Global Information Assurance Certification Paper

Microsoft Systems Management Server (SMS) 2.0 Features: Security Policy and Controls Implications Within an Enterprise

Gary A. Wong
November 21, 2000

Introduction

This paper will briefly highlight the major Microsoft's Systems Management Server (SMS) 2.0 product features that can be employed in an enterprise-wide corporate environment. A description of known vulnerabilities will be provided, as well as any security policy, legal, and controls implications stemming from the use of certain features.

Because of the complexity and integrated nature of this product, the scope of this paper will be limited to the perspective that most corporate user management would (or should) have over some of the Microsoft SMS 2.0 features that have been employed, in a predominantly Microsoft front and back-office environment.

Microsoft SMS, a Glorified Insider Hacker Tool?

In mid-1999, a major hacker group known as the Cult of the Dead Cow (cDc) issued a press release accusing Microsoft of hypocrisy over statements Microsoft had made against cDc's Back Orifice 2000 (BO2K) tool. In this announcement, cDc had compared BO2K's remote control stealth feature against Microsoft's Systems Management Server (SMS) Remote Control feature, and found little functional difference-- that both products allowed a remote control session with or without the user at the client being aware of it. [1]

According to CSI, an average insider attack cost the target enterprise some $2.7 million, compared with $57,000 for the average outside attack. [2] Compound Microsoft SMS's additional features (such as software distributing) with the above recent cost figure associated with internal over external attacks, and it would be an understatement to state in an audit or control review report that a robust systems management software such as SMS "is to be properly configured and periodically reviewed after implementation" or other similar response.

Because of its complexity, a Microsoft SMS 2.0 implementation (new installation or an upgrade from SMS 1.2) is likely to be rolled out with minimal configuration with the driving concern of keeping the number of client install errors (and subsequent help desk calls) throughout the company to the minimum. As with most other IS projects, configuring security, considering internal controls, and addressing for any specific department requirements are perceived to require additional administrative overhead and are therefore often neglected-- unless IS Security or Audit is part of the SMS implementation and review team. As such, it would be worthwhile to understand what potential exposures certain Microsoft SMS features may create in a corporate

environment.

Microsoft SMS 2.0 Features

SMS is Microsoft's integrated enterprise management product for delivering configuration and change management in Microsoft's Windows server and workstation platforms, and (to a limited extent) in other environments, such as Novell Netware NDS. From a brief technical perspective, Microsoft SMS converts certain events to Simple Network Management Protocol (SNMP) traps and reports them in an SNMP management console and/or trap listener, which logs them in a central database.

Some of the major features included in the product that can be implemented are the following: [3]

- Common Information Model (CIM)-Based Hardware Inventory Feature: SMS is able to collect and filter inventory information from various data sources including SNMP, DMI, and Win32 application programming interface.
- Discovery-Based Software Inventory Feature: SMS searches for version resource information on every executable file on the client machine rather than relying on a pre-set list.
- Software Metering Feature: SMS allows administrators to analyze, monitor, control, and report on the use of applications by user, group, workstation, time, or license quota. SMS can remove non-licensed software on workstations.
- Electronic Software Distribution Feature: SMS allows rules-based and scheduled-based distribution and installation of software from a centralized location. Software with administrator rights can be installed unattended even if a low-rights user is logged on.
- Network Tracing and Network Monitoring (NetMon) Features: SMS builds a map of network servers and devices, and identifies network problems such as unwanted protocols, duplicate IP addresses, and attempted Internet break-ins by monitoring network traffic.
- Remote Diagnostics Feature: SMS provides administrators the ability to remotely run applications, "chat" with end users, reboot, and control the keyboard and mouse.

From one integrator's perspective, Microsoft SMS rivals other network management products such as HP's Ovenview, IBM's Tivoli, and Computer Associates' Unicenter TNG, but that Microsoft SMS is also "the best bet for clients who want to control their desktop and server platforms as opposed to specific pieces of hardware." [4]

Known Vulnerabilities

Since the beginning of this year, two vulnerabilities have been reported by security firms relating to SMS 2.0. Microsoft has acknowledged both vulnerabilities by issuing subsequent security bulletins (MS00-012) and (MS00-083), and has provided a patch available for download.

The first is a "privilege elevation" vulnerability that affects companies that have employed the Remote Control feature on its machines. At the time of installation, the folder on which this particular program resides has its permissions set to the Everyone Full Control by default. While not necessarily a vulnerability within the Remote Agent itself, a malicious user who can interactively log onto the affected machine (and install malicious code) can gain complete control over the local machine.

