Bezbednost na Internetu

Softverski praktikum

Institut za matematiku i informatiku

Institut za matematiku i informatiku
Prirodno-matematički fakultet, Kragujevac

Decembar 2010. god.

Bezbednost na Internetu

- skidanje elektronske pošte (e-maila) zaražene zlonamernim softverom koji se obično nalazi u prilogu (attachmentu),
- otvoreni računarski portovi (kao posledica aktiviranja zlonamernog softvera) preko kojih je moguće preuzeti kontrolu nad napadnutim računarom – *Distributed Denial-on-Service* (DDoS),
- poseta sumnjivim sajtovima (koji su obično postavljeni na besplatnim serverima) koji preko Java ili ActiveX apleta ubacuju zlonamerni softver na računar,
- instalacija i startovanje "sumnjivih" programa koji su zaraženi zlonamernim softverom,
- bezbedonosni propusti u programima koji se inače koriste na računaru (operativni sistem, Internet pretraživači, e-mail klijenti i dr.) zbog kojih je neophodno svakodnevno ažuriranje ("skidanje") sigurnosnih dodataka (update-ova),

Bezbednost na Internetu

Nastavak

- korišćenje "zakpra" (crack-ova) koji omogućavaju nelegalno korišćenje softvera,
- mrežna krađa identiteta (*Phising*) koja predstavlja prikupljanje personalnih podataka (korisničko ime, lozinka, broj platne kartice, broj telefona i dr.) od lakovernog korisnika na lažnim web sajtovima,
- preusmeravanje na "lažni" web sajt (*Pharming*) modifikacijom lokalnog DNS servera na računaru koji je prethodno zaražen zlonamernim sofverom,
- neoprezno korišćenje servisa društvenih (socijalnih) mreža – Facebook, Twitter, My Space,...

Zlonamerni softver - *malware*

- Složenica od *malicious+software*
- računarski virus,
- crv (engl. *worms*),
- Trojanski konj ili Trojanac (engl. *trojan horse*),
- *Rootkit*,
- *Backdoor*,
- *Spyware*,
- *Adware*,
- *Phishing*,
- *Pharming*

Računarski virus

- Računarski virus je programski kod koji se ugrađuje u pojedine fajlove aplikativnog ili sistemskog softvera.
- Obično se sastoji iz dva dela od kojih je prvi samokopirajući kod koji omogućava razmnožavanje virusa, a drugi deo, glavni kod ili *payload*, može biti škodljivog ili neškodljivog sadržaja.
- Termin "virus" se svakodnevno koristi i za druge vrste zlonamernog softvera
- Postoje različite tehnike preživljavanja virusa kao što su enkripcija (šifriranje), metamorfizam (preobražavanje) i razmnožavanje
- Polimorfni virusi menjaju svoj kod svaki put kada se repliciraju kako bi izbegli šansu da budu otkriveni od strane antivirusnih sotfvera.

Crv - *Worm*

- Virusi inficiraju domaćine, dok crvi napadaju sisteme.
- Preuzimaju kontrolu nad funkcijama računara koje omogućavaju prenos fajlova i foldera i automatski se kopiraju
- Na primer, crv bi mogao da pošalje kopije samog sebe svim kontaktima iz adresara e-mail klijenta, a zatim bi zaraženi računari uradili to isto, čime se izaziva domino efekat
- Neretko jedini način njihovog uklanjanja sa računara je formatiranje hard diska i ponovna instalacija operativnog sistema

