FAKE DATA IN COMPUTER NETWORKS

Radek Hranický
Bachelor Degree Programme (3), FIT BUT
E-mail: xhrani00@stud.fit.vutbr.cz

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

Abstract: This paper describes basic principles of lawful interception systems in computer networks. Various methods of their deception are analysed. A draft of a software tool, which could be used for a demonstration of an attack on lawful interception system is proposed. Finally, a method how to avoid suggested kind of attack is offered.

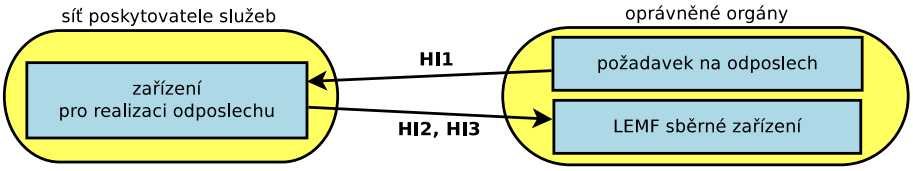
Keywords: Lawful Interception, Confusion, Secret message delivery, Fake data, Noise generating

1 ÚVOD

V souvislosti se stále větším významem internetu pro kriminální, teroristickou a podvodnou činnost roste také potřeba sledování komunikace pomocí *systému pro zákonné odposlechy* (Lawful Interception System – LIS). LIS umožňuje oprávněným orgánům zaznamenávat síťovou komunikaci mezi dvěma, či více podezřelými osobami. Zachycená data je následně možné podrobit další analýze. I přes zdánlivě vysokou efektivitu LIS existuje řada možností, jak jej oklamat – tedy realizovat komunikaci takovým způsobem, aby nebyla odposlechem zaznamenána [1].

2 SYSTÉM PRO ZÁKONNÉ ODPOSLECHY

Podle norem [2], které stanovuje *Evropský ústav pro telekomunikační normy* (European Telecommunications Standards Institute – ETSI), tvoří základní aktéry systému *poskytovatel internetových služeb* (Internet Service Provider – ISP) a *orgány činné v trestním řízení* (Law Enforcement Agency – LEA). Architekturu systému pro zákonné odposlechy zachycuje **obrázek 1**. *Rozhraní HI1* slouží po předávání požadavků na odposlech ze strany oprávněných orgánů. Od okamžiku spuštění odposlechu jsou získané informace přenášeny do cílového *sběrného zařízení* (Law Enforcement Monitoring Facility - LEMF). Zatímco *rozhraní HI2* zajišťuje přenos metadat o aktivitě sledovaných cílů (změny adres, připojení/odpojení ze sítě, apod.), *rozhraní HI3* slouží k přenosu samotného obsahu zachycené komunikace.



Obrázek 1: Architektura systému pro zákonné odposlechy

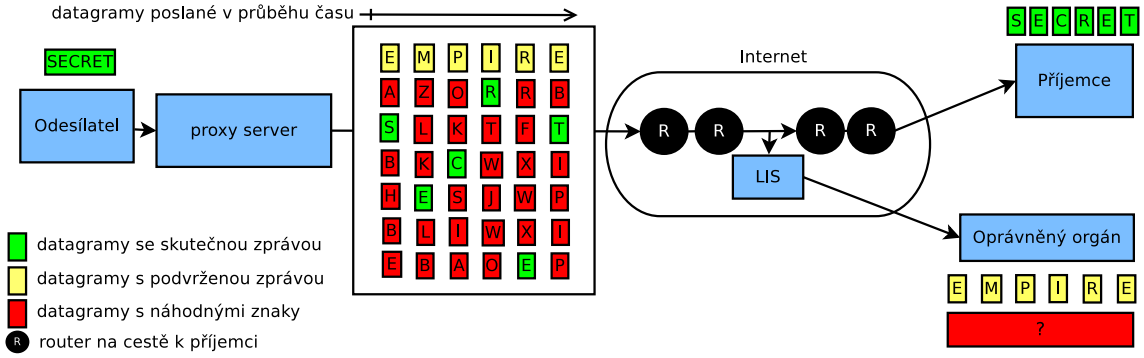
3 MOŽNOSTI OKLAMÁNÍ SYSTÉMU PRO ZÁKONNÉ ODPOSLECHY

Mezi tradiční způsoby utajení obsahu zprávy patří *kryptografie* a *steganografie*. Tyto metodiky sice mohou úspěšně sloužit k utajení obsahu zprávy, ovšem nemusí ochránit *metadata* související s danou komunikací. A především – obvykle neřeší problém, kdy potřebujeme skrýt nejen obsah, ale i to, že předání dané zprávy vůbec proběhlo. K tomuto účelu musíme zvolit odlišné techniky.

Je možné např. generovat *šum* (náhodná, či smysluplná, ale zavádějící - podvržená data) s cílem zmást odposlech a ztížit následnou rekonstrukci zprávy. Zneužitím implementace některých protokolů lze zajistit, aby šum nebyl cílovému příjemci doručován. K tomuto účelu můžeme využít např. podvržení hardwarové MAC (Media Access Control) adresy, či určitým způsobem zajistit zahození vybraných paketů na cestě.

Ve své práci jsem se rozhodl využít implementace protokolů TCP a IP. Odesílaná zpráva ve formě TCP toku je rozdělena do segmentů o velikosti 1 bajtu. Kromě skutečné zprávy je odesílán také šum, který tvoří jednak podvržená zpráva, jednak náhodně generované znaky. Každý tento segment je pak zapouzdřen v IP datagramu kde jsou hodnoty polí Time-To-Live (TTL), či Hop Limit (u IPv6) nastaveny tak, aby pakety s šumem byly zahozeny na cestě k příjemci. Pro TCP segmenty se stejným sekvenčním číslem bude vždy generován 1 bajt skutečné zprávy a několik bajtů šumu.

