Bezpečnost v informačních technologiích (KIV/BIT)

9. Bezpečnost počítačových sítí a operačních systémů
Počítačové viry

Ing. Pavel Král, Ph.D.

Katedra informatiky a výpočetní techniky
Západočeská Univerzita

20. dubna 2015

Obsah

Útoky - obvyklý postup

Obvyklý postup:

1. vyhledání vhodného počítače (PC v síti, příp. modemové připojení)
2. získání informací o stroji (OS, spuštěné daemony, apod.)
3. napadení samotné

- dostupnost nástrojů (ad 1-3) $\longrightarrow$ možnost útoků i počítačovými laiky

Vyhledání vhodného počítače:

1. mapování sítě
2. vyhledání bezdrátové sítě
3. wardialing

Mapování sítě

- zejména útoky na TCP/IP sítě (Internet, podnikový intranet)
- zjištění IP adresy (příp. množinu adres) útočníkem
  - dotaz do DNS → získání doménového jména instituce + některých IP adres
    - *nslookup* - jednoduchý DNS dotaz (př.nslookup seznam.cz)
    - *host* - základní informace o doméně (+ primární NS pro zasílání pošty)
    - *gethostbyname*, *gethostbyaddr* - převod adres ↔ jméno
- zjištění více informací (topologie sítě, aktivní adresy, adt.)
- → použití mapovacích programů
  - např. *Nmap Security Scanner* (Linux) viz `http://nmap.org/`
  - použití databáze *Whois*
    - informace o majitelích internetových domén, IP adres, infrastruktuře sítě, atd.
    - protokol whois
  - `http://ping.eu` - on-line nástroj, rozsáhlá funkčnost

Mapování sítě

ping

- zaslání požadavku *ICMP ECHO_REQUEST* zvolenému stroji
- odpověď *ICMP ECHO_REPLY*
- př: ping zcu.cz
- hromadný ping = ping na seznam adres, nečeká na odpověď (př. fping)

zahájení TCP spojení

- zaslání TCP "SYN" na zvolený port
  - na portu je *daemon* → odpověď TCP "SYN ACK"
  - port není obsazen → odpověď ICMP PORT_UNREACHABLE
- použití na sítích s blokací požadavku *ICMP ECHO_REQUEST*

Obrana proti mapování sítě

- vypnutí služby *ECHO*
- zákaz příchozích/odchozích paketů *ECHO_REQUEST*/*ECHO_REPLY* - firewall
- periodická kontrola sítě administrátorem
  - připojeny nepotřebné (nepoužívány uživateli) systémy?
  - **ano** $\longrightarrow$ odpojit

Poznámka:

- – ochrana proti nalezení počítačů prostřednictvím otevřených portů není

Vyhlednání bezdrátové sítě

- často provozovány (neoficiálně) nezkušenými uživateli → nezabezpečeny vůbec nebo zabezpečeny defaultním nastavením
- možnost zjištění (útočníkem) do vzdálenosti několika set metrů
- většinou sítě WLAN - tj. protokol *IEEE 802.11*
  - nejčastější standardy 802.11b, g a n - WiFi síť
  - identifikátor sítě *SSID (Service Set Identifier)*
  - vysílání SSID v pravidelných intervalech jako broadcast → potenciální klienti - jednoduchá možnost zobrazení dostupných bezdrátových sítí, příp. připojení
  - možnost odposlechu i v případě konfigurace bez odpovědi (posílání SSID jako otevř. textu)

Útok na bezdrátovou síť

- vybavení: notebook s WiFi kartou, přísl. SW (běžné)

1. nalezení sítě
   - bez potřeby spec. SW (zobrazení dostupných sítí defaultně v OS + info o případném zabezpečení)
   - spec. SW - např. *Netstumbler* `http://www.netstumbler.org` nebo *Kismet* - zobrazení i sítí s vypnutou odpovědí SSID
2. získání IP adresy pomocí DHCP (Dynamic Host Configuration Protocol) protokolu
   - často dostane kdokoli o ní požádá → přihlášení do sítě
   - příp. spec SW pro získání informací o síti ("odchytávání" paketů)
     - např. Ethereal `http://www.ethereal.com` příp. *Aircrack* `http://www.aircrack-ng.org`

