Analýza zpětně rozptýleného DDoS provozu v datech o síťových tocích

Martin Marušiak, Martin Žádník
Fakulta informačních technologií VUT v Brně

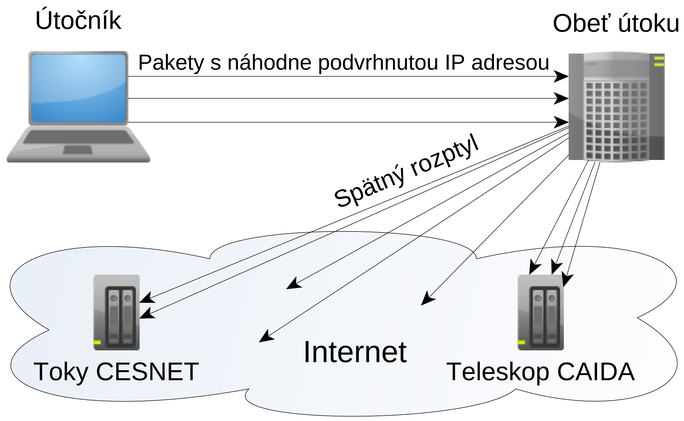
Úvod

Útoky odopretia služby (*DoS*) a ich distribuované varianty (*DDoS*) sú dnes už bežným spôsobom akým útočníci znemožňujú prístup užívateľom k službám na internete a preto je potrebné sa nimi zaoberať a skúmať ich. Na realizovanie tohto typu útoku je často použitá metóda zahltenia (*flooding*), kedy dochádza k zaslaniu obrovského množstva požiadavkov na server služby, čo môže spôsobiť vyčerpanie prenosových, výpočtových či pamäťových zdrojov servera. Takto zahltený server potom nedokáže obslúžiť požiadavky legitímnych užívateľov. Metóda zahltenia je navyše často kombinovaná s metódou podvrhnutia IP adries, kedy útočníci zmenia svoju IP adresu v útočných paketoch, pričom táto IP adresa je zvolená typicky náhodne. Náhodným podvrhnutím IP adries útočníci docielia svoje utajenie a taktiež tým sťažujú proces potlačenia (mitigáciu) útoku. Vedľajším efektom náhodného podvrhnutia IP adries v útočných paketoch je vznik tzv. spätného rozptylu. Jedná sa o komunikáciu vzniknutú reakciou obete na útočný paket, kedy obeť zasiela odpoveď na podvrhnutú IP adresu. Na základe týchto odpovedí od obete (spätného rozptylu) je potom možné detegovať prebiehajúci DDoS útok a to mimo adresového rozsahu kde útok prebieha. Spätný rozptyl teda umožňuje detegovať DDoS útoky kdekoľvek na internete, čo vyplýva z náhodnej povahy podvrhnutia IP adries.

Cieľ práce

Na detekciu DDoS útokov skrz spätný rozptyl sa používajú veľké nevyužité adresové priestory v literatúre označované pod pojmom sieťové teleskopy. V prostredí teleskopu je identifikácia DDoS útokov pomerne priamočiara a to preto, že sa tam nenachádzajú žiadne aktívne zariadenia. Vytvorenie vlastného teleskopu je však náročné pretože vyžaduje veľký adresový priestor a ten je stále obtiažnejšie získateľný vzhľadom na nedostatok dostupných IPv4 adries. Cieľom tejto práce je preto vytvoriť metódu, ktorá bude schopná použiť spätný rozptyl na detekciu DDoS útokov aj v sieťach kde sú prítomne legitímne zariadenia a komunikácia je výrazne rozmanitejšia ako v prostredí teleskopu. Metóda navrhnutá v tejto práci navyše využíva len dáta v abstrahovanej forme v podobe sieťových tokov (*NetFlow*), čo zároveň umožňuje použitie metódy v sieťach s vysokým objemom dát.

Riešenie



Obr. 1: Princíp anotácie dátovej sady na základe súčasného výskytu.

