ADDITIONS TO LAWFUL INTERCEPTION SYSTEM

Radek Hranický
Master Degree Programme (2), FIT BUT
E-mail: xhrani00@stud.fit.vutbr.cz

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

Abstract: As a part of Sec6Net project, a Lawful Interception System was developed. This paper describes an extension of the system, which provides a capability to intercept application protocols (e.g. an e-mail communication) directly in a network of an Internet service provider. This new functionality enables to detect and filter out a related TCP transfer automatically. It is also able to handle situations, where the identity (an IP address) of a target user is not known yet, or when it is difficult to detect it (NAT is enabled, user is at an Internet café, etc.).

Keywords: Lawful Interception System, Dynamic user identification, Network event analysis, Administration and control of interceptions, Packet recording and classification

1 ÚVOD

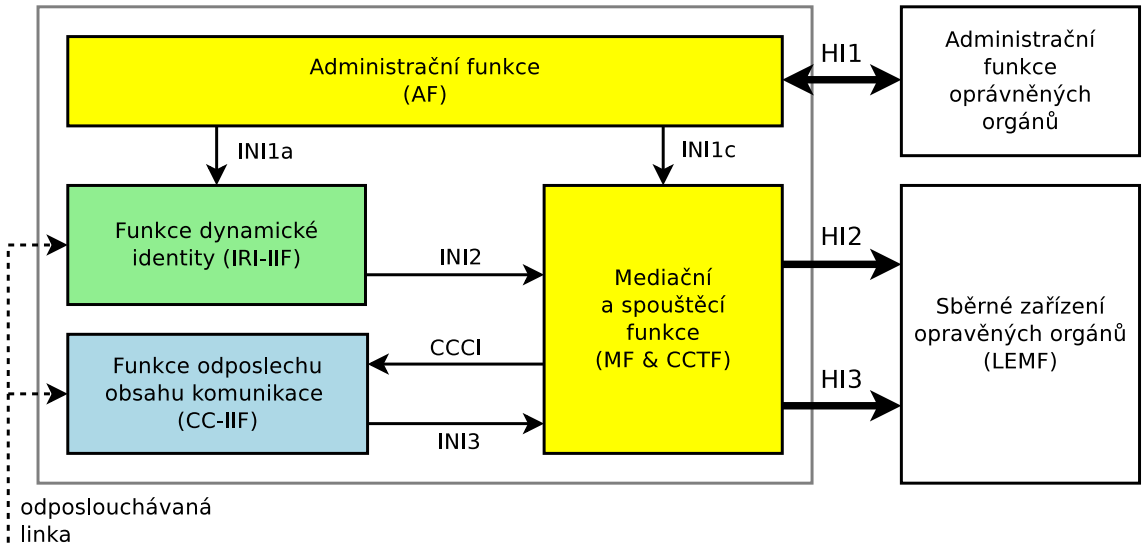
Systém pro zákonné odposlechy (*Lawful Interception System - LIS*) je nástroj, který umožňuje oprávněným orgánům sledovat komunikaci podezřelých subjektů v počítačové síti [1]. V rámci projektu *Moderní prostředky pro boj s kybernetickou kriminalitou na internetu nové generace* (Sec6Net) byl vytvořen prototyp LIS: *Sec6Net Lawful Interception System* - SLIS. Systém umožňuje sledovat aktivitu vybraného cíle včetně dynamické změny jeho identity v čase. Je schopen zachycovat, filtrovat a ukládat jak obsah komunikace, tak metadata o komunikaci (dobu přenosu, identifikace komunikujících stran, apod.)

2 PODPORA APLIKAČNÍCH PROTOKOLŮ

Dosavadní implementace umožňovala specifikovat cíl zájmu pomocí IP adresy, MAC adresy síťového rozhraní a několika dalších identifikátorů. Pro praktické použití je často vhodné speficikovat cíl formou identifikátoru aplikační vrstvy (např. pomocí e-mailové adresy) a mít možnost zachytit komunikaci v rámci konkrétního aplikačního protokolu. Normy ETSI [1] však takový odposlech definují pouze na straně poskytovatelů služeb (např. gmail.com), kteří často působí mimo ČR. Řešením je odposlech aplikačních protokolů přímo v síti národních poskytovatelů připojení.

