Bezbednost Web aplikacija

Osnovni ciljevi mera bezbednosti

- **Osnovni ciljevi mera bezbednosti u IKT sistemima su:**
  - **Poverljivost** – obezbeđuje nedostupnost informacija neovlašćenim licima.
  - **Integritet** – obezbeđuje konzistentnost podataka, sprečavajući neovlašćeno generisanje, promenu i uništenje podataka.
  - **Dostupnost** – obezbeđuje da ovlašćeni korisnici uvek mogu da koriste servise i da pristupe informacijama.
  - **Upotreba sistema isključivo od strane ovlašćenih korisnika** – obezbeđuje da se resursi sistema ne mogu koristiti od strane neovlašćenih osoba niti na neovlašćen način.

Opasnosti od hakera

Nakon što je lokacija postavljena i pokrenuta, hakeri mogu da je napadnu na različite načine:

- **Presretanjem, pregledanjem i menjanjem HTTP poruka** koje server razmenjuje sa čitačima korisnika
- **Pristupanjem datotekama koje se nalaze na serveru** i koje mogu da sadrže osetljive informacije kao što su podaci o kreditnim karticama korisnika
- **Pokretanjem hiljade zahteva serveru** koji troši resurse lokacije i posetiocima sprečavaju pristup lokaciji
- **Inficiranjem računarskim virusom** datoteka, diskova ili elektronskih poruka koje dolaze na lokaciju
- **Zaustavljanjem CGI skriptova** da ne bi pristupili serveru

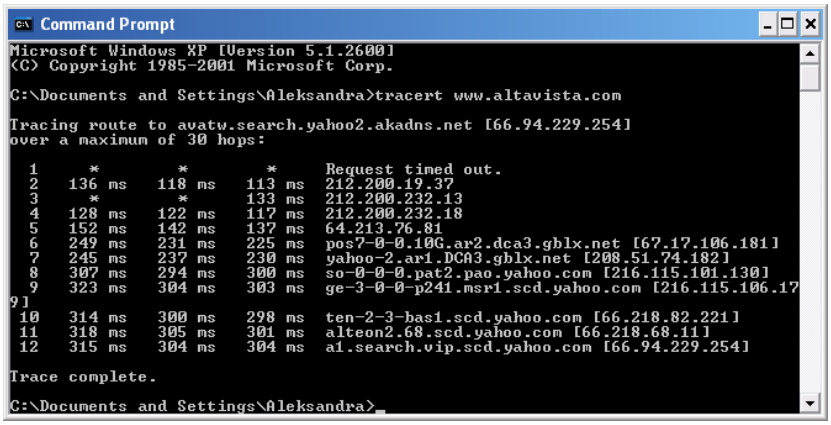
3

Presretanje mrežnih poruka

- Kada programi šalju informacije udaljenim računarima preko Interneta, poruke ne putuju direktno od računara koji ih šalje do primaoca poruke
  - Poruka prolazi kroz veliki broj lokacija na mreži
- Zadavanjem komande **tracert** (*trace route* – praćenje putanje) dobija se spisak lokacija kroz koje poruka putuje do udaljene lokacije
- Sledeći listing ilustruje putanju kojom je putovala poruka od autorovog računara do lokacije **yahoo.com**

4

Spisak lokacija kroz koje poruka putuje do udaljene lokacije



5

Poruka putuje kroz mnogo lokacija dok se kreće preko mreže

6

Presretanje mrežnih poruka

- Haker kroz čiji sistem poruka prolazi tokom putovanja može da pročita i izmeni sadržaj poruke u bilo kom trenutku tokom putovanja poruke
- Npr. ako poruka sadrži informacije o kreditnim karticama, dok poruka prolazi kroz hakerov sistem, on može da čita i snima podatke o kreditnim karticama

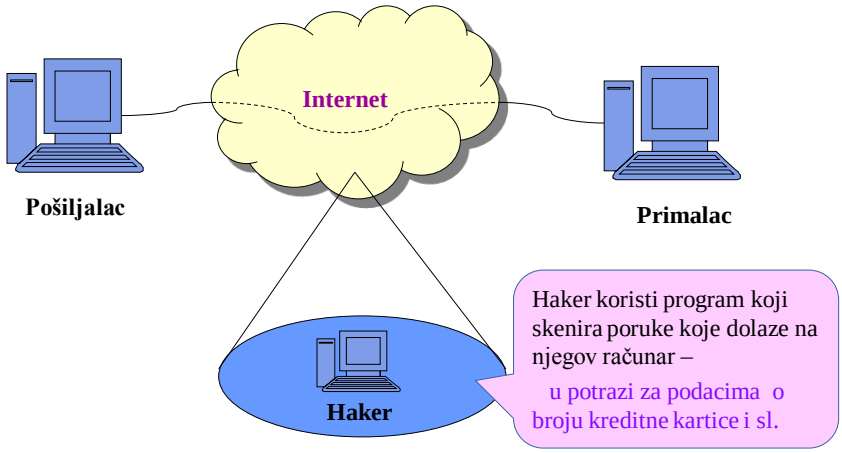
7

Korišćenje programa CommView za pregledanje HTTP poruka

- Kada korisnik pošalje neki sadržaj, čitač ga šalje serveru korišćenjem protokola HTTP
- HTTP prosleđuje poruke kao običan tekst, što znači da haker lako može da pregleda sadržaj poruke
- Korišćenjem programa **CommView** može se pregledati sadržaj velikog broja tipova poruka u sistemu
- Haker može da koristi program sličan CommView da bi nadgledao poruke koje dolaze na njegov računar

