CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Tehnike generiranja jednokratnih lozinki

CCERT-PUBDOC-2009-04-262

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

U informatičkom svijetu potvrda identiteta korisnika za pristup nekom sustavu moguća je na temelju osobnog faktora (ono što osoba zna), tehničkog faktora (ono što osoba posjeduje) i/ili ljudskog faktora (ono što osoba jest). Radi povećanja sigurnosti i zaštite od neovlaštenog pristupa, često se koristi kombinacija dva (dvo-faktorska zaštita), a ponekad i svih tri faktora autentikacije (tro-faktorska zaštita). Na primjer, autentikacija jednokratnim lozinkama spada pod dvo-faktorsku autentikaciju, što znači da se koriste dva od tri navedena faktora – ono što osoba zna i tehničkog faktora (najčešće vrijeme).

Zbog napretka u tehnikama i alatima koje napadači koriste za razbijanje statičkih lozinki sve češće se koriste i druge, naprednije tehnike sigurne autentikacije korisnika. Jedna od tih tehnika je i korištenje jednokratnih lozinki (*eng. One-time Password*). Uzevši u obzir učestalost otuđivanja ili pokušaja otuđivanja povjerljivih podataka, pogotovo kada su u pitanju bankarski sustavi i pristup udaljenim računalima (*eng. Remote access*), korisnike je potrebno zaštititi kod pristupa uslugama kojima se pristupa putem javne (nezaštićene) mreže - Interneta.

Jednokratne lozinke smanjuju mogućnost neovlaštenog pristupa povjerljivim podacima (korisnička imena, lozinke, brojevi kreditnih kartica, itd.), informacijama i/ili datotekama jer istu lozinku nije moguće upotrijebiti više nego jednom, a za svaku slijedeću prijavu u sustvaje potrebno generirati novu lozinku. Ako napadač otuđi upotrijebljenu jednokratnu lozinku od nje neće imati nikakve koristi. Kada korisnik želi pristupiti svojim podacima ili datotekama, generira se jednokratna lozinka za pristup. Tu lozinku više nije moguće koristiti za slijedeću prijavu. Razvoj ove metode zaštite korisnika ishodio je razvojem različitih tehnika generiranja jednokratnih lozinki. S obzirom na situaciju i upotrebu, određuje se tehnika koja pruža najbolju zaštitu. Ova je metoda zaštite primijenjena kod različitih vrsta tokena, čitača kartica, smart kartica i sličnih uređaja.

U nastavku dokumenta navedene su tehnike generiranja jednokratnih lozinki, te njihove prednosti i mane. Većina korisnika usluga Internet bankarstva posjeduje neki uređaj koja koristi dvo-faktorsku autentikaciju, pa je stoga važno korisnicima skrenuti pažnju na nedostatke ove vrste autentikacije kako ne bi neispravnim rukovanjem uređajima i neopreznim pregledavanjem sadržaja na Internetu ugrozili svoje (ali i tuđe) podatke. Također, prikazani su neki praktični primjeri upotrebe ove tehnike zaštite korisnika i računala.

2. Dvo-faktorska autentikacija

Autentikacijski faktor (*eng. authentication factor*) je informacija ili proces kojim se dokazuje ili potvrđuje identitet osobe koja zahtjeva pristup zaštićenoj usluzi. Dvo-faktorska autentikacija (*eng. two-factor authentication*) je sustav kod kojeg se koriste zajedno dva različita autentikacijska faktora kako bi se dokazao ili potvrdio identitet osobe. Upotreba više od jednog faktora pri autentikaciji naziva se „jakom autentikacijom" (*eng. strong authentication*).

Autentikacijske faktore moguće je podijeliti na osobne, tehničke i ljudske faktore. U tablici koja slijedi navedeni su primjeri za svaki od tri vrste faktora, te načini na koje je moguće ugroziti sigurnost ovih faktora.

Faktor	Primjer	Vektor napada
Osobni faktor	Najbolji primjer su lozinke i osobne informacije. Osobne informacije nisu nužno tajne, ali se pretpostavlja da ih nitko drugi ne zna.	Napadač mora otkriti lozinke ili osobne informacije.
Tehnički faktor	Pod ovim pojmom se podrazumijevaju objekti koji dokazuju identitet (pečati, osobni dokumenti,itd.). Tokeni za elektronsku autentikaciju su primjer takvih objekata, a mogu biti u obliku programa ili uređaja.	Napadač mora otuđiti ili krivotvoriti objekt koji dokazuje identitet.
Ljudski faktor	Autentikacijske metode temeljene na ovom faktoru nazivaju se biometrijom, i kod nje se mjere fizička svojstva korisnika (otisci prstiju, zjenice,itd.) ili se očitavaju neke druge karakteristike (poput rukopisa).	Napadač mora krivotvoriti svojstva korisnika.

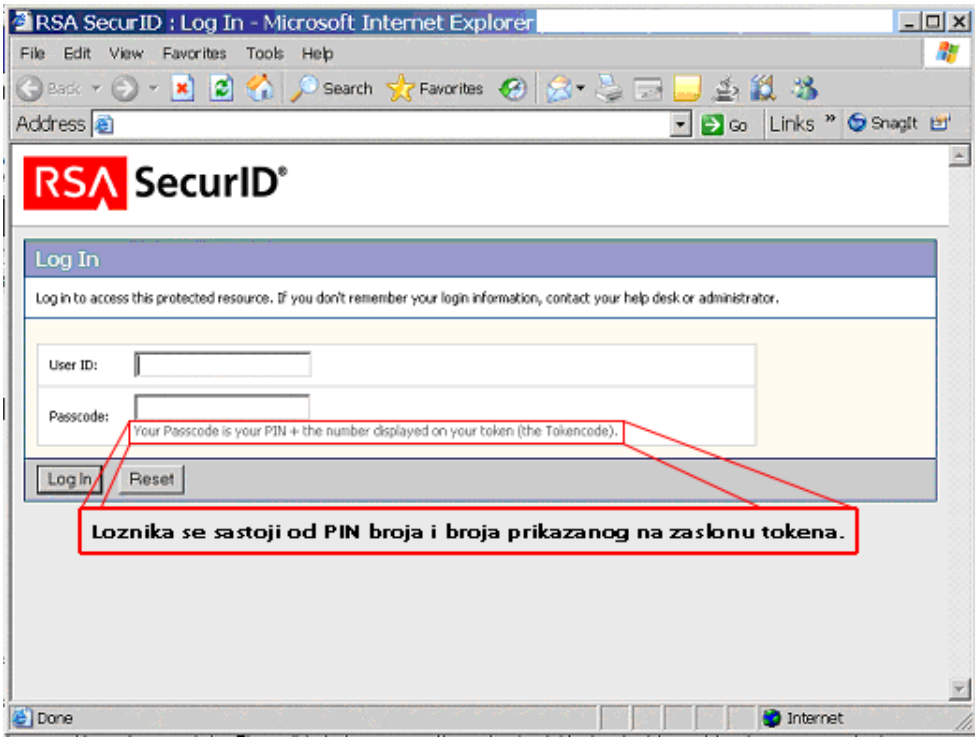
Tablica 1. Prikaz i primjeri autentikacijskih faktora

Najbolji način zaštite je svakako biometrija, jer je vrlo teško krivotvoriti svojstva korisnika, što je ujedno i tehnološki najkompleksnije za izvesti (uređaj za biometriju mora moći egzaktno klasificirati svakog korisnika prema odgovarajućim biometrijskim parametrima). Najrašireniji su uređaji koji rade na temelju osobnog faktora i tehničkog faktora.

Važno je spomenuti da autentikacijske metode koje se temelje na osobnim informacijama imaju nekoliko problema:

1. ograničen broj informacija,
2. većinu osobnih informacija nije moguće mijenjati,
3. ako je osobne informacije moguće mijenjati, svaku je promjenu potrebno zapamtiti,
4. vrijednost osobnih informacija kao autentikacijskog faktora opada s obzirom na broj organizacija koje ih posjeduju, te
5. napadač može lako otkriti osobne informacije jednostavnim istraživanjem ili korištenjem napada pogađanjem pojmova (*eng. dictionary attack*).

Dvo-faktorskom autentikacijom se smatra proces kod kojeg se koriste dva različita od gore tri navedena faktora. Dakle, upotreba lozinke i neke osobne informacije pri autentikaciji ne spadaju pod dvo-faktorsku autentikaciju jer se koristi samo osobni faktor. Dvo-faktorska autentikacija se svrstava u grupu višefaktorske autentikacije, isto kao i autentikacija s tri faktora pri kojoj se koriste sva tri gore navedena autentikacijska faktora. Dvo-faktorska autentikacija smanjuje mogućnost krađe identiteta i drugih oblika krađe, jer korisnikova statička lozinka nije vidljiva napadaču. Kod generiranja jednokratnih lozinki najčešće se koriste osobni i tehnički faktor za autentikaciju korisnika.

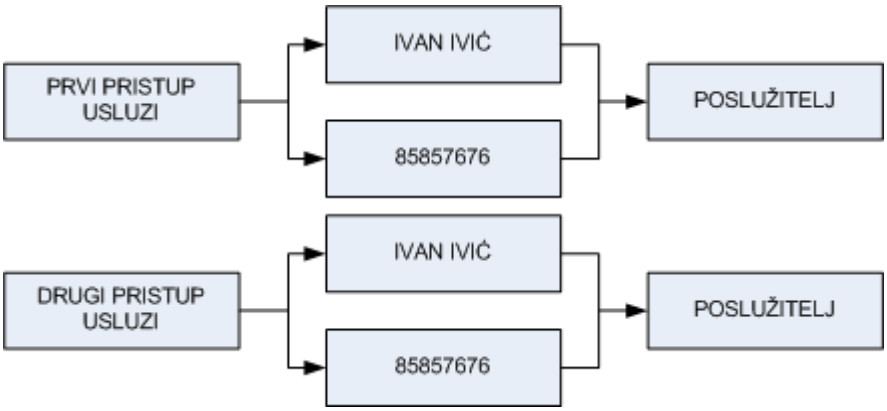


Slika 1. Primjer dvofaktorske autentikacije za pristup zaštićenoj web stranici

Izvor: Google

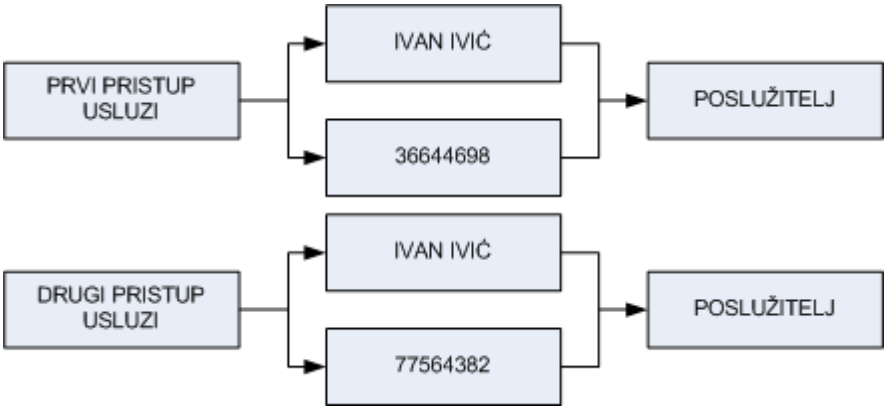
2.1. Upotreba jednokratnih lozinki

Kako i samo ime kaže, metoda generiranja jednokratnih lozinki se temelji na stvaranju jedinstvenih jednokratnih lozinki koje će korisniku omogućiti zaštitu od krađe podataka i informacija. Za razliku od jednokratnih, statičke lozinke se ne mijenjaju (osim na zahtjev korisnika). Korisnik unosi korisničko ime i lozinku kako bi dokazao svoj identitet, pri čemu su obje informacije iste kod svakog slijedećeg unosa. Ako napadač otuđi korisničko ime i statičku lozinku, dobiva pristup usluzi.



