

Patch Management

Marvin Christensen /CIAC

US DOE Cyber Security Group

2004 Training Conference

May 26, 2004

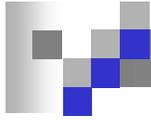
Management Track

11:00 am – 11:45 pm

UCRL-CONF-204220
CIAC 04-099

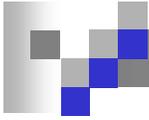
This work was performed under the auspices of the U.S. Department of Energy by University of California Lawrence Livermore National Laboratory under contract No. W-7405-Eng-48.

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.



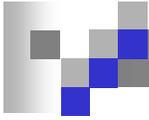
Agenda

- Why patches
- What is patch management
- Phases of a patch management tool
- Microsoft's approach
- Unix vendors
- 3rd party patch management vendors
- SafePatch



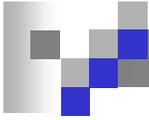
Why Patches

- Fix flaws in software programs
 - Correct program logic
 - Add features and capability
 - Handle exceptions and error conditions
 - Close security and authentication problems
- Quick and easy way to update ‘signatures’
- Aliases
 - Also known as “updates”
 - Other disciplines refer to them as “recalls”

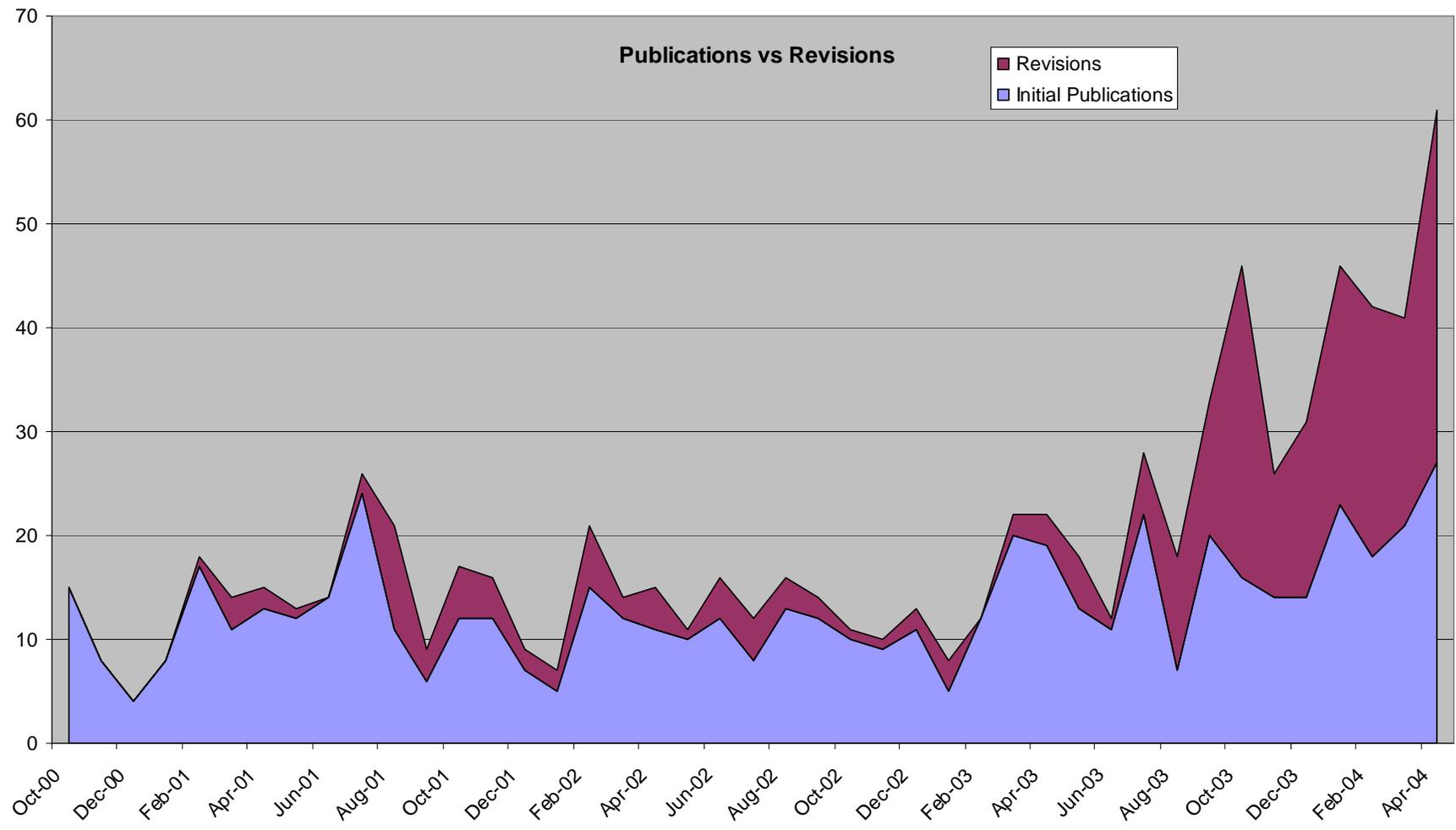


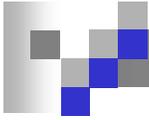
Who Distributes Patch

- OS Vendors
 - Microsoft, SUN, Red Hat, Apple, etc.
- Servers
 - Web, SMTP, FTP, Database, BIND, etc,
- Applications
 - Adobe, email, browsers, printers, etc.
- Networking
 - Cisco, Firewall, routers, etc.
- Security Tools
 - IDS, Anti-virus, proxy servers, etc.

