Session Two: Overview of Security Tools and Concepts

This session is presented on behalf of Compass.

Don Murdoch, CISSP
MCSE, MCSD

Agenda

- Discuss the general classes of security tools
  - Windows 98/2000
  - Linux Kernel 2.4 (Redhat 8)
- Discuss exploit tools
- Explain countermeasures
- Demonstrate a few specific tools
- Credits:
  - *The overall structure of this presentation is based on the SANS GSEC curricula*
  - *Some material from MSFT Security clinic*

Security Tools Overview

Trojans, Host Based Intrusion Detection, Network Based Intrusion Detection, Firewalls and Scanning Tools

Issue: Trust Relationships

- Trust describes authentication between systems
  - A “trusting” computer will allow someone in without passwords if configured
  - One way or two way, or two one way
  - “Lazy” persons’ answer to single sign on
- Unix/Linux Example(s)
  - Berkley “r” commands (rsh, rcp, rexec, rlogin)
  - /etc/hosts.equiv and $HOME/.rhosts
    - Text file example:

```
Aries – all users from this system can connect
Gemini john – john can connect w/o password
+ fred – fred can connect from anywhere
```

Trojans

- Designed to install w/o obvious trace
- Examples
  - CodeRed – designed to perform automated DoS against whitehouse.gov
- Windows Remote Control
  - NetBus
  - SubSeven
- Locating Trojans
  - Network traffic on mostly known ports
  - Odd behavior
  - Forensic analysis (clean boot)

How do they get here?

- Email attachments – allegedly from a friend
- Vulnerable network applications
- Shareware / downloads
- Sneaker Net

Host Based IDS for Unix/Linux

- TCP wrappers
  - Inserts itself between inetd and incoming connections
  - Allows / Denies connection based on rules
  - Relies on the honesty of IP addresses
- Xinetd – replaces inetd
  - Access control based on time, hostname, address, and/or domain
  - Can limit access and CPU usage to services
  - Extensive logging
  - Can bind service to an IP Address
  - Extendable to chroot environment
  - Utility to convert inetd.conf to xinetd.conf

More Host IDS for Unix/Linux

- Tripwire
- SWatch

Host based IDS for Windows

- Practically, personal firewalls
  - ZoneAlarm
  - Norton Internet Security 2003 or Personal Firewall
  - Basic firewall in Windows XP
- Server environment
  - Microsoft Operations Manager 2000
- Sysinternals tools
  - TCP monitor
  - Filesystem monitor
- Audit tools
  - Dumpel
  - CIS Security Scoring tool

Network Based IDS Tools

- Linux
  - Tcpdump with proper filters
  - Snort
    - Analysis with SnortSnarf from Silicon Defense
  - PortSentry
- Windows
  - ISS
  - Windump
  - Snort

Firewalls

- Goal: allow, deny or reject network traffic based on security policy in or out
  - Inspect source / destination address / port
  - Inspect content payload
- Personal – for the desktop user
- Network –perimeter / logical boundaries
  - Screening Router
  - Packet Filter – decisions based on individual packets not the packet content
  - Stateless – packet by packet decisions
  - Statefull – can track the progress of connection attempts

