Protecting Your PC and Your Data, Part II

Jerry Seregni
WWL-TV Channel 4
Research Director/Technology Analyst
(504) 529-6275
Jerry@wwltv.com

The Not-So-Blessed Trinity

- **Trojan horse** – A program that appears harmless but contains harmful code designed to exploit or damage the host system.
- **Worm** – Uses self-propagating malicious code that can automatically distribute itself from one computer to another through network connections.
- **Virus** – Uses code written with express intention of replicating itself. A virus attempts to spread itself from PC to PC by attaching itself to the host system

Target Environments

- **Devices** – PC, Macintosh computer, PDA, cellular phones.
- **Operating Systems** – MS-DOS, Windows 9*x*, Windows NT/2000/XP, Mac Classic OS, Mac OS X, Linux, FreeBSD, Unix, Be OS, etc. Cherobyl virus (CIH) of late 1990s only attacked Windows 9*x*.
- **Applications** – Certain app must be installed
  - LFM.926 of 2002 could only attack if Shockwave Flash (.swf) files could execute on a target system;
  - **Alternative Browser Strategy** Using Mozilla, Opera, or Netscape Communicator instead of Microsoft Internet Explorer. IE currently has 98% of the Windows market.

Carrier Objects

- **Executable files** - .exe files, but also includes .com, .sys, .dll, .ovl, .ocx, and .prg files
- **Scripts** – VB Script, JavaScript, AppleScript, Perl. Extensions: .vbs, .js, .wsh, .prl
- **Macros** – Microsoft Office macros (Word, Excel, Outlook), Lotus Ami Pro
- **Boot Sector** – Master Boot Record (MBR) or DOS boot record

Transport Mechanisms

- **Removable media** – floppy diskettes. This used to be the preferred method.
- **Network shares** – The new preferred method for attacks: Windows File and Printer Sharing
- **Network scanning** – IP port scanning
- **Peer-to-Peer Networks** – Napster, Kazaa, WinMX
- **E-Mail** – Second most popular transport method
  - **Mailer** – Uses mail client; SMTP server
  - **Mass Mailer** - Searches for address books
- **Remote Exploit** – Often seen in worms. The infamous Slammer worm took advantage of a vulnerability in MS SQL Server 2000.

Payloads

- **Backdoor** – Frequently use FTP, Port 21, or Telnet, Port 23.
- **Data corruption or deletion** – Trigger mechanism is to delete hard disk. This is why it is important to disconnect the network cable immediately when attacked.
- **Identity theft**
- **Information theft**
- **Denial of Service (DoS)**
- **Distributed Denial of Service (DDoS)**

Denial of Service Attacks

- **System shutdowns**
- **Bandwidth flooding**
- **Buffer overflow**
- **Network DoS** – SYN Flood Attacks
- **DNS Spoofing**
- **Service disruption** – Zero transactions per second mean big $$$ losses for online businesses.
- **“Five Nines”** – The goal of maintaining a system uptime of 99.999% per year.

The Reality of “Five Nines”

Availability	Downtime Per Year (3651/4 x 24)
99.9999%	32 seconds
99.999%	5 minutes, 15 seconds
99.99%	52 minutes, 36 seconds
99.95%	4 Hours, 23 minutes
99.9%	8 Hours, 46 minutes
99.5%	1 day, 19 hours, 48 minutes
99%	3 days, 15 hours, 40 minutes

Trigger Mechanisms

- **Manual execution**
  - Social engineering – email spoofing with tempting subject fields.
- **Semi-automatic execution**
- **Automatic execution**
- **Time bomb** – MyDoom.B was set to attack Microsoft.com on Feb. 3, 2004 and SCO on February 1, 2004.
- **Conditional** – “Logic bomb,” based on keystrokes, the existence of a certain file, launching a certain application, etc.

Defense Mechanisms

- **Armor** - Detecting debuggers or other tools for analysis
- **Stealth** – Attempts to hide itself
- **Encryption** – Encrypts itself to a payload. Popular with keystroke loggers. Uses static routine, not polymorphic.
- **Polymorphic** – Uses unlimited number of encryption routines to avoid detection. Mutation engine.
- **Oligomorphic** – Similar to Polymorphic, but uses a *limited* number of encryption routines to avoid detection.

