Sadržaj

Taksonomija sigurnosnih napada

Uvod

Internet je postao najbrže rastuci dio globalne mreže. Racunalne tehnologije svakodnevno napreduju i dolazi do razvoja novih tehnologija namijenjenih medusobnoj suradnji i povecanju produktivnosti. Poslovanje velikih i malih kompanija sve više i više ovisi o njihovoj prisutnosti na globalnoj mreži Internet, a u zadnje vrijeme i kucanstva postaju sve ovisnija. Ovakva ovisnost je stvorila plodno tlo za razne oblike zlocudnih i kriminalnih aktivnosti kojima je cilj nanijeti štetu ili ukrasti informaciju. Sigurnosni napadi stvorili su globalnu prijetnju, kako u lokalnim tako i u globalnim mrežama. Napadi postaju sve sofisticiraniji i imaju sposobnost širenja u vremenu od svega nekoliko sekundi. Racunalni sustavi su medusobno povezani kako bi se postigao viši stupanj ucinkovitosti i bolju razmjenu informacija. Broj potencijalnih prijetnji se povecava upravo zbog te povezanosti, dok se mogucnost procjene utjecaja na sustav time znatno otežava jer ne postoji jedinstveno ranjivo mjesto vec više njih (a ponekad nisu sva relevantna mjesta poznata). Uspješan napad sustava na Internetu predstavlja veliku prijetnju jer može utjecati na performanse sustava i na usluge koje koriste milijuni korisnika diljem svijeta. Niz nezavisnih istraživaca utvrdili su kako broj sigurnosnih prijetnji iz godine u godinu sve više i više raste unatoc velikom trudu sigurnosnih organizacija. Nužno je osigurati potrebne alate za otkrivanje, klasificiranje i obranu od razlicitih vrsta napada. Mogucnost klasificiranja ranjivosti i napada predstavlja kljucni korak u izradi strategija za otkrivanje i obranu informacijskih sustava. Razvoj sigurnosnih alata i protumjera koje omogucuju obranu sustava od napada zahtijeva duboko razumijevanje metoda kojima se napadaju sustavi. Sigurnost racunalnih sustava nalaže da racunalni sustav ispunjava svoju ulogu kao što je u svezi zaštite resursa sustava. Stoga je sigurnost racunalnog sustava jedan od najvažnijih aspekata poslovanja organizacija koje svoje poslovanje zasnivaju na racunalnim sustavima. Velik broj pojedinaca i organizacija redovito sakuplja te javno objavljuje informacije vezane za sigurnost racunalnih sustava. Vecina se informacija vezanih za sigurnost racunalnih sustava opcenito ne može uspješno usporedivati i razmjenjivati. Do nedugo je glavna prepreka predstavljala slabo razvijen sveopci jezik (terminologija), no taj problem sve više i više jenjava. Nagli porast interesa za podrucje racunalne sigurnosti potaknuo je razvoj jedinstvene terminologije. U poglavlju Terminologija navedeni su osnovni pojmovi potrebni za klasifikaciju sigurnosnih napada. Svrha tog poglavlja nije razvoj obuhvatnog rjecnika termina korištenih na podrucju sigurnosti racunalnih sustava, vec definiranje važnih termina unutar strukture, indikacijom njihovog medusobnog odnosa, a koji bi bio korišten za klasifikaciju i razumijevanje informacija o sigurnosnim incidentima racunalnih sustava. Veci problem danas predstavlja opcenito slabo mogucnost snalaženje i prepoznavanja relevantog sadržaja u obilju informacija na podrucju informacijske sigurnosti. Kako bi se smanjila kolicina vremena potrebnog za pronalaženje informacija

