Reputácia sieťových entít v kontexte manažmentu bezpečnostných informácií a udalostí

Judita Jusková

3Ib, 2016 - 2017

Abstrakt. Škodlivý kód, malware alebo spam, ktorý je vykonávaný na počítačoch môže poskytnúť širokú škálu útokov na dostupnosť siete alebo napadnutia súkromia a dôvernosti užívateľov. V tejto práci sme sa zamerali na sumarizáciu známych sieťových entít a meraní reputačného skóre, ktoré vyjadruje stupeň ohrozenia z jednotlivých IP adries. Taktiež porovnávanie prístupov k tvorbe reputácií sieťových entít.

Kľúčové slová: reputácia IP, reputácia DNS, reputácia sieťových entít

1 Úvod

V dnešnej dobe si sieťoví operátori čoraz častejšie vyžadujú monitorovanie ich siete. Je to hlavne kvôli správnemu zabezpečeniu takejto siete. Na monitorovanie sú rozmiestnené rôzne detektory škodlivých a nevyžiadaných prístupov. Takéto systémy môžu pomôcť včas varovať pred nebezpečnými udalosťami.

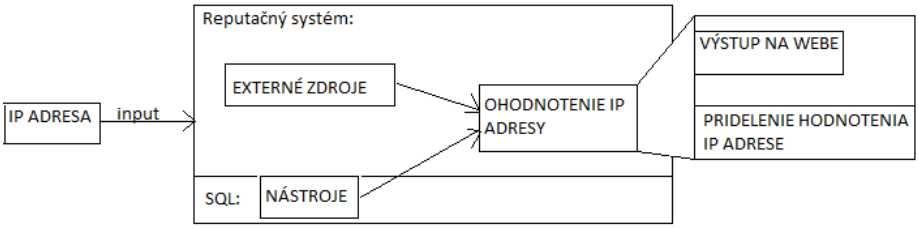
Detektory nemusia byť len v jednej lokálnej sieti, informácie môžu medzi sebou zdieľať viacero organizácii. Záznamy sa takto môžu niekoľko násobne zväčšiť a tým napomáhať upresňovaniu škodlivých činností. Zo záznamov sa môžu získavať zaujímavé vlastnosti škodlivých prevádzok. Následné získané odhadovanie miery hrozby, tzv. *povestné skóre* [3].

Sieťová bezpečnosť sa týka zabezpečenia sieti a sieťových zariadení. Rieši aj poskytovanie nepretržitej služby pre oprávnených užívateľov. S tým súvisí aj zabezpečenie proti rôznym sieťovým útokom. V dnešnej dobe sa na internete pohybuje veľa užívateľov a s nimi aj IP adries. Niektoré IP adresy sú bezpečné, iné naopak menej bezpečné. Takýmto škodlivým IP adresám je najlepšie sa vyvarovať. Na internete vzniká mnoho blacklistov, ktoré majú riešiť tento problém. Prospešné pre človeka, majú byť v tom, že sa v nich môže dopátrať k zlým, škodlivým IP adresám, ktoré boli už v minulosti označené, že sú nevhodné.

V práci sme najprv analyzovali postupne takéto blacklisty a reputačné systémy, ktoré sa snažia informovať užívateľov o škodlivých IP adresách a tak zabezpečovať siete. Zamerali sme sa na takúto reputáciu a snažili sme sa vytvoriť systém. K tomuto systému by mal prístup hocikto, kto by potreboval zistiť informácie o rôznych IP adresách. V práci hľadáme kompletné informácie o IP adresách. Nie len aké hodnotenie/ povesť Vaša IP adresa na internete má, ale aj geografické súradnice

danej adresy, polohu, zoznam blacklistov, v ktorých sa adresa nachádza, celkov počet, koľko krát sa IP adresa v blacklistoch nachádza, atď..

1.1 Ilustračný príklad



Obrázok 1. Návrh reputačného systému

Vo všeobecnosti platí, že reputačný systém pristupuje k dátam z rôznych dátových zdrojov, kde posudzuje charakter IP adresy. V závislosti od nájdenia zhody zo záznamov z minulosti, sa zvyšuje váha priradenia hodnotenia k danej IP adrese. Na obrázku 1. môžeme vidieť koncepčný model, znázorňujúci faktory, ktoré napomáhajú pri vytváraní reputačného skóre pre danú IP adresu. Na vytváranie reputačného systému budú potrebné externé zdroje, ako je znázornené na obrázku 1.. Externým zdrojom sa môže nazývať napríklad blacklist, ktorý je voľne dostupný na internete. Ďalším dôležitým faktorom pri tvorbe reputačného systému sú nástroje, ktoré budú obohacovať systém o funkcionalitu. Výstupom budú kompletné informácie o IP adrese, reputačné skóre IP adresy.

