Network Access Control

Security Professionals Conference
2006 Seminar 02P

Kevin Amorin
Harvard University

Chris Misra
University of Massachusetts, Amherst
Commercial Products

- 3com
- Bradford
- Cisco
- Checkpoint
- ConSentry
- EndForce
- Extreme
- Enterasys
- FourScout
- Full Armor
- HP ProCurve
- Impluse Point
- InfoBlox
- InfoExpress
- Ipass
- Juniper
- Latis Networks
- Lanscope
- LANDesk Lockdown Networks
- Nevis
- Nortel
- Mazu Networks
- Permeo
- Q1 Labs
- Reflex Security
- Roving Planet
- Seclarity
- SenForce
- Symantec
- Vernier
- Wave
Overview

♦ Policy Enforcement
  – Isolation Methods

♦ Open Source
  – Options
  – PacketFence

♦ Architectures
  – NAC
  – NAP
  – TNC
Policy Enforcement

- Isolation
- Notification
- Remediation
- Detection
- Registration
  - Identity
  - Integrity
Isolation Methods

- VLAN
  - Virtual Local Area Network
- 802.1x
  - IETF Standard
- ARP
  - Address Resolution Protocol
- DHCP
  - Dynamic Host Configuration Protocol
- Policy Routing
VLAN Scenario

- Network VLANs are “registered”, and “unregistered”
- Port becomes Active
  - SNMP Trap is sent
  - or host is detected during polling
  - or Default VLAN is used
- MAC Address is checked in DB and assigned to correct VLAN via:
  - SNMP write
  - or CLI expect script
VLAN
## VLAN

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ Isolated hosts are segmented from registered hosts</td>
<td>♦ Doesn’t work with</td>
</tr>
<tr>
<td>♦ Harder to bypass</td>
<td>– Hubs</td>
</tr>
<tr>
<td></td>
<td>– Older switches</td>
</tr>
<tr>
<td></td>
<td>– Shared ports</td>
</tr>
<tr>
<td></td>
<td>– APs</td>
</tr>
<tr>
<td></td>
<td>♦ Slow</td>
</tr>
<tr>
<td></td>
<td>♦ CLI expect scripts?</td>
</tr>
</tbody>
</table>
802.1x Scenario

♦ On link up network device (switch/ap) negotiates EAP session
♦ Client supplicant prompts for username password
♦ Network devices passes info to Radius
♦ RADIUS server returns accept/deny
**802.1x**

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
</table>
| ♦ Encrypted communication  
♦ Windows/Mac OS X built in support  
♦ Realms - pass secure tunnel to home institution  
♦ Almost every AP and most smart switches have support | ♦ No pre auth scan  
♦ Switch, AP, RADIUS server, and client must support EAP type (PEAP, TTLS, ..) and encryption type (WEP, WPA, WPA2, ..)  
♦ Most difficult to implement  
♦ No fail open support in the standard  
♦ Windows supplicant limited |
ARP Scenario

- System comes online and broadcast for DHCP or gateway
- ARP is seen by all
- Server checks DB for this MAC
- Gateway Router responds with his MAC address
- Server responds with his MAC Address and over writes the Gateway MAC
- After Registration, the gateway address is updated
ARP Manipulation
## ARP

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ Layer 3 independent</td>
<td>♦ ARP was not designed for this</td>
</tr>
<tr>
<td>♦ Static IPs don't circumvent</td>
<td>♦ Server needs to be same physical segment</td>
</tr>
<tr>
<td>♦ Immediate isolation, no timeout required</td>
<td>♦ Harder to debug</td>
</tr>
<tr>
<td>♦ Faster then other methods</td>
<td>♦ Static ARP entries possible</td>
</tr>
<tr>
<td>♦ No Network infrastructure changes</td>
<td></td>
</tr>
</tbody>
</table>
DHCP Scenario