Trojanski konj

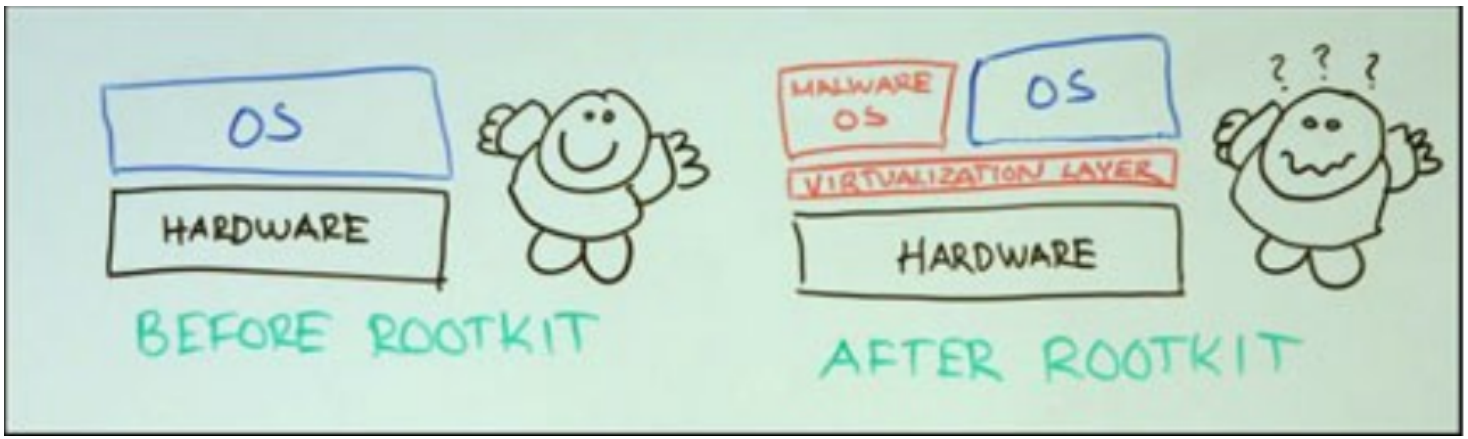
- Savremeni trojanski konji su računarski programi koji deluju kao koristan softver, a zapravo ugrožavaju bezbednost računara
- Najbolji način zaštite od njih podrazumeva izbegavanje preuzimanja softvera iz nepoznatog i nepouzdanog izvora

Operacije koje izvršava trojanac

- prikupljanje i krađa poverljivih informacija – lozinki, bankarskih računa i dr.,
- instalacija softvera (uključujući i druge oblike zlonamernog softvera),
- download, upload, brisanje, kreiranje i modifikacija fajlova,
- pregled radne površine korisnika,
- dodavanje računara u BotNet mrežu (DDoS napad),
- prikupljanje i preuzimanje teksta koji je unet sa tastature (*Keylogging*)
- zauzimanje resursa računarskog sistema i njegovo usporavanje.

Rootkit

- **Rootkit** predstavlja jednu ili skup više programskih alatki, dizajniranih u cilju prikrivenog preuzimanja kontrole nad operativnim sistemom zbog sakrivanja drugih zlonamernih aktivnosti.
- *Rootkit* ne dodeljuje administratorske privilegije korisniku, već omogućava pristup, pokretanje i modifikovanje sistemskih fajlova i procesa



Backdoor i *spyware*

- Backdoor (stražnji ulaz) je program koji instaliraju virusi, crvi ili Trojanci (bez ikakvog znanja korisnika računara) i koji služi za zaobilaženje uobičajene autentifikacije (procesa provere korisnikovih ličnih podataka u toku pokušaja prijavljivanja ili konektovanja) da bi omogućio nesmetan i neovlašćen pristup vlasnika korisnikovom sistemu.
- Adware (od ad – reklamiranje, oglas i ware – programski paket) je bilo koji softverski paket, deo zlonamernog softvera, koji automatski pokreće, prikazuje ili skida reklame na računar posle instalacije ili dok se program koristi.