8

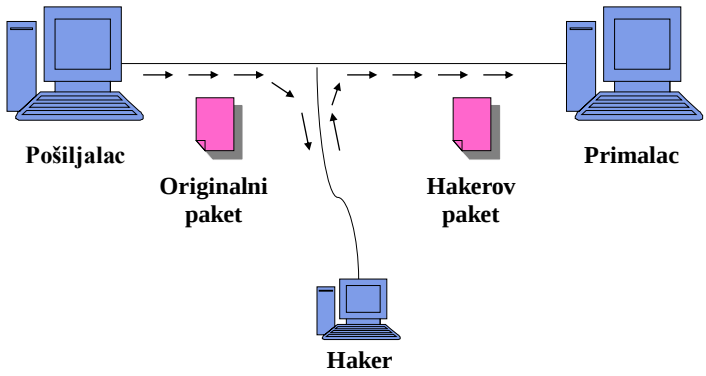
Hakeri preuzimaju osetljive informacije iz poruka koje presreću



Hakeri preuzimaju osetljive informacije iz poruka koje presreću

- Pored toga što presreće poruke, haker može i da im menja sadržaj
- Ako, npr. haker presretne poruku koja sadrži narudžbinu za kupovinu
  - on može promeniti količinu robe i adresu prispeća, tako da će roba stići njemu umesto stvarnom poručiocu
- Zaštita poruka od ovakvih opasnosti može se realizovati šifrovanjem i obezbeđivanjem Web stranica

Hakeri preuzimaju osetljive informacije iz poruka koje presreću



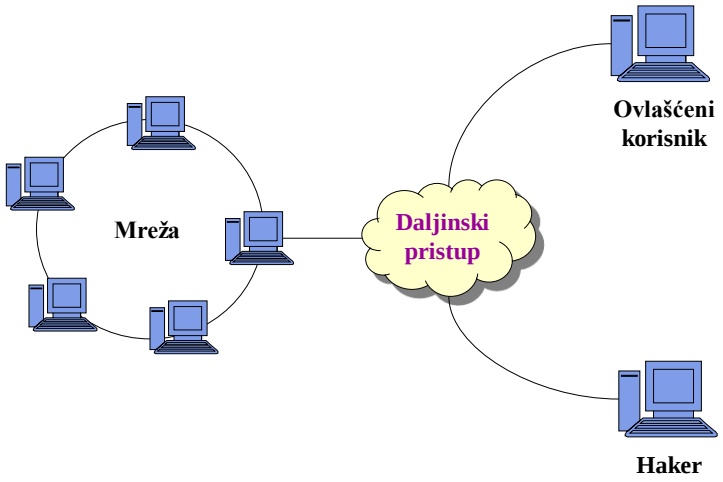
11

Kako hakeri "provaljuju" sistem

- Mnogi sistemi omogućavaju korisnicima da se preko Interneta prijave na mrežu sa udaljenih mesta. Npr.
  - Kompanija može omogućiti svojim trgovačkim putnicima da se prijave na mrežu kompanije, tako da mogu pregledati, formirati ili ažurirati informacije u narudžbini ili pristupiti e-pošti.
  - Sistem može omogućiti programerima, Web dizajnerima i drugim korisnicima da se povežu sa udaljenih mesta kako bi poslali ili preuzeli datoteke.
- Kada je sistem osposobljen za daljinski pristup, hakeri mogu da zloupotrebe programe i usluge za daljinski pristup da bi provalili u mrežu.

12

Kako hakeri “provaljuju” sistem



13

Kako hakeri “provaljuju” u sistem

- Da bi provalio u mrežu koja koristi daljinski pristup, haker obično mora da zada važeće korisničko ime i lozinku
- Haker pristupa važećim korisničkim imenima i lozinkama pomoću velikog broja tehnika:
  - koristi program za razbijanje lozinke koji napada datoteku lozinki sistema,
  - cilja na opšte podrazumevane naloge za koje mrežni administratori nisu promenili lozinke,
  - pita korisnika s važećim nalogom koje mu je korisničko ime i lozinka.

14

Softver za razbijanje lozinke

- Ranije su hakeri koristili programe pod nazivom razbijači lozinke koji su uzastopno unosili kombinacije korisničkog imena i lozinke
- Korišćenjem razbijača lozinke, haker je za minut mogao da isproba hiljade različitih kombinacija korisničko ime/lozinka
- Danas operativni sistemi blokiraju nalog ako korisnik ne unese ispravan par korisničko ime/lozinka u zadatom broju pokušaja
- Većina operativnih sistema smešta informacije o korisničkim nalozima u datoteku
  - ta datoteka je obično šifrovana
  - međutim, na Webu postoje programi koji dešifruju lozinke
  - datoteke će se najbolje zaštiti kad se zaštite nalozi administratora

15

Zaštita podrazumevanih naloga

- Kada se prvi put instalira operativni sistem ili velika aplikacija, softver obično obezbeđuje nekoliko podrazumevanih naloga koji se mogu koristiti da bi se obavila instalacija, proverili parametri sistema i slično.
  - Mnogi korisnici ne isključuju ove podrazumevane naloge nakon instaliranja aplikacije.
- Hakeri provaljuju u sistem preko Interneta korišćenjem podrazumevanih naloga koji nisu isključeni.
- Bezbednost lokacije može se poboljšati
  - obaveznom promenom lozinke za sve podrazumevane naloge,
  - onemogućavanjem korišćenja nepotrebnih podrazumevanih naloga,
  - vremenskim ograničavanjem korisničkih naloga na pristup samo tokom radnih sati.

