The Microsoft Trustworthy Computing Initiative and Exchange 2003: Vision or Vapor?

Alexa Bielefeld

January 11, 2004
GSEC Practical
Version 1.4b -Option 1

Abstract

Microsoft Exchange 2003, along with Microsoft Server 2003, were both released under the Microsoft Trustworthy Computing Initiative. The acronym SD3+C: secure by design, secure by default, and secure by deployment, plus communications has been coined by Craig Mundie, Microsoft's chief technology officer for advanced strategy and policy to encompass all aspects of this new Microsoft security framework. [1]

The purpose of this paper is to examine the security advancements and advantages that an implementation of Microsoft's Exchange Server 2003 can bring to your Messaging environment and whether the intent of the Trustworthy Computing Initiatives have made a difference in moving forward toward better security for this extremely critical element of all public and private infrastructures.

Introduction

In August 0f 2003 there were more than a million computers hit by the MSBlast worm. [2] One of these million was our site's Exchange 5.5 server. When it hit my server, the Blaster worm was not yet news; it was sheer luck that Microsoft engineers were at our headquarters location on another issue, and recognized what was occurring. Even with their presence, it took over 6 hours to identify and resolve the problem. Despite the security warning that had gone out several weeks prior to Blaster appearing in the wild, for our corporation and its 70 sites and 100+ corporate and remote Exchange servers, it took a server getting hit to mobilize resources and effectively patch all servers, thereby successfully avoiding any additional Blaster issues.

This example serves to illustrate the critical nature of what this paper addresses. Our entire organization is currently running Microsoft Exchange 5.5 servers, as are an extremely large number of organizations today. Exchange 5.5 was released in 1998 and is now two releases out of date. Operating system weaknesses, RPC vulnerabilities, viruses, Outlook Web Access vulnerabilities, SPAM, and client side (Outlook and Outlook Express) issues, are causing patches to be issued and mandated with increasing frequency by Microsoft. With the release of Windows Server 2003 and Exchange 2003, it is long past time for a better and more secure operating platform and messaging system.

Microsoft has announced that primary support will end for Exchange 5.5 on December 31st of 2003. And while Microsoft has said that it will waive fees for the first year of extended 5.5 support, the product clearly is well past its prime.[3] So while Windows 2000 SP3 will support Exchange 5.5, Exchange 2000, and Exchange 2003(with critical limitations), the Windows 2003 Operating system will only support Exchange 2003. It is clearly time to start thinking about an upgrade - if customers plan to stay on a Microsoft based platform - and want to do so with more security in place. The question then becomes; have the tenets of the Microsoft Trustworthy Computing Initiatives resulted in the release of a better, more secure, and more trustworthy Exchange Messaging environment that organizations can rely on to meet their complete messaging needs and provide for their future ones? Or is this just another example of Microsoft vaporware combined with a public relations facade to camouflage an ever-present and growing security quagmire?

This paper will first address the Trustworthy Computing Initiative: its purpose, its functionality, and its feasibility. It will then look at what the Initiative has done for the security and usability of Microsoft Exchange 2003. It will also briefly look at what the Initiative has brought to those applications integral to the security and feature set of Microsoft Exchange 2003: Microsoft Server 2003, Microsoft Outlook, Internet Information Server 6.0, and 2003 Outlook Web Access.

Trustworthy Computing Initiative

In January of 2002, the idea of trustworthy computing was launched by Bill Gates in an internal memo to employees. In a reversal of all previous Microsoft strategies, he placed the concept of security for applications above the new features that the application could provide to users. He stated that Microsoft products should "emphasize security right out of the box", and should be continually monitored and upgraded as additional threats appeared to challenge the security of the product. This new philosophy was going to govern how Microsoft functioned in all aspects of it future products; from development, to support, to operational efforts, and to the corporate side of Microsoft operations. [4]

The release of Microsoft Exchange 2003 occurred under the auspices of Trustworthy computing. Because Microsoft has utilized the acronym SD3+C (secure by design, secure by default, secure by deployment, plus communication), to define Trustworthy computing, these are the areas that will be examined to determine if a more secure product has actually been released by Microsoft with Microsoft Exchange Server 2003.

Secure by design

The concept of secure by design is meant not to allow senior VP's to be actually telling the truth when they say "We really haven't done everything we could to protect our customers. Our products just aren't engineered for security." (Orion) This admission was made by Brian Valentine at a .NET developer's conference in September of 2002. How does a company make such a statement and still be around to conduct operations? The statement and the message it delivered would be anathema to the 'secure by design' premise. The goal of secure by design is to take all possible steps to ensure that products are released with the least possible number of security flaws and vulnerabilities.

