NETWORK ACCESS PROTECTION

Windows Vista Security
End-of-Class Problem: Executive Presentation

Mitigation for Common Threats in
Higher Education Network Environment using Microsoft NAP
AGENDA

- Business issues
- Security Assessment
- Engineering Assessment
- Operations Assessment
- Conclusion
EXECUTIVE TEAM

- Team members
  - Barry Randall – U. Iowa
  - Tom Neese – U. Iowa
  - Aaron Howard – U. Iowa
  - Addam Schroll – Purdue
  - MSFT: Barbara Chung
ORGANIZATION

- Thousands of unmanaged machines
- High infection rate
- Continuing threat to resources and services
  + Lost time, services, reputation, resources
- Distributed organization
Transient customers makes security a challenge
Isolate and remediate hosts at connection time to address these threats
Need to define the “Network Edge” with Policy, not Topology
OVERVIEW OF NETWORK ACCESS PROTECTION

Typical Student PC (unmanaged)

Examine Host

Healthy?

Policy Validation (update continually)

YES

University Network

Remediate

Network Restriction (Isolate)

Ongoing Compliance

NO
SECURITY TEAM ASSESSMENT

Team members

- Aaron Howard
- Addam Schroll
SECURITY TEAM ASSESSMENT THREATS

- Continually these threats occur with varying severity
  - Increased support, ID theft, confidential data
- Serious ongoing threats that continue to consume time and jeopardize network reliability and security
  - Not all threats can be measured with $$
Worms, Bots, Remote Access Users, Guests

NAP offers network access as an incentive to voluntarily comply with University Policy.

Remediation servers allow client to help themselves to required software or patches.

Client must meet current Policy requirements before joining network.

Resulting in Lower risk of wide spread infection.

Zero Day Virus

By updating the System Health Policy, only servers with the latest definitions are allowed network access.
THREATS AND COUNTERMEASURES

- NAP does not protect against malicious users or compromised machines
  + Can a compromised machine trick the NAP agent by posing as healthy?
- NAP will protect Vista and XP SP2, other devices will be allowed as exceptions
  + Exception management is a potential loophole for infected machines
Develop risk management strategy
  + Avoid, Transfer, Mitigate, Accept
Improve host management with user education
Improved threat and vulnerability monitoring
  + Identify & communicate threats to campus
NAP is a compliance tool not a security tool
Improve Network Security
  + Firewalls, IDS, IPS, Application inspection, deviation analysis
ENGINEERING TEAM ASSESSMENT

- Team Members
  - Barry Randall
  - Tom Neese
ENGINEERING TEAM ASSESSMENT
PREREQUISITES

- Network Access dependent on AD and NAP
- Create policy to define network edge
  - Change of Mindset – expect resistance
- Evaluate enforcement methods & exemption methods
  - DHCP, DNS, 802.1x, IPSEC, Radius
  - UNIX, PDA, Game Box, Mac OSX, lab equipment
- Create procedure to manage exceptions
- Create System Health Policy
  - May involve using the SHV API
  - Can SHA perform all required checks?
ENGINEERING TEAM ASSESSMENT DEPENDENCIES

- Infrastructure Requirements
  - AD, DHCP, IPSEC and 802.1X
- Client OS level – Vista or XP with SP2
- Agent (SHA) running on client
ENGINEERING TEAM ASSESSMENT
USAGE & USER EXPERIENCE

- Unmanaged student PCs
  - Windows Vista or XP SP2
- Vendor or Guests
- User Education
- Help Desk Needs
ENGINEERING TEAM ASSESSMENT

TIMEFRAME (estimates)

- Build Network Infrastructure for NAP – 1 to 2 years
  + Implement 802.1X
  + Restricted Network
- Create Network Edge Policy – 6 months
- Build NAP Infrastructure – 3 to 6 months
  + Network Policy Server
  + Health Certificate Server
  + DHCP Server
- Create Initial System Health Policy – 3 months
- Evaluate Exceptions – 3 to 6 months
- Train Help Desk – 1 month
ENGINEERING TEAM ASSESSMENT

ISSUES

✘ Shift to define network edge with policy
✘ Exceptions
  ➕ Will others adopt the SHA API
  ➕ Require custom code to manage
✘ How to install SHA on Windows XP SP2
✘ Third party tool support
✘ Resources required to implement NAP
OPERATIONS TEAM ASSESSMENT
HOW WOULD WE MAINTAIN THIS?

- Team Members
  - Tom Neese
  - Barry Randall
OPERATIONS ASSESSMENT
RESOURCE REQUIREMENTS

- Staff to Develop and Maintain System Health Policy
- Help Desk staff time to help users navigate remediation process
- User education on System Health Check
- Support for 24/7 network access needs
OPERATIONS ASSESSMENT ISSUES

- How to manage exceptions
- Justify resources for a partial solution
- Continual maintenance of policies
- Additional layer to troubleshoot
- Buy-in from others on redefinition of Network Edge
- Enforcement Strategy
Network Edge is continually changing
  + Need Policy (NAP) to protect University Network
NAP is built-in to Vista & Longhorn (low $$)
  + Infrastructure costs could be high
Lowers risk of wide-spread network infection
Not a silver bullet, but another layer of security
RECOMMENDATIONS

- Evaluate risk from unmanaged PCs
  + Separate by exceptions
  + Cost to manage exceptions
- Recommendations
  + Assess and upgrade network infrastructure
  + Analyze Risks vs. Cost to deploy NAP
  + Watch for NAP support in other Operating Systems