16

Kako hakeri onemogućavaju pristup sistemu

- Kada haker ne može da provali u sistem, on može da izvodi sabotaže koje troše resurse sistema
  - delimično (usporava lokaciju) ili
  - potpuno (sprečava pristup posetiocima)
- Npr. Pre nekoliko godina, hakeri su oborili server za elektronsku poštu Bele kuće bombardovanjem elektronske adrese desetinama hiljada velikih elektronskih poruka –
  - iako sami hakeri nisu mogli da provale na lokaciju Bele kuće, onemogućili su druge da koriste usluge lokacije.
- Npr. HTML datoteka može da koristi oznaku <meta> da bi usmerila čitač da preuzima veliku grafičku datoteku sa lokacije www.SomeVictim.com svakih 30 sekundi

```
<html>
<meta http-equiv="Refresh" content="30" />
<img src=http://www.SomeVictim.com/LargeImageFile.jpg />
</html>
```

17

Kako hakeri napadaju CGI skriptove

- Godinama su hakeri ciljali CGI skriptove da bi provalili na Web lokacije
  - zato što skript programi koji se izvršavaju na Web serveru mogu da pristupe podacima smeštenim na disku servera
- Zavisno od obrade koju obavljaju skriptovi, haker može da (zlo)upotrebi skript tako što ga izvrši koristeći vrednosti koje mu dodeljuje izvan procesa slanja obrasca
- Ako haker može da pristupi hard disku Web servera, može da zameni skript datoteku vlastitom
- Zavisno od obrade koju obavlja hakerov novi skript, moglo bi da prođe dosta vremena dok administratori lokacije ne otkriju promenu

18

Napadi preopterećenjem bafera

- Preopterećenje bafera se pojavljuje kada korisnik (koji ne mora da bude haker) pošalje više podataka nego što skript može da smesti
  - Na primer, korisnik u polje za unos teksta unese više karaktera nego što je predviđeno
- Problem sa greškama preopterećenja bafera leži u tome što neki skript jezici izazivaju kvar skript procesora
- Zavisno od operativnog sistema koji se izvršava na serveru, takve greške mogu hakeru omogućiti pristup serveru i datotekama koje sadrži
- Da bi zloupotrebio grešku preopterećenja bafera, haker prvo izaziva kvar skript procesora – kada pristupi serveru, haker može da kopira ili briše datoteke ili pokreće druge programe koji se nalaze na serveru

Napadi preopterećenjem bafera

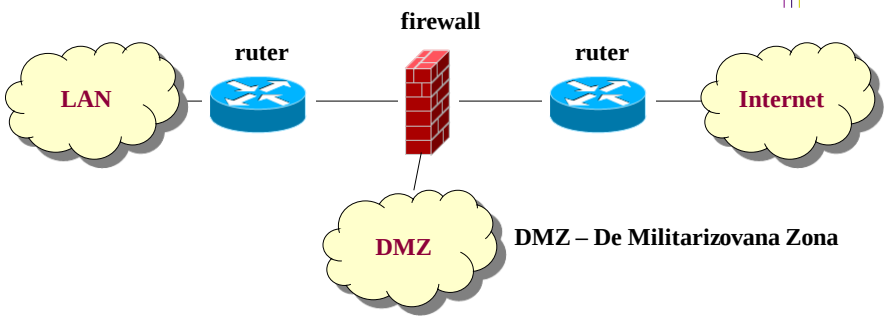
- Tokom godina, programeri operativnih sistema, programeri skript procesora i programeri koji prave Web skriptove, postali su svesni rizika od greške preopterećenja bafera
- Mnoge novije aplikacije ne kvare se nakon greške preopterećenja bafera tako da haker ne može da preuzme kontrolu nad serverom
- Na Web lokaciji CERT-a na http://www.cert.org postoji
  - pregled aplikacija koje su ranjive preopterećenjem bafera,
  - kao i slabosti drugih softvera - PHP, ActiveX, ASP i sl.

Kako barijere (firewall) štite lokaciju

- Da bi zaštitili svoju mrežu od napada hakera, administratori mreže stavljaju barijeru između Interneta i mreže
- Barijera može da bude posebna hardverska kutija ili računar na kojem je pokrenut odgovarajući softver
- Barijera filtrira mrežne poruke koje dolaze sa Interneta u mrežu
  - mrežne poruke su podaci koje programi (čitači Weba, programi za ćaskanje, za prenos datoteka ..) šalju sa jednog računara na drugi
- Barijera dozvoljava samo HTTP porukama poslatim sa udaljenog čitača da uđu u mrežu, a sprečava poruke iz aplikacija kao što su programi za ćaskanje ili programi za prenos datoteka (kao što je FTP) da uđu u mrežu

21

Korišćenje firewall-a za zaštitu (tipska šema)