If Microsoft was aggressively following its stated mandate, and actively pursuing a secure by design philosophy, security would have to be a prime factor in all phases of the lifecycle of Exchange 2003. Secure by design would mean that the idea and the specifications for a product would be created in a secure fashion, code would be written securely, code reviews, testing, and walkthroughs would be continually conducted, mandatory security training would be given to employees involved in the design, testing, and deployment process, and security and threat assessments and analysis would be done throughout the design and development process - rather than at it's conclusion, or not at all. Reputable and well known agencies outside the Microsoft domain would also be needed to try to break into the Exchange 2003 application. This total Secure by design process would entail following this basic framework throughout the product's total lifecycle; from start to finish, through all possible upgrades and service packs.

Secure by default

The concept of being secure by default is certainly new to Microsoft. In Security Focus, the following was written; "With Windows Server 2003, Microsoft has finally produced an operating system that isn't begging to be hacked on the first boot." (Mullen) This comment was a reference to the fact that in a default installation of almost any Microsoft product prior to the Secure Computing Initiative, virtually everything that could be enabled was enabled by default. This 'secure by default' concept was basically breaking new ground for the design, development, deployment, and corporate arms of Microsoft. This philosophy would mean that Microsoft would ship products with security measures in place by default and possible vulnerabilities disabled by default rather than the majority being enabled, as was the norm. It would be up to the customer to enable those features necessary to their operation. Installations which previously were engineered to install with all possible options and relied upon customers to disable or limit features not being utilized, would now install with tightened security configurations and force a more informed customer base to loosen them.

Secure by deployment

Secure by deployment's role in this initiative is to ensure that all new software that is deployed remains free from known vulnerabilities or security weaknesses. This encompasses Microsoft's ability to respond efficiently and effectively to any new threat or weakness and to react and deal with any reported or discovered vulnerability in their systems. This could mean timely and effective patches, improvements in application security, or information warning about exploits, patches, or security.

Communication

Communication is really designed to mesh closely with all three elements of the security initiative. In order to be effective, whether it might be security improvements, patches, vulnerabilities, or simply basic information, all pertinent information has to be communicated and disseminated to the customer base. Effective Communication means that the customers must receive accurate information in a timely manner when vulnerabilities, exploits, or viruses are discovered. Customers must be assisted in determining which issues apply to their deployed systems, and must be continually provided with updated information and best practices in response to current threats and ongoing changes in technology.

Microsoft Exchange 2003

Microsoft Exchange 2003 was deployed approximately 3 years after Exchange 2000 Server hit the marketplace. For customers accustomed to Exchange Server 5.5, the 2003 Exchange Server would be a brave new world. For organizations using Exchange Server 2000, it would appear little different from the 2000 Exchange server already in use - more like a service pack than an upgrade. But Exchange 2003 is different, and in order to fully address the impact of the Trustworthy Computing Initiative, the platform looked at must be an install of Microsoft Exchange 2003, running on Windows 2003, and utilizing Internet Information Server 6.0 and Outlook 2003.

Exchange 2003 - Secure by design

The design methodology of Microsoft Exchange 2003 is different from all other major Microsoft products, with the possible exception of Windows Server 2003. Exchange 2003 was basically in development for almost three years, so it did not start under the Trustworthy Computing Initiative, but it did finish under it.
As stated earlier, Exchange 2003 will run under the Windows 2000 (SP3) operating system, but is designed to work most securely, efficiently, and effectively under Windows 2003. Basically, if a more secure Exchange server is the goal, a large part of this security is dependent upon the operating system that

Exchange runs on. Some of the same design process that built Exchange 2003 also built Windows 2003. The extensive code reviews for security weaknesses that were conducted on 2003 just did not exist for 2000 and certainly were not in place for NT 4.0.

