

Policy Enforcement on Enterprise Networks

Dr. Tina Bird

Security Architect, InfoExpress

tbird@infoexpress.com

Agenda

- **Blaster blow-by-blow**
- **Stopping the insanity**
- **Short term results**
- **Long term solutions**

Recent Windows Compromises

- **2004 compromises very similar to 1989 compromises: Bad passwords, insecure configurations, unpatched software**

“Recently, the CERT/CC has been working with several Unix sites that have experienced breakins. Running tftpd, accounts with guessable passwords or no passwords, and known security holes not being patched have been the bulk of the problems.” – CERT Advisory -- October 17, 1989

Where's the pain?



- **Cost of attacks**
 - **Disruption of enterprise service**
 - **Lost end-user productivity**
 - **Time to research incident, and develop response strategy**
 - **Time to fix machines**
 - **Potential legal liability**
- **Conservative estimate: 4 hours to repair or rebuild a Windows desktop hit with an automated exploit like Nimda or Blaster**

Preventing Future Blasters

- **Two complementary changes required**
- **User and host identity not sufficient basis for access -- must also examine system properties like patch level and AV software**
- **Infrastructure must enforce granular access decisions and enable appropriate remediation of problems**

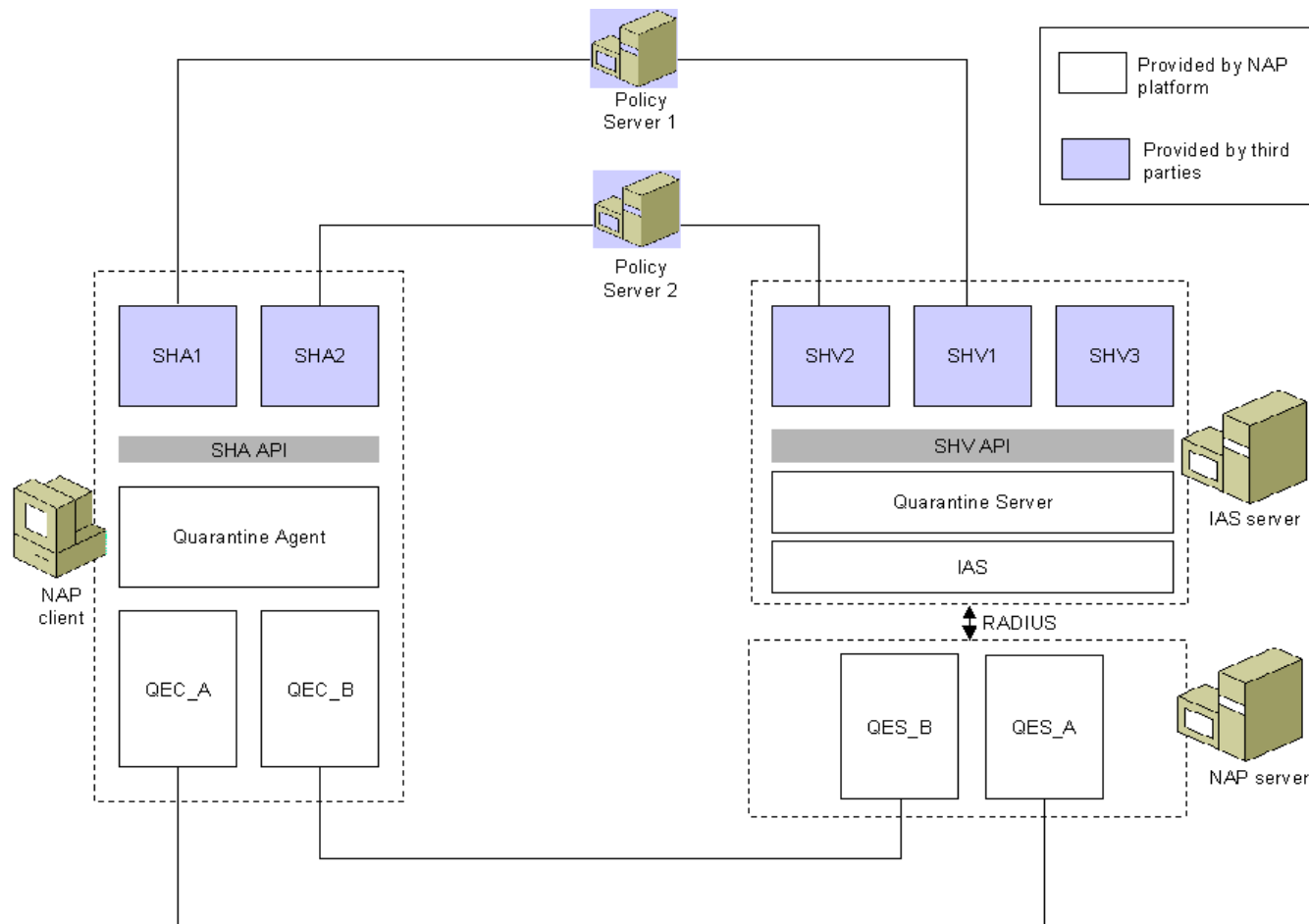
Enforcement Components

- **Policy evaluation server**
- **Network-based enforcement**
- **Communications interface**
- **Natural separation between endpoint data collection/evaluation and network access/enforcement**
- **Dynamic access management based on changing conditions on endpoint, network**

Policy Enforcement Systems

- **Third party policy solutions: InfoExpress, ZoneLabs, etc**
 - **Microsoft *Network Access Protection*: Widely available with Longhorn (2007?)**
 - **Cisco *Network Admission Control*: In early phases**
- **Not yet clear how much of enforcement architecture provided by NAP or NAC**

MS' Proposed Architecture



“Scan and Block” Workflow

- **Endpoint initiates connection**
- **[User/host authentication?]**
- **Endpoint configuration audit**
- **Observed endpoint configuration determines level of network access**
- **[Ongoing configuration audits?]**

