Špeciálne techniky prenosu dát v počítačových sieťach

Special techniques of data transmission in computer networks

Igor Halenár, UIAM MTF STU

Abstract: The reliability of information and control networks, depends on many factors. In this , great emphasis is placed on the security of transmission channels. In practice, many of the security technologies are used to provide secure communication channels. But going through the same development, there are technologies, which can bypass standard security mechanisms used in computer communication.

Key words: communication, security systems

Abstrakt: Spoľahlivosť dátovej komunikácia v informačných a riadiacich sieťach závisí od množstva faktorov. Veľký dôraz sa pritom kladie na bezpečnosť prenosových kanálov. V praxi sa využívajú mnohé technológie na zabezpečenie prenosov. Rovnakým vývojom však prechádzajú aj technológie, ktorými je možné obísť štandardné zabezpečovacie mechanizmy dátových sietí.

Kľúčové slová: komunikácia, zabezpečenie prenosov

1. Ochrana prenosov v dátových sieťach

Pre kvalitné komunikačné prenosové cesty a tým aj kvalitný prenos dát je potrebné zabezpečiť nielen spoľahlivé a výkonné prenosové cesty, ale zároveň zabezpečiť aj bezpečnosť prenosu dát a prístup k nim. Spôsoby realizácie a samotné použité metódy ochrany zodpovedajú miestu nasadenia a zvyčajne sa používajú viaceré spôsoby, ktoré sa navzájom kombinujú. Chrániť citlivé údaje je možné na niekoľkých miestach - rozhranie siete súkromná/verejná strana, vzdialený prístup, resp. vzdialená správa zariadení, zabezpečenie serverov a pod. Ako primárne prenosové médium sa často, alebo výlučne, na prenos využíva internet a jeho protokoly. Využitie internetu ako prenosového média je veľmi vhodné, vzhľadom na princíp funkcie tejto siete.

2. Techniky špeciálnych prenosov

Protokoly používané na komunikáciu vznikali pôvodne priamo kvôli vzdialenému prenosu dát. Následne s rozvojom siete a zvyšovaním technickej náročnosti komunikačných zariadení boli do prenosových systémov implementované rôzne techniky ochrany. V súčasnosti sú reprezentované ako súbor 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. Na kontrolu komunikácie a prenášaných dát slúžia všeobecne využívané zariadenia ako firewall, prípadne systém detekcie prienikov (IDS) alebo spojenie týchto technológií.

Je potrebné si uvedomiť, že nie je možné absolútne zabezpečiť žiadnu komunikačnú sieť. Okrem všeobecne známych pokusov o infiltráciu do komunikačnej siete (či už pasívne alebo aktívne) sú v súčasnosti aktuálne aj špeciálne techniky. Ide predovšetkým o nasledovné metódy:

1. skryté kanály (Covert Channel)
2. zdanlivá komunikácia (Out Of Band Communication)

Problémom pri tomto type škodlivej komunikácie je, že v súčasnosti neexistuje účinná metóda, ktorá by zabránila takémuto skrytému spôsobu prenosu dát.

2.1. Skryté kanály

Ide o metódu, ktorá predstavuje jednoduchý, ale účinný mechanizmus pre výmenu dát medzi systémami, bez akéhokoľvek rozpoznania tejto činnosti firewallom alebo IDS systémom. Princípom tejto techniky je využívanie takých komunikačných portov TCP prípadne IP protokolu, ktoré sa zvyčajne neblokujú prostredníctvom zabezpečovacích systémov (TCP/53, UDP/53 a pod.)

Okrem toho je možné využiť na takúto komunikáciu aj bežné pakety, pričom skryté dáta sa prenášajú priamo v „neškodných“ údajoch, reprezentované určitými zmenami v hlavičke TCP alebo UDP paketov.

Táto technika prenosu dát je väčšinou odolná voči všetkým štandardným firewallom, aj IDS systémom. Odhalenie skrytých kanálov je možné len neustálou analýzou komunikácie v sieti.

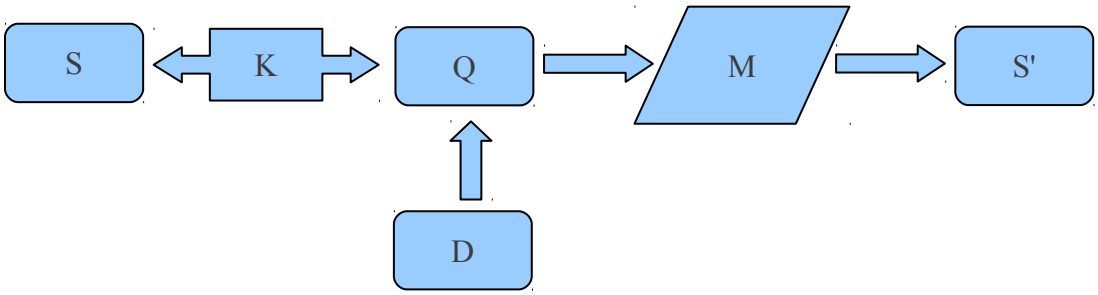
V sieti sa však môže prenášať značné množstvo údajov, a takáto analýza je v reálnych podmienkach často nemožná.