- Pozn.: nástroje zpravidla součástí *Backtrack* (dnes *Kali*) Linuxu (http://www.kali.org/)

Obrana proti útokům na bezdrátovou síť

- skrytí SSID (konfigurace bez odpovědi)
  - možnost odhalení pomocí pasivního odposlechu během několika minut
- kontrola MAC adres (= možnost připojení pouze "známých" MAC adres)
  - přenos MAC-adresy při spojení v nezašifrovaném tvaru
  - $\rightarrow$ jednoduchá možnost zjištění pomocí odposlechu
  - $\rightarrow$ nastavení na stejnou
- omezení území pokrytého signálem
  - PC v jednom směru $\rightarrow$ použití směrové antény
- vypínání WiFi, když nepoužívána
  - účinné $\times$ nepraktické :-)

Obrana proti útokům na bezdrátovou síť

- změna defaultního SSID na AP
  - změna názvu AP od výrobce → ztížení určení zařízení
  - → minimalizace použití popsaných útoků na konkrétní HW příp. předvypočtených tabulek
- šifrování WEP + hesla
  - možnost prolomení pomocí přísl. SW za několik min
- **šifrování WPA nebo WPA2 + hesla**
  - účinné → vhodné používat

Wardialing

= skenování telefonních čísel pomocí modemu

Obvykle násl. scénář útoku:

1. zjištění tel. čísel cílového/ých subjektu/ů
2. tel. na všechny klapky
3. $\rightarrow$ získání tel. čísel s připojenými modemy
4. pokus o připojení pomocí terminálového prg., zjištění typu systému a info. zda vyžadováno heslo
5. vyžadováno heslo $\rightarrow$ uhodnutí nejčastěji pomocí připravených tabulek (slovníků)

Wardialing - obrana subjektu

- def. pravidel pro připojování modemů na tel. linky
- centrální registrace všech modemů (DB nepřístupná zvenčí)
- periodická kontrola pomocí wardialingu - odpojení neregistrovaných zařízení

Poznámka:

- experiment: obvolání 2,6 M tel. v Berkeley, nalezení 20 tis modemů, 200 bez zabezpečení

Zjištění informací o stroji

- zjištění umístění stroje - např. *traceroute www.seznam.cz* v Linuxu
- scan portů = zjištění, na kterých portech servery $\times$ volné porty
- zjištění OS
- hledání zranitelných míst

Scan portů

- určení komunikace: IP adresa, protokol a port
- naslouchání serveru na daném portu (možnost změny defaultního nastavení)
- nejčastěji:
  - port 80 = http
  - porty 20 a 21 = ftp
  - 22 = ssh
  - ...
- = informace, přes který port možno vést útok

Obrana proti scanu portů

- obvykle: scan portů $\longrightarrow$ **útok**
- $\longrightarrow$ instalace SW pro aut. detekci (např. *iplogger*)
- informace o zaslání paketů na různé porty v "krátkém" čase
  - e-mail administrátorovi
  - logování
  - zákaz zdrojové IP adresy

Problém

- velmi obtížná identifikace distribuovaného skenu (z několika IP adres)

Zjištění OS

1)

- definice protokolů TCP/IP v přísl. RFC
- × nepokryty všechny odpovědi na nesprávně vytvořené pakety

Př:

- TCP SYN odpověď by měla být ACK
- odpověď v případě chybného nastavení příznaků (SYN-FIN-PUSH-URG) - závislost na OS
- → možnost **určení OS**

2)

- útočník - odposlech provozu sítě (broadcast technologie + vhodné umístění útočníka, příp. WiFi)
- → analýza komunikací v síti → **určení OS**
- Př: podle počátečního TTL (Time to Live), velikosti okénka, max. velikosti segmentu, apod.

