



O-ISC '07
Ohio Information Security Conference

Securing the Application Layer

Blaine Wilson
Reynolds & Reynolds



Reynolds
& Reynolds®

Speaker Biography

Blaine Wilson

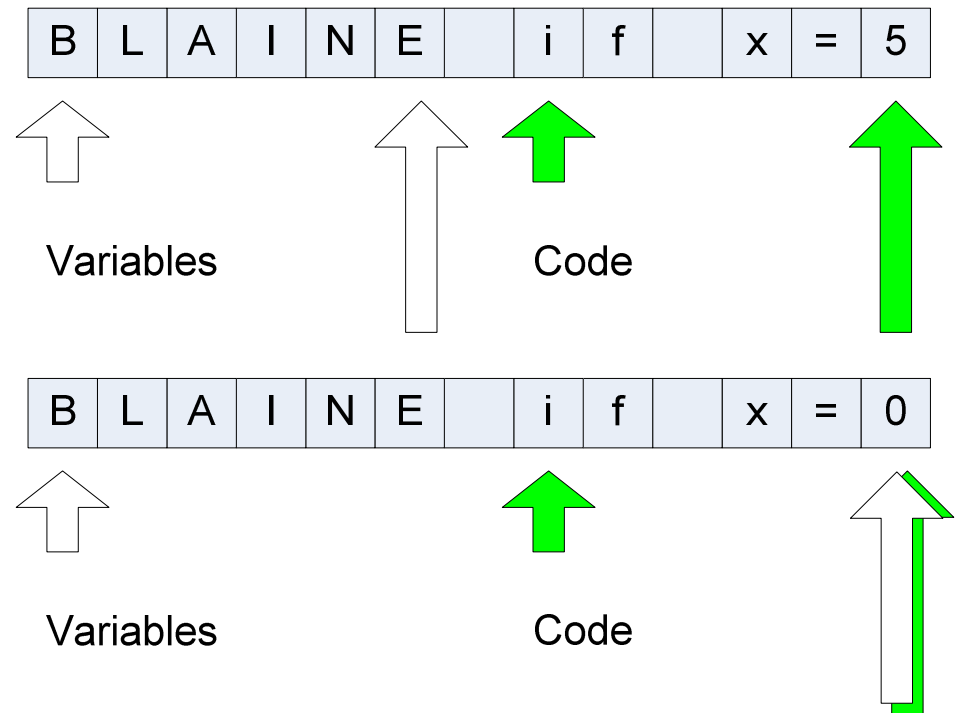
- 14 years experience in software development.
- Joined Reynolds & Reynolds in 2000 where I work on the performance, scalability and security of applications developed by the corporation.
- Before Reynolds, I worked as a consultant to medical corporations for their application, data and network needs.

Agenda

- Buffer Overflow
- Integer Overflow
- Decompiling
- Reading Memory
- Cross Site Script Injection
- SQL Injection

Buffer Overflow – The Issue

- Variables and the code are next to each other in memory
- Uncontrolled variables can overwrite the code (unknown to the application)



- Check all input
- Use safer libraries
- Patch Management
- Tools to find
 - Source code assessment tools
 - http://www.ouncelabs.com/secure_enterprise.html
 - Simple search tools
 - Code Reviews

“Writing Secure Code” by Michael Howard and David LeBlanc

buffer overflow

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci549024,00.html

Buffer Overflow Attacks and Their Countermeasures

<http://www.linuxjournal.com/article/6701>

Integer Overflow – The Issue

- Variable to hold our number may not be large enough to hold the number
 - int8 (-128 – 127)
 - unsigned int8 (0 – 255)
 - int16 (-32,768 – 32,676)
 - unsigned int16 (0 – 65535)
 - Etc.

		1	1	1	1	1	1	1	1
	+	0	0	0	0	0	0	0	1
=		1	0	0	0	0	0	0	0

Integer Overflow – Steps to Take



O-ISC '07
Ohio Information Security Conference

- Check to see if your language is vulnerable
- Ask if the values should be signed or unsigned
- Ask if the container is big enough to hold the values
- Patch Management
- Tools to find
 - Code reviews