Other misdeeds…

- **Easter Eggs** – Programmers love to put secret commands in programs. Example: Type “volcano” in 3D Text screensaver of Windows 9*x*.
- **Man-in-the-Middle** – Using *spoofing* to intercept traffic, examine or modify it, and then relay it to the intended recipient.
- **Phishing** – Impersonating legitimate Web sites for the purpose of identity theft
- **Retro Virus** – A virus that disables anti-virus software, bars access to the Registry Editor, Windows Update, etc.
- **Zapping** – Code that tries to bypass security systems, avoid IDS, detect honeypots, etc.

Other misdeeds…

- **Didling** – Data integrity, non-repudiation
- **E-Mail Jokes** – Waste bandwidth; email distribution lists can disclose otherwise confidential email addresses.
- **E-mail Hoaxes** – Harmless and not-so-harmless
- **E-mail Scams –** Nigerian fortunes, chain letters, etc.
- **SPAM**
- **Spyware**
- **Adware**
- **Cookies**

Adware / Spyware

- **Is it Legal?** Adware is a legal Trojan horse program, but spyware sometimes crosses the line. Examples: Ad Hijacking; Cookie Harvesting
- **Freeware?** A program is “free” as long as you agree to be monitored. Privacy issues; performance issues
- **User Consent?** Most users don’t know that they have agreed to be monitored. Relies on the fact that few people bother to read the EULA.
- **Easily Removable?** The monitoring component of the program is **always active** and does not go away, even after the host program is uninstalled. Spyware is not always listed in Control Panel | Add/Remove Programs.

Elements of Computer Security

- **Authentication** - Badges, passwords, biometrics
- **Authorization** - SAM, ACL, LDAP, Kerberos, Microsoft Active Directory, Novell eDirectory, Sun iPlanet
- **Confidentiality** – Encryption (EFS and IPSec)
- **Data Integrity** – Hash Algorithms, PKI, PGP
- **Software Defenses** – Anti-Virus Software, Anti-Spyware Software, Anti-SPAM Software, Personal Firewalls, Intrusion Detection Systems (Snort)
- **Physical Defenses** – Networks, Locks, Alarms
- **Fault Tolerance** - Surge Protectors, UPS
- **Data Recovery** – Backups, RAID

Multi-Factor Authentication

- **What You Know** – Username, Password, PIN
- **What You Have** – Smart Card, ATM Card
- **What You Are** – Retina Scan, Biometrics
- **What You Do** – Open Bank Account at Participating Banking Institution, activate card by telephone, insert ATM Card, input PIN, etc.

Most Transactions Today Still Rely on Single-Factor Authentication.

