Network Security: An MPE/iX Overview

Jeff Bandle
HP MPE/iX Networking Architect

CONTENTS

- General Networking Security
  - Overview of security vulnerabilities
  - What can be done to make systems more secure

- MPE/iX Specific Networking Security
  - Overview of MPE/iX networking stacks
  - What security tasks exist for MPE?

INTRODUCTION

- What is security?

  - Unique to each individual user/company
  - Solution should contain three components for completeness
    - Prevention
    - Detection
    - Reaction

GENERAL NETWORKING

- What are the threats?
  - Types of attacks
  - Types of attackers
- Plans before technology.
  - Understand the “enemy” first

“A moat around a castle does no good if attacks are from the air”

GENERAL NETWORKING

- The Unchanging and Changing Nature of Attacks
  - Unchanging – similar to “bricks and mortar” crimes
    - Robbery
    - Embezzlement
    - Fraud
    - …etc…
  - Changing
    - More common
    - More widespread
    - More difficult to track, capture and convict

GENERAL NETWORKING

- Internet has three characteristics that aid attacks.
  - Automation
    - Speed of computers and networks makes minimal rate of return attacks possible.
    - Data mining is easy and getting easier, affecting privacy
  - Action at a Distance
    - Attackers can be far away from their prey and still do damage.
    - Interstate/International differences in laws can affect prosecution

GENERAL NETWORKING

- Internet has three characteristics that aid attacks. (cont)
  - Physical techniques hard to duplicate / propagate
    - Cable descramblers
    - Counterfeiting U.S. currency
  - Electronic techniques easily transferable / duplicated
    - Counterfeiting e-money
    - Attack tools can be created by single person
      - Easily modified per situation
      - Less intellectual capital needed to make tool effective.

GENERAL NETWORKING

- Types of Attacks
  - Criminal Attacks
    - Basis is in financial gain
    - Includes fraud, destruction and theft (personal, brand,identity)
  - Privacy Violations
    - Private/personal information acquired by organizations not authorized.
    - Includes surveillance, databases, traffic analysis
  - Publicity Attacks
    - Attacker wants to get their name(s) in the papers
    - Can affect ANY system, not just related to profit centers
    - Denial of service.

GENERAL NETWORKING

- Types of Attacks (cont)
  - Legal Attack
    - Setup situation to use discovery process to gather information
    - Rare, but possibly devastating

GENERAL NETWORKING

- Who are the adversaries?
  - Categorized in multiple ways:
    - By objective – Raw damage, financial gain, information
    - By access – Insider vs. external
    - By level of resources – funding level, technical expertise..etc.
    - By level of risk – Willing to die, go to jail

GENERAL NETWORKING

- Who are the adversaries? (cont)
  - Hackers
    - Attacks for the challenge
    - Own subculture with names, lingo and rules
    - Stereotypically young, male and socially on the fringe
    - Can have considerable expertise and passion for attacks
  - Lone criminals
    - Attack for financial gain
    - Cause the bulk of computer-related crimes
    - Usually target a single method for the attack

GENERAL NETWORKING

- Who are the adversaries? (cont)
  - Malicious insiders
    - Already inside the system
    - Knows weaknesses and tendencies of the organization
    - Very difficult to catch
  - Industrial Espionage
    - Gain a competitive advantage by stealing trade secrets
  - Press
    - Gather information for a story to sell papers/commercial time
  - Organized crime
    - Lots of resources to put behind their attacks…usually very lucrative

GENERAL NETWORKING

- Who are the adversaries? (cont)
  - Police
    - Lines are sometimes crossed when gathering information to pursue a case
  - Terrorists
    - Goal is disruption and damage.
    - Most have few resources and our unskilled.
  - National intelligence organizations
    - Highly funded and skilled
    - Very risk averse

GENERAL NETWORKING

- Who are the adversaries? (cont)
  - Infowarriors
    - Military based group targeting information or networking infrastructures
    - Lots of resources
    - Willing to take high risks for short term gain

GENERAL NETWORKING

- Specific types of Network attacks and solutions
  - Viruses
    - String of computer code that attaches to other programs and replicates
      - File infectors – Oldest type of virus, now mostly extinct
      - Boot-sector viruses – Reside on the boot portion of a disk. Also mostly extinct
      - Macro viruses – Written in a scripting language and affects data files, not programs. Future of viruses.
    - No absolute cure for viruses
      - Antivirus programs work, but need continual updating.
      - Virus makers depend on laziness of users to let virus defs get out of date.