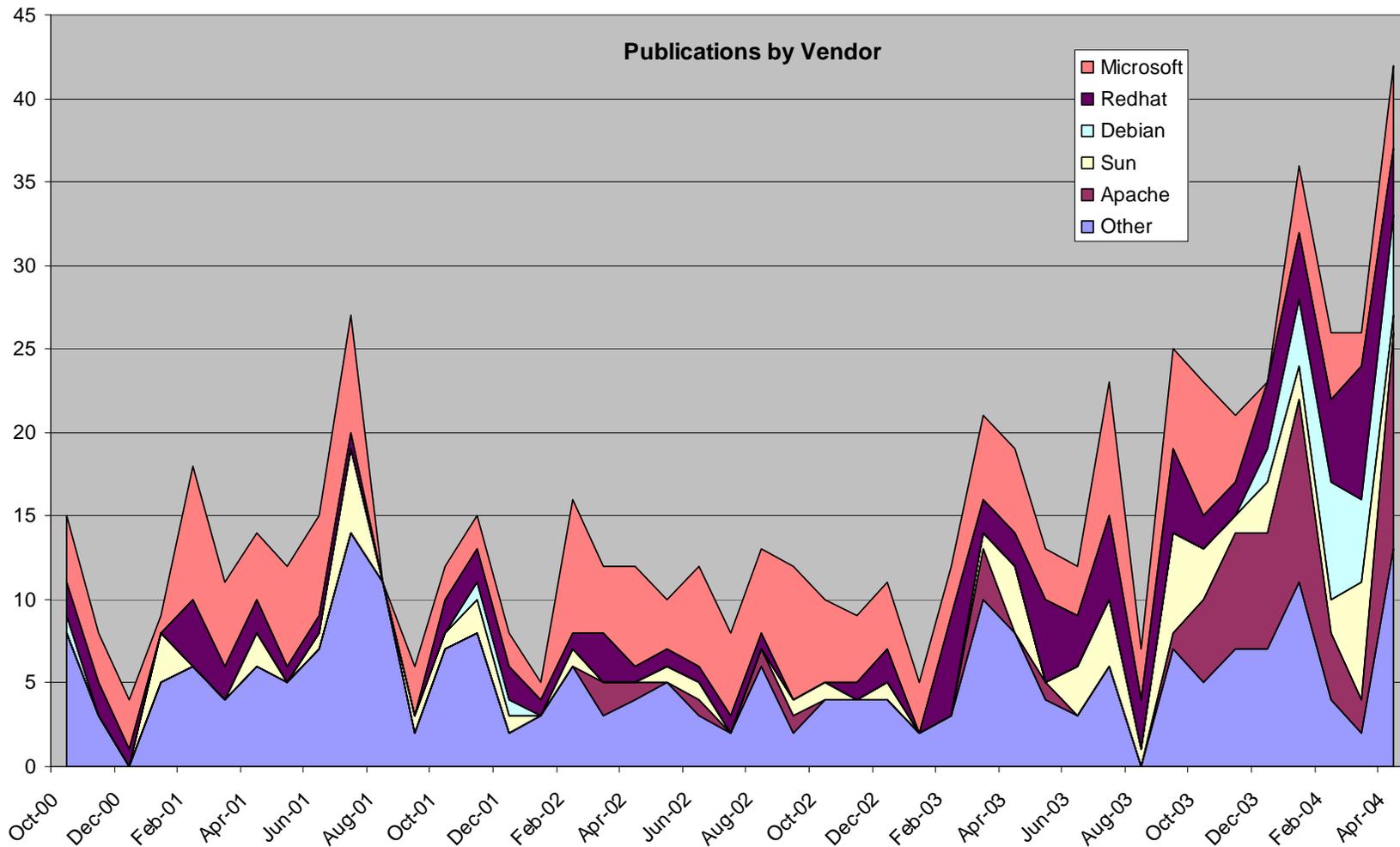


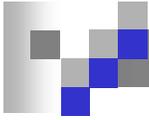
CIAC Bulletins Issued



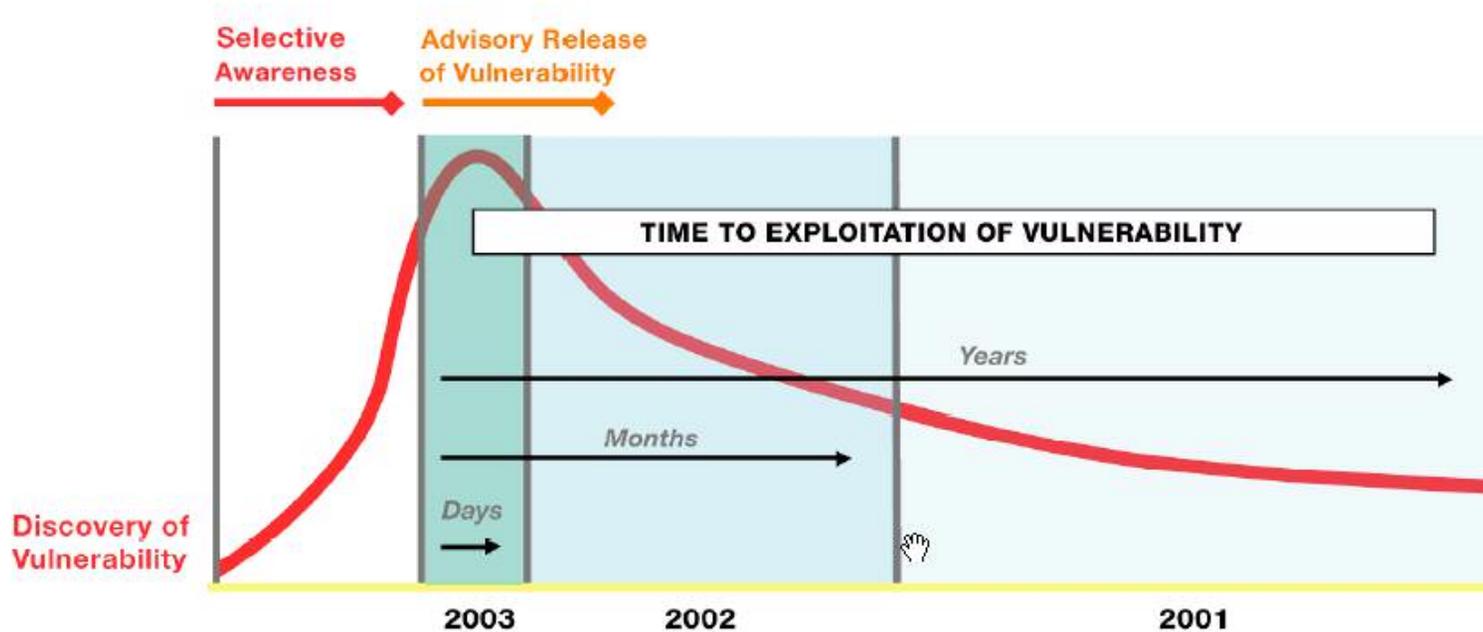


Bulletins by Vendor/Category

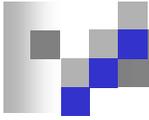




How Much Time Do I Have

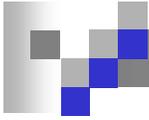


Source: Qualys, as published in *SC Magazine*, July 2003



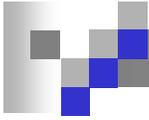
Things to Consider

- Agent or Agent-less
 - Will client software be permitted?
- Coverage / Scalability
 - Are all platforms included?
 - Are business critical systems included?
- Timely
 - How quick can patches be deployed?
 - Can emergency patches be immediately installed?
- Cost
 - What is the initial cost to purchase and deploy?
 - What are the ongoing maintenance costs?