Phishing i *pharming*

- Obe metode varaju korisnike lažnim web sajtovima (kao da su pravi), tako što se od korisnika traži da unesu personalne podatke.
- *Phishing* - šalju elektronske poruke tako da izgledaju da su došle sa nekog legitimnog web sajta kao što su eBay, PayPal ili neke druge bankarske institucije. U elektronskoj poruci se tvrdi da treba ažurirati lične podatke zbog provere i traži se unos korisničkog imena i lozinke nakon klika na link koji se nalazi u popruci.
- Dok Phishing uzima lične podatke od korisnika upućujući ga na lažni web sajt, *Pharming* preusmerava korisnika na lažni web sajt, a da on toga i nije svestan.
- Jedan od načina da se javi Pharming je preko elektronske pošte zarežene virusom koji poremeti korisnikov lokalni DNS keš.

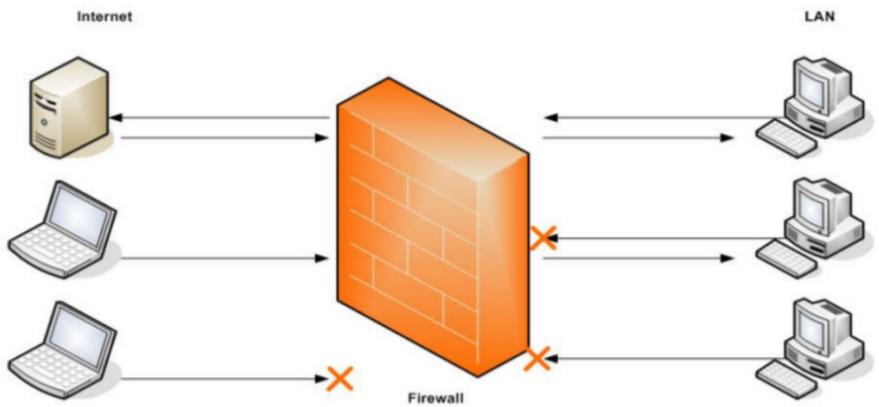
Ostali tipovi zlonamernog softvera

1. *Dialer*
2. *DDoS* (*Distributed Denial-of-Service* – distribuirano odbijanje servisa) je sinfronizovani napad sa više računara koji pokušava da ostavi napadnuti računar bez dostupnih resursa zauzimajući mu Internet protok.
3. Zombi je kompjuter sa pristupom Internetu koji je ugrožen od strane hakera, računarskog virusa ili Trojanca.
4. BotNet je veliki broj zaraženih računara, kolekcija softverskih robota ili botova, koji se pokreću automatski.
5. *Keylogging* je prikriveno i nelegalno praćenje tastera koje je korisnik pritisnuo na tastaturi,
6. Macro virusi imaju sposobnost da se sami kopiraju, brišu ili menjaju dokumente na inficiranom računaru.

Zaštita računara

Zaštitni zid - *firewall*

- Zaštitni zid je hardverski i/ili softverski sistem čija je osnovna namena da računarsku mrežu zaštiti od upada spolja, ali i da spoljašnje mreže zaštiti od eventualnih zlonamernih korisnika sa mreže koja se na ovaj način štiti.
- Dopunski mehanizam zaštite antivirusnom softveru
- Dve vrste: mrežni i personalni *firewall*



Savremeni antivirusni paketi nude:

1. antivirusnu provera fajlova – skenira spoljašnju memoriju kada se aktivira (priključi) i sprečava aktivaciju virusa, čak i kada je već ubačen na računar,
2. antivirusnu provera elektronske pošte – skenira elektronsku poštu na viruse, Trojance i ostali zlonamerni softver,
3. antivirusnu zaštita "surfovanja" – sprečava viruse koji se prenose preko HTTP protokola,
4. proaktivnu zaštita – štiti od nepoznatih pretnji, nadgleda startup selektiranih programa i štiti registar bazu operativnog sistema,
5. softver za blokadu špijunaže – sprečava krađu ličnih podataka kao što su lozinke, brojevi platnih kartica i sl., a sadrži i anti-phishing, pop-up blocker, anti-banner, anti-dialer, itd.,
6. softver za zaštitu od hakerskih napada – sprečava hakerske napade koji mogu da dovedu do krađe ličnih podataka, instaliranja virusa ili korišćenja računara za spam napade,
7. antispam proveru elektronske pošte – automatski sprečava spam poruke i
8. kreiranje sistemskog diska za oporavak sistema (rescue disk) – omogućava oporavak sistema nakon urušavanja izazvanog bilo uticajem zlonamernog softvera ili ne.

