



NSA Center for Assured Software

Information Security And Privacy Board

March 21, 2006



Software Assurance Definition

DoD Software Assurance Initiative

DoD Software Assurance Tiger Team

- **The level of confidence that software is free of exploitable vulnerabilities, either intentionally designed into the software or accidentally inserted**
- **And that the software functions in a manner as expected.**



Problem Statement (1)

“The ubiquity of software and its development and usage without consistent engineering, has resulted in ad hoc management and mitigation efforts in a race to protect systems against breaches”

NII Sponsored

Software Assurance Tiger Team



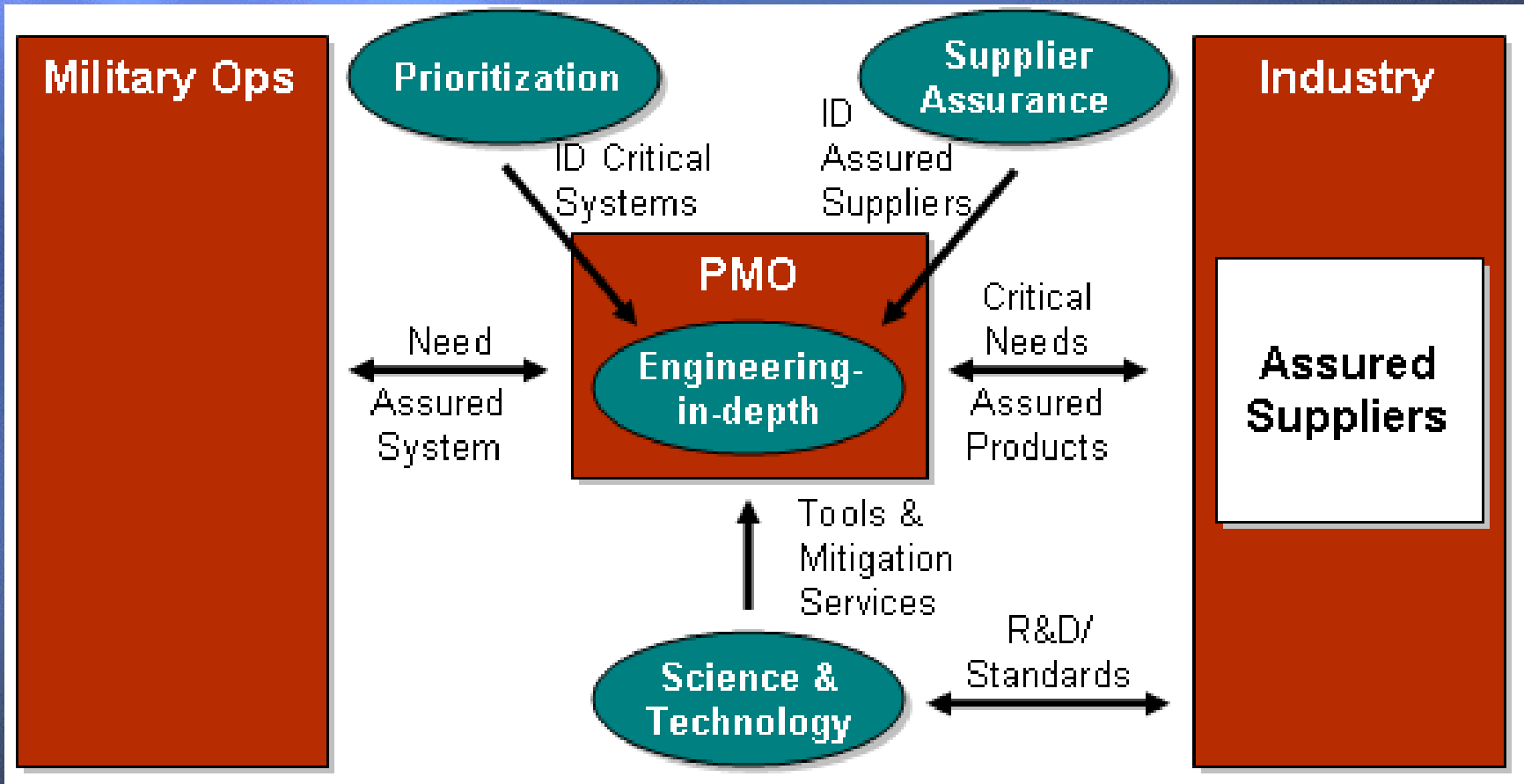
Problem Statement (2)

