NEPŘÍTEL NASLOUCHÁ? (2)

Minule jsme se seznámili s právními aspekty odposlechu na internetu a zahájili exkurzi do jeho technických tajů. Vysvětlili jsme i nejnutnější teoretické poznatky o odposlechu na úrovni síťové vrstvy a slíbili praktickou ukázku. Té se dočkáte nyní, stejně jako povídání o odposlechu na další, tj. aplikační vrstvě.

Nástroje pro analýzu síťového provozu jsou snadno dostupné. *Network Monitor* je přímo součástí operačního systému Windows NT Server nebo Windows 2000 Server. Tato verze ovšem obsahuje pro špiona nepříjemné omezení, protože umožňuje analyzovat toliko pakety určené pro jeho vlastní počítač; ke skutečné špionáži je zapotřebí verze, kterou obsahuje *Microsoft Systems Management Server*. Dalším vhodným nástrojem pro Windows je *NtSniff 1.5 (http://www.mycio.com/davidel)*, který je k dispozici zdarma včetně zdrojového kódu.

Odposlech na síťové vrstvě v praxi

Podívejme se teď krok za krokem, jak to vypadá v konkrétním případě. Předpokládejme, že uživatel v síti se zapojeným Network Monitorem se přihlásil na POP3 server, aby si vybral své e-maily, a to jako uživatel *testuser* s heslem *testpass*. Network Monitor pak zaznamenal informace, které vidíte na obrázku.

Po exportu dat do “čitelné” podoby lze získat následující popis uživatelovy komunikace s poštovním serverem (první sloupec udává v šestnáctkové soustavě relativní adresu prvního bajtu řádky, další sloupce obsahují (opět hexadecimálně) datové bajty, které na konci řádky vidíme znovu i jako text (netisknutelné znaky nahrazeny tečkami):

```
0000: 00 60 08 C3 47 7A 00 60 97 38 49 27 08 00 45 00   .`.ÃGz.`—8I'..E.
0010: 00 36 EE C3 40 00 80 06 3C 08 0A 00 00 01 C2 E4   .6îÃ@.€.<.....Âä
0020: 03 11 0A 68 00 6E ED BD 95 38 70 31 EC 35 50 18   ...h.ní½•8p1ì5P.
0030: 43 E6 37 3C 00 00 55 53 45 52 20 74 65 73 74 75   Cæ7<..USER testu
0040: 73 65 72 0A 00 60 08 C3 47 7A 00 60 97 38 49 27   ser..`.ÃGz.`—8I'
0050: 08 00 45 00 00 28 EE C4 40 00 80 06 3C 15 0A 00   ..E..(îÄ@.€.<...
0060: 00 01 C2 E4 03 11 0A 68 00 6E ED BD 95 46 70 31   ..Âä...h.ní½•Fp1
0070: EC 59 50 10 43 C2 B1 B6 00 00 00 60 08 C3 47 7A   ìYP.CÂ±¶...`.ÃGz
0080: 00 60 97 38 49 27 08 00 45 00 00 36 EE E4 40 00   .`—8I'..E..6îä@.
0090: 80 06 3B E7 0A 00 00 01 C2 E4 03 11 0A 68 00 6E   €.;ç....Âä...h.n
00A0: ED BD 95 46 70 31 EC 59 50 18 43 C2 3F 36 00 00   í½•Fp1ìYP.CÂ?6..
00B0: 50 41 53 53 20 74 65 73 74 70 61 73 73 0A         PASS testpass.
```

Je vidět, že jak uživatelské jméno (sekvence *USER testuser*), tak heslo (sekvence *PASS testpass*) byly zaznamenány, a útočník se tedy oba tyto údaje může dozvědět. Další analýzou provozu by mohl získat například obsah všech e-mailových zpráv, které si uživatel stáhl.

Použitelnost

Tato metoda je použitelná pouze tehdy, pokud má útočník možnost připojit se do některé ze sítí, kterou zpráva proběhne. Velice často se s ní můžeme setkat v prostředí místních sítí LAN, např. ve školách či firmách. Útočník je pak schopen monitorovat provoz ve svém segmentu sítě.

Uložené záznamy o síťovém provozu jsou dosti rozsáhlé. Pokud ovšem útočníkovi jde například jen o získání uživatelských jmen a hesel, může použít speciální programy schopné v reálném čase síťový provoz analyzovat a tyto klíčové informace z něj filtrovat a ukládat, takže pak “přijde k hotovému”. V případě, že by se jednalo o sledování s cílem zjistit, co a s kým si sledovaná osoba posílá, byla by analýza dat poněkud složitější, leč nikoliv nemožná.

