Druhy útoku, protokol SSL, zabezpečené připojení

Je internet v dnešní podobě bezpečný? Tuto otázku si klade pravděpodobně každý, kdo je napojen na celosvětovou síť a prostřednictvím internetu získává i zveřejňuje nějaké informace. Seznámíme vás proto s možnými útoky, které počítačovým systémům hrozí, a také se způsoby, jak se proti těmto útokům bránit.

Pozor, útok!

Druhy útoků

Jestliže je naše přítomnost na webu obchodní či jinou nutností, určitě se vyplatí znát možná rizika připojení interního informačního systému k internetu. Mezi největší nebezpečí patří poškození či kompletní zničení dat, neoprávněná modifikace dat, poškození softwaru, poškození operačního systému a zneužití dat neoprávněnou osobou.

Chceme-li být dobře připraveni na tyto hrozby, je vhodné také vědět, k jakým útokům na náš systém může dojít. Existuje jich celá řada, proberme si tedy alespoň ty nejčastější.

- ***Útoky na hesla uživatelů.*** Nejsnadnější způsob, při němž se postupně generují různá přístupová hesla. Jsou to zpravidla automatizované útoky pomocí poměrně jednoduchých, cyklicky se opakujících programů, známé rovněž pod názvem ***slovníkově založené útoky***.

- ***Útoky založené na předstírání IP adresy.*** Předstírá se IP adresa hostitele interní sítě. Tento způsob umožňuje tedy získat vnitřní přístup k systému.

- ***Náhodné prohlížení přenášených paketů*** (také tzv. ***monitorování sítě***)***.*** Je to poměrně obtížný způsob, kdy se útočníci snaží zachytit a zkopírovat pakety předávané mezi jednotlivými místy na internetu, tedy mezi komunikačními uzly (viz obr. 1).

- ***Přivlastnění sezení.*** Jde o přivlastnění IP adresy řádného klienta a jeho následné odpojení. Umožňuje jak import, tak export dat do systému.

- ***Útoky na sdílené objekty v počítačové síti.*** Útočník se snaží přepsat nebo jinak modifikovat sdílené knihovny podle svých představ a záměrů.

- ***Nevhodná či nedostatečná autorizace uživatelů***. Většina serverů stále umožňuje připojit se do systému jako anonymní uživatelé *(Anonymous, Guest, Host)*, což dovoluje útočníkům monitorovat strukturu serveru a dat na něm obsažených.

- ***Útoky, jejichž cílem je poškodit pověst tvůrce softwaru.*** Jde o snahu prolomit bezpečnostní ochrany daného softwarového produktu a tak autora tohoto softwaru zdiskreditovat, poškodit či zesměšnit.

- ***Předstírání admi-nistrátorů systému*** (také tzv. ***společenské monitorování***). V tomto případě se útočník vydává za administrátora sítě a vyžaduje po uživatelích důvěrné informace, například hesla.

- ***Předpoklad pořadových čísel paketů.*** Tento útok se používá v sítích Unix. V některých verzích Unixu se totiž pořadová čísla paketů vypočítávají podle zjistitelného algoritmu.

- ***Útoky vedené pomocí neautorizovaného softwaru***. Jednoduchá forma útoku, kdy tvůrce softwaru vědomě naprogramuje bezpečnostní trhliny svého produktu, které pak následně zneužívá ke svému prospěchu.

Secure Socket Layer

Když už teď známe rizika připojení k internetu a také nejčastější druhy útoků směřujících proti bezpečnosti počítačových sítí, je vhodné se zmínit o možnostech ochrany proti některým z nich.

Poměrně častým způsobem, jak zvýšit bezpečnost připojení k internetu, je využívání bezpečnostních protokolů. Jedním z těchto protokolů je tzv. bezpečná soketová vrstva, nazvaná ***Secure Socket Layer (SSL).***

Protokol SSL byl původně vyvinut firmou **Netscape** pro účely bezpečných přenosů. Jedná se o nekomerční protokol, tzn. že jeho tvůrce (firma Netscape) souhlasí s jeho neomezeným využíváním pro účely tvorby internetových aplikací.

Při návrhu této vrstvy se řešila mimo jiné i otázka, jak vhodně využít existujících standardů internetové komunikace (HTTP, FTP, SMTP a dalších). Na obrázku 2 je vidět řešení tohoto problému – bezpečnostní protokol SSL je umístěn mezi aplikační a transportní vrstvu.

Jak pracuje SSL?