The SecuriTeam website describes this vulnerability by illustrating the exploit: [5]

- Rename %SMS_LOCAL_DIR%\MS\SMS\CLICOMP\REMCTRL\WUSER32.EXE to *.OLD
- Copy %SystemRoot%\System32\musrmgr.exe to %SMS_LOCAL_DIR%\MS\SMS\CLICOMP\REMCTRL\WUSER32.EXE
- Reboot. After you reboot the PC, user manager will run. At this point, the non-admin user can grant administrator privileges to whomever he or she wants.

In some cases where network security configuration is weak, his or her control may be extended to the domain server. [6]

The second is a "buffer overrun" vulnerability that affects certain protocol parsers accompanying Network Monitor (Netmon), an administrator tool included in SMS 1.2 and 2.0. By exploiting these parsers that do not have a front-end to validate data received before interpreting it, a malicious user can send some specially-crafted malformed data that could either shut down Netmon from being able to capture and analyze data, or cause transmitted code to run on the machine. The US Department of Energy's Computer Incident Advisory Capability (CIAC) assessed this risk as high because the vulnerability "allows remote administrative access without prior privileges". [7]

In both vulnerabilities discussed, security configuration and "defense-in-depth" best practices (e.g., such as requiring an administrator to use Netmon in the local, rather than domain, administrative context) would help in limiting the exposures identified.

Security Policy Implications

It goes without saying that senior management support is essential for the successful development, design, implementation, and monitoring of security controls. Michele Crabb-Guel's on-line presentation at the SANS website offers an overview of the key elements and basic requirements of an information protection policy, stressing that policies "must be updated regularly to reflect the evolution of the organization". [8]

Existing security policies may need to be re-evaluated to ensure that certain controls are tightened or "loosened" to complement SMS 2.0. For instance, SMS 2.0 allows separate log files of each SMS-implemented feature, such as software distribution and remote control. Troubleshooting security issues (Windows NT File System Security on SMS) would be enhanced by a company's NT security policy that requires some auditing to be enabled and allows the use of Windows NT Event Viewer.

Another instance would be specific password and account policies that are meant to be applied enterprise-wide across all platforms. In the way that SMS was designed to operate, Microsoft has recommended that SMS accounts never be expired or that "Password never expires" option is never turned off on these accounts. [9]

In addition to reviewing current security policies, an SMS security policy should be developed that would address the particular issues that SMS introduces, and are specifically identified, in the SMS 2.0 Administrator's Guide, SMS 2.0 Resource Guide, and related publications from Microsoft.

One such policy issue is how non-standard or unlicensed software identified in the SMS Software Inventory Feature and Software Metering Feature are to be handled and communicated. If corporate policy allows for some departments or certain users to load their own purchased or licensed software on company workstations, blocking or removing such software can effectively be an "internal denial of service" attack.

Legal Implications

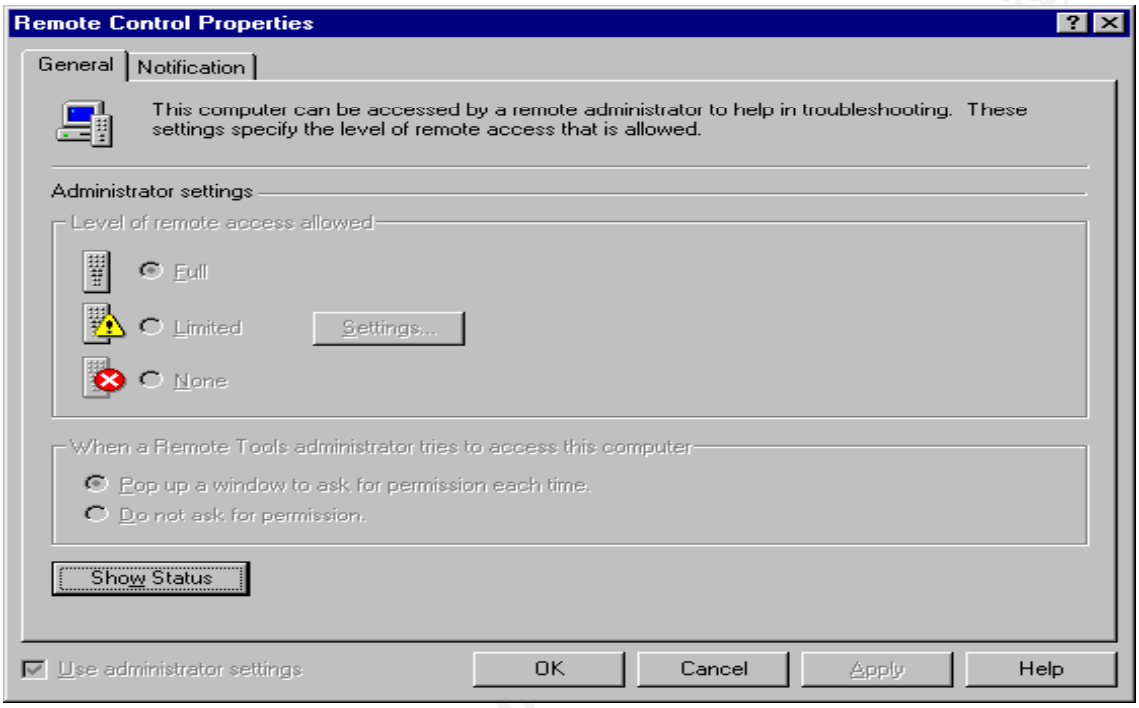
Some companies may take the position that SMS offers an additional benefit other than systems, asset, and technical support management-- to monitor employee activity. Without diving into the security framework of SMS provided by Microsoft, the fact that SMS 2.0 features are enterprise-wide should have prompted some consultation with the company's Human Resource and Legal department over whether corporate policies relating to employee privacy and employer rights need to be clarified or updated.