Po pravilu, *firewall* se realizuje kao uređaj sa dva ili više *ethernet* interfejsa. U zavisnosti od načina realizacije *firewall* može da bude:

- **Softverski** – softver koji se instalira na računar opšte namene
- **Hardverski** – namenski razvijen računar sa odgovarajućim softverom
- Softver **Integrisan sa ruterom**

22

DMZ

- U DMZ se smeštaju serveri koji treba da budu vidljivi i sa Interneta i iz lokalne mreže
- U slučaju postojanja DMZ-a, firewall najčešće ne dozvoljava direktnu komunikaciju *lokalne mreže* (*LAN*) - *Internet* već isključivo kroz DMZ
- U slučaju kompromitovanja (oštećenja, hakerskog napada) nekog od servera u DMZ-u, to neće značiti i da je automatski cela mreža kompromitovana

23

Podešavanje bezbednosnih usluga u Windowsu

Bezbednosne usluge u Windows-u

1. Fino podešavanje dodele priključaka barijere
2. Smanjenje izloženosti lokacije virusima
3. Nadgledanje sistemskih događaja radi otkrivanja uljeza
4. Onemogućavanje daljinskih usluga
5. Korišćenje sistema sa povratnim pozivom
6. Analiza ranjivosti sistema

25

Fino podešavanje dodele priključaka barijere

- Da bi komunicirao preko mreže, program pošiljalac mora da zada adresu udaljenog računara
- Pored toga, program pošiljalac mora da identifikuje aplikaciju na udaljenom računaru kojoj šalje poruku
  - Mrežni programi identifikuju udaljene aplikacije korišćenjem broja koji programeri označavaju kao broj priključka aplikacije
- Sledeći spisak prikazuje brojeve priključaka koji odgovaraju opštim aplikacijama

26

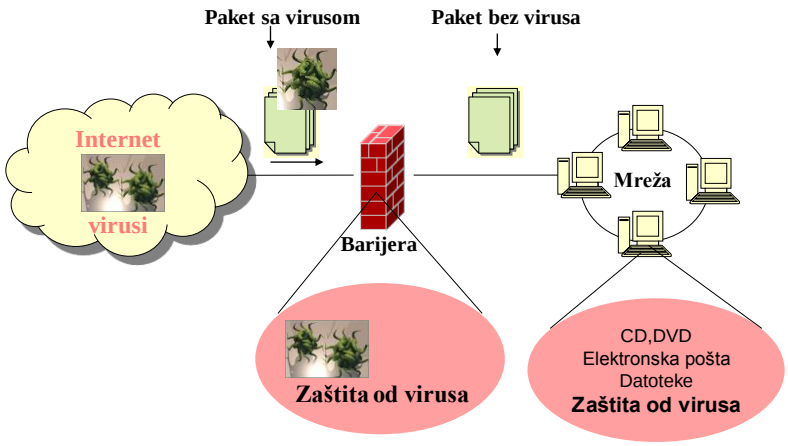
Brojevi priključaka koji odgovaraju opštim aplikacijama

Broj priključka	Aplikacija
21	Protokol za prenos datoteka (FTP)
23	Telnet
25	Jednostavni protokol za prenos pošte (SMTP)
80	Protokol za prenos hiperteksta (HTTP)
139	Sesijska usluga NetBIOS

Tokom konfigurisanja barijere, prvo je potrebno onemogućiti poruke za sve priključke, a zatim omogućiti pristup samo onim posebnim priključcima koji su potrebni

27

Smanjenje izloženosti lokacije virusima



28

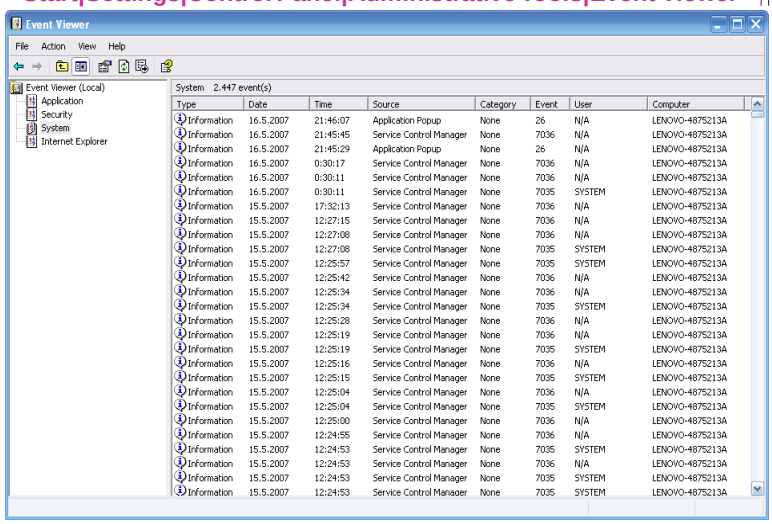
Nadgledanje sistemskih događaja radi otkrivanja uljeza

- Hakeri koriste mnoge tehnike za napade na sisteme
- Evidencija događaja se sastoji od jedne ili više datoteka evidencije koje održava operativni sistem radi praćenja korisnikovih aktivnosti
- Evidentiranje događaja pomaže da se uhvati haker koji je sa uspehom provalio u sistem
- U Windowsu poseban program pod nazivom **Event Viewer** omogućava administratorima sistema da pregledaju evidenciju različitih događaja
- **Event Viewer** evidentira tri tipa događaja: aplikacijski, bezbednosni i sistemski

