Mi is az ssh/RSA?

Az ssh (Secure Shell) egy protokoll, ami távoli gépek között biztonságos csatornán keresztüli kommunikációra (akár parancsok végrehajtására) fejlesztettek ki. Hitelesítéshez nyilvános kulcsú (RSA) titkosítást használ. Ennek lényege, hogy minden résztvev? rendelkezik két kulccsal: egy titkossal és egy nyilvánossal (privát és publikus, ha valakinek úgy jobban tetszik). A két kulcs egymást kiegészítve m?ködik, a nyilvánossal lezárt szöveget csak a titkos nyitja ki, és fordítva, a titkossal lezártat a nyilvánossal nyithatjuk ki.

Használata ssh paranccsal

Ahhoz, hogy jelszó nélkül, RSA-hitelesítéssel be tudjunk lépni, el?ször kulcsokat kell generálni az `ssh-keygen -t rsa` parancsal. A kulcsokra ekkor jelszavas védelem tehet? (opcionális). A publikus kulcsak (id_rsa) azon a gépen kell lennie, ahova be akarunk lépni (pl: omnibus), a home-ban, egy .ssh könyvtárban, a publikusnak pedig azon, ahonnan be akarunk lépni, a .ssh/authorized_keys -ben. Ez utóbbiba be kell másolnunk az imént létrehozott id_rsa tartalmát. *Fontosak a jogosultségok:* ssh könyvtár 700, a távoli gépen a home könyvtár: 755 (tudjátok, `chmod` parancs)

Maga a belépés egyszer?, parancssorban gépeld be az `ssh felhasználóneved@másik.gép.neve` parancsot (ha csak `ssh másikgép` parancsot adod ki, akkor automatikusan azzal a felhasználónévvel próbál belépni, amelyen épp be vagy jelentkezve)

A beállításokat a ~/.ssh/config fájl tartalmazza, meg lehet változtatni pl, hogy melyik gépre milyen felhasználónévvel próbáljon

Példák, leírások

http://linuxbox.hu/sshkey
http://www.inf.bme.hu/hogyan/ssh.html
http://www.suso.org/docs/shell/ssh.sdf

Farbas