Global Information Assurance Certification Paper

Windows Update and Its Derivatives – With a focus on SUS

Pei-Li Chao

4 April 2003

v.1.4b

Abstract

Automatic Updates can be configured to automatically download and install the newest patches from Microsoft web site through *Windows Update*. Although it is very convenient, it is neither the only way nor the best way to keep computers up-to-date. This paper offers four alternative means of working with *Windows Update Service* to patch up windows computers in a more manageable manner for organizations. Each of these alternatives has its pros and cons and each fits into different computation environment. *Update Catalog* provides an opportunity to download patch files to a local device, which make update files portable and convenient for computers with slow Internet connection or no Internet connection. But, the lack of automatic installation function has limited itself to small-scale updating. On the other hand with *Software Update Service (SUS)* the updates can be deployed automatically without user intervention. While its limitation to *Windows 2000* and *XP* clients can be a shortfall, but majority of computers are covered. *System Management Serve (SMS) with SUS Feature Pack* is a heavy-duty product. It seems to be an excess to implement SMS just to have automated Software Update function. However, for an existing SMS environment, SUS Feature Pack creates an ideal way for delivering Windows Update. For comparison purpose, *UpdateEXPERT*, a third party Windows Update management software is briefly discussed.

Prelude

In SANS classroom, the instructor tipped us a possible malicious attack carried out by exploiting the nature of Windows Automatic Updates. What a shocking new! If this does happen it will be devastating since we rely heavily on Automatic Updates to patch our workstations. With a sense of mission, I immediately notified our security officer of this possible attack. Although there was no breaking news on hackers taking on this route even until today, my interest in Windows Updates has grown. I wanted to learn every aspect of its mechanism, especially how it is designed to deliver files to windows computer worldwide. By understand the basic, in hope I can see the vulnerability that can be exploited on. Nevertheless, in the course of learning Windows Update, the security issue becomes my least concern. It is the various updating methods that Microsoft provides draw most of my attention and interests. As a software that is used globally on every Windows computer, I have no doubt that Microsoft will do much more than their best to make it secure. But, there are reasons other than security that companies should investigate these alternatives. The reasons such as privacy, network traffic and network management are also important to a company's asset. This paper will explore alternate methods, namely Software Updater Server (SUS), Windows Update Catalog, SMS and UpdateEXPERT.

The History of Windows Update

In the past 20 years, Microsoft has developed a long line of products from operating systems to web servers, database servers, E-mail servers, office suites and many others. Each one of these software has an average life cycle of 5-7 years [1]. In this time period, Microsoft is obligated to provide service in fixing bugs, improving the software and most importantly patching up security holes. However, it requires not only Microsoft to put in the effort in maintaining the software, but also IT personnel to religiously check for the new updates and diligently update the workstations and server accordingly. With the increasing popularity of the Internet and the fast growing of e-business, there are more business and individuals depending on the up-to-dated software, and especially up-to-dated operation systems to elude cyber attack from internet-spread worms and destructive hackers. Therefore, it is crucial to inform software users and deliver patches to needed computer in timely fashion once solution to vulnerability is found. Windows Update is the solution Microsoft provided to do just that. Starting from Windows 98 [2], Microsoft incorporated Windows Update as an on-line free service to all of its Windows Operating Systems.

How Windows Update Works

Windows Update is an on-line service that operates from http://www.windowsupdate.microsoft.com web site. Users can either type in this URL from *Internet Explore*, or click on the Window Update item from the Start menu to get to the site. In order for Windows Update to decide which update or patch is needed for a particular computer, it will need to scan the computer to gather information on the version of currently installed software. Therefore, by clicking Scan for Updates, you allow Microsoft to look inside of your hard drive to see what you have and what you don't have to generate a list of inventory. The list will then compare to a list of available components from Microsoft and make suggestions on what to download and install. Microsoft uses a technology called *AtiveX* controls to do the scanning [3] [5]. It is downloaded and installed to a local hard drive during the first visit of Windows Update site. Scanning can be an invasive act. However, according to Windows Update Privacy Statement, there is no private information collected [4]. The configuration information gathered are Operating System version number, Internet Explorer version number, version numbers of other software for which Windows Update provides updates, Plug and Play ID numbers of hardware devices, and Region and Language setting. Nevertheless, it does collect the Product ID and Product Key to confirm that the running OS has a valid license. On top of it, a *Globally Unique Identifier* (GUID) is stored onto the computer to collect the statistic information on the succeeded or failed download and installation. There are two security implementations Microsoft designs to ensure the file source is legitimate and only authorized personnel can install the updates. The rules are all the downloaded files must be digitally signed by Microsoft, and only local administrator can install the update to achieve the file authentication and authorization. Windows Update is truly a wonderful service provided by Microsoft. In addition to making the computer safe with Critical and Security Updates, it also provides downloads for new version and features to the software and Operating System files. And, with extra