Pokud by měl být sledován uživatel připojený přes telefonní linku, nenapadá nás způsob, jak by se to dalo uskutečnit bez svolení a spolupráce poskytovatele připojení k internetu (ISP). Kdyby šlo o zkompromitování jednoho určitého WWW serveru připojeného kdesi na páteři u ISP, mohl by se nicméně útočník pokusit o připojení svého vlastního počítače do stejné podsítě.

Obrana

Nejjednodušší obranou je samozřejmě vhodné šifrování. To je v zásadě možno použít na třech úrovních:

Šifrování na úrovni dat, například e-mailová zpráva zašifrovaná pomocí PGP. Odposlech bude moci prokázat, že byla přijata či odeslána zpráva, zjistit odesílatele, příjemce, datum i velikost, ale nikoliv obsah. V případě, že útočník půjde po heslech, tedy metodou osobnostní analýzy, útoku hrubou silou či podle slovníku, a heslo není na takový útok připraveno, tato metoda nebude moc platná.

Šifrování na úrovni aplikačního protokolu. Většina běžně používaných protokolů (SMTP, POP3, IMAP, HTTP, FTP, LDAP) má svůj ekvivalent, při němž je celá komunikace šifrována, zpravidla pomocí SSL *(Secure Socket Layer)*. Při použití metody tajného a veřejného klíče dostatečné délky je prakticky zaručena nedešifrovatelnost. Touto metodou je možno zabezpečit kompletní komunikaci s danou službou. Útočník sice může poznat, že komunikace nastala, s jakým serverem, jak dlouho trvala, jakého byla typu a přibližně kolik dat bylo přeneseno, není ovšem schopen zjistit obsah komunikace, včetně případných jmen a hesel. V případě e-mailu by například nedokázal určit, kolik zpráv bylo přijato, ani žádné informace o nich. Bohužel, obecná implementace bezpečných aplikačních protokolů dosud zdaleka není běžná.

VPN *(Virtual Private Network)*. VPN představuje metodu, jak i po nezabezpečené síti (jakou internet bezesporu je) vést bezpečnou komunikaci jakéhokoliv typu. Funguje tak, že mezi dvěma (případně i více) body vytvoří "šifrovaný tunel", jímž pak prochází veškerá komunikace. Tunel se zpravidla vytváří na úrovni IP, takže jím je možno prohnat jakoukoliv službu, samu o sobě nezabezpečenou. Útočník pak dokáže zjistit, že nastala komunikace s protistranou (druhým koncem tunelu), její čas i délku a třeba i přibližný objem dat, nikoliv ovšem typ komunikace a její obsah. VPN lze ustavit například pomocí prostředků přítomných ve Windows 2000 nebo také pomocí specializovaných programů (například *PGPNet*).

Doporučit můžeme tento prakticky vyzkoušený postup: nacházíte-li se ve zkompromitované síti, vytvořte si mimo její hranice bezpečný server a připojte se k němu pomocí VPN. Další komunikaci s okolím pak provádějte pouze pomocí tohoto bezpečného serveru.

Odposlech na aplikační vrstvě

Zde se nejedná přímo o aplikační vrstvu tak, jak byla popsána výše, ale o využití (eventuálně zneužití) aplikací, které uživatel tím či oním způsobem provozuje. Vhodným příkladem může být například **e-mailová komunikace**.

Na e-mailových serverech vždy běží nějaký program, který zajišťuje zpracování pošty. Takovým programem může být například *Microsoft Exchange*, *Post.Office*, *Sendmail*, *Zmail* a mnohé další. Abychom mohli posoudit případná bezpečnostní rizika, je nutno vědět, jak tyto programy pracují. (Také následující popis činnosti poštovního serveru je samozřejmě značně zjednodušený; zájemce o podrobnější informace odkazujeme na příslušná RFC a jiné zdroje na internetu.)

Představte si, že pracujete ve firmě s několika desítkami zaměstnanců. Na recepci má každý zaměstnanec přihrádku se svým jménem. Pokud je někomu zvenčí doručena zpráva (například poštou), recepční zprávu převezme, přečte si jméno na obálce a uloží ji do adresátovy přihrádky. Tam zpráva zůstane ležet tak dlouho, než si ji dotyčná osoba vyzvedne. A naopak, pokud chcete poslat zprávu ven, předáte ji recepční. Ta se opět podívá na obálku a příslušně zareaguje: pokud se jedná o člověka z firmy, rovnou zprávu uloží do jeho přihrádky. Jde-li o někoho zvenčí, zprávu předá poště, ať si s ní poradí, jak umí.