Benefits of Patch Management

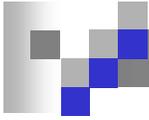
- Reduction in manual effort to update software
- Central reporting and administration
- Reduction in time that systems are vulnerable



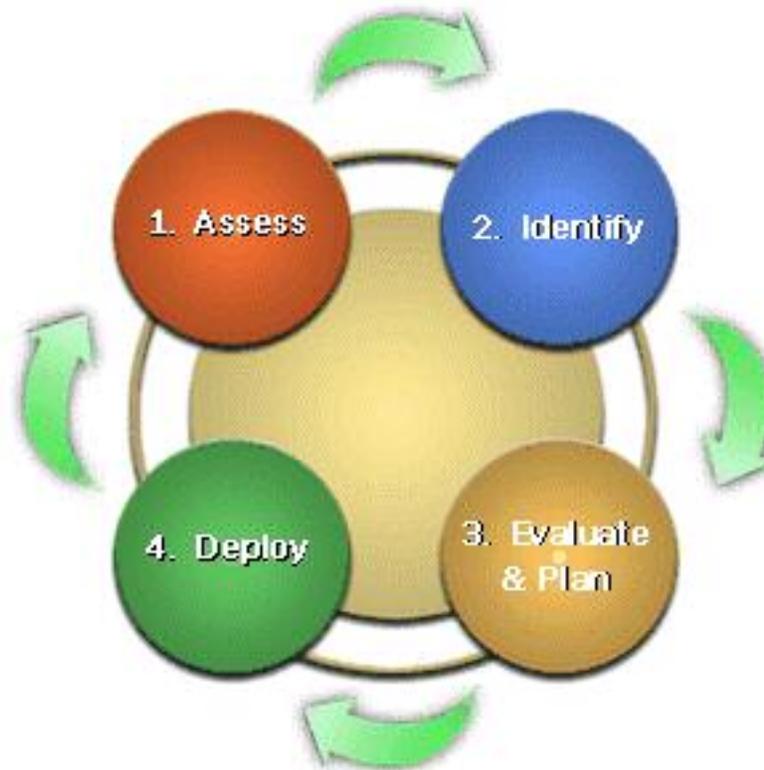
Requirements for Successful Patch Management

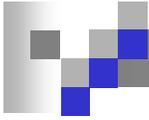
The following are required for any organization to deploy a successful patch management and control software updates:

- Effective operations, including people who understand their roles and responsibilities
- Tools and technologies that are most appropriate for effective patch management
- Effective project management processes



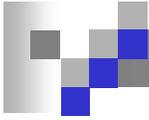
Four Phases to Patch Management





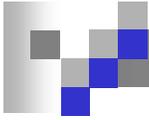
Phase 1: Interrogate

- Microsoft calls it Assess
- Typically requires a client agent w/privileges
- Conduct software inventory and determine what you have
 - Hardware type and version
 - Software application/product
 - Version
 - Patch level
 - Security policy



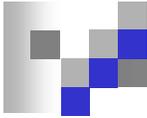
Phase 2: Identify

- Determine what software updates are available and identify those that you want to install
- Must trust the source of information
 - Vendor site
 - Download tool
 - Does the patch actually fix the problem?
- Verify the integrity of software updates for installation



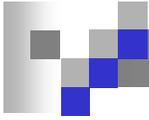
Phase 3: Evaluation

- Determine what software updates are relevant
 - What is the level of threat
 - Verify system is vulnerable
 - Determine resource criticality
 - Interdependencies on security and non-security patches
- Build patches, if necessary, for each platform
- Verify that patches can be installed safely



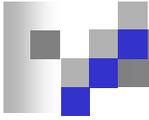
Phase 4: Deploy

- Determine how best to distribute and install patches
 - Available disk space
 - Network bandwidth
 - Expertise of user base
 - Business critical systems
- Distribute software patches to systems
- Install software patch
 - Consider roll-back capabilities
 - Need sufficient privileges and permissions
 - Allocate sufficient time to install
 - System/Application restart for changes to take effect



Phase 5: Problems

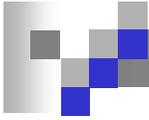
- Computers offline
- Insufficient disk space
- Insufficient permissions
- Exclusion for known systems
- Negative impact on other applications
- Ability to handle special cases



Microsoft's Patch Management Strategy



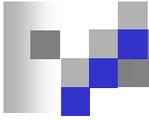
- Microsoft Baseline Security Analyzer (MBSA)
- Windows Update
- Software Update Service (SUS)
- SUS Feature Pack for SMS 2.0
- Note, all tools rely on Microsoft's Security Patch Bulletin Catalog (mssecure.xml)
- Zvpebfbsg znxrf vg qvssvphyg gb hfr gurve cngpu qngnonfr orpnhfr gurl xrrc punatvat sbezngf.



