Univerzita Pavla Jozefa Šafárika v Košiciach

Prírodovedecká fakulta

Výučba témy „Šifrovanie informácií“

Záverečná práca dištančného kurzu Klub učiteľov informatiky

2006 Ing. Anton Bača

Obsah

Úvod

Svet v 21. storočí nesie prívlastok elektronický. Elektronika, počítače, informačné a komunikačné technológie sú súčasťou nášho každodenného života. Bez týchto prostriedkov si našu existenciu už ani nevieme predstaviť. Človek, ktorý sa nevie pohybovať vo svete informačných technológií sa dostáva v spoločnosti do ústrania.

Veľmi veľkú úlohu v dnešnom svete zohráva internet. Táto gigantická sieť počítačov nám otvára nové možnosti, nové riešenia a prispieva k neohraničenej dostupnosti informácií. Všetky geniálne nápady a vynálezy ľudstva majú aj svoju temnú stránku a internet nie je výnimkou.Moderné technológie, počítače a internet nám všestranne pomáhajú a uľahčujú život. Miestami však pripomínajú oheň. Sú to dobrí sluhovia, ale zlí páni. Presne tak, ako keď deti učíme narábať s ohňom a aké bezpečnostné zásady musia dodržiavať, musíme aj našich študentov, žiakov, kolegov a zamestnancov naučiť, ako bezpečne narábať s výpočtovou technikou a internetom.

História a súčasnosť

Internet odštartoval revolúciu vo svete počítačov. S nástupom Internetu sa však objavili aj nové bezpečnostné riziká. V čase veľkých sálových počítačov bola bezpečnosť, vrátane súvisiacich kontrolných mechanizmov, centralizovaná a jasne definovaná. S nástupom osobných počítačov, lokálnych a globálnych počítačových sietí, sa však filozofia počítačovej bezpečnosti podstatne zmenila. Decentralizácia bezpečnosti spôsobila diametrálne odlišné bezpečnostné problémy ako aj potreby nových bezpečnostných mechanizmov, služieb a aplikácií. Nástup Internetu iba dovŕšil podstatnú zmenu bezpečnostnej politiky.

Internet v súčasnosti tvorí približne 30 000 000 prepojených počítačov. Počet používateľov je možné iba odhadnúť, pretože noví používatelia sa pripájajú prakticky každú minútu. Približné odhady hovoria o čísle 100 000 000. Takýto používateľský potenciál predstavuje vážnu bezpečnostnú hrozbu, pretože s rastom používateľov rastie aj počet osôb, ktoré prostredníctvom Internetu vykonávajú rozličné ilegálne aktivity. Oblasť hrozieb je veľmi široká, od priemyselnej špionáže, nekalej obchodnej súťaže, ilegálneho transferu technológií až po zvedavých študentov s množstvom voľného času.

Napriek problémom súvisiacich s bezpečným využívaním a používaním Internetu je však v súčasnej komerčnej i akademickej sfére prístup do Internetu v podstate nevyhnutnosťou. Internet je veľmi dôležitým komunikačným médiom. O vzniku Internetu nemá význam veľmi písať. Je však dôležité si uvedomiť jeden fakt. Internet síce vznikol ako projekt ministerstva obrany USA a bol pôvodne vyvinutý pre armádne účely, postupne sa však rozvíjal hlavne v univerzitnom prostredí. Jeho pôvodní používatelia nemali veľké nároky na bezpečnosť. Plne im postačovala možnosť vzájomnej komunikácie a výmeny informácií.

Skutočne, až do roku 1988 bezpečnosť Internetu nepredstavovala významnú položku. Počítačové vírusy sa iba začínali objavovať. Na bezpečnostné slabiny Internetu radikálne upozornil americký študent Robert T. Morris, ktorý v novembri 1988 napísal a "vypustil" do Internetu špeciálny program známy ako "Internetový červ". Tento program zneužíval chyby v nástrojoch a službách vtedajších verzií operačného systému UNIX a jeho sieťových aplikácií. Chyby dovoľovali programu

infikovať ďalšie počítače v Internete a Internetový červ dokázal položiť na kolená prakticky celý vtedajší Internet.