Naší hypotetické recepční se v případě poštovních serverů říká MTA *(Mail Transport Agent)*. MTA pracuje tak, že (nejčastěji) pomocí protokolu SMTP *(Simple Mail Transfer Protocol)* přijímá zprávy. Pokud je zpráva určena externímu uživateli, je zaslána příslušnému mail serveru. V případě, že je zpráva určena lokálnímu uživateli (tj. tomu, kdo má na příslušném serveru poštovní schránku neboli mailbox), je uložena do jeho schránky. Zde pak čeká tak dlouho, dokud se uživatel nepřipojí a zprávu si nestáhne (většinou pomocí protokolu POP3, *Post Office Protocol version 3*).

Doba, po kterou je zpráva uložena na poštovním serveru, může tedy být různá – v závislosti na tom, jak často si uživatel vybírá svoji schránku. Po tuto dobu je zpráva uložena buď v nějaké databázi, anebo (což je častější) jako obyčejný textový soubor na disku. A po tuto dobu má také správce serveru možnost s uloženým souborem libovolně manipulovat. Zprávu může číst, pozměnit, nebo dokonce smazat. (Mějte proto vždy na paměti následující varování: odesíláte-li mail, počítejte s tím, že si jej přečte každý správce každého serveru, přes který zpráva půjde.)

V případě, že útočník má přístup k vašemu poštovnímu serveru, není pro něj tedy problém nechat si přeposílat kopie všech zpráv, které dostáváte, a to leckdy způsobem, který je prakticky neprokazatelný. (Setkali jsme se dokonce s případem, kdy byly kopie e-mailů generálního ředitele

přesměrovány zaměstnancem, který odešel pracovat ke konkurenci...)

Jiným potenciálním nebezpečím může být **prohlížení webových stránek přes proxy**. *Proxy* (cache) je zařízení (specializovaný hardware nebo počítač s vhodným programem), které umožňuje připojení do internetu pomocí některých protokolů (typicky FTP, HTTP), přičemž požadavky zasílané klientem dále klade pod svým jménem. Důvodem použití proxy je jednak snaha o snížení zátěže sítě (pokud klient požaduje stránku, kterou chtěl někdo předtím, nestahuje se stránka znovu z originální adresy, ale jen z lokální cache), za druhé snaha o zvýšení bezpečnosti.

Proxy může být principiálně dvou druhů: první je standardní proxy cache, kterou si zapíšete do prohlížeče a používáte ji víceméně dobrovolně, druhý případ je tzv. transparentní proxy (například cache na "akademické" síti TEN-155), ta je ovšem horší z hlediska ochrany soukromí.

Klasickou HTTP proxy poznáte snadno – je nastavena ve vašem prohlížeči. Transparentní proxy už tak snadno nepoznáte – sedí na síti mezi vámi a webovým serverem a odchytává všechny požadavky, které pak předává dál nebo vyřizuje z vlastní cache. Existují sice způsoby, jak transparentní proxy detekovat, ale jsou komplikované a nespolehlivé. Řada ISP přitom transparentní proxy na svých sítích používá nebo minimálně v minulosti používala. Vede je k tomu celkem logická snaha o snížení zátěže linek.

Pro nás je důležité, že jakákoliv proxy si vytváří (nebo alespoň vytvářet může) záznamy o své činnosti, tj. kdo, kdy a jakou stránku požadoval. Z adres navštívených stránek je pak možno celkem snadno odvodit citlivé údaje o sledované osobě, například o její sexuální orientaci, zájmech a podobně.

I adresa může být nebezpečná

Další potenciální bezpečnostní riziko se skrývá v použití autentifikovaných WWW služeb. Řada z nich předává autentizační informace jako součást URL. Příkladem za všechny může být například portál Centrum *(http://www.centrum.cz)* nebo oblíbený diskusní server Mageo *(http://www.mageo.cz)*. Adresa jedné navštívené stránky může být například *http://www.mageo.cz/.chatroom/102?c=1250&u=**oElZFgFhsqkewsTBhwf***

Onen tučně zvýrazněný a zdánlivě nesmyslný řetězec je klíčem k obsahu personalizovaných stránek – podle něj server pozná uživatele a bude ochoten s ním komunikovat. Pokud ovšem tento řetězec někdo zjistí (například z "logu" proxy serveru), může pracovat pod jeho autorizací.

Jednotlivé servery se proti možnosti zneužití zpravidla brání. Žádná ochrana ovšem není stoprocentní, protože je většinou založena na vypršení tohoto kódu po nějakém časovém úseku nebo na omezení požadavku na jednu IP adresu. Obě tyto metody jsou k ničemu v okamžiku, kdy je proxy zkompromitována (tak i tak vystupujete pod její IP adresou) a je sledována v reálném čase (což není problém).

