Ochrana vzdialenej komunikácie výpočtových systémov

Security in remote communication of computer systems

Igor Halenár, STU MTF, UIAM

Bohuslava Juhásová , STU MTF, UIAM

Abstract: In present days is remote access to control of systems via internet, one of most used forms of management. This way of communication is very profitable, and in some cases essential. A protocols used for communication in internet network are developed for remote data transfers.

Base of this type of communication is protection against unauthorized access from outside. Below term protected communication we can understand all complex of protection elements (password management, access layers, data encrypting, security gates, hidden networks, trusting authority, etc.), that are used to deny unauthorized access to managed system or local network. Of course, security of computer systems, against improper use, is very complex business.

Key words: communication, safety, computer, system, interface

Abstrakt: Trendom súčasnej doby je nielen výkon, ale aj bezpečnosť prenosu dát a prístup k nim. Chrániť citlivé údaje je možné na niekoľkých miestach - rozhranie siete súkromná/verejná strana, vzdialený prístup, resp. vzdialená správa zariadení, zabezpečenie serverov a pod. Metódy realizácie potom zodpovedajú miestu nasadenia, a zvyčajne sa používajú viaceré spôsoby, ktoré sa navzájom kombinujú.

Príspevok pojednáva o ochrane na úrovni vstupu do lokálnej počítačovej siete a rozoberá možnosti ako zabrániť neoprávnenému používateľovi prístup k dátam z hľadiska ich využiteľnosti pri prevádzke priemyselných sietí v automatizovaných riadiacich systémoch, kde sa vyžaduje zvýšená úroveň spoľahlivosti a bezpečnosti údajov súvisiacich s riadením technologických procesov.

Kľúčové slová: komunikácia, bezpečnosť, počítač, systém, rozhranie

1. Bezpečnosť dát

1.1. Vzdialená správa systémov

Jedným z kvalitatívnych parametrov informačných a riadiacich systémov je možnosť vzdialene pristupovať k nim , prípadne riadiť celý proces prostredníctvom vzdialenej správy. Najrozšírenejšia sieť dostupná pre široké spektrum používateľov je v súčasnosti internet. Takýto spôsob komunikácie so vzdialeným systémom je veľmi výhodný, a v niektorých prípadoch dokonca nevyhnutný. Môže ísť o centralizované riadenie viacerých systémov z jedného centra, kontrolu prevádzkových parametrov vzdialeného pracoviska, prípadne zber výstupných údajov. Ak ide o systémy, ktoré sú fyzicky nedostupné, je takýto spôsob riadenia nenahraditeľný.

1.2. Zabezpečenie komunikácie

Využitie internetu ako prenosového média je veľmi vhodné, vzhľadom na princíp funkcie tejto siete. Protokoly používané na komunikáciu vznikali pôvodne priamo kvôli vzdialenému prenosu dát. Postupne s rozvojom siete a so zvyšovaním technickej úrovne používateľov a pripojených klientskych staníc vznikala potreba ochrany prenášaných dát. V súčasnosti je pod pojmom ochrana komunikácie možné chápať celý systém ochranných prvkov (správa hesiel, úrovne prístupov, šifrovanie komunikácie, bezpečnostné brány, skryté siete, certifikačné autority a pod.), ktoré slúžia k zabráneniu neoprávneného prístupu k systému alebo vlastnej počítačovej sieti. K dispozícii pritom máme celú sústavu noriem a protokolov. Aplikáciou týchto protokolov sa môžeme vyhnúť väčšine útokov.

Zabezpečenie systémov sa často neberie komplexne. Znamená to, že často je vytvorená pomerne silná ochrana na vstupe do lokálneho systému z internetu, ale samotná komunikácia prebieha nezabezpečeným (nezašifrovaným) kanálom. Prípadnému útočníkovi tým priamo poskytujeme priestor na získanie údajov odpočúvaním komunikácie. Po analýze ethernetových rámcov takto odpočúvanej komunikácie je možné získať všetky dáta, ktoré boli prenášané, vrátane prístupových hesiel.

