Zabezpečené spojení se vzdáleným počítačem

Bohuslav Moučka, Radim Peša, ÚVT MU

Bylo již popsáno značné množství papíru o nevhodnosti používání síťových protokolů, které přenáší hesla uživatelů přes počítačovou síť v nezašifrované podobě. Přesto je tato riskantní praxe u značné části uživatelů na MU stále ještě běžnou záležitostí. Dovolíme si proto zmínit se stručně o tom, jaké jiné – bezpečnější – alternativy mají uživatelé k dispozici.

Jednou z nejpoužívanějších síťových služeb je interaktivní, či dávková práce na vzdáleném serveru. Protokolu SSH, který poskytuje bezpečné řešení této služby, je věnována první část příspěvku. Ve zbývající části uvádíme přehled alternativních metod pro vzdálené přístup a také si všimneme zabezpečení jiných aplikací a protokolů.

Protokol SSH

Pro přístup ke vzdálenému počítači se obvykle používají programy telnet, rlogin, rsh, rcp, ftp a poštovní klienti využívající protokoly pop3 a imap. Tyto programy však nešifrují data přenášená mezi klientem a serverem, a protože je přenášejí zpravidla po veřejně přístupné síti, může nepovolaný jedinec data včetně uživatelského hesla odposlechnout a zneužít. K výše uvedeným programům byly proto vytvořeny bezpečnější alternativy, které celou komunikaci šifrují a případný útočník tak odposlechem nezíská žádné užitečné informace. Náhradou programů telnet, rlogin, rsh, rcp a ftp jsou programy využívající protokol SSH (Secure Shell). Protokol SSH je implementován programem běžícím na serveru (sshd) a klientskými programy spolu s dalšími pomocnými programy. V současnosti existují dvě verze protokolu SSH; novější a bezpečnější verze 2.0 obsahuje také program sftp.

Popišme stručně, jak probíhá komunikace mezi serverem a klientem. Na serveru čeká program sshd na žádosti o spojení obvykle na portu 22. Spojení navazuje příslušný klientský program. Obě strany si nejprve vymění verzi protokolu, kterou používají, a server poté pošle svůj veřejný hostitelský klíč (je zpravidla vygenerován při instalaci programu sshd a zapsán na disku) a veřejný server-klíč (mění se jednou za hodinu a neukládá se na disk). Klient vytvoří klíč pro toto spojení, zašifruje ho pomocí klíče svého i serveru a pošle serveru. Tento klíč je následně používán pro šifrování celé komunikace. Všechna data jsou od této chvíle šifrována domluveným klíčem. Klient zkontroluje, zda je server zapsán v seznamu známých serverů. Pokud není, je na to uživatel upozorněn – tato situace nastane buď tehdy, když se klient hlásí na server poprvé, resp. na serveru byl vygenerován nový klíč (většinou při instalaci nové verze SSH), nebo pokud se někdo cizí vydává za server uživatele.

Server sám se pokusí také zjistit, zda se uživatel hlásí z důvěryhodného stroje. Tato metoda využívá souborů `/etc/hosts.equiv` a `.rhosts`, ale bývá standardně z bezpečnostních důvodů zakázána. Jinou metodou je autentifikace založená na šifře s veřejným a soukromým klíčem. Klient odešle veřejný klíč uživatele, server ho porovná s klíčem uloženým na serveru a zakóduje jím náhodné číslo. Klient je poté musí rozkódovat odpovídajícím soukromým klíčem a poslat zpět kontrolní součet. Pokud obě předchozí metody selžou, je nutné se přihlásit zadáním hesla, které se ovšem přenáší v zašifrované podobě.

Bezpeční klienti pro prostředí MS Windows

Součástí každé instalace operačního systému MS Windows je klient služby telnet. Jedná se sice o velmi univerzální prostředek přístupu ke vzdálenému počítači, nicméně je vhodné se jeho použití vyvarovat a dát přednost některé bezpečnější alternativě. Nejrozšířenější náhradou služby telnet je služba ssh popsaná výše. Pro použití na klientské stanici MS Windows jsou zdarma dostupné dvě implementace ssh klienta:

PuTTY ke stažení na adrese `http://www.chiark.greenend.org.uk/~sgtatham/putty/`

TeraTerm ke stažení na adrese `http://www.zip.com.au/~roca/ttssh.html`

Službu ssh je možné použít i pro bezpečný přenos souborů mezi počítači. Například jako náhradu služby ftp. Řádkový klient pro přenos souborů je součástí balíku PuTTY. Příznivci grafického rozhraní jistě ocení vynikající nástroj **WinSCP** (`http://winscp.vse.cz/cze/`).

Použití ssh v unixovém prostředí

Pro připojení na vzdálený počítač z unixového stroje můžete obvykle použít namísto programu telnet nebo rlogin program **ssh.** Lze zadat příkaz `ssh počítač` případně `ssh -l username počítač` (druhý způsob se používá v případě, pokud se uživatel hlásí pod jiným uživatelským jménem).