Obrana proti útokům na zjištění OS

- samostatně nepříliš užitečná
- proxy firewall - všechny stroje skryty za firewallem (informace o hlavičce neprojdou mimo LAN)
- Linux 2.4 možnost nastavení klamné "osobnosti OS" více viz `http://ippersonality.sourceforge.net`

Hledání zranitelných bodů a obrana proti útoku

- existence řady chyb v OS
  - Windows např. viz: `http://technet.microsoft.com/en-us/security/advisory`
- útočník - snaha minimalizace ruční práce (manuální spouštění SW nástrojů)
- $\longrightarrow$ obvykle DB skriptů (jednoduché přidání dalšího testu)

Obrana

- zastavení všech nepotřebných serverů
- instalace bezpečnostních aktualizací
- periodická kontrola sítě - okamžité řešení nalezených problémů

Napadení

- ruční - pokus o přihlášení (odhadnutí jména a hesla)
  - úspěch ← používání nevhodných hesel (viz přednáška č. 5)
- prostřednictvím SW nástrojů
  - slovníky hesel
  - hádání hesla hrubou silou
  - zjištění hesla odposlechem sítě

Obrana

- **dodržování zásad pro tvorbu hesel !!!**
- **neposílat jméno/heslo otevřeným kanálem !!!**
- změna všech defaultních hesel po instalaci OS
- logování úspěšných/neúspěšných přihlášení
  - Linux viz /var/log/auth.log
- při přihlášení informace o posledním přihlášení (datum, čas, stroj)
  - → možnost odhalení neoprávněného přístupu

Zjištění hesla odposlechem sítě

- síť založena na *broadcast* technologii (např. Ethernet + HUBy, příp. WiFi síť)
- $\longrightarrow$ možnost sledování provozu lib. PC na segmentu
- zasílání hesel v otevř. textu některými protokoly
  - telnet
  - ftp
  - pop
  - ...

Obrana

- nepoužívání broadcast technologie, tj. nahrazení HUBů pomocí switchů, šifrovat WiFi sítě
- zákaz nešifrovaných služeb, tj.
  - telnet $\longrightarrow$ ssh
  - ftp $\longrightarrow$ sftp/scp
  - pop $\longrightarrow$ imap

Napadení OS
Příklady bezpečnostních chyb v OS Windows

- "0day vulnerability" = příklad využití bezpečnostní chyby zveřejněn
- → aktivně využíván

- všechny verze MS Windows
- útok prostřednictvím IE
- zpracování MHTML (Mime Encapsulation of Aggregate HTML)
- → kontrola nad OS
- více viz http://technet.microsoft.com/en-us/security/advisory/2501696

Napadení OS
Příklady bezpečnostních chyb v OS UNIX

- použití utility *lpr* - tisk daného souboru
- *lpr -r soubor* - smazání souboru po vytištění
- starší verze UNIXu - možno provést *lpr -r /etc/passwd*

Napadení OS
Příklady bezpečnostních chyb

- chyba v přehrávači VLC (do verze 0.8.6)
- nabourání podvržením vhodně konstruovaného URL (angl. URL format string injection),
- v open dialogu pro přehrávání Audio a Video CD formátů
- určité podobnosti s zápisem v jazyku C
- zneužití $\longrightarrow$ spuštění lib. kódu s právy lokálního uživatele
- více viz `http://diit.cz/clanek/mnoho-verzi-vlc-az-po-086-obsahuje-bezpecnostni-diry`

IDS (Intrusion Detection System)
Systém pro odhalení průniku

- obranný systém, monitoring síťového provozu, snaha odhalení podezřelých aktivit
- nejen proniknutí samotné, ale i předcházející aktivity (např. skenování portů, apod.)
- upozornění na podezřelé aktivity (mail, SMS), zákaz IP adresy

Př:

- Snort (http://www.snort.org/)
- OSSEC (http://www.ossec.net/)