29

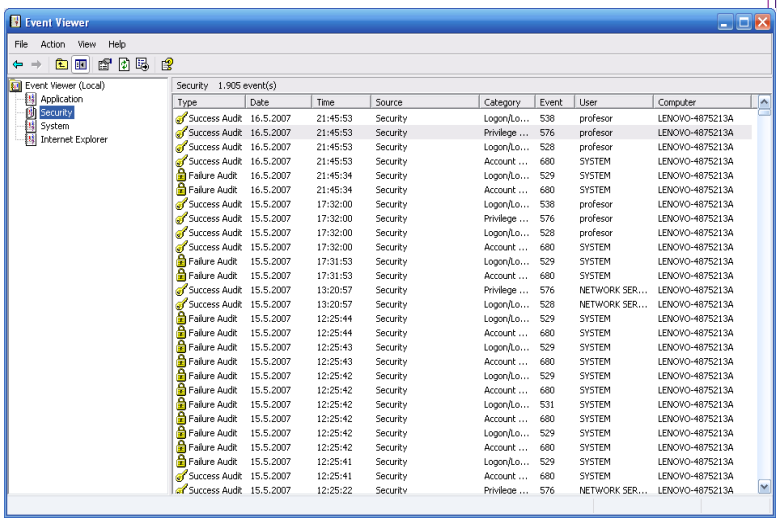
Event Viewer za praćenje događanja na sistemu

Start|Settings|Control Panel|Administrative Tools|Event Viewer



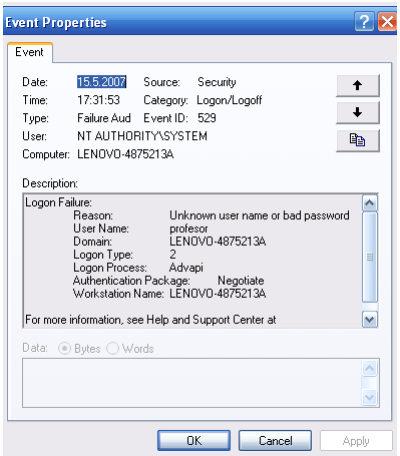
30

Izgled evidencije bezbednosti u Event Vieweru



31

Izgled evidencije bezbednosti u Event Vieweru



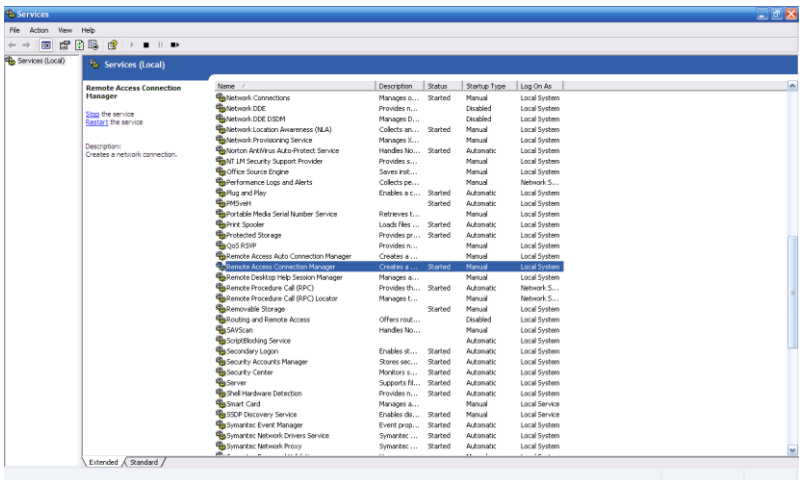
32

Onemogućavanje daljinskih usluga

- Mnoge Web lokacije dozvoljavaju korisnicima da se prijave na mrežu sa udaljenih mesta
- Ako to lokaciji nije potrebno, trebalo bi onemogućiti daljinske usluge da bi se smanjio rizik od hakerske zloupotrebe usluga za pristupanje sistemu
- Zavisno od operativnog sistema, razlikuju se koraci koji se moraju izvesti da bi se sprečio daljinski pristup
- U nastavku je dat prikaz onemogućavanja daljinskih usluga u Windowsu
- **Start|Settings|Control Panel|Administrative Tools|Services**

