PORTATION OF LAWFUL INTERCEPTION SYSTEM TO MICROPROBE

Jan Dražil
Bachelor Degree Programme (3), FIT BUT
E-mail: xdrazi00@stud.fit.vutbr.cz

Supervised by: Jan Viktorin
E-mail: iviktorin@fit.vutbr.cz

Abstract: The Microprobe is an embedded device for intercepting of network communication. It is a part of the Sec6Net Lawful Intercept System (SLIS). It would be useful to run the Microprobe as a standalone device. Without it, the microprobe requires connection to SLIS infrastructure which is a prerequisite to run the Microprobe. The goal of this paper is to describe ways how to transfer SLIS to the Microprobe architecture.

Keywords: Microprobe, SLIS, Lawful Intercept

1 ÚVOD

Spáchání zločinu v kybernetické sféře je v dnešní době na denním pořádku a pro jejich stíhání je potřeba mít důkazy. Mikrosonda je zařízení, které odposlouchává komunikaci na síti, ke které je připojena, a vybranou komunikaci předává dál ke zpracování. Aktuálně je Mikrosonda součástí SLIS (Sec6Net Lawful Interception System[2]) a nelze ji použít jako samostatné zařízení. To vede k důvodům zabývat se přenesením tohoto systému na Mikrosondu.

2 SYSTÉM PRO ZAKONNÉ ODPOSLECHY

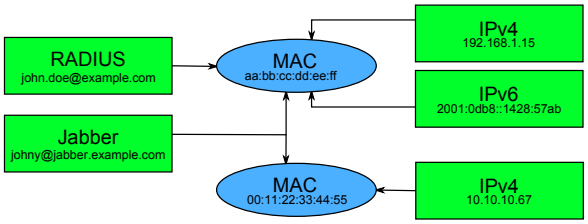
Architektura SLIS vychází z referenčního modelu ETSI[1]. Obrázek č. 2 zobrazuje funkční bloky SLIS a jejich vzájemné propojení.

SLIS obsahuje uživatelské prostředí, přes které je možné vkládat požadavky na odposlech, které obsahují kdo a v jakém časovém rozmezí bude odposloucháván. Úlohou Administrační funkce (AF) je převzít požadavky na odposlech a vložit je do fronty neaktivních požadavků, kde čekají na zahájení odposlechu. Ve chvíli, kdy má být odposlech zahájen je požadavek na odposlech vyjmut z fronty neaktivních požadavků a zařazen do fronty aktivních požadavků a ostatním částem systému jsou zaslány potřebné příkazy pro zahájení odposlechu. Při ukončení odposlechu je požadavek vyřazen z aktivní fronty a jsou rozeslány příkazy pro ukončení odposlechu ostatním částem systému.

Funkce dynamické identity (IRI-IIF) slouží k identifikaci odposlouchávaného zařízení, její úlohou je sledovat všechny zprávy spojené s identitou komunikujícího. Sleduje například uživatelské jméno k RADIUS serveru, změnu IP adresy prostřednictvím DHCP, apod. IRI-IIF se skládá z modulů, každý modul zpracovává jeden protokol. Na základě zpráv, které jsou posílány z modulů, je sestavován graf identit. Graf se skládá z MAC adres, ke kterým je přidělena IP adresa a případně známá uživatelská jména podporovaných protokolů, viz obrázek č.1.

Zařízení, které zajišťuje odposlech a filtraci komunikace, je např. Mikrosonda. V SLIS je Mikrosonda označována jako Funkce odposlechu komunikace (CC-IIF).

Mediační funkce (MF) je centrální složkou SLIS, přijímá informace o identitách, požadavky na odposlech předává sondám a přijímá odposlechnutou komunikaci. Informace o identitách od IRI-IIF trans-



Obrázek 1: Ukázka grafu identit

formuje do uživatelsky přívětivého formátu. Z těchto dat lze následně snadno vyčíst, jak se v průběhu odposlechu identita měnila. MF získává od sond odposlechnutou komunikaci a transformuje ji do souborů ve formátu PCAP[1]. Součástí MF je Triggerovací funkce (CCTF). Její úlohou je rozesílání zpráv připojeným sondám k SLIS. Zprávy obsahují rozsahy IP adres, které mají být odposlouchávány. Pro správnou funkčnost CCTF potřebuje znát, v jakých bodech sítě jsou jednotlivé sondy umístěny.

3 MIKROSONDA

Mikrosonda je vestavěné zařízení, které vybírá ze síťového provozu v počítačové síti pouze komunikaci, která vyhovuje filtrovacím pravidlům. Filtrovací pravidla jsou mikrosondě doručovány od CCTF. Jádrem Mikrosondy je FPGA. Hlavní část FPGA firmwaru je tvořena soft-procesorem Microblaze[3] a filtrační jednotkou. Microblaze nabízí jen omezený výpočetní výkon, avšak z pohledu SLIS slouží pouze ke konfiguraci filtrační jednotky.

4 PORTACE SYSTÉMU

Mikrosonda je silně závislá na ostatních částech SLIS, od kterého získává filtrovací pravidla. Důvodem portace je získání nezávislosti Mikrosondy na připojení k SLIS. Po portaci bude možné provozovat odposlechy i v místech, kde se nelze připojit k jiné než odposlouchávané lince. Celý systém je příliš náročný pro výpočetní výkon procesoru Microblaze, proto budou portovány pouze vybrané funkce SLIS.

