CHAPTER 17

THE FUTURE OF WINDOWS SECURITY

This chapter will take a look ahead at some new security-related technologies that will shape the Windows platform. Specifically, we will examine these technologies across soon-to-ship add-on features of Windows Server 2003 and also the next wave of Windows operating systems, code named Longhorn.

TOOLS AND ADD-INS

The following security-related tools are either currently available or will be soon from the Windows server 2003 Downloads site. (See "References and Further Reading" at the end of this chapter.)

NAT Traversal (NAT-T)

Remember the bad old days when IPSec wouldn't work through a Network Address Translator (NAT) device or firewall? Well, the Internet Draft standard "UDP Encapsulation of IPsec Packets," also known as NAT Traversal (NAT-T), provides a solution to this conundrum, and Microsoft has implemented it in an update to Windows 2000 and XP as described in KB Article 818043. Simply install the update described in this article and you will be able to traverse NATs via the following protocols (the NAT must be configured to permit these):

- **Layer Two Tunneling Protocol (L2TP)** User Datagram Protocol (UDP) 500, UDP 1701
- **NAT-T** UDP 4500
- **Encapsulating Security Payload (ESP)** Internet Protocol (IP) protocol 50

Now two great security technologies can be enjoyed simultaneously.

NOTE Windows Server 2003 supports this functionality natively.

Group Policy Management Console (GPMC)

We've talked a lot in this book about the power of Group Policy to manage Windows 2000 and later Active Directory infrastructures. However, since it was first introduced in Windows 2000, Group Policy has suffered a bit from lack of unified, cohesive management and automation interfaces. Microsoft has sought to redress this with GPMC, which consists of a new MMC snap-in and a set of programmable interfaces for managing Group Policy. GPMC is shown in Figure 17-1 examining the details of the Default Domain GPO.

GPMC is a welcome addition, and anyone who uses Group Policy in her daily work will love this tool. It unifies editing, reporting, modeling, Resultant Set of Policy (RSoP), enforcement, and even GPO backup into one interface.

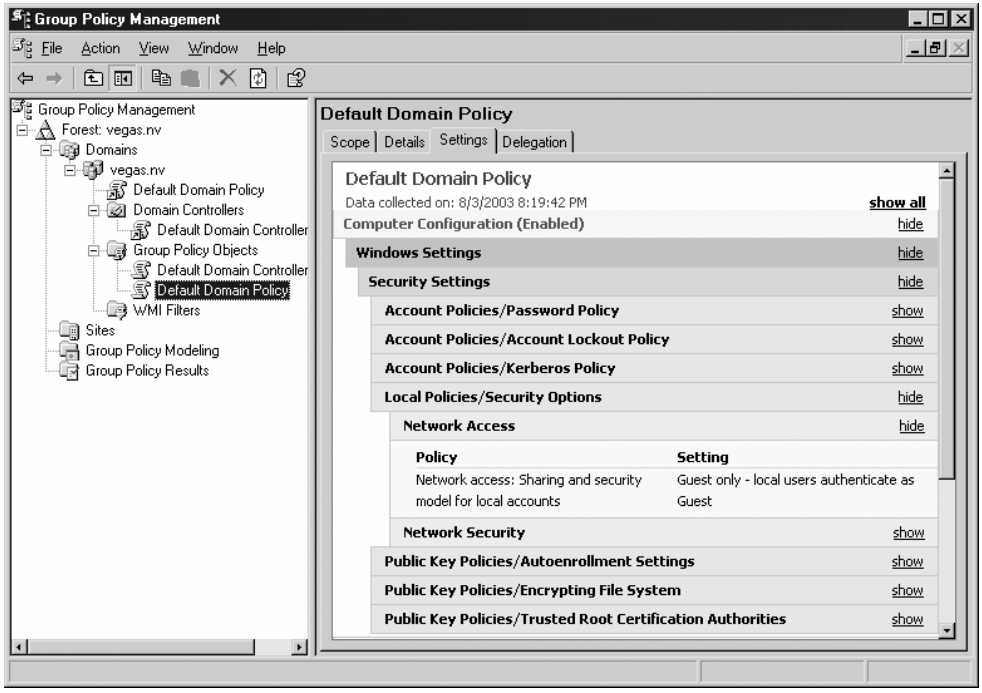

Figure 17-1. The Group Policy Management Console, a Windows Server 2003 add-on

TIP You don't have to run Windows Server 2003 to enjoy the benefits of GPMC—it can be run on Windows XP Service Pack 1 systems with the .NET Framework installed.

