Příloha A: Podrobný přehled výstupů projektu MV SEC6NET

Název projektu: **Moderní prostředky pro boj s kybernetickou kriminalitou na Internetu nové generace (SEC6NET)**

Kód projektu: **VG20102015022**

Příjemce: **Vysoké učení technické v Brně**

Seznam hlavních výsledků projektu

1 Prototyp systému pro sběr a uchování dat na lokální síti dle vyhlášky č.450/2005 Sb. pro komunikaci protokolem IPv6
2 Prototyp vysokorychlostní sondy pro monitorování IPv6 provozu
3 Prototyp mikrosondy sondy pro monitorování IPv6 provozu
4 Softwarový nástroj pro dohledání pachatele počítačové kriminality
5 Softwarový nástroj pro monitorování a kontrolu komunikace řídících a pomocných protokolů IPv6
6 Nástroj pro síťovou forenzní analýzu NetFox Detective
7 Akcelerovaný nástroj pro obnovu hesel dokumentů Wrathion
8 Paketový filtr pro síťový provoz s rychlostí 100 Gb/s

1. Prototyp systému pro sběr a uchování dat na lokální síti dle vyhlášky č.450/2005 Sb. pro komunikaci protokolem IPv6

Popis výsledku

Prototyp systému pro sběr a uchování dat na lokální síti zajišťuje uchování a zpřístupnění provozních a lokalizačních údajů v sítích IPv4 a IPv6. Realizace prototypu vychází z mezinárodních norem ETSI s nezbytnými modifikacemi pro funkční realizaci a monitorování v prostředí protokolu IPv6. Systém byl vytvořen s ohledem na vyhlášku 357/2012 Sb. o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.

Prototyp DR systému využívá platformy Flowmon a opensource nástrojů pro dlouhodobé uchování dat o komunikaci uživatele a jeho identitě. Implementace systému kopíruje jeho návrh, prezentovaný v publikaci GRÉGR Matěj, PODERMAŃSKI Tomáš, ŠOLTÉS Miroslav a ŽÁDNÍK Martin. Design of Data Retention System in IPv6 network. FIT-TR-2011-07, Brno: Fakulta informačních technologií VUT v Brně, 2011.

Informace o prototypu

Pro získání všech potřebných údajů k identifikaci uživatele a k uchovávání uživatelovy komunikace je třeba získat celou řadu informací. Získání těchto potřebných informací závisí na topologii sítě, používaných síťových zařízeních aj. Prototyp ukazuje možný způsob řešení nad kampusovou infrastrukturou sítě VUT. Jako síťová zařízení se v síti VUT používají primárně prvky od společnosti HP, ale je podporována většina ostatních výrobců.

Díky tomu, že každý poskytovatel Internetu má síť postavenou rozdílným způsobem, je prototyp navržen jako modulární řešení a využívá primárně svobodný software. Díky tomu ho lze provozovat na celé řadě

různých topologií s rozdílnými výrobci. Pokud bude zájemce provozovat systém na vlastní infrastruktuře a serverech, požadavky jsou následující:

- exportér a kolektor NetFlow. Kolektor musí podporovat binární formát souboru, který používá např. nfdump
- systém NAV nakonfigurovaný na sběr informací z hlavních přepínačů/směrovačů
- skript Skript_ipmac společně s nftool umožňující doplnit adresy MAC do dat NetFlow

Pro prezentaci dat slouží webové rozhraní, k dispozici v práci „SALAČ Radek. Interaktivní webové rozhraní pro zobrazení ip flow dat, Brno, 2015“, případně lze data zobrazit nástrojem nfdump.

NetFlow

Prototyp je postaven nad platformou Flowmon, která slouží pro získání základních dat NetFlow. Pro ukládání dat slouží interní kolektor, v nastavení prototypu lze ale data NetFlow přesměrovat na jiný, externí kolektor. Podporován je open source kolektor nfdump. Data NetFlow jsou následně doplněna o adresy MAC z přepínačů/směrovačů v síti. Pokud uživatel používá přechodové mechanismy, jsou v datech NetFlow uloženy informace o vnitřní, tunelované komunikaci.

IP - MAC

Pro získání vazby mezi adresou IP/IPv6 a adresou MAC slouží open source systém NAV. Tento systém je vhodné z výkonnostních důvodů provozovat odděleně, není tedy přímo součástí prototypu. Systém NAV slouží k získání neighbor cache a arp cache z přepínačů pomocí protokolu SNMP. Systém NAV je třeba nakonfigurovat na základě topologie sítě, kde má být prototyp nasazen. U prototypu systému, běžícím na VUT je k dispozici skript, který zmíněné tabulky nezískává skrz SNMP ale protokolem SSH a zpracováním výstupu z konzole jednotlivých zařízení. Toto řešení je provozováno zejména z výkonnostních důvodů. Údaje jsou následně doplněny do dat NetFlow pomocí skriptu ipmac Skript_ipmac.

Demonstrace funkčnosti

Prezentace dat

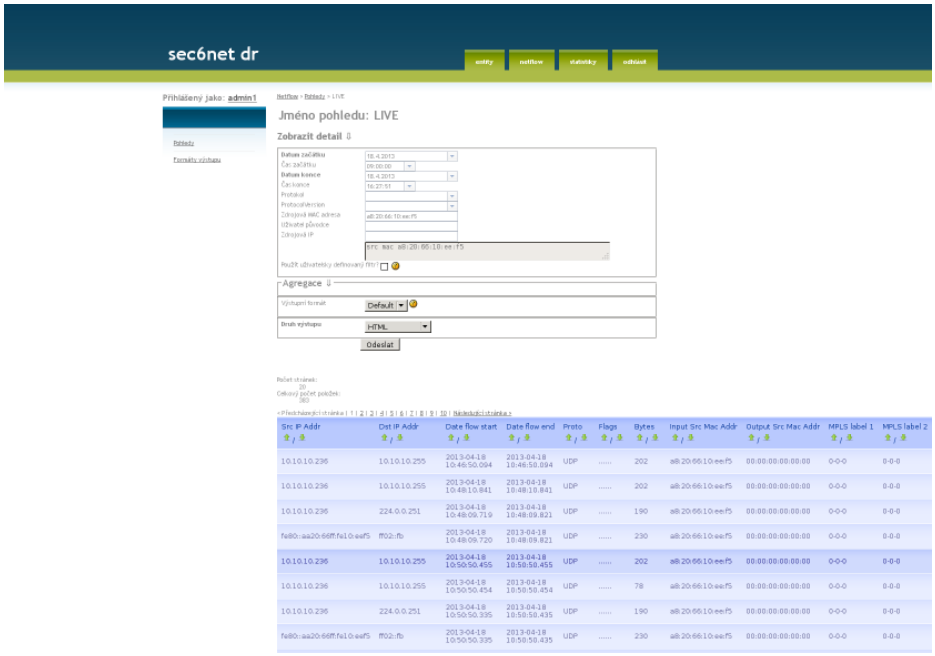
Formát prezentace dat NetFlow, rozšířený o všechny další nutné informace potřebně k dohledání uživatele je popsána v práci Salač Radek, Ing.: Interaktivní webové rozhraní pro zobrazení ip flow dat, Brno, 2015.

Instalace

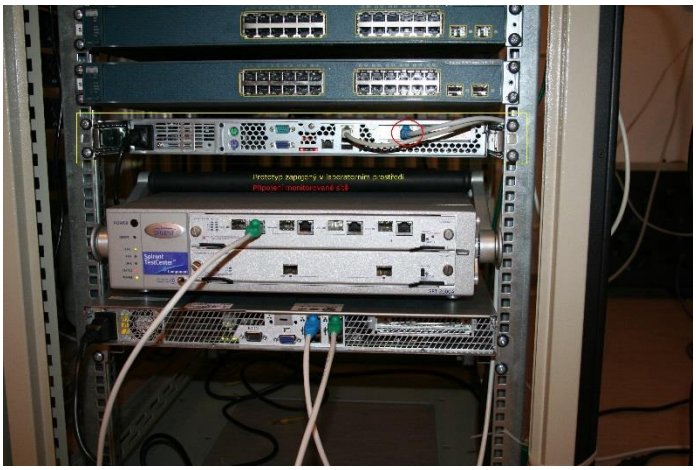
K dispozici je prototyp, kde jsou nainstalována všechna potřebná rozšíření a skripty. Je třeba nakonfigurovat skript ipmac aby se dokázal připojit k serveru NAV, kde se ukládá vazba mezi IP/IPv6 a adresou MAC a časové údaje, kdy byla daná adresa použita. Na webovém rozhraní daného prototypu je k dispozici přístup k jednotlivým datům NetFlow pomocí nástroje pro prezentaci dat. Prototyp je k dispozici v laboratoři C304 na FIT VUT.

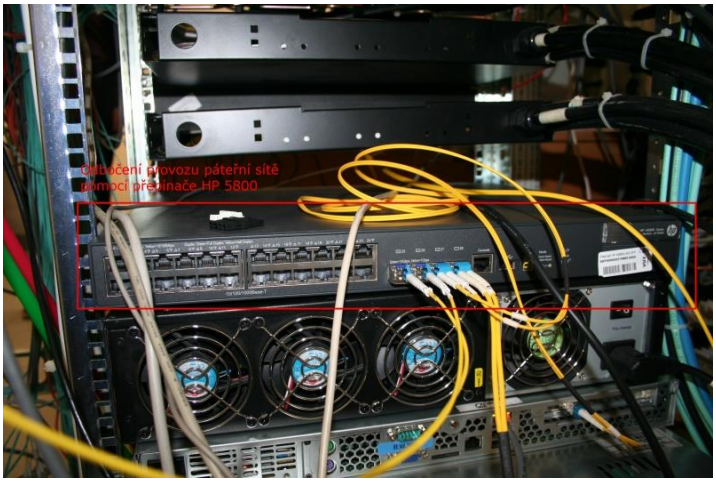
Ukázky výstupu

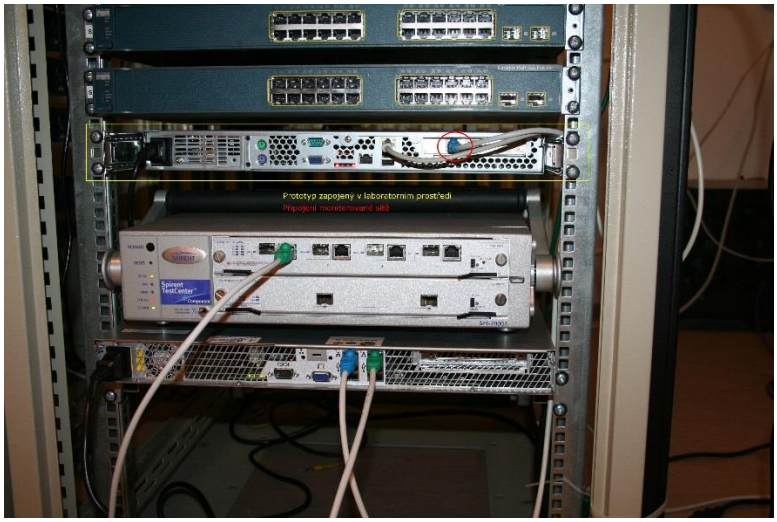
- Ukázka zobrazení dat příslušející adrese MAC:



- Schéma zapojení prototypu v laboratorním prostředí je znázorněno na následujících snímcích s popisky daného zapojení







- Prototyp DR systému využívá platformy Flowmon a opensource nástrojů pro dlouhodobé uchování dat o komunikaci uživatele a jeho identitě. Implementace systému kopíruje jeho návrh, prezentovaný v GRÉGR Matěj, PODERMAŃSKI Tomáš, ŠOLTÉS Miroslav a ŽÁDNÍK Martin. Design of Data Retention System in IPv6 network. FIT-TR-2011-07, Brno: Fakulta informačních technologií VUT v Brně, 2011.

Související neplánované výsledky

- Vykázán v IS/RIV, viz Prototyp systému pro sběr a uchovávání dat na lokální síti pro komunikaci protokolem IPv6, http://www.fit.vutbr.cz/~poderman/prods.php?id=311&notitle=1.
- Publikace - GRÉGR Matěj, PODERMAŃSKI Tomáš a ŠOLTÉS Miroslav. Flow Based Monitoring of IPv6. Brno, 2012.
- Publikace - GRÉGR Matěj, PODERMAŃSKI Tomáš a ŠVÉDA Miroslav. Deploying IPv6 - practical problems from the campus perspective. Reykjavik, 2012.
- Publikace - GRÉGR Matěj, PODERMAŃSKI Tomáš a ŠVÉDA Miroslav. User identification in IPV6 network. IP Networking 1 -- Theory and Practice. Žilina: Vydavatelství Žilinské univerzity, 2012, s. 5-8. ISBN 978-80-554-0494-3.
- Publikace - PODERMAŃSKI Tomáš a VESELÝ Vladimír. Support for the operation of IPv6 multicast and anycast. Amsterdam, 2012.
- Publikace - PODERMAŃSKI Tomáš. IPv6 v praxi. Brno, 2012.
- Publikace - PODERMAŃSKI Tomáš. Security challenges in IPv6 from the campus perspective. Oslo, 2012.
- Software - Spolehlivý a bezpečný transport NetFlow dat, software, 2012, Autoři: Podermański Tomáš, Štěpánek Adam, Grégr Matěj

Aktuálnost výsledku a použití v praxi

Prototyp využívá několik dílčích výsledků: Spolehlivý a bezpečný transport NetFlow dat, který umožňuje zasílat data bezpečným a spolehlivým kanálem mezi sondou a kolektorem a obchází tak omezení protokolu NetFlow, který není nikterak šifrovaný. Nástroj pro monitorování přechodových mechanismů v IPv6, který umožňuje prototypu sbírat informace z řady přechodových mechanismů používaných v sítích IPv6. Aplikační rozhraní v jazyce Perl pro práci se soubory nástroje nfdump umožňuje efektivně a rychle upravovat data NetFlow a rozšířit je o potřebné informace z jiných databází, aby měl prototyp kompletní pohled na data.

2. Prototyp vysokorychlostní sondy pro monitorování IPv6 provozu

Popis výsledku

Prototyp vysokorychlostní sondy se sestává ze serveru, síťové karty Combo100G, firmware pro kartu Combo100G a programového vybavení (software) pro server. Karta Combo100G umožňuje hardwarově akcelerovat zpracování síťového provozu tak, aby bylo možné zaznamenávat veškerou komunikaci odposlouchávaných entit. Karta je zapojena v hostitelském PC do PCI-Express x8 generace 3. Po restartu serveru je do karty nahrán firmware, který implementuje část funkcionality legálních odposlechů (legal interception --- LI). Firmware komunikuje se softwarem běžícím v hostitelském serveru. Pro komunikaci a přenos dat je využita knihovna NetCOPE.

Firmware LI nahraný do karty Combo realizuje následující funkce:

- přiřazení časové značky každému příchozímu paketu,
- parsování IP adres, čísel transportních portů a protokolu ze záhlaví paketu,
- filtrace a označení paketu na základě vyparsovaných polí (SDM),
- zahození nezájmových paketů na základě pravidel vkládaných ze software a přeposlání nezahozených paketů do software.

Software LI běžící v hostitelském serveru realizuje následující funkce:

- nahrání a konfigurace firmware, konfigurace a spuštění LI programů,
- připojení se na LI systém (k mediační funkci),
- konfigurace odposlechů přes rozhraní CCCI,
- parsování aplikačních protokolů za účelem získání Intercept Related Information (IRI),
- odesílání IRI na LI systém přes rozhraní INI2,
- záchyt zájmových paketů,
- odesílání odposlechnutých paketů přes rozhraní INI3,
- řízení Softwarově Definovaného Monitoringu (SDM).