Pozitívnym dôsledkom Internetového červa bola radikálna zmena bezpečnostnej paradigmy Internetu. Bezpečnosť sa začala dostávať do popredia ako dôležitý aspekt využívania služieb Internetu a samotnej prevádzky Internetu. Na Carnegie Mellon University v USA bola založená skupina CERT (Computer Emergency Response Team) s cieľom centralizovať informácie o bezpečnosti v Internete, spolupracovať s výrobcami hardvéru a softvéru a upozorňovať na chyby v ich výrobkoch ako aj asistovať pri riešení bezpečnostných incidentov. Neskôr boli založené ďalšie bezpečnostné tímy vo viacerých štátoch a organizáciách na celom svete.

Heslá

Každý z nás sa už s nejakým heslom stretol a vôbec to nemuselo mať nič spoločné s výpočtovou technikou. Heslá sa už od nepamäti využívajú ako akási forma autorizácie. Aby sa obchodní cestujúci dostali cez brány starobylých miest, museli často poznať to správne heslo. V dnešnej dobe si pripomeňme napríklad heslo na vkladnej knižke alebo PIN na platobnej karte. Heslo teda predstavuje akúsi informáciu, ktorá je známa len obmedzenému počtu ľudí. Teda poznanie nejakého hesla nám zabezpečuje prístup k nejakým informáciám alebo prostriedkom. S rozvojom informačných systémov a výpočtovej techniky nadobúda heslo veľmi významné postavenie v metódach autorizácie prístupu. Dnešná spoločnosť si však málokedy uvedomuje riziká, ktoré takáto forma autorizácie so sebou prináša.

Reprezentácia hesiel

Najrozšírenejším operačným systémom na serveroch a pracovných staniciach (napríklad Sun, SGI atď.) je dnes operačný systém UNIX/Linux, ktorý má dlhú históriu a dnes určuje smer vývoja operačných systémov. V starších verziách OS UNIX/Linux boli autorizačné informácie uložené v súbore /etc/passwd, v ktorom každý riadok mal nasledujúcu štruktúru:

username:password:uid:gid:full name:home:shell

Teda každý riadok v tomto súbore nesie informácie o jednom používateľovi, je tam používateľské meno, zašifrované heslo a nejaké ďalšie informácie. Problém je v tom, že tento súbor musí byť prístupný pre všetkých používateľov, je teda možné získať zašifrované heslo ktoréhokoľvek používateľa a potom si toto heslo nejakým spôsobom rozšifrovať. V dnešných OS UNIX/Linux sa takisto využíva pre autorizáciu súbor /etc/passwd, lenže položka password je prázdna. Zašifrované heslá sa totiž ukladajú do súboru /etc/shadow, ku ktorému má prístup len správca systému, navyše sa používa bezpečnejšie šifrovanie.

Operačný systém Windows je najpoužívanejším systémom na osobných počítačoch v kanceláriách a domácnostiach. Reprezentácia a bezpečnosť hesiel je v tomto systéme rôzna od verzie k verzii. Začnime od začiatku, vo Windows 95/98 sa používateľské heslá ukladajú priamo do súborov, ktoré sú uložené v priečinku C:\WINDOWS, kde napr. používateľ Ferko má svoje jednoduchým spôsobom zašifrované heslo v súbore C:\WINDOWS\FERKO.PWL. Takže zistiť heslo nejakého z používateľov Windows 95/98 po prihlásení na počítač už nie je vôbec problém.

Výrazne lepšia bezpečnosť hesiel je v rade systémov Windows NT, tam patrí aj Windows 2000 a Windows XP. Heslá vo Windows NT sú uložené v bezpečných systémových štruktúrach nazývaných SAM (Security Accounts Manager) a to v dvoch formách: LM (Lan Manager) a NTLM (NT Lan Manager), s Windows 2000 prišla forma NTLM v2. Tieto zašifrované heslá sa dajú zo systému "vydolovať" len s určitou mierou systémových privilégií zo systémového súboru C:\WINDOWS\repair\sam, ten však musí byť aktualizovaný. Kameňom úrazu je, že Windows NT/2000 umožňuje zvoliť prázdne heslo a to dokonca aj pre účet administrátora. V skutočnosti to umožňuje aj Windows XP, ale ten, ak je heslo prázdne, tak aspoň zablokuje sieťové pripojenie cez tento účet. Bežne sa stáva, že používatelia pri inštalácii Windows NT/2000 zvolia prázdne heslo administrátora v domnienke, že s týmto počítačom pracujem aj tak len ja, tak načo dávať nejaké heslo. Ono je to síce pekné, že daný používateľ pracuje so systémom sám, ale ak je pripojený na internet, tak sa k nemu môže cez počítačovú sieť pripojiť ktokoľvek iný. Zadá účet administrátora, heslo žiadne a kľudne si pripojí celý disk C: s právom na zápis (a teda aj mazanie) a tak získa neobmedzené možnosti nad daným počítačom.