“Scan and Block” Options

- **Agent or agentless?**
- **What client properties can be audited?**
- **Policy evaluation server – stand alone, integrated with authentication server?**
- **How are results communicated to endpoint?**
- **How is remediation implemented?**
- **Where is access control decision enforced?**

Cisco NAC Implementation

- **Cisco Trust Agent required on client – can validate presence of Cisco Security agent, some AV software, OS and patch levels**
- **Policy Server – CiscoSecure Access Control server and third-party add-ins**
- **Enforcement managed through Cisco network devices – phased integration**

Cisco NAC Implementation cont.

- **Access managed through Layer 3 devices running Cisco IOS (routers)**
- **Supports multiple assessment results: assigns *Healthy, Checkup, Quarantine, Infected* or *Unknown* tokens to endpoints**
- **HTTP redirect for “automated” remediation**

Cisco NAC Implementation cont.

- **Audit and access management occurs after IP address granted, but before traffic flows through router**
- **Third-party vendors leveraged to provide endpoint audit capability, policy management**

Microsoft NAP Implementation

- **Client: WinXP Pro with new components**
- **Windows Longhorn server**
- **Enforcement managed through DHCP or VPN/Remote Access ACLs (Windows infrastructure, not network infrastructure)**
- **Client initiates checks to policy servers for ongoing monitoring**

Microsoft NAP Implementation cont.

- **Server functionality – access management, server health validation (MS-based), APIs – embedded in Internet Authentication Service (MS RADIUS)**
- **DHCP Quarantine – no default route sent to client, static routes used to access custodial network**

Microsoft NAP Implementation cont.

- **VPN Quarantine – ACLs/ IP filters managed through Remote Access Server**
- **Again, based on projected implementation, highly likely to change!**

802.1x

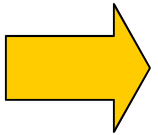
- **Relatively new mechanism for port access control, enforced before IP layer is available to endpoint**
- **Authentication framework -- leverage to include other information about endpoint**
- **Standard includes variety of mechanisms for authenticating endpoints and encrypting authentication dialogue**

802.1x cont.