Po startu sondy se sonda automaticky připojí k předem nakonfigurovanému LI systému. Ovládání sondy z LI systému probíhá pomocí CCCI (CC Configuration Interface) rozhraní, pomocí INI2 jsou odesílány na LI systém IRI zprávy a pomocí INI3 rozhraní je odposlouchávaný provoz odesílán na LI systém. Sonda je kompatibilní s LI systémem SLIS.

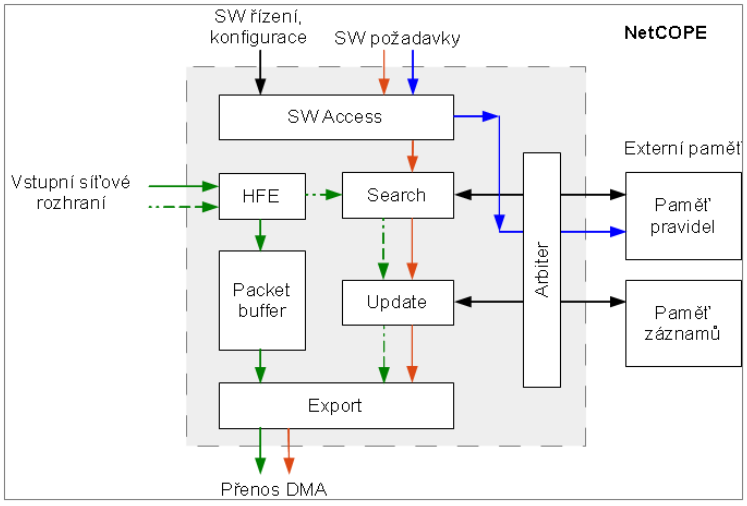
Architektura firmware je zachycena na obrázku 1. Pro řešení komunikace s periferiemi a pro komunikaci přes PCI-Express je využita knihovna NetCOPE. V rámci knihovny NetCOPE jsou využity následující bloky:

- Vstupní síťové rozhraní. V rámci NetCOPE a vstupních síťových bloků je nad příchozími ethernetovými rámci prováděna řada kontrol (dodržení limitů velikosti rámce, správnost hodnoty pole FCS). Kromě vlastních dat přenášených příchozími rámci jsou na tomto rozhraní předávány přidružené přídavné informace o přijímaných datech (přesná časová značka příchodu rámce, identifikace fyzického vstupního rozhraní, velikost příchozích dat). Rozhraní tvoří primární zdroj požadavků pro zpracování procesorem.
- Řídicí a konfigurační rozhraní platformy NetCOPE. Rozhraní je součástí propojovacího systému sběrnic platformy NetCOPE. Slouží ke čtení a zápisu hodnot konfiguračních a˜stavových registrů komponent v rámci platformy. Prostřednictvím tohoto rozhraní budou také přicházet požadavky softwarového řadiče systému.
- Rozhraní pro přenosy DMA. Jednotné rozhraní slouží k přenosu dat do operační paměti počítače prostřednictvím řadiče DMA a systémové sběrnice PCI-Express. Kromě určení DMA kanálu pro

přenos a samotných dat je nutné specifikovat také jejich přesnou velikost a identifikaci formátu. Řadič DMA vkládá před vlastní data určitý typ záhlaví obsahující tyto informace a umožňující jejich odpovídající zpracování softwarovým nástrojem.

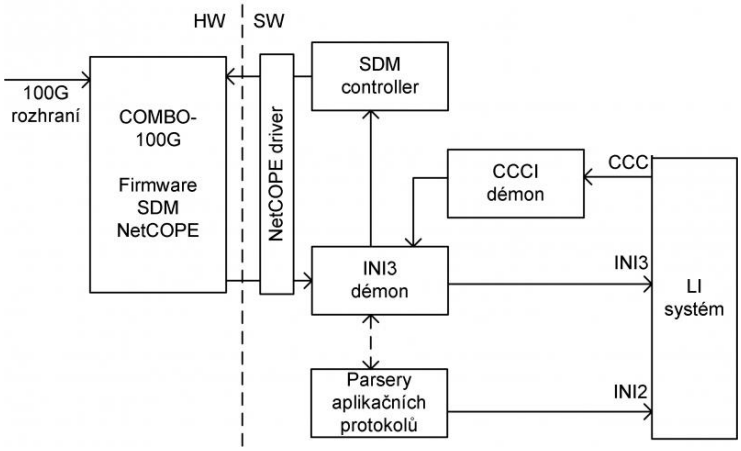
- Rozhraní externí paměti QDR. Do externí paměti QDR budou ukládána pravidla pro zpracování síťového provozu a agregované záznamy a statistiky o síťových tocích. Jednotné rozhraní poskytuje několik paralelních čtecích a zápisových slotů a slouží pro přístup k těmto položkám v externí paměti. V rámci platformy NetCOPE poskytuje odstínění od řadiče konkrétní paměti umístěné na akcelerační kartě.

Hlavní funkcionalitu firmware (tj. filtraci nezájmového provozu) zajišťuje firmware pro softwarově definovaný monitoring (SDM). Počáteční zpracování všech příchozích paketů ze vstupního síťového rozhraní (zeleně znázorněná datová cesta) probíhá v jednotce HFE (Header Field Extractor). Začíná analýzou a extrakcí jejich záhlaví a synchronizací s dodatečnými informacemi o přijímaných datech ze vstupních síťových bloků. Původní přijatý paket je dočasně odložen do FIFO paměti. Extrahovaná data jsou v jednotném formátu předána k dalšímu zpracování (přerušovaná, zeleně znázorněná datová cesta). Jednotka Search dále podle identifikace síťového toku vyhledá příslušné pravidlo v externí paměti. Je-li pravidlo nalezeno, je předáno spolu s extrahovanými daty jednotce Update, která počítá statistiky pravidel. Blok Export dále zajistí vyzvednutí přijatého paketu z vyrovnávací paměti, jeho další zpracování (zkrácení, zahození) a případně odeslání paketu nebo extrahovaných dat do softwaru. V případě, že není nalezeno odpovídající pravidlo, se provede výchozí způsob zpracování (všechny neznámé příchozí pakety jsou ve výchozím stavu odesílány do softwaru k další analýze). Odesílání dat do softwaru se realizuje přímým přístupem do operační paměti (DMA). Paměť pravidel je spravována softwarovým řadičem skrze jednotku SW Access (modře označená datová cesta).



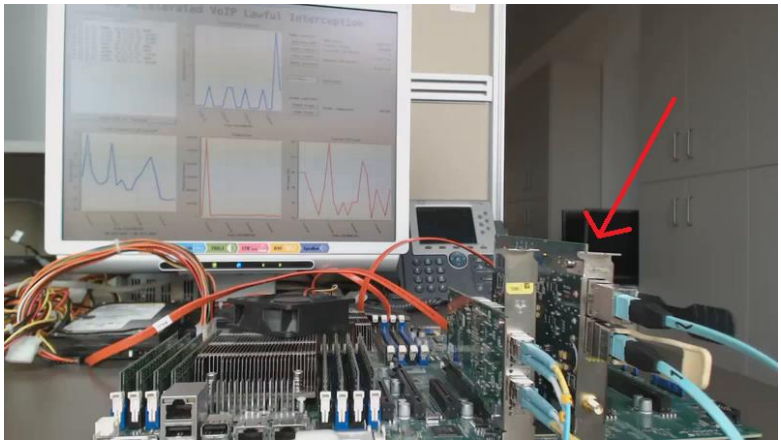
Architektura software je zachycena na obrázku 2. CCCI démon přijímá požadavky na odposlech z SLIS a vydává příkazy na odposlech do INI3 démonu. Rozhraní pro příjem požadavků na odposlech ze SLIS je tvořeno TCP/IP soketem. CCCI démon tvoří klienta, který se připojí ke SLIS. Aplikační protokol pro přenos požadavků na odposlech přes TCP soket je specifikován v Content of Communication Control Interface. Rozhraní mezi CCCI démonem a INI3 démonem je tvořeno TRAP (TCP soket). Díky tomu je možné zapojit více INI3 procesů a využít tak výkonnosti několika jader pro další filtrování provozu z karty. INI3 démon načítá příkazy na odposlech z CCCI, filtruje pakety na základě vlastního filtru zájmového provozu, vydává příkazy na filtrování provozu v kartě, dle příchozího provozu nebo příchozích požadavků z CCCI, předává vybrané pakety do INI2 procesu. INI3 démon se po spuštění připojí na SZE rozhraní pro příjem paketů z

karty (SZE rozhraní je poskytnuto přes NetCOPE driver). Dále se připojí na TRAP rozhraní pro příjem požadavků na odposlech z CCCI démonu. Rovněž naváže spojení se SLIS pro INI3 rozhraní přes TCP/IP. Dále si zažádá o sdílenou paměť SDM kontroleru (sdm_init, sdm_open) pro vydávání příkazů. INI3 démon se sestává ze dvou typů vláken: CCCI vlákno (filter_manager) zajišťuje komunikaci s CCCI démonem přes TRAP a aktualizuje filtrovací tabulky. Dále na základě pravidel uložených v tabulkách ovládá sdílenou paměť SDM kontroleru. SZE vlákno (filter_report) zajišťuje příjem paketů ze SZE, vyhledání pravidla ve filtrovacích tabulkách dle příchozího paketu, předání paketu do INI2 procesu, zahození/odeslání paketu na LI systém přes INI3 rozhraní. INI2 proces běží v rámci INI3 démonu. INI2 se po spuštění připojí k LI systému přes INI2 rozhraní. Přes toto rozhraní posílá LI systému zprávy o Intercept Related Information (IRI). Díky tomu, mohou být odposlechy zadávány na základě aplikačních identifikátorů například SIP URI. LI systém přeloží tento identifikátor na IP adresu a zašle jako odposlech přes CCCI rozhraní na sondu.



Demonstrace funkčnosti

Prototyp vysokorychlostní sondy se nachází v učebně L311 na FIT VUT v Brně, Božetěchova 2, 612 00 Brno. Následující video demonstruje funkcionalitu vysokorychlostní sondy při záchytu VoIP provozu. Demo ukazuje snížení ztrátovosti provozu na nulu a snížení procesorové zátěže v případě zapnutí SDM funkcionality.



Zpráva z testování byla popsána v technické zprávě FIT-TR-2015-1, viz https://wis.fit.vutbr.cz/FIT/db/vav/view_pub.php?id=10999. K dispozici je i dokumentační video, viz http://www.fit.vutbr.cz/research/prod/index.php?id=438&notitle=1. Součástí je i dokumentace pro sestavení a zprovoznění prototypu hardwarově akcelerované sondy pro zákonné odposlechy, viz

https://wis.fit.vutbr.cz/FIT/db/vav/view_pub.php?id=11000. Výsledný prototyp je vykázán na http://www.fit.vutbr.cz/research/prod/index.php?id=438&notitle=1.

Související neplánované výsledky

- Kekely Lukáš, Žádník Martin, Kořenek Jan: Funkční vzorek vysokorychlostní sondy pro monitorování IPv6 provozu, funkční vzorek, 2013
- Kekely Lukáš, Kořenek Jan, Žádník Martin: Paketový filtr pro síťový provoz s rychlostí 100 Gb/s, software, 2014
- KEKELY Lukáš, ŽÁDNÍK Martin, MATOUŠEK Jiří a KOŘENEK Jan. Fast Lookup for Dynamic Packet Filtering in FPGA. In: 17th IEEE Symposium on Design and Diagnostics of Electronic Circuits and Systems. Warszawa: IEEE Computer Society, 2014, s. 219-222. ISBN 978-1-4799-4558-0.
- Hardware accelerated packet filter for 100Gbps, technická zpráva, FIT VUT v Brně, 2014.
- ŽÁDNÍK Martin, KEKELY Lukáš, VRÁNA Roman, HOLKOVIČ Martin a FRANKOVÁ Barbora. Dokumentace pro sestavení a zprovoznění prototypu hardwarově akcelerované sondy pro legální odposlechy. Brno: Fakulta informačních technologií VUT v Brně, 2015.
- KEKELY Lukáš, VRÁNA Roman a ŽÁDNÍK Martin. Report z testování prototypu 100Gb/s sondy pro zákonné odposlechy. FIT-TR-2015-001, Brno: Fakulta informačních technologií VUT v Brně, 2015.

Aktuálnost výsledku a použití v praxi

Prototyp vysokorychlostní sondy je cílen na použití pro tzv. zákonné odposlechy, které v ČR upravuje §97 zák. 259/2010Sb., který vychází z evropské legislativy a norem ETSI pro zákonné odposlechy, zejména ETSI TR 101 943 a souvisejících. Ty umožňují v definovaných případech provádět odposlechy komunikace podezřelých osob.

Samotné nasazení sondy cílí na vysokorychlostní linky v datových centrech či páteřních linkách operátorů.

Přínos pro uživatele

Oproti současným řešením dovoluje vyvinutá sonda zachytit zájmový provoz na linkách s rychlostí 100 Gb/s. Dále sonda průběžně analyzuje provoz až na úroveň aplikační vrstvy a díky tomu dovoluje zachytit zájmový provoz na základě aplikačních identifikátorů, například SIP URI.

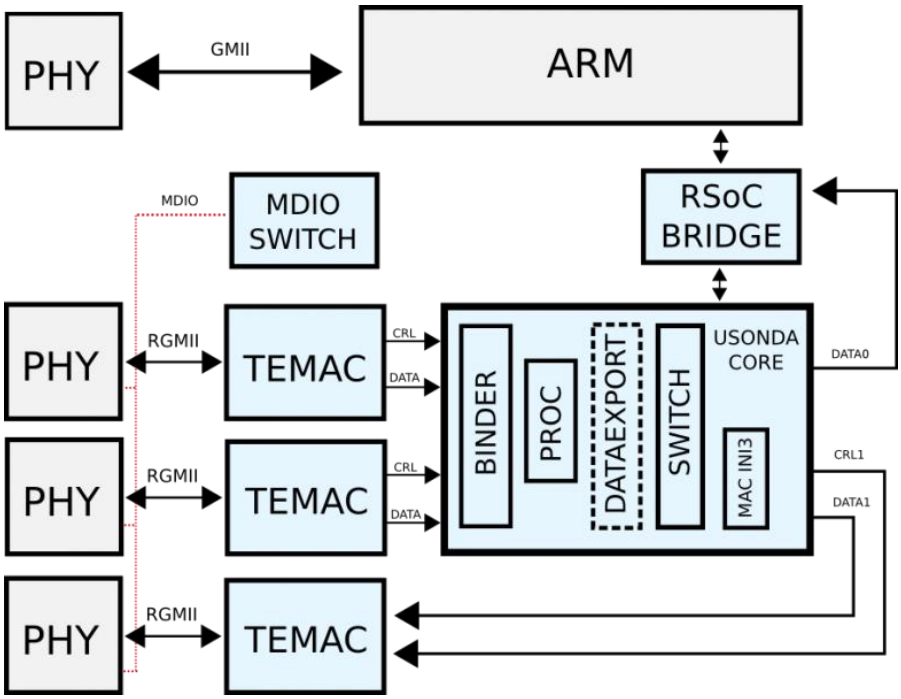
3. Prototyp mikrosondy sondy pro monitorování IPv6 provozu