1.2 Prehľad súčasného stavu

- Systéme NOTOS v práci [5] je novo vytvorený systém, ktorý mal ako prvý určovať dynamicky reputačný systém DNS. Skúmali jednotlivé názvy domén. Snažili sa vytvoriť up-to-date DNS informácie o vhodných ale aj nežiadúcich doménových menách. Využíva združovanie algoritmov modelovania siete a zón správania vhodných a nežiadúcich domén. Tieto algoritmy používajú na výpočet reputačného skóre pre doménu.

- V práci [2] sa snažia povedať o zdanlivo odlišných útokoch ako podobné sú. Teda čo ich spája. Následne analyzujú či takéto útoky nie sú z rovnakých lokálnych sieti. Ak sú, vytvárajú sa časti siete, o ktorých môžeme povedať, že je pravdepodobný útok. V práci [4] sa nadväzuje na túto, tým, že skúmajú agregácie takýchto štvrtí. Skúmajú ako pravdepodobné je, že každá IP adresa z takéhoto rozsahu je nežiadúca a snaží sa o útok.

Hlavné ciele práce možno zosumarizovať do nasledovných bodov:

(1) Analyzovať reputácie sieťových entít v manažmente bezpečnostných informácií a udalostí
(2) Analyzovať a porovnať prístupy k tvorbe reputácií sieťových entít.
(3) Navrhnúť a implementovať reputačný systém pre manažment bezpečnostných informácií a udalostí.

2 Návrh riešenia

Základným stavebným kameňom nášho reputačného systému sú dáta, ktoré sa získavajú zo starších už nameraných záznamov. Dáta sú čerpané z našej fakulty, teda Prírodovedecká fakulta UPJŠ.

2.1 Navrhovaný prístup:

Základná vec pri navrhovaní prístupu je formálna definícia významu reputácie, reputačného systému a reputačného skóre. Ako uviedli v práci [3] slovo "reputácia" definuje spoločnú mienku, ktorú majú subjekty o objektoch. Je založená na spoločnom zdieľaní názorov o objekte, skúsenosti s nimi a doterajšom správaním sa objektu, resp. subjektu. Reputačné skóre je definované ako pravdepodobnosť, že subjekt bude vykonávať škodlivú činnosť v blízkej budúcnosti, na základe jeho správania v minulosti.

Reputačné skóre je založené na predpokladoch budúcich útokov. Preto je vhodné definovať prístup k predikcii.

Vstupom do algoritmu predikcie bude súhrn všetkých škodlivých udalostí za určité uplynulé obdobie. Môže byť dopĺňané rôznymi ďalšími vstupmi ako štatistika o možno riziku. V našej práci to budú rôzne vstupy ako krajina, mesto, systém, ktorý zisťuje či je uvedená IP adresa na niektorých zoznamoch blacklistov, či má statický alebo dynamicky priradenú IP adresu.

2.2 Ďalšie problémy

2.2.1 Časový rozsah zozbieraných dát

Jedným z problémov pri reputácií je časový úsek zozbieraných dát. Je potrebné si správne určiť veľkosť dát, ktorú chceme analyzovať aby ich nebolo veľa ale na druhej strane aby výsledok nebol skreslený nedostatkom dát a teda nepresného výsledného skóre.

2.2.2 Najdôležitejšie informácie

Aký druh škodlivej aktivity nás bude v práci zaujímať. Keďže informácií môže byť veľa, je nutné vybrať si najdôležitejšie informácie, ktoré nás budu zaujímať najviac.

2.2.3 Druhy útokov

Na ktoré útoky sa budeme zameriavať? Je nutné si presne špecifikovať útoky, pretože sa môže stať, že IP adresa je skúmaná na jeden druh útoku, ktorý nikdy nevykonávala. Preto môže byť jeho povestné skóre veľmi dobré no pritom môže škodiť v inom druhu útoku, ktorý my nezaznamenávame.

2.2.4 Staré informácie

Ak je IP adresa označená ako zlá, škodlivá, znamená to, že bola pravdepodobne súčasťou botnetu ale inak prítomna pri útoku. Teda bola zaznamenaná v zozname blacklistu. Následné tejto IP adrese bolo pridelené zlé hodnotenie. Avšak s pribúdajúcim časom od posledného útoku sa skóre IP adresy nezmenilo a stále má nízke hodnotenie. Daná IP adresa mohla byť za takýto čas pridelená aj inému počítaču, ktorý nevykonával žiadne útoky a má neprávom pridelené zlé hodnotenie.