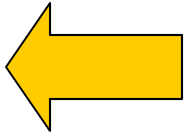
- **802.1x does not collect endpoint data or evaluate configuration**
- **802.1x does not enforce policy**
- **802.1x provides secure communications between endpoint system, authenticator/policy enforcement point/network infrastructure, policy server**

802.1x Conversation

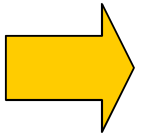
Supplicant initiates Layer 2 link



Authenticator: EAP- Request/Identity



Supplicant: EAP- Response/Identity



RADIUS EAP-Response/Identity → AAA

AAA → Auth Challenge

Supplicant → Auth Response

AAA → Auth Result

802.1x Conversation cont.

- **Auth result is communicated to authenticator (for final establishment of network access) and supplicant (for communication to end user)**
- **Auth result may include “access allowed/access denied,” RADIUS user group assignment, VLAN ID**

Policy Enforcement – Access Decisions

- **Identity isn't enough!**
- **User auth may make compromises *more* severe, if it allows propagation through network resources like shared drives**
- **Similarly, mere assertion of host identity doesn't fix problems related to vulnerabilities and infections**

Policy Enforcement Server

- **Agent collects endpoint properties and communicates information to health verifier/policy server/AAA server**
- **Server compares observed-to-required configuration and returns access decision**
- **Communication may use 802.1x or other (secure) protocol**

Improving Access Decisions cont.


- **How do we define and examine “qualifications” for network access?**
- **What configuration requirements help?**
- **Minimum impact on end users, granular, efficient admin for success**



**Especially
Nobel prize
winners**

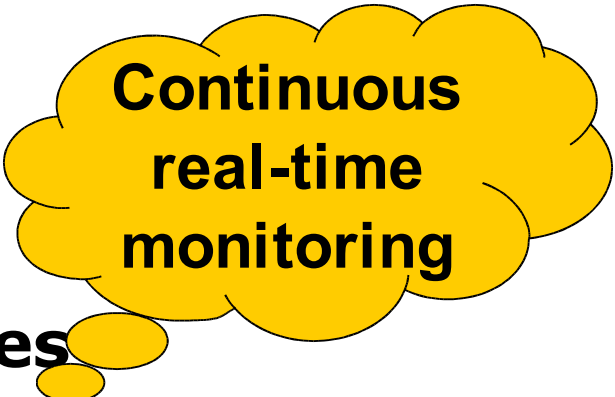
Improving Access Decisions cont.

- **Agent with admin privileges permits maximum inspection of untrusted endpoint machines**
- **Integrated into VPN client, 802.1x supplicant, Web browser, personal firewall**
- **Don't want to disrupt end user experience!**
- **Collects data, shouldn't enforce access decision**



We don't trust the client!

Dynamic Access Control



**Continuous
real-time
monitoring**

- **Endpoint environment changes**
 - **OS/application updates released**
 - **New AV signatures**
 - **Applications enabled/disabled**
- **Agent should report changes in endpoint, so access levels can be adjusted appropriately**

Stopping the Insanity

- **Is it patched?**
- **Is the AV software running?**
- **Does it have good passwords? Does it have passwords at all?**
- **Is it listening on stupid ports?**
- **Is it generating lots of bad traffic?**
- *(Can I do anything to keep people from installing unsolicited executables?)*

“Positive” vs. “Negative” Policies

- **Positive: Desired characteristics are present (Windows Update enabled, AV signature updates enabled, apps running)**
- **Verify configurations that protect against compromises, disruptions in service, disclosure of confidential information**
- **Most efficient long-term approach**

“Positive” vs. “Negative” Policies

- **Negative: Undesirable characteristics are blocked (Blaster is not present, KaZaa is not running)**
- **Prevent infected machines from connecting in the first place**
- **Useful as a “point solution,” but inefficient as long term philosophy – reactive, not proactive**

Hybrid Policies

- **Check that updates are automatically installed (or that patch management system is enabled), security software is running, critical OS/application patches are present, *lack* of known-bad applications or infections**
- **Definition of *critical* is context-dependent**

Critical OS Vulnerabilities?