Firewall Examples

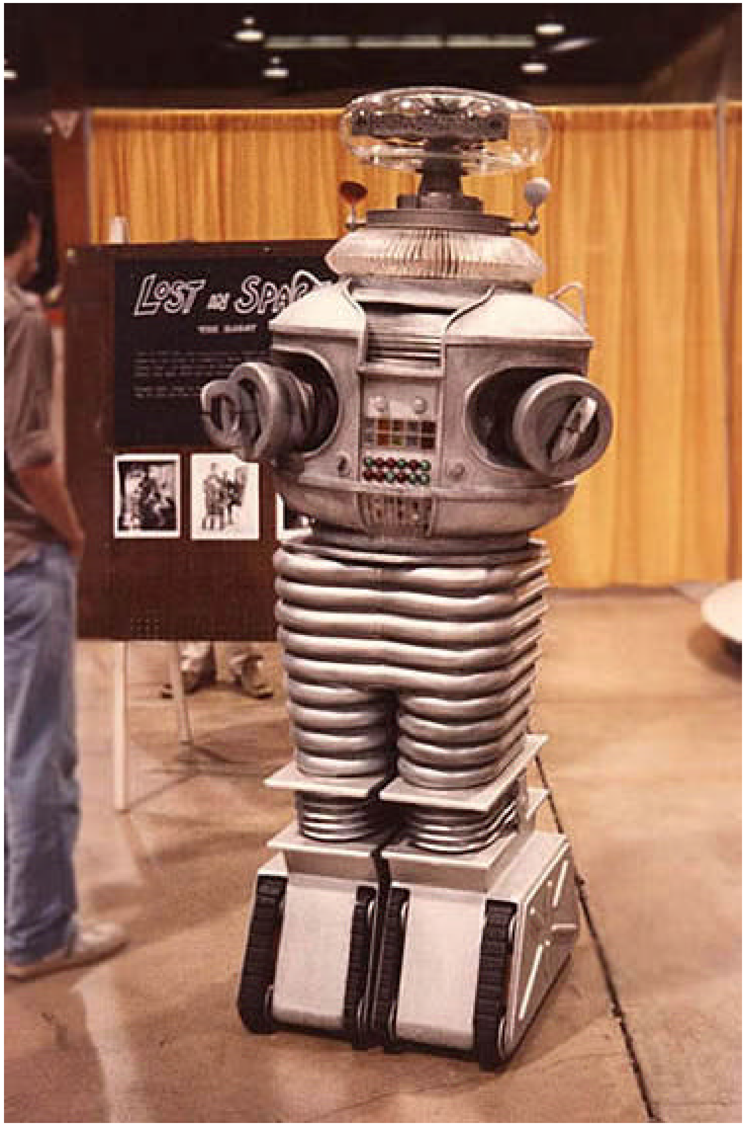
- Linux/Unix
  - Ipchains – kernel 2.2 and 2.3
    - packet filtering decides to allow | deny | reject
    - Decisions based on address, port, and protocol
  - Iptables – kernel 2.4
- Windows – personal
  - Tiny Firewall, ZoneAlarm, NIS 2003, NetDefense
- Corporate
  - ISA Server 2000
  - CheckPoint VPN1
  - Raptor
  - Gauntlet

Scanning Tools

- Purpose
  - Reconnaissance – critical for success
  - Verification – proving to ourselves system is running what it needs to run
  - Penetration testing – chinks in the armor
- Examples:
  - NMAP – network, fingerprint
  - hping2
  - SuperScan – network, ports
  - Nessus – find vulnerabilities (Danger! Danger!)
  - SMB Scanners
    - Legion, SMBscanner, ShareSniffer

Be Aware ...

- Various scanning tools and techniques will trigger sensors
- “Scanning” is illegal in the US
- Vulnerability testers can disable systems



Security Concepts

Exploits, Password Analysis, Forensic Backups, Denial of Service, Web Security and Policy Development

Exploits

- Windows Null Session
  - Logon with null username/password
  - Windows will answer with basic information
  - Members of “everyone” and “network” group
  - Limited functions; quality information released
  - Tools: Foundstone hunt, net view, DumpSec

Password Analysis

- Audit or interrogate users and passwords to insure policy conformance
- Usernames are guessable – ½ the battle
- IF passwords are guessable ... battle is lost
- Example tools
  - John the Ripper
  - L0pht Crack (lc3)

Forensic Grade System Backups

- Allows for system study
- Can snapshot a system and then put it back on the air
- Unix / Linux
    - Use dd – tar, cpio, dump, fbackup don’t cut the mustard
- Windows
    - Ghost – about the only usable tool – be careful to know ***which disk is which***!

