Network Security in the Patched Environment

Guy Helmer, Ph.D.

Palisade Systems, Inc.

Introduction

- Target audience: Network Managers
- Topic: Transport and Application Network-layer techniques
  - Defend vulnerabilities before, during, and after applying patches
  - Protecting against likely future security problems
  - Detecting new problems

Security Areas

- Data disclosure
  - Trade secrets
- Data modification
  - Accounting records
- Denial of service
  - Database access

Introduction

- Vulnerabilities of patched/partially patched/unpatched systems
- Worms and viruses
- Onion approach
  - Defense in depth

Palisade

Vendor patching facilities

- Range from fully-manual to fully-automated
- Deployment may be limited by
  - Testing requirements
  - Maintenance windows
  - Lack of vendor support

Patch-related Vulnerabilities

- Vendor lag time
- Prior to patch installation
- Undesired side effects of patches
- When patches failure to protect
- Reverse-engineered attacks based on patches (e.g., Sasser)

Patching Facilities

- Microsoft
  - Windows Update / Software Update Services (SUS)
  - Systems Management Server (SMS)
- Symantec ON iCommand
- Shavlik HFNetCheckPro

Palisade

Mitigating the vulnerabilities at layers 4 and 7

- System inventory & Vulnerability assessment
- Compartmentalization
- Restricting applications
- Monitoring

Palisade

Inventory & Vulnerability Assessment

- Hardware and software
- Points of ingress
  - Internet
  - Laptops
  - VPNs
  - Floppies/ZIP disks/USB keychains

Palisade

Compartmentalization by Firewalls

- Layers 3 & 4 (IP/TCP)
  - "Classic" firewall
  - Host firewall
- Layer 7 (Applications)
  - SMTP (anti-virus/spam) filter
  - HTTP (web site) filter
  - Peer-to-peer filter

Palisade

Compartmentalization by Network Firewalls

- Layers 3 & 4
  - Router access control lists
  - CheckPoint Firewall-1
  - Cisco PIX

Compartmentalization by Application Firewalls

- Layer 7
  - Email spam, virus and worm filtering
    - SpamAssassin
    - BrightMail
  - HTTP
    - Symantec Web Security

Palisade

Compartmentalization by Firewalls

- Pros
  - Flexibility
    - Change configuration to protect critical systems during major situations
    - Require authentication for network access
  - Cost
    - Available in many routers and switches
    - Can build a cheap box to implement (e.g., Linux, FreeBSD, OpenBSD packet filtering firewall)

Compartmentalization by Firewalls

- Issues
  - Flexibility
    - Overlapping network access
    - Configuration
  - Cost
    - Number of devices needed
  - Performance
    - Increased network latency
    - Decreased bandwidth
    - Additional points of failure

Compartmentalization by IDS/IPS

- Recognize/counteract attacks
  - Prioritize patches
  - Verify patch solution
    - If IDS/IPS identifies successful/unsuccessful intrusions
  - Tune firewalls/filters/IPS to close vulnerabilities until patches can be applied

Compartmentalization by IDS

- Pros
  - Detect attacks and respond
- Issues
  - False positives
  - Signature updates

Compartmentalization by VLANs

- Leverage layer 2 Ethernet and/or Layer3 IP switching capabilities
- Separate subnets via firewall, proxy server, or filtering router
  - E.g., separate VLAN for laptops, linked to internal network through a firewall

Palisade

Compartmentalization by VLANs

- Pros
  - Usually available at little extra cost
- Issues
  - Configuration complexity
  - Overlapping groups
  - Enforcement of VLAN membership
  - Bandwidth use

Compartmentalization by VPNs

- Isolate untrusted/insecure systems or networks
  - IPsec, SSL, L2TP
- Protect data in transit, plus:
- Use firewall, proxy server, or filtering router to isolate VPN termination point

Compartmentalization by VLANs/VPNs

- Issues
  - Network engineering
  - Placement of devices
  - Maintenance of configuration

Restricting Applications

- Limit allowed applications
  - Prohibit spyware, adware, peer-to-peer applications, other malware
  - Lavasoft AdAware
  - Palisade PacketHound

Restricting Applications

- Pros
  - Limit points of vulnerability
- Issues
  - Extra maintenance

Detecting

- Intrusion Detection & Prevention Systems
  - Network
    - Snort
    - Network Associates IntruShield
    - Symantec ManHunt
  - Application
    - Palisade PacketHound
  - Host-based
    - ZoneAlarm
    - McAfee Desktop Firewall
    - Symantec Intruder Alert

Detecting

- Anomaly Detection
  - Tends to require manual analysis of graphs or reports
  - Network usage trends by port and/or IP
    - Cisco NetFlow
    - MRTG, ntop
  - Application trend analysis
    - Palisade PacketHound

Detecting

- Pros
  - Stay abreast of network activity
  - Automatically isolate problems
- Cons
  - False positives
  - False negatives
  - Maintenance

Summary and Conclusion

- System inventory
- Vulnerability assessment
- Compartmentalization
- Monitoring

Palisade