Fragmentaci zprávy a generování šumu bude provádět proxy server v lokální síti odesílatele. V jiné síti (za *n* směrovači) se nachází příjemce zprávy. Odposlech může být lokalizován kdekoliv na cestě mezi proxy serverem a příjemcem. Pokud není prováděna analýza TTL / Hop Limitu, je velmi obtížné ze zachycených dat zrekonstruovat původní zprávu.



Obrázek 2: Oklamání odposlechu pomocí generování šumu a modifikace TTL / Hop Limitu

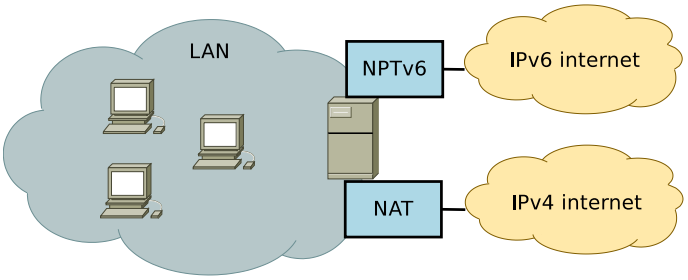
Útok však vždy závisí na umístění sondy pro odposlech. Čím blíže příjemci, tím větší je pravděpodobnost zachycení paketů se skutečnou zprávou. Ideální pro oprávněné orgány je lokalizace sondy bezprostředně před příjemcem, kde již není žádný šum. Ne vždy je to ale v praxi možné realizovat, protože na cestě mohou být i routery umístěné přímo v síti příjemce, které nejsou pod správou ISP.

V rámci scénáře útoku vyobrazeného na **obrázku 2** je sonda lokalizována uprostřed cesty mezi odesílatelem a příjemcem. Příjemce úspěšně obdrží přenášenou zprávu. Odposlech zachytí množství TCP segmentů s kolizními sekvenčními čísly. Tyto segmenty obsahují znaky, které na první pohled nedávají smysl. Na straně oprávněných orgánů probíhá analýza zachycené komunikace, jejímž cílem je zrekonstruovat přenášenou zprávu. Smysluplný text je získán, pokud je pro každé sekvenční číslo použit pouze znak z prvního zachyceného segmentu. Jde ale o podvrženou zprávu.

Tuto techniku je možné modifikovat přenášením podvržené zprávy v posledním odeslaném segmentu dané sekvence, či využitím kombinace obou možností. Čím více šumu je generováno, tím je rekonstrukce zprávy náročnější, ovšem stoupají také nároky na přenosové pásmo linky a výpočetní výkon.

4 NÁVRH NÁSTROJE PRO PROVEDENÍ ÚTOKU

Nástroj pro realizaci útoku bude fungovat jako proxy server a zároveň jako *brána* (gateway) oddělující vnitřní síť od vnější sítě (internetu). Zapojení je vyobrazeno na **obrázku 3**. Z těchto důvodů jsou součástí implementace programu také NPTv6 a IPv4 NAT překladače. Ve vnitřní síti se tak může nacházet jeden, či více odesílatelů zprávy. Cesta ke vzdálenému příjemci zprávy vede skrz internet, přičemž nástroj podporuje jak IPv6, tak IPv4 připojení k internetu. Pro účely oklamání odposlechu je použita technika generování šumu a modifikace TTL / Hop Limitu popsaná v bodě 3.



Obrázek 3: Princip zapojení proxy serveru

5 MOŽNOSTI DETEKCE ÚTOKU

Pokud známe princip útoku, jsou jeho detekce a získání přenášené zprávy poměrně jednoduché. Je zřejmé, že musí existovat minimální hodnota TTL / Hop Limitu potřebná k dosažení cíle (příjemce). Víme také, že pro každé sekvenční číslo musí být doručen přesně 1 TCP segment (jinak by došlo k porušení toku, či kolizi). Pro 1 sekvenční číslo tedy nebude existovat žádný další datagram s vyšší hotnotou TTL / Hop Limitu než ten, který obsahuje skutečnou zprávu. Pokud tedy pokaždé vybereme datagram s nejvyšší hodnotou TTL / Hop Limitu, úspěšně sestavíme přenášenou zprávu.

6 ZÁVĚR

Existuje řada možností oklamání systému pro zákonné odposlechy. Vzhledem k povaze internetu může útočník zneužít implementace mnoha síťových protokolů ve svůj prospěch. V rámci své práce vytvořím nástroj pro demonstraci útoku pomocí generování šumu a modifikace hodnot TTL / Hop-Limitu a také nástroj pro detekci tohoto útoku.

PODĚKOVÁNÍ

Tato práce je součástí projektu VG20102015022 podporovaného ministerstvem vnitra České republiky. Tato práce vznikla za podpory projektu MŠMT CZ.1.07/2.3.00/09.0067 TeamIT – Budování konkurenceschopných výzkumných týmů pro IT.

REFERENCE

[1] Bellovin, S.: Wiretapping the net. The Bridge, 2000, pp. 21-26.

[2] European Telecommunications Standards Institute: ETSI TR 101 943: Lawful Interception (LI); Concepts of Interception in a generic Network Architecture. 2001, version 1.1.1.

[3] E. Cronin, M. B., M. Sherr: Volume 222, Advances in Digital Forensies II. IEEE Communications Surveys & Tutorials, 2006, pp. 199-213.

[4] S. Zander, P. B., G. Armitage: A Survey of Convert Channels and Countermeasures in Computer Network Protocols. IEEE Communications Surveys & Tutorials, 2007, 1553-877X.