bonus, it also helps in updating device drivers to improve the functionality of the hardware. However, with all the good things about Windows Updates, there are things to consider if it is right for your organization. First of all, if every workstation in your organization goes to Microsoft Update site to get updates, what kind of network traffic will it generate especially with slow WAN connection? Secondly, user may not know if the updates are necessary for his or her computer. Thirdly, the patches cannot be tested before install. Finally, do you want to or can you afford to give Microsoft access rights to your computers? For instance, in a hospital setting where patient confidentiality might be jeopardized by the scanning and information collection of Windows Update. Fortunately, there are other options. The table below provides a comparison overview of these options. The following sections further explain the options in details.

	Windows Update	**Windows Update Catalog**	**SUS**	**SMS + SUS**	**UpdateEXPERT**
Price	Free	Free	Free	$$	$$
Automatic Install	Yes	No	Yes	Yes	Yes
Report Feature	No	No	No	Yes	Yes
Downloadable patches	NO	Yes	Yes	Yes	Yes
Platforms	98, ME, NT, 2000, XP, 2003	98, ME, 2000, XP, 2003	Windows 2000, XP	98, ME, NT, 2000, XP, 2003	98, ME, NT, 2000, XP, 2003

Windows Update Catalog

Windows Update Catalog is a useful tool for home and small business users. When you use Windows Update through Microsoft site, there is no option to save the patch files to local storage devices. So, each computer has to do its own downloads. It doesn't make much sense for a person with multiple computers and with slow Internet connection to repeat this step over and over again. Windows Update Catalog is able to fulfill this missing function for Windows Update.

Procedures [6]

To use the Windows Update Catalog function, go to http://v4.windowsupdate.microsoft.com/en/default.asp by clicking on the Windows Update shortcut from Start button. However, Microsoft has hidden this function from this page. You need to click on "Personalize Windows Update" link on the left hand pane and put a check mark on "Display the link to the Windows Update Catalog under See Also" check box before the link to Windows Update Catalog will display on the welcome page. Once you can get to the link, the catalog is very well organized by Microsoft and very simple to use. Windows

Update Catalog provides option to download all possible updates ranging from critical, security updates to new device drivers. Not only that, the downloadable files are organized by Operating systems and provide updates for Windows 98, 2000, XP, 2003 and many of their family products excluding Windows NT [7]. When you have finished choosing which Operation System, language version, and the update types, clicks on the Search button. It will then do the search for you and return a list of updates. After you have made your selection from the available list, click on the link to go to Download Basket and give it a depository location either on local hard drive or a shared network drive. When download finishes, it will open Download history and give you a statistic view of success or fail operations. One very amazing feature of Windows Update Catalog is its thoughtfulness in organizing the downloaded files for you. The updates are automatically organized in a subdirectory structure base on Update type, Locale, OS, and component name (e.g., C:\Updates\Software\en\x86WinXp\component name). Along with each component folder, there is a ReadMore IE shortcut that directly takes you to Microsoft *TechNet* web site to view detail description of the update.

There is no client or server software installation required when using Windows Update Catalog and it is very simple to use. Once the files are downloaded to the local hard drive, there are several ways to distribute the patches. Files can be copied to a recordable CD and distribute to other computer with or without network connection. Or, put the files on the network drive and distribute them through network share. Or, if you will, use System Management Server (SMS) to automatically deploy patches to all the computers on the network.