Strukturu systému znázorňuje obrázek 1. Požadavek na odposlech je předáván přes rozhraní HI1 *Administrační funkci* (AF), která konfiguruje zbytek systému [2]. Zachycení zájmových dat provádí *Funkce odposlechu obsahu komunikace* (CC-IIF), která je schopna realizovat odposlech zadané IP adresy, resp. rozsahu IP adres. Cílem *Mediační a spouštěcí funkce* (MF&CCTF) je konfigurace bloku CC-IIF skrz rozhraní CCCI, kategorizace zachycených dat a jejich předávání do příslušného sběrného zařízení oprávněných orgánů. Pro úspěšnou realizaci odposlechu je nutné detekovat identitu (IP adresu) cíle. Je třeba také uvažovat, že identita cíle se může měnit (např. přiřazení nové IP adresy serverem DHCP) [3]. Nalezení IP adresy cíle je úkolem *Funkce dynamické identity* (IRI-IIF).

IRI-IIF se skládá z jádra a modulů pro zpracování různých protokolů (např. modul pro DHCPv6, Instant Messaging, apod.). Moduly sledují události na síti a informují o nich jádro. Cílem jádra je uchovávat stav sítě a na základě něj detekovat identitu požadovaných cílů (uživatelů v síti).



Obrázek 1: Struktura systému SLIS

V rámci této práce jsem provedl novou implementaci jádra IRI-IIF. Stav sítě je uchováván ve formě grafové reprezentace, jejíž příklad ukazuje obrázek 2. Uzly grafu jsou síťové identifikátory, hrany označují protokoly z nichž byla vazba mezi identifikátory odvozena. Událost na síti (přidělení IP adresy, přihlášení k serveru, apod.) může znamenat přidání nebo odebrání uzlu. Prohledáváním grafu jsou nalezeny všechny známé identifikátory související s daným cílem. Nová implementace jádra IRI-IIF uvažuje kromě stávajících (především L2 a L3) identifikátorů také identifikátor TCP spojení a identifikátory některých protokolů pro Instant Messaging (XMPP, YMSG, OSCAR a Jabber). V budoucnu je plánováno přidání podpory protokolů pro IP telefonii a dalších.

Při současném návrhu je systém SLIS schopen identifikovat zájmový provoz i v situaci, kdy ještě neznáme identitu cíle (IP adresu) nebo v případech kdy identitu nelze snadno zjistit (např. probíhá překlad adres – NAT: uživatel je v knihovně, internetové kavárně, aj.) [2].

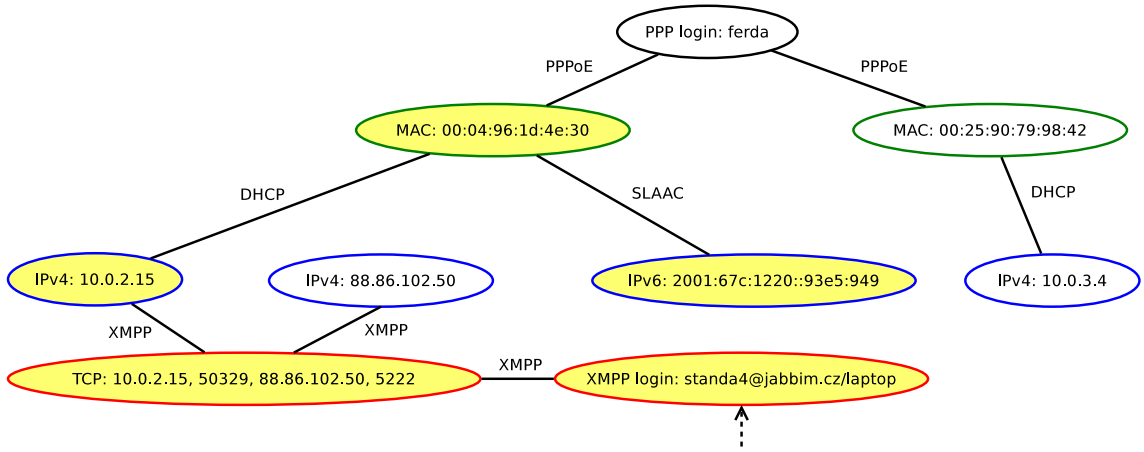
Až dosud blok IRI-IIF detekoval jako cíl odposlechu pouze konkrétní IP adresu, resp. rozsah IP adres. S novým rozšířením však může být cílem i konkrétní TCP spojení. Pro účely podpory aplikačních protokolů jsem tedy musel upravit také blok MF&CCTF. Do tohoto bloku jsem přidal podporu kategorizace zachycených dat a konfigurace odposlechů také na základě identifikátorů TCP spojení. Dále jsem musel upravit rozhraní CCCI a blok CC-IIF, kde jsem implementoval možnost filtrace dat spadajících do konkrétního TCP toku.