GENERAL NETWORKING

- Specific types of Network attacks and solutions
  - Worms
    - Particular to networked computer systems
    - Gains access to resources that point to other computers
    - Replicates itself to multiple systems
    - Rarely dangerous, mostly annoying
  - Trojan Horses
    - Code that imbeds itself into something useful
    - Collects information and sends to known site on the network
    - Also can allow external takeover of your system (Back Orifice)

GENERAL NETWORKING

- Modern Malicious Code – “Malware”
  - Around 1999 was first occurrence of large propagation of e-mail infecting malware
  - Virus protection is now more reactive
  - E-mail infections are insidious by bypassing firewalls.
  - Multi-module programs and plugins increase vulnerability
  - Dynamic linking increase problems also
  - Mobile code (Java, JavaScript, ActiveX, Plugins) allows for easier delivery mechanism

GENERAL NETWORKING

- Methods of Attacking the Network
  - Password sniffing
    - Collect first parts of data packet and look for login attempts
  - IP Spoofing
    - Fake packet to “hijack” a session and gain access
  - DNS Overrides
    - Malicious access to a DNS server can compromise a network
  - Denial of Service Attacks – Single and Distributed
    - Large number of “SYN” packets to establish dummy connections
      - System gets throttled handling all the “hello” requests.
    - Massive number of e-mail messages will flood a system.

GENERAL NETWORKING

- Methods of Attacking the Network (cont)
  - Port scanning
    - Automated process that looks for open networking ports
    - Logs positive hits for later exploits
  - Buffer overrun packets
    - Attacker sends carefully built packet to computers on network that support specific services. (E-mail, IIS)
    - Packet causes accepting process to abort, leaving system in unknown state, potentially with root access
    - Packet contains code that executes to get root access.

GENERAL NETWORKING

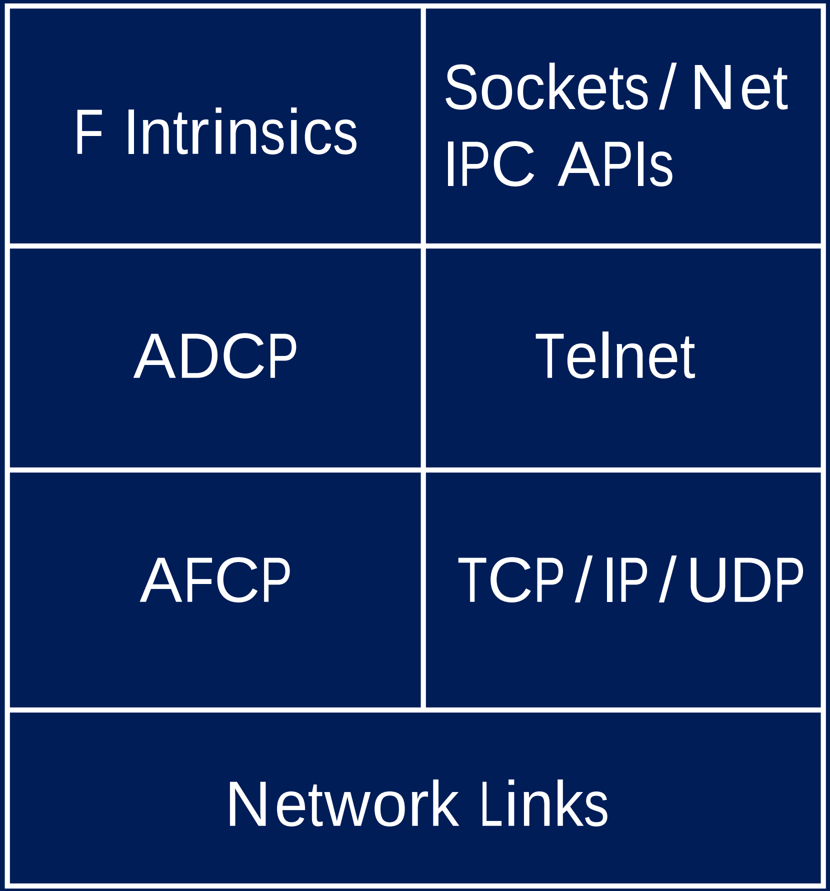
- Methods of Defending a Network
  - Firewalls
    - Networking devices (routers) that check traffic coming into a private network
    - Needs to be complete and properly configured to ensure protection
    - Good protection for general networking traffic, but specific traffic will still get through.
  - DMZs
    - Network space between two firewalls
  - VPNs
    - Provides encrypted access from outside a network.
    - Current versions aren't reliable enough and aren't useful against "slow" attacks.