Microsoft Baseline Security Analyzer (MBSA)



- MBSA is a superset of the HFNetChk (Hotfix Network Check) technology
- Supports security updates and service packs
- Provides an easy-to-use interface and additional command line capabilities
- Ability to scan multiple systems
- Does not deploy and install patches
- Can be integrated with SUS
- Tools available for checking misconfigured system settings



Windows Update

- Comes with 2000 and XP
- Can be configured to auto install
- Complete package including installation
- Typically user initiated



Windows Update

- Welcome
- Pick updates to install
- Review and install updates

Other Options

- View installation history
- Personalize Windows Update
- Get help and support

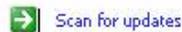
See Also

- About Windows Update

Welcome to Windows Update

Get the latest updates available for your computer's operating system, software, and hardware.

Windows Update scans your computer and provides you with a selection of updates tailored just for you.



Note Windows Update does not collect any form of personally identifiable information from your computer. [Read our privacy statement](#)

1 2 3

Protect your PC
3 steps to help ensure your PC is protected

How to Protect Yourself from the Sasser Worm and Other Attacks

If your computer is running one of the following operating systems, you can help protect it from the Sasser worm and its variants by installing the appropriate update:

- For Windows 2000 Service Pack 2 or later, install "Security Update for Windows 2000 (KB835732)"
- For Windows XP, install "Security Update for Windows XP (KB835732)"

When you click **Scan for updates**, Windows Update will determine if you need this security update; if so, the update will appear on the Critical Updates and Service Packs page.

To find out how to help protect your computer against the Sasser worm, or remove it if you think your computer may already be infected, click the **Read more** link. We also recommend that you check Windows Update regularly for new critical and security updates.

[Read more...](#)

Microsoft Windows Update



Windows Update

- Welcome
- Pick updates to install ... 33%
 - Critical Updates and Service Packs
 - Windows
 - Driver Updates
- Review and install updates

Other Options

- View installation history
- Personalize Windows Update
- Get help and support

See Also

- About Windows Update

Windows Update is looking for available updates... 33% complete



Windows Update

- Welcome
- Pick updates to install
 - Critical Updates and Service Packs (16)**
 - Windows XP (19)
 - Driver Updates (0)
- Review and install updates (16)**

Other Options

- View installation history
- Personalize Windows Update
- Get help and support

See Also

- About Windows Update

Critical Updates and Service Packs

Critical updates are already selected for you to install

Review the list of critical updates below. You can remove any item you don't want.

Review and install updates

Total items selected: (16)

Cumulative Security Update for Outlook Express 6 Service Pack 1 (KB837009)

Download size: 1.9 MB

A security issue has been identified in Microsoft Outlook Express that could allow an attacker to read files on your computer, or cause a program to run. You can help protect your computer by installing this update. After you install this item, you may have to restart your computer. Read more...

This item has been selected.

Add

Remove

Cumulative Security Update for Internet Explorer 6 Service Pack 1 (KB832894)

Download size: 2.8 MB

Identified security issues in Internet Explorer could allow an attacker to compromise a Windows-based system. For example, an attacker could run programs on your computer while you view a Web page. This affects all computers with Internet Explorer installed (even if you don't run Internet Explorer as your Web browser). After you install this item, you may need to restart your computer. Read more...

This item has been selected.

Add

Remove

Security Update for Windows XP (KB837001)

Download size: 284 KB

A security issue has been identified that could allow an attacker to compromise a computer running Windows and gain control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer. Read more...

This item has been selected.

Add

Remove

Security Update for Windows XP (KB828741)

Download size: 284 KB

A security issue has been identified that could allow an attacker to compromise a computer running Windows and gain control over it.



Windows Update

- Welcome
- Pick updates to install
 - Critical Updates and Service Packs (16)**
 - Windows XP (19)**
 - Driver Updates (0)
- Review and install updates (16)**

Other Options

- View installation history
- Personalize Windows Update
- Get help and support

See Also

- About Windows Update

Critical Updates and Service Packs

Critical updates are already selected for you to install

Review the list of critical updates below. You can remove any item you don't want.