Slika 2. Prikaz autentikacije sa korisničkim imenom i statičkom lozinkom

Za razliku od statičkih lozinki, ako napadač otuđi jednokratnu lozinku neće je moći upotrijebiti jer istu lozinku nije moguće upotrijebiti više nego jednom. U velikoj većini slučajeva, prilikom korištenja metode jednokratnih lozinki korisničko ime ostaje isto, a lozinka se mijenja (kod svakog zahtjeva za pristup usluzi generira se nova jednokratna lozinka, različita od prethodne).



Slika 3. Prikaz autentikacije sa korisničkim imenom i jednokratnom lozinkom

Jednokratne lozinke su oblik „jake autentikacije", koja pruža veću razinu zaštite i koriste se za bankovne transakcije preko Interneta, mrežnim sustavima u tvrtkama i drugim sustavima koji sadrže osjetljive i povjerljive informacije kao npr. vojske, policije i sl.

Korisnička imena i statičke lozinke ne spadaju u jaku autentikaciju, jer koriste isti faktor, osobni, a kao što je prije napomenuto, jaka autentikacija podrazumijeva identifikaciju korisnika pomoću dva različita faktora, npr. pomoću tehničkog i osobnog faktora. U jaku autentikaciju spadaju još i pametne kartice, PGP ključevi (*eng. Pretty Good Privacy key*), biometrija, USB tokeni, itd.

Ako se dogodi da napadač zabilježi lozinku koju korisnik još nije unio, nakon kratkog vremenskog perioda neće imati nikakve koristi od iste (isteklo je vrijeme valjanosti takve lozinke). Po isteku tog vremenskog perioda poslužitelj neće prihvatiti jednokratnu lozinku, te će korisnik morati generirati novu jednokratnu lozinku.

Većina sustava za generiranje jednokratnih lozinki zahtjeva unos statičke lozinke koju je korisnik zaprimio od proizvođača ili ponuđača usluga. Na temelju statičke lozinke se pomoću posebnih algoritama generiraju jednokratne lozinke. Algoritmi koji generiraju jednokratne lozinke na temelju statičke lozinke mogu biti tablice ili naprednije matematičke funkcije.

Jednokratnim lozinkama se povećava razina sigurnosti, te onemogućava napadače da ukradu povjerljive ili osjetljive informacije i dokumente. Generiranjem nove jednokratne lozinke pri svakoj prijavi, korisnik osigurava svoje informacije. Jednokratne lozinke štite korisnike od phishing i pharming napada, te štete koja se otkrivanjem povjerljivih informacija može prouzročiti (krađa i zlouporaba identiteta, financijska šteta, itd.). U nastavku će biti navedene prednosti i nedostaci jednokratnih lozinki kako bi se korisnicima objasnila ograničenja na koja je potrebno obratiti pozornost.

3. Tehnike generiranja jednokratnih lozinki

Tehnike generiranja jednokratnih lozinki temelje se na nekoliko različitih načina rada. Može ih se podijeliti u pet kategorija:

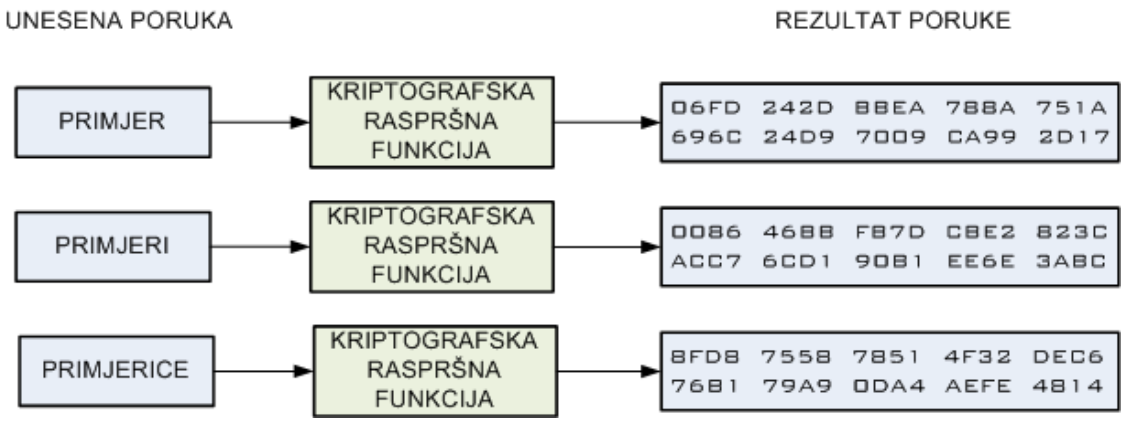
1. Matematički algoritmi
2. Vremenska sinkronizacija
3. „*Challenge-based*“ generiranje
4. Transakcijski autentikacijski brojevi
5. Jednokratne lozinke primljene SMS porukom (*eng. Short Message Service*)

Svaka od navedenih tehnika biti će detaljnije objašnjena u nastavku dokumenta.

3.1. Matematički algoritmi

Kod ove tehnike generiranje jednokratnih lozinki se matematičkim algoritmima generira niz jednokratnih lozinki iz korisničke statičke lozinke. Pri generiranju jednokratnih lozinki koristi se jednosmjerna funkcija (*eng. one-way function*). Funkcija je konstruirana upravo tako da je nemoguće obrnutim postupkom doći do statičke lozinke korisnika (upravo zato kako napadač ne bi mogao iz privremene lozinke otkriti statičku te kasnije po potrebi generirati nove privremene lozinke). Ovakva se funkcija naziva kriptografska raspršna funkcija (*eng. cryptographic hash function*) i ima veliku primjenu u kriptografskim sustavima.

Kriptografska raspršna funkcija je funkcija koja na temelju proizvoljno unesenih podataka generira niz podataka točno određene duljine, tj, raspršnu vrijednost (*eng. hash value*). Slučajne ili namjerne promjene u unesenim podacima će također promijeniti i raspršnu vrijednost. Podaci koje je potrebno šifrirati nazivaju se porukama (*eng. message*), a raspršne vrijednosti rezultatom poruke.



Slika 4. Primjer rada kriptografske raspršne funkcije

Važno je primijetiti da male promjene u izvornoj poruci izazivaju velike promjene u rezultatu poruke. To znači da korisnikova statička lozinka mora biti ispravno upisana kako bi se dobila „ispravna“ jednokratna lozinka.

Četiri svojstva karakteriziraju idealnu kriptografsku raspršnu funkciju, a to su:

1. lakoća generiranja raspršne vrijednosti za bilo koju unesenu poruku,
2. nemoguće je promijeniti poruku bez da se promijeni i raspršna vrijednost,
3. nemoguće je naći dvije različite poruke koje će imati iste raspršne vrijednosti i
4. nemoguće je na temelju raspršne vrijednosti naći upisanu poruku.

Kriptografske raspršne funkcije se koriste u elementima za zaštitu informatičkih sustava prilikom izrade digitalnih potpisa (*eng. digital signature*), PKI sustava (*eng. Public Key Infrastructure system*),

autentikacijskih kodova poruka (*eng. message authentication code*), autentikaciju kod programa za povezivanje ravnopravnih računala (*eng. peer-to-peer*), te u raznim drugim oblicima autentikacije.

Kriptografska raspršna funkcija mora biti sposobna oduprijeti se svim poznatim kripto-analitičkim napadima. Više o kripto-analitičkim napadima moguće je saznati na:

http://en.wikipedia.org/wiki/Cryptanalysis#Types_of_cryptanalytic_attack

Minimalni zahtjevi koji se nameću kriptografskoj raspršnoj funkciji su:

- otpornost na otkrivanje inverzne raspršne funkcije (*eng. preimage resistance*), tj. napadač ne smije otkriti unesenu poruku na temelju raspršne vrijednosti.
- ne smiju postojati dvije različite unesene poruke koje bi nakon pretvorbe u kriptografskoj raspršnoj funkciji davale jednake raspršne vrijednosti (*eng. second preimage resistance*). Ovo se svojstvo naziva i slaba otpornost na preklapanje (*eng. weak collision resistance*).
- otpornost na preklapanje (*eng. collision resistance*) pri čemu mora biti gotovo nemoguće naći dvije različite poruke koje bi davale istu raspršnu vrijednost. Ovo se svojstvo naziva i jaka otpornost na preklapanje (*eng. strong collision resistance*).

Iz ovih se zahtjeva može zaključiti da niti napadač ne može promijeniti ili zamijeniti poruku za unos bez da se promijeni i raspršna vrijednost. Također, očito je da ako dvije poruke imaju istu raspršnu vrijednost da su identične.

Kriptografske raspršne funkcije se koriste kod generiranja jednokratnih lozinki na način da korisnik unese poruku (statičku lozinku), nakon čega kriptografska raspršna funkcija korisniku prikaže rezultat poruke. Kod autentikacije korisnik mora poslužitelju poslati rezultat poruke na temelju kojeg poslužitelj otkriva o kojem se korisniku radi.

3.1.1. Sigurnost

Postoji velik broj kriptografskih raspršnih funkcija, a u većini su pronađene određene ranjivosti zbog čega se ne preporuča njihova upotreba. U nastavku je navedena tablica sa najčešće korištenim kriptografskim algoritmima.