Software Update Services (SUS)

There are many organizations out there that put the job of updating computer to the hands of the users. On the Internet, one can see some company IT help desk web pages that urge users to click on Windows Update link at least once a week. And, download whatever patches Microsoft has suggested for them. It is understandable for a smaller business that usually does not have an IT department to do so. It is quite incomprehensively for medium and large organizations, such as schools or government agencies to just count on the users to do the job that can be critical at time. Software Update Services is a tool Microsoft developed to let company IT administrators take the control back to their hands. And, allow companies to manage and distribute Windows patches with their own Intranet. Instead of having users go out to Internet to reach Microsoft site for updating their computers, a company Web server running SUS can act as a distribution point of the update files. By doing so, there is only one machine needs to go through WAN line to download patch files from the live Microsoft Windows Update site. Moreover, it become possible for the computers on the network but without Internet connection to receive updates. The IT administrator can then make a decision on which patch is needed and which is not according to their computing environment. With Automatic Updates scheduled to run on the client computers at a specific time, patches can be installed without user intervention. SUS not only reduces network traffic, but also

gives an IT department more controls in making sure of each computer in the company is up-to-date with necessary patches. Although SUS only provides critical updates and security roll-ups, it is enough for security purpose.

SUS installation

Similar to Windows Update, SUS also is free. Software Update Services Server 1.0 (*SUSSetup.msi*) is about 47MB, which can be downloaded from http://download.Microsoft.com. SUS needs to reside on Windows 2000 Server with SP2 or higher with *IIS 5.0* and Internet Explorer *5.5* installed. Microsoft takes one step further in helping you secure a web server box by installing *IIS Lockdown Tool* as part of SUS installation[8][9]. During this process, there are two URL need to be aware of. One is the download address, usually http://SUS_ServerName, for the client to download updates. The other is the administrative address, usually http://SUS_ServerName/susadmin, for configuration and administration. The Web based administrative page means SUS can be administered remotely with Internet Explorer from any computer on the network. However, it also means you need to remove anonymous access to the web site to ensure authenticated access and allow only users with local administration privileges on the server to administer the web site. For a greater security purpose, the Admin site can also be configured for Secure Administration through *SSL*.

SUS Configuration and Administration

After the installation, there are some configurations that need to be setup and customized for your organization. Open SUSAdmin page from your browser, you will see the configuration options on the left hand pane. Synchronize Server option provides an easy route to download updates from the Microsoft Windows Update server. Click on Synchronize Now will start the download manually or click on Synchronization Schedule to configure scheduled file download at specific time. All the executable update files are downloaded to your SUS server on a folder named "Content". Once the Synchronization is completed, it is ready for you to approve new updates. Approve Updates option allow SUS administrator to select the necessary update files to distribute to clients. The Set Options option has several choices. "The Proxy server configuration" is to setup *Proxy Server*. "The Server Name Specification" is to specify the SUS server name for the clients to locate this update server. "Select Which Server to Synchronize Content" is to make selection of the synchronization server either directly from Microsoft or from another local SUS. The Set Options also provides the configuration of where to store the updates, either on Microsoft site or on the local SUS. If you choose to host the update at the Microsoft site, only *AUCatalog.cab* that contains the list of the available packages will be downloaded but not the actual package files. When the client connects to your SUS server, it will then go to Microsoft site to download only the approved packages. If you

choose to host the update locally, the initial synchronization will download about 150MB of data.

SUS Loggings

For easy management, there are two XML log files (*history-sync.xml* and *history-approve.xml*) generated which can be viewed from a SUSAdmin page. The Synchronization Log gives the detail of the date, time, and the name of files that were downloaded during synchronization. The Approval Log keeps a record of approved update files and the date, time they were approved. In addition to the two log files; every action of synchronization and approval will also be logged into the *System Log* in Event Viewer as a successful or failing activity.

SUS Monitoring

Update files information is grouped according to OS platforms and IE versions. They can be viewed from Monitor Server option to display a statistic view on how many item of files are available under each group.

Clint Software

Automatic Update software 2.2 or higher on Windows 2000 or Windows XP is required to work with SUS. It can be downloaded from http://www.microsoft.com/windows2000/downloads/recommended/susclient/default.asp. It is now included with Windows 2000 SP3. Automatic Update can be configured in many different ways to receive updates. It can be configured locally to receive automatic or scheduled updates from Microsoft Windows Update site. Or, it can be configured remotely through *Group Policy* or by editing Registry manually to receive updates from an internal SUS server.