Companies do have the right to manage and control all company assets to reduce liability. This right effectively includes the access and review of all data and records (e.g., e-mail messages, Internet logs, archived files, personal files, and operating system logs) on computers and related peripherals, of users of company computing systems, whether the policy is explicitly or implicitly stated. With the increasing need to allow remote access to company networks-- including telecommuting and VPN access-- the employment of SMS throughout the company can help visually deter internal threats.

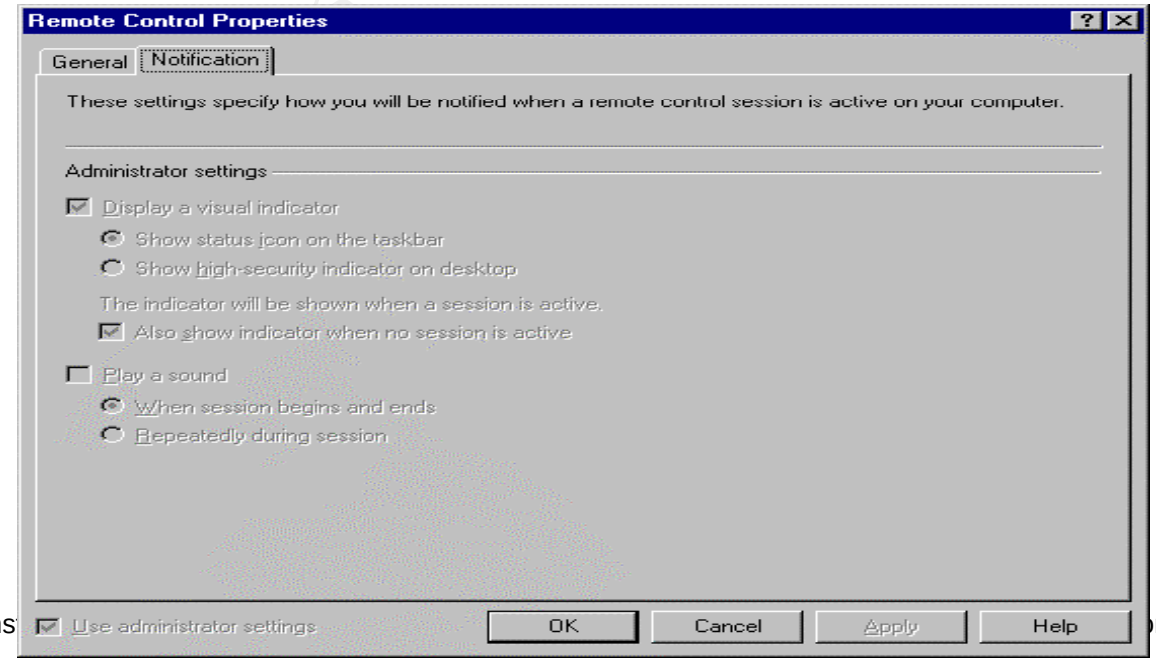
However, legal and privacy issues can arise in enterprises that allow the use of an employee's own personal computer to remotely access the company network, particularly if SMS required to be installed in order to connect. SMS should be

configured to detect such access.

Legal and forensic issues can also arise if SMS is not configured with security in mind.
In the case of the SMS Remote Diagnostics feature, displayed are the following Remote Control properties options in the Control Panel.



At least a few departments within any enterprise public or private (such as Payroll, Executive, and Legal department) should have some confidentiality concerns that would require this feature to be locked down from abuse. SMS can prompt the target user for permission to access or can provide visual or audio indicators indicating that Remote Control is (or is not) in use.