Algoritam	**Otpornost na preklapanje**	**Otpornost na otkrivanje inverzne raspršne funkcije**
HAVAL	DA	
MD2	DA/NE	
MD4	DA	DA (sa ranjivostima)
MD5	DA	NE
PANAMA	DA	
RadioGatun	NE	
RIPEMD	DA	
RIPEMD - 128/256	NE	
RIPEMD - 160/320	NE	
SHA-0	DA	
SHA-1	DA (sa ranjivostima)	NE
SHA - 256/224	NE	NE
SHA - 512/384	NE	NE
Tiger(2) - 192/160/128	NE	
WHIRLPOOL	NE	

Tablica 2. Prikaz kriptografskih raspršnih algoritama i ranjivosti na određenu vrstu napada

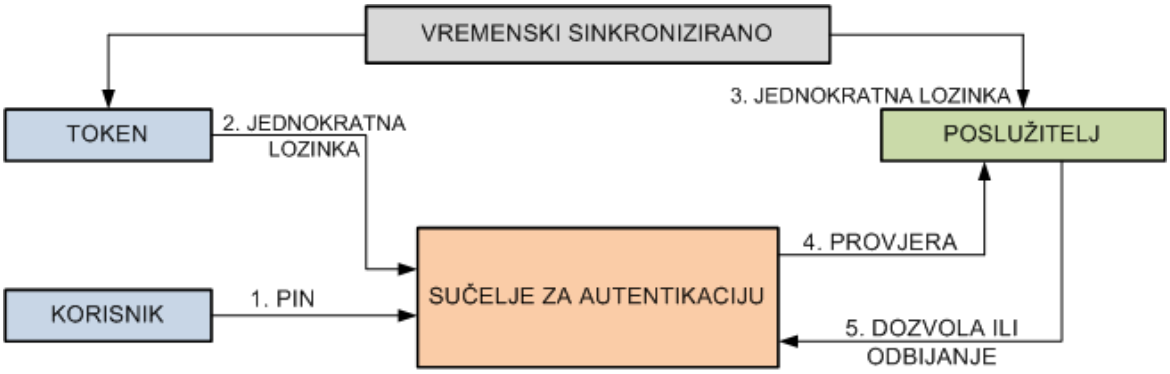
U 2004. godini su pronađene ranjivosti u većem broju često korištenih raspršnih funkcija, uključujući SHA-0, RIPEMD, i MD5. Pronalazak ranjivosti u ovim funkcijama doveo je u pitanje sigurnost funkcija koje su proizašle iz navedenih, primjerice SHA-1 (ojačana inačica SHA-0 funkcije), RIPEMD-128 i RIPEMD-160 (ojačane inačice RIPEMD funkcije). U 2005. godini pronađena je ranjivost u SHA-1 funkciji. Najčešće korištene funkcije u 2009. godini su MD5 i SHA-1, iako su u obje funkcije pronađene ranjivosti. Više o kriptografskim raspršnim funkcijama moguće je saznati u dokumentima „Napad na MD5 algoritam" (CCERT-PUBDOC-2009-04-260) i „Nedostaci PKI infrastrukture" (CCERT-PUBDOC-2009-02-255) objavljene na službenim stranicama CERT-a.

3.2. Vremenska sinkronizacija

Ova je tehnika generiranja jednokratnih lozinki najčešće vezana uz fizičke uređaje (npr. korisnik dobiva svoj token pomoću kojeg generira jednokratne lozinke). Unutar uređaja postoji točan vremenski sklop koji je sinkroniziran sa glavnim poslužiteljem. Kao što i sam naziv sugerira, sustavi koji se temelje na vremenskoj sinkronizaciji, za generiranje jednokratnih lozinki koriste vremensku komponentu. Uređaj generira jednokratnu lozinku upravo na temelju vremena te, za razliku od ostalih sustava, u nekim slučajevima nije potrebna korisnikova statička lozinka ili tajni podatak. Za generiranje jednokratnih lozinki ovom tehnikom moguće je koristiti i mobilne uređaje.

Slika 5. Prikaz uređaja koji generiraju jednokratne lozinke na temelju vremenske sinkronizacije

Vremenski sinkronizirani uređaj kojim se generiraju jednokratne lozinke sadrži prethodno uneseni ključ kojim proizvođač raspoznaje korisnike (svaki korisnik ima različiti ključ!). U vremenskim razmacima od 30 do 60 sekundi uređaj generira jednokratne lozinke temeljene na ključu. Korisniku se potom na zaslonu uređaja ispisuje jednokratna lozinka koju u kombinaciji sa svojom statičkom lozinkom (npr. PIN) koristi kako bi dokazao ili potvrdio svoj identitet. Važno je napomenuti da ne postoji mogućnost da uređaj u dva različita vremenska trenutka generira istu lozinku. Jednokratnu lozinku prikazanu na zaslonu uređaja moguće je iskoristiti u određenom vremenskom razmaku (najčešće 2 minute). Po isteku tog vremena poslužitelj više neće prihvaćati lozinku kao važeću, te će korisnik morati generirati novu lozinku putem uređaja.



Slika 6. Prikaz generiranja jednokratnih lozinki tehnikom vremenske sinkronizacije

Postupak kod autentikacije ovom tehnikom je slijedeći:

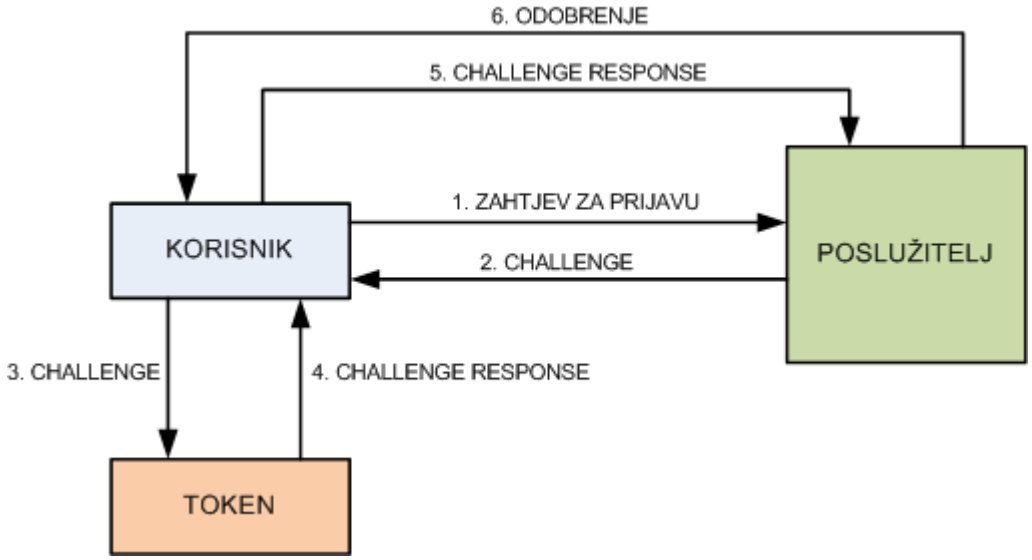
1. Korisnik se pomoću Internet preglednika spoji na sučelje za autentikaciju (npr. web stranica banke). U sučelje za autentikaciju korisnik unese svoj PIN.

2. Korisnik pokreće postupak generiranja jednokratne lozinke uključivanjem tokena. Token pomoću vremenskog sklopa i unaprijed upisanog ključa generira jednokratnu lozinku. Korisnik potom upiše prikazanu jednokratnu lozinku u sučelje za autentikaciju.
3. Poslužitelj istovremeno generira jednokratnu lozinku.
4. Poslužitelj uspoređuje generiranu lozinku s lozinkom koju je unio korisnik.
5. Ukoliko su lozinka koju je generirao korisnik i ona koju je generirao poslužitelj jednake, poslužitelj će korisniku odobriti pristup. U protivnom, poslužitelj će odbiti korisnikov zahtjev.

Važno je napomenuti da ako napadač uspije otuđiti jednokratnu lozinku (mpr. presretanjem mrežnih paketa) po isteku njezinog vremenskog roka valjanosti ili nakon što je upotrijebljena, neće imati nikakve koristi od lozinke jer je poslužitelj neće priznati.

3.3. „Challenge based" tehnika

Pod pojmom „challenge" (nadalje upit) smatra se numerička vrijednost koju korisnik prima od poslužitelja kako bi pomoću uređaja ili programa generirao jednokratnu lozinku. Ova se tehnika također temelji na vremenskoj sinkronizaciji.



Slika 7. Prikaz rada "challenge based" tehnike

Autentikacija „challenge based" tehnikom ima slijedeći tijek:

1. Korisnik šalje poslužitelju zahtjev za prijavu.
2. Na temelju poslanog zahtjeva za prijavu, poslužitelj korisniku šalje upit.
3. Korisnik upit mora unijeti u token kako bi token prikazao odgovor na upit (*eng. challenge response*).
4. Korisnik očitava odgovor na upit prikazan na zaslonu tokena.
5. Korisnik unosi odgovor na upit u sučelje za autentikaciju, kako bi mu poslužitelj odobrio pristup.
6. Poslužitelj također generira odgovor na upit. Ako su oba odgovora na upit (onaj na zaslonu tokena i na poslužitelju) jednaka, poslužitelj odobrava korisniku pristup.

