Bezbjednost i zaštita informacionih sistema

1. UVOD

Osnovni pojmovi

Prof. dr Nikola Žarić

e-mail: zaric@ucg.ac.me

Napadi na sigurnost, servisi i mehanizmi

Ubrzani razvoj računarskih mreža, širenje i primjena distribuiranih sistema i komunikacija uticali su na sigurnost sistema kojima se može pristupiti kroz javne mreže.

Generičko ime za skup alata, procedura, polisa i rješenja koji se projektuju da se sistem odbrani od napada naziva se **sigurnost računarskih mreža (Computer Network Security).**

Napadi na sigurnost, servisi i mehanizmi

Da bi se efikasno procijenile sigurnosne potrebe, treba razmotriti sledeće elemente sigurnosti informacija:

- **Sigurnosne napade**: to su akcije koje kompromituju sigurnost informacija

- **Sigurnosne mehanizme**: koji treba da detektuju, preduprijede i oporave sistem od napada na sigurnost

- **Sigurnosne servise**: koji povećavaju sigurnost sistema za obradu i prenos podataka. Sigurnosni servisi najčešće koriste jedan ili više sigurnosnih mehanizama

Sigurnosni napadi i prijetnje

Sigurnosni napadi su akcije usmjerene na sigurnost informacija. Oni se mogu klasifikovati u četiri osnovne kategorije:

1.Presijecanje ili prekidanje (Interruption) je napad na raspoloživost **(availlability)**. Ovim napadom se prekida tok informacija, onemogućava pružanje usluge ili funkcionisanje sistema

2.Hvatanje (Interception) je napad na povjerljivost **(confindentiality)**. Hvatanje se sprovodi kao prisluškivanje, nadziranje ili uvid u osjetljive informacije. Spada u kategoriju pasivnih napada i teško se otkriva jer ne mijenja podatke. Obično služi kao priprema za sledeće napade.

Sigurnosni napadi i prijetnje

3. Izmjene (Modification) predstavljaju napad na integritet (integrity). Spada u kategoriju aktivnih napada.

Ako se odvija na komunikacionom putu prenosa podataka može se ispoljiti kao napad tipa "čovek u sredini" (man in the middle). Unutar računarskih sistema se manifestuju kao izmjena podatka, načina funkcionisanja programa ili prava pristupa itd.

4. Fabrikovanje (fabrication) je napad na autentičnost (authenticity) i sastoji se u generisanju lažnih podataka, lažnog saobaraćaja ili davanju neovlašćenih komandi. Spada u kategoriju aktivnih napada.

Anatomija napada na sigurnost

Da bi se shvatila anatomija napada potrebno je prepozanti osnovne korake i metodologije koje koristi napadač. One se sastoje u sledećim koracima:

1. Ispitivanju i procjeni (Survey and assesment).

Prvi korak je istraživanje potencijalne mete i identifikacija njenih karakteristika. Ove karakteristike mogu biti servisi koji se isporučuju, ili protokoli koji se koriste na ulaznim tačkama sistema.

Na osnovu ovih informacija napadač pravi plan za napad.

Anatomija napada na sigurnost

2. Eksploataciji i prodoru (Exploit and penetrate). Nakon ispitivanja mete slijedi pokušaj eksploatacije slabih tačaka i pokušaj prodora u mrežu/sistem

Ako su mreža i host osigurani sledeća meta napada su **aplikacije**.
Za napadača je najlakše da prodre **ako koristi isti ulaz kao i legalni korisnici**.

3. Povećanju privilegija (Escalate privileges). Nakon što kompromituje aplikacije ili mrežu napadač može ubacivanjem koda u aplikaciju ili kreiranjem autentifikovane sesije na operativnom sistemu da poveća svoje privilegije.

Posebno mu je u interesu da preuzme administratorske privilegije.

Anatomija napada na sigurnost

4. Održavanje pristupa (Maintain access). Kad jednom uspije da pristupi sistemu napadač pokušava da olakša svoje buduće upade. Uobičajeno se koriste programi sa "zadnjim vratima" (back door) ili postojeći nalozi sa slabom zaštitom. Prikrivanje tragova podrazumijeva brisanje log fajlova i skrivanje alata. Log fajlovi su primarni cilj napadača.