Popis výsledku

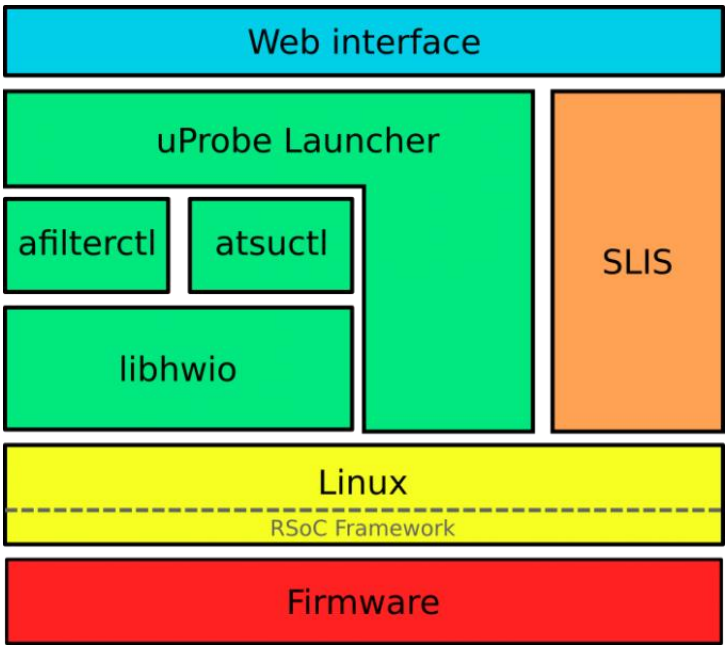
Prototyp mikrosondy je vestavěné zařízení určeno pro nasazení k menším ISP (Internet Service Provider), či přímo do infrastruktury mezi ISP a koncového uživatele. Pro napojené slouží několik metalických Ethernetových přípojek. Prototyp je postaven na technologii FPGA. Použitím FPGA je dosaženo naprosto tajného odposlechu komunikace IPv4 nebo IPv6 paketů. V průběhu projektu byl nejprve vyvinut funkční vzorek na vlastní hardwarové platformě (uG4-150). FPGA se staralo o záchyt i další analýzu paketů. Kromě toho jsme do FPGA integrovali tzv. soft-procesor (typu Xilinx MicroBlaze), který byl určen pro správu datové cesty (vzdálené konfigurace cez webové rozhraní či SSH připojení apod.). Výkonově však na tyto úlohy byl procesor slabý (frekvence jenom cca. 100 MHz) což omezovalo uživatele například pomalou odezvou při nastavování. I proto jsme se rozhodli finální variantu prototypu postavit na hardwarové platformě ZE7000 s výkonným čipem Xilinx Zynq kombinující ARM procesor a FPGA na jednom čipu. FPGA část obsahuje stejnou procesní část jako předešlý funkční vzorek s mírnými rozšířeními (např. úprava exportního INI3 protokolu). Softwarová část obsahuje také stejné vybavení s některými rozšířeními (např. časová synchronizace, spouštěcí skripty, apod.), které nová platforma

umožnila. Kromě platformy tedy prototyp pozůstává ze specifického firmwarového a softwarového vybavení. Toto je umístěného na SD kartě platformy ZE7000.

Firmware uSondy (modrou) spolu s napojením na okolí:



Software uSondy:



Ostatní dokumentace, návod na použití i možné případy použití je možné najít na http://www.fit.vutbr.cz/research/view_product.php?id=428.

Demonstrace funkčnosti

uSodna byla počas vývoje nasazena v laboratoři, kde byla testována na syntetických datech.

Související neplánované výsledky

- Sada síťových testů pro vestavěné procesory (2010, software)
    - Aby bylo možné vybrat pro mikrosondu vhodný procesor a identifkovat časově kritické operace, vytvořili jsme sadu výkonnostních testů zaměřených na vestavěné procesory. Provedli jsme implementaci testu výkonnosti při hledání nejdelšího shodného prefixu IP adresy (tzv. longest prefix match - LPM) a vyhledávaní vzorů (tzv. pattern match). Obě uvedené operace jsme z důvodu jednodušší přenositelnosti na různé procesory naprogramovali v jazyku C, přičemž pro generování datových sad jsme vytvořili skripty v jazyku Python. Protože je uvedený software obecnějšího charakteru, byl vydán jako samostatný balíček sloužící na otestování procesoru určených převážně pro vestavěné síťové aplikace jakými jsou např. routery. Nástroj měří čas běhu různých algoritmů s různými konfiguracemi a také s různými datovými sadami vždy pro daný algoritmus. Konfigurace a datové sady jsou součástí balíku.
    - Dostupný zde: http://www.fit.vutbr.cz/research/prod/index.php.cs?id=174

- KOŘENEK Jan, KORČEK Pavol a KAŠTIL Jan. Sondy pro monitorování provozu. FIT-TR-2011-09, Brno: Fakulta informačních technologií VUT v Brně, 2011.
    - Technický report se zabývá návrhem vysokorychlostní sondy a mikrosondy, které jsou určeny pro sběr síťových dat v systémech zaměřených na zákonné odposlechy. Vysokorychlostní sonda je určena do sítí velkých ISP s propustnosti v řádech desítek gigabitů, zatímco mikrosonda je navržena pro menší koncové sítě s propustností v řádu jednotek gigabitů. V systémech zaměřených na zákonné odposlechy je nutné zajistit zachycení požadovaného provozu beze ztráty jediného paketu, což klade značné nároky na konstrukci sond. Při návrhu obou sond byla proto použita hardwarová akcelerace filtrace síťového provozu s využitím technologie FPGA. Díky hardwarové akceleraci bude možné dosáhnout nejen zpracování síťového provozu na plné propustnosti linky, ale v případě mikrosondy i malých rozměrů a malé spotřeby zařízení. Návrh architektury vysokorychlostní sondy vychází z vlastností platformy NetCOPE a akcelerační karty COMBO. V případě mikrosondy byla i na základě testu dostupných platforem navržena a vytvořena vlastní hardwarová deska.
    - Dostupný zde: http://www.fit.vutbr.cz/research/view_pub.php?id=9817

- Zaváděč z karty SD pro procesory v FPGA (2011, software)
    - Další software, který je obecně použitelný pro libovolné procesory v FPGA. Je určen pro zavedení programu, či operačního systému z karet typu SD, SDHC a SDXC využívajíc

jednoduchého SPI módu. Je plně integrovatelný do vývojového nástroje Xilinx EDK/SDK. Volitelně podporuje souborový systém FAT16 nebo FAT32, šifrovaní pomocí XXTEA, testování paměti a v případě minimální konfigurace je možno ho uložit do necelých 16 kB.
    - Dostupný zde: http://www.fit.vutbr.cz/research/view_product.php?id=219

- Knihovna Device Tree (2012, software)
    - Tato knihovna je určena pro vyčítání informací o připojených zařízeních ve vestavěném systému. Využívá přitom struktury device tree, která je v operačním systému Linuxového typu umístěná v /proc/device-tree. Obsahem je také jednoduchá aplikace busio, která demonstruje použití rozhraní knihovny. Umožňuje z příkazové řádky zobrazit informace o v systému dostupných zařízeních, dále číst jejich paměťový prostor případně i zapisovat do něj.
    - Dostupná zde: https://github.com/jviki/dtree/tree/

- Knihovna HWIO (2012, software)
    - Knihovna poskytuje rozhraní pro konfiguraci hardwarových komponent na konfigurovatelných systémech postavených typicky nad FPGA. Cílem je odstínění od softwarového prostředí, které se může na různých systémech výrazně lišit. Rozhraní umožňuje identifikovat komponenty a přistupovat k jejich uživatelskému adresovému prostoru. Každá komponenta je identifikována trojicí (vendor, name, version), ke které může aplikace určit rozložení adresového prostoru a způsob přístupu k registrům. Ke každé komponentě lze dále přistupovat funkcemi pro zápis a čtení. Jsou dostupné dvě implementace a to pro embedded Linux (umístěný typicky přímo v procesoru na FPGA) využívající knihovnu dtree a pro přístup ke komponentám na kartách COMBOv2 pomocí knihovny libcombo.
    - Dostupná zde: http://www.fit.vutbr.cz/research/view_product.php?id=274

- Vestavěná vývojová platforma pro gigabitové síťové aplikace (2012, funkční vzorek)
    - Vestavěná vývojová platforma (později označována jako uG4-150) pro gigabitové síťové aplikace je určená pro obecnou hardwarovou akceleraci ale zejména pro zpracování síťového provozu na plné rychlosti linky. S využitím platformy je možné realizovat sběr kvalitních dat pro systémy zajišťující monitorování a bezpečnost sítě. Základem platformy je velice výkonné FPGA Xilinx Spatran-6 s největší dostupnou kapacitou a rychlostí (tzv. speedgrade). Díky konfigurovatelnosti technologie FPGA je možné měnit funkci platformy v závislosti na požadavcích konkrétní aplikace, což umožňuje optimalizovat hardwarovou akceleraci zpracování síťového provozu pro konkrétní algoritmy zajišťující sběr dat, filtraci zájmového provozu nebo detekci síťových anomálií. Platformu je možné využít taky pro vývoj a experimenty a je dále využita jako hardwarový základ pro vývoj mikrosondy. Samotná platforma má čtyři metalické RJ45 porty na připojení k sítí, dvě DDR3 paměti o kapacitě každé z nich 256 MB pro RAM, rychlé úložiště 16 MB flash pro bootovaní FPGA a pomalé úložiště v podobě mikro SD (HC/HX) slotu pro paměťové karty. Disponuje také výkonným USB 3.0 čipem pro rozhraní na periférie s požadavkem vysoké propustnosti (USB flash disk), sériovým (UART) rozhraním na mikro USB typu B konektor, standardním JTAG konektorem pro jednoduché ladění a několika signalizačními LED. Platforma samozřejmě obsahuje i další komponenty (zdroje, krystaly, pasivní součástky a pod) nezbytné pro správnou činnost platformy. Všechny výrobní podklady jsou dostupné. Vývoj pro platformu u4G-150 je doporučen pod systémy Xilinx EDK a Xilinx SDK. Pro platformu je dostupná vlastní verzi Linuxu pro procesor Xilinx MicroBlaze.
    - Dostupný zde: http://www.fit.vutbr.cz/research/view_product.php?id=251

- KOŘENEK Jan, KORČEK Pavol, KOŠAŘ Vlastimil, ŽÁDNÍK Martin a VIKTORIN Jan. A New Embedded Platform for Rapid Development of Networking Applications. In: Proceedings of the 2012 Seventh ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS 2012). Austin: IEEE Computer Society, 2012, s. 81-82. ISBN 978-1-4503-1684-2.
    - V tomto článku je prezentovaná nová vestavěná platforma uG4-150 založená na FPGA Xilinx Spartan-6, která je určená pro prototypování síťových aplikací. Je popsána nejen HW architektura ale také SW a FW výbava. Ukázkovou aplikací je vestavěná síťová sonda pro gigabitové sítě.
    - Dostupný zde: http://dl.acm.org/citation.cfm?id=2396573

- KORČEK Pavol a ŽÁDNÍK Martin. Lightweight benchmarking of platforms for network traffic processing. In: Proceedings of the 2012 IEEE 15th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS). Tallin: IEEE Computer Society, 2012, s. 278-283. ISBN 978-1-4673-1185-4.
    - V této práci se snažíme poodhalit výkonnost procesorů síťových vývojových desek a routerů v oblasti síťového zpracování a propustnosti. Byl použít software, který je dostupný samostatně a jsou v něm implementovány funkce jako vyhledávaní nejdelšího shodného prefixu, filtrace či vyhledávaní vzorů. Článek sumarizuje výsledky těchto algoritmických testů ale i testů propustnosti pro rozličné, ale dostupné platformy.
    - Dostupný zde: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6219074

- DRAŽIL Jan, KORČEK Pavol, VIKTORIN Jan a KOŠAŘ Vlastimil. Testování skriptovacích jazyků a webových serverů na procesoru Xilinx MicroBlaze a ARM Cortex-A9. FIT-TR-2013-04, Brno, 2013.
    - Technický report se zabývá výkonnostnímy testy na soft procesoru Xilinx Microblaze (funkční vzorek mikrosondy) a procesoru ARM Cortex-A9 který je součástí SoC Xilinx Zynq (finální prototyp mikrosondy). Testy jsou implementovány v několika skriptovacích jazycích. Konkrétně se jedná o Lua, PHP, Python 2 a Python 3. Soft procesor Xilinx Microblaze je testován ve 4 různých konfiguracích. Kde je snaha co nejlépe pokrýt způsob, jakým jednotlivé volby ovlivní výkon procesoru. Pro všechny jazyky je vytvořená sada testovacích skriptů, kde se zaměřujeme na co nejlepší zachování stejných abstraktních datových typů napříč všemi testovanými jazyky. U každého testu je měřena doba běhu celého skriptu a samotná doba výpočtu. Společně se skriptovacími jazyky jsou testovány i webové servery Lighttpd a Hiawatha. U webových serverů je porovnávána rychlost implementace CGI skriptů a odvozených technologií od CGI. Pro testované webových serverů se používají stejné testovací sady, jako byly použity u testování samotných interpretů.
    - Dostupný zde: http://www.fit.vutbr.cz/research/view_pub.php.en?id=10411

- KORČEK Pavol. uG4-150 embedded platform for wire-speed network packet processing. FIT-TR-2013-03, Brno: Faculty of Information Technology BUT, 2013.
    - Tento technický report detailně popisuje hardware vyvinuté FPGA platformy určené pro zpracování a akceleraci síťových paketů na rychlosti 1Gbps.
    - Dostupný zde: http://www.fit.vutbr.cz/research/view_pub.php?id=10402

- Mikrosonda pro monitorování gigabitových sítí (2013, funkční vzorek)
    - Tento funkční vzorek mikrosondy pro monitorování gigabitových sítí pozůstává z hardwarové platformy uG4-150 s příslušenstvím (zdroj, uSD karta), z krabičky pro platformu vytvořené pomocí 3D tisku, z aplikačního firmware pro FPGA, které je uloženo perzistentně na Flash paměti platformy. Nedílnou součástí je také software, který je uložen na uSD kartě a pozůstává z operačního systému Linuxového typu a potřebných aplikací pro procesor v FPGA. Mezi vlastnosti patří: filtr paketů je založený na kukaččí hash a postavený pro 1000 pravidel,

jak bylo domluveno se zástupci PČR a MV, odchycení dat včetně filtrace na plné rychlosti 1Gb pro dvě linky, celková propustnost tedy 2Gb/s, ke každému paketu se generují správné časové značky apod.
    - Dostupný zde: http://www.fit.vutbr.cz/research/view_product.php?id=331

- Klient protokolu CCCI (2013, software)
    - Jedná se o aplikaci využitou pro mikrosondu i vysokorychlostní sondu. Aplikace přijímá a dekóduje požadavky protokolu CCCI, které předává modulům ke zpracování. Typicky tyto požadavky slouží pro konfiguraci hardwarových filtrů IP provozu v FPGA.
    - Dostupný zde: http://www.fit.vutbr.cz/research/prod/index.php.cs?id=324

- VIKTORIN Jan, KORČEK Pavol, KOŘENEK Jan and FUKAČ Tomáš. Network monitoring probe based on Xilinx Zynq. In: Proceedings of the 2012 Tenth ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS 2014). Marina del Rey, CA, USA: Association for Computing Machinery, 2014, pp. 237-238. ISBN 978-1-4503-2839-5.
    - Konferenční článek popisuje návrh nové varianty mikrosondy nad novou platformou.
    - Dostupný zde: http://dl.acm.org/citation.cfm?id=2661769

- VIKTORIN Jan. Využití dynamické rekonfigurace vestavěných systémů pro monitorování počítačových sítí. In: Počítačové architektury a diagnostika 2014. Liberec: Technická universita v Liberci, 2014, s. 50-55. ISBN 978-80-7494-027-9.
    - Článek představuje architekturu vestavěného systému pro monitorování počítačových sítí. Architektura využívá systém na čipu s integrovanou rekonfigurovatelnou logikou (FPGA). Díky úzké integraci procesoru a FPGA je možné využít částečné dynamické rekonfigurace pro akceleraci časově kritických operací. Lze tak vytvořit systém s nižší cenou, menšími nároky na spotřebu a s menšími rozměry při zachování dostatečné výkonnosti.
    - Dostupný zde: http://pad2014.fm.tul.cz/docs/PAD2014-elektronicky_online.pdf

- IP core pro podporu vývoje aplikací na heterogenních platformách (2014, software)
    - IP core je určeno pro prototypování aplikací prostavěných na heterogenních platformách, které pozůstávají z programovatelné logiky - (Field Programmable Gate Array - FPGA) a procesoru (např. ARM). Typickým příkladem je platforma Xilinx Zynq. IP core obsahuje sadu standardních rozhraní, pomocí kterých je možné propojit FPGA komponentu s procesorem. Je implementováno v jazyce VHDL pro FPGA Xilnx řady 7 a je určeno pro vývojové prostředí Xilinx EDK (verze 14.3).
    - Dostupný zde: http://www.fit.vutbr.cz/research/view_product.php?id=368

- INI3 Dissector (2014, software)
    - Dissector pro INI3v1 Payload (INI3 Header neparsuje) je ve formě pluginu pro Wireshark a pro snazší instalaci je pro některé verze už zkompilován. Tento plugin slouží pro zobrazení paketů, které jsou odchyceny mezi sondou a tzv. mediační funkcí a tedy obsahují INI3v1 Payload hlavičku. Také obsahuje variantu, která správně zobrazuje případ kdy namísto MAC adres jsou položky z INI3.
    - Dostupný zde: http://www.fit.vutbr.cz/research/view_product.php?id=398

- Nástroj pro zachycení paketů ve formátu INI3 (2015, software)
    - Nástroj pro zachycení paketů ve formátu INI3 (ini3_dump) slouží k uložení paketů generovaných nejen mikrosondou do souboru formátu PCAP (INI3). Podporuje všechny režimy exportu mikrosondy, tj. direct export, TCP a UDP. Nástroj z přijatého paketu extrahuje časové razítko a správně ho přiřadí k paketu. TCP/UDP exportu je možné volitelně uložit i

samotnou INI3 hlavičku do výstupního PCAP souboru. Pro jednodušší zobrazení rámců, které obsahují oproti normálním ethernetovým rámcům INI3 hlavičky, byl vytvořen právě předchozí plugin do Wiresharku.