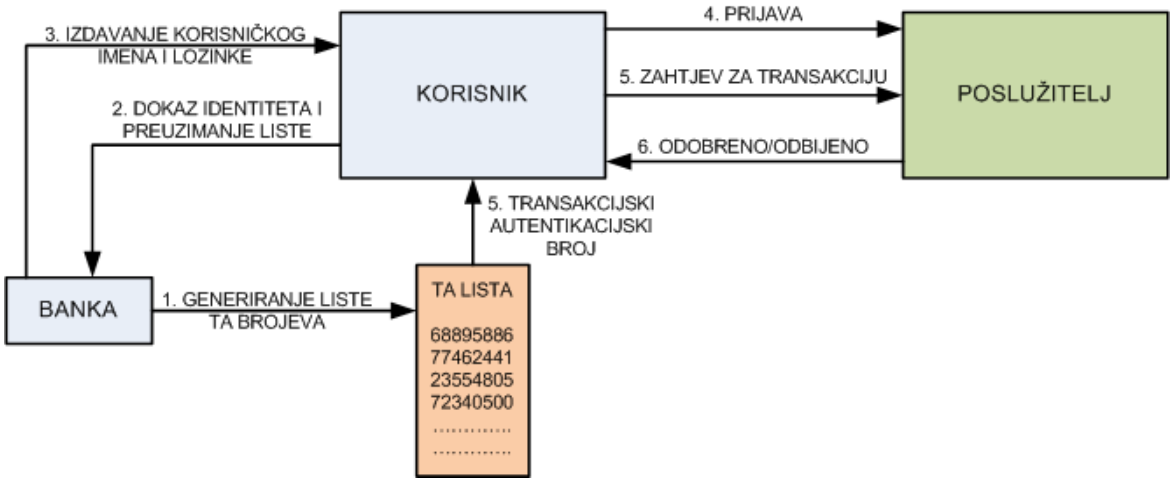
Čak i ako se dogodi da poslužitelj korisniku pošalje isti upit dva puta, korisniku će uređaj prikazati dva različita odgovora na upit, jer se radi o različitim vremenskim trenucima. Ovo upućuje na činjenicu da nije moguće dva ili više puta generirati istu jednokratnu lozinku, bez obzira na upit. Ova je tehnika sigurnija od vremenske sinkronizacije. Uređaj za generiranje jednokratnih lozinki je također vremenski sinkroniziran sa poslužiteljem, ali ovdje je dodana još jedna zaštita, upit poslužitelja. Uređaj generira jednokratne lozinke na temelju vremenskog trenutka i upita poslužitelja. Primjer autentikacije ovom tehnikom moguće je vidjeti kod izvršavanja transakcija putem Internet bankarstva.

3.4. Transakcijski autentikacijski brojevi

Transakcijski autentikacijski brojevi (*eng. transaction authentication number*) su jednokratne lozinke koje neke bankarske ustanove daju korisnicima kako bi izvršavali financijske transakcije.

Transakcijski autentikacijski brojevi funkcioniraju na sljedeći način:

1. Banka generira određeni broj transakcijskih autentikacijskih brojeva za pojedinog korisnika. Najčešće korisnik ima dovoljno transakcijskih autentikacijskih brojeva za vremenski period od šest mjeseci do godine dana.
2. Korisnik pri preuzimanju liste lozinki u banci mora dokazati svoj identitet nekim osobnim dokumentom.
3. Korisnik od banke prima također i korisničko ime i statičku lozinku koju koristi za prijavu na traženu uslugu.
4. Kako bi koristio uslugu, korisnik se mora prijaviti putem preglednika i upisati dobiveno korisničko ime i statičku lozinku. Napadač može saznati korisničko ime i lozinku, ali neće moći nanijeti štetu jer je za obavljanje financijskih transakcija potreban transakcijski autentikacijski broj sa liste koju je izdala banka.
5. Da bi korisnik izvršio transakciju, potrebno je upisati transakcijski autentikacijski kod. Poslužitelj potom provjerava da li se taj broj nalazi na listi pridijeljenoj tom korisniku i da li je taj broj već korišten. Ako se broj ne nalazi na listi ili ako je već korišten za neku prethodnu transakciju, poslužitelj neće izvršiti traženu akciju (npr. isplatu novčanih sredstava).
6. Ukoliko je transakcija uspješno provedena, uneseni transakcijski autentikacijski broj je izbrisan sa korisnikove liste na poslužitelju i nije ga moguće više koristiti.
7. Ako je u pitanje dovedena sigurnost liste transakcijskih autentikacijskih brojeva, korisnik može prijaviti banci da poništi staru listu i izda novu sa novim transakcijskim autentikacijskim brojevima.



Slika 8. Prikaz postupka autentikacije pomoću transakcijskih autentikacijskih brojeva

U nekim slučajevima, moguće je umjesto izdavanja liste transakcijskih autentikacijskih brojeva zatražiti da se kod izvršavanja transakcije transakcijski autentikacijski broj pošalje na mobilni telefon. u tom slučaju, kod zahtjeva za transakciju banka korisniku putem SMS poruke pošalje transakcijski autentikacijski broj. Korisnik po primitku SMS poruke unese dobiveni transakcijski autentikacijski broj u sučelje za autentikaciju.

Tehnika transakcijskih autentikacijskih brojeva pruža jaku zaštitu korisnicima, jer napadač može nanijeti financijsku štetu korisniku samo ako uspije saznati korisničko ime i lozinku i otuđi listu transakcijskih autentikacijskih brojeva. Sigurnost ove tehnike leži u činjenici da napadač ne može putem zlonamjernih programa otuđiti listu transakcijskih autentikacijskih brojeva (jer je ista ispisana na listu papira i pohranjena na zaštićeno mjesto). Također, korisniku nisu potrebni nikakvi uređaji za generiranje transakcijskih autentikacijskih brojeva jer lozinke prethodno generira banka.

3.4.1. Primjeri zlouporabe transakcijskih autentikacijskih brojeva

Unatoč visokoj razini sigurnosti postoje slučajevi u kojima je nanesena ozbiljna financijska šteta korisnicima. Ukoliko se radi o sustavu koji transakcijske autentikacijske brojeve korisnicima šalje putem SMS poruka, postoji način da napadač nanese korisniku financijsku štetu. Ovakav napad je izveden u Južnoafričkoj Republici i nazvan je „prijevara zamjenom SIM kartica" (*eng. SIM Swap Fraud*). Napadač je na prijevaru, oponašajući žrtvu, od operatera mobilnih usluga „Vodacom" zatražio zamjensku SIM (*eng. Subscriber Identity Module*) karticu tvrdeći da je kartica ukradena. Korisničko ime i lozinku za prijavu na uslugu napadač je otuđio zlonamjernim programima.

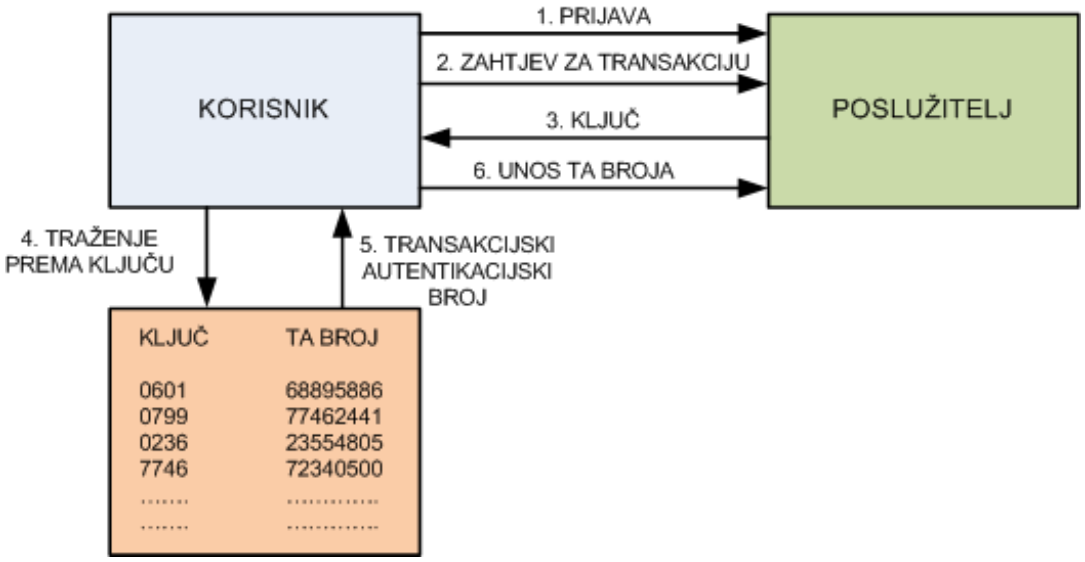
Napadač također mora saznati i otuđiti povjerljive podatke žrtve kako bi operateru mobilnih usluga „dokazao identitet". Ukoliko operater mobilnih usluga napadaču izda zamjensku karticu, napadač će moći pri pokušaju izvršavanja transakcija na ukradenom korisničkom računu primiti transakcijski autentikacijski broj i tako oštetiti žrtvu.

Međutim, da bi korisnike obranile od ove vrste napada, banke su promijenile metodu rada. Neke banke korisnicima izdaju dvije liste transakcijskih autentikacijskih brojeva, jednu za prijavu na uslugu, a drugu za provođenje transakcija. Također, i kod ove metode napadači su uspjeli nanijeti štetu korisnicima.

Korisnik je primio krivotvorenu e-poruku od napadača. Napadač je izradio e-poruku tako da izgleda kao da je poslana od banke. U e-poruci je sadržana poveznica (*eng. hyperlink*), čije se web adresa čini kao stvarna web adresa korisnikove banke, te tekst u kojem se od korisnika zahtjeva da se prijavi i izvrši neku vrstu transakcije. Web stranica koju korisnik posjeti je krivotvorena i kontrolira ju napadač. Ako korisnik unese oba transakcijska autentikacijska broja napadač ih može zloupotrijebiti i nanijeti ozbiljnu financijsku štetu korisniku.

Kako su i u ovoj metodi pronađeni načini za nanošenje financijske štete, bankarske ustanove su morale razinu sigurnosti korisnika podići na sljedeću razinu.

Banke su korisnicima dale liste transakcijskih autentikacijskih brojeva, te je svaki broj imao svoj ključ. Korisnik se morao prijaviti na uslugu s prvim transakcijskim autentikacijskim brojem. Pri obavljanju transakcije poslužitelj je korisniku poslao nasumično odabrani ključ koji postoji na korisnikovoj listi. Korisnik je potom na temelju ključa našao transakcijski autentikacijski broj i upisao ga pri autentikaciji transakcije. Opisana metoda prikazana je u nastavku:



Slika 9. Prikaz postupka pri autentikaciji transakcijskim autentikacijskim brojem

Uporabom ove metode onemogućeni su napadi zavaravanjem, jer napadači ne mogu saznati transakcijski autentikacijski broj koji je potreban za provođenje transakcije. Čak i ako se dogodi da napadač sazna ključ, ne može znati koji je transakcijski autentikacijski broj povezan s trenutno aktualnim ključem.

3.5. Jednokratne lozinke primljene SMS porukom

Kao što je u nekim prethodnim poglavljima napomenuto jednokratne lozinke je moguće primati na mobilni telefon putem SMS poruke. Korisnik pri prijavi na uslugu dobiva na mobilni telefon jednokratnu lozinku. Većina ovakvih usluga zahtijeva da se na mobilnom telefonu ugradi neki dodatni program.