Identity Integration Feature Pack

This add-on to Windows Server 2003 Enterprise Edition is also available from the Windows Server 2003 Downloads site. The feature pack is a limited version of the full-blown Microsoft Identity Integration Server 2003 (MIIS), which is designed to synchronize identity information across a wide variety of repositories (including directory services, network operating systems, e-mail systems, applications, databases, and even file-based systems). MIIS was formerly called Microsoft Metadirectory Services (MMS), and MIIS marks the third major release of the product. MIIS also centrally provisions and revokes account and identity information across stores, and it enables self-service and help-desk initiated password management and reset from a web browser.

The feature pack synchronizes identity information only between multiple Active Directory forests or between Active Directory and Active Directory Application Mode (ADAM). It also can provision user accounts across forests.

NOTE MIIS and the Identity Integration Feature Pack require the Enterprise Edition of Windows Server 2003 and also SQL Server 2000, Enterprise, or Standard Edition SP3.

MIIS and the feature pack are most useful to organizations that have separately managed identity repositories. For example, consider a large corporation that has both internal and external IT divisions. For security and structural reasons, the external Active Directory infrastructure is maintained separately from the internal, although many of the accounts belong to the same people (being employed by the same larger company). Thus, some way must exist to synchronize the external and internal account data without creating a trust or otherwise integrating the two directories in a way that violates security. MIIS is perfect for this scenario—it harmonizes accounts, allows the company to keep a "single source" of identity (an important concept in the ISO17799 security policy standard—see Chapter 1), ensures that revoked accounts cascade throughout both directories, and, last but not least, allows self-help password management between the two infrastructures, greatly saving on help desk costs and providing a consistent mechanism for password management across all users. We recommend you try out the feature pack and consider moving to the full-blown version if you are a large organization that has separately managed identity repositories.

Active Directory in Application Mode

We think of ADAM as "Active Directory Lite." It is a stand-alone product that runs as a nonoperating system service (it runs as the Network Service account) that provides all of the features of an LDAP-based directory, but it does not require such tight integration with Windows. It also offers a more easily customized schema than full-blown AD. Essentially, it is a simple directory service targeted at applications that need only limited features (without the complexity, operational overhead, and relative inflexibility of full-blown AD).

ADAM is perfect for online service providers who want to manage customers using a directory service but blanch at the thought of a full AD deployment. It also has the advantage of being able to host user objects that are not Windows security principals, but that can be authenticated using LDAP simple binds. Thus, any application that can talk LDAP can use ADAM as the user store.

Of course, some disadvantages should be mentioned. ADAM does not support features such as Group Policy, which is one of the key benefits of full-blown AD. Also, the administration tools are not as robust as full-blown AD—most are command line tools, and the only graphical tools are essentially the LDAP client ldp (see Chapter 4) and a low-level Active Directory Services Interface (ADSI) editing tool (ADAM ADSI Edit, which is shown in Figure 17-2).

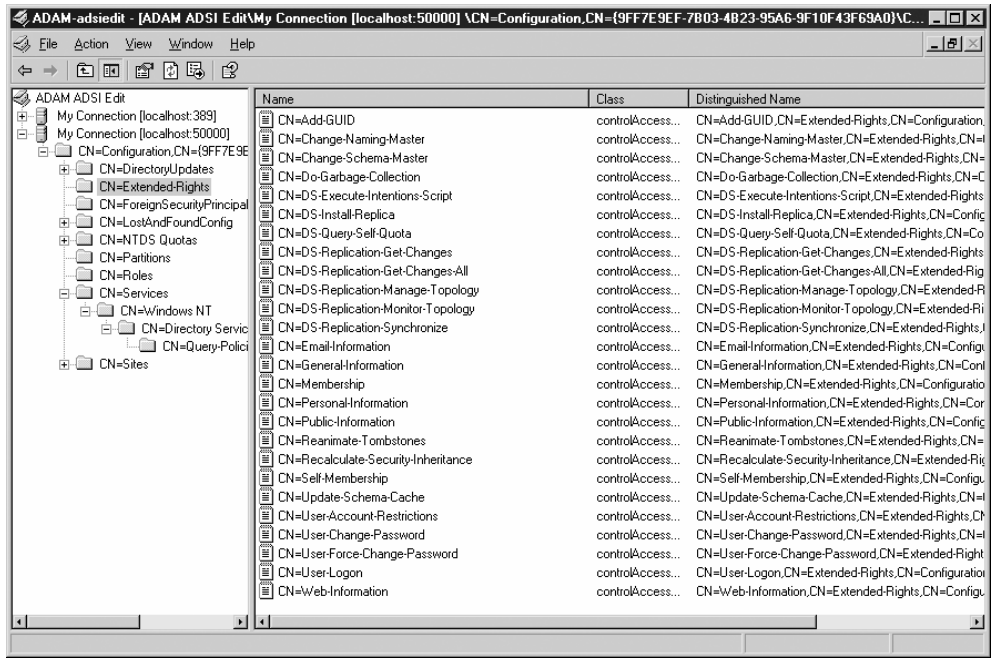

Figure 17-2. ADAM ADSI Edit; note the two connections, one to the full-blown AD instance on 389 and the other to TCP 50,000, ADAM's default port (50,001 is SSL-ized)