Controls Implications

Microsoft provides the following checklist to ensure that security issues related to SMS 2.0 are considered in the planning, implementing, and periodic review of SMS features: [9]

1) Review overall computer security, including sources of risk, physical security, your organization's security policies and procedures, and your network security. This is to help understand the internal controls environment, and to understand the issues that SMS security must address.
2) Review your implementation of security for technologies that SMS uses, including Microsoft SQL Server, Windows NT (including domains), and other technologies related to the SMS environment. This is to allow any adjustment in the security of specific technologies when it could benefit SMS security.
3) Review your use of SMS connection, service, and special purpose accounts, where SMS does not automatically manage them. This is to minimize opportunities for future problems, and take advantage of SMS's modular security model.
4) Review who has access to your site servers at the Windows Management Instrumentation (WMI) level and distributed Component Object Model (DCOM) level (by using the SMS Admins group or similar accounts or groups), to ensure that only authorized individuals have appropriate levels of access to the SMS systems.
5) Review who has access to SMS objects, by using SMS class and instance security rights, as administered in the SMS Administrator console.
6) Review access to software distribution shares, to ensure that users have access only to the software that they are authorized to access.
7) Review Remote Tools security, to ensure that only authorized staff can remotely control appropriate client computers.
8) Review the security issues of your reporting solutions, to restrict access to sensitive system details.
9) Review security issues related to your SMS Installer scripts. Review the scripts and their availability, to ensure that there is no opportunity to expose security details that you do not want to expose.
10) Review Network Monitor (Netmon) security. Assess the risk that unauthorized Netmon use might pose, to ensure that it is not abused.
11) Review your SMS security policies and procedures documentation, to ensure that your documentation is up-to-date and complete.
12) Review the SMS 2.0 Security Essentials document fully and watch for alerts about security issues at the Microsoft Web site or on SMS community mailing lists and newsgroups. Look for weaknesses in your SMS security model, to minimize the possibility that security holes remain in your security model, or that new ones will develop as technologies evolve.

Professional associations such as the Information Systems Audit and Control

Association (ISACA) and the Institute of Internal Auditors (IIA) also offer controls guidance over the review of existing and emerging technology, from an enterprise-wide perspective. Internet resources are also available to assist in a review (e.g., SMS-dedicated websites like Swynk http://www.swynk.com/sysapps/sms.asp).

Internet References

[1] The Cult of the Dead Cow. "Don't Worry Window Users, Everything Will BO2K". Release, July 19, 1999. URL: http://www.cultdeadcow.com/news/pr19990719.html. (Nov. 20, 2000)

[2] Shaw, Eric; Post, Jerrold; and Ruby, Kevin. "Managing the Threat from Within". Information Security Magazine. July 2000. URL: http://www.infosecuritymag.com. (Nov. 20, 2000)

[3] Microsoft Corporation. "Microsoft Systems Management Server 2.0: The most scalable way to reduce the cost of change and configuration management for Windows-based desktop and server systems". September 10, 1999. URL: http://www.microsoft.com/smsmgmt/exec/sms20datasheet.asp (Nov. 20, 2000)

[4] Cirillo, Rich. "Managing Networks, Managing Relationships -- Four network management companies tell us what makes their relationships with SMS vendors tick". VAR Business, Issue: 1621. October 16, 2000. URL: http://www.techweb.com/se/directlink.cgi?VAR20001016S0026 (Nov. 20, 2000)

[5] Monroe, Frank. "Default security permissions of SMS 2.0 Remote Control opens a security hole". Securiteam. March 1, 2000. URL: http://www.securiteam.com/windowsntfocus/Default_security_permissions_of_SMS_2_0_Remote_Control_opens_a_security_hole.html (Nov. 20, 2000)

[6] Microsoft Corporation. "Patch Available for 'Remote Agent Permissions' Vulnerability". Microsoft Security Bulletin February 22, 2000. URL: http://www.microsoft.com/technet/security/bulletin/ms00-012.asp (Nov. 20, 2000)

[7] U.S. Dept of Energy. "L-016: Microsoft Netmon Protocol Parsing". Computer Incident Advisory Capability (CIAC) Information Bulletin. November 2, 2000. URL: http://www.ciac.org/ciac/bulletins/l-016.shtml (Nov. 20, 2000)

[8] Crabb-Guel, Michele. "Section Three: Policies and Procedures". Building an Effective Security Infrastructure. SANS Presentation 1999. URL: http://www.sans.org/newlook/resources/policies/bssi3/index.htm (Nov. 20, 2000)

[9] Microsoft Corporation. "SMS 2.0 Security Essentials" Technology Paper. March

22, 2000. URL: http://www.microsoft.com/smsmgmt/techdetails/secessentials.asp (Nov. 20, 2000)

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS