Network Security

Information Security, Network Security, And Network Access Control

Agenda

- □ Security Resources
- □ Security Concepts
- □ Information Security
- □ Information Security Hot Topics
- □ Network Security
- □ Network Access Control

Security Resources

SANS "The SysAdmin Audit Network Security Institute"
http://www.sans.org/

http://www.sans.org/reading_room
"802.11 Denial of Service Attacks and Mitigation"
"Detecting and Preventing Rogue Devices on the Network"

Top 20 Vulnerabilities on the Internet
http://www.sans.org/top20

"NewsBites" and "@Risk" Newsletters
http://www.sans.org/newsletters

Security Resources

SecurityFocus
http://www.securityfocus.com/

Mailing Lists
BugTraq, Wireless Security, Etc.
mailto:bugtraq-digest-subscribe@securityfocus.com

CERT
http://cert.org/

Computer Emergency Readiness Teams
See Also: http://www.us-cert.gov/
http://www.us-cert.gov/cas/techalerts/
http://www.us-cert.gov/cas/bulletins/

Security Resources

Insecure.Org
http://insecure.org/

The Home of NMAP
http://nmap.org/

Security Tools
http://sectools.org/

Security Concepts

- Secure By Design
  - Not Security as an Afterthought. It is very Difficult To Go back Later and Add a Security Layer -- look at the Internet Protocols for example.
- Defense In Depth
  - Create Multiple Layers of Defense. Not the “tootsie pop” hard shell, soft inside. Layers include Host Security, Data Security, Firewalls, Anti-Virus, etc.

Security Concepts

- ☐ **Least Privilege**
  - Allow the minimum level of access needed to perform a task. This applies in account management, as well as the generation of access control policy.
- ☐ **End-to-End Security**
  - The higher up in the Layers you are, the better. If you can secure the application, then problems at the lower layers are less important. Example: PGP Encrypted Mail.

Security Concepts

- □ What are You Trying To Protect?
  - Evaluate Risk. What exactly is the reason you are wanting to perform a particular security task?
  - In many cases, It’s the Data!
  - Risk Analysis and Periodic Audits of the Network are tasks that are too often ignored.
- □ Security Involves TradeOffs
  - Security usually requires compromises which involve cost, complexity, and convenience. Security is hard work. And there are limits to how much security can reasonably be performed.

Security Concepts

- There is No Silver Bullet
  - A Silver Bullet is a simple, single solution that can be used to Kill a Werewolf. There is no such solution in security.
- There is No Such Thing as Perfect Security
  - See the book: "Secrets and Lies" by Bruce Schneirer, Bruce discusses his realizations about the folly of trying to achieve perfect security solutions.
  - Even so, this does not mean you should not keep trying to achieve <u>BETTER</u> security.
  - You will get Hacked. You will have to Respond. Plan Ahead for these events.

Security Concepts

- Raising The Bar
  - This is a sport metaphor. If you raise the bar in the highjump, some people will not get over the bar. Doing even minimal security will prevent some breakins.
- Keep It Simple (Stupid)
  - The “KISS” principle. Complexity is the enemy of security. If your system is too complicated, it may be difficult to secure or to manage.
- Pulling the Plug
  - Some information is sensitive and should be kept away from the Internet. In such cases, Isolated LANS, may be correct.

Information Security

Information Security

- ☐ **Definition**
  - An organized program designed to protect critical information assets from exposure, modification, or disruption.
- ☐ **ISO Standard**
  - International Organization for Standardization and International Electrotechnical Commission
  - ISO17799 (27002) Information Technology, Security Techniques, Code of Practice for Information Management
  - Define Requirements, Assess Risk, Implement Controls

Information Security

- ISO 17799 Summary
  - Risk Assessment
  - Security policy
  - Organization of information security
  - Asset management
  - Human resources security
  - Physical and environmental security