GENERAL NETWORKING

- Methods of Defending a Network (cont)
  - Burglar alarms
    - Traps set on specific networked objects that go off if accessed
  - Honey pots
    - Dummy objects used to attract attacks. Range from single devices to whole sub networks.
  - Vulnerability scanners
    - Tools that scan a network periodically for holes/open gateways/misconfigured routers
    - Limited in scope because of potential damage to the network
  - Cryptography
    - Has potential, but complexity limits its use to local sites.

MPE/iX SPECIFIC NETWORKING

- MPE/iX Networking Stacks Made of Multiple Layers



F Intrinsics	Sockets/Net IPC APIs
ADCP	Telnet
AFCP	TCP/IP/UDP
Network Links	

MPE/iX SPECIFIC NETWORKING

- MPE/iX Networking Security

In securing your MPE/iX system there are a few things that need to be considered/understood before even thinking about security technology

- How is your MPE/iX system laid out on your network

- What is the important resource on your MPE/ix system you want to protect

- Who are the users that you want access to you MPE/iX system

- Where are these users coming from…internal vs. external

MPE/iX SPECIFIC NETWORKING

- MPE/iX Networking Security
- Once a good understanding of the MPE/iX systems roll has been understood, there are some basic first steps to take with strengthening security.
  - Change default passwords
  - Keep the OS up-to-date
  - Keep applications up-to-date
  - Monitor security bulletins
  - Use appropriate file and user security
  - When possible, carefully validate all input data
  - Social engineering
    - communicate the importance of protecting sensitive or proprietary data
    - no password sharing

MPE/iX SPECIFIC NETWORKING

- MPE/iX Networking Security
  - Top security advantage is MPE/iX nature
    - Common types of attacks would not work
    - Worst result would be a process abort with a loss of a networking service
  - Other options for securing network into MPE/iX

MPE/iX SPECIFIC NETWORKING

- MPE/iX security measures (cont)
  - API layer – Secure sockets
    - RSA Bsafe SSL Toolkit
    - Software suite for building SSL enabled applications
      - Includes 128 bit encryption, V.509 authentication and session caching
    - Available for download from http://jazz.external.hp.com
    - Not supported directly by HP and requires an RSA user license for support.

MPE/iX SPECIFIC NETWORKING

- MPE/iX security measures (cont)
  - Services layer - HP Webwise MPE/iX Secure Web Server
    - Secure,encrypted communications between browser and server
    - What does it include?
      - Apache 1.3.22
      - Mod_ssl 2.8.5 SSL security add-ons for Apache
      - MM 1.1.3 shared memory library
      - Openssl 0.9.6b cryptographic/SSL library
      - RSA BSAFE Crypto-C 5.2 cryptographic library (for the RC2, RC4, RC5, and RSA algorithms)

MPE/iX SPECIFIC NETWORKING

- MPE/iX security measures (cont)
  - Services layer - HP Webwise MPE/iX Secure Web Server (cont)
    - IT IS NOT…?
      - a substitute for a firewall (explicitly allow acceptable connections, etc.)
      - a substitute for good host security practices (change default passwords, keep the OS up-to-date, etc.)
      - a substitute for good application security practices (use appropriate file and user security, carefully validate all input data, etc.)
      - a substitute for good human security practices (communicate the importance of protecting sensitive or proprietary data, no password sharing, etc.)