- DHCP broadcast request
- Assigned “unregistered” IP
- Registration
- Scope change & often DHCP restart
- After lease timeout or reboot, the host will get a “registered” IP
DHCP

Router

Switch

DHCP & DNS Server

DHCP & DNS Requests

Internet

User

Host

Router

DHCP & DNS Server

Internet

User

Host
## DHCP

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ Easiest method to implement</td>
<td>♦ Static IPs</td>
</tr>
<tr>
<td>♦ Vendor agnostic</td>
<td>♦ Easy to bypass</td>
</tr>
<tr>
<td>♦ DHCP is a mature technology</td>
<td>♦ Slow, need to wait 50-100% of lease time for</td>
</tr>
<tr>
<td></td>
<td>the client to request new address</td>
</tr>
<tr>
<td></td>
<td>♦ Less control of violations</td>
</tr>
</tbody>
</table>

DHCP is a mature technology.
Policy Routing Scenario

♦ Host comes online and is redirected to registration host via default policy route
♦ After registration the policy is updated via CLI command
♦ Host is now allowed to pass through the router
Policy Routing

- Enforcement Point
- Router
- Switch
- Web Redirect
- Internet
- Host
- User
- Router
- Switch
- Host
- User
### Policy Routing

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
</table>
| ♦ Existing Network gear  
♦ No network architecture reconfiguration | ♦ Upstream router dynamic changes could cause problems  
♦ Expect scripts may be required  
♦ May need to replace entire policy with every change |
Open Source options

♦ PacketFence (DHCP & ARP)
  – http://www.packetfence.org

♦ CMU NetReg (DHCP)
  – http://www.net.cmu.edu/netreg

♦ Southwestern NetReg (DHCP)
  – http://www.netreg.org

♦ NetPass (VLAN)

♦ Open Source List - NetAuth Wiki
What is PacketFence

♦ Open-source network registration and worm mitigation solution
  – Co-developed by Kevin Amorin and David LaPorte
    • GUI developed by Randy Heins
  – Captive portal
    • Intercepts HTTP sessions and forces client to view content
  – Based on un-modified open-source components
Features

♦ Network registration
  – Register systems to an authenticated user
    • LDAP, RADIUS, POP, IMAP...anything Apache supports
    • Can support multiple authentication methods
  – Force AUP acceptance
  – Stores assorted system information
    • DHCP computer name & Web browser user-agent string
    • Presence of some NAT device
    • Switch/VLAN/Port information via DHCP option 82
    • DHCP Fingerprint
  – Stores no personal information
    • ID->MAC mapping only
Features

♦ Worm mitigation
  – Behavioral and signature-based detection
  – Optional isolation of infected nodes
  – Self-remediation
    • Empower users
    • Provides remediation instruction specific to infection
  – Redirection to the captive portal
    • via Proxy
    • via Firewall pass-through
  – Helpdesk support number if all else fails
Features

♦ Multiple Isolation Methods
  – DHCP
  – ARP
  – VLAN (in development)
♦ Queue-based Violation/Registration
♦ Remote PF Client via SOAP
♦ Vulnerability scans
  • at registration
  • scheduled/ad hoc
PacketFence Differences

♦ Static IP Detection
♦ DHCP option 82 sniffing
♦ Multi-Authentication Methods
♦ OS detection
♦ Detection of many NAT systems
♦ Banning of undesirable OSes (win 95/98, ME)
♦ NAT/AP Banning
PacketFence Differences

- Violation Actions
  - Email, log, trap, win popup, external
- Scheduled Scanning with Nessus
- Well designed Web Admin UI
- integration with MRTG for trending
- Auto Registration of consoles, IP Phones
Implementations

♦ UK, New Zealand, Canada, Mexico, US
♦ Several dozen academic environments in production
♦ Several Commercial installations
♦ Canadian Support company
♦ ~10k hosts at a large well known University
In Closing