Takto môže reputačný systém nadobudnúť určitú mieru neistoty ku všetkým údajom. Je ťažké určiť, ako sa IP adresy presne menia. Môže to závisieť aj na rôznych aspektoch, napríklad či ide o IP adresu ktorá je pridelená staticky alebo adresu, ktorá je pridelená dynamicky.

2.2.5 Neistota v informáciách

Už v predchádzajúcom bode sme sa dozvedeli problém s neistotou v dátach. Reputačný proces hodnotenia môže byť nepresný, nespoľahlivý alebo inak neistý ak sa nedodržia a neurčia presne definície.

2.2.6 Mapovanie IP adresy

Hlavným cieľom reputačnej databázy je získavať vedomosti o nebezpečnom hostiteľovi lenže nás systém pracuj s IP adresami nie s konkrétnymi hostiteľmi. Avšak sledovanie individuálnych hostiteľov je praktický nemožné, pretože sa môže jednať o zasahovanie do súkromia hostiteľa. Preto je lepšie rozpoznávať aspoň dynamické rozsahy adries a NAT. Tým aj upraviť ich bodovanie.

3 Predbežné výsledky

Začali sme s analýzou dát na jednotlivých príkladoch IP adries, ktoré sú nám zatiaľ k dispozícií. Dáta boli získané z honeypotov, z našej univerzity (Prírodovedeckej fakulty UPJŠ). A zisťovali zatiaľ „ručne“ informácie o IP adrese. Týmto sme si vytvorili akoby prototyp ako by mal systém vyzerať. Získavali sme informácie o blacklistoch, v ktorých sa jednotlivé IP adresy nachádzali. Koľkokrát bola spomenutá IP adresa v jednom blackliste a taktiež aj analyzovali rôzne útoky, ktoré boli zaznamenané. Je to hlavne kvôli tomu aby sme vedeli aké útoky máme zahrnúť do našej práce. Ďalšie informácie, ktoré sme zozbierali o IP adrese sú geografické súradnice, štát, mesto. V prípade veľkých miest aj oblasť. Na IP adresu sme aplikovali aj program, ktorý nám zistil, ktoré porty na konkrétnej IP adrese sú momentálne otvorené. Taktiež akým spôsobom sa prideľovala IP adresa, či dynamicky alebo staticky.

4 Potrebné technológie

V práci využívame rôzne technológie. Na programovanie v systéme používame programovací jazyk Python. Keďže získané informácie je potrebné

niekam ukladať, rozhodli sme sa pre SQL databázu. Ako výstup budú informácie na webovej stránke, na ktorú budeme používať framework Bootstrap. Vytvorenie stánky sa bude realizovať cez javascript. V práci tiež využívame skenovanie otvorených portov, na prácu s portami nám bude slúžiť Nmap.

5 Záver

V práci sme začali s analyzovaním externých zdrojov. Aké externé zdroje by sme mohli v našom systéme použiť. Následne sme skúmali konkrétne IP adresy v týchto vybratých externých zdrojoch. Skúmali sme v ktorých blacklistoch sa nachádzajú a aké najčastejšie útoky boli realizované. Tiež aj otvorené porty IP adresy a geografické údaje o IP adrese. Momentálne sa pracuje na základoch systému. Taktiež na analýze prístupov. V najbližšej budúcnosti nás čaká vytvorenie databázy na ukladanie informácií o IP adrese, implementácia systému a testovanie IP adries.

Poďakovanie Týmto by som chcela poďakovať vedúcemu svojej práce RNDr. JUDr. Pavlovi Sokolovi za trpezlivosť, cenné pripomienky a obetavosť počas tvorby bakalárskej práce.

Literatúra

(1) JACOBS, Jay; RUDIS, Bob. Data-Driven Security: Analysis, Visualization and Dashboards. John Wiley & Sons, 2014.
(2) MOURA, Giovane César. Internet bad neighborhoods. Giovane Cesar Moreira Moura, 2013.
(3) BARTOŠ, Václav; KOŘENEK, Jan. Evaluating Reputation of Internet Entities. In: IFIP International Conference on Autonomous Infrastructure, Management and Security. Springer International Publishing, 2016. p. 132-136.
(4) MOURA, Giovane CM, et al. Internet bad neighborhoods aggregation. In: 2012 IEEE Network Operations and Management Symposium. IEEE, 2012. p. 343-350.
(5) ANTONAKAKIS, Manos, et al. Building a Dynamic Reputation System for DNS. In: *USENIX security symposium*. 2010. p. 273-290.