Sadržaj

1. Naslovnica
2. Potreba za taksonomijom sigurnosnih napada
3. Terminologija
4. Pregled postojecih taksonomija sigurnosnih prijetnji
5. Taksonomija sigurnosnih napada
6. Klasifikacija sigurnosnih napada

Pregled postojećih taksonomija sigurnosnih prijetnji

Na području mrežne i računalne sigurnosti postoji određen broj taksonomija pomoću kojih je moguće razvrstati sigurnosne prijetnje. U ovom poglavlju se spominju neke poznatije taksonomije sigurnosnih prijetnji.

Kjaerland

Kjaerland u svom radu [1] predlaže taksonomiju napada temeljenu na zabilježenim slučajevima CERT-ove (engl. Computer Emergency Response Team) biblioteke. Rad je povezan sa profiliranjem računalnih zločina (engl. computer crime profiling), a ističe zloćudne korisnike i žrtve. U ovom radu napadi su analizirani uz pomoć teorije aspekata (engl. facet theory) i višedimenzionalnog skaliranja (MDS – multidimensional scaling) a osi su: žrtva napada, izvor, utjecaj i način rada. Svaki aspekt sadrži određen broj elemenata sa opisom. Aspekti se koriste za usporedbu komercijalnih i državnih sigurnosnih incidenata. Cilj taksonomije je razumijevanje napadačevih motiva i pokušaj kvantificiranja mjesta i razloga napada. Ova taksonomija je ograničena jer se problem razmatra sa visoke razine apstrakcije i time se ne daje konkretan odgovor o tome koje metode koristiti u prepoznavanju napada.

Hansman i Hunt

Hansman i Hunt u svom radu [2] predlažu taksonomiju sa četiri jedinstvene dimenzije koje pružaju potpunu klasifikaciju koja pokriva napade računala i mreža. Njihova taksonomija pruža pomoć za poboljšanje računalne i mrežne sigurnosti ali i konzistentnost u definiciji napada. Taksonomija se sastoji od sljedeće četiri dimenzije:

- Prva dimenzija – vektori napada
- Druga dimenzija – meta napada
- Treća dimenzija – ranjivost koja se identificira sa CVE brojem ili sa vlastiti opisom ako ne postoji unos u CVE-u
- Četvrta dimenzija – ističe korisni teret (engl. payload) ili popratne učinke

Unutar svake dimenzije daje se različita razina informacija za opis ranjivosti. Hansman spominje

potrebu za budućim radovima koji bi poboljšali klasifikaciju miješanih napada, što je nedostatak njihove taksonomije. Drugi nedostatak je manjak informacija o ranjivostima što sprječava skupljanje informacija koje su potrebne za poboljšanje zaštite sustava.

Mirkovic i Reihner

Mirkovic i Reihner su u svom radu [3] su ponudili opsežnu taksonomiju DDoS napada i načina obrane. Ovaj rad ističe značajku strategija napada. Točnije, strategija napada je ključna u primjeni protumjera. Taksonomija kategorizira napade po:

- Razini automatizacije (engl. Degree of Automation)
- Ranjivosti koja se iskorištava (engl. Exploited Weakness)
- Valjanost izvorne adrese (engl. Source Address Validity)
- Mogućnost karakterizacije (engl. Possibility of Characterization)
- Skup upornih agenata (engl. Persistent Agent Set)
- Tip žrtve (engl. Victim Type)
- Utjecaj na žrtvu (engl. Impact on Victim)

Lough

Lough u svom radu [4] predlaže taksonomiju temeljenu na analizi napada, a nosi naziv VERDICT (engl. Validation Exposure Randomness Deallocation Improper Conditions Taxonomy). Taksonomija je oblikovana analizirajući četiri glavne sigurnosne propuste:

- Nedovoljna provjera (engl. Improper Validation)
- Neispravno izlaganje (engl. Improper Exposure)
- Nedovoljna razina slučajnosti (engl. improper Randomness)
- Neispravno odlaganje (engl. Improper Deallocation)

Prilikom opisivanja ranjivosti koristi se jedan ili više propusta. Hansman i Hunt kritiziraju Lough-ovu taksonomiju zbog nedostatka relevantnih informacija koje bi bile korisne tijelima kao što su CERT za klasificiranje novih napada i izdavanje preporuka. Dodatno, taksonomija ne podržava klasifikaciju virusa, crva, trojanskih konja i sličnih zlođudnih programa.

Howard

Howard u svom radu [5] pruža taksonomiju incidenata koja klasificira napade prema događajima koji ciljanu metu tjeraju da promijeni svoje stanje. Događaj uključuje akciju i metu. Taksonomija ističe sve korake koje čine napad. Svaki napad se prema Howardu sastoji od 5 koraka: alat, ranjivost, akcija, meta i rezultat. Iako ova taksonomija pruža informativnu osnovu za računalne ranjivosti nedostaje joj pojedinosti potrebne za temeljit uvid u napad.