- Dostupný zde: http://www.fit.vutbr.cz/research/view_product.php?id=429

Aktuálnost výsledku a použití v praxi

Prototyp mikrosondy je cílen na použití pro tzv. zákonné odposlechy, které v ČR upravuje §97 zák. 259/2010Sb., který vychází z evropské legislativy a norem ETSI pro zákonné odposlechy, zejména ETSI TR 101 943 a souvisejících. Ty umožňují v definovaných případech provádět odposlechy komunikace podezřelých osob.

V současné době je při realizaci zákonných odposlechů využíváno specializovaných FPGA akceleračních karet (např. řešení od společnosti Invea-tech, a.s.: https://www.invea.com/cs/produkty-sluzby/li-system/li-sonda). Tyto řešení však vyžadují standardní server (montovatelné např. do racku), čímž je významně omezeno použití pro nesnadnou manipulaci a přemísťovaní. Mikrosonda tyto problémy odstraňuje díky svým kompaktním rozměrům a porovnatelnou funkcionalitou.

Zájem o prototyp mikrosondy projevili zástupci PČR, kteří jej již testují. Mezinárodní zájem může být doložen např. relativně vysokým počtem unikátních stáhnutí námi publikovaného článku o mikrosondě na prestižní mezinárodní konferenci (http://dl.acm.org/citation.cfm?id=2661769).

Přínos pro uživatele

Hlavním přínosem pro uživatele mikrosondy (tj. vyšetřovací orgány činné v trestním řízení, např. zástupci PČR) je nasezení zařízení pro zákonné odposlechy libovolně v terénu, tj. či už u menších lokálních ISP nebo přímo u podezřelých osob. Prototyp mikrosondy tedy přináší možnost zákonných odposlechů na 1Gbps linkách pomocí kompaktního zařízení schopného přenosu na libovolné místo dle potřeb uživatele.

4. Softwarový nástroj pro dohledání pachatele počítačové kriminality

Popis výsledku

Softwarový nástroj pro dohledání pachatele počítačové kriminality byl realizován pomocí vlastní implementace systému pro zákonné odposlechy: Sec6Net Lawful Interception System – SLIS. Nástroj SLIS byl implementován s přihlédnutím ke standardům ETSI.

Cílem aktivity související s tímto výstupem bylo vytvoření takového systému, který by byl vhodný pro potřeby výzkumu v oblasti zákonných odposlechů, analýzy dat a jejich rekonstrukce a hardwarové akcelerace sond určených pro sběr a identifikaci dat. SLIS dokáže spolupracovat se sondami vytvořenými v rámci tohoto projektu (Moderní prostředky pro boj s kybernetickou kriminalitou na Internetu nové generace).

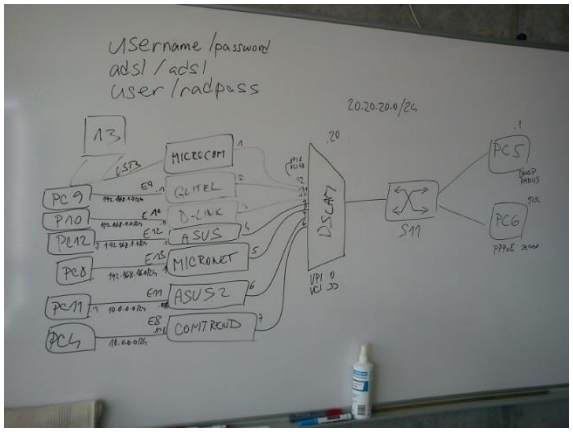
Systém SLIS tedy tvořil a tvoří základní prostředí pro: a) vývoj nových technik dynamické identifikace uživatele v prostředí IPv6 sítí, b) sběr dat a vývoj nových metod v oblasti rekonstrukce a vizualizace zachyceného provozu a c) jako základní testovací prostředí pro vývoj mikro-sondy a vysokorychlostní sondy.

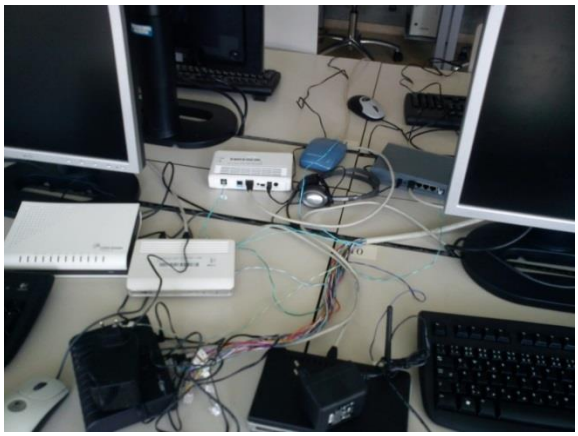
Detailní popis výsledku je obsažen v závěrečné technické zprávě skupiny pro zákonné odposlechy, viz POLČÁK Libor, MARTÍNEK Tomáš, HRANICKÝ Radek, BÁRTA Stanislav, HOLKOVIČ Martin, FRANKOVÁ Barbora a KRAMOLIŠ Petr. Zákonné odposlechy v moderních sítích - Shrnutí výsledků skupiny pro zákonné odposlechy projektu Moderní prostředky pro boj s kybernetickou kriminalitou na Internetu nové

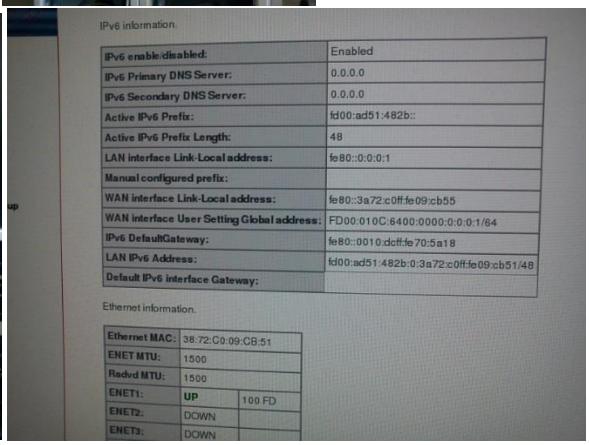
generace. FIT-TR-2014-07, Brno: Fakulta informačních technologií VUT v Brně, 2014. Technická zpráva je dostupná na: http://www.fit.vutbr.cz/~ipolcak/pubs.php?id=10788.

Demonstrace funkčnosti

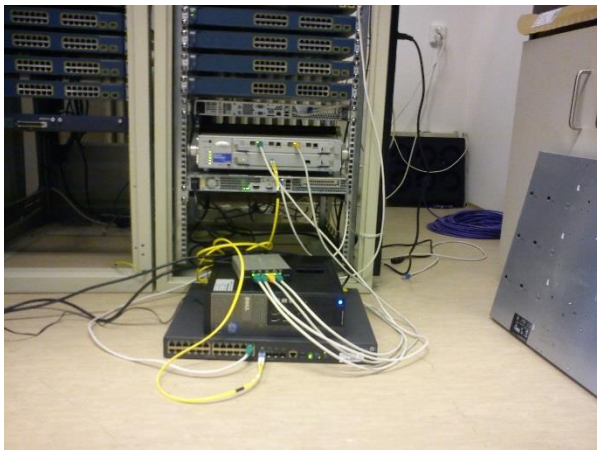
- Testovací prostředí pro xDSL: Schéma sítě; zapojení sítě v racku; testované modemy zapojené kabelem k DSLAMu; Konfigurace modemu Comtrend s podporou IPv6.

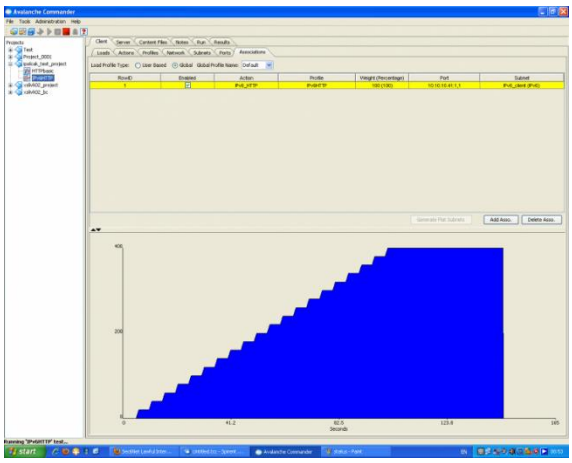


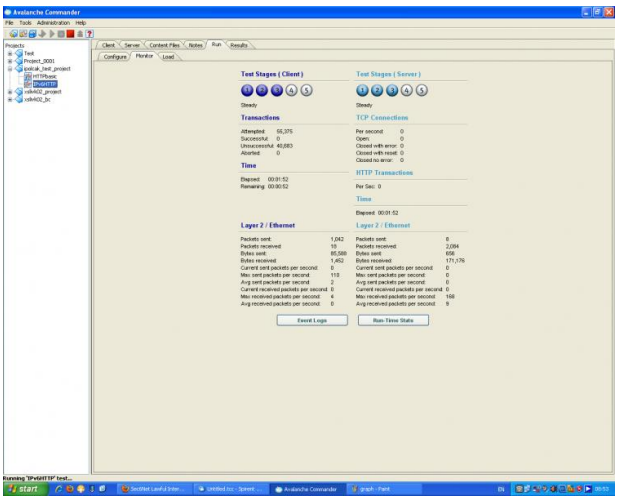


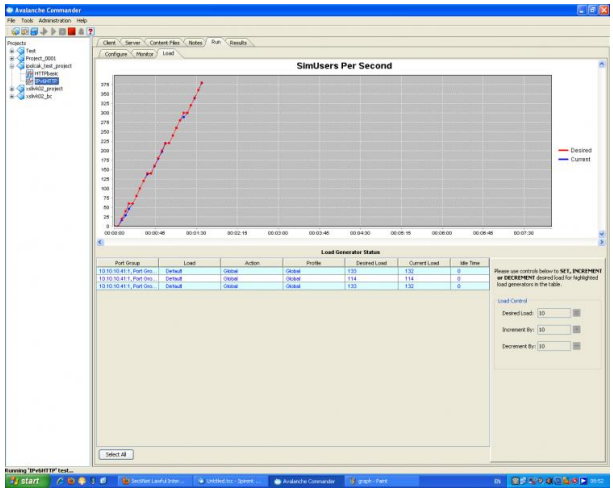


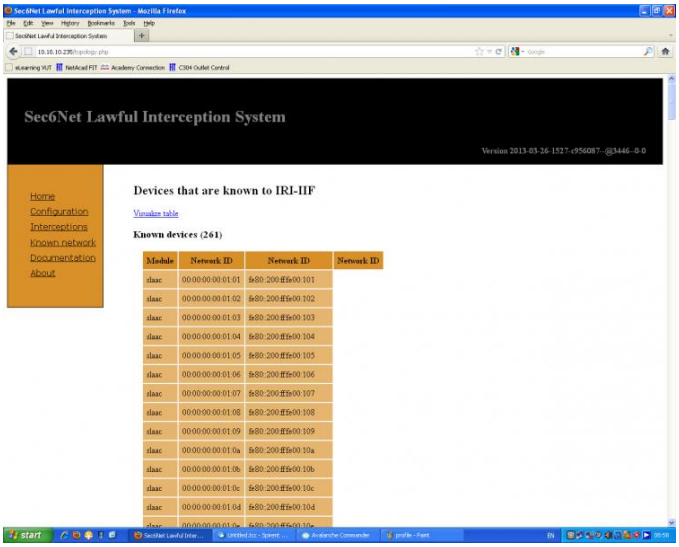
- Výkonnostní testování SLIS: testování pomocí generátoru provozu Spirent TestCenter (na dalších 3 obrázcích konfigurace pomocí programu Avalanche), na posledním obrázku výstup běžícího systému SLIS.



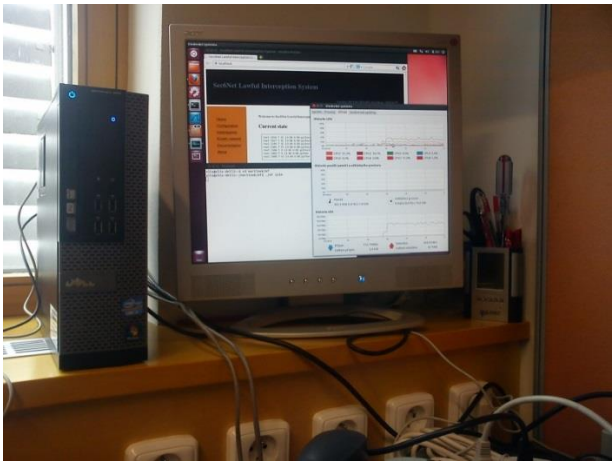


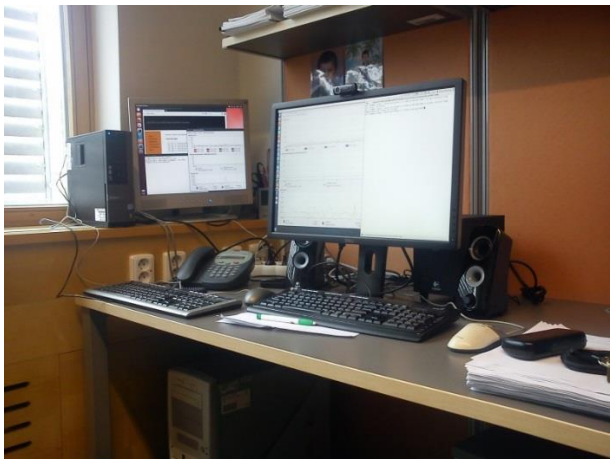




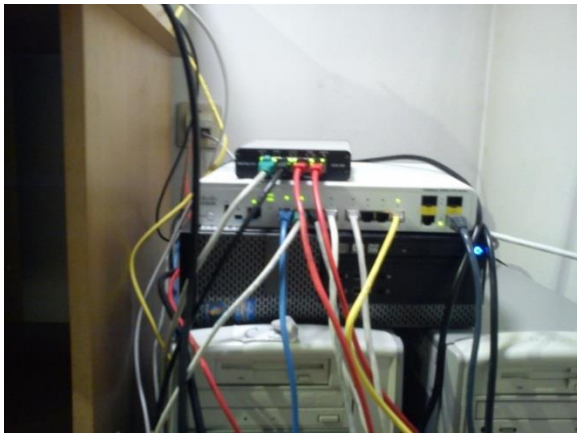


- Testování možnosti přenosů pomocí TCP a rychlosti zápisu na disk: Měření možností sytému SLIS a jednotlivých konfigurací disků.