Lámanie hesiel

Heslo je často to jediné, čo nás v skutočnosti na internete chráni, resp. heslo predstavuje akýsi imaginárny internetový zámok, ktorý zabezpečuje naše súkromie a chráni naše dáta a naše osobné informácie. Na to, aby sme si vedeli vytvoriť skutočne bezpečné a nezlomiteľné heslo, musíme poznať rôzne druhy techník akými sa dajú heslá zlomiť. Tie najbežnejšie, najúčinnejšie a teda aj najviac využívané si predstavíme teraz.

Jednou z najjednoduchších a najpriamočiarejších metód je *hádanie hesla*. Útočník musí poznať nejaké informácie o svojej *„obeti“*, na základe ktorých sa pokúsi odhadnúť, aké má obeť heslo. Táto metóda možno vyznieva na prvý pohľad nereálne, ale v skutočnosti sa často a úspešne využíva. Útočník tu nemusí byť žiaden expert na programovanie alebo na výpočtovú techniku všeobecne, ale skôr veľmi dobrý psychológ, ktorý sa vie dobre vžiť do uvažovania a myslenia obete. Úspech tejto metódy je založený na tom, že málokto dáva svojmu heslu takú dôležitosť, ako by bolo treba. Preto sa veľmi často stretávame s heslami ako meno používateľa, meno partnerky, či meno nejakého štvornohého miláčika, prípadne kombinácia čísel dátumu narodenia a podobne. Toto všetko sú ľahko predvídateľné heslá a predstavujú veľké bezpečnostné riziko. Táto metóda je často využívaná aj preto, že niekedy to je jediná možná. Iné metódy lámania hesiel sú totiž založené na veľkom množstve pokusov a väčšina dnešných systémov sa proti takýmto útokom chráni. Jednoducho po šiestich neúspešných pokusoch o prihlásenie sa dané konto na niekoľko minút zablokuje.

Ďalšou často využívanou metódou lámania hesiel je *slovník*. Prakticky ide o to, že tajné heslo nebýva nejaké úplne nezmyselné slovo alebo nejaký náhodný reťazec znakov, ale nejaké obyčajné slovo, ktoré môžeme nájsť v slovníku. Často sa zvykne používať napríklad nejaké meno alebo niečo podobné. Takže v konečnom dôsledku si stačí zostaviť dobrý slovník predpokladaných výrazov a skúšanie hesiel môže začať. Pod pojmom slovník si netreba predstavovať bežný slovník slovenského jazyka. Na hádanie hesiel pomocou tejto metódy sa využívajú veľmi rozsiahle súbory slov, kde sa predpokladajú aj slová, ktoré by bežného používateľa ani vo sne nenapadli. V takýchto slovníkoch sa nachádzajú aj slová ako napríklad qwerASDF - prvé dva riadky na klávesnici zľava, druhý s použitím klávesy shift. Samotné lámanie

hesla potom vyzerá tak, že daný slovník a používateľské meno pošleme ako vstup nejakému programu a ten potom skúša všetky heslá, jedno po druhom. Takáto akcia môže trvať dlho, ale veď nikto sa nikam neponáhľa.