Mere zaštite bankovnih portala

1. TAN (*Transaction Authorization Numbers*) kodovi – lozinke za potvrdu samo jedne transakcije,
2. virtuelne tastature,
3. povezivanje klijenata na fiksnu IP adresu,
4. tajna pitanja i ključne reči i
5. korišćenje CD-a i USB fleša sa digitalnim sertifikatom za autorizaciju klijenta.

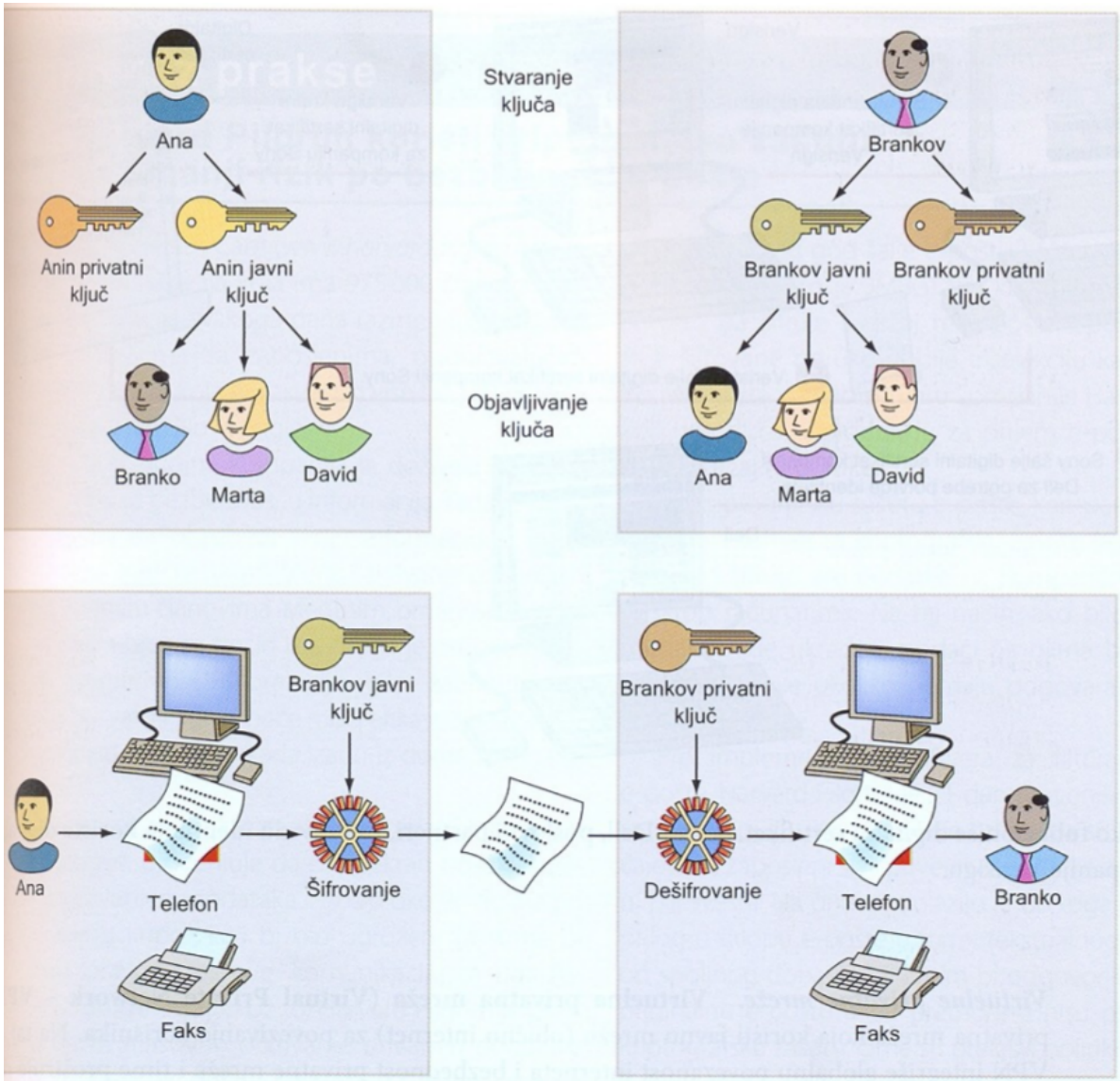
Kriptografija

1. tajnost informacija (sprečavanje otkrivanja njihovog sadržaja),
2. integritet informacija (sprečavanje neovlašćene izmene informacija) i
3. autentičnost informacija (definisanje i proveru identiteta pošiljaoca).

Asimetrično šifrovanje

Asimetrično šifrovanje ili šifrovanje javnim ključem je šifarski sistem u kome svaki učesnik koristi dva ključa – javni i privatni. Javni se može slobodno distribuirati putem elektronske pošte ili web sajta, dok je drugi privatni, i dostupan je samo njegovom vlasniku. To znači da je moguće bilo kome poslati šifrovanu poruku, ako je poznat javni ključ osobe kojoj se šalje, a samo primalac svojim privatnim ključem može da dešifruje poruku.

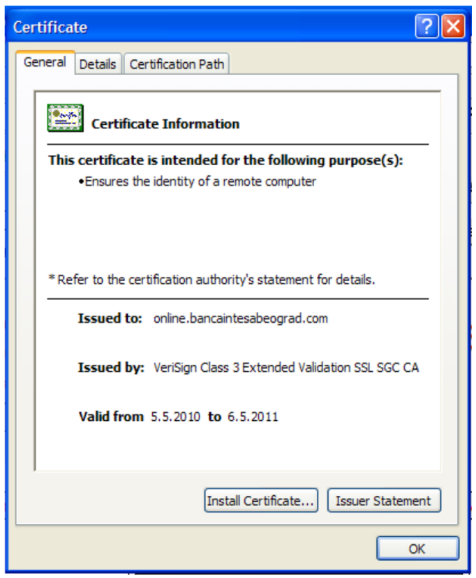
Asimetrično šifrovanje



Asimetrično šifrovanje

Digitalni sertifikati