Pro kopírování jednotlivých souborů mezi dvěma počítači lze místo programu rcp využít program **scp.** Typické použití je např: `scp zdrojový-soubor username@server:cílový-soubor`. Program zkopíruje zdrojový soubor z počítače, na němž je spuštěn, na server pod jménem uživatele do příslušného cílového souboru.

Jako bezpečná náhrada programu ftp slouží program **sftp,** který se ovládá prakticky stejně jako ftp. Pro jeho použití je nutné, aby na straně serveru byl spuštěn sftp-server.

Pokud se chcete na vzdáleném počítači přihlašovat bez zadávání hesla, je třeba spustit na klientském stroji program **ssh-keygen.** Program vygeneruje klíč a zeptá se na jméno souboru, do kterého má uložit soukromý klíč. Veřejný klíč uloží do souboru stejného jména s příponou .pub. Dále se zeptá na přístupové heslo klíče, které bude nutné zadat při navazování spojení. Heslo může být prázdné. Soukromý klíč se standardně ukládá do souboru `$HOME/.ssh/identity`, veřejný do souboru `$HOME/.ssh/identity.pub`. V případě generování klíče pro protokol verze 2.0 je nutné spustit program s parametrem `ssh-keygen -t dsa` nebo `ssh-keygen -t rsa`. Odpovídající soubory jsou pak `$HOME/.ssh/id_dsa` a `$HOME/.ssh/id_dsa.pub` nebo `$HOME/.ssh/id_rsa` a `$HOME/.ssh/id_rsa.pub`. Soubor se soukromým klíčem musí být čitelný pouze pro majitele. Obsah souboru s veřejným klíčem je nutné zapsat do souboru `$HOME/.ssh/authorized_keys` na vzdáleném stroji. V případě protokolu verze 2.0 jde o soubor `$HOME/.ssh/authorized_keys2`.

Alternativy k ssh

Kromě SSH existuje řada jiných mechanismů a aplikací zajišťující bezpečnou komunikaci. K takovým mechanismům patří například protokol Kerberos, který poskytuje velmi solidní základ pro realizaci bezpečné síťové komunikace. Řada aplikací (jako je telnet, ftp, rsh, i samotné ssh) bylo upravena tak, aby mohly využívat tento autentizační mechanismus. Další využívaným prostředkem pro zabezpečení komunikace je protokol SSL, založený na certifikátech veřejných klíčů (podle standardu X.509) a struktuře certifikačních autorit. Protokol SSL slouží jako základ, nad kterým se provozuje běžný aplikační protokol, příkladem je např. ssltelnet. V případě, že je třeba zajistit pouze autentizaci a nikoliv ochanu přenášených dat, lze použít jednorázová hesla (OTP), kdy má uživatel seznam hesel, z nichž každé lze použít pouze pro jedno přihlášení. Všechny uvedené mechanismy jsou v prostředí ÚVT používány. Kerberos je základním autentizačním prostředkem v MetaCentru (bližší popis lze nalézt např. v [2]), telnet nad protokolem SSL je používán pro přístup k některým částem ekonomické agendy MU.

Zabezpečení dalších služeb

Vedle vzdáleného přístupu uživatelé požadují řadu jiných služeb. K nejpoužívanějším patří *přístup k elektronické poště*. Řada uživatelů, kteří používají pro čtení elektronické pošty POP3 nebo IMAP klienta, si často vůbec neuvědomuje, že také jejich heslo je přenášeno na poštovní server v nezašifrované podobě. Přitom uvedené aplikace podporují bezpečný přístup využívající protokol SSL. Pokud server tuto možnost podporuje, stačí, když si ji uživatel vybere v nastavení svého poštovního klienta. Po tomto nastavení se budete k poštovnímu serveru hlásit obvyklým způsobem, ale komunikace včetně hesla bude šifrovaná. Uživatel dokonce může místo hesla použít pro autentizaci svůj osobní certifikát. Klient při navazování spojení s poštovním serverem kontroluje, zda je klíč serveru podepsán známou certifikační autoritou a může ho tedy považovat za bezpečný. Certifikát na relay.ics.muni.cz je podepsán certifikační autoritou Masarykovy univer-

zity [1]. Zabezpečení komunikace při odesílání pošty bylo popsáno v [3].

Literatura

[1] D. Rohleder. Certifikační autorita Masarykovy univerzity. Zpravodaj ÚVT MU. ISSN 1212-0901, 2000, roč.10, č.5, s.14-18.

[2] M. Ruda, A. Křenek, L. Matyska. Infrastruktura MetaCentra. Zpravodaj ÚVT MU. ISSN 1212-0901, 1999, roč.10, č.2, s.9-14.

[3] M. Ruda. Autentizace v protokolu elektronické pošty SMTP. Zpravodaj ÚVT MU. ISSN 1212-0901, 2000, roč.10, č.3, s.6-8. □