Denial of Service

- Goals of an attacker
  - Disable your system by using exposed services
  - “look like” its normal overloading traffic
  - Prevent others from using services
  - Camouflage source by spoofing
- Example tools
  - Trin00 (or Wine00)
  - TFN2K

Web Security

- Sanitize any publicly available information
- Search for your sites, staff, topics of interests, projects often – see what's available
- Use camouflaged email address when posting / reading news
- Review content with mirroring tools
  - BlackWidow, Websleuth
- Research authentication methods

Security Policy – Internet Access Example

- Scenario
    - Alice has new responsibilities that require eCommerce (research, purchase via credit card, orders)
- Assessment
    - How will Alice "get to the Internet"? Why?
    - Who authorizes the change? Why?
    - Who instructs the network manager to allow access? Why?
- Resulting policy statement
    - "Employee access requests must be justified and approved by dept. head. IS manager provides final approval, instructs network admin to make appropriate changes to support request."

Network Security

Network Design Topics and Network Security Tools

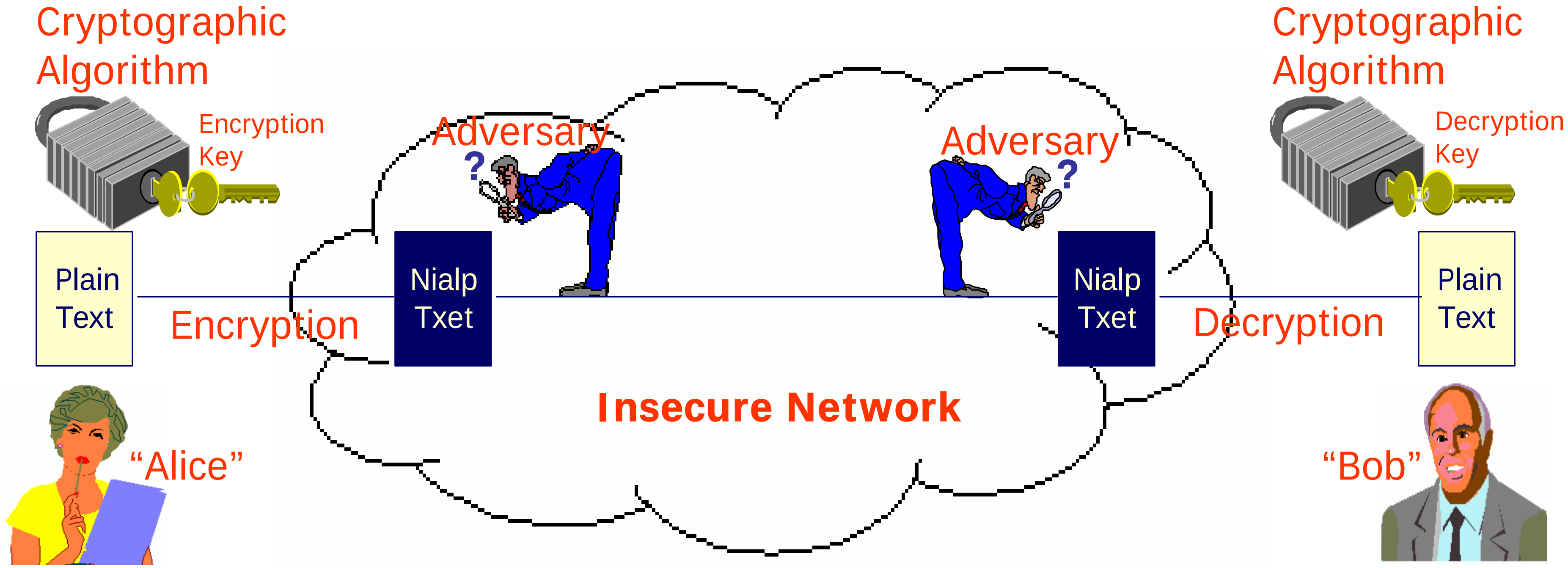
Design Topics

- Use private IP address space – RFC 1918
  - The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:
    - 10.0.0.0 - 10.255.255.255 (10/8 prefix)
    - 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
    - 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
- Scanning tools (covered previously)
- DNS
  - Be cautions about entries
  - Separate internal and external servers
- Routers
  - Access control lists at perimeter
  - Separate internal networks as needed
  - Filtering – ingress and egress