In March of 2002, two months after Bill Gates announced his initiative, the 450 members of the Exchange team spent two months attending classes to be trained in the components of trustworthy computing. Microsoft shut down design and development for all 175 developers and 175 testers to ensure that employees had an understanding of this new critical philosophy. The Exchange personnel were just a subset, as Microsoft spent over $200 million dollars in this "Windows Security Push", which kicked off Trustworthy computing with a 10 week halt to all Windows development work. Over 8500 developers were trained in more secure coding techniques. Employee adherence and diligence would be a critical element in the success or failure of this new and dramatic shift in the Microsoft paradigm. [7]

There are a number of new and enhanced security features in Exchange 2003 that fall under the secure by design process. Exchange 2003 was designed to support connection filtering - mail could now be rejected based upon access to safe and block lists from a variety of organizations. VSAPI, the virus scanning API, was enhanced to enable this and allows antivirus software to run on gateway and bridgehead servers. Messages could be rejected or accepted based upon the sender's IP address. Inbound messages could be rejected based upon recipient ID. Kerberos for user credentials could be utilized between Exchange stores and Outlook Web Access (OWA) or Outlook Mobile Access devices to increase security. IPSEC was available to encrypt HTTP traffic through these same front and back-end servers/devices. Protection against spoofing was designed to function under Exchange 2003.

IIS 6.0 was locked down to increase security for the OWA product. Microsoft engineers redesigned how the HTTP protocol operates. This redesign enables IIS 6.0 to use the Worker Process Isolation Mode (WPIM). This means that Web sites can now operate independently and are isolated from any other sites on the web server. Processes, performance parameters, and security parameters can now be set for each individual web site and sites are isolated and protected from whatever else might be running on the same physical server. As is evident, this configuration will aid in lessening the impact of Denial of Service (DOS) attacks, as multiple and simultaneous attacks will be necessary to bring down all sites. [8]

Outlook Web Access now supports sending email messages using the S/MIME (Secure Multipurpose Internet Mail extensions) security protocol, which will allow for the scrambling of messages and requiring a public key for reading/viewing. By utilizing a Windows 2003 Server platform remote procedure calls (RPC) over HTTPS can now securely connect Outlook 2003 clients to Exchange 2003 without having to utilize VPN technology. While the safety of this is currently being debated, it is a design feature designed to increase security, rather than open yet another hole.

For probably the first time, Microsoft spent time doing code reviews for Exchange 2003. Microsoft Research developed tools to analyze every bit of code for known vulnerabilities and code weaknesses. Coding was not an around the clock operation. More seats were shipped out to the Joint Development Partners (170,000), feedback was received on a weekly basis from Microsoft end users (never done before during development), three months were spent checking features and release criteria before the first beta release, and two months were spent after the code was locked to focus on finding and fixing any security issues. Penetration testing was done by @stake (L0pht) and apparently only 30 bugs were found. Internal task force reviews were done and months were spent on release criteria tests. This was to be the ongoing new development process. [9]

Exchange Server 2003 - Secure by default

The ‘secure by default’ component of the Trustworthy Computing Initiative is perhaps the most visible and easily correctable element in moving toward a more secure messaging platform. Microsoft now has security measures in place by default and has disabled vulnerable components that previously were enabled by default. Customers are responsible for enabling features necessary for operation; rather than having to disable unneeded features.

Some of the key default configuration changes are as follows:

1> Accounts with only user level access are no longer allowed to log on locally to the Exchange 2003 server.
2> Seldom used protocols disabled by default [Post Office Protocol (POP3), Internet Message Access Protocol (IMAP), Network News Transfer Protocol (NNTP)].
3> Anonymous authentication for NNTP is disabled.
4> Send and receive messaging limits are set at 10mb.
5> Maximum posting size for public folder messages is 10mb.
6> Outlook Mobile Access is disabled. (Service enables access from mobile Devices)
7> ’Everyone’ account removed from creation of top-level public folder creation - only Domain admins, Enterprise admins, and Exchange Domain servers groups can create.
8> Anonymous logon from organization container removed by default.
9> Secure Sockets Layer (SSL) recommended when/if server is promoted to front-end status.
10>Site replication is disabled. [10]

Microsoft has never before attempted to protect customers from themselves. Users with little or no knowledge of new products would select the default installation and open the door to intrusion and possible compromise for their organizations. With the changes instituted, users would no longer be as vulnerable from the start; they would stand a fighting chance to learn and make additional changes in a proactive, rather than reactive mode.

Default install changes - Server 2003, IIS 6.0, and Internet Explorer

The default installation of Windows Server 2003 and the changes made to enable a stronger password policy is also critical to security in Exchange. Key elements of this policy are:

1> Last 24 passwords are remembered.
2> Age restrictions set at range from 1 to 42 days.
3> Passwords must be at least 7 characters long with a minimum of one lowercase, one uppercase, and one numeric character. [11]

It will never be called the strongest password policy, but at least it is a policy and a starting point for increased security. A new or clean installation of Windows 2003 also disables many unneeded, but previously enabled services. By disabling services like Telnet and Alerter, exchange admins can make the decision to enable them as necessary, preferably with additional security precautions in place.