sve se cešce koriste taksonomije. Poglavlje Potreba za taksonomijom sigurnosnih napada daje pregled zašto su taksonomije korisne te koje su prednosti njihova korištenja. Cilj je istaknuti potrebu za strukturiranjem velike kolicine znanja na podrucju sigurnosti kako bi bilo jednostavnije pocetnicima ali i strucnjacima dolaziti do novih spoznaja. Klasifikacija je proces korištenja terminologije za razdjeljivanje i uredenje sveukupnog znanja odredenog podrucja istraživanja. To je shema koja razdjeljuje sveukupno znanje na odredenom podrucju te definira medusobne odnose pojedinih dijelova. Univerzalni model klasifikacije sigurnosti ne postoji, ali postoje razne taksonomije koje pomažu u klasificiranju znanja za uporabu u raznim segmentima podrucja (kao što su izrada alata, predvidanje/sprecavanje upada i drugo). Kroz poglavlje Pregled postojecih taksonomija sigurnosnih prijetnji analiziraju se postojece taksonomije s ciljem uocavanja zajednickih svojstava postojecih taksonomija te njihove primjene. Zajednicko svojstvo taksonomija je utjecaj na razne sigurnosne zahtjeve mreža, usluga i aplikacija. Osnovni sigurnosni zahtjevi mogu se svrstati u sljedece osnovne skupine:

- **Autentifikacija** (engl. *Authentication*) – potvrda autenticnosti korisnika. Odgovarajuce metode provjere autenticnosti korisnika primjenjuju se ovisno o aplikaciji i uslugama koje ih koriste.
- **Cjelovitost** (engl. *Integrity*) – garancija da su informacije poslane, primljene ili pohranjene i izvornom i nepromijenjenom obliku. Samo ovlaštenim osobama dopušteno je upisivanje, promjena, promjena statusa, brisanje, stvaranje, kašnjenje ili ponavljanje podataka.
- **Povjerljivost** (engl. *Confidentiality*) – zaštita komunikacije ili pohranjenih informacija od presretanja i stavljanja na uvid neovlaštenim osobama.
- **Neporicanje** (engl. *Nonrepudiation*) – sudionici ne mogu odbiti ili poreci akciju u kojoj su sudjelovali, npr. slanje i primanje informacija.
- **Kontrola pristupa** (engl. *access control*) – ogranicavanje pristupa informacijama i ogranicavanje provodenja akcija.
- **Raspoloživost** (engl. *Availability*) – informacije moraju biti raspoložive, a sustavi i usluge u stanju operativnosti, usprkos mogucim neocekivanim i nepredvidljivim dogadajima, primjerice nestanku struje, prirodnim nepogodama, nesrecama i zlonamjernim napadima.

Taksonomija

Cilj ovog rada je predložiti taksonomiju koja ce na jasan i jednostavan nacin prikazati najbitnije svojstva sigurnosnih napada. U nastavku se razmatraju svojstva dobre taksonomije kao i detaljan opis predložene taksonomije.

Kriteriji za taksonomiju

Prije nego što se predloži nova taksonomija sigurnosnih napada potrebno je definirati kriterije za taksonomiju. Kriteriji taksonomije sastoje se od skupa zahtjeva sastavljenih iz razlicitih izvora koje je Daniel Lowry Lough sumirao u svojoj doktorskoj disertaciji [1]. Lough navodi kako taksonomija mora biti:

- **Prihvacena** (Amoroso, 1994.; Howard, 1997.): taksonomiju je potrebno strukturirati na nacin koji ce olakšati njezinu opcenitu prihvacenost.
- **Razumljiva** (Lindqvist i Jonsson, 1997.): razumljivu taksonomiju ce moci koristiti strucnjaci iz podrucja, ali i oni koji imaju interes za to podrucje.
- **Cjelovita** (Amoroso, 1994.) / Iscrpna (Howard, 1997.; Lindqvist i Jonsson, 1997.): da bi

taksonomija bila cjelovita treba pokriti sve moguce napade i pružiti odgovarajuce kategorije. Iako je teško dokazati cjelovitost taksonomije, moguce ju je opravdati kroz uspješnu kategorizaciju stvarnih napada.
- **Deterministicka** (Krsul, 1998.): postupak razvrstavanja mora biti jasno definiran.
- **Medusobno iskljuciva** (Howard, 1997; Lindqvist i Jonsson, 1997.): medusobno iskljuciva taksonomija ce svaki napad kategorizirati u najviše jednu kategoriju.
- **Ponovljiva** (Howard, 1997; Krsul, 1998): postupak klasifikacije bi se trebao moci ponoviti.
- **Uskladena sa utvrdenom sigurnosnom terminologijom** (Lindqvist i Jonsson, 1997): taksonomiju treba oblikovati korištenjem postojeceg nazivlja kako bi se izbjegle zabune i dvosmislenost.
- **Jednoznacna** (Howard, 1997; Lindqvist i Jonsson, 1997): svaka kategorija taksonomije mora biti jasno definirana tako da nema dvosmislenosti u klasifikaciji napada.
- **Korisna** (Howard, 1997; Lindqvist i Jonsson, 1997): taksonomija je korisna ukoliko se može koristiti u sigurnosnoj industriji, a posebice u razrješavanju sigurnosnih incidenata.