Problémy vyplývajúce z tohto typu útoku na sieť sú nasledovné:

- správca (vlastník) prenosovej cesty nemá žiadnu kontrolu nad obsahom prenášaných dát, nie je schopný určiť cieľ a ani zdroj. Pritom môže ísť o vysoko citlivé údaje, ktoré sú v skrytej forme „pašované“ z komunikačnej siete.
- skryté kanály na svoj prenos používajú veľké percento šírky prenosového kanálu pre prenos relatívne malého množstva skrytých informácií v upravenom objekte [1]. Tento jav je dôsledkom toho, akým spôsobom sa implementuje skrytá informácia do legitímneho dátového prenosu.

Existujú v podstate dva hlavné spôsoby využitia prenosu dát formou skrytých kanálov. Prvým je klasický spôsob ukladania skrytej informácie modifikáciou nejakého objektu. Ako príkladom v tomto prípade môže slúžiť asi najznámejší a najjednoduchší spôsob skrývania informácie v grafických obrázkoch, kde malou zmenou jednotlivých bitov obrázku zakódujeme nejakú informáciu (stenografia) [3].

Formy stenografie môžu byť rôzne. Závisia od použitej technológie, použitého média a objektov, ktoré sa zúčastnia v samotnom procese. Spôsob implementácie je možné popísať jednoduchou schémou [4].



S - originálny súbor

K - sprostredkovací kanál

Q - stenografický systém

D - údaje určené na prenos (tajná správa)

M - použitá metóda zapuzdrenia

S' - modifikovaný súbor

Druhým spôsobom implementácie je využitie časových slotov (kanálov). V tomto prípade nejde o modifikáciu statických objektov ako v prvom prípade (obrázky, zvuky), ale o modifikáciu objektov s časovou postupnosťou. V prípade počítačovej komunikácie napríklad manipulácia TCP paketov (timestamp) [5].

2.1.1. Riziká existencie skrytých kanálov v dátovej sieti

V prostredí výpočtových systémov ide predovšetkým o dosiahnutie prenosu takej formy dát (von alebo do siete), ktorá odporuje bezpečnostnej politike organizácie. Prípadne sa uvedený spôsob priamo využíva na kradnutie technológie a výrobných postupov. Všeobecne je možné rozdeliť riziká vyplývajúce z uvedenej techniky prenosu do nasledovných kategórií:

1. Odosielanie súkromných (citlivých) informácií zo siete smerom von bez kontroly.

   Ide predovšetkým o kradnutie duševného vlastníctva firiem a organizácií. Spôsob realizácie predpokladá zainteresovanie zamestnanca vo vnútri siete, ktorý spustí špecializovaný softvér na počítači v lokálnej sieti.

2. Doručenie škodlivého spustiteľného súboru na počítač v internej sieti

   V prípade korektnej implikácie mechanizmu skrytých kanálov na výpočtovom systéme v lokálnej sieti je možné smerom dovnútra preniesť ľubovoľnú spustiteľnú aplikáciu.

3. Doručovanie riadiacich informácií pre inštalovanú aplikáciu (BOTNETS

   V tomto prípade sa jedná o riadenie procesu „robota“ v lokálnej sieti. Robot môže v rámci lokálnej siete automaticky vykonávať rôzne funkcie (zbieranie hesiel, mapovanie konfigurácie a pod.). Rovnakou cestou môže robot odosielať (na požiadanie) získané informácie.

2.1.2. Implementácia skrytej komunikácie v protokoloch TCP/IP

Ako vyplýva z definície protokolov štandardov ISO 7498 (ISO/OSI model), protokoly tretej vrstvy v modele TCP/IP môžu byť zneužité pre techniku prenosu ako v prvej t.j. ukladacej forme, tak i v druhej, teda forme časových slotov. To je spôsobené hlavne nedostatočnou presnosťou definície IP protokolu. Priamo v hlavičkách sa nachádzajú nevyužité dátové polia a samotný spôsob doručovania paketov, prípadne zlá implementácia štandardov v praktickej fáze operačných systémov priamo umožňujú implementáciu tohto typu komunikácie. Medzi najjednoduchšie spôsoby implementácie môžeme zahrnúť už spomenutý systém DNS a

komunikácia na porte TCP/53, prípadne UDP/53. Ďalej sa s úspechom využívajú polia príznakov v TCP hlavičke (ACK) , pole identifikácie ICMP paketu, pole zdrojovej IP adresy v hlavičke paketu IP a podobne. Rovnako je možné na prenos skrytej informácie použiť ICMP správy (PORT,HOST UNREACHABLE,ECHO), prípadne odpovede DNS.