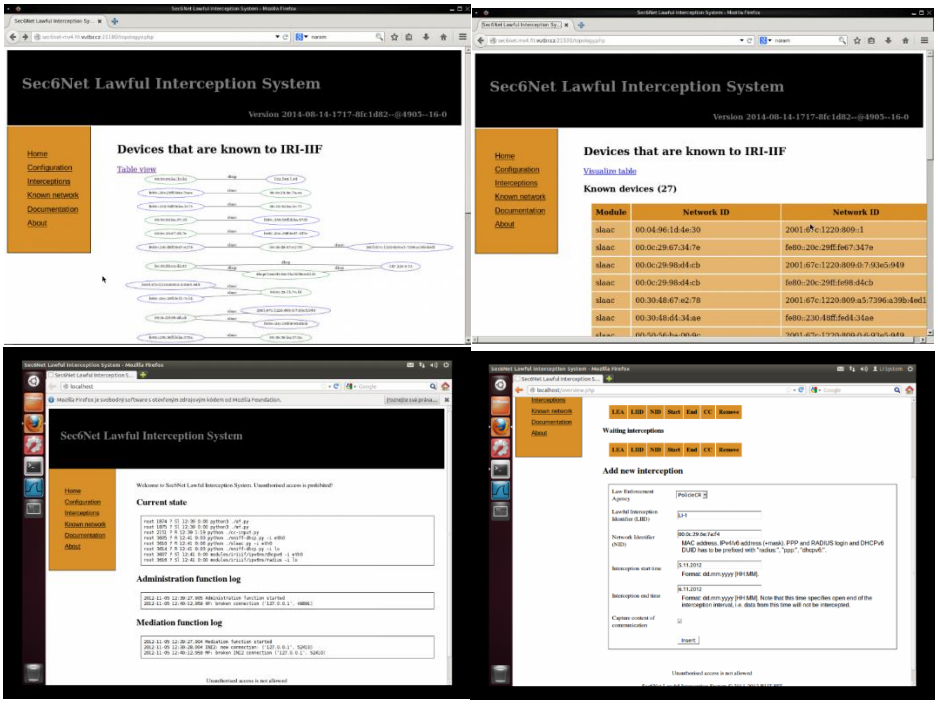


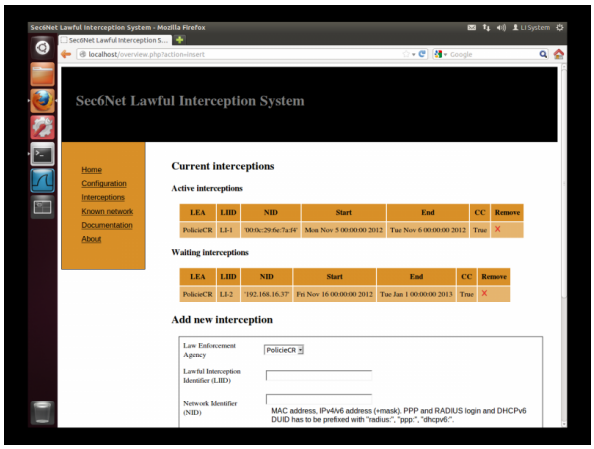
- Nasazení systému: Monitorovací stanoviště v jedné z kanceláří Fakulty informačních technologií Vysokého učení technického v Brně.

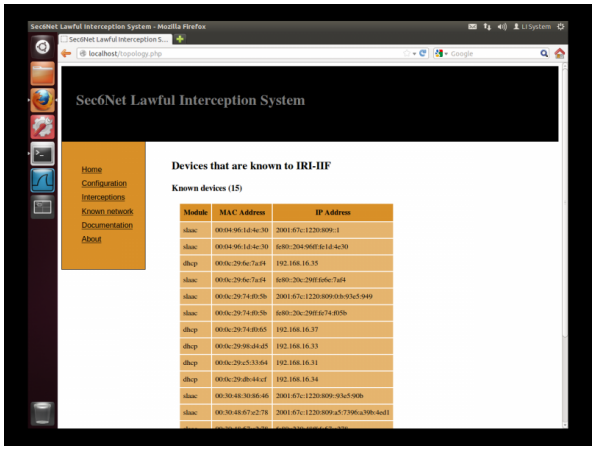


- Monitorovací stanoviště na kolejích Vysokého učení technického v Brně.

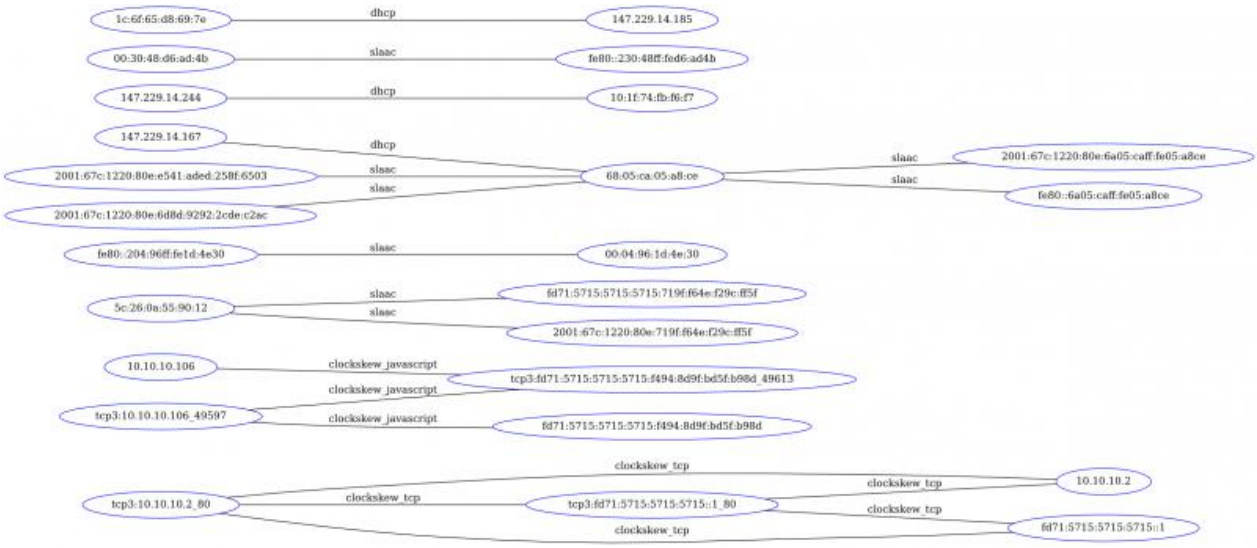
- Snímky obrazovek nástroje SLIS: Konfigurace a výpisy







- Detekované identifikátory a jejich vztahy při použití několika modulů pro detekci identity



Související neplánované výsledky

- POLČÁK Libor, GRÉGR Matěj, KAJAN Michal, MATOUŠEK Petr a VESELÝ Vladimír. Designing Lawful Interception in IPv6 Networks. In: Security and Protection of Information. Brno: Universita Obrany v Brně, 2011, s. 114-126. ISBN 978-80-7231-777-6
    - Zpočátku jsme se zabývali návrhem systému pro zákonné odposlechy na základě norem ETSI vhodného pro moderní počítačové sítě. Tento článek popisuje hlavní problémy systému pro zákonné odposlechy, který by byl schopný pracovat v sítích s podporou protokolu IPv6.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/pubs.php?id=9620

- POLČÁK Libor, KRAMOLIŠ Petr, KAJAN Michal a MARTÍNEK Tomáš. Architektura systému pro zákonné odposlechy. FIT-TR-2011-008, Brno: Fakulta informačních technologií VUT v Brně, 2011.
    - Tato technická zpráva popisuje návrh architektury prototypu vyvíjeného systému pro sběr dat pro zákonné odposlechy se zaměřením na vývoj nových technik dynamické identifikace uživatele v prostředí IPv6 sítí, pro sběr dat a vývoj nových metod v oblasti rekonstrukce a vizualizace zachyceného provozu a také jako základní testovací prostředí pro vývoj mikro-sondy a vysokorychlostní sondy. Součástí zprávy je podrobný popis

architektury navrhovaného systému a způsob komunikace mezi jednotlivými bloky. Zdůrazněny jsou problémy, které bylo potřeba při návrhu zohlednit, včetně způsobů jejich řešení. Zvláštní pozornost je věnována problematice dynamické identifikace cíle v prostředí IP sítí a návrhu architektury bloku IRI-IIF, který je za tuto funkci v systému pro sběr dat pro zákonné odposlechy zodpovědný.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/pubs.php?id=9829

- POLČÁK Libor. Designing Lawful Interception System. In: Proceedings of the 17th Conference STUDENT EEICT 2011 Volume 3. Brno: Fakulta informačních technologií VUT v Brně, 2011, s. 569-573. ISBN 978-80-214-4273-3
    - Během práce na předešlých dvou výstupech vznikl také příspěvěk na studentskou konferenci EEICT. Příspěvek se zabývá návrhem systému pro zákonné odposlechy. Přináší původní architekturu, která řeší i některé problémy dosud nepojednané v legislativních doporučeních, jako jsou identifikace komunikace podezřelého a podporu nových protokolů.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/pubs.php?id=9610

- KAJAN Michal, KORANDA Karel a POLČÁK Libor. Spolehlivá a zabezpečená komunikace v rámci systému pro zákonné odposlechy. FIT-TR-2012-007, Brno: Fakulta informačních technologií VUT v Brně, 2012.
    - Tato technická zpráva popisuje způsob zajištění spolehlivého a bezpečného přenosu dat ve vyvíjeném systému pro zákonné odposlechy. Součástí zprávy je analýza dostupných přenosových protokolů a možností zabezpečení komunikace pomocí šifrování. Na základě analýzy přenosových protokolů byl vybrán protokol TCP pro zajištění spolehlivosti přenosu dat v rámci vytvářeného systému.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/pubs.php?id=10204

- MARTÍNEK Tomáš, KRAMOLIŠ Petr, HOLKOVIČ Martin a POLČÁK Libor. Dynamická identifikace uživatelů v prostředí sítí IPv4 a IPv6. FIT-TR-2012-006, Brno: Fakulta informačních technologií VUT v Brně, 2012.
    - Tato technická zpráva je zaměřena na návrh bloku IRI-IIF, který je součástí systému pro zákonné odposlechy a zodpovídá za sledování identity odposlouchávaných cílů. V prostředí počítačových sítí je za identitu uživatele považována zejména IP adresa a úlohou bloku IRI-IIF je proto sledovat protokoly pro přidělování IP adres jako jsou DHCP, RADIUS, PPPoE, DHCPv6, SLAAC apod. a identifikovat aktuální adresy odposlouchávaných uživatelů. Součástí této technické zprávy je podrobný návrh architektury bloku IRI-IIF, který zahrnuje jednak společnou část, ale také jednotlivé moduly pro analýzu protokolů pro přidělování IP adres. Navrhovaná architektura se vyznačuje svou modularitou, která zajišťuje, že s příchodem nového protokolu stačí pouze doplnit příslušný modul, bez nutnosti modifikovat ostatní části bloku IRI-IIF. V neposlední řadě se blok také vyznačuje schopností spojovat informace z různých protokolů a realizovat tak odposlechy napříč několika vrstvami referenčního modelu ISO/OSI.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/pubs.php?id=10210

- POLČÁK Libor a HRANICKÝ Radek. Útoky na systémy pro zákonné odposlechy. FIT-TR-2012-008, Brno: Fakulta informačních technologií VUT v Brně, 2012.
    - Tato technická zpráva popisuje útoky na systémy pro sběr dat pro zákonné odposlechy, možnosti skrývání dat v síti a možná protiopatření. V práci práce jsou představeny normy a standardy pro zákonné odposlechy platné v Evropské unii i Spojených státech amerických a referenční architektura představená společností Cisco. Na základě těchto

norem je podán přehled možných útoků, kterými je možné systém pro zákonné odposlechy obelstít a znesnadnit tak analýzu nasbíraných dat. Kromě metod útoků jsou představena i možná protiopatření a je diskutována jejich vhodnost pro účely sběru dat pro zákonné odposlechy. V rámci práce je představen nástroj pro skrytí komunikace a nástroj pro detekci tohoto útoku. Demonstrací běhu tohoto programu je ukázáno podvržení zprávy při komunikaci využívající veřejnou komunikační síť IRC.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/pubs.php?id=10201

- LDP - Proxy pro oklamání systému pro zákonné odposlechy, software, 2012
    - Soubor nastroju LIS Deception Proxy (LDP) slouží k demonstraci útoku na systém pro zákonné odposlechy. LNC dokáže utajit vybraná spojení, přičemž odchozí zprávy budou fragmentovány a odesílány společně se šumem. Díky vhodně zvolenému Hop Limitu je docíleno zahození šumu před doručením koncové stanici. Možnostmi nástroje se zabývá technická zpráva FIT-TR-2012-008.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/prods.php?id=255&notitle=1

- LNC - Odstraňovač šumu pro systém pro zákonné odposlechy, software, 2012
    - Soubor nástrojů LIS Noise Cleaner (LNC) slouží k odfiltrování šumu vytvořeného nástrojem LDP. Možnostmi nástroje se zabývá technická zpráva FIT-TR-2012-008.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/prods.php?id=256&notitle=1

- IMMC - Tvorba metadat pro odposlech komunikace v reálném čase, software, 2012
    - Tento nástroj obsahuje podporu pro zpracování protokolů pro komunikaci v reálném čase a následné vytváření metainformací (zpráv IRI) ze zachycené komunikace. Nástroj umožňuje zpracování protokolů XMPP, IRC a OSCAR. Nástroj je použitelný buď samostatně, nebo jako modul systému SLIS.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/prods.php?id=257&notitle=1

- pcf - Nástroj pro hledání počítačů v síti, software, 2012
    - Nástroj PC Fingerprinter (PCF) je schopný na základě síťové komunikace nad protokolem TCP, ICMP, či vkládaných časových značek (např. v HTTP pomocí JavaScriptu) identifikovat počítač. Program naslouchá na síťovém rozhraní a podle nastavení v konfiguračním souboru analyzuje (veškerou) komunikaci. Zúčastněné počítače a naměřené hodnoty jsou ukládány do výstupního XML souboru a jiných výstupů. Ke každému ze sledovaných počítačů je průběžně generován graf odchylky jeho vnitřních hodin ve formátu SVG. Nástroj je použitelný buď samostatně, nebo jako modul systému SLIS.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/prods.php?id=254&notitle=1

- POLČÁK Libor, HOLKOVIČ Martin a MATOUŠEK Petr. A New Approach for Detection of Host Identity in IPv6 Networks. In: Proceedings of the 4th International Conference on Data Communication Networking, 10th International Conference on e-Business and 4th International Conference on Optical Communication Systems. Reykjavík: SciTePress - Science and Technology Publications, 2013, s. 57-63. ISBN 978-989-8565-72-3.
    - Správcům sítě se hodí znalost o vztazích mezi IP a MAC adresami. Zjištění těchto vztahů je v IPv6 složitější než u IPv4. Tento článek představuje nový způsob sledování přiřazení IPv6 adres v lokálních sítích. Navržená metoda je založena na studii implementace IPv6 v různých operačních systémech. Rozpoznání je pasivní pro koncová zařízení a nepotřebuje žádné SW nebo HW změny v síťových zařízeních.