Zloupotreba jednokratnih lozinki primljenih na ovaj način je moguća na način kako je opisano u prethodnom poglavlju. Tehnika jednokratne lozinke primljene SMS porukom ne zahtjeva dodatni uređaj koju korisnik mora posjedovati, već samo mobilni telefon. Većina aplikacija koje se koriste za generiranje lozinki na mobilnim telefonima je izrađena pomoću Java programskog jezika, pa postoji i dodatan sigurnosni rizik - sigurnosni propusti u aplikacijama za rukovanje jednokratnim lozinkama. Kako su mobilni telefoni vrlo rašireni, vjeruje se da će ova tehnika postati vrlo popularna.

Slika 10. Primjer generiranja jednokratne lozinke na mobilnom telefonu

3.6. Prednosti i nedostaci tehnika za generiranje jednokratnih lozinki

Jednokratne lozinke pružaju korisnicima dodatnu sigurnost, međutim svaka metoda zaštite korisnika ima svoje prednosti i nedostatke, pa tako i ova.

Prednosti korištenja jednokratnih lozinki su:

- Sustavi za generiranje jednokratnih lozinki su jednostavni i većina ih ne zahtjeva ugradnju bilo kakvih programa. Za razliku od njih, kod većine ostalih autentikacijskih sustava potrebno je ugraditi upravljačke ili druge programe (što ih čini složenijima za uporabu).
- Sustave za generiranje jednokratnih lozinki je jednostavno koristiti jer su vrlo slični sustavima za obične lozinke (korisnik za pristup aplikaciji upisuje korisničko ime i lozinku).
- Uređaji za generiranje jednokratnih lozinki koji koriste vremensku sinkronizaciju (npr. tokeni) i sustavi koji rade na temelju upita/odgovora (*eng. challenge/response*), kod kojih poslužitelj korisniku šalje upit, a korisnik na temelju upita pomoću uređaja generira jednokratnu lozinku (odgovor), se mogu koristiti na više usklađenih računala. Prednost je što se korisnik može spojiti putem bilo kojeg računala u sustavu, ali također i spajanje više korisnika na istu uslugu istovremeno.
- Upotrebom uređaja za generiranje jednokratnih lozinki i ispisanih lista jednokratnih lozinki, korisnik neće osjetiti posljedice čak i ako lozinka bude ukradena (jer istu lozinku nije moguće upotrijebiti više nego jednom). Problem se može pojaviti ako napadač uspije otuđiti i upotrijebiti lozinku prije korisnika.
- Pružaju primjerenu zaštitu od napada zavaravanjem (*eng. replay attack*) kod kojeg napadač presretne podatke i otuđi lozinku, koju nakon toga pokušava upotrijebiti. Ova vrsta napada neće imati nikakvog učinka jer, kao što je prije napomenuto, ista se lozinka na može upotrijebiti više puta. Također, onemogućen je i napad presretanjem (*eng. shoulder-surfing attack*) kod kojeg napadač promatranjem žrtve dok koristi npr. bankomat ili javna računala pokušava

otuđiti podatke. Krađa podataka i informacija prisluškivanjem (*eng. eavesdropping attack*), gdje napadač prisluškuje vezu žrtve kako bi saznao povjerljive podatke, i keylogger programima je uz nemogućnost korištenja iste lozinke više nego jednom ograničena još i vremenskim periodom trajanja.

Međutim metode prijave koje se temelje na jednokratnim lozinkama imaju i neke nedostatke. Najvažnije su navedene u nastavku:

- Korisniku i ponuđaču usluga su potrebni posebni programi ili uređaji kako bi sustav funkcionirao. Proizvođač također mora imati sustav za zaštitu korisničkih statičkih lozinki kako ih napadač ne bi otuđio i nanio štetu korisnicima.
- Ako se jednokratne lozinke generirane tehnikom vremenske sinkronizacije koriste na više usklađenih računala moguće je da napadač otuđi lozinku i upotrijebi je. Kraći vremenski razmaci (20-30 sekundi) smanjuju mogućnost otuđivanja. Ovakve je napade moguće spriječiti odgovarajućom zaštitom veze sa poslužiteljem.
- Većina uređaja za generiranje jednokratnih lozinki koji zahtijevaju unos korisnikove statičke lozinke ne pružaju jednaku razinu zaštite, jer napadač može napadom otkriti korisnikovu statičku lozinku, kao npr. uređaji koji rade na temelju vremenske sinkronizacije ili upita poslužitelja (challenge based) kod kojih nije potrebna statička lozinka.
- Sustavi koji jednokratne lozinke generiraju na temelju unaprijed zapisanih tablica su vrlo osjetljivi na napade. U unaprijed zapisanim tablicama se nalaze jednokratne lozinke koje se korisniku nasumično prikazuju pri zahtjevu za autentikaciju. Ukoliko napadač otkrije tablicu, otkrio je sve jednokratne lozinke i korisnik nije niti svjestan da ih napadač može upotrijebiti.

4. Usporedba tehnika generiranja jednokratnih lozinki

U ovom će poglavlju biti navedene prednosti i nedostaci pojedine tehnike kako bi se pokazalo pri kojim postupcima korisnici moraju biti oprezni, te koje su opasnosti od krađe podataka i nanošenja nekog oblika štete.

Tablica 3. Prikaz prednosti i nedostataka pojedine tehnike generiranja jednokratnih lozinki

Tehnika	Prednosti	Nedostaci
Matematički algoritmi	- nemoguće je pronaći funkciju koja bi na temelju jednokratne lozinke generirala korisnikovu statičku lozinku - vrlo dobra zaštita kriptografskom raspršnom funkcijom - u fizičkim uređajima koje koriste ovu metodu nisu potrebni brojači	- u većini postojećih kriptografskih raspršnih funkcija su pronađeni sigurnosni propusti - ukoliko napadač ukrade statičku lozinku i jednokratnu lozinku koja nije bila korištena moguće je nanošenje štete korisniku - zavaravanjem i krivotvorenjem web stranice napadač može otuđiti i zloupotrijebiti jednokratnu lozinku
Vremenska sinkronizacija	- u nekim slučajevima nije potreban tajni podatak za generiranje jednokratne lozinke - jednokratnu lozinku nije moguće upotrijebiti nakon što joj istekne period valjanosti - pri unosu krive lozinke, poslužitelj i uređaj će se ponovno sinkronizirati i uređaj će korisniku pokazati novu jednokratnu lozinku	- vremenska ograničenja za korištenje lozinki - ukoliko napadač otkrije algoritam koji generira jednokratnu lozinku na temelju ključa i vremena, moguće je nanošenje štete korisnicima - zavaravanjem i krivotvorenjem web stranice napadač može otuđiti i zloupotrijebiti jednokratnu lozinku - uređaji koji koriste ovu tehniku su tehnološki složene
„Challenge based“ tehnika	- jednokratna lozinka se generira na temelju upita poslužitelja i vremenskog trenutka - ako napadač i otuđi upit poslužitelja neće moći generirati valjanu jednokratnu lozinku	- zavaravanjem i krivotvorenjem web stranice napadač može otuđiti i zloupotrijebiti jednokratnu lozinku - uređaji koji koriste ovu tehniku su tehnološki složeni
Transakcijski autentikacijski brojevi	- lista brojeva je u posjedu korisnika, najčešće na listu papira što pridonosi sigurnosti (jer listi nije moguće pristupiti putem računala) - poslužitelj korisniku šalje ključ prema kojem korisnik nalazi transakcijski autentikacijski broj - mogućnost primanja transakcijskih autentikacijskih brojeva SMS porukom	- zavaravanjem i krivotvorenjem web stranice napadač može otuđiti i zloupotrijebiti jednokratnu lozinku - mogućnost prijevare korisnika putem mobilnog telefona i otuđivanje jednokratne lozinke
Jednokratne lozinke primljene SMS porukom	- nije potreban nikakav drugi uređaj koji bi generirao jednokratne lozinke	- mogućnost prijevare korisnika putem mobilnog telefona - nema garancije da će korisnik primiti SMS poruku s lozinkom

5. Praktične implementacije

Navedene tehnike generiranja jednokratnih lozinki je trebalo na neki način približiti korisnicima i to je učinjeno sa fizičkim uređajima (tokenima) ili programima za računala koji će korisniku generirati jednokratne lozinke za prijavu na uslugu.

5.1. Tokeni

Najčešće korišteni uređaji koji rade na temelju osobnih i tehničkih faktora su svakako tokeni. Sigurnosni token (*eng. security token*) je fizički uređaj koji korisnik koristi kako bi elektroničkim putem dokazao ili potvrdio svoj identitet. Tehnologija koja se koristi u ovim uređajima je vremenski sinkronizirana ili se temelji na upitu (*eng. challenge based*).

Za tokene koji se temelje na upitu potreban je poslužitelj koji će korisniku poslati upit. Taj upit se unosi u token kako bi se generirala jednokratna lozinka. Tehnike sinkronizacije zahtijevaju da token i poslužitelj istovremeno generiraju jednokratnu lozinku koristeći iste parametre (npr. redni broj pokušaja ili vrijeme). Ako su jednokratne lozinke generirane na poslužitelju i tokenu jednake, autentikacija je uspješna.

Slika 11. Prikaz izgleda tokena koji radi na temelju upita poslužitelja (challenge based)

Tokeni moraju zadovoljavati određene ISO standarde (ISO 13491-1:2007, ISO DIS 13491-2, ISO 9564, ISO 16609, ISO 11568) kojima se propisuju radne karakteristike uređaja, kriptografski procesi koje koriste uređaji, načini zaštite uređaja i kojima se standardizira način autentikacije.

Tokeni su obično dovoljno maleni kako bi ih korisnici mogli nositi sa sobom. Većina tokena ima kućište koje je gotovo nemoguće otvoriti ili sklop koji onesposobi i uništi uređaj kada se poklopac otvori kako ne bi bilo moguće kopirati tehnologiju i tako naštetiti drugim korisnicima.

Postoji više vrsta tokena podijeljenih s obzirom na način pokretanja, a to su:

- tokeni koje se pokreću statičkom lozinkom,
- tokeni koje se pokreću jednokratnom sinkroniziranom lozinkom,
- tokeni koje se pokreću jednokratnom lozinkom koja nije usklađena sa poslužiteljem i
- tokeni koji se pokreću upitom.