Na riešenie problému detekcie DDoS útokov bolo vzhľadom na vyššiu rozmanitosť komunikácie oproti teleskopu uplatnené strojového učenie s učiteľom. Dôležitú rolu preto zohrávala tvorba a anotácia dátovej sady. Dáta pre túto prácu boli poskytnuté organizáciou CESNET, ktorej adresový rozsah pokrýva skoro milión IP adries. Celkovo bolo zachytených 5 dní komunikácie vstupujúcej a vystupujúcej do tejto siete v podobe tokov, čo predstavuje viac ako 1 TB dát. Tieto dáta boli ďalej redukované rôznymi heuristikami tak, aby obsahovali len dáta relevantné pre detekciu spätného rozptylu. Zvyšné dáta boli následne združené do väčších logických celkov – udalostí, pričom jedna udalosť odpovedá jednému potencionálnemu DDoS útoku. Počas tvorby udalostí boli zároveň ku každej udalosti priradené rysy (*features*) štatistického charakteru. Jedným z rysov bol napríklad počet rôznych IP adries, s ktorými napadnutá služba komunikovala. Udalosti boli potom anotované do dvoch kategórii, podľa toho či sa skutočne jednalo o útok alebo nie. Anotácia bola vykonaná na základe časovej korelácie medzi dátami CESNETu a teleskopu organizácie CAIDA, ktorý obsahuje viac ako 16 miliónov IP adries. Princíp anotácie zobrazuje obrázok 1, ak je útok pozorovateľný v dátach CESNETu, potom by mal byť pozorovateľný na teleskope, kde je jeho identifikácia pomerne jednoduchá.

Celkovo bolo v dátovej sade 7 217 udalostí v triede DDoS a 14 545 mimo túto triedu pre protokol TCP, respektíve 7 004 udalostí v triede DDoS a 44 503 mimo túto triedu pre protokol ICMP. Pre oba protokoly boli následné vytvorené modely pomocou strojového učenia rozlišujúce dané triedy. Pre každý z protokolov bol vytvorený model osobitne nakoľko sa udalosti pre dané protokoly líšili v počte rysov.

Výsledky

Dátová sada bola rozdelená na tri časti: trénovaciu, validačnú a testovaciu. Trénovacia a validačná sada boli použité na nájdenie vhodného typu strojového učenia s pomocou mriežkového vyhľadávania (*grid search*). Ako najvhodnejšia z overených metód sa ukázala metóda *Gradient Boosting*. Výsledky tejto metódy na testovacej sade zobrazuje tab. 1 v podobe metrík citlivosti (*recall*) a presnosti (*precision*), nakoľko sú tieto metriky vhodné aj v prípade nevyváženej dátovej sady, pričom citlivosť vyjadruje pomer medzi počtom správne klasifikovaných útokov voči všetkým útokom v sade a presnosť vyjadruje pomer medzi počtom správne určených útokov a počtom udalostí klasifikovaných modelom ako útok. Uvedená tabuľka ďalej zobrazuje vzťah týchto metrík voči zvolenému klasifikačnému prahu, ktorý je nastaviteľný a čím vyšší je tento prah, tým je väčšia presnosť a teda menej falošne pozitívnych prípadov klasifikácie, ale klesá citlivosť.

Rozhodovací prah	TCP Presnosť	TCP Citlivosť	ICMP Presnosť	ICMP Citlivosť
0,50	95,4	96,1	94,6	97,9
0,70	96,7	95,0	95,2	96,9
0,90	97,7	92,9	95,6	95,4
0,99	98,4	85,0	97,0	91,4

Tab. 1: Vyhodnotenie natrénovaného modelu.

Aplikácia a použité technológie

Táto práca vznikla v rámci spolupráce s organizáciou CESNET, kde je metóda nasadená ako súčasť systému NEMEA. DDoS útoky, ktoré metóda deteguje sú zasielané do európskeho projektu monitorovania bezpečnostných incidentov SPARTA.

Metóda je implementovaná vo forme dvoch modulov vytvorených v prostredí otvoreného frameworku NEMEA vyvíjaného organizáciou CESNET. Prvý modul zabezpečuje tvorbu udalostí z prúdových dát tokov a je za účelom vyššej efektivity implementovaný v jazyku `C++`. Druhý modul klasifikuje udalosti zaslané od prvého modulu do DDoS triedy a za týmto účelom používa prostriedky strojového učenia a práce s dátami dostupného v jazyku `Python`, akými sú napríklad knižnice `sklearn` a `pandas`.