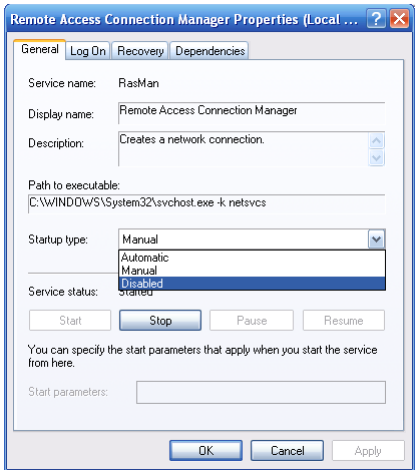
33

Prozor Services



34

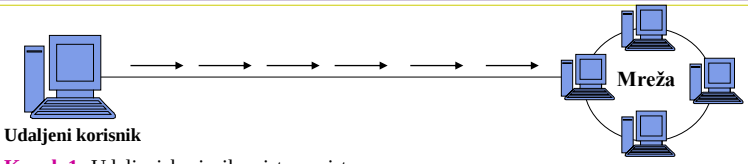
Onemogućavanje daljinskih usluga



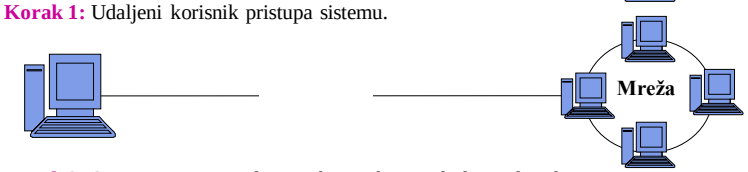
Onemogućavanje daljinskih usluga

- U nekim trenucima korisnici imaju opravdanu potrebu da pristupe mreži iz daljine
- Ako postoje jedan ili više korisnika koji pristupaju mreži preko modema, može se povećati bezbednost sistema korišćenjem sistema sa povratnim pozivom
  - Udaljeni korisnik pristupa sistemu preko svog modema
  - Zavisno od softvera za povratni poziv, korisnik može da pozove određeni broj ili se od korisnika može tražiti da nakon biranja broja dostavi korisničko ime i lozinku ili digitalni sertifikat
  - Sistem sa povratnim pozivom zatim će prekinuti poziv i ponovo pozvati korisnika na unapred određeni broj – kao što je broj telefona modema u korisnikovoj udaljenoj kancelariji ili kući
- Na ovaj način haker na bilo kom drugom mestu ne može daljinski da pristupi sistemu, zato što sistem s povratnim pozivom neće uputiti povratni poziv hakerovom modemu

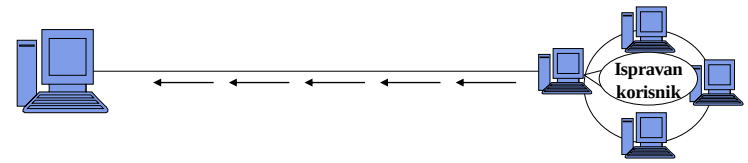
Sistem sa povratnim pozivom



Korak 1: Udaljeni korisnik pristupa sistemu.



Korak 2: Server proverava identitet korisnika i prekida modemsku vezu.



Korak 3: Ako je udaljeni korisnik ispravan, server ga poziva na unapred određen broj.

Analiziranje ranjivosti sistema

- Postoji nekoliko Web lokacija na kojima se može proveriti koliko je lokacija ranjiva
- Većina provera koje obavljaju ove lokacije odnose se na probleme karakteristične za mrežu, za razliku od ranjivosti operativnog sistema
- Postoji nekoliko uslužnih programa koji se mogu preuzeti i pokrenuti radi obavljanja tih posebnih provera
- Na lokaciji http://www.insecure.org/tools.html može se pregledati lista najefikasnijih bezbednosnih alata

KRIPTOGRAFSKE TEHNOLOGIJE

Kriptografske mere bezbednosti

Kriptografija (Criptography)	⟺	skup tehnika i aplikacija koje se zasnivaju na matematički teškim problemima
Kriptoanaliza (Cryptoanalysis)	⟺	oblast u kojoj se nastoje kompromitovati (razotkriti) kriptografski mehanizmi
Kriptologija (Cryptology)	⟺	nauka o tajnim komunikacijama - objedinjuje kriptografiju i kriptoanalizu

- **Kriptovanje (Encrytion)** - transformacija podataka u oblik koji je nemoguće pročitati bez određenog znanja (tajne, ključa) - šifriranje
- **Svrha kriptovanja** - privatnost podataka, skrivanje informacije od svakog kome ona nije namenjena
- **Dekriptovanje (Decryption)** - transformacija kriptovanih podataka u razumljivu formu - dešifrovanje

40

Kriptografske mere bezbednosti

osnovni kriptografski zahtevi ►►

- integritet podataka
- autorizacija korisnika
- poverljivost podataka
- neporecivost

Sistemi plaćanja ne izvršavaju ni jednu delikatnu operaciju dok se ne izvrši eksplicitna provera autentičnosti korisnika.

41

Kako šifrovanje štiti poruke koje se šalju preko mreže

- Nemoguće je sprečiti hakere da presreću poruke u mreži
- Šifrovanjem poruka koje se šalju sprečava se haker da pregleda i izmeni informacije u njima
- Da bi razmenjivali šifrovane poruke, dva programa, kao što su programi čitača i servera, moraju prvo da usvoje zajednički algoritam koji će koristiti da bi šifrovali poruke
- Na primer –ABC šifruje se kao BCD pomeranjem svakog slova za jedno mesto unapred
- Čitač i server utvrđuju koju metodu šifriranja će koristiti
  - moraju da se slože o broju mesta za koje će se znakovi pomerati — utvrđuju **ključ za šifru**

42

Kako šifrovanje štiti poruke koje se šalju preko mreže

- Algoritmi šifrovanja na Webu su slični prethodnom, ali mnogo složeniji
- Kada čitač Weba pokrene bezbedan prenos na Webu, prvo šalje serveru spisak algoritama šifrovanja koje podržava
- Server pregleda spisak i bira algoritam koji podržavaju i on i čitač, potom čitaču šalje poruku koja zadaje izabrani algoritam
- Pre nego što dva programa mogu da koriste algoritme za šifrovanje poruka, oni moraju da se slože oko ključa za šifru