MPE/iX SPECIFIC NETWORKING

- MPE/iX security measures (cont)
  - Services layer - HP Webwise MPE/iX Secure Web Server (cont)
    - Available from http://jazz.external.hp.com
    - Supported through HP
    - Latest version is A.03.00
      - Bundled in 7.5 in FOS
      - Available as a patch on 7.0 WBWGDT7A

MPE/iX SPECIFIC NETWORKING

- MPE/iX security measures (cont)
  - Services layer - Configurations
    - Networking services controlled by configuration files
      - SERVICES.NET.SYS – Configures the ports the MPE/iX networking subsystem will handle requests.
      - INETDCNF.NET.SYS – Configures the services INETD will handle.
      - INETDSEC.NET.SYS – Configures security domains for the INETD process

MPE/iX SPECIFIC NETWORKING

- MPE/iX security measures (cont)
  - SERVICES.NET.SYS

```
echo        7/tcp                  # Echo
echo        7/udp                  #
discard     9/tcp   sink null      # Discard
discard     9/udp   sink null      #
daytime     13/tcp                 # Daytime
daytime     13/udp                 #
chargen     19/tcp  ttytst source  # Character Generator
chargen     19/udp  ttytst source  #
ftp         21/tcp
telnet      23/tcp
time        37/tcp  timeserver     # Time
time        37/udp  timeserver     #
```

MPE/iX SPECIFIC NETWORKING

- MPE/iX security measures (cont)
  - INETDCNF.NET.SYS
    - echo stream tcp nowait MANAGER.SYS internal
    - echo dgram udp nowait MANAGER.SYS internal
    - daytime stream tcp nowait MANAGER.SYS internal
    - daytime dgram udp nowait MANAGER.SYS internal
    - time stream tcp nowait MANAGER.SYS internal
    - time dgram udp nowait MANAGER.SYS internal
    - discard stream tcp nowait MANAGER.SYS internal
    - discard dgram udp nowait MANAGER.SYS internal
    - chargen stream tcp nowait MANAGER.SYS internal
    - chargen dgram udp nowait MANAGER.SYS internal
    - telnet stream tcp nowait MANAGER.SYS internal

MPE/iX SPECIFIC NETWORKING

- MPE/iX security measures (cont)
  - INETDSEC.NET.SYS

```
telnet        allow   10.3-5 192.34.56.5 ahost anetwork

# The above entry allows the following hosts to attempt to access your system
# using telnet:
#               hosts in subnets 3 through 5 in network 10,
#               the host with Internet Address of 192.34.56.5,
#               the host by the name of "ahost",
#               all the hosts in the network "anetwork"
#
tftp     deny    192.23.4.3
```

MPE/iX SPECIFIC NETWORKING

- MPE/iX security measures (cont)
  - Other checking measures
    - NETCONTROL checks
      - Run NETCONTROL to take periodic traces of your network for potential attacks
      - Check to see if unused ports are being probed
      - NETCONTROL TRACEON=MSDB;PROT=TCP – Starts tracing
      - NETCONTROL TRACEOFF;PROT=TCP – Stops tracing
      - Use NMDUMP to format data – TCP is type 3
    - Network Packet Sniffers
      - Some MPE/iX networking tools are difficult to use
      - Independent checks maybe easier and quicker to grasp

MPE/iX SPECIFIC NETWORKING

- MPE/iX security measures (cont)
  - Other checking measures
    - Enable logging within INETD
      - Starting INETD with the –l option will force verbose logging to console
      - RUN INETD.NET.SYS;info="-l pri=cs"
      - Use this to check for strange inetd traffic
    - Check the FTP log file, FTPLOG.ARPA.SYS for unusual FTP behavior
      - These log entries include originating IP addresses
    - SHOWCONN
      - Connection display command that includes connection information of user

```
JOBNUM INTRO DATE AND TIME    LDEV   USERNAME
 REMOTE ADDRESS  RPORT  LPORT  FLAGS  PIN(PROGRAM)
#S1025  WED MAR 12 2003 08:18   34   JEFF.PTD,BANDLE
   15.61.193.201  2581  telnet jtcibd  155(JSMAIN.PUB.SYS)
```

WRAPUP

- Continue to monitor and evolve
  - Listen to CERT bulletins and evaluate those to your systems
  - Network with industry acquaintances for possibly new styles of attacks
  - Try to be proactive
  - Formalize a security strategy:
    - WHO is accessing your data?
    - WHAT is the key resource(s) you need to protect?
    - WHEN is data access expected?
    - WHERE are your users who are accessing your data?

hp®

invent