- **Present in default configuration of OS, or otherwise widely deployed**
- **Impossible or undesirable to disable**
- **Accessible over the network, without user or host authentication**
- **(No user intervention required to trigger)**
- **(Exploit in circulation)**

Auditable Endpoint Properties

- **OS base version, service packs, patches, configuration**
- **Corporate applications (security, productivity) base version, signatures, configuration**
- **Processes running/not running**
- **Network environment (LAN, VPN, hotel)**

Enforcing Policy Decisions

- **Must address all mechanisms used by endpoints to connect to production network**
- **LAN, wireless, VPN/remote access, SSL-based VPNs**
- **If they're not all covered, production network is exposed!**

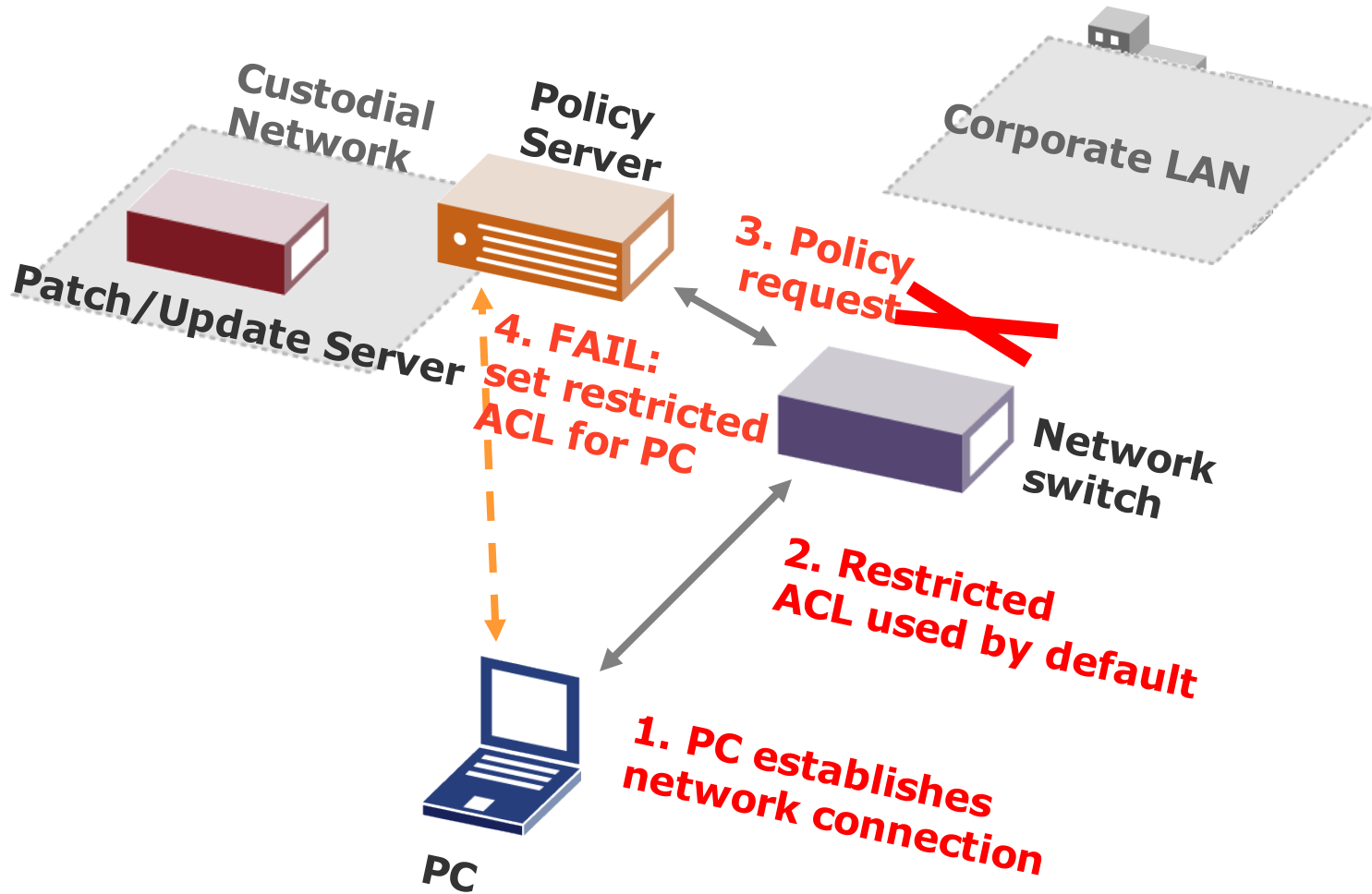
Infrastructure Enforcement

- **Access Control Lists limit which machines are allowed to connect to which hosts/networks via which services/protocols**
- **Policy audits usually put endpoints into PASS or FAIL groups to which ACLs are applied (maybe more)**

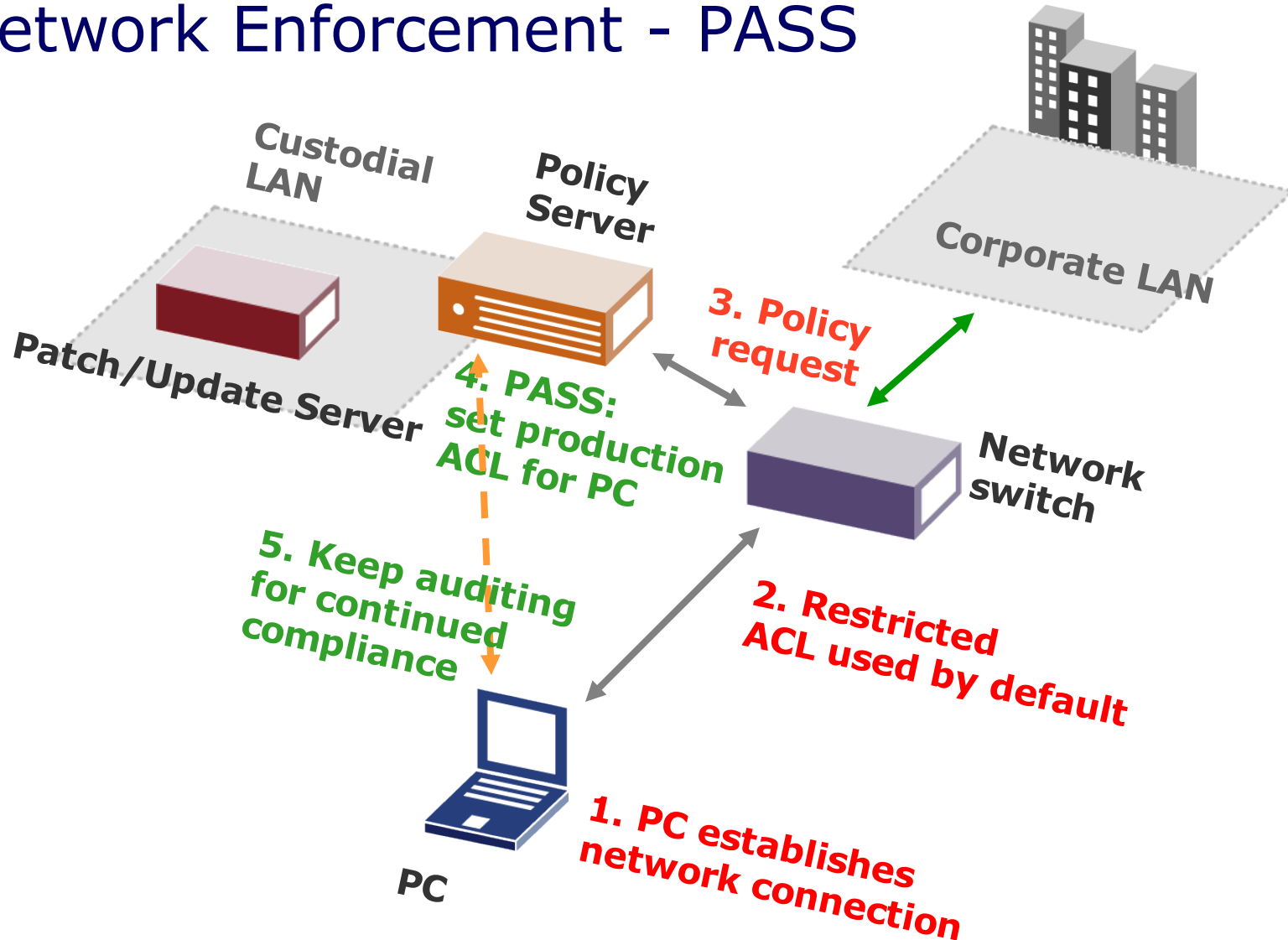
Infrastructure Enforcement cont.