We'll admit firsthand that we haven't used or seen ADAM used in production, but we like the idea of a dedicated LDAP directory product. Microsoft's biggest problem with ADAM may ultimately be convincing customers why they have to implement full-blown AD at all.

Microsoft Operations Manager (MOM)

Our experiences in managing large Windows deployments has taught us that above all, information is king—if you don't know what's going on out there in the data center, you might as well forget about security. The reason for our discussion of MOM in this chapter on the future of Windows security is this: although MOM is available today, we believe that it will provide the framework in the near future for all monitoring of Microsoft server environments, so it behooves us at least to give an overview of how it can support security.

We'll let readers follow the links in "References and Further Reading" to download the "marketecture"; we'll focus here on the security benefits of MOM. The primary benefit it provides is a secured, centralized database of events from across the environment. This is done primarily through MOM's security log aggregation feature, which sends

collected events to a secured, central computer. This aggregation integrates many potential data sources, including Simple Network Management Protocol (SNMP) and UNIX syslog. For those of you who have struggled to manage Event Logs across thousands of servers, here's your solution. MOM can also monitor security settings for systems grouped into organizational units (OUs) (such as all IIS servers).

Of course, monitoring and collecting events is not enough; we know plenty of organizations that keep reams of log data that no one ever reviews or takes action on. You must also keep alert on critical events and proactively enforce selected policies that should never be violated. MOM can also respond to security events with scripts to alert administrators and/or enforce security policy proactively across the environment. For example, MOM can send a notification to a specified administrative account, disable an account showing aberrant behavior, or shut down a potentially compromised computer (also selectively enforceable by OU).

Last but not least, MOM has a reporting and trend analysis component that will keep those management types happily pouring over graphs and pie charts until their eyes water. After all, you have to justify that security budget somehow, right?

Of course, MOM installs an agent that must run as Administrator, but most of us are used to that from Microsoft. (When are they ever going to develop a global read-only account?) MOM 2004, scheduled for release in the first half of 2004, and the new Extended Management Packs (XMP) that extend MOM to manage AD, .NET Framework, Exchange, Biztalk, ISA Server, and SQL Server (just to name a few) that are available now, are something any smart security administrator should look into.

Microsoft Audit Collection System (MACS)

MACS is a client-server application that collects security events real-time and stores them in a remote SQL Server database. It also supports sending filtered streams of events to intrusion detection applications in real time. Rather than examining the Event Logs on each individual machine, MACS provides a centralized repository for log information in a format (SQL) that is easily analyzed. As we've noted, MOM provides similar functionality, and MACS may be integrated into MOM in the future. Look for a stand-alone MACS release sometime after Windows Server 2003 launches.

Systems Management Server (SMS)

MOM is for monitoring, alerting, and proactive enforcement, but it's not designed to deploy bits. That's what SMS is for. As you might imagine, this makes SMS the go-to product for deploying security patches, one of the most critical processes in a Microsoft environment.

Microsoft's patch management history has been checkered, and it is still fragmented as of this writing. SMS is the preferred method of patch deployment for large environments, offering automated inventory, distribution, and reporting via the Software Update Services (SUS) Feature Pack. For smaller businesses or those unwilling to undertake the expense and overhead of SMS, Microsoft offers a stand-alone version of SUS that has more limited features and is focused primarily on Windows 2000 and XP. The Microsoft

Baseline Security Analyzer (MBSA, see Chapter 16) can also be used manually to inventory out-of-date patches across the NT family, IIS, SQL, and IE.

Going forward, it seems clear that the most robust patch management solution will remain SMS for the near term, with the possibility of migrating into the core OS sometime in the future, depending on how loudly Microsoft's customers continue to complain about this painful topic.

NOTE Many good third-party patch management systems are available as well; our favorite is Shavlik's HFNetChk Pro.