Information Security

- ISO 17799 Summary (continued)
  - Access control
  - Information systems acquisition, development and maintenance
  - Information security incident management
  - Business continuity management
  - Compliance

Information Security

- Common Names For These Areas
  - Risk Analysis
  - Vulnerability Assessment
  - Host Security
  - Network Security
  - Intrusion Detection
  - Incident Handling
  - Education and Training
  - Policy Development
  - Enforcement

Information Security

Job Positions

- Chief Security Officer (Policy Development)
- Acceptable Use Policy Officer (Policy Enforcement)
- Accounts Manager (Identity Management)
- Network Engineer (Firewalls, VPNs, IDS, NAC)
- Incident Response Team (Forensics)
- Training Specialist (Education and Training)
- Systems Manager (OS Support, Anti-virus Software)
- Auditor

Information Security

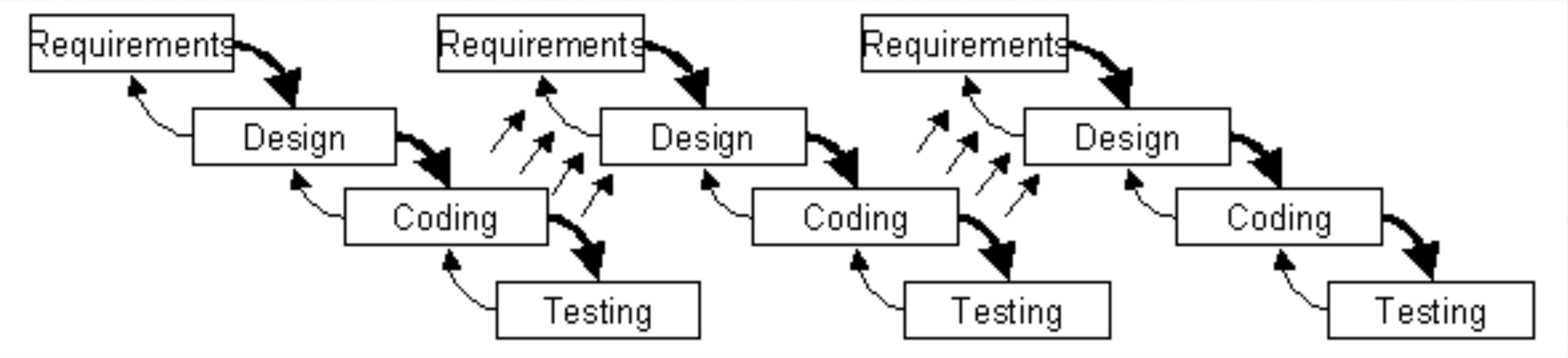
- □ **Constraints On Security Programs**
  - Personnel
  - Amount of Time/Money
  - The Size of the Task
  - See Also: The 9-Layer Model

Information Security

Political
Financial
Application
Presentation
Session
Transport
Network
DataLink
Physical

Information Security

- The Security Lifecycle
  - Like a Software Programming Lifecycle
  - An “Iterative Waterfall” Process Model
  - Are we Secure Yet?



Information Security

- Hot Topics
  - Policy Development
  - Data Security
  - Application Security
  - Identity Theft
  - Network Access Control

Network Security

- □ **Sean's Definition:**
  - "A collection of network-connected devices, technologies, and best practices that work in complementary ways to provide security to information assets."
- □ **Another Way To Say It:**
  - Network Security is a branch of Information Security which deals with systems that operate primarily at the network level. This includes the managment of network devices such as Firewalls, VPNs, Proxies, NAC solutions, IDS/IPS, as well as the management and protection of the network infrastructure."

Network Security

- Network Security Is Hard
  - It is difficult to guard at this level. The Application Level is where most of the controls are.
  - The Most Popular Protocols Were Not Designed With Security In Mind
  - Which packets are the "BAD" packets? A bad connection looks just like a good one.
  - In many cases, Network Security will Not Be Effective
  - But remember: Defense In Depth and Raising the Bar.