Integer Handling with the C++ SafeInt Class

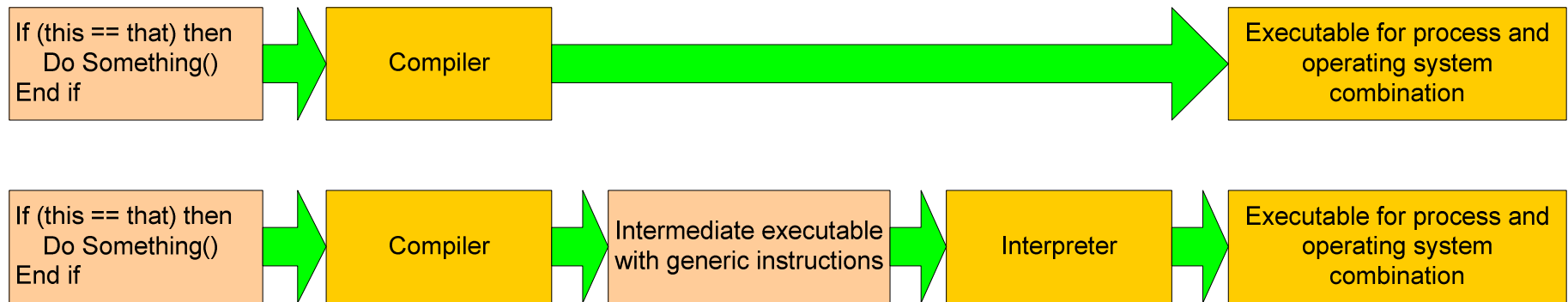
<http://msdn2.microsoft.com/en-us/library/ms972705.aspx>

Reviewing Code for Integer Manipulation Vulnerabilities

<http://msdn2.microsoft.com/en-us/library/ms972818.aspx>

Decompiling – The Issue

- Compilers originally created executables targeting a processor and operating system.
- New environments (like Java and .Net) compile to an intermediate language. This intermediate language is very easy to decompile.



- Restrict access to your executables and libraries
- Check to see what options are available with your compiler
- Don't send out your debug symbols
- Encrypt, Obfuscate and Wrap
- Tools to find
 - Decompilers

Decompiling References



The Common Language Runtime (CLR) and Java Runtime Environment (JRE)

<http://www.codeproject.com/dotnet/clr.asp>

Introduction to .NET

<http://www.codeproject.com/dotnet/dotnet.asp>

How-To-Select an Obfuscation Tool for .NET™

<http://www.howtoselectguides.com/dotnet/obfuscators/>

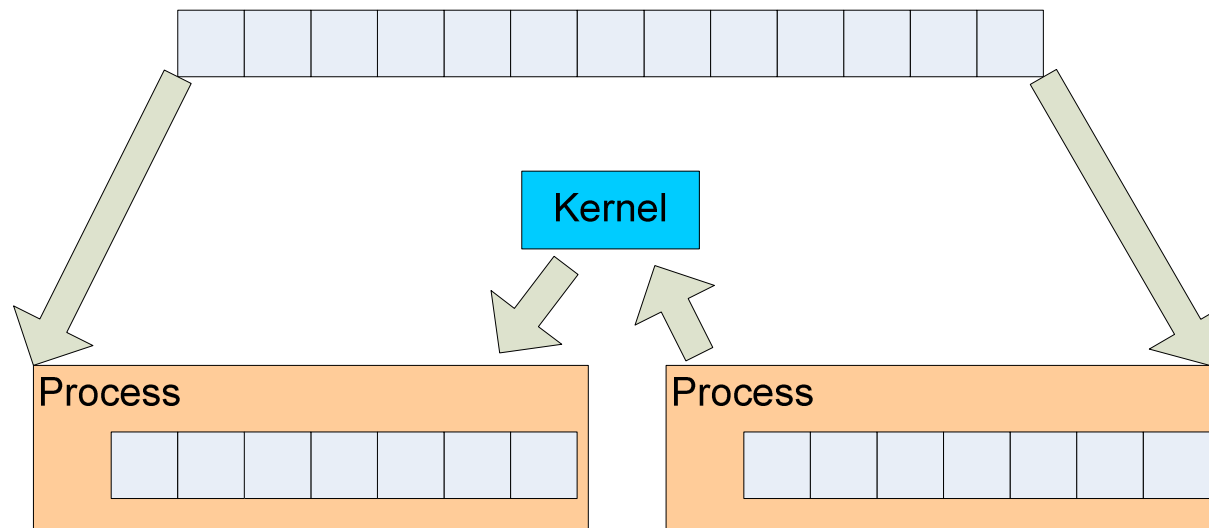
Lutz Roeder's .NET Reflector

www.aisto.com/roeder/dotnet



Reading Memory – The Issue

- The kernel allocates memory to each process
- The kernel allows one process to access another's memory



Reading Memory – Steps to Take



O-ISC '07
Ohio Information Security Conference

- Run under least privilege
- Control access to the system
- Don't load information if you don't need it!
(select * from user to get an email address)
- Scrub sensitive data before releasing memory. (remember not all memory types can be scrubbed)
- Check with operating system vendors on isolation options
- Tools to find
 - Memory debuggers