System Center

On March 18, 2003, Microsoft announced a new strategic initiative that would unite MOM and SMS into a single suite called the System Center Suite, which would evolve over time into a single integrated product called System Center (code named Sydney). System Center is based on Microsoft's System Definition Model (SDM) for managing objects ranging from desktops, laptops, personal digital assistants, applications, and servers. SDM is a core feature of Microsoft's Dynamic System Initiative (DSI), which aims to bake management into applications and systems rather than bolt it on later via agents (as SMS and MOM do). Although it's too early to tell whether DSI will get traction, and the assimilation of heterogeneous platforms remains a big question, today Microsoft is clearly banking a lot on SMS and MOM as the future of Windows operational management.

LONGHORN

Any book on Windows security would be incomplete without an examination of the new security features being planned for the next version of the OS. As of this writing, only the barest of speculation is available concerning the next wave of Windows OSs, code-named Longhorn and tentatively schedule to start releasing in 2005, so complete analysis of these features is premature. (A prerelease version was leaked onto the Internet in May 2003 that generated mostly discussion of the UI and file system features.) However, we will conduct a brief survey and render our initial impressions here.

Vision

The tagline for Windows Server 2003 was "Do more with less," in keeping with that product's launch during the tail of the technology industry slowdown that began in 2001. For Longhorn, Microsoft seems to be returning to its roots in mass-marketing of computing based on ease-of-use, focusing on greater simplicity in

- Deployment and operations
- Providing a platform for distributed applications
- Information sharing

As we noted in Chapter 1, one of our favorite security principles is simplicity, since complex systems are invariably more difficult to secure. We hope that this focus on simplicity also bodes well for the security of Longhorn, but we won't hold our breath in light of Microsoft's history of packing new features into major Windows releases. Alas, we're not here to discuss the entire feature set of Longhorn, only those relevant to security. Off we go….

Longhorn Security Features

A dearth of information about Longhorn security is available, not surprising for the early planning phases of the product. Here are some of the areas we think will play a major role in the new OS.

Web Services Security

A Web service is a self-contained software component that performs specific functions and publishes information about its capabilities to other components over a network. Web services are based on a set of much-hyped Internet standards-in-development, including the Web Services Definition Language (WSDL), an XML format for describing the connection points exported by a service; the Universal Description, Discovery, and Integration (UDDI) specification, a set of XML protocols and an infrastructure for the description and discovery of Web services; and the Simple Object Access Protocol (SOAP), an XML-based protocol for messaging and remote procedure call (RPC)-style communication between Web services. Leveraging these three technologies, Web services can be mixed and matched to create innovative applications, processes, and value chains.

In Chapter 10, we talked about some attacks against Web services components available in the Microsoft platform. Although no high-profile vulnerabilities have been published in this evolving technology, clearly such technologies as SOAP, WSDL, and UDDI will present new interfaces for application hacking that must be locked down. To this end, in April 2002 Microsoft, IBM, and VeriSign announced the publication of a new Web services security specification called the Web Services Security Language, or WS-Security. (See links to the specification in the "References and Further Reading" section at the end of this chapter.) WS-Security subsumes and expands upon the ideas expressed in similar specifications previously proposed by IBM and Microsoft (namely SOAP- Security, WS-Security, and WS-License).

In essence, WS-Security defines a set of extensions to SOAP that can be used to implement authentication, integrity, and confidentiality in Web services communications. More specifically, WS-Security describes a standard format for embedding digital signatures, encrypted data, and security tokens (including binary elements such as X.509 certificates and Kerberos tickets) within SOAP messages. As more of the operating system becomes "webified," the greater the need for a standard security paradigm like WS-Security, and Longhorn will likely lead the way in integrating that standard into the core of the OS.

NOTE See *Hacking Exposed: Web Applications* (Osborne/McGraw-Hill) for more information about Web services security.

TrustBridge

Currently, the most visible mechanism for leveraging WS-Security is TrustBridge, the code name for a set of technologies that enable applications to authenticate credentials created on a wide range of systems, including Active Directory, Passport, and other products. Originally announced in June 2002 as a Kerberos-based technology, TrustBridge has subsequently been refocused to leverage WS-Security as the lingua franca of authentication.

One of the key motivators behind TrustBridge is the concept of *federation*, which could allow WS-Security compatible businesses to form arms-length relationships more easily via a common authentication infrastructure. For example, a company that used Active Directory as its primary identity store could authenticate users from another organization that used a different technology, with TrustBridge mediating the authentication using a common language such as WS-Security or Kerberos. TrustBridge has been slated to ship with Longhorn.

NOTE Microsoft Identity Integration Server (MIIS, discussed earlier in this chapter) is potentially a halfway step to TrustBridge.

