 na Fakulteti za elektrotehniko v Prištini. Ukvarja se z načrtovanjem in postavitvijo informacijskih sistemov ter celovitih rešitev s področja varnosti IS. Pokriva tudi področje upravljanja IS in zagotavljanja nivoja storitev .
Je avtor in soavtor več referatov na strokovnih konferencah v Sloveniji.
Zaposlen je v podjetju ISKRATEL d.o.o., kjer je vodja službe za razvoj informatike.