43

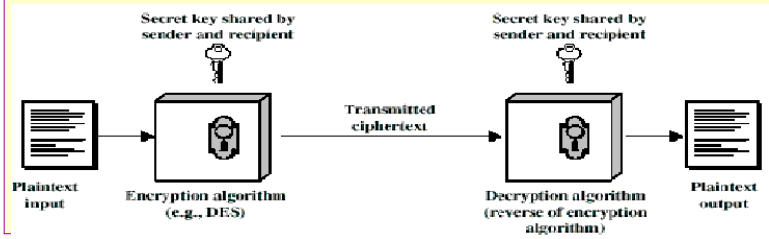
Kriptografske mere bezbednosti

- Svaki šifarski sistem obuhvata par transformacija podataka, koje se nazivaju šifrovanje i dešifrovanje.
- **Kriptovanje (šifrovanje)** je procedura koja transformiše originalnu informaciju (otvoreni tekst) u šifrovane podatke (šifrat).
- Inverzna operacija, **dekriptovanje (dešifrovanje)**, rekonstruiše otvoreni tekst na osnovu šifrata.
- Kriptovanje i dekriptovanje koriste određeni vid tajne informacije, poznate pod nazivom **ključ** (*eng. key*).

44

Kriptografske mere bezbednosti

- Šema šifrovanja ima 5 komponenti:
  1. Tekst koji se šifruje (plaintext)
  2. Algoritam šifrovanja
  3. Tajni ključ
  4. Šifrovani tekst (ciphertext)
  5. Algoritam dešifrovanja



45

Kriptografske mere bezbednosti

- Šifrovanje je, pojednostavljeno, matematička funkcija čiji izlaz zavisi od dva ulazna parametra :
  - originalna poruka koja se šifrira P (Plaintext)
  - ključ K
- Rezultat je niz naizgled nepovezanih brojeva koji se mogu, bez straha od mogućnosti da poruka dođe u neželjene ruke, prenositi do osobe kojoj je namenjena.
- Da bi šifrovanu poruku druga osoba mogla da koristi potrebno je sprovesti obrnuti postupak od šifrovanja, dešifrovanje.

46

Kriptografske mere bezbednosti

- Dešifrovanje je, pojednostavljeno, matematička funkcija čiji izlaz zavisi od dva ulazna parametra:
  1. šifrovana poruka C (Chiphertext)
  2. ključ K^{-I}
- Kao rezultat funkcije dobija se originalna poruka
- Minimalna i potrebna informacija koju dve osobe moraju da dele, ako žele da razmenjuju podatke na siguran način jeste skup ključeva (K, K^{-I})
- Prema odnosu ključeva K i K^{-I} i algoritmima šifriranja kriptografske sisteme delimo na simetrične i asimetrične.

47

Vrste kriptografskih mehanizama

Dve osnovne vrste kriptografskih mehanizama

Simetrična kriptografija

Asimetrična kriptografija

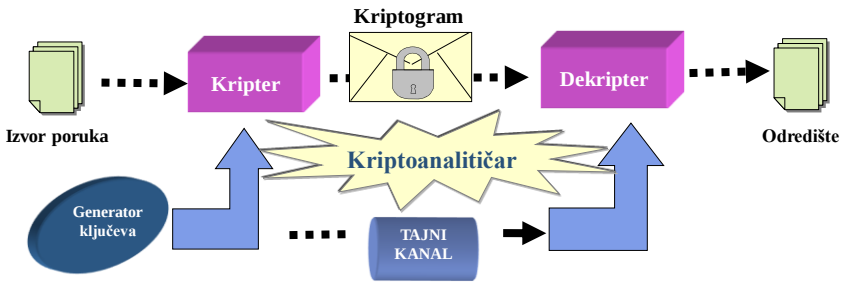
48

Simetrična kriptografija

- **Simetrična kriptografija** ili **kriptografija sa tajnim ključem** - tradicionalni oblik kriptografije u kom se isti ključ koristi kako za kriptovanje tako i za dekriptovanje. $K = K^{-1}$
- Kriptografski algoritam vrši obradu originalne poruke, koja se naziva **kriptogram** (*eng. ciphertext*), kojom se ostvaruje prvi cilj kriptografije.
- Kako oba korespodenta koriste identične ključeve - uveden je pojam tajnog kanala kojim se ključ razmenjuje.
- Egzistencija tajnog kanala je najslabije mesto simetričnog kriptografskog sistema.

49

Simetričan kriptografski sistem



50

Simetrična kriptografija

- U klasičnoj kriptografiji oba korespodenta znaju i koriste isti tajni ključ.
- Svako ko zna tajni ključ može da ga upotrebi za čitanje, modifikaciju i zloupotrebu svih poruka koje su kriptovane ili autorizovane pomoću tajnog ključa.
- Generisanje, prenos i skladištenje ključeva zove se **upravljanje ključem** (*eng. key managment*).
- Kriptografija sa tajnim ključem ima problem u obezbeđivanju tajnosti u upravljanju ključem, naročito u otvorenim sistemima sa velikim brojem učesnika.
- Prednost simetrične kriptografije leži u praktičnoj realizaciji gde se ovaj metod pokazuje kao vrlo brz, jer nema velikih zahteva u računanju.