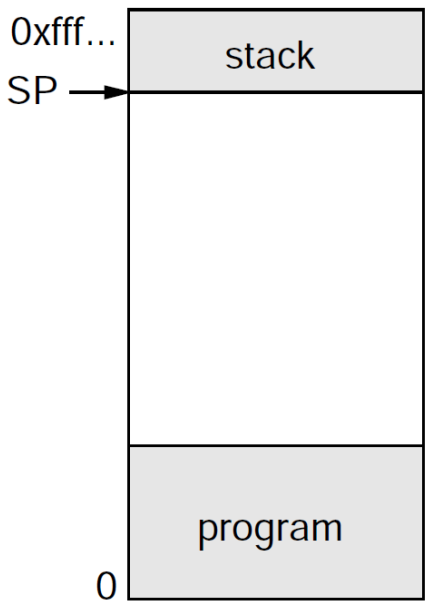
Přetečení bufferu na zásobníku (Buffer Overflow)

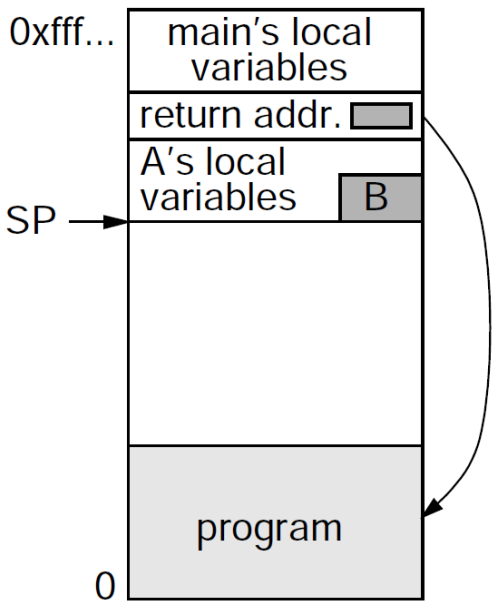
- téměř všechny OS + většina systémových SW v jazyce C (efektivita kódu)
- $\times$ bez kontroly mezí polí (pole = jiný zápis operace nad ukazatelem)
- $\longrightarrow$ možnost přepsání části paměti $\longrightarrow$ závažný problém
- $\longrightarrow$ spouštění škodlivého kódu, převzetí kontroly nad strojem

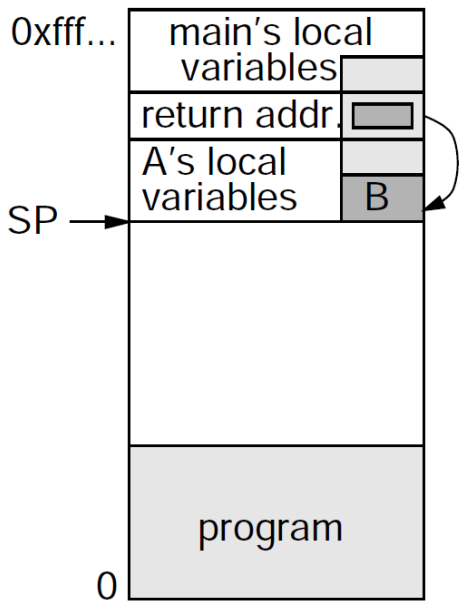
Přetečení bufferu - princip

- běh programu - zavolání procedury A
- uložení návratové adresy na zásobník, spuštění procedury
  - procedura - vytvoření na zásobníku místa pro loc. proměnné - např. velikost 512B
  - zadání "delších" dat - např. 1000B $\rightarrow$ přepsání návratové adresy (+ části paměti)
  - návrat z procedury, vykonávání instrukcí na "nové" návratové adrese
  - náhodný obsah $\rightarrow$ pád programu
  - připravený škodlivý kód $\rightarrow$ např. kontrola stroje

Přetečení bufferu - princip







Přetečení bufferu - triviální příklad


```
void get_input() {
   char buf[512];
   gets(buf);
}
void main(int argc, char *argv[]) {
   get_input();
}
```