A critical application required for Exchange 2003 is IIS. Long perceived as one of the weakest links in the Microsoft chain, IIS 6.0 has been shored up and now installs in a more secure configuration by default. Because IIS is an optional component for Windows 2003, and Exchange by default disables SMTP, NNTP and POP3, these protocols must be enabled in order to run IIS with Exchange 2003. These transport protocols of are required for the exchange engines in order to allow routing and access. As Exchange will require dynamic web page access and IIS by default now only installs with static web page support, IIS ASP and ASP.NET support must be added/enabled.

Exchange 2003 - Secure by deployment

The secure by deployment element of the Trustworthy computing initiative has several layers. The first is determining whether Microsoft has made changes in how it handles customer ability to effectively and securely handle an installation or deployment of Exchange 2003 into their environment. The second is whether Microsoft has designed a product that can be effectively deployed. There is some overlap with the secure by design factor here; however this will be viewed from a deployment angle rather than a design one.

Microsoft has released a new set of tools to aid in the deployment of Exchange 2003 and has provided documentation to assist customers in a secure deployment. According to Microsoft, the Exchange Server Deployment Tools will greatly assist in an upgrade from Exchange 5.5 to Exchange 2003. These tools will assist in the total deployment of the product, but it will still be a challenging endeavor, especially coming from a non Active Directory 5.5 environment. [12]

The tools will also need to be verified and/or watched, as they will install some features which will be enabled, despite their non tool default configuration of being disabled. Deployments will also be different depending on whether the installation is a new install, an upgrade form 5.5, or an upgrade from 2000. There is a multitude of tools available, from Microsoft and from third party vendors. But even with these tools, deployment is not easy - especially secure deployment. Enterprise News & Reviews made the following comment:

“During tests, eWEEK Labs found Microsoft's deployment tools useful for diagnosing problems before installing the server. The Exchange 2003 resources include a number of helpful recommendations for planning to build a secure messaging environment.” (Caton)

Microsoft Exchange 2003 Deployment Tools has documentation, checklists, tools, and utilities that will be specific to whatever install or upgrade that is being attempted. It is designed to make the process easier, with wizards and management snap-ins and extensive documentation. But customers still have to do the work; the must know what they are doing; they need to know from what environment they are coming from and where they want to go.

Deployment also means ensuring that that Exchange 2003 is deployed with all the proper patches, services packs and/or fixes in place at install and maintaining this level of coverage throughout the product’s life cycle. Clearly the deployment tools are an asset to be utilized by admins installing Exchange. But there are a multitude of tools provided my Microsoft. The learning curve required to learn and use the tools is similar (on a smaller scale) to actually learning the intricacies of Exchange 2003. Microsoft has designed a product that can be effectively deployed; but it will not be a simple process.

Exchange 2003 - Communication

The first reported flaw in Microsoft Exchange 2003 was disclosed on November 14, 2003 and is currently being investigated by Microsoft. This possible flaw was found in the Outlook Web Access (OWA) component of Exchange 2003 and allows users logging in to OWA to have access to other user’s mailboxes at random and have full and complete access to all email. And while Microsoft states that indications are that Kerberos was manually disabled in the installation, the customer claims the default installation is to blame. [14]

Nothing has yet been released to customers as Microsoft is testing a patch and the customer affected has had to turn off OWA in order to circumvent the problem. This incident will be an interesting test case to assist in determining whether the communication element of the Trustworthy Computing Initiative has made advances with the newly released Exchange 2003.

Communication from Microsoft has undergone revision in recent months with the revamping of Security bulletin protocol after the last flurry of patch releases for a number of products. Security bulletins will now be released on a monthly basis, on the second calendar Tuesday of each month. Microsoft does plan to make exceptions if customers are deemed to be at immediate risk from viruses, worms, or attacks. These changes were undertaken under the Trustworthy Computing Initiative and were based upon feedback from the customer base. Communication and information was seen to be contradictory; one path was specified in the knowledgebase and another in the security bulletins. Customers wanted and needed better guidance on the risks involved; both in the patch and the responsible vulnerability/bug/virus. Customers needed to know who and what was affected and how to easily download the fix. The security bulletins were redesigned in order to be more easily readable and functional. These new procedures are Microsoft's attempts to satisfy the numerous drawbacks in the current system, and will be modified as the need arises. [15]