- **PASS/FAIL/other groups identified by VLANs, SSIDs, RADIUS usergroups (system dependent)**
- **For ongoing monitoring, must have mechanism to change an endpoint's "policy assessment group" dynamically**

Network Enforcement - FAIL



Network Enforcement - PASS



Result?

- **Harder for an infected or vulnerable machine to spread contagion throughout production environment**
- **Equity between all network infrastructures (wired, wireless, remote access, SSL VPN) in terms of compartmentalization and security policy enforcement**

Notes on Custodial Network

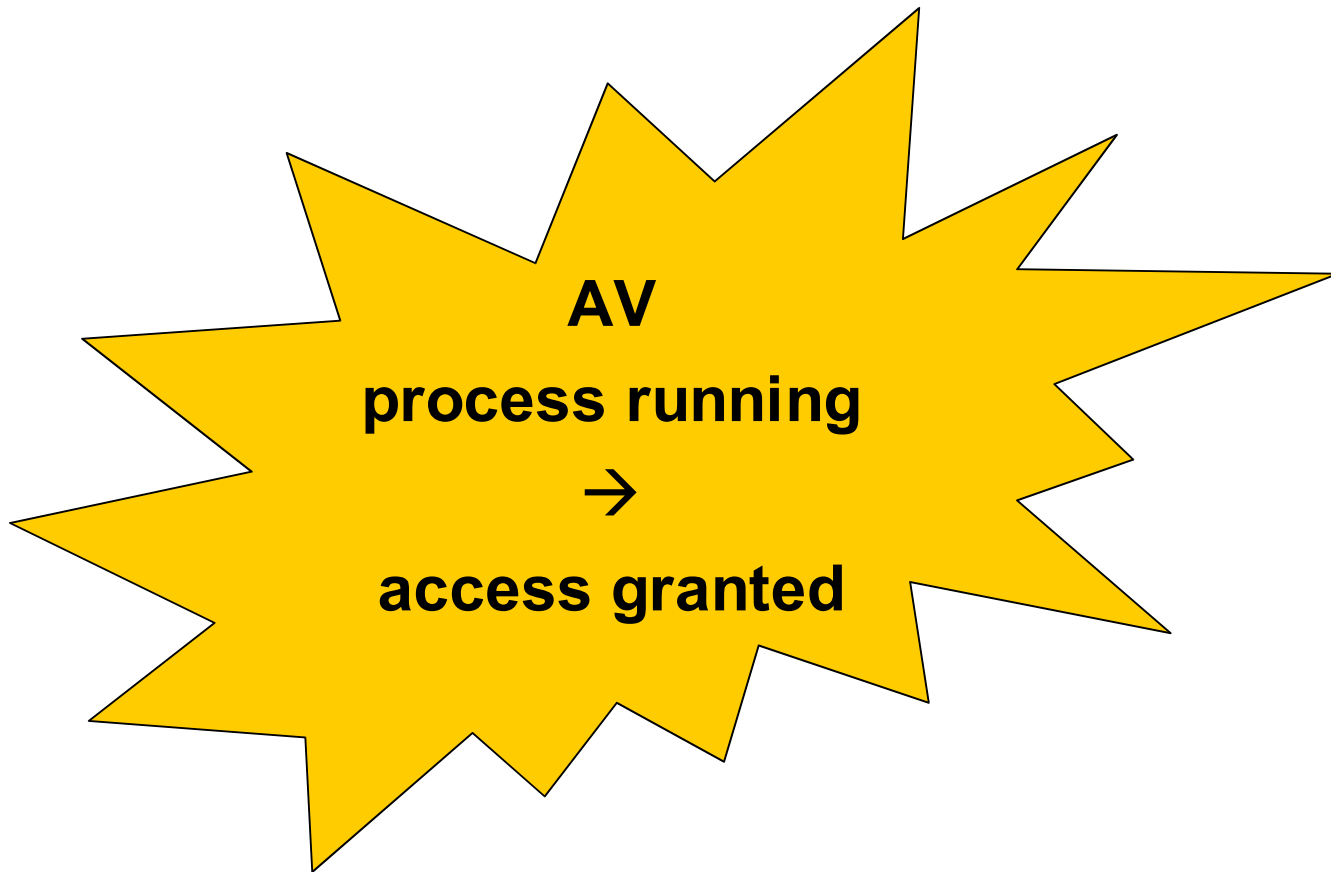
- **Two basic options – shared remediation resources between quarantined and production networks, or completely isolated remediation for quarantined machines**
- **Maximum security vs. cost/ease of maintenance**