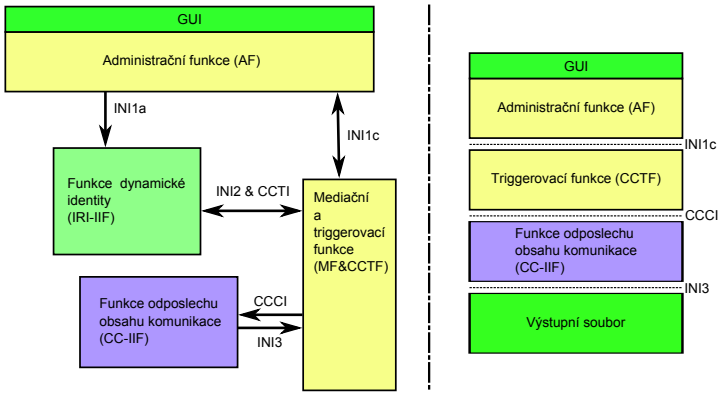
Funkci, kterou je potřeba přenést na Mikrosondu je AF, protože zajišťuje správu požadavků na odposlech. AF by měla být konfigurovatelná tak, aby bylo možné stále zapojit Mikrosondu do SLIS. Také by měla podporovat i běh, kdy nebude připojena k žádné síti, přes kterou by mohla komunikovat. To lze zařídit tak, že Mikrosonda bude schopná pracovat ve dvou režimech. První bude označovat stav, kdy pracuje samostatně, bude to tzv. standalone zařízení. V tomto režimu bude možné vkládat požadavky na odposlechy manuálně přímo na Mikrosondě. V druhém režimu bude možné pouze nakonfigurovat rozhraní pro připojení k SLIS a ruční zadávání přímo na Mikrosondě nebude umožněno.

Podstatnou funkcí SLIS je IRI-IIF. V rámci této funkce běží paralelně jednotlivé moduly na rozpoznání protokolů, podle kterých lze určit identitu. Do modulů se posílá celá komunikace, ze které se vybírají právě ty pakety, které jsou pro ně určeny. Například pokud jsou aktivní 3 moduly, pak jeden paket je zpracován třikrát. Tento přístup nelze použít na Mikrosondě, protože takový objem dat nemůže zpracovat dostatečně rychle tak, aby nedocházelo k zaplnění vstupní fronty a pakety nebyly zahazovány.

Problém lze vyřešit přidáním FIFO fronty do FPGA. Filtrační jednotka, která již v FPGA je, by do fronty vkládala pouze pakety obsahující informace o identitě. Řešení vyžaduje přidat značné množství logiky do firmwaru, která by zajistila rozpoznání protokolů na různých vrstvách ISO OSI.

Z výše zmíněných důvodů není vhodné IRI-IIF na Mikrosondu portovat. V režimu standalone bude

[1] http://www.tcpdump.org/pcap/pcap.txt



Obrázek 2: Architektura systému SLIS před portací (vlevo) a po portaci (vpravo)

Mikrosonda schopna filtrovat provoz pouze na základě staticky definovaných IP adres. Na Mikrosondu stačí přenést pouze část MF, protože není nutné zpracovávat zprávy z IRI-IIF. Převod do formátu PCAP není okamžitě po odchycení potřeba a lze jej provést až v době zpracování odchycené komunikace, proto bude odchycená komunikace zapsána z filtrační jednotky přímo do výstupního souboru, který se bude nacházet na lokálně dostupném úložišti. Příkladem úložiště může být externí HDD připojený přes USB, které je dostupné na Mikrosondě.

Potřebná část MF pro funkčnost Mikrosondy je CCTF. Ta zajistí správnou konfiguraci filtrovací jednotky na Mikrosondě. V této variantě není potřeba znát umístění sond v síti, protože vždy bude konfigurace probíhat pouze na konkrétní Mikrosondě.

5 ZÁVĚR

Po portaci vybraných částí SLIS na Mikrosondu je možné používat ji jako samostatné zařízení. Na rozdíl od zapojení v SLIS nebude možné rozpoznávat zařízení pomocí uživatelských jmen, ani nebude možné sledovat změnu IP adresy odposlouchávaného zařízení.

Nyní je ve vývoji nová generace Mikrosondy na platformě NetModule ZE7000[2], která obsahuje procesor ARM Cortex-A9. Na tuto platformu by již mělo být možné přenést více funkcí SLIS. Jednalo by se hlavně o IRI-IIF, čímž by bylo možné sledovat identitu odposlouchávaných.

PODĚKOVÁNÍ

Tento článek vznikl za podpory projektu VG20102015022 podporovaného Ministerstvem vnitra ČR a za podpory projektu VUT v Brně FIT-S-14-2297.

REFERENCE

[1] European Telecommunications Standards Institute: *ETSI TR 101 943. Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture*. 2006, version 2.2.1.

[2] Polčák, L.; Kramoliš, P.; Kajan, M.; aj.: Architektura systému pro zákonné odposlechy. Technická zpráva, 2011.

[3] Xilinx; Inc.: MicroBlaze Processor Reference Guide - Xilinx User Guide UG081. 2011, version 13.3.

[2] http://www.netmodule.com/products/sbc-eval-sys/ZE7000.html