Summary

This paper has attempted to briefly discuss the tenets of the Microsoft Trustworthy Computing Initiative and how they have aided in the increase or decrease of the security posture and position of the newly deployed Microsoft Exchange 2003 Server. Because the design, default, deployment, and communication elements are tied closely with the total suite of products that will create the Exchange 2003 environment, this paper was forced to consider the initiative from the perspective of numerous Microsoft upgrades, changes, and installs. Exchange 2003 security is not complete unless the platform utilizes 2003 Server, runs Internet Information Server 6.0, uses 2003 Outlook Web Access, and enables client access from Outlook 2003. While it is not feasible to expect all these changes to happen immediately, the true impact of the security enhancements will not be felt until all these pieces are in place.

Conclusion

Has the Trustworthy Computing Initiative resulted in a more secure Exchange

2003? Of course it has…how could the current environment fail to be anything but improved? The total security infrastructure has clearly been improved. The design process has been altered to actually consider security. Default services and options that are disabled by default are now the norm, rather that the exception. Deployment tools are ready available to assist in what will be a strenuous deployment. Communication from Microsoft has been made more accessible and more usable. Will these fundamental changes in the Microsoft corporate philosophy last? That remains to be seen. But the Trustworthy Computing Initiative has resulted in a more secure Exchange 2003. Do these security enhancements make Exchange 2003 impregnable? Of course they do not. There are security holes in Exchange 2003. There certainly will be more found - but it is certainly the most secure Microsoft product to date. While I am not convinced that security is now Bill Gates and Microsoft's top priority, it seems clear that security is no longer at the bottom. And with continued pressure by the industry and the corporate and private consumer base, the security of Exchange and other Microsoft products can only continue to improve.

References

1. Cherry, Michael. “Slammer Worm: Code Red déjà vu” Directions on Microsoft. 10 February 2002
URL: http://www.directionsonmicrosoft.com/sample/DOMIS/update/2003/03mar/0303swcrdv.htm

2. “Get Up to Speed: Enterprise Security” C/NET News.com 24 November 2003
URL: http://news.com.com/2001-7355-0.html#players

3. Swoyer , Stephen. “Exchange 5.5 Support: Get it while it lasts?” ENT News. 9 June 2003
URL: http://www.entmag.com/news/article.asp?EditorialsID=5840

4. Lemos, Robert and Kane, Margaret. “Gates: Security is top Priority” C/NET News.com. 17 January 2002
URL: http://news.com.com/2100-1001-816880.html

5. Orion, Egan. “Microsoft admits Windows is Insecure” The Inquirer. 6 September 2002
URL: http://www.theinquirer.net/?article=5313

6. Mullen, Tim. “Secure by Default” Security Focus. 27 April 2003
URL: http://www.securityfocus.com/columnists/157

7. Dow Jones Business News. “Microsoft increases aid for Software Fixes” ComputerUser. 17 May 2003
URL: http://www.computeruser.com/news/03/05/17/news6.html

8. De Clercq, Jan. “Exchange Server 2003 Security” Windows & Net Magazine. November 2003 42-48

9. Fontana, John. “Exchange ready for security test in real world” Computerworld. 1 July 2003.
URL: http://idg.net.nz/news.nsf/UNID/CC256CED0016AD1ECC256D5500128A28

10. White Paper. “Microsoft Exchange Server 2003 Security Enhancements” Microsoft Exchange Server. 2 June 2003
URL: http://www.microsoft.com/exchange/evaluation/Security_e2k3.asp

11. De Clercq, Jan. “Exchange Server 2003 Security” Windows & .Net Magazine. November 2003 42-48

12. Exchange Documentation Team. “What’s New in Exchange 2003” May 2003 (October 2003)

URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=84236bd9-ac54-4113-b037-c04a96a977fd&DisplayLang=en

13. Caton, Michael. "Exchange Tools Aid Deployment Tasks" eWeek. 22 September 2003
URL: http://www.eweek.com/print_article/0,3048,a=107599,00.asp

14. Evers, Joris. "Microsoft investigates possible Exchange 2003 flaw" IT World.com. 24 November 2003
URL: http://www.itworld.com/App/4149/031124exchangeflaw/

15. White Paper. "Revamping the Security Bulletin Release Process" Microsoft Technet. October 2003 (November 2003)
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/revsbwp.asp