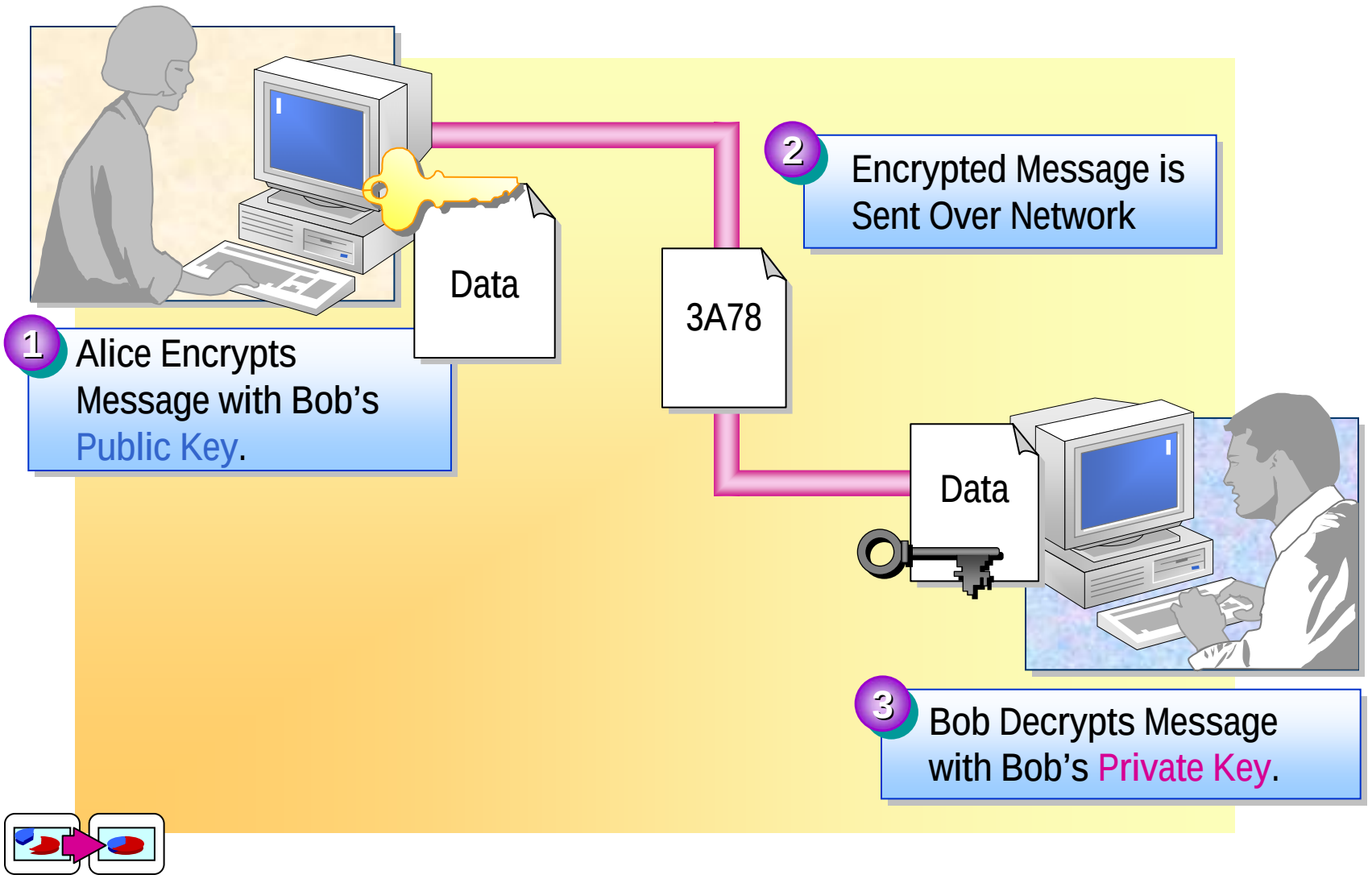
Coming Soon: More Encryption

- **Encryption** - scrambling of messages to protect privacy, can be decrypted by receiver using a “key.”
- **EFS -** Encrypt files stored on local hard disks; stolen laptops
- **IPSec -** Encrypt data in packets as they traverse the Web; prevents “sniffing”