    - Tento článek získal cenu za nejlepší studentský článek na konferenci 4th International Conference on Data Communication Networking.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/pubs.php?id=10362

- POLČÁK Libor, HRANICKÝ Radek a MATOUŠEK Petr. Hiding TCP Traffic: Threats and Counter-measures. In: Security and Protection of Information 2013, Proceedings of the Conference. Brno: Universita Obrany v Brně, 2013, s. 83-96. ISBN 978-80-7231-922-0.
    - Směrovače v počítačových sítítch nekontrolují integritu přenášených dat. Útočník tak může modifikovat svůj provoz takovým způsobem, že analyzátor provozu vidí jiný obsah než cílová stnaice. Tento článek navazuje na technickou zprávu FIT-TR-2012-008 a zabývá se proveditelností takového útoku a možnými opatřeními, jak útoku předcházet.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/pubs.php?id=10333

- ndtrack, software, 2013
    - Nástroj ndtrack analyzuje protokol Neighbor Discovery. Program detekuje použití IPv6 adresses koncovými zařízeními v lokální síti. Možnostmi nástroje se zabývá článek A New Approach for Detection of Host Identity in IPv6 Networks. Nástroj je použitelný buď samostatně, pak vypisuje detekované události na standardní výstup, nebo jako modul systému SLIS.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/prods.php?id=308&notitle=1

- POLČÁK Libor, JIRÁSEK Jakub a MATOUŠEK Petr. Comment on "Remote Physical Device Fingerprinting". IEEE Transactions on Dependable and Secure Computing. Los Alamitos: IEEE Computer Society, 2014, roč. 11, č. 5, s. 494-496. ISSN 1545-5971.
    - V tomto článku jsme znovu prozkoumali metodu pro zjišťování identity počítačů na základě jejich odchylky měření času zjišťované z časových značek přenášených protokolem TCP. Pro tyto účely jsme vytvořili vlastní nástroj pro zjišťování odchylek v měření času počítačů zapojených v síti - pcf. Ověřili jsme, že původní metoda je použitelná pro identifikaci počítačů, ale také jsme objevili, že počítače s OS Linux synchronizující čas pomocí NTP již nejsou identifikovatelné pomocí zkoumané metody.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/pubs.php?id=10377

- POLČÁK Libor, HOLKOVIČ Martin a MATOUŠEK Petr. Host Identity Detection in IPv6 Networks. Communications in Computer and Information Science. Heidelberg: Springer Verlag, 2014, roč. 2014, č. 456, s. 74-89. ISBN 978-3-662-44787-1. ISSN 1865-0929.
    - Tento článek je knižní, rozšířenou verzí článku A New Approach for Detection of Host Identity in IPv6 Networks. Oproti původní verzí se rozšířená verze zabývá především softwarově definovanými sítěmi.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/pubs.php?id=10467

- POLČÁK Libor, HRANICKÝ Radek a MARTÍNEK Tomáš. On Identities in Modern Networks. The Journal of Digital Forensics, Security and Law. 2014, roč. 2014, č. 2, s. 9-22. ISSN 1558-7215.
    - Na základě implementace spojování částečných identit v rámci bolku SLIS vznikl tento článek. V počítačových sítích se používají různé identifikátory. Některé z nich jsou stabilní, jiné jsou dynamicky přidělované. Článek se zabývá několika problémy, které přináší moderní síťové prostředí pro zákonné odposlechy.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/pubs.php?id=10633

- POLČÁK Libor a FRANKOVÁ Barbora. On Reliability of Clock-Skew-Based Remote Computer Identification. In: Proceedings of the 11th International Conference on Security and

Cryptography. Vídeň: SciTePress - Science and Technology Publications, 2014, s. 291-298. ISBN 978-989-758-045-1.
    - Tento článek shrnuje naše zkušenosti s používáním programu pcf pro identifikaci počítače na základě odchylky jeho vnitřních hodin.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/pubs.php?id=10612

- POLČÁK Libor. Challenges in Identification in Future Computer Networks. In: ICETE 2014 Doctoral Consortium. Vídeň: SciTePress - Science and Technology Publications, 2014, s. 15-24.
    - Tento rozšířený abstrakt vznikl jako souhrn pokroků disertační práce jeho autora. Abstrakt představuje problémy týkající se identifikace uživatele v moderních sítích a nastiňuje možnosti jejich řešení.
    - Tento článek vyhrál soutěž studentů Ph.D. za nejlepší rozšířený abstrakt disertační práce. Soutěž se konala při konferenci ICETE 2014.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/pubs.php?id=10516

- COUFAL Zdeněk a POLČÁK Libor. Anonymizační síť Tor. FIT-TR-2014-02, Brno: Fakulta informačních technologií VUT v Brně, 2014.
    - Metadata obsažená v hlavičkách síťových protokolů do značné míry prozrazují identitu komunikujících stran. Někteří uživatelé však potřebují, či chtějí komunikovat anonymně. Síť Tor si klade za cíl takovou komunikaci umožnit. Tato technická zpráva navazuje na technické zprávy a nástroje zabývající se útoky a možnostmi obelstění systémů pro zákonné odposlechy. Zpráva popisuje fungování sítě Tor po technické stránce.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/pubs.php?id=10626

- Správa identity z projektu Sec6Net, software, 2014
    - Jednou z podstatných zkoumaných částí při vytváření systému SLIS byla funkce dynamické identity pachatele. Úloha identifikace uživatelů se však vyskytuje i v jiných oblastech souvisejících s počítačovými sítěmi. Tento software umožňuje využití vytvořené funkce pro zjišťování dynamické identity uživatele mimo systém SLIS.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/prods.php?id=399&notitle=1

- POLČÁK Libor, MARTÍNEK Tomáš, HRANICKÝ Radek, BÁRTA Stanislav, HOLKOVIČ Martin, FRANKOVÁ Barbora a KRAMOLIŠ Petr. Zákonné odposlechy v moderních sítích - Shrnutí výsledků skupiny pro zákonné odposlechy projektu Moderní prostředky pro boj s kybernetickou kriminalitou na Internetu nové generace. FIT-TR-2014-07, Brno: Fakulta informačních technologií VUT v Brně, 2014.
    - Cílem této souhrnné technické zprávy je shrnutí výsledků dosažených skupinou pro zákonné odposlechy projektu. Tato technická zpráva obsahuje aktualizované podstatné informace zveřejněné v rámci předešlých technických zpráv a publikovaných článků souvisejících s projektem. Současně tato zpráva obsahuje podstatné informace pro instalaci a konfiguraci systému SLIS, či jeho budoucí rozšíření.
    - Dostupný zde: http://www.fit.vutbr.cz/~ipolcak/pubs.php?id=10788

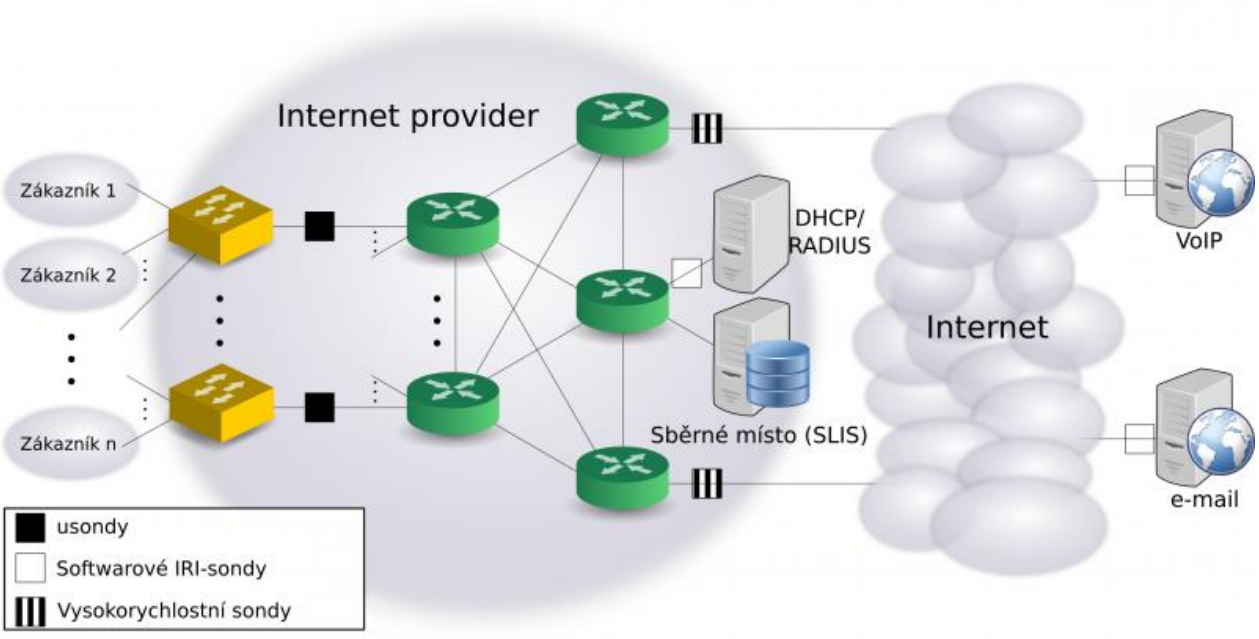
- POLČÁK Libor a FRANKOVÁ Barbora. Clock-Skew-Based Computer Identification: Traps and Pitfalls. Akceptováno Journal of Computer Science. ISSN 0948-6968.

Aktuálnost výsledku a použití v praxi

Z hlediska legislativy ČR plyne požadavek na zákonné odposlechy ze zákona č. 127/2005 Sb. ve znění pozdějších předpisů, Zákon o elektronických komunikacích, hlava V, díl 1, odposlech a záznam zpráv. Obdobně je tato povinnost ukotvena také v legislativě Evropské unie, v usnesení rady ze dne 17.1.1995 (96/C 329/01) z roku 1996.

Systém SLIS je možné nasadit jak v síti poskytovatele Internetu využívající nejnovější protokoly. Funkce pro určování dynamické identity uživatele umožňuje využití pro nejčastější protokoly používané poskytovateli Internetu. Systém podporuje protokoly DHCP, RADIUS, PPPoE, DHCPv6, mechanismus objevování sousedů v IPv6 (ND) včetně bezstavové konfigurace IPv6 adres (SLAAC). Dále systém podporuje aplikační protokoly XMPP, IRC, OSCAR, YMSG a SMTP. Experimentálně systém umožňuje identifikaci počítače na základě unikátní odchylky v měření času konkrétního počítače. V dnešní době je stále častěji diskutován koncept softwarově definovaných sítí (SDN). Vytvořený systém podporuje získávání identity z kontrolérů SDN Open Daylight a Pox.

Následující obrázek představuje očekávané schéma zapojení systému ve spolupráci s mikro-sondami a vysokorychlostními sondami v síti poskytovatele Internetu:



Přínos pro uživatele

Cílem vytvářeného softwarového nástroje byla detekce pachatele trestné činnosti v počítačových sítích. Proto jsme se při vytváření nástroje SLIS zaměřili především na dynamickou identitu uživatelů v počítačových sítích. V průběhu řešení projektu jsme publikovali řadu souvisejících vědeckých článků, které jsou především přínosné pro vědeckou komunitu. Na základě diskuzí se zástupci Policie ČR jsme si ověřili, že i pro ně je užitečné znát možnosti identifikace uživatele a proto jsou vytvořené výsledky vhodné i pro jejich práci.

Kromě vytváření samotného nástroje pro zákonné odposlechy jsme se zabývali i možnostmi obelstění systémů pro zákonné odposlechy. Vytvořené výstupy a technické zprávy jsme prezentovali zástupcům Policie ČR.

5. Softwarový nástroj pro monitorování a kontrolu komunikace řídících a pomocných protokolů IPv6

Popis výsledku

Základní verze nástroje ndwatch pro supervizi IPv6 sítí byla implementována v roce 2011 a v dalších letech dále rozšířena. V současné verzi obsahuje knihovnu v jazyce C++ pro dekódování a kódování IPv6/ICMPv6 paketů (packet-lib). Tato knihovna je obecná a využívá ji nástroj ndwatch, který umožňuje monitorovat protokol Neighbor Discovery Protocol (NDP) sloužící jako řídící protokol v sítích IPv6. Nástroj umožňuje detekovat zneužití zpráv protokolu NDP, primárně zpráv Duplicate Address Detection, Router Solicitation/Advertisement a Neighbor Solicitation/Advertisement. Nástroj je implementován pro systémy FreeBSD a Linux a dostupný na webové stránce ndwatch, viz http://www.fit.vutbr.cz/~lampa/ipv6/, kde lze také nalézt další informace.

- Příklad konfiguračního souboru:

```
# BDB nodes database
nodes /var/db/nodes.db
# RA packet rate_limit (packets/s) email_interval (secs/email)
ra_limit 10 3000
# email events
email nobody@company.org new_node upd_node invalid_ra invalid_na dad_dos
# IPv6 subnet and router(s) definition
subnet 2001:db8:1c0:1234::/64
  # monitoring interface
  dev em0         # or eth0, igb0, etc.
  # router MAC address Link-Local address       Global Unicast
address...
  mac 0:ab:cd:ef:12:34 fe80::2ab:cdff:feef:1234 2001:db8:1234::1
```

- Příklad spuštění: ndwatch -d -u -i em0
- Požadavky pro instalaci
  - C++ compiler (gcc-4.2 nebo novější)
  - libpcap (FreeBSD or Linux)
  - klientská knihovna pro BDB, GDBM, NDBM nebo MySQL

Demonstrace funkčnosti

- Ukázka výpisu databáze MAC a IPv6 adres.

```
MAC 00:30:68:30:86:46 Sat Apr  2 17:01:58 2011
   IPv4 192.168.9.11 Sat Apr  2 16:59:31 2011
   LLA fe80::230:68ff:fe30:8646 Sat Apr  2 16:57:23 2011
   IPv6 2001:db8:1c0:1234::90b Sat Apr  2 16:53:40 2011
   IPv6 2001:db8:1c0:1234::913 Sat Apr  2 16:59:25 2011
MAC 00:04:a6:1d:4e:30 Sat Apr  2 17:02:25 2011
   LLA fe80::204:a6ff:fe1d:4e30 Sat Apr  2 17:02:25 2011
   IPv6 2001:db8:1c0:1234::1 Sat Apr  2 16:53:47 2011
```

- Ukázka emailové notifikace zaslané síťovému správci.

```
Update node MAC 00:30:68:30:86:46
IPv4 address: 192.168.9.11 (test.example.com) last Sat Apr  2 17:18:49 2011
```

```
IPv4 address: 192.168.9.19 (test2.example.com) last Sat Apr  2 17:18:43 2011
IPv6 LLA address: fe80::230:68ff:fe30:8646 last Sat Apr  2 17:12:23 2011
IPv6 address: 2001:db8:1c0:1234::90b last Sat Apr  2 16:53:40 2011
IPv6 address: 2001:db8:1c0:1234::913 last Sat Apr  2 16:59:25 2011
```

Aktuálnost výsledku a použití v praxi

Software je možné využívat kýmkoliv na základě Open Source licence. Software je volně ke stažení na adrese http://www.fit.vutbr.cz/~lampa/ipv6/.