5. Odbijanje usluge (Deny services). Napadači koji ne mogu da ostvare pristup sistemu često preduzimaju napad koji pruzrokuje odbijanje usluge (Denial of services). Ova vrsta napada onemogućava legalne korisnike da koriste servise i aplikacije

Najčešći napadi i prijetnje

Računarski sistemi i mreže se mogu napasti na mnoštvo načina. Najčešće korišćene metode su sledeće:

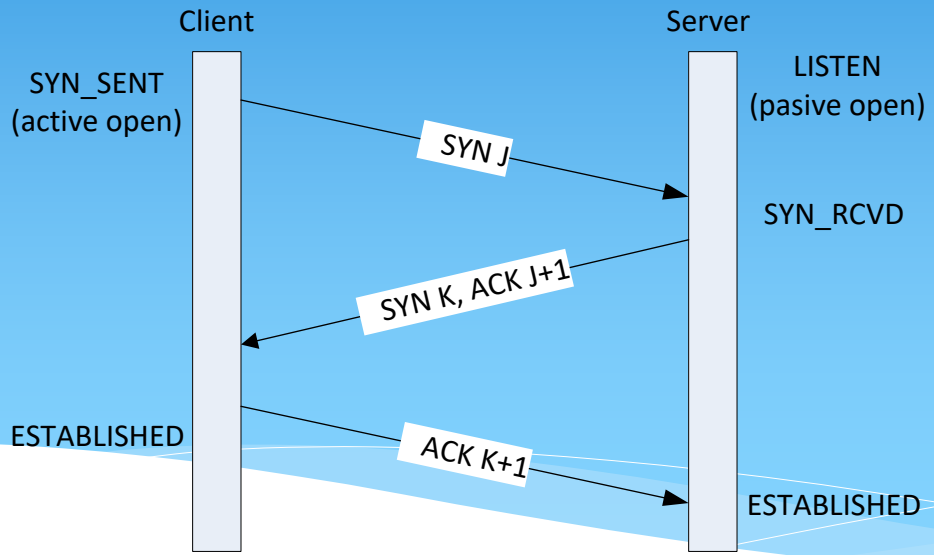
1. Odbijanje usluge (Denial of services) DoS. DoS napad izaziva prekid rada servisa ili programa, čime je drugima onemogućen rad sa njima.

DoS napad se najlakše izvodi na transportnom (četvrtom) sloju slanjem velikog broja sinhronizacionih SYN paketa (TCP CONNECTION REQUEST).

Zaštita se sprovodi kontrolisanjem broja SYN paketa u jedinici vremena.

Najčešći napadi i prijetnje

Procedura uspostavljanja TCP konekcije



Najčešći napadi i prijetnje

2. Lažiranje IP adresa (Spoofing). Napadač prati IP adresu u IP paketima i pritom se predstavlja kao drugi računar.

Kako DNS (Domain Name System) ne provjerava porijeklo informacija napadač izvodi spoofing napad dajući pogrešnu adresu, tj ime računara od povjerenja DNS-u. Dobar način zaštite od ovog napada je sprječavanje rutiranja sa izvorišnim adresama, tj. sprječavanje izlaska paketa iz mreže koji nemaju IP adresu te mreže.

3. Njuškanje (Sniffing). U ovom slučaju napadač specijalnim programom presrijeće TCP/IP pakete i pregleda njihov sadržaj. Ako se kroz mrežu kreću podaci koji nisu šifrovani napadač dolazi do eventualnih povjerljivih informacija.

Najčešći napadi i prijetnje

Posebne metode za izvođenje napada su **programske prijetnje**. U njih se ubrajaju:

1. Trojanski konj, je ilegalni segment kôda podmetnut u kôd programa sa ciljem da promijeni funkcije ili karakteristike originalnog programa.

Specijalna varijanta trojanskog konja je program koji oponaša procedure prijavljivanja na mrežu ili sistem. Program ovoga tipa presrijeće log-in procedure i prikazuje odzivnik na prijavu, identičan pravom odzivniku.

Zatim napadač čeka da korisnik unese korisničko ime i lozinku. Kad to korisnik unese, trojanski konj podatke smiješta u datoteku dostupnu napadaču i obavještava korisnika da je pogrešno unio lozinku

Najčešći napadi i prijetnje

Trojanski konj nakon toga predaje proceduru pravoj proceduri prijavljivanja na sistem. Korisnik smatra da je pogrešno unio lozinku i ponovo se prijavljuje na sistem.

Napadač nakon toga provjerava datoteku i prijavljuje se na sistem pod tuđim imenom.

2. Klopka (trap door). Ukoliko autori programa ostave prazna mjesta u svom kôdu (klopke), napadač koji zna za ta mjesta može da podmetne svoj kod u tom prostoru.