Obrana?

Opět šifrovat, šifrovat, šifrovat! E-maily pomocí PGP, komunikaci na webu pomocí SSL. Webové servery, u nichž "o něco jde" (kde například zadáváte osobní údaje nebo číslo platební karty), by **vždycky** měly používat zabezpečené (šifrované) spojení.

Jak poznat, je-li spojení šifrované? Například podle adresy. Nezabezpečený web má URL začínající *http://*, zabezpečený *https://*. Ono písmenko "s" za názvem HTTP protokolu znamená *secure*, tedy *zabezpečený*. Většina prohlížečů navíc stránky se zabezpečeným připojením nějak identifikuje – například MS Internet Explorer při prohlížení zabezpečených stránek zobrazí ve stavovém řádku symbol visacího zámku.

Z veřejných e-mailových služeb bohužel přístup zabezpečeným protokolem poskytuje jenom *Email.cz* a *Centrum.cz*. Vadou na kráse však je, že jak ATC (email.cz), tak NetCentrum (centrum.cz) šetří na nepravém místě a certifikáty si vydávají samy, místo aby zaplatily renomované certifikační autoritě. Výsledkem sice není signifikantní snížení bezpečnosti, ale zato ohavné a odstrašující hlášky o neplatných certifikátech, generované browserem.

Špioni ve vašem počítači

Nebezpečí číhá i tehdy, když zrovna aktivně "nebrousíte" nebo nemailujete. Řada programů (zejména z kategorie sharewaru) obsahuje funkce, které odesílají potenciálně nebezpečné údaje svým tvůrcům.

Odstrašujícím příkladem může být například přehrávač *RealPlayer (http://www.real.com)*, dílko to společnosti Real Networks. Vypnout v něm všechny funkce reportující kdeco je počin vyžadující prohlédnutí mnoha dialogových oken a několikanásobné potvrzení sugestivních hlášek, které vás před tímto krokem varují, neboť tak přijdete o polovinu skvělých funkcí, které RealPlayer nabízí (jako například pravidelné spamování). Firma Real Netowrks má přitom za sebou několik afér spojených s bezpečnostními dírami a ohrožením soukromí... Poněkud slušněji se chová

nejrozšířenější přehrávač MP3 – *WinAMP*, v němž se dá zasílání těchto informací alespoň snadno vypnout.

Další nebezpečí se skrývá v sharewarových programech, které zobrazují bannery (např. *CuteFTP*). Ty často využívají systémů, které pro snazší cílení reklamy (s vaším vědomím i bez něj) shromažďují data a odesílají je autorovi. Bližší informace o této problematice najdete například na stránkách Gibson Research Corporation *(http://www.grc.com)*.

Skoro optimistický závěr

Na každou kličku existuje smyčka a na každou smyčku zase háček. Nikdy nezmizí rozpor mezi bezpečností systému a jeho uživatelskou přívětivostí – bezpečné systémy prostě nejsou snadno použitelné. Pokud chcete bezpečně a neodposlouchávatelně komunikovat s předem definovanými protistranami, není to většinou problém – je možno používat silné šifrování (například již zmiňované PGP – i když, jak se dočtete na jiném místě, ani ono není bez slabin), což činí komunikaci prakticky zcela bezpečnou.

Proti sledování běžné činnosti obrany není. Riziko sice můžete minimalizovat vhodnými opatřeními, z nichž některá jsme nastínili v tomto článku, ale jistoty nedosáhnete nikdy.

A ještě něco je – zejména ve světle výše řečeného – nutno zdůraznit. Jsme velice znepokojeni snahami některých vlád a jiných organizací o postavení silného šifrování mimo zákon, tedy o faktické omezení práva na soukromí pod záminkou boje proti kriminální činnosti. Na druhou stranu chápeme jejich obavy, protože, alespoň v civilizovaných zemích, neexistuje legální postup, jak z pachatele nebo podezřelého dostat klíč či heslo.[1]

Samozřejmě nechceme z čtenářů vychovat paranoiky, ale trocha opatrnosti neškodí. Přejeme vám bezpečnou komunikaci po internetu, mějte však na paměti starou internetovou moudrost: To, že jsi paranoidní, ještě neznamená, že po tobě nejdou.

Vladimír Smejkal | www.pravni-sluzby.cz,
Michal A. Valášek | altair@altair2000.net

[1] Viz také články autorů Kodl, J., Sokol, T., Smejkal, V.: Šifry, státní zájmy a lidská práva, Chip 4/95, str. 34 – 36, a Smíme šifrovat?, Chip 5/95, str. 30 – 32.