Secure Communications

Email Security
Steganography
VPN Methods
Web Server Security

The Challenge That We Face



Communications in the presence of adversaries...

Confidentiality ★ Integrity ★ Authentication ★ Non-Repudiation

Alice's Perspective…

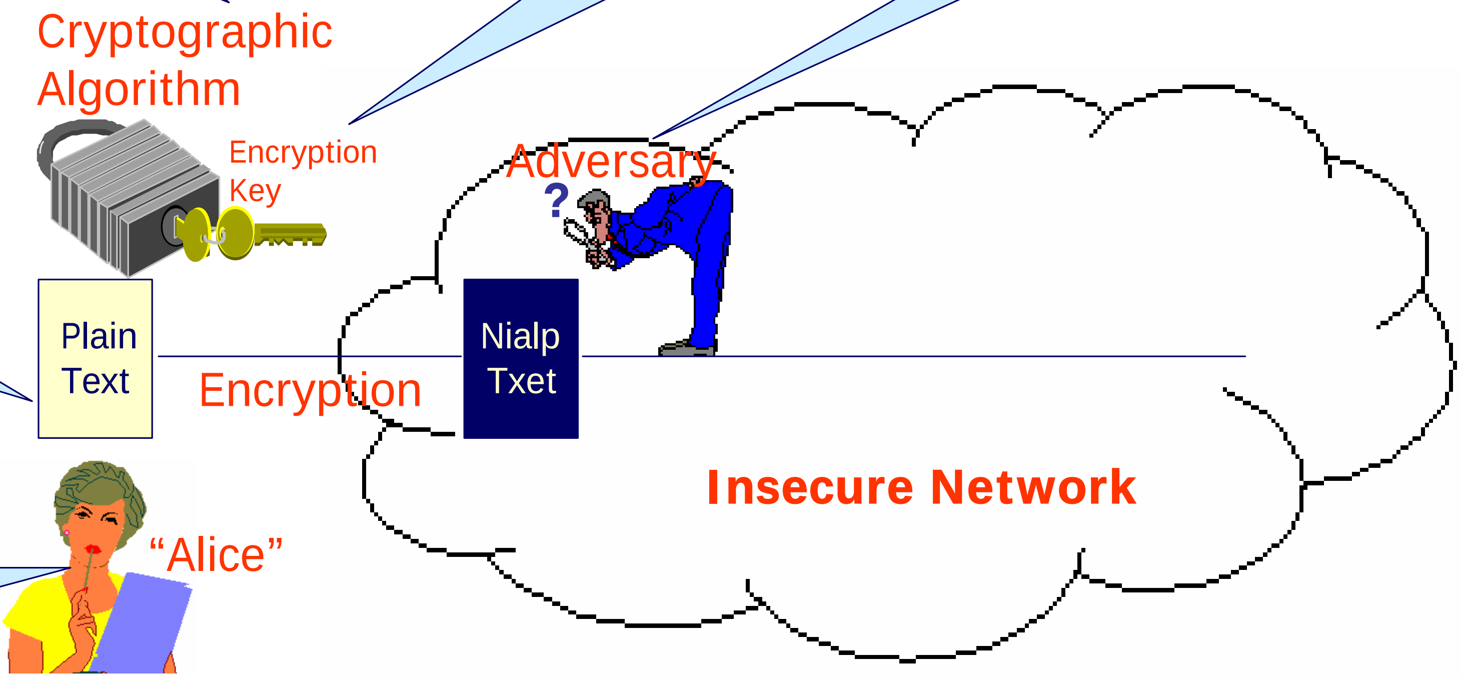
Details of Cryptographic Algorithm must be publicly known and intensely scrutinized by the global cryptographic community