Reading Memory References



Installing Debugging Tools

<http://www.microsoft.com/whdc/devtools/debugging/installx86.msp>

Debugging Tools and Symbols - Resources

<http://www.microsoft.com/whdc/devtools/debugging/resources.msp>

Windows Debugging Tools for Use with Visual Basic

<http://support.microsoft.com/default.aspx?scid=kb;en-us;104156>

Traversing the gc heap (and introducing PSSCOR.DLL)

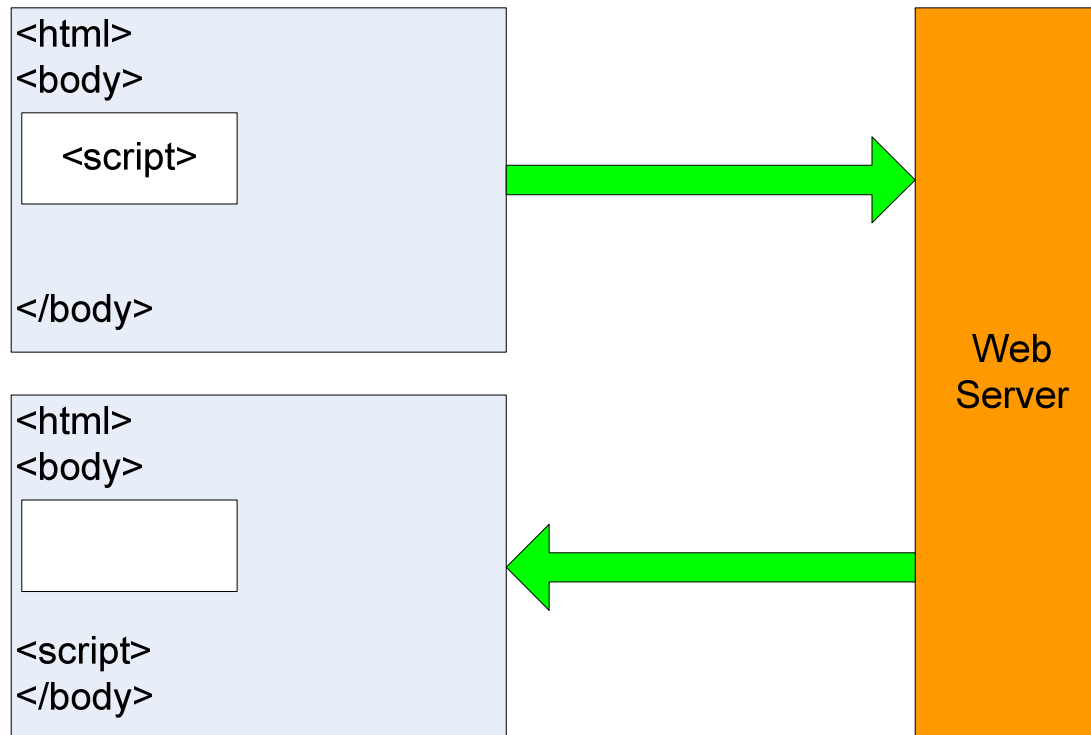
<http://blogs.msdn.com/mvstanton/archive/2004/04/05/108023.aspx>

Solaris Containers Consolidating Servers and Applications

<http://www.sun.com/software/solaris/howtoguides/containersLowRes.jsp>

XSS Injection – The Issue

- Script gets injected as it was part of the original page Web server



XSS Injection – Steps to Take



- Check all input
 - Users
 - Outside systems
- ASP.NET 1.1 and greater should use the built in checker
- Build your own checker (remember the scripts don't have to start with <script)
- Tools (Can be destructive!!)
 - Hailstorm
 - WebInspect

XSS References



When Output Turns Bad: Cross-Site Scripting Explained

<http://msdn2.microsoft.com/en-us/library/ms972823.aspx>

Cross Site Scripting Explained

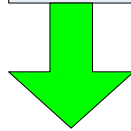
<http://www.linuxsecurity.com/content/view/115087/65/>



SQL Injection – The Issue

- Building the SQL statement to execute dynamically allows users to alter the statement to run.

Enter a location



“Andy, go to the” + Store + “.”

SQL Injection – Steps to Take



- Check your input
- Use stored procedures
- Use parameterized queries
- Control your string concatenation
(remember string concatenation in a stored procedure is still dangerous)
- Tools (Can be destructive!!)
 - Hailstorm
 - WebInspect

SQL Injection References



SQL Injection

<http://msdn2.microsoft.com/en-us/library/ms161953.aspx>

Advanced SQL Injection In SQL Server Applications

http://www.nextgenss.com/papers/advanced_sql_injection.pdf

(more) Advanced SQL Injection

http://www.nextgenss.com/papers/more_advanced_sql_injection.pdf

Questions & Answers

Session Evaluation Form



- Please fill out the form
- ... after completing the form, please leave it on the table as you leave the room