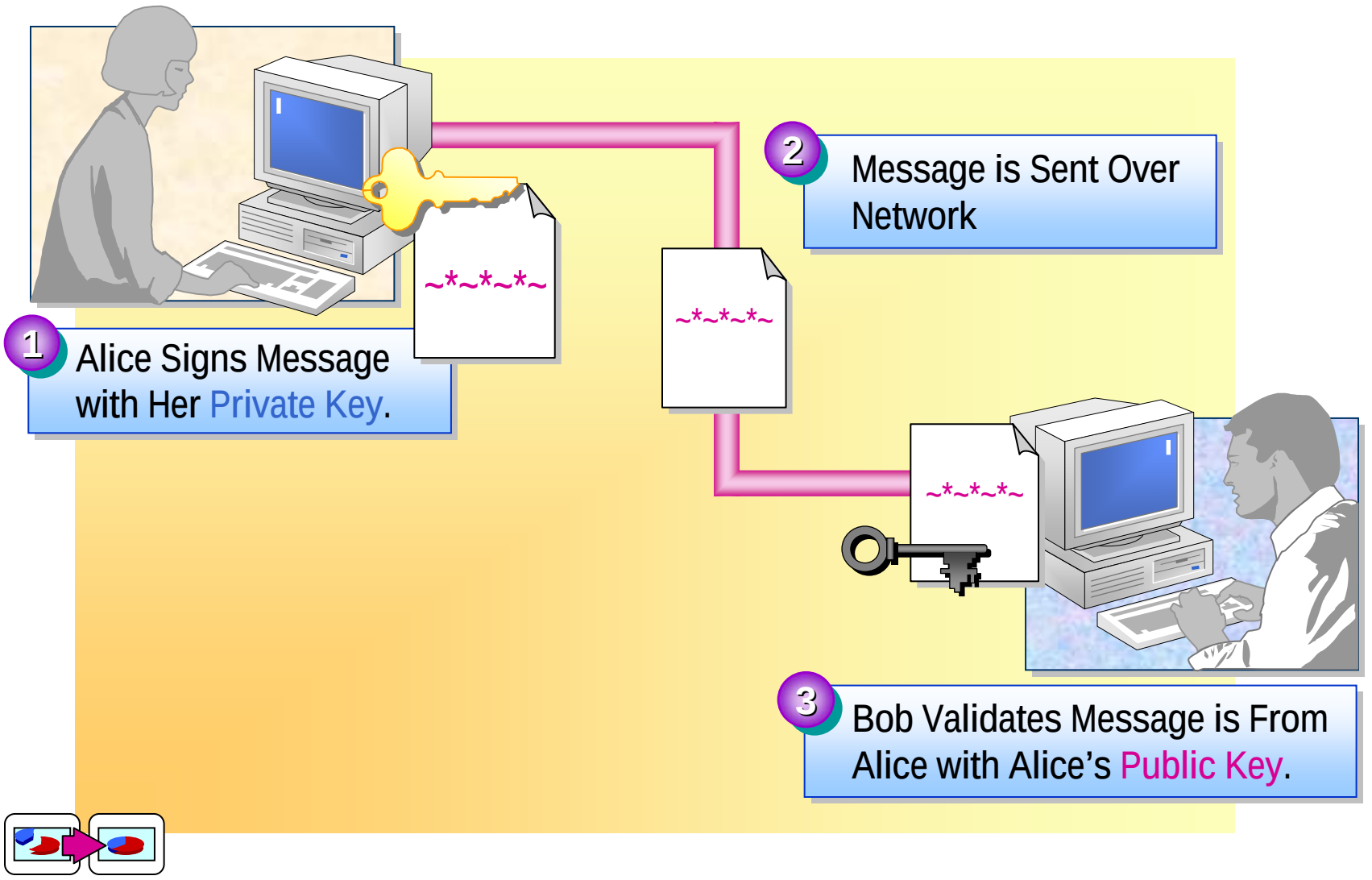
Coming Soon: More PKI

- **Public Key Infrastructure (PKI)** – Public and Private Keys (asymmetrical keys) used in combination with symmetrical keys (shared secret)
- **Certificate Authorities** – 3P rely on a commercial CA: Thawte, Verisign, etc.
- **Self-Signing CA** - Microsoft Windows Server Operating Systems, PGP