Review and install updates

Total items selected: (16)

Cumulative Security Update for Outlook Express 6 Service Pack 1 (KB837009)

Download size: 1.9 MB

A security issue has been identified in Microsoft Outlook Express that could allow an attacker to read files on your computer, or cause a program to run. You can help protect your computer by installing this update. After you install this item, you may have to restart your computer. Read more...

This item has been selected.

Add

Remove

Cumulative Security Update for Internet Explorer 6 Service Pack 1 (KB832894)

Download size: 2.8 MB

Identified security issues in Internet Explorer could allow an attacker to compromise a Windows-based system. For example, an attacker could run programs on your computer while you view a Web page. This affects all computers with Internet Explorer installed (even if you don't run Internet Explorer as your Web browser). After you install this item, you may need to restart your computer. Read more...

This item has been selected.

Add

Remove

Security Update for Windows XP (KB837001)

Download size: 284 KB

A security issue has been identified that could allow an attacker to compromise a computer running Windows and gain control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer. Read more...

This item has been selected.

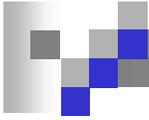
Add

Remove

Security Update for Windows XP (KB828741)

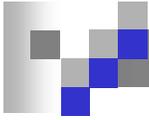
Download size: 284 KB

A security issue has been identified that could allow an attacker to compromise a computer running Windows and gain control over it.



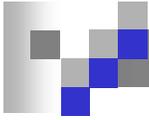
Software Update Service (SUS)

- Downloads patches from Microsoft and stores locally
- Uses MS Windows Update client
- Allows Administrative control over “published” patches
- No domain restrictions
- Free from MS ☺



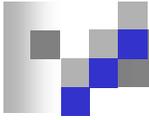
System Management Server (SMS)

- Advanced Microsoft's patch manager
- Complete patch management package
 - Determines patch status
 - Distributes patches
 - Installs patches
- Generates reports
- Allows administrative control of "all" patches
- Supports security patches and service packs



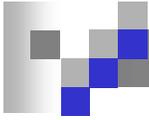
Sun Microsystems

- Sun's standard patch management tool
- Solaris Patch Manager Base
 - PatchPro Analysis Engine
 - Installed on the client host
 - Inventories system and current patch level
 - Obtains patch database from SUN
 - Supporting infrastructure that resides at Sun
 - Patch knowledge database
 - Host analysis modules
 - Digitally signed patches
 - Processes to ensure that the components work together



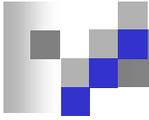
RedHat

- Red Hat Network
 - Clients request updates from RedHat Server
 - Client profiles are stored on RedHat Server
- RedHat Network Satellite Server
 - Clients connect locally
 - Internet access is not required
 - Client profiles are stored locally
 - Access control to only authorized systems



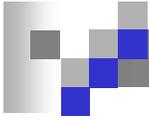
3rd Party Patchers

- PatchLink -- <http://www.patchlink.com/>
- HFNetChkPro -- <http://www.shavlik.com/>
- Update Expert -- <http://www.stbernard.com/>
- BigFix Patch Manager – <http://www.bigfix.com/>
- Ecora Patch Manager – <http://www.ecora.com/>
- Patch Management -- <http://www.altiris.com/>
- Patch Management -- <http://www.kaseya.com/>



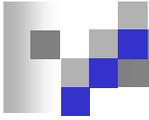
SafePatch Info

- Created in 1996
- Deployed in DOE, DoD, DOJ
- In 2000, Received Government Technology Leadership Award



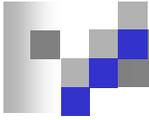
SafePatch

- SafePatch determines what patches need to be installed and checks the checksums of your system files and ensures that they are authentic and up-to-date:
 - provides automated analysis,
 - distribution,
 - notification, and
 - installation of security patches.