Notes on Custodial Network cont.

- **Web server hosting required patches, AV signatures, instructions for end users**
- **Access to patch management/ “live update” server for real-time signatures**
- **Auto-remediation – Install updates transparently to end users**
- **minimizes opportunity for user to make suboptimal security decisions**

Does It Help?

- **Imagine implementing single check**



Exploits & Viruses that Interfere with AV Processes:

Sasser

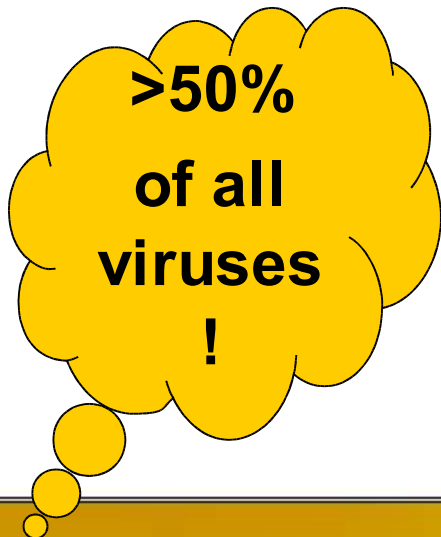
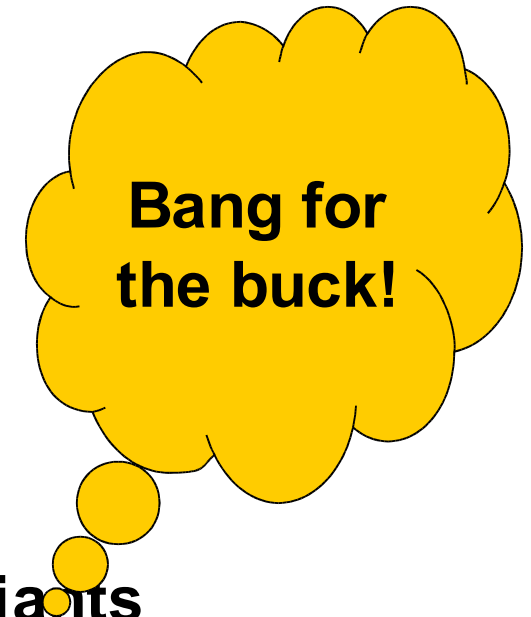
Phatbot/Agobot

Darby & variants

Beagle/Bagle variants

Bagz & variants

MyDoom



Conclusions

- **Even relatively simple checks can greatly limit damage from viruses and worms**
- **Makes threats from wired and wireless LANs more comparable**
- **End user security decisions are far less likely to bring down the production environment**