David Maynor Internet Security Systems

NX: How Well Does It Say NO to Attacker's eXecution Attempts?

NX. It's known by different names to different people. AMD calls it Enhanced Virus Protection, or EVP. Microsoft calls its support Data Execution Prevention, or DEP. After the press about how this new technology will stop hackers and worms in their tracks, many people call it a modern marvel. But this new technology has several layers of confusion surrounding it in regards to where it is implemented, how it protects and even when its on. This talk will unwrap the information while showing that at best NX is a speed bump and not a stop sign to malicious intruders.

U ACK HA Π TING

David Maynor is a research engineer with the ISS Xforce *R&D* team where his primary responsibilities include reverse engineering high risk applications, researching new evasion techniques for security tools, and researching new threats before they become widespread. Before ISS Maynor spent the 3 years at Georgia Institute of Technology (GaTech), with the last two years as a part of the information security group as an application developer to help make the sheer size and magnitude of security incidents on campus manageable. Before that Maynor contracted with a variety of different companies in a widespread of industries ranging from digital TV development to protection of top 25 websites to security consulting and penetration testing to online banking and ISPs.

















INTERNET SECURITY SYSTEMS © 2006 Internet Security Systems. All rights reserved. Contents are property of Internet Security Sys

The journey of a thousand miles...













INTERNET SECURITY SYSTEMS
 2005 Internet Security Systems Al fable reserved, contents are presently of internet Security System



D OK HAT UU N







	Lets look under the hood										
Fig. 1	Performance Options										
	Sector Determination (SEP) (helps protect particular determination										
© INTERNET SEC © 2005 Internet Security Systems. All rights of	URITY SYSTEMS Reved Centeris as property of Internet Society Systems.										

U LACK HAT I ING





Lets look under the hood...

Again, why?

Different loader? Pages are not marked correctly? Different Memory management?

Why do you care?

No-execute technology isn't extended to everything. Default settings for DEP? False sense of security.

NX protection has to have OS support to work. It can be selectively enabled/disable VirtualProtect (for windows)

© INTERNET SECURITY SYSTEMS* © 2005 Internet Security Systems. All rights reserved. Contents are property of Internet Security System





Windows supports it...

Hardware enforced DEP close up

This is what we have been discussing most of the talk Requires no-execute enable chip

Protection/enforcement is done on a per virtual memory page basis Protects both 32bit and 64bit versions of the OS if correct chip is used.

32bit versions of the OS require PAE enabled

Protection is configurable via control panel and boot.ini options

[INTERNET SECURITY SYSTEMS*

© 2005 Internet Security Systems. All rights reserved. Contents are property of Internet Security Systems



Software DEP close up

Software only attempt to detect bufferoverflows Attempts to detect "Stupid SEH Tricks"

Uses SafeSEH

Before an exception is run SafeSEH makes sure it's a valid handler Makes sure its not in executable memory

Processor independent

A lot of popular exploits use SHE tricks to get execution

....Alot don't.

© INTERNET SECURITY SYSTEMS* © 2005 Internet Security Systems. All rights reserved. Contents are property of Internet Security System



















BLACK HAT BRIEFINGS



				Windows support				
	60 Memory bash.exe							
	BaseAddr	AllocBase	AllocProtect	Size	State	Protect	Туре	Module
n easier way?	00000000	N/A	N/A Boodulitie	65536	Free	N/A Readultite	N/A Disate	
	00011000	N/A	N/A	61440	Free	N/A	N/A	
Prc\/iew	00020000	00020000	Read//rite	4096	Commit	Readwrite	Private	
	00021000	N/A 00030000	N/A Bandulika	2035712	Filee Determs	N/A N/A	N/A Divete	
	00221000	00030000	Read//ite	4096	Commit	RAW Guard	Private	
	00222000	00030000	Readwirke	57344	Commit	Readwirke	Private	
	00230000	00230000	ReadUnly	12288	Commit	ReadUnly	Mapped	
	00240000	00240000	Beads/rite	65536	Commit	Beachwrite	Private	
	00250000	00240000	Read/v/rite	983040	Reserve	N/A	Private	
	00340000	00340000	Readw/rite	24576	Commit	Readwrite	Private	
	00346000	00340000	Read//inte	40960	Reserve	N/A Decedución	Pirvate	
	00353000	00350000	Read//ite	53248	Receive	N/A	Mapped	
	00360000	00360000	ReadOnly	90112	Commit	ReadOnly	Mapped	
	00376000	N/A	N/A	40960	Foee	N/A	N/A	
	00300000	00380000 N/A	N/A	243656	Eann	HeadUnly N/A	Mapped N/A	
	003c0000	003c0000	ReadOnly	24576	Commit	ReadOnly	Mapped	
	003c6000	N/A	N/A	40960	Free	N/A	N/A	
	00340000	00340000	Read//rite	4096	Commit	ReadWrite	Private	
	003e0000	003e0000	Readwhite	4096	Commit	Readwrite	Private	
	003e1000	N/A	N/A	61440	Free	N/A	N/A	
	00310000	00310000	Read/rite	16384	Commit	Read//rite	Private	
	00364000	00310000	ReadWrite	49152	Reserve	N/A Recelled	Private	back and
	00401000	00400000	ExecWitCopy	397312	Commit	ExecRead	Image	bath eve
	00462000	00400000	ExecWICopy	20480	Commit	Readwhite	Image	bash exe
	00467000	00400000	ExecWrCopy	94208	Commit	ReadOnly	Image	bash exe
	0047e000	00400000	ExecW/rCopy	35354	Commit	Head/vite	Image	bash exe
	00488000	N/A	N/A	32768	Fann	N/A	N/A	Dater 688
	00490000	00490000	ReadUnly	266240	Commit	ReadUnly	Mapped	
	004d1000	N/A	N/A	61440	Free	N/A	N/A	
	Internin	In Meltin	NOADOREE	81921	Lound	HearWole	Privale	
				Private: 3	52 K. Mapped	2756 K, Image: 6808	IK	
				NT NORMATIAN	NAMES OF A DESCRIPTION OF	Colored Children Carrier and	1955	
FEDNIET CECUDITY	VETI	IMC						
ERNEL SECURITY								















INTERNET SECURITY SYSTEMS*
2006 Internet Security Systems. All rights reserved. Contents are properly of Internet Security System

<section-header><section-header><section-header><section-header><text><text><text><text>





LACK HAT FING











Why isn't this the silver bullet?

The problem is very complex.

Airport metal detectors and fingernail clippers.

A patch on top of a band alde on the outside of a bandage wrapped around a cast.

Its time to start fresh.

Can you blame anyone for NX not living up to the hype?

Its less about programming errors and more about the architecture being to open.

[INTERNET SECURITY SYSTEMS*