Jednostavnim sigurnosnim tokenima nije potrebna izravna veza sa računalom korisnika. Naprednije vrste tokena zahtijevaju neki oblik veze sa računalom (npr. USB ili Bluetooth) kako bi stupili u kontakt sa poslužiteljem. Iz ovoga slijedi podjela tokena prema načinu spajanja:

- tokeni koje je potrebno fizički spojiti na računalo, npr. putem USB-a, su tokeni koji će nakon spajanja na računalo ispisati autentikacijske podatke na računalu korisnika. Za upotrebu ovakvih tokena potrebni su pokretački programi. Ovakvi tokeni se najčešće koriste pri autentikaciji korisnika kod spajanja na neki zaštićeni mrežni sustav.
- tokeni koje je potrebno spojiti na računalo ili poslužitelj bežičnom vezom, npr. Bluetooth vezom, obično ne zahtijevaju od korisnika unos statičke lozinke. Spajaju se na računalo korisnika, kako je već ranije naglašeno nekom vrstom bežične veze. Jedino ograničenje kod ove vrste tokena je životni vijek i trajanje baterije koja ih pogoni. Vrlo često se koriste za provođenje transakcija putem Interneta (npr. kupovine putem Interneta).
- tokeni koje nije potrebno spajati nikakvom vezom su najčešće korištena vrsta tokena. Da bi korisnik generirao jednokratnu lozinku potrebna mu je statička lozinka. Za komunikaciju s korisnikom u ovu vrstu tokena ugrađeni su zaslon i tipkovnica kojom se korisnik služi kako bi

generirao jednokratnu lozinku. Ova vrsta tokena najčešće se koristi kod usluge Internet bankarstva.

Slika 12. Prikaz izgleda različitih vrsta tokena

Izvor: SecurityPro News

5.2. Programi

Programski alati za generiranje jednokratnih lozinki su namijenjeni za uporabu na osobnim računalima, prijenosnim računalima, džepnim računalima ili mobilnim telefonima. Programi za generiranje jednokratnih lozinki su osjetljiviji od fizičkih uređaja jer su izloženi zlonamjernim programima kojim se može zaraziti korisničko računalo (npr. virusi, crvi, keyloggeri, itd.). Međutim, programi imaju neke prednosti nad fizičkim uređajima:

- nije potrebno posjedovati fizički uređaj,
- kod programa, za razliku od fizičkih uređaja, nije potrebno posebno održavanje (baterije) i
- programi su ekonomski isplativiji.

Slika 13. Prikaz izgleda sučelja programa za generiranje jednokratnih lozinki

Izvor: SecurityPro News

Postoje dvije metode na kojima se temelje programi za generiranje jednokratnih lozinki:

- dijeljena tajna (*eng. shared secret*) i
- kriptografija s javnim ključem (*eng. Public-key cryptography*).

Dijeljena tajna je podatak poznat samo osobama koje sudjeluju u zaštićenoj komunikaciji. Dijeljena tajna može biti tajna riječ, rečenica, broj s velikim brojem znamenaka ili polje nasumično odabranih podataka. U slučaju da se tajna dodjeljuje korisnicima prije početka komunikacije, ista se naziva unaprijed dijeljena tajna (*eng. pre-shared key*). Također je moguće pri početku komunikacije uspostaviti dijeljenu tajnu uz pomoć protokola za uspostavljanje dijeljenih ključeva.

Kod kriptografije s javnim ključem se koriste asimetrični algoritmi za šifriranje pomoću ključeva, tj. algoritam za šifriranje nije isti kao i algoritam za dešifriranje. Svaki korisnik ima dva ključa, javni i osobni ključ. Osobni ključ je korisnikova tajna, dok javni ključ može biti poznat većem broju osoba. Poruke koje korisnik šalje se šifriraju javnim ključem, ali ih je moguće dešifrirati jedino odgovarajućim osobnim ključem. Dakle, velik broj osoba može primiti ili čak presresti poruku, ali je dešifrirati može jedino osoba koja ima odgovarajući osobni ključ (tj osoba kojoj je poruka upućena). Prednost ovakvog pristupa je visoka razina sigurnosti poruka koje izmjenjuju korisnici međusobno ili pri komunikaciji sa poslužiteljem. Više informacija o kriptografiji s javnim ključem moguće je saznati u dokumentu „Nedostaci PKI infrastrukture“ (CCERT-PUBDOC-2009-02-255) objavljenom na javnom webu CERTa (www.CERT.hr).

6. Praktična primjena

Velik broj novčanih transakcija i ostalih financijskih djelatnosti obavlja seputem Interneta, stoga je većina bankarskih ustanova počela svojim korisnicima dijeliti tokene za pristup Internet uslugama. Bankarske su ustanove također pribavile i odgovarajuće poslužitelje koji korisnicima omogućuju pristup bankarskim uslugama putem Interneta.

Većina napada na korisničke podatke se događa zbog pokušaja napadača da stekne nekakvu financijsku korist i tako nanese štetu korisnicima. Dvo-faktorskom autentikacijom je uvelike smanjen rizik od krađe podataka ili financijskih sredstava, međutim rizik nije moguće potpuno ukloniti jer je uvijek prisutan ljudski faktor - napadač može zavarati korisnika i otuđiti podatke. Stoga je kod korištenja usluga putem Interneta potrebno obratiti posebnu pažnju na krivotvorene stranice. Gotovo svi ponuđači ovakvih usluga su za korisnike pripremili posebne upute u kojima je navedeno kako se ispravno koriste dobiveni uređaji i na što treba obratiti dodatnu pažnju pri pristupanju i korištenju usluga putem Interneta.

Iako se pokazalo da su tokeni dovoljno pouzdani, neke se bankarske ustanove ipak nisu odlučile za primjenu ovakvih sustava. Manji dio bankarskih sustava svojim korisnicima nudi mogućnost autentikacije transakcijskim autentikacijskim brojevima i SMS porukama, što ima svoje prednosti, ali i mane. Također, ovo je područje u kojem je sigurnost od velike važnosti, pa su inovacije s naprednijim zaštitnim sustavima stalna pojava.

Jednokratne lozinke se također primjenjuju i kod pristupa udaljenim računalima na kojima se nalaze povjerljivi i osjetljivi podaci. Takvi su mrežni sustavi obično zaštićeni sa nekoliko vrsta zaštite kako bi se spriječila krađa osjetljivih podataka. Ako korisnici imaju potrebu spajati se na mrežni sustav sa udaljene lokacije, potrebno je osigurati sigurnu vezu kako ne bi došlo do gubitka podataka (npr. korištenjem nekog oblika VPN veze).

U edukacijskim ustanovama potrebno je svakodnevno nadgledati velik broj korisnika. U ovakvim okruženjima zaštita statičkom lozinkom više nije dovoljna, jer se radi o provjerljivim i osjetljivim podacima. Edukacijske ustanove su zakonski obvezane štititi privatnost podataka članova zajednice. Proizvođači uređaja za generiranje jednokratnih lozinki su omogućili korisnicima zaštitu s jednim uređajem kod lokalnog i udaljenog pristupa mrežnom sustavu, pristupa Internet uslugama i digitalnog potpisivanja podataka i poruka.

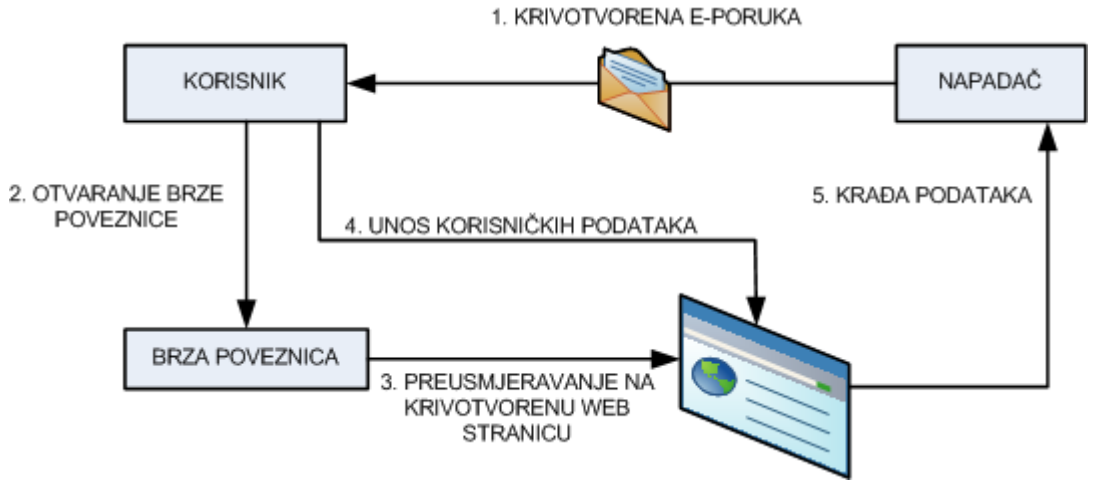
Na primjeru nekoliko sveučilišta i fakulteta, npr. Sveučilište za učenje na daljinu u Hagenu i Dartmouth College, prikazano je koliko je važna zaštita informacija koje posjeduju. Sveučilište za učenje na daljinu u Hagenu moralo je primijeniti zaštitu dvo-faktorskom autentikacijom, jer se sve radnje vezane uz obrazovanje, učenje ili polaganje ispita, odvijaju putem Interneta. Administracija sveučilišta je morala učiniti sve podatke vezane uz studente, osobne podatke, sadržaje predavanja, rezultate ispita ili administrativne podatke, dostupnima putem Interneta. Međutim, te je podatke bilo potrebno zaštititi od nedozvoljenog pristupa, izmjena ili krađe. Upotrebom jednog tokena koji je kombinacija više autentikacijskih tehnologija studenti su dobili primjerenu razinu zaštite.

7. Napadi na sustave koji koriste jednokratne lozinke

Iako jednokratne lozinke korisnicima pružaju visoku razinu zaštite od napadač, ipak tehnika nije savršena pa je moguće ukrasti i otuđiti podatke i nanijeti financijsku štetu. Napadači se najčešće koriste metodama poput *phishing*-a ili *man-in-the-middle* napada.

7.1. Phishing napad

Primjer phishinga su svakako poruke e-pošte u kojima je adresa pošiljatelja krivotvorena kako bi zavarala korisnika da se radi o autentičnoj poruci, npr. korisnikove banke. Iz sadržaja poruke korisnik ne može zaključiti da se radi o pokušaju krađe osobnih informacija ili podataka. U ovakvim slučajevima se u poruci nalazi poveznica (*eng. hyperlink*) koja bi korisnika trebala odvesti na službenu stranicu banke. Međutim, ta je poveznica izmijenjena na način da korisnika odvede na krivotvorenu stranicu. Korisnik potom pokušava pristupiti usluzi pri čemu njegovi autentikacijski podaci bivaju ukradeni.