Knowledge of the Key must be mandatory in order to successfully perform meaningful encryption and decryption operations

It must be impossible to determine the Plaintext by simply examining the Ciphertext

It must be possible for "Alice" to clearly indicate that she is the sender of the message, and to provide a mechanism for the recipient ("Bob") to detect any tampering.

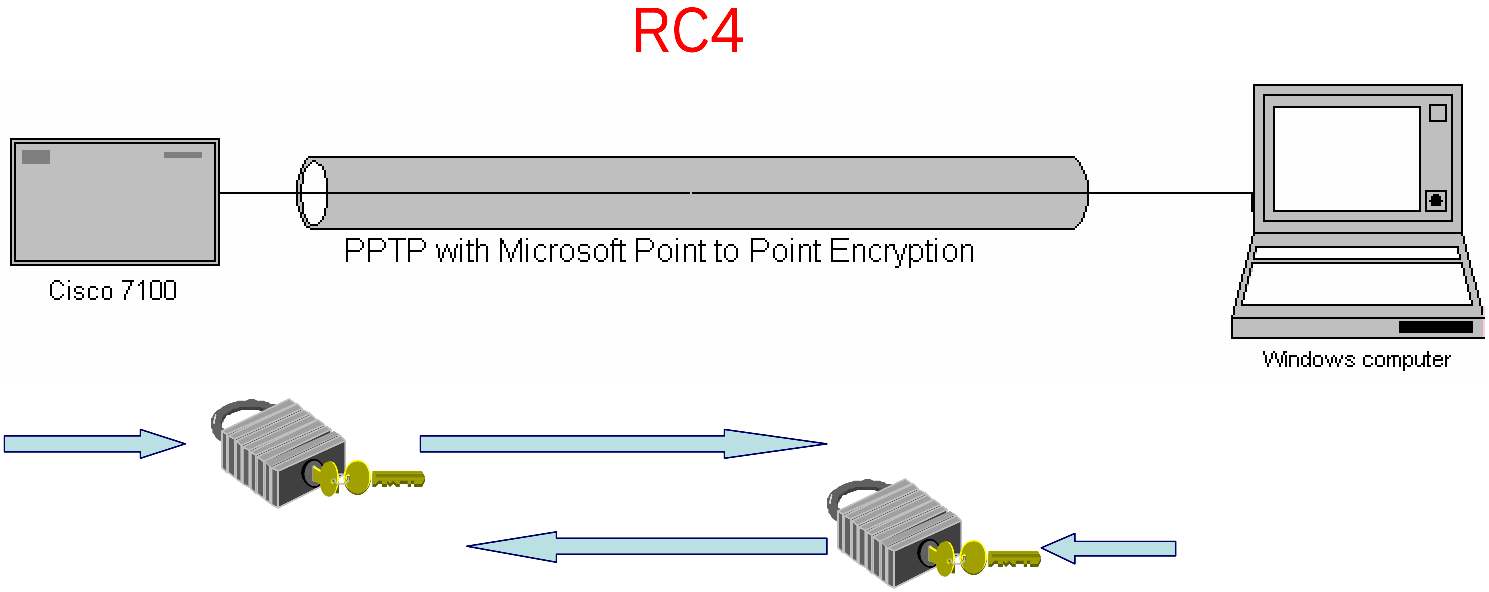
"Alice" must be trained in the proper use of the cryptosystem



When All is “Said and Done”

- Bob and Alice need a Cryptosystem
  - Provides confidentiality
  - Works on both sides
  - Has authentication
  - Maintains integrity of the data in transit
  - And … supports non-repudiation
- Cryptography …
  - Occurs in an environment where there are adversaries