Zabezpečenie lokálnej počítačovej siete pred týmto spôsobom útoku je veľmi ťažké, prakticky v súčasnej dobe nemožné. Napríklad v prípade využitia ICMP paketov je asi jediným spôsobom zákaz všetkých ICMP paketov v sieti. Tento spôsob však má za následok čiastočné obmedzenie funkčnosti komunikačnej dátovej siete. Obdobné je to aj v iných prípadoch.

Možným riešením je práve aplikácia zariadenia riadeného neurónovou sieťou (čo v podstate môžeme nazvať inteligentný firewall), ktorá dokáže spracovávať vzorce správania sa komunikačnej sústavy pri prenose. Systém detekcie prienikov (IPS), respektíve detekčný systém (IDS) v spojitosti s inteligentným firewallom je schopný sa naučiť obsah štandardného ICMP paketu pre používané systémy a následne filtrovať datagramy s neštandardným dátovým poľom. Takýto proces je samozrejme náročný na výpočtový výkon a nie je možné zaručiť odhalenie všetkej skrytej komunikácie.

2.2. Zdanlivá komunikácia

Tento spôsob prenosu dát je využívaný dvomi spôsobmi. Normálne, známym spôsobom ako doplnok komunikačných prenosov (ISDN) a skryto za účelom nelegálneho získania dát. Všeobecne sa jedná o špeciálnu techniku prenosu dát, pri ktorej sa využívajú zdanlivo nesúvisiace údaje v informačných systémoch. Príkladom môže slúžiť zmena prístupových práv nejakého súboru. Ak sa vykonávajú neustále zmeny (zákaz zápisu, povolenie zápisu do súboru, zmena vlastníckych práv a pod.), je možné monitorovaním týchto zmien prenášať dáta. Tieto techniky prenosu sú veľmi komplikované a prakticky je nemožné ich odhaliť. Dôvodom je, že je možné na takýto prenos dát kombinovať rôzne parametre hardvérových a softvérových prvkov. Môže ísť pritom o hodne „exotické“ kombinácie, ako už spomenutá zmena prístupových práv spolu so zmenou frekvencie procesora, prípadne obsadením alebo neobsadením nejakej adresy v pamäti a podobne.

Pri tomto spôsobe skrytej komunikácie neexistuje žiadny známy spôsob ochrany.
Možnosť detekcie asi existuje iba v spojitosti s vyššie uvedenou technológiou aplikácie prevenčných a detekčných systémov na vstupe a výstupe lokálnej siete spolu s rozsiahlou neurónovou sieťou. Uvedená neurónová sieť by mala byť schopná rozpoznávať vzorce

komunikácie pri prenose (upravené napríklad fourierovou transformáciou) a upozorniť na prípadné odlišnosti od štandardného prenosu.

3. Zhrnutie

Je zrejmé, že uvedené metódy prenosu dát predstavujú nezanedbateľný stupeň rizika a je nutné sa nimi zaoberať pri projektovaní a riadení komunikačných kanálov. Vývoj metód môže byť predmetom skúmania v budúcnosti. Môžeme konštatovať, že vzhľadom na množstvo dát prenášaných v sieťach a pomer aký z tohto objemu môžu tvoriť skryté prenosy prakticky vylučujú použitie súčasných metód kontroly komunikácie. Navyše je evidentná potreba kontroly v reálnom čase a bežne dostupné výpočtové prostriedky pochopiteľne nie sú schopné poskytnúť adekvátny výpočtový výkon.

4. Zoznam bibliografických odkazov

(1) TYLER, J. : *Covert Data Storage Channel Using IP Packet Headers.* [online, cit. 20.9.2011], http://www.sans.org/reading_room/whitepapers/covert/covert-data-storage-channel-ip-packet-headers_2093

(2) SBRUSH, R.: *Network Covert Channels: Subversive Secrecy.* [online, cit. 20.9.2011], http://www.sans.org/reading_room/whitepapers/covert

(3) NEIL, J. – ZORAN, D. – SUSHIL, J.: *Information hiding: steganography and watermarking: attacks and countermeasures.* Berlin: Springer 12/2000, ISBN 978-0-7923-7204-2

(4) CHVARKOVA, I. - TSIKHANENKA, S.- SADAU, V.: (15 February 2008). *Steganographic Data Embedding Security Schemes Classification. Steganography: Digital Data Embedding Techniques.* In:Intelligent Systems Scientific Community, Belarus, 2011.

(5) Gi, J. - Greenstadt, R. - Litwack ,P. - Tibbetts, R.: *Covert Messaging Through TCP Timestamps*[online cit. 10.09.2011] http://www.eecs.harvard.edu/~greenie/tcpcovertchannels.ps

5. Adresa autora :

Igor Halenár, Ing. PhD.
UIAM MTF STU
Hajdóczyho 1
917 01 Trnava
igor.halenar@stuba.sk