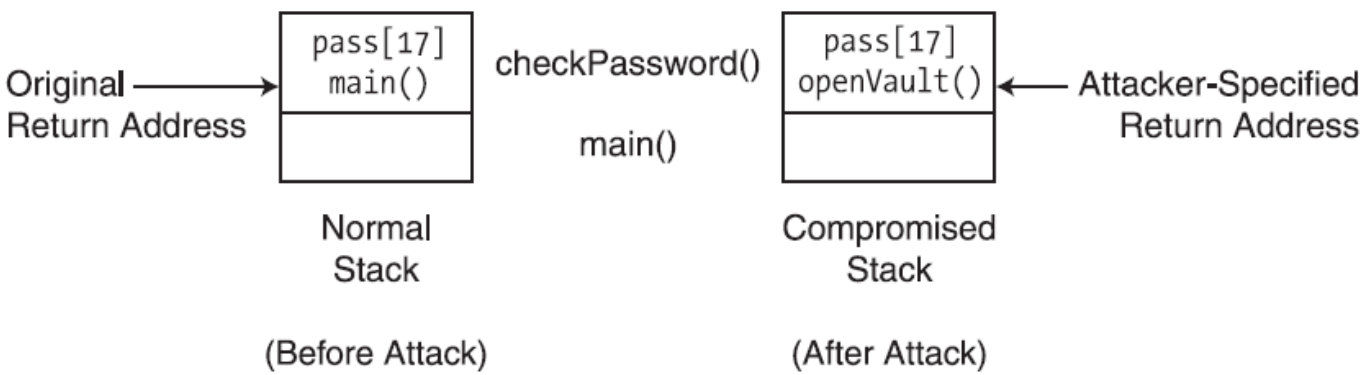
- zadán vstup delší než 512 znaků $\rightarrow$ přetečení zásobníku

Přetečení bufferu - složitější příklad


```
int checkPassword() {
   char pass[16];
   bzero(pass, 16); // Initialize
   printf ("Vlozte heslo: ");
   gets(pass);
   if (strcmp(pass, "heslo") == 0)
        return 1;
   else
        return 0;
}
```

```
void openVault() {
// Opens the vault
}

main() {
   if (checkPassword()) {
      openVault();
      printf ("Vault opened!");
   }
}
```



Přetečení bufferu - obrana

- **programy - kontrola, zda délka_vstupu $\leq$ velikost_bufferu**
- minimalizace počtu programů se spec. právy v OS
- konfigurace OS - zákaz spouštění kódu v zásobníku ($\times$ vyžadováno některým SW, neřeší vše - odskok na rutinu mimo zásobník)
- více viz kniha [1]

Počítačové viry

PRÁVĚ JSTE OBDRŽELI MANUÁLNÍ VIRUS:
Tento virus pracuje na čestné bázi. Takže prosím nejprve tuto zprávu rozešlete na všechny adresy ve vašem mailing listu, a pak náhodně zrušte několik souborů na vašem disku.

z povídky Josefa Pecinovského "Troglodyt a maska"

Počítačové viry [2]

- = název pro škodlivý SW různého druhu
- tzv. MALWARE - MALicious softWARE
- zpravidla - proniknutí do systému bez vědomí uživatele → škodlivá činnost
- výskyt především v prostředí OS Windows
  - velké rozšíření
  - množství uživatelů laiků

Rozdělení

- počítačový virus
- počítačový červ (worm)
- trojský kůň (trojan horse)
- Rootkit
- Ostatní malware - Adware, Spyware, atd.

Počítačový virus

= SW, schopnost vytváření kopie sebe sama a infikovat tímto počítač často spojeno s nějakou destruktivní činností (mazání/změny souborů, formátování disku, apod.)