PPTP VPN and IPSec



PPTP has different shared keys both ways

PGP – Pretty Good Privacy

- Public key cryptography (DH/DSS, RSA) to encrypt/sign email and files
- Developed by Philip Zimmermann (1991)
  - Confidentiality: CAST, IDEA, Triple-DES
  - Integrity: MD5
  - Authentication: knowledge of private-key
  - Non-Repudiation: digital signature
- Gnu Privacy Guard (GPG) is available as a replacement – RFC 2466 compliant
  - http://www.gnupg.org/
  - IDEA free
  - Variety of front ends

Installing and Using PGP

- What you will need
  - An email system to exchange email
  - To get PGP and get more information on PGP 6.5.x:
    - http://web.mit.edu/network/pgp.html
  - To get the latest International version of PGP 6.5.xi
    - http://www.pgpi.org/
- System requirements for PGP 6.5.x.
  - You will need.
    - A machine running Windows 95b or 98, or a Windows NT system with at least service pack 3 or higher.
    - Note! Will not work on Windows 95 or Windows 95a!
    - You will of course need TCP/IP and TCP/IP connectivity for your email to work!
    - This free version of PGP does not support certificates with PGPnet. Certificates will be covered in a latter section, but PGPnet will not.

PGP – Moving Forward

- PGP and PGPnet has more support - especially the commercial version - for certificates (X.509 type, discussed later in these lessons). Earlier versions of PGP did not.
- PGPnet is a VPN client and a server.
- PGP has freeware certificate servers for many platforms, including Windows.

SSL – Secure Sockets Layer

- Encryption at TCP/IP transport layer
- De facto standard by Netscape in 1994
- https://[host].[enterprise].com/
- SSL provides
  - Confidentiality: Triple-DES, RC4
  - Integrity: MD5, SHA-1
  - Authentication: RSA, Diffie-Hellman
  - Non-Repudiation: digital signature

PKI – Public Key Infrastructure

- Main uses
  - Secure data (hide data)
    - Email – encryption and message signature
    - VPN
    - Digitally sign data
  - Authentication
    - E-commerce
    - Logon security (Windows)
    - Web authentication
  - PKI is a controlled application of public/private key systems

Windows Security Tools

MBSA

IIS specific Tools

Local security policy and templates

MBSA – Microsoft Baseline Security Analyzer

- Can scan a machine or a network
- Checks for current service pack and hot fix level, updated from Microsoft.com
- Provides aid/assistance on how to better secure system
- Designed to check:
  - Operating system
  - Domain security if participating in 2000 AD
  - IIS 4/5
  - Office
  - MS SQL Server

Security Configuration and Analysis Tool

- Baseline analysis tool
- Applies templates to the system
- Can reset the system – cannot recover security settings
- Has been around since Wn NT SP4
- Highest degree is the Gold Standard

Registry Startup Environment

- Which programs start when the computer starts:
  - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Which services start when the computer starts
  - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
- Check which services starts the svchost
  - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Svchost
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Svchost

Other Topics

- Startup Cop – from PCMagazine
- HFnetChk
  - Searches network machines for Hot Fix level
  - Updated from Microsoft site
  - Much more powerful commercial version
- System Update Service
  - Centralized deployment of Hot Fixes
- Backup
  - System State
- IIS
  - Lockdown Tool and URL Scan
  - Socket 80 Unicode scan tool

Linux / Unix Security Tools

Sudo or Runas, Syslog and syslog-ng, Network Commands

Linux Security Topics

- Avoid ‘root’ - Use runas or sudo
  - Can limit who can run which commands
  - Logs activity for analysis
  - “ALL” will allow a shell to be executed
- Syslog – centralized reporting
  - Make sure filesystem can accommodate logs
  - Read them …
  - Understand log rotation
  - Use syslog-ng if possible
- The three times
  - atime
  - ctime
  - mtime