Slika 14. Prikaz phishing napada

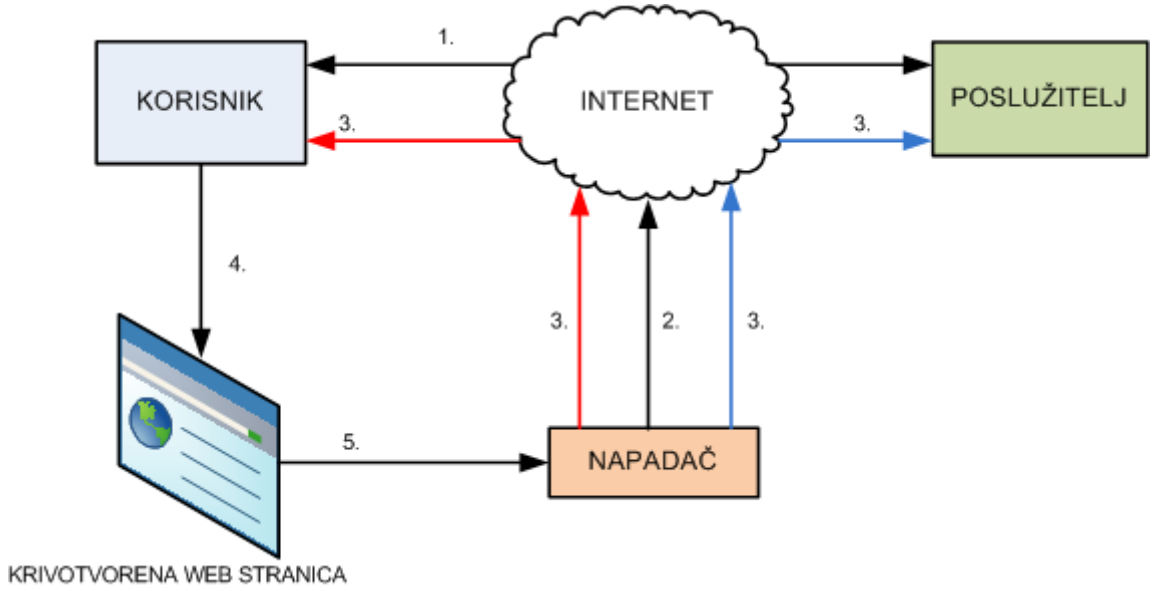
Napad se odvija na slijedeći način:

1. Napadač korisniku šalje krivotvorenu e-poruku koja sadrži poveznicu na krivotvorenu web stranicu.
2. Korisnik prima krivotvorenu e-poruku i otvara poveznicu.
3. Poveznica korisnika usmjerava na krivotvorenu stranicu. Krivotvorena je stranica izgledom jednaka kao i stvarna stranica.
4. Korisnik unosi svoje podatke i ne shvaća da je napadnut.
5. Nakon što je korisnik unio svoje podatke, napadač ih otkriva i zloupotrebljava.

7.2. Man-in-the-middle napad

Drugi česti oblik napada na sustave koji koriste jednokratne lozinke je *man-in-the-middle* napad. *Man-in-the-middle* napad je oblik aktivnog prisluškivanja u kojem napadač stvara zasebne veze sa žrtvama (korisnikom i poslužiteljem) pri čemu žrtve vjeruju da komuniciraju izravno jedna s drugom na „privatnoj“ vezi. Napadač mora biti sposoban presresti sve poruke koje se izmjenjuju između legitimnih sudionika komunikacije. Napad je uspješan jedino kada napadač uspije oponašati svaku žrtvu bez da bude zamijećen.

Korisnik šalje poslužitelju zahtjev za prijavu, a napadač presreće korisnikov zahtjev za prijavu i stvara krivotvorenu web stranicu identičnog izgleda kao i na stvarnom poslužitelju. Napadač također mora presresti i korisniku proslijediti upite i zahtjeve poslužitelja kako ne bi bio zamijećen. Ukoliko korisnik ne zamijeti da se radi o krivotvorenoj web stranici napad se nastavlja i korisniku bivaju ukradeni podaci.



Slika 15. Princip izvođenja man-in-the-middle napada

Man-in-the-middle napad se odvija na slijedeći način:

1. Korisnik šalje poslužitelju zahtjev za spajanje.
2. Napadač presreće korisnikov zahtjev i onemogućuje spajanje na stvarnog poslužitelja.
3. Napadač stvara zasebne veze sa korisnikom i poslužiteljem kako bi zavarao obojicu i izvršio napad (veza stvorena sa korisnikom označena je crvenom bojom, a veza stvorena sa poslužiteljem plavom bojom).
4. Korisnik biva preusmjeren na krivotvorenu web stranicu.
5. Korisnik unosi podatke i napadač ih otuđuje.

Međutim, moguće je zaštititi se od *man-in-the-middle* na sljedeće načine:

- infrastrukturom javnog ključa (*eng. public key infrastructure*),
- jakom uzajamnom autentikacijom (*eng. strong mutual authentication*),
- tajnim ključevima,
- dodatnim lozinkama,
- biometrijom (prepoznavanje glasa, otiska prsta ili zjenice),
- edukacijom korisnika i
- opreznim postupanjem s dobivenom tehnologijom (djelovanje u skladu s preporukama proizvođača).

8. Usporedba tehnike jednokratnih lozinka s drugim tehnikama dvo-faktorske autentikacije

Jednokratne lozinke nisu jedina vrsta dvo-faktorske autentikacije, stoga svakako vrijedi skrenuti pažnju i na druge tehnike. U nastavku poglavlja biti će pobliže opisane pametne kartice i biometrija, koji su također raširene tehnike dvo-faktorske autentikacije.

8.1. Pametne kartice

Pametne kartice (*eng. smart card*) su kartice koje sadrže integrirani sklop za obradu podataka. Dakle, u integrirani sklop na kratici se mogu unositi podaci ili iščitavati sadržaj s kartice. Integrirani sklop koji pametna kartica sadrži je nositelj autentikacijskog mehanizma. Najčešće se koriste za prijavu na velike mrežne sustave u tvrtkama i organizacijama. Pametne kartice je moguće podijeliti u dvije vrste:

- memorijske kartice na kojima su zapisani podaci i
- mikroprocesorske kartice koje sadrže promjenjive podatke i mikroprocesorske jedinice.

Slika 16. Primjer pametne kartice

Pametne kartice imaju sljedeće prednosti u odnosu na druge tehnike:

- koriste se za identifikaciju, autentikaciju i pohranu podataka
- zahtijevaju minimum ljudskog zalaganja jer je cijeli postupak automatiziran
- moguće ih je koristiti u bankarskim sustavima i tvrtkama za prijavu na računala ili usluge

Također, pametne kartice je moguće podijeliti prema izvedbi i to na:

- pametne kartice s kontaktom i
- pametne kartice bez kontakta.

Pametne kartice s kontaktom imaju na prednjoj strani vidljiv integrirani sklop, a autentikacija se izvodi izravnim dodirom sa električnim kontaktima u čitaču kartica.

Slika 17. Primjer čitača pametne kartice sa kontaktom

Izvor: Gemalto

Za razliku od pametnih kartica sa kontaktom, pametnim karticama bez kontakta nije potreban izravan dodir sa čitačem kartica, već samo približavanje kartice na dovoljnu udaljenost kako bi se izvršila identifikacija. Pametne kartice bez kontakta koriste identifikaciju pomoću radio frekvencija (*eng. radio frequency identification*). Ovakve kartice je moguće pronaći npr. kod naplate cestarina, evidencije radnog vremena, ali također i kod izvođenja brzih transakcija.

Pametne kartice omogućuju autentikaciju korisnika bez unosa korisničkih podataka, što svakako ubrzava proces autentikacije. Uređaji za generiranje jednokratnih lozinki nikada ne sadrže nikakve podatke o korisniku (npr. ime i prezime, matičnih broj, itd.), što nije uvijek slučaj kod pametnih kartica. Za razliku od uređaja za generiranje jednokratnih lozinki, pametne kartice je moguće krivotvoriti i tako korisniku nanijeti štetu.

8.2. Biometrija

Biometrija (*eng. biometrics*) se odnosi na metode raspoznavanja ljudi na temelju jedne ili više svojstvenih osobina i značajki. Biometriju je moguće podijeliti na fizička svojstva i svojstva u ponašanju. Fizička svojstva se svakako odnose na oblik tijela ili dijelova tijela pojedinca. Neki od primjera su: otisci prstiju, tehnike prepoznavanja lica, DNK, geometrija ruku i dlanova, itd. Svojstva u ponašanju se odnose na npr. ritam tipkanja na računalu, glasovno prepoznavanje, držanje osobe, itd.

Ljudske osobine ili svojstva koja zadovoljavaju sljedeće kriterije mogu se koristiti kao sredstvo za identifikaciju:

- **univerzalnost** - svaka osoba bi trebala imati karakteristično svojstvo/osobinu,
- **jedinstvenost** - govori koliko su biometrijska svojstva/osobine pojedinaca različite,
- **trajnost** - govori koliko je biometrijsko svojstvo/osobina otporna na starenje,
- **mogućnost prikupljanja** - govori koliko je jednostavno prikupiti uzorke za potrebna mjerenja.

Kako bi se osigurala autentikacija, odnosno ispravna identifikacija, kod biometrijskih sustava potrebno je prvo unijeti biometrijska svojstva pojedinca koji će koristiti sustav. Dakle, ukoliko se radi o identifikaciji otiska prsta, korisnik će prvo morati unijeti otisak u bazu podataka sustava kako bi se kasnije mogao putem istog sustava identificirati, tj. prijaviti. Postoji nekoliko podataka prema kojima se mjeri izvedba biometrijskog sustava:

- postotak lažnih podudarnosti (*eng. false accept rate*) je vjerojatnost da će sustav prihvatiti krivo biometrijsko svojstvo kao ispravno uspoređujući uneseno biometrijsko svojstvo sa onim koje se nalazi u bazi podataka biometrijskog sustava.
- postotak ispravnih, ali odbijenih svojstava (*eng. false reject rate*) je vjerojatnost da će sustav odbiti ispravno biometrijsko svojstvo.
- operativna karakteristika čitača biometrijskih svojstava (*eng. receiver operating characteristic*) je algoritam kojim se podešava omjer postotka ispravnih, ali odbijenih svojstava i postotka lažnih podudarnosti.
- omjer jednakosti greški je omjer postotka ispravnih, ali odbijenih svojstava i postotak lažnih podudarnosti. Što je manji omjer jednakosti greški, sustav je točniji.
- postotak zatajenja uslijed neispravnog unosa biometrijskog svojstva ili unosa biometrijskog svojstva loše kvalitete.
- postotak zatajenja jer sustav nije uspio učitati biometrijsko svojstvo kada je ispravno uneseno.
- broj uzoraka koji je moguće unijeti u bazu podataka biometrijskog sustava.