3 KONFIGUROVATELNÉ ÚROVNĚ ODPOSLECHŮ

S ohledem na různé typy soudních povolení je také potřeba mít možnost definovat úroveň odposlechu. Odposlech může být povoleno realizovat pouze na úrovni konkrétní IP adresy, na úrovni konkrétního síťového rozhraní, nebo můžeme vyžadovat odposlech veškeré komunikace daného uživatele. Specifikace úrovně je součástí vstupního požadavku a dle ní je také řízeno prohledávání grafu v jádru IRI-IIF. V modelové situaci na obrázku 2 je cílem odposlechu XMPP login *standa4@jabbim.cz/laptop*. Uvažujme, že je požadován odposlech pouze na úrovni jednoho síťového rozhraní.

Procházením grafu je nejprve nalezeno TCP spojení v rámci nějž komunikace probíhá. Z TCP spojení je získána IP adresa klienta (*10.0.2.15*) a serveru (*88.86.102.50*). Cílem zájmu je pouze cílový uživatel, IP serveru je tedy ignorována. Dále je zjištěno, že IP adresa *10.0.2.15* byla přidělena serverem DHCP síťovému rozhraní s MAC adresou *00:04:96:1d:4e:30*. Pomocí bezstavové konfigurace

SLAAC byla tomuto rozhraní přidělena také IPv6 adresa *2001:67c:1220::93e5:949*. Úroveň odposlechu je stanovena pouze na jedno síťové rozhraní, prohledávání grafu tedy končí. Na obrázku jsou nalezené identifikátory zvýrazněny.



Obrázek 2: Ukázka grafové reprezentace stavu sítě

Nalezené identifikátory předá IRI-IIF bloku MF&CCTF. Všechny identifikátory jsou z důvodu vyšetřování ukládány do sběrného zařízení jako metadata. TCP spojení a IP adresy jsou nezbytné také k samotné realizaci odposlechu. MF&CCTF pak řeší případy, kdy se cíle různých odposlechů navzájem překrývají. Pomocí specifických algoritmů je hledána nejvhodnější množina identifikátorů pro efektivní realizaci odposlechu a minimalizaci případných duplicit v zachycených datech.

4 ZÁVĚR

V rámci této práce jsem implementoval nové jádro bloku IRI-IIF a upravil bloky CC-IIF, MF&CCTF a rozhraní CCCI. Provedené úpravy umožňují systém SLIS použít k odposlechu aplikačních protokolů přímo v síti národních poskytovatelů přípojení. Konfigurovatelné úrovně odposlechů umožňují přesnější specifikaci množiny zájmových dat. Vyvíjený prototyp systému se tak stává univerzálnějším a flexibilnějším nástrojem jak pro další výzkum, tak pro případné budoucí nasazení v praxi. Z hlediska zpracování dat a výpočetní náročnosti je kritickým místem celého systému blok MF&CCTF. Součástí další práce proto bude profilace jeho výkonnosti, hledání kritických míst a následná optimalizace.

PODĚKOVÁNÍ

Tento příspěvek vznikl za podpory grantu MV a výzkumného záměru Moderní prostředky pro boj s kybernetickou kriminalitou na internetu nové generace: VG20102015022 a projektu Výzkum pokročilých metod ICT a jejich aplikace: FIT-S-14-2299.

REFERENCE

[1] European Telecommunications Standards Institute: ETSI TR 101 943: Telecommunications security; Concepts of Interception in a generic Network Architecture. Červenec 2001, verze 1.1.1.

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

[3] Martínek, T.; Kramoliš, P.; Holkovič, M.; aj.: Dynamická identifikace uživatelů v prostředí sítí IPv4 a IPv6. Technická zpráva, 2012.