Vlastnosti

- neschopnost samostatného šíření - potřeba "hostitele"
  - spustitelný soubor
  - systémová oblast disku
  - různé dokumenty (word/excel - tzv. makro-viry, apod.)
- obvykle infikace spuštěním zavirovaného prg. - zdroj (Internet, přátelé)
- replikace - připojování sebe sama k existujícím programům, které jsou spuštěny
- *rezidentní* $\longrightarrow$ v paměti i po ukončení hostitelského programu

Př:

- Sušenka - rezidentní; napadání spustitelných COM souborů (prodloužení); vlastní obsluha přerušení časovače (INT 1Ch) a klávesnice (INT 9) $\longrightarrow$ zastavení práce uživatele, napsání textu "Dej mi susenku"; napsání "susenka" $\longrightarrow$ možnost pokračování v práci

Počítačový červ

=SW, schopnost šíření seba sama bez potřeby hostitele

Vlastnosti

- šíření pomocí síťových paketů
- pravidelné rozesílání infikovaným počítačem
- využívání bezpečnostních děr v OS/aplikacích
- zpravidla neničení souborů $\times$ kontrola a narušení síťového připojení

Př:

- Lovsan / Blaster - využití přetečení zásobníku DCOM RPC rozhranní (vzdál. volání procedur, Windows XP)

Trojský kůň

na první pohled užitečný SW → na hostitelský počítač umístěn z vůle uživatele
většinou užitečná funkce (spořič obrazovky, zpracování fotografií, apod.), současně škodlivá činnost

Vlastnosti

- neschopnost replikace (potřeba instalace v dobré víře)
- obvykle shromažďování informací (hesla, apod.) → tvorba zadních vrátek (backdoor) - možný vstup hackera
- zneužití stroje (rozesílání spamu, zamaskování identity pro DoS a další útoky, atd.)

Př:

- Waterfalls.scr - volně šiřitelný spořič obrazovky; spuštění → otevírání portů a poskytování crackerům vzdáleného přístupu do PC

Rootkit

= program, umožnění hackerovi zakrytí provedené nekalé činnosti
nahrazení některých systémových programů (login, ls, atd.) a systémových knihoven (libproc.a)

Vlastnosti

- velmi obtížná zjistitelnost ← narušení činnosti SW určeného pro jejich odstranění
- (zpravidla) neodstranitelnost ← instalace jako součást jádra OS → reinstalace OS
- neschopnost samostatného šíření (tj. infikace jiného PC)

Adware

= obvykle užitečný SW, nabízen zdarma, ztěžování práce uživatele zobrazováním reklamy

Vlastnosti

- neschopnost samostatného šíření
- obtěžování uživatele
- zatížení síťového připojení a OS
- zpravidla snadná odhalitelnost (obvykle souhlas s instalací)

Spyware

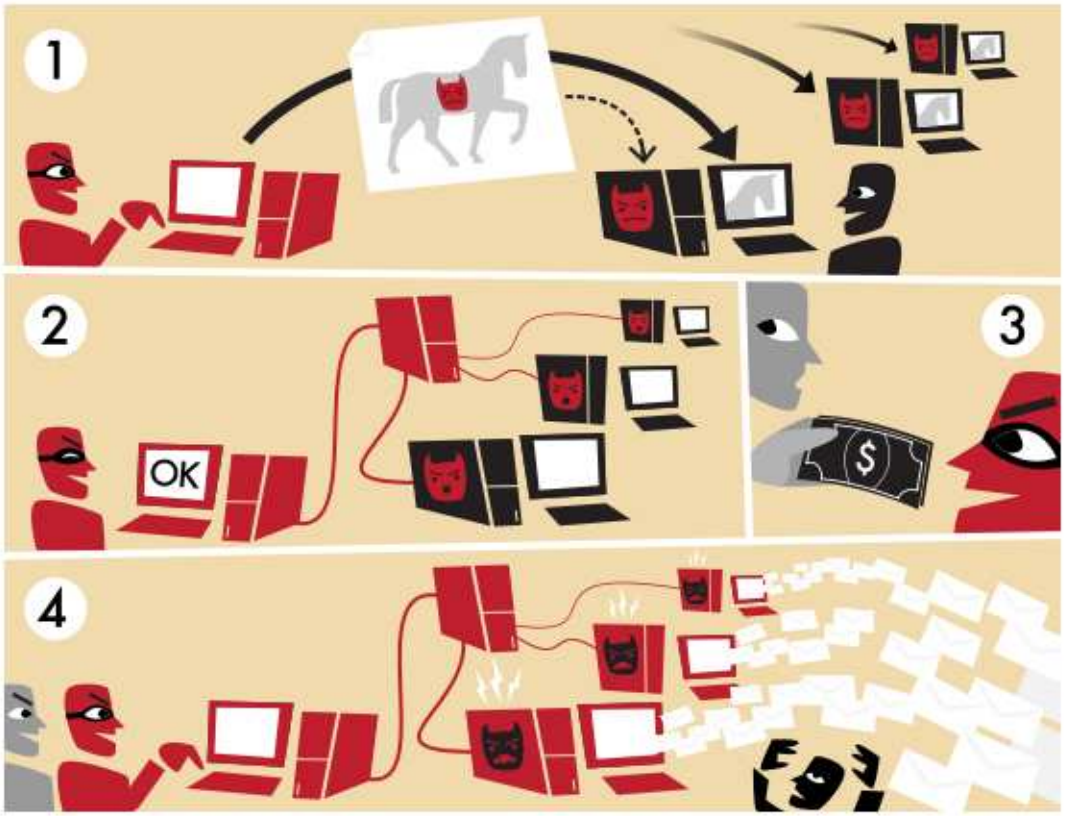
= malware, odesílání informací (adresy navštívených stránek, instalované prg., apod.) bez vědomí uživatele po Internetu