Poslednou známou metódou je metóda *brute—force*. Ako už z názvu vyplýva, ide o brutálny útok a úplne konkrétne o skúšanie všetkých možností. Program využívajúci túto metódu hádania teda začne skúšať všetky možné heslá. Začne asi takto: a, b, c, d, ... x, y, z, 0, 1, 2, ... 9, aa, ab, ac, ... Samozrejme, že určite nezabudne ani na veľké písmená a interpunkčné znamienka. Táto metóda teda skôr či neskôr odhalí každé heslo. Otázkou je teraz, čo znamená neskôr. Abeceda má 25 písmen a je rozdiel, či ich napíšeme veľké alebo malé. A keď k tomu prirátame ešte aj čísla, znaky s diakritikou a interpunkčné znamienka, mohli by sme sa dostať tak asi na číslo 100 (v skutočnosti však na oveľa menšie, pretože znaky s diakritikou a interpunkčné znamienka sa v heslách skoro vôbec nepoužívajú). Ak má teda heslo dĺžku jeden znak, tak metóda brute—force ho musí odhaliť najneskôr po 100 pokusoch. Ak by malo heslo dva znaky, tak by bolo treba najviac 10 000 pokusov = 100 x 100. A k tomu by sme ešte mali prirátať tých 100 pokusov, ktoré sme urobili, keď sme skúšali len jedno písmeno, pretože vlastne nevieme aké dlhé to nami hľadané heslo vlastne je. Ak by sme mali heslo s dĺžkou 8 znakov, tak by sme potrebovali 10 000 000 000 000 000 pokusov a samozrejme ešte aj tie na 7 znakov, 6, 5, ... Dokopy by ich bolo 10 101 010 101 010 100. Dnešné počítače (Pentium 4 - 3,2 GHz) vedia vyskúšať zhruba 6 090 hesiel (zašifrovaných cez FreeBSD MD5) za sekundu. Takže heslo o dĺžke 8 znakov by nám trvalo 1 658 622 348 278 sekúnd = 460 728 430 hodín = 19 197 018 dní = 52 595 rokov. Inak povedané heslá s dĺžkou 8 a viac znakov sa dajú považovať voči tejto metóde za bezpečné.

Bezpečné heslo

V prvom rade by nemala existovať žiadna vyvoditeľná spojitosť s našou osobou, ktorú by mohol šikovný psychológ vedieť odhadnúť. Určite by to nemalo byť žiadne celé slovo alebo reťazec znakov, ktorý predstavuje susedné klávesy na klávesnici. Heslo by malo mať dostatočnú dĺžku, teda minimálne 8 znakov (tým myslíme 8 znakov rôzneho charakteru - bežne sa používajú veľké písmená, malé písmená a čísla), aby sa nedalo uhádnuť ani metódou brute—force. Za bezpečné sa považujú heslá, ktoré sa skladajú z viacerých, nezávislých slov, ktoré sú písané

veľkými a malými písmenami, doplnené nejakými číslicami, prípadne interpunkčnými znamienkami. Často sa zvyknú aj nahrádzať niektoré písmená číslami. Dobrým receptom na bezpečné heslo sú aj prvé písmená slov nejakej známej vety. Len si treba dávať pozor, aby sme si tú vetu hovorili pri písaní naozaj iba v duchu.

Šifrovanie

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. V tejto kapitole hovoríme o princípoch a základnom rozdelení šifrovania informácií. Šifrovanie sa vo všeobecnosti delí na symetrické a asymetrické. Ďalej si povieme ako funguje elektronický podpis.

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 K. Symetrické šifrovanie sa skladá z dvoch častí, zašifrovanie (Encryption) a dešifrovanie (Decryption), pričom platí:

$$E(M, K) = T$$

a

$$D(T, K) = M$$

Kde 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).

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:

$$E(M, K1) = T$$

$$D(T, K2) = M$$

$$K2 \mathrel{!}= f(K1)$$

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
dpl6XLnt/LtaqNcpUjXceR38GR/zB7g5ZdO0VLWWiWfcUWVLIfOQnsnYL0OAl6no
fR1EB54hasQV4flWcVfrDXigRZr6E1STDSmSAJWtorRCTWFyZWsgTmVtZWNrYXkg
KEFkbWluaXN0cmF0b3IpIDxuZW1lY2theUBzcHJpdGUuZWRpLmZtcGgudW5pYmEu
c2s+iLQEEwECAB4FAkH/pyUCGwMGCwkIBwMCAxUCAwMWAgECHgECF4AACgkQYk7P
+SBqae63hwQArsVQpFUAKR5t2+gcvQumuFoCamgRoLMjYIL7d04XXo4Wb1iwW3my
sTzR3tSdlkZuQEeLNs3Rg3Yoe6KLhPdohNwOrXKmAAVkUkSBTjFsm+ICDYdPXgqo
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-----

Šifrovanie v praxi

Ak teda chceme napríklad poslať zašifrovaný e—mail s nejakou dôvernou informáciou, ako napríklad "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).

Použitá literatúra

Roman Baranovič, Ľudmila Moravčíková, Ľubomír Šnajder - **Internet pro střední školy**, Computer Press (1999)

www.cert.org

www.disa.gov

www.manualy.sk

http://cert.utc.sk

www.dtca.sk