Přínos pro uživatele

Použití SW umožňuje správci realizovat bezpečný provoz protokolu IPv6 v lokální síti.

6. Nástroj pro síťovou forenzní analýzu NetFox Detective

Popis výsledku

Prototyp NFX Detective implementuje funkcionalitu potřebnou pro analýzu zachycené komunikace s možností snadné extrakce obsahu z podporovaných aplikačních protokolů. Mezi základní vlastnosti patří:

- Vytvoření projektu, ve kterém je možné analyzovat související PCAP soubory. Celková velikost souborů v projektu může dosahovat desítek až stovek GB zachycených dat.
- Vizualizace v různých pohledech a úrovních detailu - od zobrazení přehledu pro všechen provoz až po jednotlivé přenesené pakety.
- Kolekce extraktorů pro nejčastější aplikační protokoly pro získání obsahu z komunikace.
- Filtrování a vyhledávání v obsahu zachycené komunikace.

NFX Detective představuje rozšiřitelnou platformu přizpůsobitelnou specifickým požadavkům.

- Možnost vytvoření nových extraktorů pro další aplikační protokoly. Toto vyžaduje definici syntaxe/formátu protokolu a mapování sémantiky.
- Možnost přidání plugins pro implementaci specifických analytických metod, které mohou přistupovat ke všem datových zdrojům v prostředí.
- Možnost definice nových pohledů na data. Data jsou uložena v databázi a jsou zpřístupněna přes jednotné rozhraní.

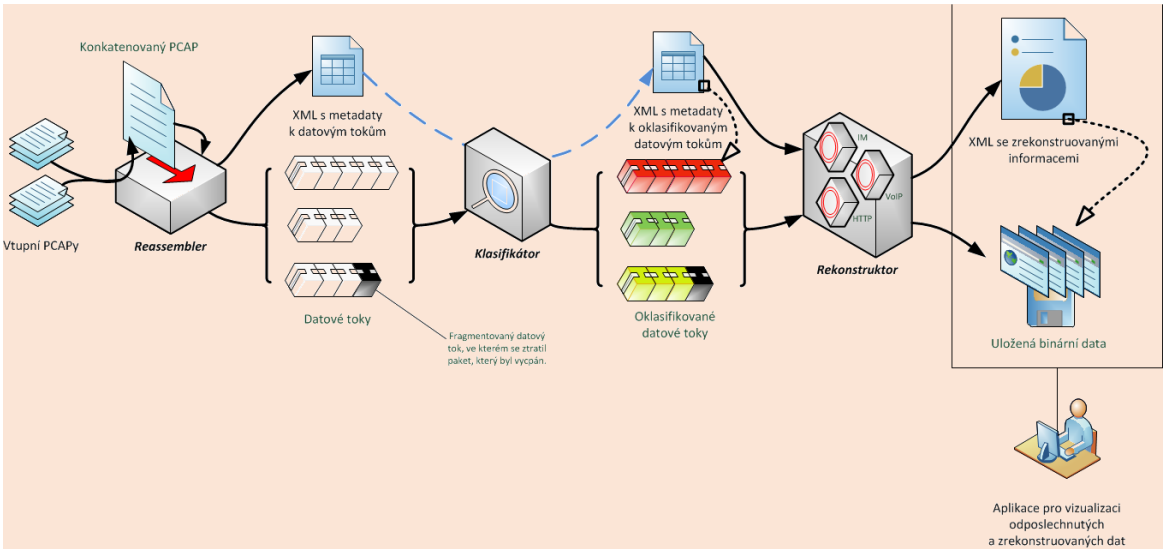
NFX Detective implementuje funkcionalitu potřebnou pro zpracování PCAP souborů až po rekonstrukci obsahu zachyceného provozu. Toto zahrnuje několik komponent, které realizují jednotlivé kroky zpracování:

- Zpracování PCAP souborů a nalezení konverzací (obousměrná komunikace mezi koncovými uzly): V případě, že zachycená komunikace je kompletní a pakety nejsou duplikovány, je tento krok triviální. Na základě údajů o cílových adresách a použitých transportních portech a protokolu jsou identifikovány jednotlivé konverzace a jednotlivé pakety jsou uspořádány v rámci konverzace. Složitější je situace, kdy je nutné zpracovávat data, která jsou neúplná, obsahují duplicity, či poškozené pakety. V nástroji NFX Detective jsou implementovány mechanismy, které dokáží s vysokou přesností detekovat konverzaci i pro neúplné datové toky. V tabulce X je srovnání s existujícími nástroji. PCAP soubor obsahuje 126 konverzací. Naměřené hodnoty jsou pro různou hodnoty ztracených paketů. Jak je vidět, při větší ztrátě paketů dochází k tomu, že nástroje detekují původně jednu konverzaci jako dvě odlišné konverzace.

File	NFX Det	Wireshark	MS Monitor	NetWitness	Net Miner
0% missing	126	126	132	128	76
1% missing	126	126	132	128	75
5% missing	129	125	129	127	71
10% missing	131	125	129	127	66

- Identifikace aplikačního protokolu: Pro správnou analýzu komunikace a extrakci informací je důležité správně určit aplikační protokol. V nástroji Netfox Detective se pro určení aplikačního protokolu pro jednotlivé konverzace používá kombinací několika metod: (1) identifikace známých služeb na základě vyhrazených čísel komunikačních portů, (2) fingerprinting pro identifikaci RTP konverzací, (3) statistických metod pro identifikaci šifrované konverzace nebo konverzací na nevyhrazených portech.
- Parsování obsahu aplikačních protokolů: Dle identifikované aplikace je na konverzaci použit aplikační parser, který získává data z komunikace pro jejich zobrazení uživateli nebo další analýzu Příkladem může být analýza WebMail komunikace, kdy HTTP parser je použit pro získání obsahu HTTP komunikace a její následnou rekonstrukci pomocí WebMail analyzátoru specifického pro konkrétní službu. V současné době jsou podporovány služba gmail.com, seznam.cz/email.cz, yahoo.cz, centrum.cz, Roundcube a Horde.
- Šifrovaný provoz: velká část Internetového provozu je šifrována s použitím SSL/TLS. Nástroj podporuje dešifrování této komunikace v případě znalosti privátní klíče serveru. Tento je nástrojem použit pro vygenerování session klíče a následnému dešifrování SSL/TLS datového kanálu a jeho zpřístupnění analytikovi.
- Speciální použití: nástroj je možné vybavit doplňky pro analýzu specifických aplikací. Jednou z nich je možnost analyzovat BitCoin protokol. Analýzou tohoto protokolu je možné získat informace o uzlech podílejících se na transakcích, těžících bitcoiny, popřípadě vytvořit graf Bitcoin uzlů.

Způsob zpracování vstupních dat nástroje je ukázán na následujícím obrázku:



Demonstrace funkčnosti

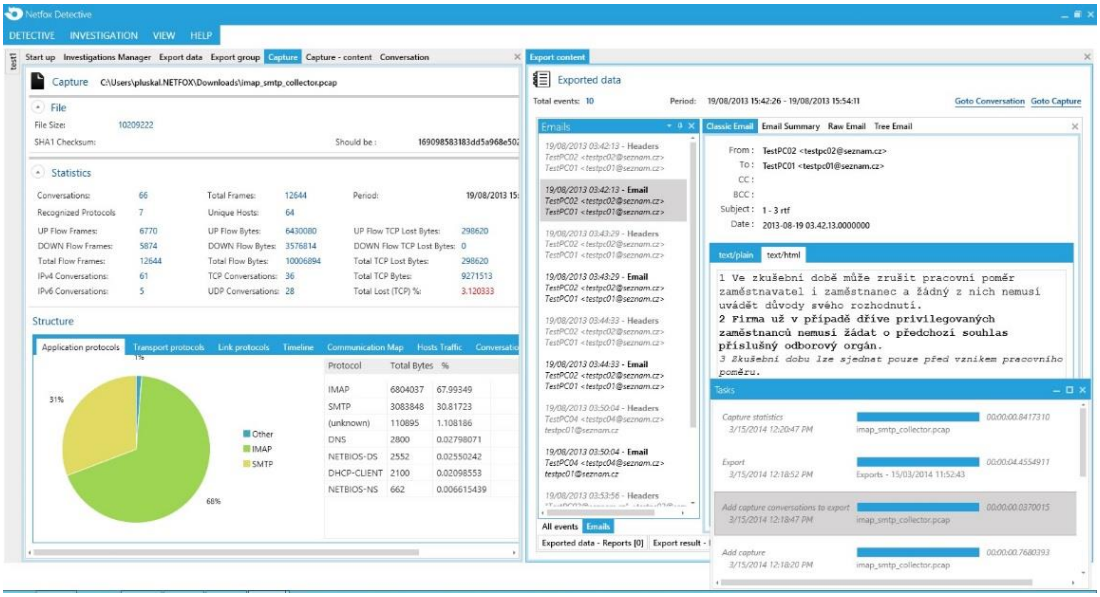
Vytvořený nástroj je softwarovým produktem, který je k dispozici ve formě instalačního balíčku pro platformu Microsoft Windows. Tento instalační balíček je dostupný na stránkách nástroje (http://netfox.fit.vutbr.cz/). Nástroj pro svůj běh vyžaduje Windows 7 a novější, prostředí minimálně

.NET 4.5 a odpovídající hardwarovou konfiguraci. Pro otestování bez nutnosti instalaci je připraven obraz operačního systému s předinstalovaným nástrojem.

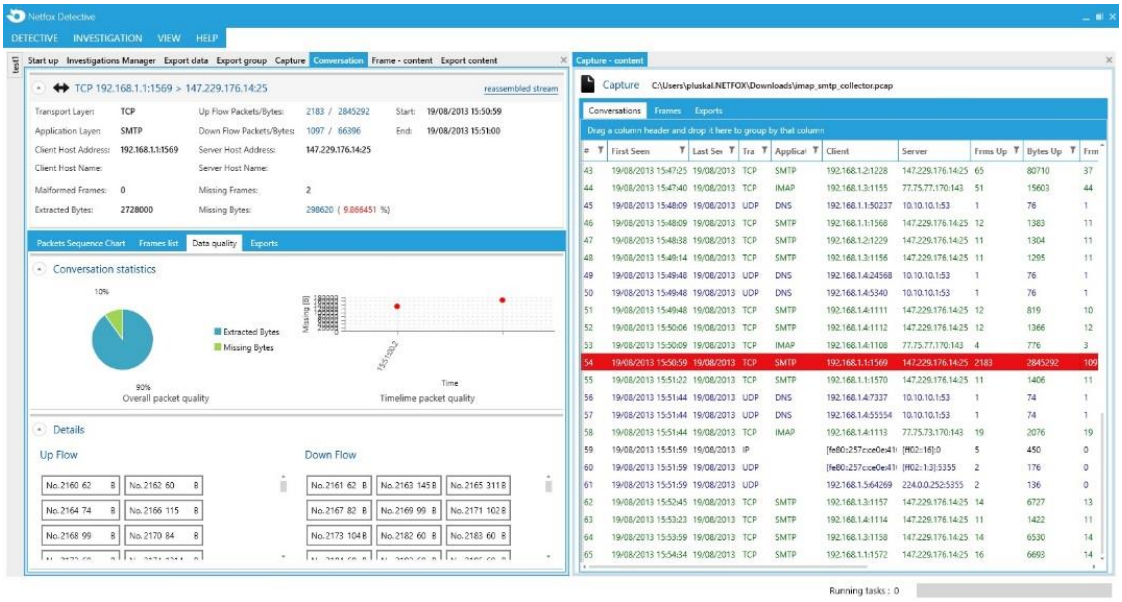
Další informace k vytvořenému produktu je možné najít na http://www.fit.vutbr.cz/research/prod/index.php?id=440&notitle=1.

Ukázky výstupů analýzy jsou na následujících obrázcích:

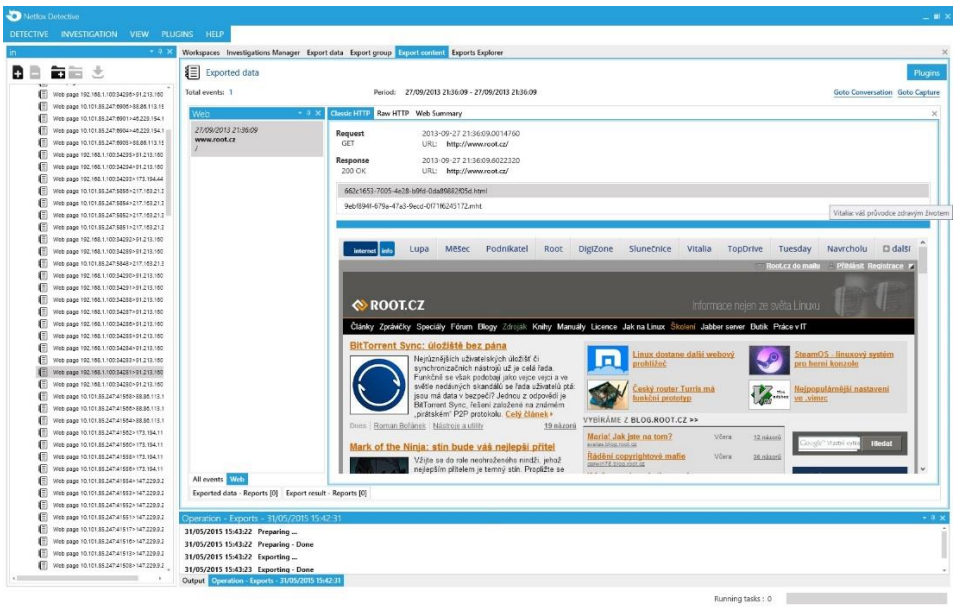
- Zpracování emailové komunikace



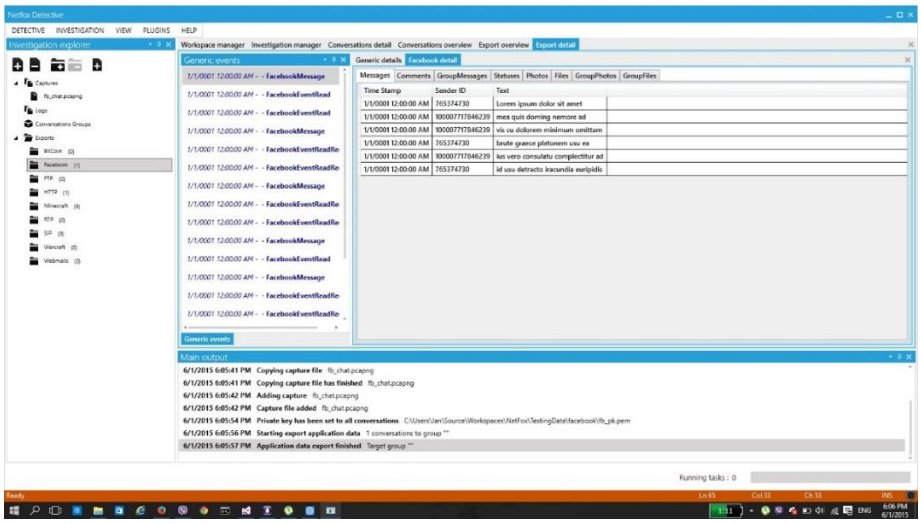
- Přehled detekované a exportované emailové komunikace



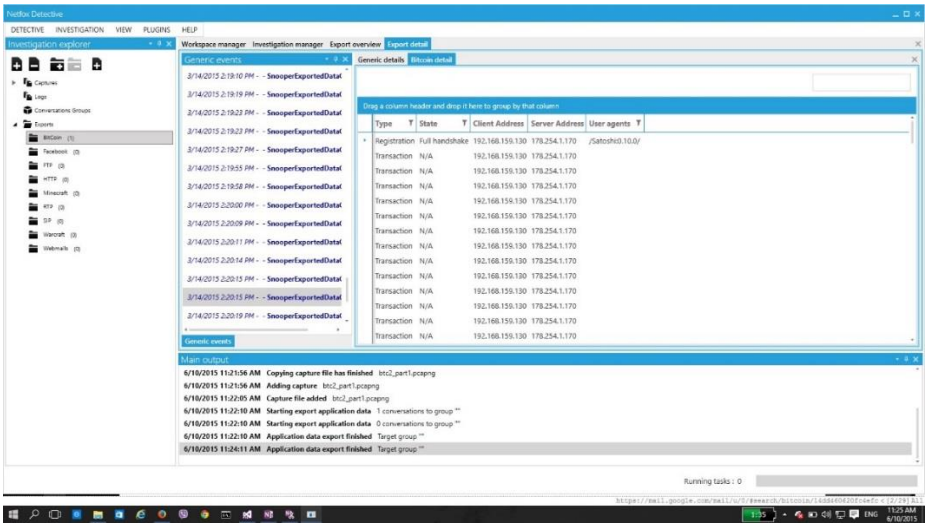
- Zpracování webových dat



- Zpracování komunikace přes Facebook



- Analýza komunikace Bitcoin



Související neplánované výsledky

- PLUSKAL Jan, MATOUŠEK Petr, RYŠAVÝ Ondřej, KMEŤ Martin, VESELÝ Vladimír, KARPÍŠEK Filip and VYMLÁTIL Martin. Netfox Detective: A tool for advanced network forensics analysis. In: Proceedings of Security and Protection of Information (SPI) 2015. Brno: Brno University of Defence, 2015, pp. 147-163. ISBN 978-80-7231-997-8.
- PLUSKAL Jan, RYŠAVÝ Ondřej and VESELÝ Vladimír. NetFox - The network forensic extandable analysis tool. In: 6th AFCEA Student Conference Future of Information and Communication Technology. Bucharest: University Politehnica of Bucharest, 2014, pp. 68-71. ISBN 978-606-551-047-0.
- MATOUŠEK Petr, RYŠAVÝ Ondřej a KMEŤ Martin. Fast RTP Detection and Codecs Classification in Internet Traffic. The Journal of Digital Forensics, Security and Law. 2014, roč. 2014, č. 2, s. 99-110. ISSN 1558-7215.
- MATOUŠEK Petr, RYŠAVÝ Ondřej, GRÉGR Matěj a VYMLÁTIL Martin. Towards Identification of Operating Systems from the Internet Traffic. IPFIX Monitoring with Fingerprinting and Clustering. In: DCNET2014. Proceedings of the 5th International Conference on Data Communication Networking. Wien: SciTePress - Science and Technology Publications, 2014, s. 21-27.
- PLUSKAL Jan, RYŠAVÝ Ondřej a VESELÝ Vladimír. NetFox - The network forensic extandable analysis tool. In: 6th AFCEA Student Conference Future of Information and Communication Technology. Bucharest: University Politehnica of Bucharest, 2014, s. 68-71. ISBN 978-606-551-047-0.
- PLUSKAL Jan. NetFox.Framework - The network forensic extandable analysis tool. In: Proceedings of the 20th Conference STUDENT EEICT 2014 Volume 2. Brno: Vysoké učení technické v Brně, 2014, s. 280-282. ISBN 978-80-214-4923-7.
- VESELÝ Vladimír. Rozšíření porovnávací studie o spojování PCAP souborů. ElectroScope. Plzeň: Západočeská univerzita v Plzni, 2012, roč. 2012, č. 5, s. 1-6. ISSN 1802-4564.
- VESELÝ Vladimír. Srovnávací studie spojování PCAP souborů. In: Proceedings of the 18th Conference Student EEICT 2012 Volume 3. Brno: Fakulta informačních technologií VUT v Brně, 2012, s. 457-461. ISBN 978-80-214-4462-1.
- HTTP ReconProxy - Nástroj pro cachování provozu za účelem následné rekonstrukce, software, 2012, viz http://www.fit.vutbr.cz/research/prod/index.php?id=277&notitle=1
- S6N vizualizátor zachyceného obsahu, viz http://www.fit.vutbr.cz/research/prod/index.php?id=333&notitle=1
- Netfox.Framework - Nástroj pro zpracování obsahu zachyceného provozu, viz http://www.fit.vutbr.cz/research/prod/index.php?id=344&notitle=1
- Detektor provozu RTP, viz http://www.fit.vutbr.cz/research/prod/index.php?id=343&notitle=1
- Databáze vzorků VoIP komunikace s různými kodeky, viz http://www.fit.vutbr.cz/research/prod/index.php?id=386&notitle=1

Aktuálnost výsledku a použití v praxi

Pokročilá forenzní analýza jak surových (záchyty komunikace, NetFlow, logy atp.), tak výsledných dat (rekonstruovaný provoz, incidenty) je náročná a bez vizualizace problematická. V současné době lze pro tyto účely využít různé jednoúčelové, často volně dostupné, nástroje, které řeší pouze dílčí problematiku. Tyto nástroje realizují standardní přístup, tedy umožňují zachytávat a analyzovat PCAP soubory s různým stupněm automatizace jednotlivých kroků. Pro pokročilou vizuální analýzu existuje komerční prostředí IBM I2. Toto prostředí je velmi komplexní nástroj pro analýzu a vizualizaci různorodých dat. Jedním z možného použití je i vizualizace dat síťové forenzní analýzy. V tomto případě je nutné prostředí rozšířit o příslušné moduly pro cílovou doménu. Vzhledem licenční politice je nutné při použití IBM I2 počítat s vyšší cenou výsledného řešení. Navíc, prostředí IBM I2 obsahuje množství funkcionality, která může být pro cílovou doménu nerelevantní. Problematická je také vlastní integrace řešení s ohledem na snadnou

použitelnost a další rozšiřitelnost. Na druhé straně se nachází open source nástroje. Jedním z nejznámějších nástrojů pro analýzu síťové komunikace je nástroj Wireshark. Tento nástroj umožňuje zobrazení obsahu přenášených paketů. Vzhledem k délce vývoje a aktivní komunitě jsou podporovány prakticky všechny dnes používané komunikační protokoly. Tento nástroj však není přímo určen jako ucelené řešení pro forenzní analýzu, neboť neobsahuje pokročilé analytické a vizualizační funkce. Nástroj je také svou podstatou zaměřen pouze na analýzu zachyceného síťového provozu a jeho funkcionalita je pro potřeby forenzní analýzy zmiňovaných dat nedostatečná. Výsledkem řešení je softwarová platforma síťové forenzní analýzy. Platforma je přizpůsobitelná různým specifickým potřebám v oblasti síťové forenzní analýzy. Efektivní zpracování dat je založeno na principu spolupráce mezi analytiky a integrace automatických analytických metod. Zpracování dat na nejnižší úrovni je tak do maximální možné míry automatizováno, například generováním anotací pro vstupní data.

Přínos pro uživatele

Nástroj pro forenzní analýzu síťové komunikace je určen především bezpečnostním analytikům, kteří potřebují efektivně zpracovávat velké množství dat z proběhlých bezpečnostních incidentů. Přínos nástroje pro jednotlivé oblasti použití je následující:

- Bezpečnostní administrátoři počítačových sítí mohou využít nástroj pro získání přehledu o situaci v rámci sítě, vytvoření baseline komunikace a případně pro detekci možných bezpečnostních problémů v síti.
- CERT týmy a bezpečnostní analytici mají zájem o nástroj, který bude umožňovat zpracovávat data ze zařízení pro monitorování a zabezpečení sítí s cílem analyzovat okolnosti bezpečnostních incidentů, odhadnout rozsah možné škody, detekovat slabá místa v systému a navrhnout protiopatření, případně zajistit důkazy celého incidentu.
- Zpravodajské služby a bezpečnostní složky mají zájem primárně o nástroj, pomocí kterého mohou analyzovat data ze zachycené komunikace. Zde se primárně jedná o efektivní metody pro identifikaci případu a nalezení důkazů v dostupných datech.

Ve všech případech platí, že základem je zde nástroj, který by byl přizpůsobitelný konkrétním požadavkům zákazníka. Různé agentury a bezpečnostní týmy pracují odlišným způsobem a preferují jiné analytické postupy a způsoby prezentace informací. Je tedy nutné vytvoření nástroje s akceptovatelnou cenou, který by se přizpůsobil potřebám konkrétních zákazníků. Navržená platforma integruje důležité přístupy a umožňuje modifikaci dle konkrétních požadavků. Vytvořený výstup je základní verzí nástroje, který je možné doplňovat o další funkcionalitu a přizpůsobovat jej konkrétním požadavkům.

7. Akcelerovaný nástroj pro obnovu hesel dokumentů Wrathion

Popis výsledku

Wrathion je nástroj pro nalezení hesla, které je použito pro zabezpečení přístupu k dokumentu. Jako základní metodu používá postupné generování a ověřování hesla pomocí nastavených parametrů. Volitelně je možné rozšířit nástroj o heuristiky, které definují odlišný způsob generování hesel, například slovníkový přístup, nebo generování hesla pomocí gramatiky.

Wrathion má následující parametry:

- podporuje celou řadu formátů, například DOX, PDF, ZIP, RAR
- má otevřenou architekturu a je tedy možné přidat podporu pro další formáty
- je přenositelný na různé OS, Linux, WIndows, MAC OS X
- používá GPU pro akceleraci hledání hesla

- podporuje hledání hesla pro PDF až do verze 5

Nástroje je postupně rozvíjen. Jsou přidávány další podporované formáty a pro existující formáty je přidávána podpora pro různé verze.

Demonstrace funkčnosti

Vytvořený nástroj je softwarovým produktem, který je k dispozici na vyžádání ve formě binárních souborů pro požadovanou platformu. Pro svůj běh vyžaduje hardware, který odpovídá standardům v době vytvoření nástroje. Pro použití GPU akcelerace je nutné mít kompatibilní grafickou kartu. Více informací je uvedeno v manuálu k nástroji.

Podrobné informace k nástroji lze najít na webové stránce http://www.fit.vutbr.cz/research/prod/index.php?id=441&notitle=1.

Související neplánované výsledky

- MATOUŠEK Petr, HRANICKY Radek, RYŠAVÝ Ondřej and VESELÝ Vladimír. EXPERIMENTAL EVALUATION OF PASSWORD RECOVERY IN ENCRYPTED DOCUMENTS. Submitted to:SADFE'15, Malaga, SPAIN, 2015.
- Akcelerovaný nástroj pro obnovu hesel dokumentů (softwarová verze), viz http://www.fit.vutbr.cz/research/prod/index.php?id=402&notitle=1

Aktuálnost výsledku a použití v praxi

Vytvořený výsledek je použitelný pro hledání hesel zabezpečených dokumentů pro účely získání jejich obsahu v rámci forenzních aktivit. Nástroj je výkonnostně srovnatelný s obdobnými nástroji, například John the Ripper a nástroji z Elcomsoft Password Recovery Bundle. Z provedených experimentů vyplývá, že nástroje je schopen nalézt libovolné heslo z běžně používané abecedy (63 znaků) pro PDF verze 5 o délce maximálně 8 znaků nejdéle za 60,5 hodiny. Vzhledem k tomu, že podle publikovaných studií 65% hesel je složeno z maximálně 8 znaků, je tento nástroj použitelný pro získání obsahu z více než poloviny zachycených dokumentů.

Přínos pro uživatele

Nástroj pro hledání hesla k zabezpečenému dokumentu je určen primárně pro zpravodajské agentury a bezpečnostní složky, které potřebují hledat důkazy v zachycených datech. Nástroj poskytuje možnost podívat se do obsahu zabezpečeného dokumentu.

Ve všech případech platí, že základem je zde nástroj, který by byl přizpůsobitelný konkrétním požadavkům zákazníka. Různé agentury a bezpečnostní týmy pracují odlišným způsobem a preferují jiné analytické postupy a způsoby prezentace informací. Je tedy nutné vytvoření nástroje s akceptovatelnou cenou, který by se přizpůsobil potřebám konkrétních zákazníků. Navržená platforma integruje důležité přístupy a umožňuje modifikaci dle konkrétních požadavků. Vytvořený výstup je základní verzí nástroje, který je možné doplňovat o další funkcionalitu a přizpůsobovat jej konkrétním požadavkům.

8. Paketový filtr pro síťový provoz s rychlostí 100 Gb/s

Popis výsledku

Výsledek implementuje proces filtraci paketů tak, aby byla dosažena propustnost dat 100 Gb/s. Dále filtr zajišťuje rychlou a atomickou změnu filtračních pravidel a efektivně využívá dostupnou paměť. Cílovou platformou je FPGA. Princip filtrace spočívá v kombinaci tzv. kukaččí hash a binárního prefixového stromu. Filtr podporuje vyhledání IPv4 a IPv6 adres a dále vyhledání IPv4 či IPv6 prefixů určitých pevných délek. Díky binárnímu prefixovému stromu jsou podporovány i prefixy jakýchkoliv délek.

Demonstrace funkčnosti

Díky tomuto filtru je možné rozhodovat o zahození či přijetí paketu na rychlosti 100 Gb/s. Výsledky měření parametrů filtru byly publikovány v článku Fast Lookup for Dynamic Packet Filtering in FPGA na mezinárodní konferenci DDECS. Filtr je obsažen v Prototypu vysokorychlostní sondy pro monitorování IPv6 provozu, čímž je demonstrována jeho praktická využitelnost a funkčnost. Měření propustnosti filtru je tedy obsaženo v měření propustnosti Prototypu vysokorychlostní sondy pro monitorování IPv6 provozu, který je k dispozici zde: https://merlin.fit.vutbr.cz/wiki-sec6net/index.php/File:Tr.pdf Zpráva ukazuje, že karta COMBO-100G s firmwarem, který obsahuje Paketový filtr pro síťový provoz s rychlostí 100 Gb/s, dosahuje propustnosti 100 Gb/s na všech paketových délkách. Implementace filtru je dostupná zde: http://www.fit.vutbr.cz/research/view_product.php?id=369

Související neplánované výsledky

- KEKELY Lukáš, ŽÁDNÍK Martin, MATOUŠEK Jiří a KOŘENEK Jan. Fast Lookup for Dynamic Packet Filtering in FPGA. In: 17th IEEE Symposium on Design and Diagnostics of Electronic Circuits and Systems. Warszawa: IEEE Computer Society, 2014, s. 219-222. ISBN 978-1-4799-4558-0.
- Hardware accelerated packet filter for 100Gbps, technická zpráva, FIT VUT v Brně, 2014.

Aktuálnost výsledku a použití v praxi

Paketový filtr byl využit jako součást Prototypu vysokorychlostní sondy pro monitorování IPv6 provozu. Výsledek je velmi aktuální, neboť v současné době začíná probíhat obměna síťových propojení právě na 100 Gb/s technologii. Je tedy nutné zajistit filtraci paketů na této rychlosti, kdy mezi začátky dvou po sobě následujících nejkratších paketů je interval menší než 7 ns.

Přínos pro uživatele

Filtr umožňuje bez ztráty paketu filtrovat provoz na rychlosti 100Gb/s a díky tomu, je možné filtr použít ve firmware síťových karet obsahujících FPGA, zachytit zájmový provoz bez ztráty paketu. V roce 2015 začíná být 100 Gb/s technologie nasazována v datových centrech, agregovaných linkách operátorů a velkých poskytovatelů připojení k Internetu.