Network Security: Firewalls

- One of Many Tasks Expected to be Performed by a “Network Security Engineer”
- Lots of Different Types of Equipment -- Router ACLS, Cisco, Juniper, Linux, etc.
- Lots of Different Deployment Models -- Briding, Routing, IPSEC VPNs

Network Security: Firewalls

- Preparing for A Firewall is a Multi-Dimensional Task
  - Deployment Requires Risk Assessment
  - Policy Development Occurs Before Deployment
  - Network Design Is Part of the Process
  - Financial/Political Issues Are Always There

Network Security: Firewalls

- □ **Actual Deployment Is Complicated As Well**
  - Arrange for Console Access
  - Setup Change Control Management on Configuration
  - Manage Firewall Logs
  - Document the Network
  - Document the Policy
  - Establish Remote Access Policies
  - Establish a Process for Policy Changes
  - Maintain Software Support
  - Schedule Software Updates

NAC - Network Access Control

NAC - Network Access Control

- NAC is a combined set of Network Security Technologies designed to control who has access to a Network.
- NAC brings together a range of Network Security Systems including Identity Management, Firewalls, IDS, Anti-Virus Software...
- NAC is a relatively new idea.
- (All of the Pieces might not Fit Together.)

NAC - Network Access Control

- **NAC, Standard Questions**
  - How do you know who someone is?
  - Can Anyone Just Plug Into an Open Jack?
  - Can Anyone Associate to the Wireless Network And Get Service?
  - Once someone is on the Network, Can they be Removed?
  - What is the mechanism used to control access?
  - Do I want to block everyone by default?
  - How well is this thing going to work?

