IDENTITY DETECTION IN TCP/IP ARCHITECTURE

Martin Holkovič
Bachelor Degree Programme (3), FIT BUT
E-mail: xholko00@stud.fit.vutbr.cz

Supervised by: Libor Polčák
E-mail: ipolcak@fit.vutbr.cz

Abstract: This work describes a passive monitoring tool for detection of IPv6 addresses used in the network. Since stateless address autoconfiguration allows locally generated IPv6 addresses, there is not a central device that controls address assignments. This work also describes analysis of behaviour of various operating systems. The method was implemented in a tool, which was successfully tested in real network.

Keywords: Dynamical network identity, Neighbor Discovery, SLAAC, lawful interception.

1 ÚVOD

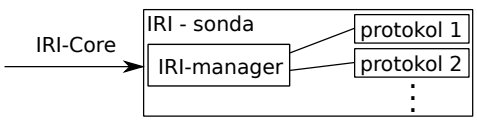
Jedným z problémov, ktoré je nutné v počítačových sieťach riešiť je dynamická identita užívateľov v rámci siete. Jedná sa o problém kedy užívatelia pri práci v sieti využívajú viacero identifikátorov, pričom sa veľa z nich môže meniť napr. pri každom prístupe do siete. Používanie identifikátorov nemusí nepodliehať žiadnej centrálnej správe čo problém ešte viac komplikuje.

Mať informácie o priradených identifikátoroch je nutné pre viacero oblastí ako napr. správa a zabezpečenie siete. Bohužial sú siete taktiež používané aj na nezákonné aktivity. Orgány činné v trestnom konaní chcú o týchto aktivitách byť informovaný a preto využívajú systémy pre zákonné odpočúvanie (LIS), ktoré sú v krajinách EU vytvárané podľa standardu ETSI [1]. Jedna zo súčastí definovaných v štandarde ETSI je blok pre pasívne sledovanie identity užívateľov v sieti (Intercept Related Information Internal Interception Function - IRI-IIF). Mojou úlohou je vytvorenie modulu pre konkrétny systém pre zákonné odpočúvanie.

2 SYSTÉM PRE ZÁKONNÉ ODPOČÚVANIE

V rámci projektu Sec6Net je vyvíjaný systém pre zákonné odpočúvanie s názvom SLIS. Vzhľadom k tomu, že existuje veľké množstvo používaných protokolov s odlišným spôsobom používania identity, je vhodné k tomu prispôsobiť štruktúru bloku IRI-IIF.

Blok IRI-IIF sa skladá z IRI-Core a niekoľko sond. IRI-Core je ústredná časť IRI-IIF, ktorá komunikuje s jednotlivými sondami. Každá sonda môže obsahovať viacero modulov (obrázok č.1) a správcu týchto modulov (IRI-Manager), pričom každý modul sa stará o rozpoznávanie identity užívateľa v inom sieťovom protokole. Pre zjednodušenie pridávania podpory ďalších protokolov je podpora protokolov implementovaná modulárne [2]. Táto práca sa zameriava modulom pre rozpoznávanie IPv6 adries používaných v sieti.



Obrázok 1: Vnútorná štruktúra IRI-IIF v projekte Sec6Net.

3 NEIGHBOR DISCOVERY

Protokol Neighbor Discovery (ND) [3] slúži na preklad IPv6 adries na MAC adresy, vyhľadanie smerovača v lokálnej sieti a ohlásenie smerovača v lokálnej sieti. Protokol sa nachádza na sieťovej vrstve architektúry TCP/IP, pričom pre svoju činnosť využíva niektoré správy protokolu ICMPv6.