Klopke se teško otkrivaju jer je potrebna cjelokupna analiza sumnjivih programa.

Najčešći napadi i prijetnje

3. Prelivanje bafera (buffer overflow) izvršava se na stek ili heap dijelu memorije. Prelivanje bafera je najčešći napad sa mreže pri pokušaju ne-autorizovanog pristupa. Takođe i autorizovani korisnici mogu izvesti ovu vrstu napada da bi ostvarili veća prava.

Po pravilu napadači koriste greške u programima, odnosno nedovoljnu kontrolu razdvajanja steka, podataka i kôda. Napadač šalje više ulaznih podataka nego što to program očekuje, preplavljuje ulazna polja, argumentne komandne linije ili ulazni bafer da bi došao do steka.
Zatim prepisuje važeću adresu u steku adresom svoga kôda i puni dio steka svojim kôdom koji izvršava neku komandu.

Najčešći napadi i prijetnje

Savremeni oparativni sistemi imaju mehanizme pomoću kojih se mogu kreirati drugi procesi. U takvom okruženju moguće je zlonamjerno korišćenje datoteka i drugih resursa. Ova vrsta prijetnji naziva se **sistemskim prijetnjama.** To su crvi i virusi.

1. Crvi (worms) su samostalni zlonamjerni programi koji se šire sa jednog računara na druge. Uobičajene metode prenosa su putem elektronske pošte ili Interneta.

Crv ekspolatiše ranjiva mjesta žrtve (prekoračenje bafera na primer) ili koristi metode obmanjivanja i prevare i navodi korisnika da ga pokrene.

Najčešći napadi i prijetnje

2.Virusi su fragmenti kôda koji se ubacuju u legitimne programe i zahtijevaju nosioca u vidu izvršne datoteke.

Nakon pokretanja virus se ubacuje i “inficira” i druge izvršne datoteke u okviru sistema.

Virusi su veoma destruktivni i teško se odstranjuju .

Danas virusi predstavljaju jedan od najvećih problema presonalnih računara. Za odstranjivanje virusa je potrebno da se raspolaže “zdravim” kopijama izvršnih datoteka.

Način modeliranja prijetnji

Modeliranje prijetnji treba da bude proces koji se razvija od rane faze dizajniranja aplikacija i treba da traje kroz njihov životni ciklus. On služi prepoznavanju prijetnji i pružanju adekvatnih odgovora.

Razlozi za modeliranje prijetnji su sledeći:
1. Nemoguće je registrovati sve prijetnje u jednoj iteraciji.
2. Aplikacije najčešće nisu statične već se dinamički adaptiraju na nove zahtjeve pa je potrebno pratiti razvoj prijetnji kroz njihovu evoluciju.

Proces modeliranja prijetnji sastoji se od 6 faza i može se primijeniti kako za aplikacije u razvoju tako i za gotove aplikacije.

Način modeliranja prijetnji

1. **Identifikovanje vrijednosti.** U ovoj fazi se identifikuju vrijednosti i utvrđuje šta sistem treba da zaštiti.
2. **Kreiranje pregleda arhitektura.** Korišćenjem dijagrama i tabela stvara se dokumantacija za aplikaciju sa uključivanjem podsistema i tokova podataka.
3. **Dekompozicija aplikacija.** Arhitektura aplikacije se dekomponuje uključujući arhitekturu mreže i hostova da bi se kreirao **sigurnosni profil** aplikacije.

Sigurnosni profil ima namjenu da otkrije slaba mjesta u dizajnu, implemantaciji, instalaciji i konfigurisanju aplikacije

4. **Identifikovanje prijetnji.** Uzimajući u obzir ciljeve napadača i ranjivost aplikacija identifikuju se prijetnje

Način modeliranja prijetnji

5. Dokumentovanje prijetnji. Prijetnje se dokumentuju korišćenjem zajedničkog šablona (template), koji definiše centralni skup atributa kojim se može uhvatiti svaka prijetnja.

6. Procjena prijetnji. Prijetnje se rangiraju po prioritetu kako bi se prvo rješavale najopasnije prijetnje. Proces rangiranja kao kriterijum uzima vjerovatnoću pojavljivanja prijetnje u odnosu na štetu koju može prouzrokovati napad.

Rangiranje može da dovede do zaključka da određene prijetnje ne zahtijevaju bilo kakvu akciju kad se uporedi rizik sa štetom koja može nastati. Kao rezultat modeliranja prijetnji formira se dokument koji pomaže u pronalaženju pristupa u rješavanju problema.