Ovisno o ciljevima, taksonomija ne mora nužno zadovoljiti sve navedene kriterije. Svi kriteriji predstavljaju korisna svojstva taksonomije ali nisu svi potrebni. Na primjer, neke taksonomije nisu medusobno iskljucive.

Definicija pogleda taksonomije

Predložena taksonomija sigurnosnih napada strukturirana je kroz razlicite poglede. Svaki pogled pobliže opisuje napad, odnosno omogucuje njegovo klasificiranje. Osnovni pogledi su:

- Svrha napada
- Meta napada
- Metoda napada
- Ranjivost koja se iskorištava u napadu

Svrha napada

Ovim pogledom se identificira svrha napada. Svrha racunalnog napada predstavlja namjeru, težnju koju napadac pokušava ostvariti ugrožavajuci ili narušavajuci sigurnost ciljnog racunalnog sustava. Najcešci uzroci napada su:

- **Dobivanje (krada) informacija** – narušavanje povjerljivosti informacija. Legitimni korisnici nisu sprijeceni u korištenju sustava, a ne moraju nužno saznati da su povjerljivi podaci dostavljeni neovlaštenim osobama.
- **Korupcija informacija** – neovlaštena izmjena podataka na racunalnom sustavu kojom se narušava cjelovitost resursa sustava. Posljedica za legitimne korisnike sustava su nemogucnost korištenja resursima sustava ili korištenje neispravnim podacima
- **Krada racunalnih resursa** – neovlašteno korištenje resursa racunalnog sustava bez osjetne degradacije raspoloživosti resursa legitimnim korisnicima.
- **Uskracivanje usluga ili resursa** – degradacija ili blokiranje resursa racunalnog sustava. Korist za napadaca ostvarena racunalnim napadom je sprjecavanje legitimnih korisnika u korištenju sustava.
- **Narušavanje ugleda žrtve** – kombinacija uskracivanja usluga, deformacija web sjedišta i drugih radnji kojima je cilj stvoriti dojam nekompetentnosti žrtve, najcešce organizacije.

- **Povecanje pristupa** – neovlašteno ostvarenje ili povecanje razine pristupa resursima racunalnog sustava.

Meta napada

Ovaj pogled identificira metu napada. Odnosno, koji element sustava ce osjetiti štetnu posljedicu napada. Mete, ciljeve racunalnih napada možemo podijeliti na logicke i fizicke. Logicki ciljevi sastoje se od tri entiteta – racun, proces i podaci. Fizicki ciljevi se sastoje od komponenata, racunalnih uredaja i mreže. Primjeri mogucih meta sigurnosnih napada su:

- **Covjek** – fizicka osoba, korisnik ili vlasnik racunalnog sustava.
- **Racun** – domena korisnickog pristupa na racunalo ili mrežu koji je pod kontrolom prema zapisniku informacija koji sadrži ime korisnickog racuna, zaporku i korisnicka ogranicenja.
- **Proces** – osnovni program u izvodenju. Sastoji se od izvršnog programa, programskih podataka i programskog stoga te svih drugih informacija potrebnih za izvršavanje programa.
- **Komponenta** – jedan od dijelova koji cine racunalo ili mrežu.
- **Racunalni uredaj** – sastoji se od jedne ili više udruženih komponenta, ukljucujuci jedinice za procesiranje i periferne jedinice koje su pod kontrolom upravljackog programa.
- **Mreža** – grupa medusobno povezanih racunala, elemenata za preusmjeravanje i ogranaka za medusobno povezivanje.