Client Software Configuration

In a non-Active Directory environment, you can manually edit Registry by adding additional keys and values at *HKLM\Software\Plicies\Microsft\Windows\WindowsUpdate\AU* and *HKLM\Software\Plicies\Microsft\Windows\WindowsUpdate* location. These Keys and values specify how Windows Update should behave, the time interval for getting the updates, and the name of SUS server that client should contact with [9, p.60]. These Registry keys can be exported and deployed to all the clients on the network through logon script. In an Active Directory environment, you can utilize *Group Policy for the Domain* to apply above registry changes to all computers on the network automatically. Create a new group policy and add *wuau.adm* to the administrative templates for an added ability of setting policies on Windows Update. There are two policies you can configure with, "Configure Automatic Updates" and "Specify intranet Windows Update server location". You need to enable both policies and decide how, when and where clients should receive the updates through these two policies. Once the policy is applied, you

can check the Registry key to confirm the changes. The Windows Update user interface will also be disabled through this action. When every configuration is set and ready, the client will then query the SUS server for new updates in approximately 24 hours interval.

Clients Update Confirmation

There are several clues on both of the client computers and SUS servers for you to check to ensure the updates are actually downloaded and installed. On the client machine, you can check *windowsupdate.log* file under Windows or WinNT directory. Windowsupdate.log file should be updated each time with entries regarding download and installation of package through Windows Updates. You can also check the *Add/Remove Program* and Registry for Hotfix entry. On the SUS server, you can check the IIS logfile from *W3SVC* folder. On the log file you should see the entries regarding clients making request to the server when checking for updates.

Overall, SUS is very easy to implement, especially with Windows 2000 and Windows XP which client software is incorporated in the OS, eliminates the need to deploy it. Also, with Group Policy and Active Directory, it doesn't take too much effort to configure client software to receive updates from local SUS. SUS is scalable that you can have one SUS server or you can have multiple SUS servers on the network. Multiple SUS servers with multiple distribution points in combination with *Network Load Balancing* serves well with large organizations. Microsoft SUS Deployment White Paper provides very detail information on implementing SUS in many kinds of situations [9]. It also included detail instruction on Server backup and disaster recovery. It is a must read document if you are planning to work with SUS. Microsoft's continuing effort in improving SUS is also an encouraging factor to implement SUS. For example, at the time of doing the research last year, there was SUS 1.0. Today, there is SUS 1.0 with SP1 with several enhancements ready for download [12]. The new features include the ability to install on Windows 2000 Domain Controller, better integration with IIS lockdown, the new software catalog files, better administrator controls on scheduling download, and more flexible reboot options after installing a patch that requires restart. SUS 2.0 is currently under development [10]. We can all look forward to its release.

SMS 2.0 Software Update Service Feature Pack

System Management Server has been a long-standing product in system management for Windows based computer [11]. It provides organization a cost effective way to do hardware and software inventory with license tracking. Its ability to remotely deploy software to all computers on the network provides an instant product delivery and saves lots of tech time. To increase SMS's support for software update, Microsoft develops a feature pack called Software Update Services [17]. It actually is a combination of SMS + SUS. SUS 1.0 is not oriented towards an enterprise environment; it lacks a sophisticated management function. SMS + SUS feature pack is an enterprise solution for Windows updates delivery [15]. For companies with existing SMS implementation, the SUS add-

on is an easy-to-incorporate bonus feature. SMS provides SUS a management ability. And, SUS provides SMS a way to identify which patches to download and install promptly.

The feature pack can be downloaded for free from http://www.microsoft.com/smserver/downloads/20/default.asp. The feature pack is free but you need to have SMS 2.0 SP3 or later installed for the feature pack to work. The Feature Pack comes with several tools. *The Security Update Inventory Tool* is used to scan all computers and take an inventory of their security updates, and to obtain the latest catalog of updates. *The Microsoft Inventory Tool for Updates* is used to do the same with Office updates. *The Distribute Software Update Wizard* is a comprehensive tool that evaluates the updates, authorizes the suggested update, downloads authorized updates and distributes the update using SMS software distribution features. *SMS Web Reporting Tool* with Web Reports Add-in for Software Updates generates a web-enabled report that allows software update inventory information to be viewed from the web. With all these tools, SMS + SUS feature pack provides lots of service the SUS alone won't be able to do. For examples, deploy Microsoft Office patches, generate in-depth reports on the status of patch installation for easy problem identify, provides central rollback function in case of problematic patch, and able to work on wider range of OS (Windows 98, NT, 2000, NT 4.0, 2003) [14].

UpdateEXPERT, The Third Party Software

Every one of the free software that comes with Windows OS has a counter part on the software market that is written by other companies to do the same task. UpdateExpert is the counter part for Windows Update Service. It is developed by *St Bernard Software* [13], a company specializing in network security and updating tools. In search of non-Microsoft Windows Update Management software, I came across an UpdateExpert power point presentation done by Chris Gardner from St. Bernard Software Inc. My impression about UpdateExpert was it basically acts like a middleman between you and the Microsoft. UpdateExpert maintains its own database of Service Packs, hotfixes and other patches that come from Microsoft. The company claims it will test the patches for you before releasing it to the database for you to download. It also provides comprehensive information on patch deployment sequence and its prerequisites to ensure successful install. UpdateExpert also comes with a well-organized reporting system that gives a clear view of patches and service pack inventory on each computer [16]. From my assessment, UpdateExpert is a lightweight version of SMS + SUS. It is just another SUS with a reporting tool.

Conclusions

Updating critical and security patches needs to be prompt to prevent attacker from taking advantage of the vulnerability. Therefore, to be able to deliver the updates to all the computers on the network in timely fashion is a challenging task for IT administrators. Automatic Windows Update Service is the solution Microsoft offered to Windows-based environment. Many tools evolving around Windows Update Service are all designed to

make this task much more manageable when comes the time to patch up more than one computers. During the time of testing with SUS in my computer lab, I found it a great difficulty to confirm patch installation. There is no central location to find all pieces of information. To make sure if a fix is installed, one may need to look into log files in IIS server, the scattered log files and registry entry in client computer one at a time. The lack of inventory and management tool in SUS 1.0 probably is the reason Microsoft decided to combine it with SMS. For companies do not use SMS, they will have to live with the deficiency or find other solutions from the third party software. In the future, I would hope to see major changes and improvements in this area in SUS 2.0. No matter what, companies big or small all recognize keeping their computers up-to-date is critical. Not only because it is important in protection their assets, but also because it is very important in keeping their business alive by keeping their systems healthy and well. Therefore, establishing a good automatic Software Update procedure is a must for every proactive windows users and organizations.

References

[1] "Product Support Lifecycle". 15 Oct. 2002. URL: http://support.microsoft.com/default.aspx?scid=fh;[LN];lifecycle

[2] Feinberg, Joshua. "Windows Update keeps Your PC from Spawning Digital Cobwebs". 2002. URL: http://www.agora-business-center.com/0102windowsupdate.htm

[3] "5-Minute Security Advisor-Getting the Most from Windows Update". 2002. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/Columns/Security/5Min/Default.asp

[4] "About Windows Update" 15 Oct. 2002. URL: http://v4.windowsupdate.microsoft.com/en/default.asp

[5] "Windows Update Frequently asked questions". 12 Nov. 2002. URL: http://support.microsoft.com/default.aspx?scid=/support/windows/update/FAQ/default.asp#savedisk

[6] "Microsoft Knowledge Base Article-32316. How to: Download Windows Updates and Drivers from the Windows Update Catalog". 17 Feb. 2003. URL: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B323166

[7] "Microsoft Knowledge Base Article-313191. Windows Update Catalog is Not Available on Windows NT 4.0-Based". 24 Jan. 2003. URL: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B313191

[8] "IIS Lockdown tool". 2003. URL: http://microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/locktool.asp

[9] “Software Update Services Deployment White Paper” 29 Jan. 2003. URL: http://www.microsoft.com/windows2000/windowsupdate/sus/susdeployment.asp

[10] “SMS Feature Pack and Patch Management”. 18 Feb. 2003. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itcommunity/chats/trans/SMS/sms0218.asp

[11] “System Management Server Product Overview”. 29 Jan. 2002. URL: http://www.microsoft.com/smserver/evaluation/overview/default.asp

[12] “Applying Service Pack 1 to Microsoft Software Update Services version 1.0”. Jan. 2003. URL: http://www.microsoft.com/windows2000/docs/SUS_sp1_install.doc

[13] “StBernard Software”. URL: http://www.stbernard.com/

[14] Pawlak, Peter. “Feature Packs Aid SMS Admins”. 18 Nov. 2002. URL: http://www.directionsonmicrosoft.com/sample/DOMIS/update/2002/12dec/1202fpasa.htm

[15] “Enterprise Software Update Management Using System Management Server 2.0 Software Update Service Feature Pack”. 2003. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/sms/deploy/confeat/SMSFPDEP.asp

[16] “UpdateEXPERT”. URL: http://www.stbernard.com/products/updateexpert/products_updateexpert.asp

[17] “Introducing System Management Server Feature Packs”. 15 Nov. 2002. URL: http://www.microsoft.com/smserver/evaluation/overview/featurepacks/default.asp