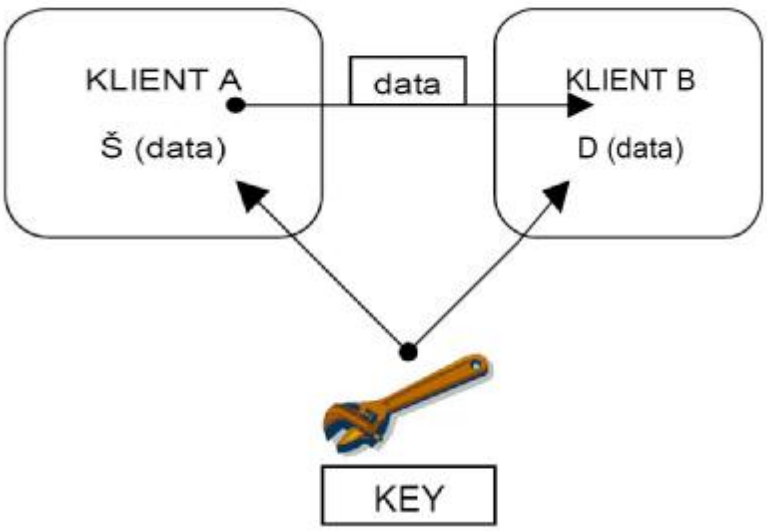
1.3. Spôsoby šifrovania komunikácie

1.3.1. Kontrolný súčet – HASH

Vytváranie kontrolného súčtu je asi medzi najjednoduchší, ale pri tom efektívny spôsob kontroly prenášaných dát. Hash je jednocestná funkcia, pomocou ktorej sme schopní z ľubovoľne dlhého textu vyrobiť krátky reťazec konštantnej dĺžky. Výsledný reťazec by mal maximálne charakterizovať pôvodný text. Typická veľkosť takéhoto textu je 16B (algoritmus MD-5) alebo 20B (algoritmus SHA-1). Výpočtový výkon potrebný na vytvorenie takejto funkcie je malý, ale nájsť pôvodný text k kontrolnému reťazcu je technicky extrémne náročné. Takéto algoritmy nie sú použiteľné ako šifrovacie algoritmy (všeobecne neexistuje inverzná funkcia), ale používajú sa ako odtlačok prstu pôvodného dokumentu (fingerprint). Algoritmus kontrolného súčtu je priamo používaný protokolom Ethernet , a je popísaný v príslušnej norme. Používa sa predovšetkým na zistenie integrity prenášaných dátových rámcov na linkovej vrstve.

1.3.2. Symetrické šifrovanie

V prípade , že potrebujeme zachovať určité súkromie pri komunikácii, musíme komunikáciu nejakým spôsobom šifrovať. V tomto prípade je nutné sa rozhodnúť pre konkrétnu šifru. Je možné použiť symetrické šifrovanie (obr. 1)

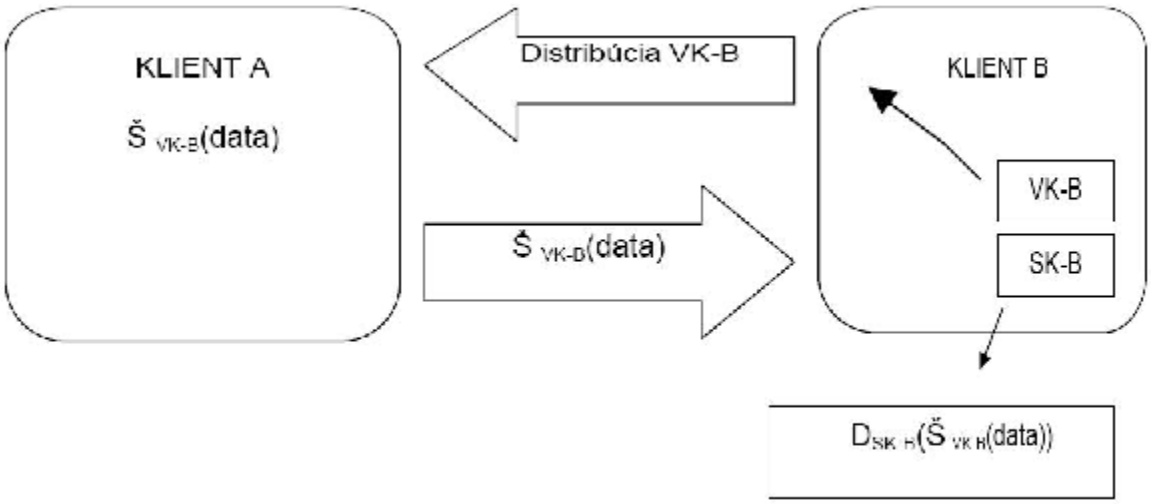


Obrázok 1: Symetrické šifrovanie

Pri tomto type komunikácie je potrebné, aby obaja klienti mali k dispozícii symetrický šifrovací kľúč (KEY). Ak má byť tento spôsob komunikácie bezpečný, je potrebné zamedziť prístup ku kľúču tretím osobám. Symetrická šifra má určitý autorizačný účinok . Symetrických šifrovacích algoritmov je veľa. Najrozšírenejším je DES s dĺžkou 56 bitov. Dnes sa považuje za nedostatočný. Odvodeným nástupcom je 3DES s dĺžkou 112 bitov, prípadne 128 bitov (IDEA, RC2,RC4).