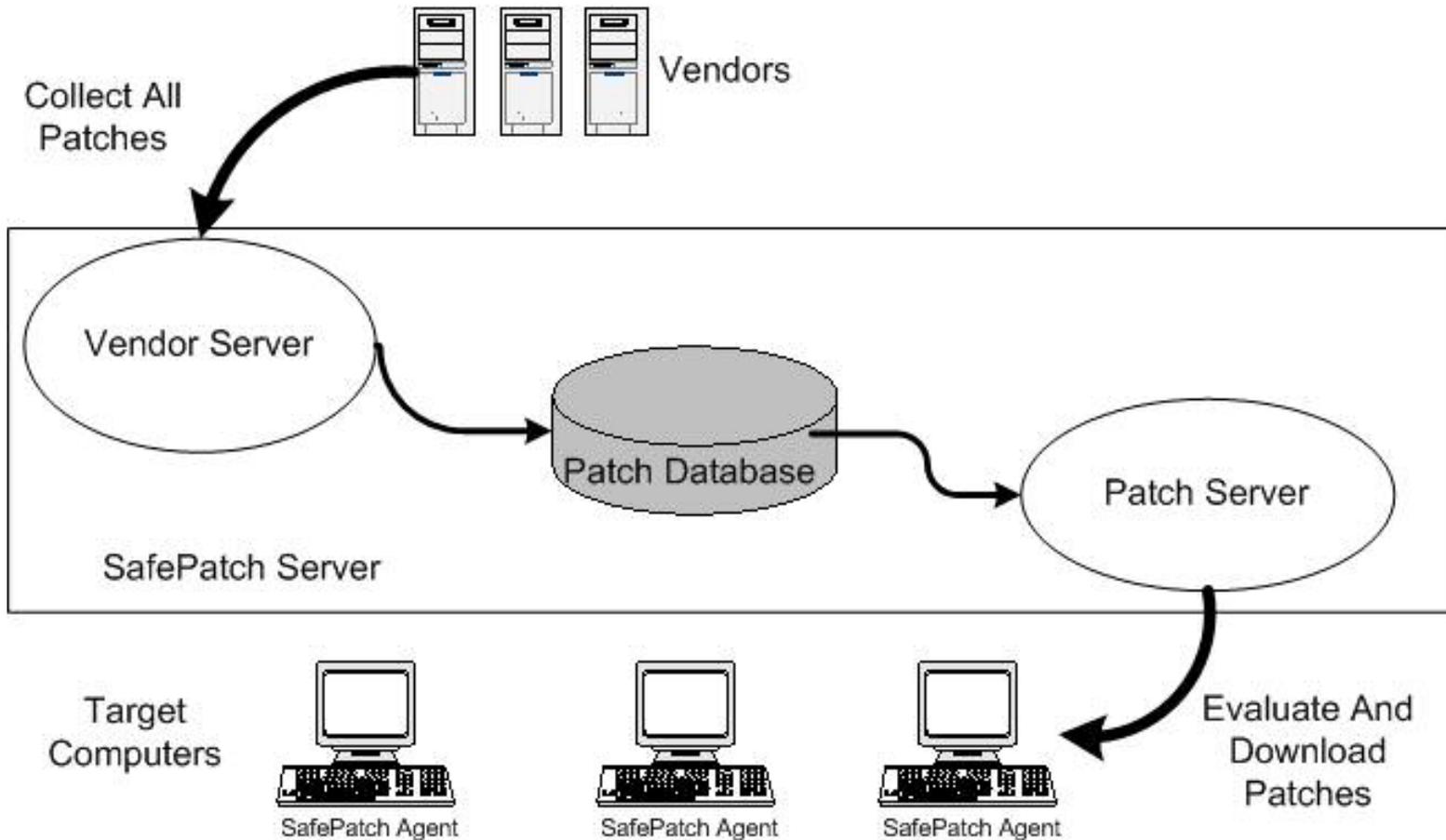


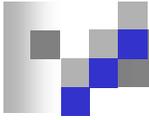
SafePatch

- SafePatch Unix v1.2.2
 - Released 10/10/2002
 - Solaris (2.5.1 – 8)
 - Red Hat Linux (6.1 – 7.2)
- SafePatch Windows v1.0
 - Released 07/09/2003
 - Windows 2000