Protokol ND pomocou svojich správ definuje mechanizmus Duplicate Address Detection (DAD). Mechanizmus DAD slúži na overenie unikátnosti IPv6 adresy v rámci lokálnej siete predtým, ako bude adresa ľubovoľným spôsobom priradená. Príkladom je statické nastavenie IPv6 adresy. Po zadaní príkazu na zariadení si zariadenie najprv overí, či danú IPv6 adresu nepoužíva iné zariadenie v sieti. Ak dotazovanú adresu nikto nepoužíva, adresa sa môže začať používať. Ďalšie možnosti priraďovania IPv6 adries na zariadeniach je pomocou protokolov DHCPv6 a SLAAC.

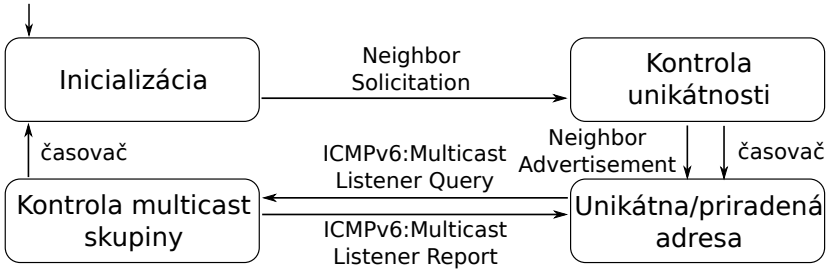
Protokol SLAAC slúži na distribúciu sieťového prefixu v lokálnej sieti, pričom si koncové stanice sami z tohto prefixu vytvárajú IPv6 adresy. Protokol k svojej činnosti využíva správy protokolu ND. Pomocu správ vyhľadanie a oznámenie smerovača získa zariadenie IPv6 prefix. Následne si ľubovoľným spôsobom z prefixu odvodí spodnú časť IPv6 adresy (napr. náhodne) a pomocou mechanizmu DAD si overí unikátnosť tejto adresy.

4 ANALYZOVANIE PROTOKOLU NEIGHBOR DISCOVERY

Mojou úlohou bolo analyzovať dve podmnožiny protokolu ND, protokol SLAAC a DAD. Cieľom bolo zistiť či bežne používané operačné systémy na koncových staniciach implementovali uvedené protokoly podľa normy. Zároveň vzhľadom k tomu, že protokol SLAAC nedefinuje mechanizmus na oznámenie o ukončenia používania IPv6 adresy, bolo nutné sa zamyslieť ako tento problém vyriešiť.

Výsledkom testovania 20 operačných systémov bolo, že všetky systémy podporujú protokol SLAAC a správne sa zachovajú pri detegovaní duplicitnej adresy protokolom DAD (duplikovanú adresu nepoužijú). Norma RFC 4862 však určuje aj poradie činností pri použití protokolu SLAAC: vytvorenie IPv6 adresy, prihlásenie do multicastovej skupiny a kontrola unikátnosti adresy, čo už všetky systémy nedodržiavali. Niektoré systémy sa totiž prihlasujú do multicastovej skupiny až po kontrole unikátnosti adresy, či sa opakovane prihlasovali a odhlasovali z multicastovej skupiny. Spoliehaním sa tak na normu by neviedlo k maximálnej úspešnosti modulu.

Ďalším výsledkom testovania operačných systémov bolo zistenie možnosti detekcie ukončenia používania adries. Smerovače v pravidelných intervaloch rozosielajú správy, v ktorých sa klientov dotazujú na ich členstvo v multicastových skupinách (funkcia MLD querier). V prípade ak operačný systém adresu stále používa, tak je stále prihlásený v multicastovej skupine a tým pádom odpovie na dotaz smerovača. Na základe toho môže modul danú IPv6 adresu stále považovať za priradenú (používanú). V opačnom prípade modul deteguje koniec používania IPv6 adresy.