1.3.3. Asymetrické šifrovanie

Pri tomto type šifrovania sa používa iný systém kľúčov. Nepoužíva sa jeden tajný šifrovací kľúč zdieľaný medzi odosielateľom a príjemcom, ale dvojica kľúčov. Jeden pre šifrovanie a jeden pre dešifrovanie (verejný a súkromný). Najpoužívanejší je algoritmus RSA



Obrázok 2: Asymetrické šifrovanie

Ak je chceme šifrovanie správy asymetrickou šifrou, je nutné najprv vygenerovať dva kľúče (klient B). Ide o verejný kľúč (VK-B) a súkromný kľúč (SK-B). Súkromný kľúč klienta B (SK-B) bude uložený na dôveryhodnom mieste (pevný disk, USB kľúč) verejný kľúč klienta B (VK-B) je distribuovaný voľne partnerom vo svete (klient A). Klient A potom pri posielaní zašifruje posielaný text svojím verejným kľúčom, pričom príjemca (klient B) si správu rozšifruje súkromným kľúčom.

Základnou vlastnosťou asymetrického šifrovania je tá vlastnosť, že je relatívne jednoduché verejným kľúčom šifrovať text (data), ale na základe poznania verejného kľúča a verejným kľúčom šifrovanej správy je veľmi zložité získať pôvodný, nezašifrovaný text.

Veľkosť šifrovacích kľúčov pre RSA sa v súčasnosti považuje za bezpečnú aspoň dĺžky 1024 Bitov. Často sa však používajú kľúče dlhé 2 alebo 4 K, v závislosti od potrieb používateľa a citlivosti prenášaných dát.

Na ďalšie zvýšenie bezpečnosti je možné použiť napríklad certifikáciu verejného kľúča, časové pečiatky, prípadne DV-certifikáty.

2. Protokol SSH

Protokol SSH (Secure SHell) je bezpečným variantom protokolu Telnet. Pracuje na báze asymetrickej kryptografie, a navyše okrem nahradzovanie Telnet-u, ponúka aj šifrovaný ekvivalent protokolu Ftp. Nad protokolom SSH je navyše možné otvárať bezpečné komunikačné kanály (kľúče RSA, DSA).

Poskytuje silnú autentizáciu a a bezpečnú komunikáciu na nezabezpečenom kanále. Je možné ho použiť ako náhradu prakticky všetkých nezabezpečených protokolov pre vzdialenú komunikáciu (RLogin,RSH,RCP,RSYNC,RDIST). Vlastnosti a výhody SSH je možné zhrnúť do nasledovných bodov:

- šifrovanie prenášaných dát. Šifrovací kľúč sa pritom prenáša bezpečnou asymetrickou šifrou, dáta sú potom šifrované symetrickým algoritmom
- autentizácia podľa potreby heslom, alebo v prípade potreby pomocou RSA kľúča (prípadne DSA)
- možnosť vytvorenia šifrovaného kanálu pre ľubovoľný protokol TCP (napríklad POP3)
- možnosť presmerovania komunikácie pre X-Server cez šifrovaný kanál
- možnosť využitia overovacieho agenta bežiaceho na klientskom počítači pre úschovu RSA kľúčov
- znemožňuje, alebo výrazne komplikuje niektoré formy útoku (DNS spoofing, IP spoofing)
- umožňuje použitie kompresie prenášaných dát

Protokol SSH sa skladá z niekoľkých služobných protokolov. Základnými sú: Transport layer Protocol, Authentication Protocol, Connection Protocol a SSH File Transfer Protocol.

3. Praktická časť

3.1. Autentizácia

Počítače spolu bežne komunikujú prostredníctvom nezabezpečenej IP siete. V prípade SSH žiada klient o spojenie so serverom, na ktorom je spustený SSH démon (štandardne na porte 22/tcp). Po počiatočnom overení identity klienta a servera, sa textové identifikačné reťazce nahradia binárnou komunikáciou. Server odošle svoj verejný statický kľúč (host key, veľkosť 1024 bit) a verejný dynamický kľúč (server key, veľkosť 768 bit). RSA satické kľúče sa generujú hneď po inštalácii SSH servera. Nemenia sa, kým sa nevygenerujú nové. Naproti tomu RSA dynamické kľúče sa štandardne menia raz za hodinu.

