



6/25/2004

## The New Approach to Windows Security

*Rob Enderle  
Jasmine Noel*

### Executive Summary

***With per incident security costs that range, on average, from twelve thousand dollars for small businesses to nearly three hundred and fifty thousand dollars for large businesses, and the rate of attack increasing significantly year over year, security management has never been more important or more difficult. A company's life blood is often in its systems which contain customer data, transactions records, and intellectual property and the protection of that data is the responsibility of the company's IT organization which has the unenviable responsibility to protect it. Security budgets more than doubled in the last four years to address this threat, but it is clear that a comprehensive security strategy needs to be in place to insure the asset protection responsibilities that IT has are met.***

***Simply using Anti-Virus software is not enough. Viruses move too quickly and by the time an anti-virus vendor can respond millions of users can be infected with adverse implications to the related companies and networks. To address this threat a unique software + hardware approach is needed. One that not only identifies and blocks certain threats but keeps some of the most damaging, like buffer overflow exploits, from executing at all.***

***This hardware plus software approach will be available late in 2004 through a combination of the upcoming Microsoft Windows XP Service Patch 2 (SP2), and processors capable of running the DEP (Data Execution Protection) code that is part of this release. At the time of this report the only processors capable of running DEP (formerly NX for "No Execute") code are the AMD Athlon™ 64, the AMD Opteron™ and the Itanium® from Intel. The DEP code's functionality is directly tied to the EVP (Enhanced Virus Protection) component of AMD Athlon™ 64 and AMD Opteron™ processors.***

***An additional benefit can be derived from an early migration to 64-bit processors. Older 32-bit applications, which (because they were developed during a time when security exposures were lower and not as well understood) are an increasing percentage of the remaining vulnerabilities, will have to be replaced (and often won't run). This helps insure that line organizations don't compromise otherwise secure systems by placing older 32-bit applications on them once IT has put the complete solution in place.***

***Given the increasing threat and the substantial risk associated with leaving systems unprotected the recommendation is clear: shift purchasing behavior to DEP compliant hardware immediately and move to Windows XP SP-2 as soon as possible.***



## Findings

### **The Vulnerability Problem**

Today network security management is increasingly challenging because of the growing number of attacks directed at businesses, governments and institutions. According to the 2003 CSI/FBI survey<sup>i</sup> the number of respondents citing the Internet as a source of attack grew to 78% in 2003 from 57% in 1999. This jump is unsurprising given the wide-spread changes in business practices driven by the e-Business initiatives and powered by Internet and Web technologies. Email and web-based remote access to enterprise systems are standard computing capabilities for every business. The number of businesses conducting retail transactions online has skyrocketed. Enterprises are lowering costs by electronically integrating their supply chains. IP telephony and wireless LANs are beginning to gain footholds in some industries to lower infrastructure costs and improve employee connectivity to business systems. All of these business practice changes have increased access to business systems through the Internet and therefore have increased the vulnerability of those systems to attack.

The other component of the vulnerability equation is the increasing volume of attacks. According to Symantec's threat report<sup>ii</sup>, the number of Win32 viruses and worms observed increased by two and a half over the same period in 2002. This trend is driven by the increasing ease with which attacks can be created. The amount of exploit code published for documented system vulnerabilities is increasing year after year making it easier for attackers to construct new attacks. Additionally, the percentage of vulnerabilities needing no specialized exploitation code is increasing. For these reasons 70% of vulnerabilities were classified by the Symantec report as easy to exploit. Furthermore, the time between disclosure of a system weakness and widespread exploitation is shrinking<sup>iii</sup>. It is therefore no surprise that a recent CSI/FBI study found that virus incidents were one of the most cited forms of attack or abuse.

As exploiting individual system weaknesses becomes easier, sophisticated attackers have shifted their focus to creating blended attacks. Blended attacks combine multiple techniques (such as viruses, worms, Trojan horses, and malicious code) to rapidly broadcast and execute an attack. Blaster, Welchia, Sobig.F, and Dumaru are recent examples of rapidly spreading blended threats. Symantec reports that 54% of the top ten threats in the last six months were blended attacks. This increasing attack sophistication is a disturbing trend because coordinated attacks are more difficult to identify and repel. It means businesses of all sizes must have a seamless security strategy with protective technology at every level of computing including hardware, operating systems, networking, applications, databases, and integration software.

Today's high level of computing security threat is created by the combination of three trends: 1) the increasing connectivity of critical business systems via Internet technology, 2) the increasing volume of network-based threats and 3) the increasing sophistication of severe attacks. This combination of threats creates a risky environment for businesses using personal computers and servers to deliver a competitive advantage.

**Bottom-line cost of vulnerabilities**

Companies of all sizes attempt to mitigate the risks with various computing security solutions. Security spending remains a top priority in spite of the IT budget tightening over the last few years. Morgan Stanley’s CIO surveys have security as one of the top ten CIO priorities since 2001. CIO Magazine Tech Poll conducted in November 2003 showed that only 5.1% of respondents expect their security budget to decrease in 2004.

Companies of all sizes have ratcheted up their efforts to defend their networks from attack (see Tables). Companies worldwide spent \$1.4B on anti-virus software<sup>iv</sup> and \$1.6B on managed security services<sup>v</sup> in 2002. Virtually every company has invested in firewall technology and the percentage of companies deploying intrusion detection systems leaped from 42% in 1999 to 73% in 2003.<sup>vi</sup>

**Figure 1: Security spending by large and small businesses**

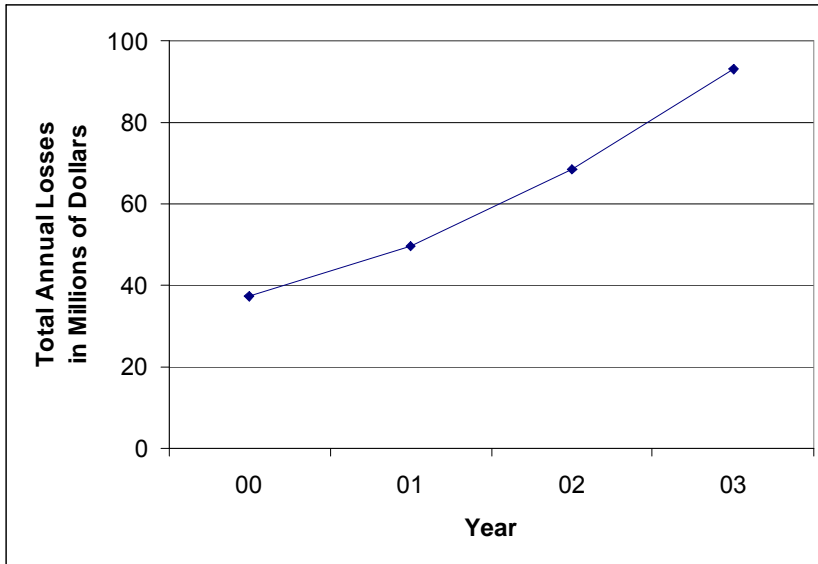
<b>Security Spending as a % of Global 2000 Companies' IT Budgets, 2001-2003</b>		<b>US Small Business Spending on Networking Storage and Security Solutions, 2002-2004 (in millions)</b>		
2001	3.20%		Firewalls	Intrusion detection
2002	7.60%	2002	\$211	\$11
2003	8.20%	2003	\$279	\$36
n=304 organizations Source: META Group, November 2003		2004*	\$348	\$66
		Source: AMI-Partners, October 2003		
		*Estimated		

Companies are also investing in configuration and change management solutions. With the time between vulnerability announcement and attack shrinking, rapid deployment of newly available security patches to every system is an imperative. As a result patch management is a growing component of a system’s total cost of ownership. Depending on the number and type of systems, a sophisticated patch management system and the dedicated administrative resources to deploy patches can raise the total cost of system ownership between 10-15%.

**The top-line cost of vulnerability**

In spite of all the money spent to secure computing systems some attacks still manage to overcome the defenses and wreck havoc on the business. Computing technology is now completely interwoven with most businesses’ ability to produce, sell and deliver goods and services. This dramatically increases the top-line business risk of security-related attacks. Figure 2 shows that the total dollar amount lost due to denial of service and virus attacks is still increasing year after year. This increase is occurring because of the increasing amount of business that is transacted over the Internet which can be disrupted during an attack. We believe these estimates are low because the CSI/FBI report acknowledges that while 75% of the survey respondents admitted financial losses, only 47% could quantify the losses for inclusion in the final dollar values listed in the report.

**Figure 2: Total dollar amount lost due to denial of service and virus attacks**



Source: 2003 CSI/FBI Computer Crime and Security Survey

The total top-line costs for an individual company can vary widely depending on the type of business conducted over the Internet and severity of the attack. Figure 3 shows the estimated costs of a single severe security breach. With Symantec reporting between 2-8 severe attacks for every 10,000 events, a well-protected, large company can expect at least four costly attacks per year resulting in costs between \$0.4 – \$1.4 million.

**Figure 3: Estimated cost of the worst security breach for each UK business\***

	<b>Overall</b>	<b>Large business</b>
Disruption to business	\$9,000 – \$18,000 over 1-2 days	\$90,000 – \$270,000 over 1-3 days
Time spent responding to incident	\$900 – \$1,800 2-4 person days	\$5,400 – \$10,800 10-20 person days
Direct cash spent responding to incident	\$1800 – \$3,600	\$5,400 – \$18,000
Direct financial loss (e.g. loss of assets, fines, etc.)	\$360 – \$900	\$3,600 – \$7,200
Damage to reputation	\$180 – \$540	\$3,600 – \$36,000
<b>Total cost of worst incident on average</b>	<b>\$12,600 – \$25,200</b>	<b>\$117,000 – \$342,000</b>

\* 1£ to \$1.8 conversion rate used

Source: "Information Security Breaches Survey" PricewaterhouseCoopers and Department of Trade and Industry, April 2004

**Anti-virus and network-based security is not enough**

It is not that all the money spent so far on security systems is wasted; it helps to ward off a large (and increasing) number of attacks of a particular type. For example, firewalls that monitor network traffic can provide solid protection from network-based

attacks on layers 1-4 of the OSI network stack. Anti-virus software mitigates risk from well known issues and relegates the thousands of “juvenile” assaults to back-ground noise.

However the newest and most serious attacks now focus at the application layer. Buffer overflows, SQL injections, and cross-site scripting are application software layer attacks which bypass firewall inspection. Similarly, the increasing use of blended attacks means that businesses cannot rely solely on perimeter defenses and recognition of known attack patterns. The estimated \$2 billion<sup>vii</sup> in worldwide damages attributed to the Blaster, Welchia, and Sobig.F attacks in 2003 are the clearest evidence that additional security methods are necessary.

The Software layer is the hardest to secure for several reasons. Software development best practices differ from vendor to vendor and within enterprise development organizations, therefore adherence to any security-related software guidelines is difficult to ensure. Software vulnerabilities may take years to identify because today’s software applications are extremely complex aggregates of modules, class libraries and third-party services. The interaction between complex applications and equally complex operating systems will always leave gaps for the malicious to exploit.

To battle the security breaches at the application level requires the hardware infrastructure itself to become smarter about recognizing unusual application behavior.

### **Hardware + Software: The New Approach to Comprehensive Security**

The cost of not being secure has risen to unprecedented highs and given the rate at which viruses are spreading we are quickly reaching a point where virus checking products alone are inadequate<sup>viii</sup>. This required both software and hardware vendors to begin to rethink the PC platform and laid the groundwork for one of the most rapid technological changes the market has ever seen.

What drove this change was the realization, largely by Microsoft, that much of the problem actually resided beyond the vendors control and was tied to older applications which IT organizations were unwilling to get rid of. By simply moving to another, similar, operating system these organizations would migrate these older applications over onto the new more secure systems. To make these applications run, in many cases, security features would have to be turned off compromising the reliability of the platform and undoing much of the work Microsoft had done to secure it in the first place.

The end result was acceleration into 64-bit computing which would provide a stronger incentive for businesses of all sizes to move away from these old applications and allow both Microsoft and supporting vendors a better way to surround their related product efforts with effective marketing programs. AMD was first to come forward with a 32/64-bit platform at a price acceptable to the existing market of Desktop and Laptop Computers, Workstations and high volume servers. As a result the new AMD Opteron and AMD Athlon 64 processors became the primary target for the upcoming Microsoft 64-bit version of Windows XP which is expected to enter the market by December of 2004.

But, as noted above, denial of service attacks have become so incredibly costly and painful that there was a need to go further. Microsoft’s researchers found that the only

way to definitively address this problem was to make physical changes in both the processor and the operating system. Thus NX, which stands for "No Execute" was born. It is also known by a number of other terms. Microsoft now calls this technology Data Execution Protection (DEP), and AMD refers to it as Enhanced Virus Protection (EVP). The only problem was that no existing 32-bit processor had the headroom to run NX component and today it only runs on the 64-bit Athlon and Opteron processors. For the purpose of this project we will refer to this as DEP for the remainder of this document.

The DEP mechanism will be available in Windows XP SP2, Windows Server 2003 SP1, Windows Server 2003 for 64-bit extended systems, Windows Server 2003 for 64-bit Extended Systems, and Windows XP 64-bit Edition for 64-bit Extended systems.

As a result AMD will be the primary launch partner for the upcoming Windows XP SP-2 and Windows XP 64 releases that will contain the DEP components. This was a role traditionally held by Intel and even Microsoft seemed surprised they weren't on board earlier in the process.

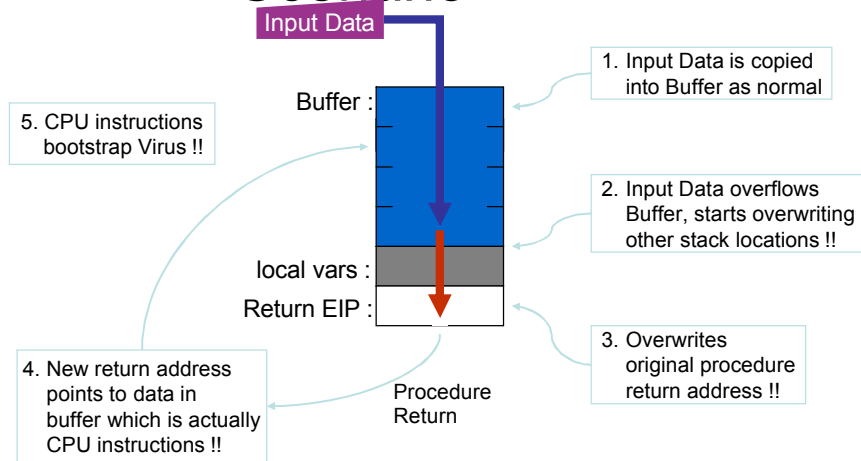
### **How DEP Works**

Buffer Overflow attacks are some of the most costly and common attacks currently in the market. Code Red cost \$1.2B according to USA Today and Melissa cost \$385M according to Trusecure Corp<sup>ix</sup>. In fact Buffer Overflow vulnerabilities permeate the SANS top 20 list of CERT security vulnerabilities<sup>x</sup> and it is ranked 5<sup>th</sup> in the Top Ten Vulnerabilities by Orthus Information Security Solutions<sup>xi</sup>. By any measure this is one of the most painful and expensive kind of exposure in the market today.

Buffer Overflow attacks attempt to insert and execute code from memory locations that do not normally contain executable code. For example, these sections include User and Kernel Procedure Stacks, and User and Kernel Data section and default heaps. Apparently the User Stack is one of the key locations exploited by buffer overflow attacks. How the attack works is the attacker gives more data than the program is expecting and this overflows the programs procedure return stack which then tricks the system into executing that data. In effect the attacker seizes control of the computer and then uses it to run most of the attacker's instructions or load a virus.

You can see in the figure on the following page how 1) the data is first copied into the buffer, 2) the data overflows the buffer, 3) the data overwrites the original procedure return address, 4) this new return address then points to new data which are actually CPU instructions, and 5) how these CPU instructions actually bootstrap the virus.

# Simple Buffer Overflow Scenario



Source: AMD/Microsoft

NX, or No Execute, works by intercepting and blocking these attempts and creating a Windows Exception that can be reported to the user or to the support organization responsible for the computer. In most cases this means the computer will kill the program and notify the user that an attempt has been made to seize control of his or her computer. These attacks, in some cases, can override default protection on the system by altering boot.ini and Windows Registry settings.

This will impact some applications, specifically Just in Time applications, adversely and simply make it so they can't execute. Much of the tuning being done during the release candidate phase for the upcoming Windows XP SP 2 has been to insure that the number of applications impacted by this is extremely small. If there is a problem making some minor changes you may be able to overcome this shortcoming. In any case, the benefit of reducing the risk of someone hijacking your PC or server should generally be worth the risk of having to rewrite a JIT application.

DEP isn't absolute protection either. For instance, procedure return interception is still possible with DEP enabled, but the risk for real harm is lower. Used in conjunction with recommended programming practice NX is a powerful tool in preventing successful Buffer Overflow attacks.

## Looking Forward the Risks Only Increase

Given current business and technology trends the following expectations about the future of network management and security can be deduced:

**Sophisticated attacks will become more common** as tools for creating them are developed and become more widely available. The application layer of today's business systems is the most vulnerable, therefore perimeter defenses alone will not suffice.

**The complexity of networked application architectures will increase.** J2EE, .Net and Web Services based applications and a variety of wired and wireless networking technology will continue to grow in popularity to support the need for flexible yet integrated business processes that connect multiple business departments together. Therefore, a comprehensive approach must be taken to secure all of these new "moving parts."

### **Top-line business losses for a single severe attack will continue to increase.**

The volume and value of online transactions continues to grow rapidly as more enterprises automate business processes that connect remote customers, employees and partners. Figure 2 shows that reported business losses have been increasing steadily at approximately 34% year after year since 2000. We believe that rate will be higher over the next few years for two reasons. First, IT-related financial reporting capabilities are improving which allows companies to better quantify the losses associated with a particular attack. Second, J2EE, .Net and Web Services technologies increase the reuse of existing software for multiple business services. This reuse and application integration increases the likelihood of several business services being affected by a single vulnerable system, leading to higher attack losses. We estimate that these would increase the loss growth rate anywhere from 45-65%. Thus a typical large business would see per incident losses from \$170,000 to \$193,000 on the low end and as much as \$495,000 to 564,000 on the high end<sup>1</sup> for 2004.

Thus, it is no surprise that enterprises will be under increasing pressure to limit the number of severe attacks they experience. If business systems can be hardened against unusual application behavior and weak application development practices then the likelihood of a successful application level attack can be lowered.

## AMD's Solution

AMD enables enterprises and businesses to protect themselves today. Servers are often not the first target of viruses and worms that exploit buffer overflow. These viruses and worms depend on client computers to be the receivers of their malicious code through infected email messages or files, and rely on a user opening the message or executing the file to activate the virus.

- Servers suffer more ill effects from the high rate of network traffic generated when these viruses access a user's email address book and begin sending infected messages to other users.
- In general, having DEP (EVP) protection available on all computers in an organization, including servers, would be a general safety precaution.

---

<sup>1</sup> Baseline per attack loss taken from Figure 3

- For a server to be able to make use of the DEP (EVP) protection, the server operating system needs to provide support for this feature. Windows Server 2003 SP1 and Windows Server 2003 for 64-bit Extended Systems are planned to offer support for EVP. The Linux kernel and various popular distributions of Linux already offer this capability.

As companies make the business decisions to purchase or refresh desktop and mobile computers, the investment and security protection offered with AMD64 processors in tandem with upcoming Microsoft Windows XP SP2 will change RFP and selection criteria.

- As an extended part of the network, mobile users can be especially vulnerable to viruses and other forms of attack and increase risk to the whole network.
- Mobile computing is the fastest growing part of the business network, growing at over 18% CAGR<sup>xii</sup>, and also exposes key data to attack.
- Mobile users tend to use their PCs for both personal and business activities, exposing them to more threats.

With increasingly connected business models including e-business and billions of e-mails crossing global corporation firewalls, advanced desktop security is mandatory.

- As corporations purchase desktop and notebook systems to replace systems acquired for Y2K readiness (timed with the industry average 3-5 year refresh cycle) any AMD64 processor-based system will automatically offer increased security capabilities when combined with SP2.
- DEP/SP2 is the first instantiation of the next phase in security-hardware/software solutions are required to battle the ever-increasing sophistication of malware.

When combined across all Servers and Clients DEP/SP2 help form a more secure line of defense for Enterprise networks and can potentially prevent serious attacks that rob companies of both time and money.

Rob Enderle  
[renderle@enderlegroup.com](mailto:renderle@enderlegroup.com)  
(408) 272-8560

## **Authors:**

### **Rob Enderle:**

Ranked as one of the most influential technology analysts since 1995, Rob Enderle has over 10 years experience as an analyst and over 20 years of line and staff experience in technology companies. Rob is currently President and Principle analyst for the Enderle Group which is focused on emerging technologies. Previously Rob was a Research Fellow for Giga Information Group and Forrester Research where he ran the Security, eCommerce, and Desktop and Mobile research groups at different times. Prior to this Rob held a number of executive positions at IBM including Competitive Analysis, Internal Audit, Marketing, and Finance. Rob is widely quoted by the technology media and the general press, and writes for eWeek, TechNewsWorld, Internet Week, Computer User, and MacNewsWorld.

Rob holds a bachelor of science and an MBA from the Long Beach State University in Southern California and a CMA certificate from Pace University in New York.

### **Jasmine Noel:**

A recognized expert in infrastructure management, Jasmine Noel has 8 years experience as analyst and researcher. Noel served previously as director of systems and applications management at Hurwitz Group, where she formulated and managed the company's research agenda. She was also a senior analyst at D.H. Brown Associates, where her responsibilities included technology trend analysis in the network and systems management space. Noel is regularly quoted in publications such as CIO Magazine, eWeek, InformationWeek, InfoWorld, and NetworkWorld. She also has contributed articles to several leading publications on various IT management topics.

Noel holds a bachelor of science from the Massachusetts Institute of Technology and a master of science from the University of Southern California.

## References

- <sup>i</sup> 2003 CSI/FBI Computer Crime and Security Survey, [www.gocsi.com](http://www.gocsi.com)
- <sup>ii</sup> Symantec Internet Security Threat Report, March 2004
- <sup>iii</sup> For example, the appearance of the Blaster worm occurred only 26 days after the announcement of the Microsoft DCOM RPC vulnerability last year. In April 2004 the first appearance of the Sasser worm occurred only 18 days after Microsoft announced the vulnerability.
- <sup>iv</sup> Gartner report “Antivirus Software Market Surges to \$1.4 Billion,” August 2003
- <sup>v</sup> In-Stat/MDR report “Managed Security Services: A Market Analysis,” October 2003
- <sup>vi</sup> 2003 CSI/FBI Computer Crime and Security Survey, [www.gocsi.com](http://www.gocsi.com)
- <sup>vii</sup> Computer Economics estimates the economic impact of these outbreaks. These numbers may not include costs such as stock value decline, customer confidence, and negative publicity.  
[www.computereconomics.com/article.cfm?id=867](http://www.computereconomics.com/article.cfm?id=867)
- <sup>viii</sup> PC Magazine “Why your antivirus program won't catch the next attack”,  
<http://www.pcmag.com/article2/0,1759,1593152,00.asp>, June 8, 2004
- <sup>ix</sup> [University of Virginia Department of Computer Science](http://www.cs.virginia.edu) Introduction to Software Dynamic Translation, February 27, 2002
- <sup>x</sup> SANS Top 20 Internet Security Vulnerabilities <http://www.sans.org/top20/> 10/08/2003
- <sup>xi</sup> Orthus Top Ten Vulnerabilities <http://www.orthus.com/ttvuln.html> 2004
- <sup>xii</sup> Gartner Dataquest Worldwide PC Forecast Q1 2004