Public Key Encryption



Public Key Authentication



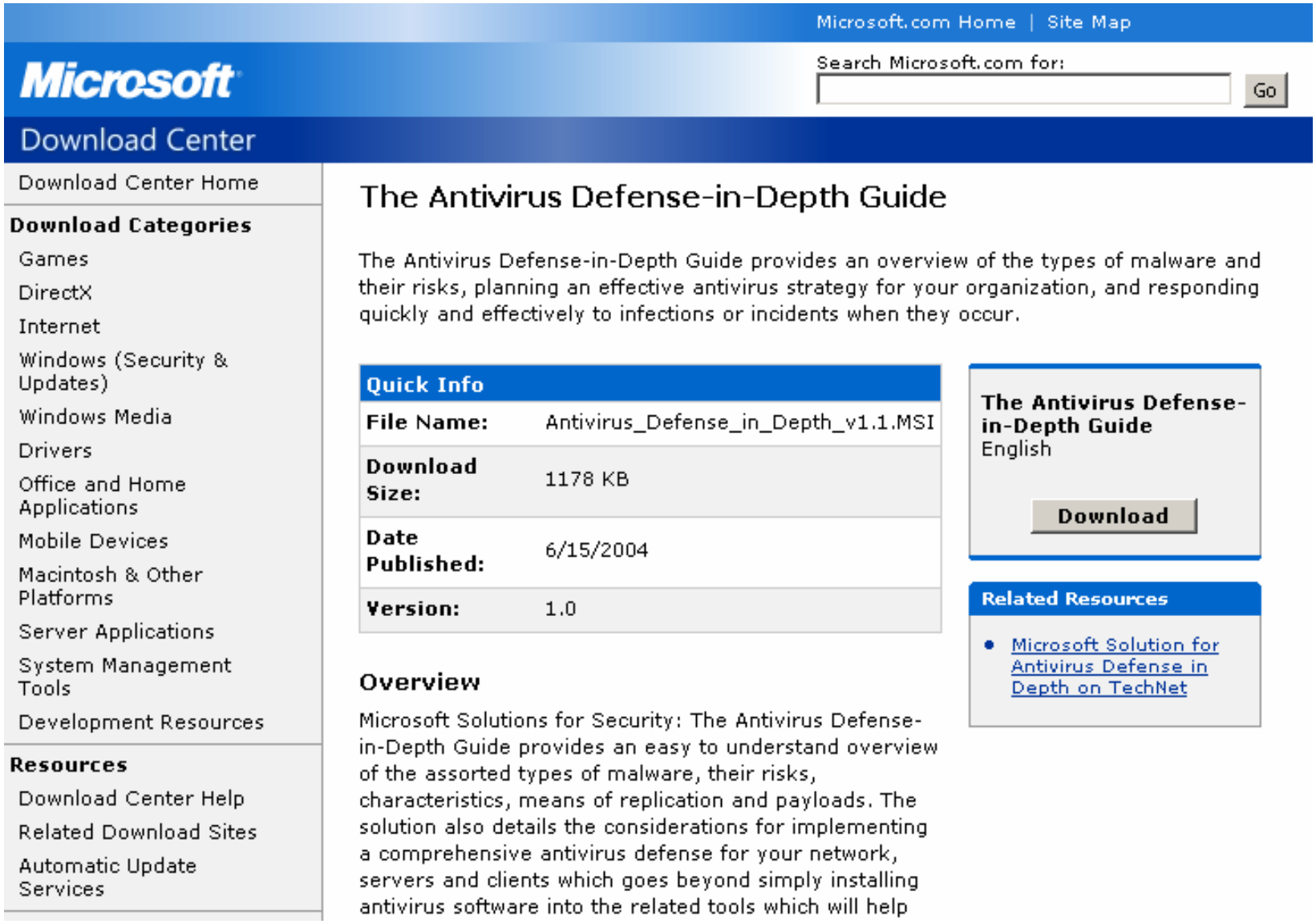
Eliminating Junk E-mail

- White-List Filters - Qurb 2.0
- Black-List Filters - I Hate SPAM, SPAM Assassin, Outlook Express
- Heuristic Filters
- Bayesian Filters
- Laws – CANSPAM Act of 2003
- Verify Senders: MS Caller ID; DomainKeys (Yahoo and Sendmail); Sender policy Framework (SPF)
- Assign a cost for sending e-mail? Bill Gates says “make them solve a puzzle.”

Microsoft®

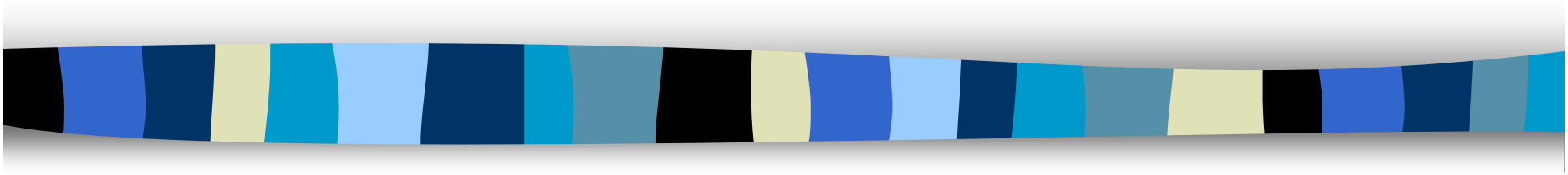
- Windows XP Server Pack 2
  - *Windows Security Center in Control Panel*
  - *Pop-up Ad Blocker in IE (enabled by default)*
  - *Windows Update v.5 (enabled by default)*
  - *Windows Firewall (formerly Internet Connection Firewall)*
- *Microsoft Office 2003: Windows Rights Management*
- *Hotmail: SmartScreen Anti-Spam Filter*
- Coming Soon: Windows Update Services / Baseline Security Analyzer 2.0
- Coming Soon: Sender ID (formerly Caller ID)
- Coming Soon: WinFS (New File System)
- Coming Soon: Windows Anti-Virus Software?

MS TechNet: Overview of the Types of Malware and Risks



http://www.microsoft.com/technet/security/guidance/avdind_0.mspx

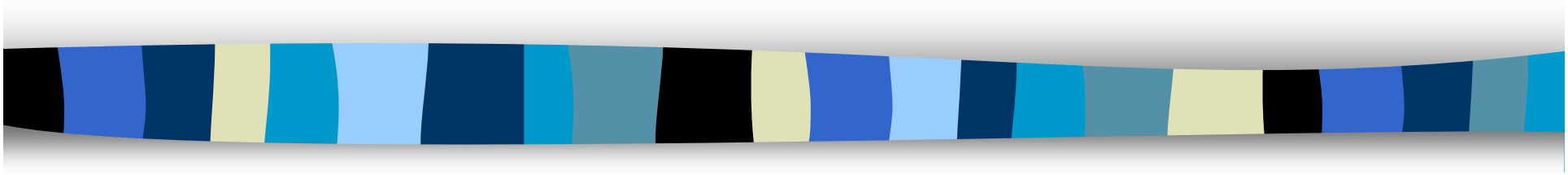
DEMONSTRATION



“Why is my computer so slow?”

Using System Monitor and Task Manager

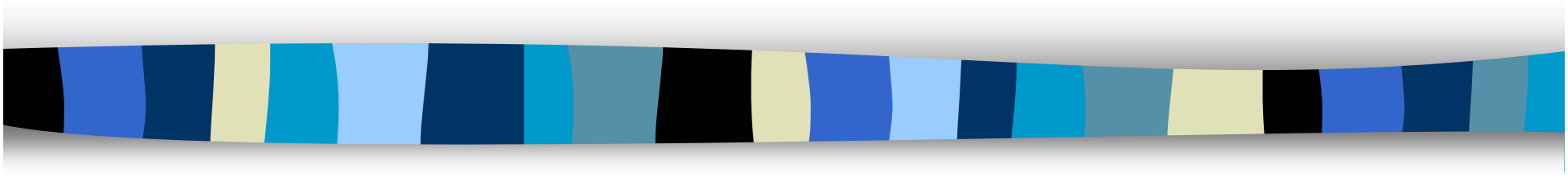
DEMONSTRATION



Spyware Shootout

- **Lavasoft Ad-Aware 6.0 Build 161 (FREE)**
- **Spy Bot Search & Destroy (FREE)**
- **Webroot Spy Sweeper 3.0 ($39.95)**
- **HiJackThis! (FREE)**

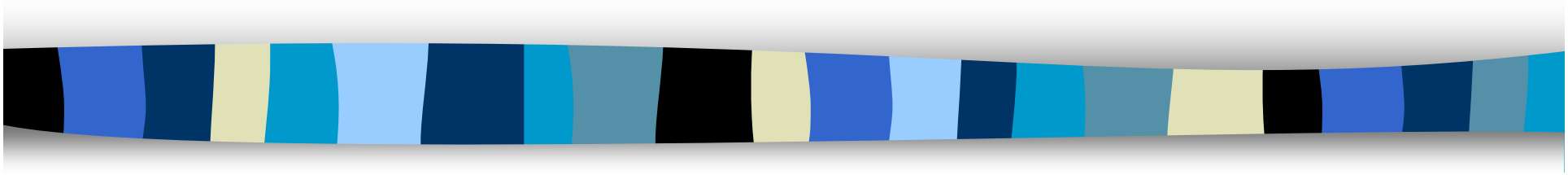
DEMONSTRATION



FREE DNS Tool

Blighty Design Sam Spade

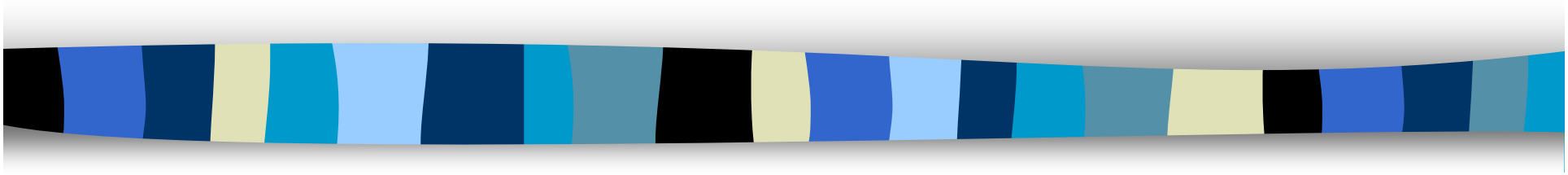
DEMONSTRATION



FREE Virus Removal Tool

Trend Micro Housecall

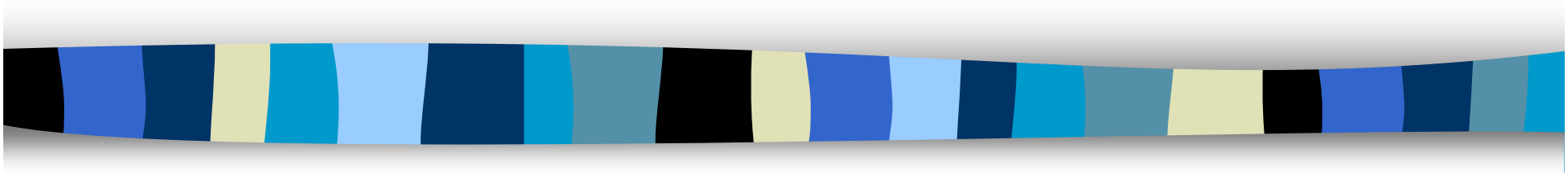
DEMONSTRATION



FREE Virus Removal Tools

McAfee AVERT Stinger

DEMONSTRATION



FREE Real-time Anti-Virus Software

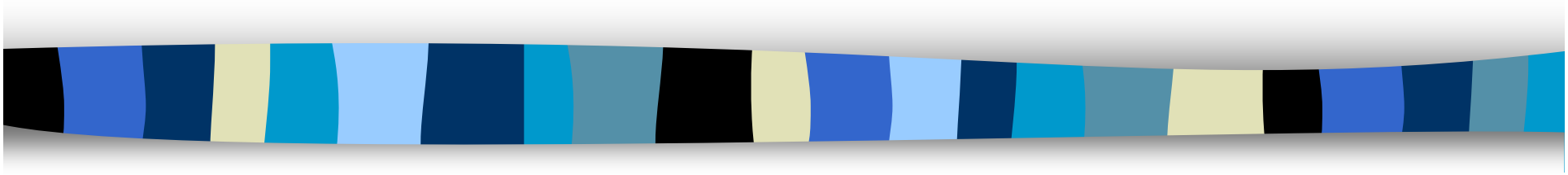
AVAST! 4 Home Edition
BitDefender Free Edition v.7
AntiVir Personal Edition