Neumanna i Parkera

Među empirijskim pristupima klasifikacije sigurnosnih napada ističe se rad Neumanna i Parkera [6]. U tom radu oblikovan je popis kategorija pod nazivom „Taksonomija Empirijskog popisa“ (engl. Empirical List Taxonomy). Kategorije taksonomije empirijskog popisa imaju neke nedostatke, primjerice, kategorija zlouporabe kroz nedjelovanje (engl. abuse through inaction) u većini slučajeva se ne može smatrati kao napad jer nepažljiv administrator može uzrokovati problem na samo u sigurnosti nego i u većini drugih aspekata sustava. Dodatno, loše upravljanje sustavom nije pokušaj neovlaštenog pristupa ili korištenja resursa što pokazuje da ovaj pristup ne može jasno razlučiti između sigurnosnih prijetnji i bilo koje druge vrste kvarova. Osim toga, taksonomija empirijskog popisa ima preklapanja između klasa. Na primjer, u procesu pretvaranja (engl. masquerading) može se koristiti metoda zaobilaženja autentifikacije ili autorizacije što dovodi do preklapanja dviju kategorija.

Landwehr

Taksonomija bazirana na trodimenzionalnoj matrici koju uvodi Landwehr [7] precizira tri faze u životnom ciklusu sustava u kojim je moguće uvesti sigurnosni propust. To su faze razvoja, održavanja i rada. Razvojna faza uključuje sve sustavne procese od specifikacije zahtjeva do implementacije sustava. Faza održavanja uključuje sve aktivnosti koje sustavu omogućuju prilagodbu, izmjenu i poboljšanje performansi nakon prvog puštanja u pogon. Konačno, faza rada uključuje prilagodbu i unošenje bilo kakvih propusta za vrijeme rada sustava. Postoji očito preklapanje između faze održavanja i faze rada, ali unatoč tome su dovoljno različite da ih se može koristiti za izradu protumjera za sigurnosne zahtjeve.

Bishop

Bishop je donio nekoliko važnih doprinosa na području sigurnosnih taksonomija. U svom radu [8] 1995. godine predstavlja taksonomiju sigurnosnih ranjivost Unix sustava u kojemu koristi klasifikacijsku shemu „šest osi” (engl. Six axes model). U nastavku si navedene Bishopove osi:

- Priroda – prirodi nedostatak se opisuje koristeći kategorije za analizu i zaštitu (engl. Protection Analysis categories)
- Vrijeme uvođenja – vrijeme kad je ranjivost uvedena u sustav
- Domena iskorištavanja – što se dobiva iskorištavanjem ranjivosti
- Domena utjecaja – na što se može utjecati iskorištavanjem ranjivosti
- Minimalni broj – minimalni broj komponenata potrebnih za iskorištavanje ranjivosti
- Izvor – izvor identifikacije ranjivosti

Bishopov pristup odudara od do sada spomenutih taksonomija. Umjesto hijerarhijskih ili ravnih taksonomija, Bishopova taksonomija koristi osi. Taksonomija koja se predlaže u ovom radu također koristi sličan koncept za kategoriziranje ranjivosti, poglede. Bishop i Bailey u [9] izvode analizu drugih sigurnosnih taksonomija. Također, istražuju se pitanja koja okružuju taksonomije a posebno ono što čini dobru taksonomiju. Bishop sugerira da je jedna od glavnih prednosti taksonomija njezina potpora u upravljanju resursima.

Usporedba taksonomija

Taksonomija	Primjena	Nedostatak
Kjaerlan	Profiliranje zloćudnih korisnika	Ne pruža konkretan odgovor o tome koje metode koristiti u prepoznavanju napada
Hassman i Hunt	Klasifikacija mrežna i računalna prijetnji	Ne podržava klasifikaciju miješanih napada, manjak informacije o ranjivostima
Mirkovic i Reihner	Klasifikacija DDoS napada	Ograničena samo na DdoS napade
Lough	-	Ne podržava klasifikaciju zloćudnih programa (cvri, virusi...), nedostatka relevantnih informacija za izdavanje preporuka
Howard	Klasifikacija događaja	Taksonomija ne pruža dovoljno detalja za dublje razumijevanje napada
Neumann i Parker	-	Preklapanje kategorija
Landwehr	Klasifikacija ranjivosti u fazi razvoja	Preklapanja kategorija

Reference

1. Kjaerland, M., A taxonomy and comparison of computer security incidents from the commercial and government sectors, Computer and Security, 2005.Kjaerland
2. Hansman S., Hunt R., A taxonomy of network and computer attacks. Computer and Security, 2005. Hansman i Hunt
3. Mirkovic, J., Reiher, P., A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, ACM CCR, 2004. Mirkovic i Reiher
4. Lough DL. A taxonomy of computer attacks with applications to wireless networks. Doktorska disertacija, Virginia Polytechnic Institute and State University. 2001. Lough
5. Howard J., Longstaff T., A Common Language for Computer Security Incidents, Sandia National Laboratories, 1998. Howard i Longstaff
6. Neumann P., Parker D., Summary of Computer Misuse Techniques, Processing of the 12th National Computer Security Conference, 1989. Neumann i Parker
7. Landwehr, Carl E., Bull, Alan R., McDermott, John P., Choi, William S., A Taxonomy of Computer Program Security Flaws, with Examples. ACM Computing Surveys, 1994. Landwehr
8. Bishop M., A taxonomy of (Unix) system and network vulnerabilities, Department of Computer Science, University of California at Davis; 1995. Bishop
9. Bishop M, Bailey D., A critical analysis of vulnerability taxonomies, 1996. Bishop i Bailey