Bezpečnost protokolu SSL je zajištěna třemi základními prvky: 1. Spojení je **soukromé**, neboť přenášená data jsou zašifrována pomocí symetrického šifrování (např. DES). 2. Server, případně

i klient jsou **autentizováni** (pro TCP/IP). 3. Spojení je spolehlivé. Integritu přenášených dat totiž zajišťují hašovací algoritmy (např. SHA, MD5 a další).

Komunikace mezi prohlížečem klienta na straně jedné a bezpečným serverem na straně druhé probíhá zjednodušeně podle následujícího postupu:

1. Klient pošle požadavek na připojení k bezpečnému serveru spolu se svým veřejným klíčem (public key). Tento jedinečný klíč je generován při instalaci prohlížeče.

2. Server pošle svůj certifikát klientskému prohlížeči spolu se svým veřejným klíčem. Tyto informace jsou zašifrovány pomocí veřejného klíče prohlížeče.

3. Klientský prohlížeč prozkoumá, zda je certifikát platný. V případě, že není vystaven certifikační autoritou (někdy označovanou jako VeriSign), může prohlížeč postupovat dvěma způsoby: buď pokračuje výzvou uživateli, nebo automaticky přeruší spojení se serverem.

4. Prohlížeč porovná informace obsažené v certifikátu se jménem domény serveru a se serverovým veřejným klíčem. V případě shody je server akceptován jako autentický.

5. Prohlížeč zašle serveru seznam číslic.

6. Pokud je serveru umožněna autentizace klienta, klient zašle svůj certifikát. Server prozkoumá, zda je tento certifikát platný a zda je vystaven certifikační autoritou. Pokud tomu tak není, je spojení s klientem přerušeno.

7. Server vybere číslice a zašle je klientskému prohlížeči.

8. Prohlížeč používá vybrané číslice k vytvoření klíče relace (session key), následně zašifruje tento klíč relace pomocí veřejného klíče serveru a takto zašifrovaný klíč zašle serveru.

9. Server přijme klíč relace a rozšifruje jej pomocí svého soukromého klíče (secret key).

10. Server a klient používají dále tento klíč relace k šifrování a dešifrování přenášených dat.

Poznámka: V některých modifikacích může proces tvorby klíče relace probíhat na straně serveru.

Bezpečné připojení

Jak zjistíme, že jsme připojeni na bezpečný server? Snadno. Jednoduchou metodou je podívat se na URL adresu serveru. Pokud začíná *https://,* jedná se o bezpečné spojení – příkladem je server *https://www.verisign.com.*

Navíc jsme ještě informováni naprostou většinou prohlížečů, že následující přenos bude probíhat zabezpečenou formou. Na obrázku 3 je vidět dialogové okno prohlížeče Microsoft Internet Explorer, které nás o zabezpečném připojení informuje.

Analogicky při odchodu na jinou URL adresu (nezabezpečenou) budeme varováni, že opouštíme zabezpečený server (viz obr. 4).

MS Internet Explorer nás dále informuje o existenci bezpečného spojení pomocí malé ikonky visacího zámku (viz obr. 5).

O zabezpečeném připojení jsme obdobným způsobem informováni také v případě, že používáme prohlížeče od jiných společností.

Závěr

Protokol SSL podstatně zvyšuje úroveň zabezpečení přenosu dat v rámci internetu. Podporuje využívání šifrovacích mechanismů pro výměnu informací, dále podporuje firewally i proxy servery, což ještě o nějaký stupeň zvyšuje úroveň bezpečnosti.

S dalšími možnostmi zvýšení bezpečnosti na internetu se seznámíme příště.

Ing. Milan Pinte

Infotipy:

Netscape

home.netscape.com/eng/ssl3/index.html

What is

www.whatis.com/ssl.htm

VeriSign

http://www.verisign.com

Slovníček:

DES – *Data Encryption Standard* – metoda šifrování užívající veřejné nebo soukromé klíče.

FTP – *File Transfer Protocol* – standardní protokol umožňující výměnu souborů v rámci internetu.

HTTP – *Hypertext Transport Protocol* – množina pravidel pro výměnu souborů na webu.

MD5 – *Message-digest* – hašovací funkce.

SHA – *Secure Hash Algorithm* – hašovací algoritmus.

SMTP – *Simple Mail Transfer Protocol* – protokol používaný k přijímání a odesílání elektronické pošty.

SSL – *Secure Server Layer* – bezpečná soketová vrstva, sloužící ke zvýšení bezpečnosti komunikace dvou účastníků prostřednictvím internetu.

TCP/IP – *Transmission Control Protocol / Internet Protocol* – nejčastěji používaný komunikační protokol navržený r. 1969 pro internet.

URL – *Uniform Resource Locator* – metoda indikování místa (adresy) dokumentu nebo ostatních položek dostupných v elektronické podobě.