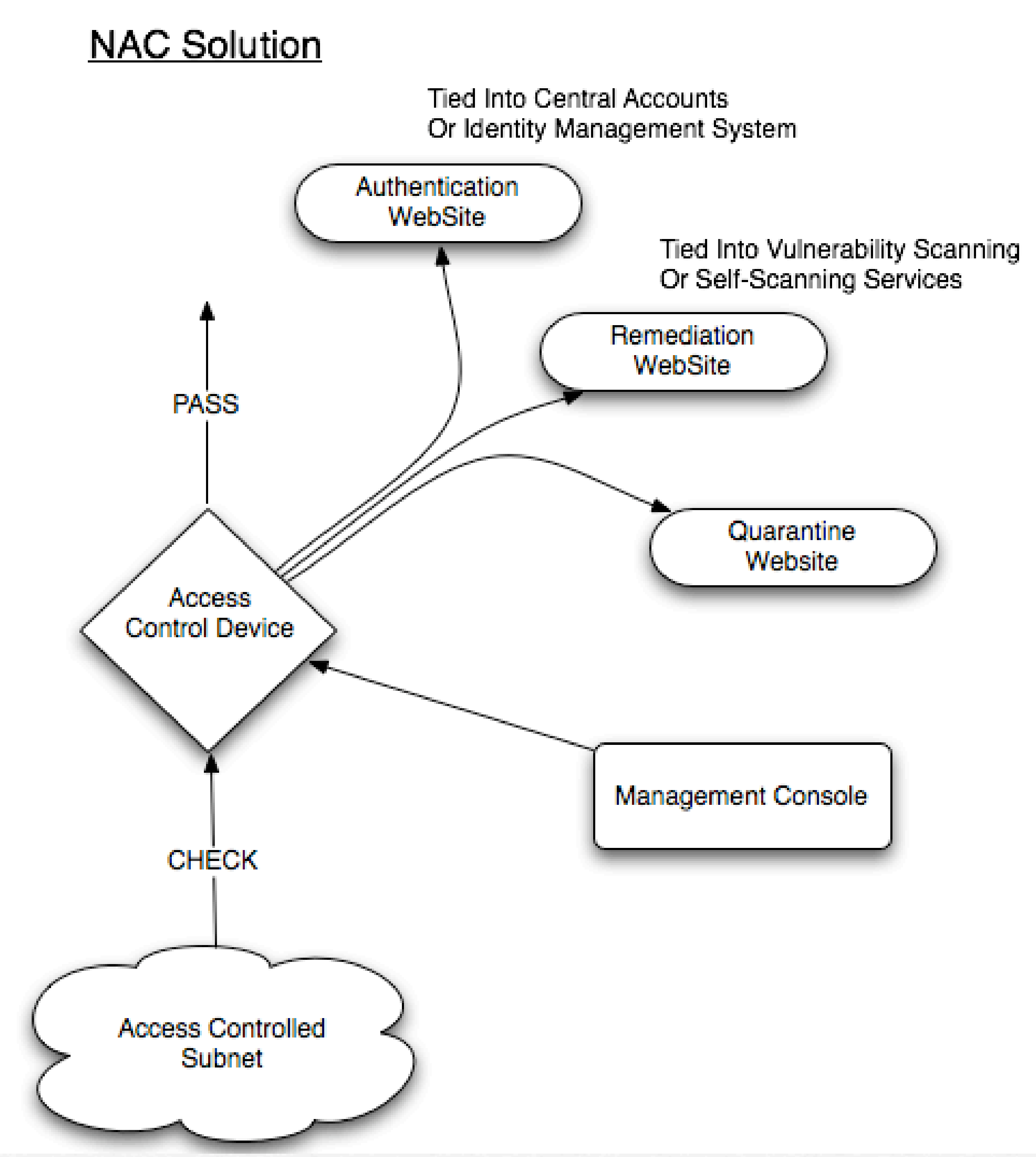
NAC - Network Access Control

- Authentication
- Quarantine
- Client Assessment
- Remediation
- Access Control Mechanism
- Intrusion Detection
- Vulnerability Assessment

NAC - Network Access Control

- **The Access Control Mechanism**
  - This is the Key Character of Any NAC Solution
  - Popular Access Controls are: IP Address, MAC Address, IP +MAC Address, VLAN Assignment, DHCP Control, and even ARP Poisoning

NAC - Network Access Control



NAC - Network Access Control

- Commercial Solutions
  - Enterasys NAC, http://www.enterasys.com/
  - (High-speed IP+MAC Switch Access Control)
  - Bradford Campus Manager
  - http://www.bradfordnetworks.com/
  - (Per-port VLAN Assignement Access Control)
  - Cisco NAC, Clean Access
  - http://www.cisco.com/
  - (Based On Perfigo, IP+MAC ACL's)
  - Juniper and Cisco VPNS

NAC - Open Source Solutions

- Open Source Captive Portals
  - M0n0Wall, NoCat, CoovaChilli, PacketFence, OpenVPN
- Open Source Vulnerability Scanners
  - SARA http://www-arc.com/sara/
  - NESSUS http://nessus.org/
  - nikto http://www.cirt.net/
- Open Source Intrusion Detection
  - SNORT http://www.snort.org/
  - BRO http://www.bro-ids.org/

NAC - Network Access Control

- □ **Criteria For Judging Solutions**
  - The Access Control Mechanism
  - Assessment/Remediation/Quarantine Feature Set
  - GUI or API Management Interfaces
  - Integration with Commercial IDS & Vulnerability Scanners
  - Level of Difficulty to Operate
  - Reliability
  - Cost

NAC - Network Access Control

- NAC, An Open Question
  - NAC Systems Are Potentially Large, Complex, Costly, and Tend To Be Tied to Single Vendors
  - With The Above In Mind, Many People Are Finding It Difficult To Buy Into The Idea of A Single-Vendor Solution

NAC - Network Access Control

- **NAC, The Good News**
  - Authentication Gateway Gets You Most of the Way There
  - If You Do Vulnerability Scanning, You are Even Further
  - Doing A Good Job In Those Two Areas, Makes The Rest Of the Arguments for a Commercial NAC System Less Compelling