Generovanie kľúčov je možné vykonať jednoducho príkazom *ssh-keygen*

```
laura:/etc/ssh # ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
d3:cc:6c:16:bc:68:66:4c:ea:3a:e6:d3:b8:cf:28:87 root@laura
```

Obrázok 3: Generovanie RSA kľúčov

3.2. Tunelovanie s programom IPIP

Tunel IP je do značnej miery podobný sieti VPN, ale nie každý tunel je šifrovaný. Vytvoreným tunelom obvykle prechádza sieťová komunikácia, a tým môžeme cez internet prepojiť dve lokálne siete. Pre jednoduchý tunel je možné využiť protokol IPIP. Súbory pre podporu protokolu je možné stiahnuť z adresy *ftp://ftp.inr.ac.ru/ip-routing/*.

Prepojenie dvoch lokálnych sietí s adresami 192.168.1.0/24 a 192.168.2.0/24 je možné vykonať nasledovne. Predpokladajme, že smerovač č.1 ma verejnú IP adresu 195.12.128.1 a smerovač č.2 má IP adresu 195.12.128.2. Pre vytvorenie jednoduchého tunela je potrebné vykonať nasledujúce. Najprv je potrebné zaviesť do jadra modul. Vykonáme to príkazom:

 # modprobe ipip

Na smerovači s internou adresou 192.168.1.0/24 je potrebné napísať nasledovné príkazy:

*# ip tunnel add moj_tunel mode ipip remote 195.12.128.2 *

local 195.12.128.1 ttl 255

 # ifconfig moj_tunel 192.168.1.1

#route add –net 192.168.2.0/24 dev moj_tunel

A podobne na smerovači č. 2 symetricky:

*# ip tunnel add moj_tunel mode ipip remote 195.12.128.1 *

local 195.12.128.2 ttl 255

 # ifconfig moj_tunel 192.168.2.1

#route add –net 192.168.1.0/24 dev moj_tunel

Po tomto je možné vykonať ping 192.168.2.1 zo smerovača 1 a naopak.

3.3. Šifrovaný tunel pomocou SSH

Balík OpenSSH je možne okrem vyššie spomenutého vzdialeného prihlasovania sa a vzdialeného vykonávania príkazov využiť na odovzdávanie ľubovoľného TCP portu na druhý koniec nadviazaného spojenia. Ako príklad takéhoto použitia je možné použiť komunikáciu s mailovým serverom , protokol POP a port 110/tcp.

 # ssh –f –N –L110:mail_server:110 –l pouzivatel mail_server

Pre fungovanie tohto tunelu samozrejme treba upraviť konfiguráciu klienta pre sťahovanie pošty na *localhost:110* .

Skutočné využitie však bude mať skôr predávanie komunikácie napríklad dotazov na databázový server umiestnený vo vzdialenej sieti, kde chceme zabezpečiť súkromie prenášaných údajov. Odovzdávanie kompletnej komunikácie , napríklad na porte 5000/tcp na ľubovoľný vzdialený systém na port 4500/tcp môžeme vykonať príkazom:

 # ssh –f –N –L5000:195.12.128.1:4500 195.12.128.2

Využívame pritom všetky výhody protokolu ssh, teda RSA 1024bit asymetrické kľúče, prípadne môžeme podľa potrieb použiť silnejšie šifrovanie.

4. Záver

Potreba ochrany citlivých dát pred zneužitím je v dnešnom svete viac než zrejmá. Účelom článku je iba jemne načrtnúť problematiku a poskytnúť jednoduché riešenie problému. Samozrejme, oblasť ochrany systémov pre zneužitím je veľmi komplexná , a dalo by sa povedať interdisciplinárna záležitosť.

Keďže neexistuje žiadna medzinárodná právna úprava proti útokom vedeným z internetu, je možné teoreticky predpokladať, že na každý náš systém teoreticky útočia milióny útočníkov z celého sveta. Internet je veľmi nebezpečné prostredie, a je na každom používateľovi , aby si svoje systémy a dáta chránil pred poškodením.

5. Zoznam bibliografických odkazov

(1) FLICKENGER, R. 2005. Linux server na maximum. CP Books, a.s., 2005. strán 231, ISBN 80-251-0586-5

(2) DOSTÁLEK, L. A kol. 2003. Velký pruvodce protokoly TCP/IP: Bezpečnost. CP Books, a.s., 2005. strán 592. ISBN 80-7726-849-X

6. Adresa autorov:

Igor Halenár, Ing.
Slovenská technická univerzita MTF
Hajdóczyho 1
917 01 Trnava
Igor.halenar@stuba.sk

Juhásová Bohuslava, Ing.
Slovenská technická univerzita MTF
Hajdóczyho 1
917 01 Trnava
Bohuslava.juhasova@stuba.sk