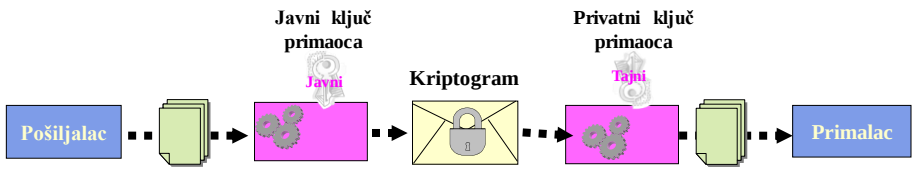
51

Asimetrična kriptografija

- Motivisani problemom upravljanja ključem, *Diffie* i *Hellman* su 1976. godine predstavili koncept **kriptografije sa javnim ključem**
- Kriptografija sa javnim ključem ima dve značajne primene:
  - kriptovanje i
  - digitalni potpis.
- U sistemu koji koristi asimetričnu kriptografiju, svaki učesnik dobija par ključeva:
  - jedan **tajni** ključ i
  - jedan **javni** ključ.
- Javni ključ se objavljuje, dok tajni čuva korisnik.

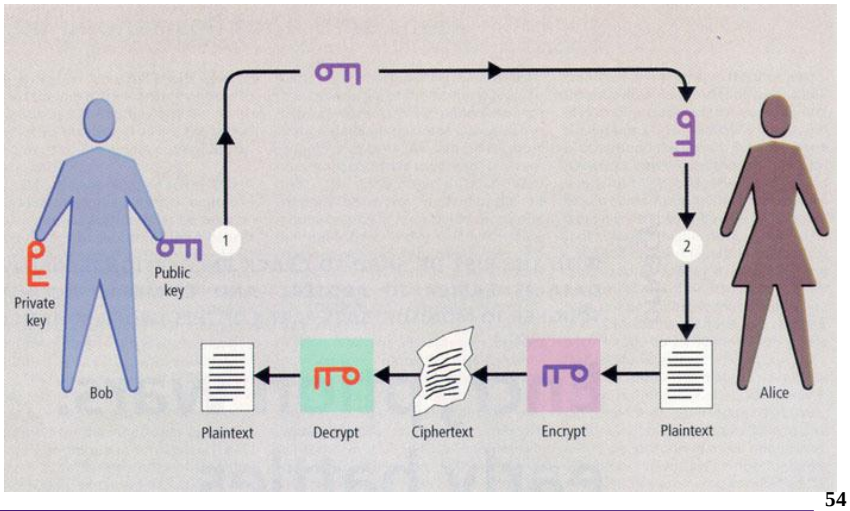
52

Asimetričan kriptografski sistem -



53

Asimetričan kriptografski sistem - suština rada sistema



54

Asimetričan kriptografski sistem

- Ako pošiljalac hoće da pošalje poruku, prvo potraži javni ključ primaoca u imeniku, koristi ga za kriptovanje poruke i šalje kriptogram
- Primalac pak koristi svoj tajni ključ za dekriptovanje kriptograma i čita poruku
- Svako može slati kriptovane poruke primaocu, ali samo primalac može da ih čita (jer jedino on zna svoj tajni ključ)
- Primarna prednost kriptografije sa javnim ključem jeste rešavanje problema distribucije ključeva
- Mana – složeniji algoritmi, duže računarsko vreme obrade

55

Sigurnost kriptovanog algoritma

- Vreme potrebno za "razbijanje" algoritma mora da bude
  - duže od vremena u kome podaci moraju da ostanu tajni.
- Takođe, potrebno je da bude zadovoljen i uslov da
  - broj podataka šifrovanih jednim ključem bude manji od broja potrebnih podataka da se dati algoritam "razbije".

56

Preuzimanje i instaliranje javnog ključa

- Postoji nekoliko načina da se preuzme javni i privatni ključ
- Web lokacija Verisign (http://verisign.com) omogućava da se preuzme probni skup (važi 60 dana) javnih i privatnih ključeva ili da se kupe ključevi za šifru
- U uputstvima o preuzimanju koja se prime sa VeriSigna navode se koraci koji se moraju slediti da bi se koristili ključevi
- Pored toga, sa Web lokacije M.I.T na http://web.mit.edu/network/pgp.html može se preuzeti besplatan softver za korišćenje **PGP (Pretty Good Privacy)** šifrovanje
- Obe navedene Web lokacije nude uputstva koja vode kroz korake za slanje i primanje šifrovanih poruka

57

Pronalaženje korisnikovog javnog ključa

- Nakon što primite svoj javni ključ, možete ga poslati prijateljima preko elektronske poruke – oni će ga koristiti za šifrovanje poruka koje vam šalju
- Pored toga, svoj javni ključ možete postaviti u spisak javnih ključeva na Webu – kada korisnik kojem niste poslali svoj javni ključ treba da šifruje poruku da bi vam je poslao, on može da pronađe ključ na serverima sa javnim ključevima
- Naredna slika prikazuje server sa javnim ključevima na MIT-u na kome možete potražiti korisnikov javni ključ

58

Server sa javnim ključevima

Primena kriptografije

Najjednostavnije:

- tajna komunikacija,
- identifikacija,
- autentifikacija i
- razmena tajne

Složenije

- elektronska trgovina,
- sertifikacija,
- tajna elektronska pošta,
- rekonstrukcija ključa i
- bezbedan pristup računarskom sistemu