DEMONSTRATION

FREE Windows Security Checkup

Microsoft.com Security

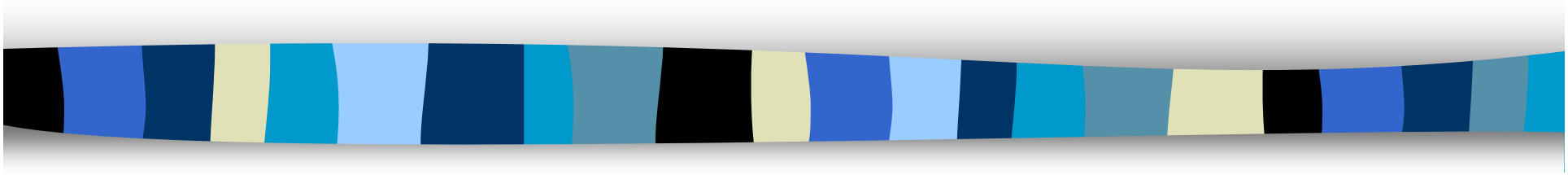
DEMONSTRATION



Sometimes It Feels Like Somebody's Watching Me…

Perfect Keystoke Logger

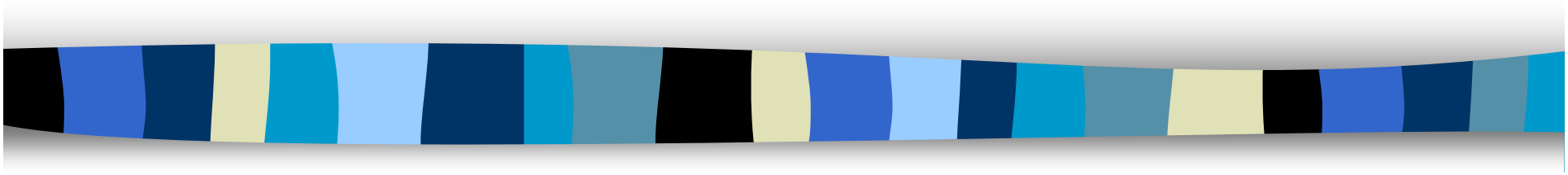
DEMONSTRATION



FREE IP Ping Sweeper

Foundstone SuperScan4

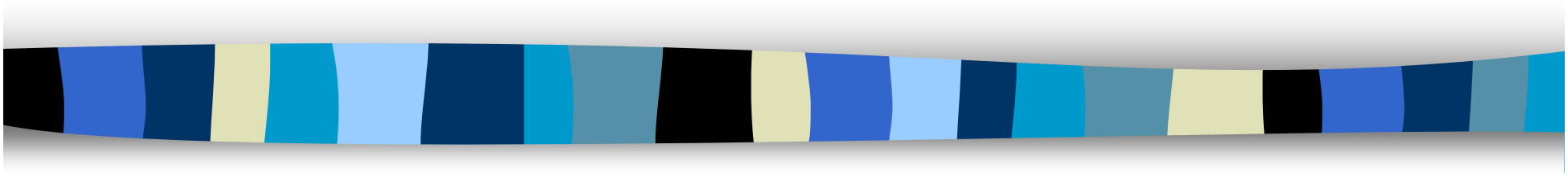
DEMONSTRATION



FREE TCP/UDP Port Listener

Foundstone Attacker

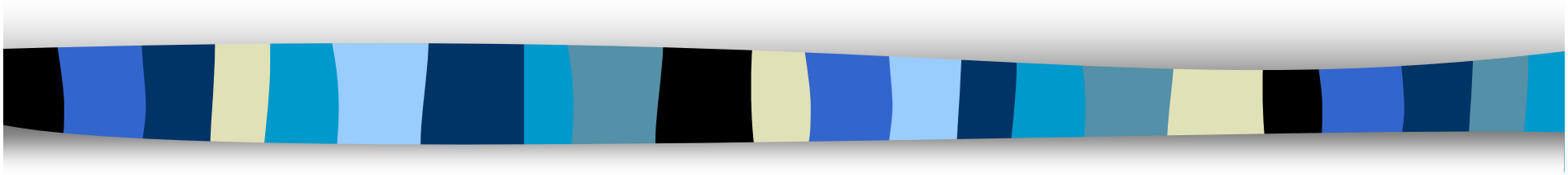
DEMONSTRATION



FREE Protocol Analyzer

Ethereal

DEMONSTRATION



Commercial System Analyzer

SISUtilities Sandra

Thank You!

Jerry Seregni
WWL-TV Channel 4
Research Director/Technology Analyst
(504) 529-6275
Jerry@wwltv.com