



Automated Patching

Paul Asadoorian
IT Security Specialist
Brown University



Outline

- Automated Patching Introduction
- Tools from Microsoft
 - Microsoft SUS
 - Microsoft SMS
- Others
 - HFNetCheck Pro (Shavlik)
 - Novell ZenWorks
 - BigFix



Automated Patching

- No longer a nice to have, now a requirement
- Development cycles on malicious software is now much shorter
- Users will not respond in time



Automated Patching

- Vulnerable systems will be exploited within seconds of being on the network
- We need ways to manage our vulnerable systems
- Policies need to exist, esp. when pushing software to users



Automated Patching

- Pushing a patch to 80% of your users is easier than:
 - A. Leaving it up to the user to do it themselves
 - B. Going around to every machine and patching them manually
 - C. Replacing all the desktops with Macs running OS X
 - D. All of the above



Automated Patching

- There is no perfect solution
- Patches will fail to push
- Rather focus on the exceptions
- In the end we save time and money



Microsoft SUS 1.0

- Software Update Services
- **Free** Product from Microsoft
- Allows patching of Windows XP, 2000 (SP2 or later, Windows Server 2003



Microsoft SUS 1.0 - Features

- Allows you to manage:
 - Windows Critical Updates
 - Windows Security Patches (Critical, Important, Moderate, and Low)
 - Windows Update Rollups
 - Windows 2000, Windows XP, and Windows Server 2003 Service Packs



Microsoft SUS 1.0 - Features

- Approve Patches before deploying
- Test Patches first
- Then deploy to all systems



Microsoft SUS 1.0 - Features

- Uses built-in auto-update client
- Uses BITS (Background Intelligent Transfer Service)
 - Doesn't take down the network when downloading patches



Microsoft SUS 1.0 - Drawbacks

- Does not handle Win95/98/ME/NT
- Does not support Office, IIS, or SQL
- Cannot add your own updates
- Does not update drivers



Microsoft SUS 1.0 - Drawbacks

- Cannot choose to patch just one platform (All or nothing)
- Users still need access to run windows update for other things



Microsoft SUS – 2.0

- Support for Windows, Office, SQL, and Exchange patches
- Reporting capabilities – deployment status about download, install and impacted machines.
- Ability to uninstall patches that support uninstall



Microsoft SUS – 2.0

- More Administrative controls – patch install, uninstall, install by a deadline, and configurable client polling intervals.
- Targeting of different updates to administrator defined groups of machines.
 - Push patches by OU



Microsoft SMS 2.0

- Systems Management Server
- Full desktop management application
- Controls all software
 - Software metering
- Inventory of Hardware and Software



Microsoft SMS 2.0

- Requires software client and domain membership
- Cost associated with server and possibly every client
- Network and System monitoring



Microsoft SMS 2.0

- Deploy, Patch, and Inventory all software and patches
- Powerful tool
- Requires more effort than other solutions



HFNetCheckPro 4.0

- From Shavlik, licensed MS technology
- Not a free product
 - Cost for each administrator
 - Cost for each desktop



HFNetCheckPro 4.0 - Features

- Clientless patch inventory and push technology, Requires:
 - Administrative rights on the remote machine
 - NetBIOS (tcp139) or CIFS (tcp445) ports must be accessible
 - The Server service must be running



HFNetCheckPro 4.0 - Features

- Requirements (Cont.):
 - The Remote Registry service must be running
 - The %systemroot% share (usually C\$ or similar) must be accessible



HFNetCheckPro 4.0 - Features

- Finds all Windows computers on your network
- Stores results in a SQL Database
- Supports Office, Exchange, SQL
- Does not require Domain login/membership

HFNetCheckPro 4.0 - Drawbacks



- Client configuration has to be just right or it doesn't work
- It's a push, so personal firewalls prevent patching
- Competes with SUS and SMS (future direction?)



Other Solutions

- BigFix (www.bigfix.com)
 - Client based solution similar to SMS
 - Exepensive

- Novell ZenWorks
(<http://www.novell.com/products/zenworks/>)
 - Relies on Novell Infrastructure
 - Requires Client
 - Already Covered by Scott



What about Unix?

- Solaris (See Nancy)
- Red Hat Linux (up2date)
 - Based on RPM
- Debian Linux (apt)
 - Based on deb, also used with RPM
- Others?
 - Patching console application?