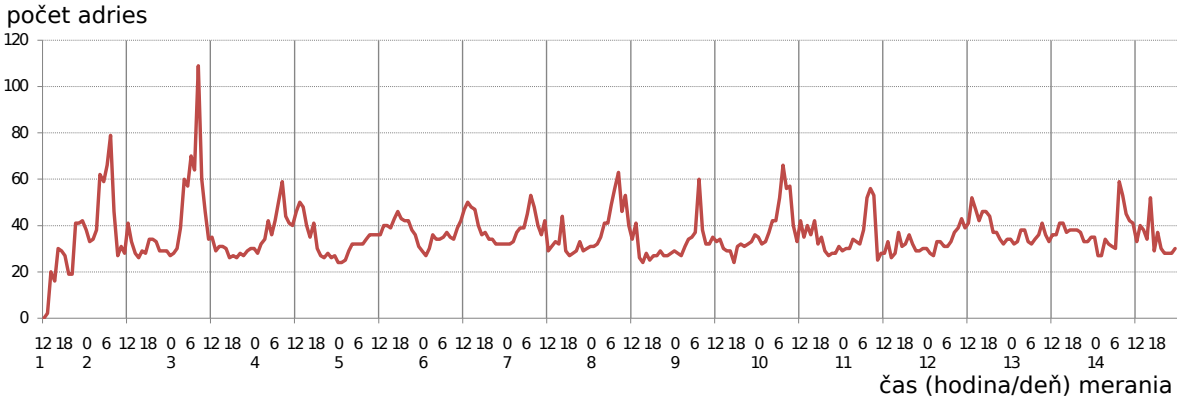
Obrázok 2: Diagram chovania modulu pre protokol ND.

Zlúčením oboch výsledkov analýzy bol vytvorený diagram chovania (obrázok č.2) modulu pre protokol ND, ktorý sa aplikuje na každú IPv6 adresu zvlášť. Diagram bol následne implementovaný

v programovacom jazyku Python a integrovaný do IRI-IIF. Naimplementovaný modul spĺňa požiadavku noriem, aby sa modul správal pasívne a negeneroval žiadne pakety do siete.

5 TESTOVANIE VYTVORENÉHO MODULU

Modul pre detekovanie protokolu ND bol následne otestovaný na malej počítačovej sieti vytvorenej v laboratórnych podmienkach a na produkčnej sieti v jednej z fakultných podsietí. Cieľom týchto testov bolo overenie či po zapojení známeho zariadenia do siete sme schopný zistiť, akú adresu bude používať. Po úspešnom otestovaní sa začalo dlhodobé testovanie modulu, pričom počet adries používaných v sieti počas prvých 14 dní testovania je zobrazený na obrázku č.3.



Obrázok 3: Počet detegovaných adries počas 14-dňového testovania.

6 ZÁVER

Na základe analýzy chovania rôznych OS som vytvoril modul pre zisťovanie IPv6 adries používaných v sieti. Nástroj bol úspešne otestovaný v laboratórnych podmienkach a na produkčnej sieti. V súčasnosti je modul nasadený na jednej z fakultných podsietí, ktorá pokrýva niekoľko budov a prebieha dlhodobé testovanie.

Okrem modulu pre protokol ND som pre účely projektu Sec6Net vytvoril modul pre PPPoE protokol, ktorý bol otestovaný v laboratórnych podmienkach. Aktuálne mám rozpracované moduly pre protokoly SMTP a SIP.

POĎAKOVANIE

Tato práca je súčasťou projektu VG20102015022 podporovaného MVČR. Tento príspevok vznikol za podpory grantu FIT-S-11-1 a výskumného zámeru MSM 0021630528.

REFERENCIE

[1] European Telecommunications Standards Institute: ETSI TR 102 528: Lawful Interception (LI); Interception domain Architecture for IP networks. 10 2006, version 1.1.1.

[2] Martínek, T., Kramoliš, P., Holkovič, M., Polčák, L.: Dynamická identifikace uživatelů v prostředí sítí IPv4 a IPv6, FIT-TR-2012-006, Brno, CZ, FIT VUT, 2012, p. 31

[3] Narten, T., Nordmark, E., Simpson, W., and Soliman, H. (2007b). Neighbor Discovery for IP version 6 (IPv6). RFC 4861 (Draft Standard). Updated by RFC 5942