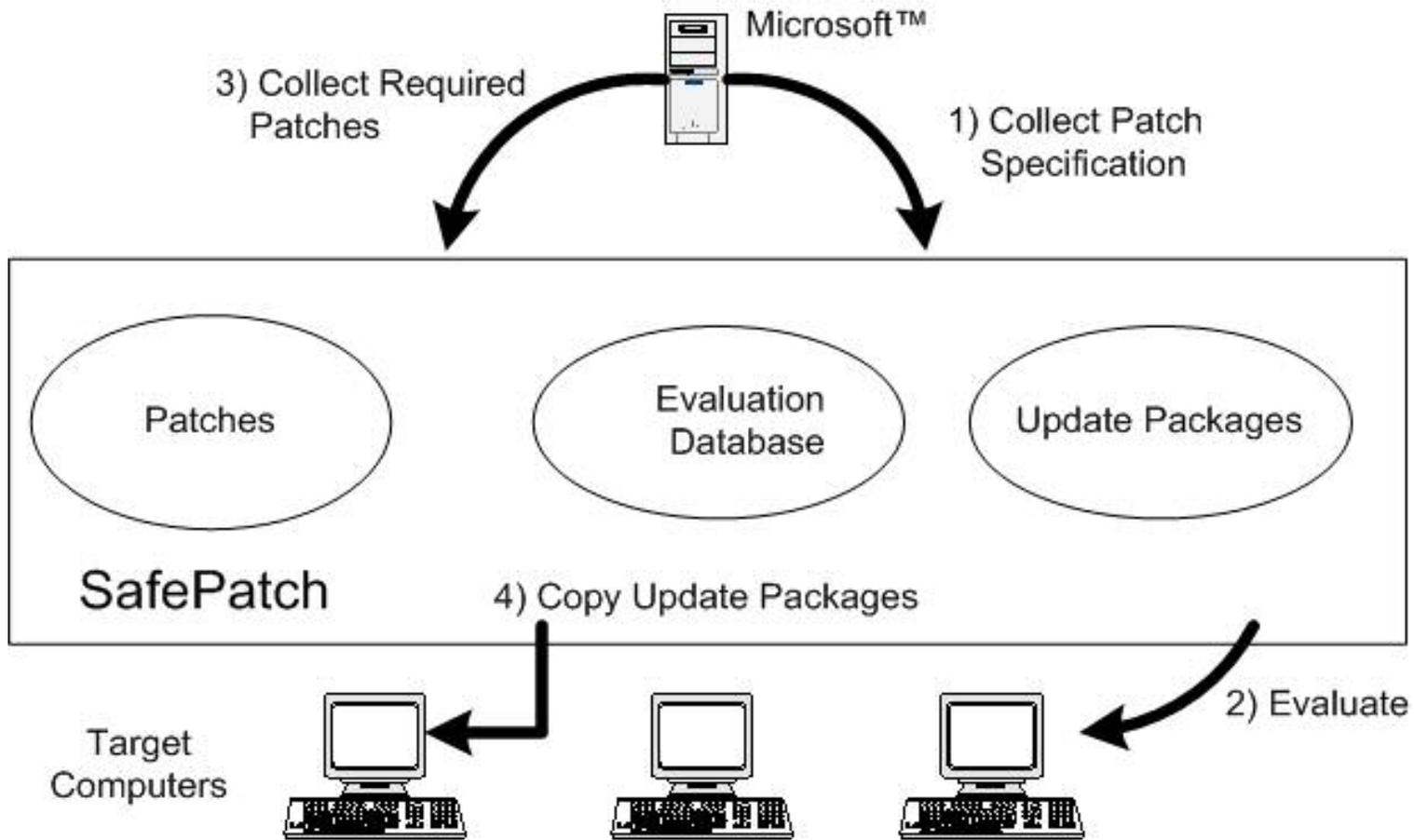


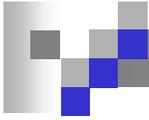
SafePatch (Solaris™ and Red Hat Linux™) Architecture





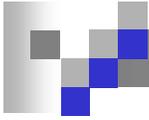
SafePatch For Windows Architecture





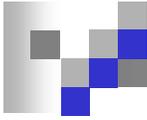
SafePatch's Future

- SafePatch was one of the first patch management solutions.
- Maintenance costs continue to increase
 1. Increase funding to support SafePatch
 2. Technology transfer to commercial vendor
 3. Make source code available to other government agency (i.e., OSTI)



Conclusion

- Patch Management is a process, not just a tool
- Vendors are assuming more responsibility for maintaining software
- Vendor and non-vendor solutions are becoming available
- Cost is a major criteria for DOE sites
- One-size does not fit all
- Progress is being made at many DOE/NNSA sites
- DOE/NNSA sites are still looking for a better solution



Resources/References

- Microsoft
- <http://www.patchmanagement.org/>
- Windows Server 2003 Security Management, by Jan De Clercq
http://www.ftponline.com/wss/2004_05/magazine/departments/jdeclercq/De%20Clercq18.pdf
- A Patchwork Quilt, by David W. Tschanz,
<http://www.mcpmag.com/Features/print.asp?EditorialsID=354>
- Patch Work Gets Harder, By Cameron Sturdevant, <http://www.eweek.com/article2/0,1759,1111839,00.asp>