- Ukoliko primalac poruke nije siguran da poseduje ispravan javni ključ pošiljaoca poruke rešenje problema je sadržano u posedovanju digitalnog sertifikata
- Digitalni sertifikat može izdati samo ovlašćena institucija (CA – *Certificate Authority*) čija je uloga provera i utvrđivanje identiteta.
- Ako korisnik ima poverenja u CA i ima CA javni ključ, može biti siguran u ispravnost sertifikata.



Verzija formata sertifikata (V3)
Serijski broj sertifikata
Identifikator algoritma za potpis sertifikacionog tela
Naziv sertifikacionog tela
Rok validnosti sertifikata
Vlasnik sertifikata
Informacija o javnom ključu vlasnika: Identifikator algoritma / Javni ključ
Polje dodatnih atributa
Digitalni potpis sertifikata

Preventivne mere zaštite

1. kvalitetan i više puta dnevno ažuriran antivirusni program,
2. redovno ažuriranje operativnog sistema sigurnosnim zakrpama (update-ovima),
3. permanentno aktivan zaštitni zid,
4. korišćenje lozinke sa velikim brojem karaktera (kombinacija slova i brojeva) i njene česte promene,
5. izbor pouzdanog Internet pretraživača najnovije verzije podešenim na najviši stepen sigurnosti i
6. po mogućstvu, korišćenje web-mail servisa.