Metoda napada

Ovaj pogled identificira nacin na koji se ostvaruje svrha napada. Neke od metoda napada su:

- Prevara ili socijalni inženjering (engl. Social Engineering) – predstavlja tehniku racunalnih napada kojom napadaci ostvaruju neovlašteni pristup osjetljivim informacijama ili privilegijama, a koja je zasnovana na izgradnji neprikladnog i povjerljivog odnosa s legitimnim korisnikom sustava. Ljudi su obicno najslabija veza u sigurnosnom lancu, a socijalni inženjering najefikasnija metoda stjecanja osjetljivih informacija .
- Prisluškivanje – tehnikom prisluškivanja prometa napadaci su u mogucnosti ostvariti pristup ispravnim zaporkama koje se koriste, na primjer, za Internet pristup ili prijavu za rad na udaljenom racunalu. Ovaj proces je jednostavan ukoliko se zaporke prenose korištenjem protokola koji ne kriptiraju podatke, nego se zaporke prenose u obliku cistog teksta (engl. clear text).
- Napadi lažnim predstavljanjem – tehnike racunalnih napada lažnim predstavljanjem obuhvaca racunalne napada zasnovane na sigurnosnim propustima TCP/IP protokola. TCP/IP protokol koji je danas vrlo korišten sadrži velik broj ozbiljnih sigurnosnih propusta, bez obzira na nacin implementacije. Buduci da su racunalni napadi ove tehnike po sebi fundamentalni za TCP/IP protokol, bilo koji sustav koji pruža ili se koristi mrežnim servisima zasnovanim na TCP/IP protokolu, potencijalna su meta ovih napada. Više o propustima u TCP/IP protokolu može se naci u dodatnoj literaturi pod [18].
- Iskorištavanje slabosti – podrazumijeva iskorištavanje posebne skupine ranjivosti koje se nazivaju slabosti. Ova skupina je vrlo slicna ranjivostima, opcenito se mogu razlikovati time da za ranjivosti uvijek postoji rješenje a za slabosti ne. Opci primjeri elemenata sigurnosti koji trpe od ove skupine ranjivosti su kriptografija, sigurnost zaporki, zastarjela sklopovlja i programska potpora, korisnici sustava.
- Pogadanje – tehnika pogadanja zaporki obuhvaca ucestalo unošenje cesto korištenih zaporki, rucno ili automatizirano koristeci skripte. Vecina korisnika koristi jednostavne zaporke ne

poštivajuci sigurnosne preporuke. Iako u praksi napadacima nije potrebno mnogo vremena da bi pogodili zaporku, tehnika pogadanja zaporki obicno je neefikasna zbog glasnoce cijelog procesa. Naime, u vremenu kojem je potrebno za pogadanje zaporke, administratori sustava na jednostavan nacin mogu prepoznavanja i sprijeciti napad.
- Gruba sila (engl. Brute-Force) – opce rješenje za pogadanje zaporke nabrajanjem svih mogucih kombinacija znakova i provjeru svake od njih. U teoriji se svi moderni kriptosustavi (i racunalni sustavi) mogu razbiti ovom metodom. No, u praksi je znatno teže izvesti uspješan napad ove vrste. Korištenjem složenih zaporki povecava se prostor pretraživanja što dovodi do mnogo mogucih kombinacija koje cesto nije moguce u konacnom vremenu proizvesti. Dodatno, dodavanjem ogranicenja na broj mogucih pokušaja i korištenjem dodatnih polja za provjeru legitimnosti korisnika (npr. Captcha images) onemogucuje se ovaj napad na aktivnoj žrtvi.

Ranjivost koja se iskorištava u napadu

Ovim pogledom se identificira ranjivost koja je omogucila izvodenje napada na sustavu. Napadaci moraju iskoristiti prednosti koje im pruža ranjivost racunalnog sustava kako bi ostvarili svoje ciljeve. Neke ranjivosti koje je moguce iskoristiti su:

- Greška u dizajnu – ranjivost sustava uzrokovana dizajnom ili specifikacijom sklopovske opreme ili programske podrške, pored koje i savršena implementacija rezultira ranjivošcu sustava.
- Greška u implementaciji – ranjivost sustava uzrokovana je pogreškom napravljenoj pri implementaciji željenog dizajna u kojem nema pogrešaka ili ranjivosti.
- Konfiguracija – ranjivost sustava uzrokovana pogreškom u konfiguraciji sustava. Na primjer, racuni sustava s osnovnim (engl. default) zaporkama, loše postavljene zabrane za pristup datotekama i drugo.
- Ljudska slabost – ranjivost uzrokovana ljudskom nepažnjom ili neznanjem.