Vlastnosti

- zpravidla odesílání pouze "statistických" informací (ne hesla, apod.)
- zdůvodněno potřebou cílené reklamy
- zatížení síťového připojení a OS $\rightarrow$ snadná odhalitelnost

Botnet

= síť infikovaných počítačů, které jsou centrálně řízeny z jednoho centra k provádění škodlivé činnosti



Obrázek: [Wikipedie]

Antiviry
Obrana proti virům

= programy určené na detekci a odstranění malware

Základní antivirové techniky:

- **1) použití virové DB** - zjištění shody části souboru/paměti/místa na disku s některým známým virem
- nalezena shoda →
  1. oprava/vyléčení souboru odstraněním viru
  2. umístění souboru do karantény (zamezení šíření)
  3. smazání infikovaného souboru (i s virem)
- nutnost aktualizace virové DB ← odhalení "nových" virů
- **2) identifikace "nebezpečného" chování** SW
  - pokus o zápis dat do spustitelného souboru
  - → řada falešných poplachů
  - → upouštění od používání

Antiviry

Základní antivirové techniky

- **3) heuristická analýza**
- identifikace potencielně škodlivého SW pomocí sady pravidel příp. vážících metod (nastavení dle znalostí chování virů)
- princip = simulace spuštění SW na specif. virt. stroji
- **4) kontrola integrity**
- porovnání aktuálního obsahu souborů se stavem po instalaci (případně inicializace antiviru)
- použité informace (délka, datum, CRC, apod.)

Antiviry - poznámky

- antivirus = základ zabezpečení každého PC s OS Windows
- → **používat vždy !!!**
- kvalitní (české) antiviry:
  - Avast `http://www.avast.com`
  - AVG `http://www.avg.com`
  - NOD 32 `http://www.eset.cz`
- vhodné použití tzv. *Internet suite* = antivir, antispyware + firewall; stále aktivní
- Linux & Mac OS X - jiná technologie → mnohem lepší ochrana před viry (i bez antiviru)

Hoax

- ???
- http://www.hoax.cz

Phishing (Rhybaření)

- ???
- http://www.hoax.cz/phishing

Užitečné adresy

- http://www.viry.org/ - kódy virů ke stažení a studiu


Neil Daswani, Christoph Kern, and Anita Kesavan,
Foundations of Security: What Every Programmer Needs to Know,
Apress, February 15 2007,
ISBN: 978-1-59059-784-2.


Igor Hák,
Moderní počítačové viry,
http://www.viry.cz, 2005.