♦ PacketFence
  – Open-source
  – Passive deployment
    • “plug and play”
    • no infrastructure changes needed
  – Proactive and reactive remediation
  – Extremely configurable
It's QUESTION TIME!!
Architecture Solutions

♦ Cisco Network Admission Control (NAC)
  – Phase 1: Routers – Aug 2004
  – Phase 2: Switches - Nov 2005
♦ Microsoft Network Access Protection (NAP)
  – Windows Longhorn – Q1 2007
♦ Trusted Computing Group
  – Trusted Network Connect (TNC)
  – Architecture & Basic API - May 2005
  – Complete Spec – May 2006?
## Cisco NAC AntiVirus Participants

<table>
<thead>
<tr>
<th>Shipping</th>
<th>Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>F-Secure</td>
<td>Sophos</td>
</tr>
<tr>
<td>McAfee</td>
<td>Kingsoft</td>
</tr>
<tr>
<td>Symantec</td>
<td>Norman</td>
</tr>
<tr>
<td>CA</td>
<td>Panda</td>
</tr>
<tr>
<td>Trend Micro</td>
<td>Rising</td>
</tr>
</tbody>
</table>

- 63 manufacturers (2/06)
- 22 shipping – 41 in development
- No other big network companies?

www.cisco.com/web/partners/pr46/nac/partners.html
Cisco NAC Support

- Identity and Integrity
- IOS 12.3(8)T
- Cisco Routers (83x, 18xx, 28xx, 38xx, 1701, 1711, 1712, 1721, 1751, 1751-V, 1760, 2600XM, 2691, 3640, 3660-ENT, 72xx)
- Cisco Switches (6500, 4500, 4000, 3750, 3560, 3550, 2970, 2955, 2950, and 2940)
- All APs, VPN 30xx
- Clean Access/Perfigo is not part of the NAC Framework - “NAC Appliance”
Cisco NAC Cost

- Cisco Network Gear
  - 4500, 4000, 3xxx, 2xxx, $$$
- Cisco Secure Access Control Server (ACS)
  - AAA Radius Server + Policy Control
- Cisco Trust Agent (CTA) 2.0
  - Windows 4.0, 2000/3, XP, RHEL 3-4
  - Includes Meetinghouse 802.1x supplicant
  - Free? ... Ahhhh wired only...
  - EAP-Fast only
### MS NAP AntiVirus Participants

#### Development

<table>
<thead>
<tr>
<th>F-Secure</th>
<th>Trend Micro</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee</td>
<td>Sophos</td>
</tr>
<tr>
<td>Symantec</td>
<td>Panda</td>
</tr>
<tr>
<td>CA</td>
<td></td>
</tr>
</tbody>
</table>

- 53 manufacturers (2/06)
  - 0 shipping – 53 in development
  - Lots of Cisco competitors Enterasys, Extreme, Foundry, ProCurve (HP), Juniper

Microsoft NAP Support

♦ Identity and Integrity
♦ NAP Clients
  – Windows Vista client late 2006
  – Windows XP SP2 + “update” 2007
♦ NAP Server
  – Windows Longhorn Q2 2007
  – Total rewrite of Network Access Quarantine Control in Windows 2003
♦ DHCP, VPN, 802.1x (PEAP), IPsec
♦ IPSec is the “strongest” form of NAP
  – Can only talk to healthy clients with “Health Cert”
Microsoft NAP Co$t

♦ Windows Longhorn Server
  – IAS AAA Radius Server + Policy Control
  – Routing and Remote Access (VPN)

♦ Upgrade Windows client cost
  – Minimum windows client is XP+patch (2007)
  – Windows Vista "better"

♦ May require AD

♦ Minimal change to network gear
TNC AntiVirus Participants

<table>
<thead>
<tr>
<th>Development</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee</td>
<td>Symantec</td>
</tr>
<tr>
<td>Trend Micro</td>
<td></td>
</tr>
</tbody>
</table>