IPv6

IPv6 support was included in Windows Server 2003 and is available for Windows XP SP1 and later through the Advanced Networking Pack for Windows XP (see KB Article 817778). Of course, IP version 6 is interesting in its own right as the next generation Internet Protocol, but us security wonks get most excited over the interesting new security functionality built into the protocol, specifically IPSec.

Unfortunately, the IPv6 IPSec features in Windows Server 2003 are quite crude. For example, the Encapsulating Security Payload (ESP) is supported, but data encryption is not. Windows Server2003 IPv6 IPSec also does not support the use of Internet Key Exchange (IKE) to negotiate security associations (SAs); all parameters must be manually configured using the `netsh` command. Finally, IPv6 IPSec security policies are not managed with the IP Security Policies snap-in; they must instead be manually configured with the ipsec6.exe tool. We expect these shortcomings will be addressed in Longhorn or sooner.

Despite these shortcomings, we have reason to be optimistic. The Windows XP IPv6 implementation includes an IPv6 Internet Connection Firewall (ICF), carrying forward a great security feature first introduced in Windows XP and Server 2003. The IPv6 ICF can be configured using the `netsh firewall` command.

Teredo

Teredo is an IPv6/IPv4 transition technology that provides tunneling of unicast IPv6 connectivity through IPv4 networks and through IPV4 Network Address Translators (NATs). To traverse IPv4 NATs, IPv6 packets are sent as IPv4-based User Datagram Protocol (UDP) messages.

Why choose UDP? IPv4-encapsulated IPv6 packets are sent with the Protocol field in the IPv4 header set to 41. Most NATs translate only TCP or UDP traffic and do not have the capacity to translate protocol 41, breaking IPv6 communications. By encapsulating IPv6 as an IPv4 UDP message containing both IPv4 and UDP headers, UDP messages can be translated by most NATs and can even traverse multiple layers of NATs.

It is important to note that Teredo is designed as a last resort transition technology for IPv6 connectivity. Microsoft supports other IPv6 transition technologies, including native IPv6, 6to4 relay routers, or Intrasite Automatic Tunnel Addressing Protocol (ISATAP), and these are preferable to Teredo if available.

SUMMARY

Microsoft's Trustworthy Computing initiative has clearly focused new attention on the importance of security in the company's products. The slew of add-on feature packs and products slated for release just following the release of Windows Server 2003 shows some strategic thinking around the major themes of identity management, improved Active Directory policy management, centralized operations orchestration, and further work on network security features such as IPSec and ICF that started in Windows XP and Server 2003. Although Longhorn security features are not clear today, it appears likely that Microsoft will continue to focus on these themes in its next-generation operating system.

REFERENCES AND FURTHER READING

Reference	Link
General References	
L2TP/IPSec NAT-T Update for Windows XP and Windows 2000	http://support.microsoft.com/?kbid=818043
"UDP Encapsulation of IPsec Packets" (NAT-T) Draft 06 (Draft 02 is supported by Windows)	http://www.ietf.org/internet-drafts/draft-ietf-ipsec-udp-encaps-06.txt
Windows Overview & History	http://www.microsoft.com/windows/WinHistoryIntro.mspx

Reference	Link
Windows Server 2003 Downloads (includes Tools and Ad-ins)	http://www.microsoft.com/windowsserver2003/downloads/default.mspx
Active Directory in Application Mode (ADAM)	http://www.microsoft.com/windowsserver2003/adam/default.mspx
"Security Overview for Microsoft Infrastructures" by Microsoft Security Solutions	http://www.microsoft.com/uk/security/downloads/ Security_Overview.ppt
Microsoft Operations Framework (MOF)	http://www.microsoft.com/mof
Microsoft Operations Manager	http://www.microsoft.com/mom/
Patch Management Using Microsoft Systems Management Server - Operations Guide	http://www.microsoft.com/technet/itsolutions/msm/swdist/pmsms/pmsmsog.asp
Securing IT with Systems Management Server (SMS)	http://www.microsoft.com/smserver/evaluation/overview/secure.asp
Microsoft Guide to Security Patch Management	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/patch/secpatch/Default.asp
Shavlik Technologies LLC, makers of HfNetChkPro for patch management	http://www.shavlik.com
"Microsoft Windows Longhorn"	http://reviews.cnet.com/4505-5_7-21008729.html?legacy=cnet
WS-Security	http://msdn.microsoft.com/ws-security/
Web Services Security Specs and TrustBridge	http://msdn.microsoft.com/msdnmag/issues/02/10/resourcefile/default.aspx
Microsoft Identity Integration Server 2003	http://www.microsoft.com/miis
Microsoft Windows XP web page	http://www.microsoft.com/windowsxp/