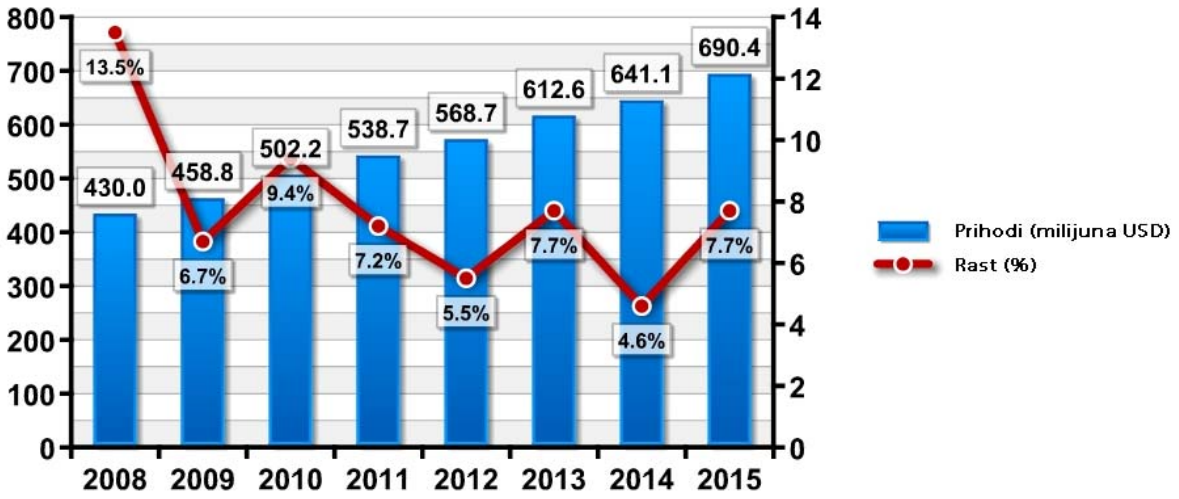
Biometrija je u odnosu na jednokratne lozinke mnogo sigurnija metoda, jer je vrlo teško krivotvoriti fizičke karakteristike osobe. Za razliku od jednokratnih lozinki, autentikacija pomoću biometrije se najčešće neće odvijati putem Interneta, već direktno putem uređaja za prepoznavanje svojstva osobe što svakako smanjuje mogućnost nanošenja štete korisniku. Nedostatak biometrije u odnosu na jednokratne lozinke je zasigurno cijena (cjenovne razine biometrijskih uređaja su neusporedivo skuplji od onih za generiranje jednokratnih lozinki). Također, uređaje za generiranje jednokratnih lozinki je relativno lako izvesti, tehnologija je komercijalizirana, za razliku od biometrijskih uređaja koji zahtijevaju tehnološki složene sklopove.

9. Budućnost tehnologije jednokratnih zaporki

Kako bi se osigurala nesmetana i sigurna komunikacija između krajnjih korisnika putem nesigurne mreže - Interneta, koriste se različite metode za autentikaciju sudionika komunikacije i zaštitu podataka. Jedna od novijih tehnologija – OTP pruža dodatne sigurnosne elemente (lozinka je valjana samo u određenom vremenskom trenutku, i dozvoljava samo jednu prijavu) za prilično nisku cijenu implementacije. Kako bi se poboljšala sigurnost i dalo veću slobodu korisnicima pri korištenju sustava koji koriste jednokratne lozinke, naglašava se razvoj novih i poboljšanih tehnika i tehnologija. Cilj je načiniti sustav koji će korisnicima pružati slobodu pri odabiru tehnologije, sustav koji će se moći primijeniti na specifične sustave.

"Initiative for Open Authentication" je organizacija koja se bavi poboljšanjem autentikacijskih protokola i mehanizama. Organizacija se sastoji od vodećih tvrtki koje se bave autentikacijskim uređajima i tehnikama. Standardizacija metoda za autentikaciju će pridonijeti sigurnom povezivanju industrijskih sustava i njihovih korisnika, te podizanju razine sigurnosti računalnih sustava tvrtki.

Stručnjaci navedene organizacije predviđaju veliki rast upotrebe jednokratnih lozinki, u svim područjima računalne djelatnosti. Kao što je vidljivo na slici 18., prihodi ostvareni poslovanjem sa sustavima koji koriste jednokratne lozinke u 2008. godini dostigli su vrijednost od 430 milijuna USD (2.4 milijarde kuna). Međutim, u 2015. godini se predviđa razina prihoda od oko 690 milijuna USD (3.9 milijardi kuna), uz prosječnu godišnju stopu rasta od 7.8 %.



Slika 18. Predviđanje rasta prihoda sustava koji koriste jednokratne lozinke na svjetskoj razini

Izvor: Initiative for Open Authentification, 2008.

Tržište sustava koji koriste jednokratne lozinke je još uvijek u razvoju, tako da se očekuje značajan rast upotrebe kroz slijedećih par godina. Najveći dosadašnji rast je zabilježen kod sustava koji koriste programe za generiranje jednokratnih lozinki, ali isto tako i pametnih kartica. Korištenje tokena još uvijek ima prednosti u odnosu na programska rješenja, tako da je u bankarskim okruženjima najčešća primjena različitih vrsta tokena. Državne ustanove također koriste ovu metodu autentikacije jer je važno osigurati podatke korisnika (npr. matični brojevi građana, brojevi osiguranja, putovnica, itd.).

Velike tvrtke zahtijevaju visoku razinu sigurnosti, isto kao i državne ustanove, pa su proizvođači uređaja za generiranje jednokratnih lozinki, kako bi se prilagodili potrebama korisnika, počeli kombinirati više različitih uređaja zajedno (npr. uređaj za autentikaciju kod prijave na računalo, na operacijski sustav, uređaj za digitalno potpisivanje i šifriranje poruka e-pošte, uređaj za generiranje jednokratnih lozinki kod prijave na uslugu putem Interneta, itd.).

10. Zaključak

Zbog rizika koji je prisutan pri korištenju usluga putem Interneta potrebna je primjerena zaštita koja će korisnicima zaštititi podatke. Statičke lozinke su podložne otkrivanju jer korisnici često ne obraćaju dovoljno pažnje na pokušaje napadača da otuđe njihove lozinke. Statičke lozinke također mogu biti zaboravljene ili izgubljene, a njihovoj osjetljivosti također pridonosi činjenica da ih velik broj korisnika zapisuje umjesto pamti. Kod usluga financijskog karaktera (i sličnih, gdje se obrađuju osjetljivi podaci) primjenjuju se različite tehnike dvo-faktorske autentikacije. Tehnike dvo-faktorske autentikacije su također primijenjene kod udaljenog pristupa mrežnim sustavima i računalima koji sadrže povjerljive podatke.

Jednokratne lozinke, kao tehnika dvo-faktorske autentikacije, pokazale su se kao učinkovito i sigurno rješenje pri rukovanju osjetljivim podacima. Međutim, gotovo svaka tehnika ima neke ranjivosti, tako da je potrebno pratiti upute za korištenje uređaja koji su dani korisnicima. Postojanje ovakvih sustava ne umanjuje vrijednost konvencionalnih alata za zaštitu, jer ukoliko je korisnikovo računalo zaraženo nekim zlonamjernim programom, napadač može otkriti unesene podatke. Stoga je i ovdje (kao i općenito kad se radi o sigurnosti) važno voditi aspekta o svim elementima zaštite, a ne temeljiti svoju zaštitu samo na jednom rješenju.

Mogućnosti za otkrivanje jednokratnih lozinki su male, ali ipak postoje. Upravo kako bi se zaštitilo korisnika u slučaju krađe jednokratne lozinke, kod nekih tehnika generiranja, lozinke imaju vremenski ograničen period upotrebe. Kod tehnološke izvedbe uređaja za generiranje jednokratnih lozinki pokušava se što manje opteretiti korisnika, tj. smanjiti mogućnost ljudske greške, na način da se cijeli postupak autentikacije automatizira. Tehnike generiranja jednokratnih lozinki su napredovale zbog tehnološkog razvitka, što korisnicima omogućuje veću razinu zaštite.

Jednokratne lozinke su metoda dvo-faktorske autentikacije koja se svakim danom širi na sve veći broj mrežnih sustava, edukacijskih ustanova i tvrtki. Uz ispravno korištenje uređaja za generiranje jednokratnih lozinki, edukaciju korisnika i oprez pri pregledavanju Interneta, sigurnost korisnikovih podataka je zagarantirana.

11. Reference

[1] Jednokratna lozinka, http://en.wikipedia.org/wiki/One-time_password, travanj 2009.

[2] Kriptografska raspršna funkcija, http://en.wikipedia.org/wiki/Cryptographic_hash_function, travanj 2009.

[3] Rasprava o autentikacijskim metodama, http://www.e.govt.nz/standards/e-gif/authentication/guide-multi-factor-auth/chapter5.html, travanj 2009.

[4] Dvo-faktorska autentikacija, http://en.wikipedia.org/wiki/Two-factor_authentication#Two-factor_authentication_methods, ožujak 2009.

[5] Jaka autentikacija, http://www.securitypronews.com/2004/0121.html, siječanj 2004.

[6] Sigurnosni tokeni, http://en.wikipedia.org/wiki/Security_token, travanj 2009.

[7] Programi za generiranje jednokratnih lozinki, http://en.wikipedia.org/wiki/Software_token, travanj 2009.

[8] Dijeljena tajna, http://en.wikipedia.org/wiki/Shared_secret, travanj 2009.

[9] Kriptografija s javnim ključem, http://en.wikipedia.org/wiki/Public-key_cryptography, travanj 2009.

[10] Pametne kartice, http://en.wikipedia.org/wiki/Smart_card, travanj 2009.

[11] Biometrija, http://en.wikipedia.org/wiki/Biometrics, travanj 2009.

[12] Initiative for Open Authentication, http://www.openauthentication.org/, travanj 2009.

[13] Autentikacija u edukacijskim ustanovama, http://www.aladdin.com/solutions/business-compliance/higher-education.aspx, travanj 2009.

[14] Pregled tržišta sustava koji koriste jednokratne lozinke, https://rsa-email.rsa.com/servlet/campaignrespondent?_ID_=rsa.4694&WPID=10096, travanj 2009.

[15] RSA, http://www.rsa.com/, travanj 2009.

[16] Aladdin, http://www.aladdin.com/, travanj 2009.