- More then 60 manufacturers “involved”
  - switch and network equipment manufacturers, security vendors, managed service providers, chip manufacturers
  - Lots of software companies

www.trustedcomputinggroup.org/groups/network
TNC Support

♦ Identity and Integrity
♦ Use of existing network standards 802.1x IPSec
♦ Composed of mostly of Software/Appliance companies
♦ Missing some big name support from Anti-virus, Network companies
♦ Future Trusted Platform module (TPM) integration
TNC Co$t

♦ TNC Client
  – Funk, Meetinghouse, InfoExpress, iPass, etc...

♦ TNC Server (Radius/Policy Server)
  – Funk, Meetinghouse, InfoExpress, iPass, etc...

♦ No Vendor lock in?
  – No validation of interoperability
  – The TNC Client and Server “should” work together if you don’t use the same vendor

♦ Supported Network gear
  – Juniper, Extreme, Foundry, Enteresys
### Cisco NAC Pros/Cons

<table>
<thead>
<tr>
<th>Pros:</th>
<th>Cons:</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ Best fit for Cisco shops</td>
<td>♦ No support for older models (5000, 5500..)</td>
</tr>
<tr>
<td>♦ IOS upgrades for newer switches</td>
<td>♦ Currently Cisco network gear only</td>
</tr>
<tr>
<td>♦ First to market, fastest to respond, and BIGGEST</td>
<td>♦ Must use Cisco agent (CTA) and Radius Server (ACS)</td>
</tr>
<tr>
<td>♦ Full interoperability testing</td>
<td></td>
</tr>
<tr>
<td>♦ CTA is free</td>
<td></td>
</tr>
</tbody>
</table>
# MS NAP Pros/Cons

<table>
<thead>
<tr>
<th>Pros:</th>
<th>Cons:</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ Best fit for Windows environments</td>
<td>♦ All Windows</td>
</tr>
<tr>
<td>♦ Easiest and cheapest architecture</td>
<td>♦ At least 2007 before you can get your hands on it</td>
</tr>
<tr>
<td>♦ Huge Microsoft install base</td>
<td>♦ AD environment may be required</td>
</tr>
<tr>
<td>♦ FREE! with Longhorn</td>
<td></td>
</tr>
</tbody>
</table>
## TNC Pros/Cons

<table>
<thead>
<tr>
<th>Pros:</th>
<th>Cons:</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ Best fit for mixed network/desktop environments</td>
<td>♦ Focus on Client/Server software not on the network</td>
</tr>
<tr>
<td>♦ Open source plugins possible (open API)</td>
<td>♦ No compliance program, no integration testing</td>
</tr>
<tr>
<td>♦ No requirements on network architecture</td>
<td>♦ Architecture is not fully defined</td>
</tr>
<tr>
<td>♦ Most flexible of all other options</td>
<td></td>
</tr>
</tbody>
</table>
Market Survey

♦ 1/17/06 Infonetics “Enforcing Network Access Control”

– Over 1,101% increase over the next three years from $323 million to 3.9 billion 2008
– NAC Appliance market will increase 3,062% and network devices will increase 1,000% from 2005 to 2008
– “will be a volatile space over the next three years, with significant consolidation in the market”
– “Cisco's NAC solution is the most recognized brand of the three main NAC solutions, followed by Microsoft's NAP, and then the Trusted Computing Group's Trusted Network Connect solution in distant third “

♦ Maybe, Maybe not…but it will be a fun ride…
In Closing

♦ Slow……. Very Very Slow….
♦ With 70% of networking market Cisco & NAC will be around to stay
♦ Microsoft NAP will be HUGE in 2008
♦ Don’t count out TNC
♦ IETF Anyone?
♦ I2 NetAuth Working group
  – Security.internet2.edu/netauth
  – strategies, architecture, components, case studies, FAQ
It's QUESTION TIME!!