There's too much software

There's too little assurance



DoD SwA CONOPS: Interacting Processes





Science & Technology

- **Provide software evaluation services**
- **Use tools to detect vulnerabilities**
- **Coordinate DoD R&D for vulnerability detection and mitigation**
- **Work with industry to develop standards/solutions**
- **Recommended a DoD Executive Agent for Software Vulnerability Mitigation and Discovery**
 - **Establish a DoD Center for Assured Software**



NSA Center for Assured Software (CAS)

- **Stood up in November, 2005**
- **A Focal Point for Software Assurance (SwA) Issues with the following objectives:**
 - **Partner with our customers, government, the private sector and academia to identify SwA Issues and resolutions**
 - **Develop and utilize tools and methods to analyze the trustworthiness of software**



NSA Center for Assured Software (CAS) (cont)

- Objectives (cont)
 - Evaluate mission critical components
 - Establish/Identify software standards and practices to increase the availability of assured software products



CAS “domain of operation”

Role of Formal Methods

Binary analysis tools/techniques

Source Code analysis tools/techniques

Developmental Processes

Static/Dynamic analysis

Product Evaluation

Requirements	Design	Implementation	Testing	Deploy	Maintenance
--------------	--------	----------------	---------	--------	-------------

Safe Language Standards

Development Tools/techniques



What we look like today...

NSA Center for Assured Software

Standards

Tools and Techniques

Outreach

Evaluations

NIAP

SwAE



Where we are working today ...

- **NIAP**
 - Fully operational
 - Beginning to address recommendations from the GAO and IDA NIAP review reports

- **Software Assurance Evaluations**
 - Are evaluating some specific software of interest to NSA in the context of a pilot
 - First report due in 30 days



Where we are working today (cont) ...

- A repeatable SwAE methodology based upon available tools
 - Involves a tools survey as well as incorporating lessons learned from our pilot
- Strategies for :
 - Public Software Assurance Standards participation
 - Internal NSA Software Assurance Standards and compliance
 - Outreach
 - High Assurance



Using Tools for to gain Confidence in Software



Measuring Software Assurance

- Looking for properties of software that are indicators of the assurance level
 - Degree of confidence that software will securely and appropriately perform its intended functions
 - Degree of confidence that software will not perform any unauthorized functions
 - Degree of confidence that software does not contain implementation flaws that could be exploited.



Measuring Software Assurance

Process Phases:

- **Acceptance**
- **Extraction/Inspection**
- **Analysis**
- **Meta-Analysis**
- **Reporting**



Acceptance

- Are there existing tools and techniques that address the software to be evaluated?
 - Platform/Machine Language
 - x86, Sparc, ARM, etc.
 - Source Language
 - C/C++, Java, Microcode, etc.
 - File Format
 - PE, ELF, ROM Image, etc.
 - Environment
 - Windows, Real-time O/S, Linux



Measuring Software Assurance

CAS: Identify and fill capability gaps

Phase Report Card:

- C+** • **Acceptance**
- **Extraction/Inspection**
- **Analysis**
- **Meta-Analysis**
- **Reporting**



Extraction/Inspection

- **Apply tools and techniques that extract relevant metadata from the software**
 - **Control Flow Graphs**
 - **Complexity Metrics**
 - **Module Dependencies**
 - **Disassembly/Decompilation**
 - **Functional Extraction**
 - **Instruction Effects Analysis**
 - **Identification of Code vs. Data**



Extraction/Inspection

- **Extraction/Inspection tools are the most sophisticated tools available today**
 - **Most academic and commercial research and development is in this area**
 - **Much of the research is driven by the need to port legacy applications to newer platforms and binary formats**



Extraction/Inspection

- **Extraction/Inspection tools have complex output**
 - Use requires a high level of training
- **Tool results create the environment for analysis, but in most cases only indirectly indicate assurance**
- **Integration of extraction/inspection tools with analysis tools is poor**
 - Metadata formats are typically proprietary with specialized programming interfaces

Sample tool output ...



Extraction/Inspection

IDA - C:\Documents and Settings\My Documents\Projects\Software Assurance Tools and Techniques\calculator.exe

File Edit Jump Search View Debugger Options Windows Help

IDA View-A Hex View-A Exports Imports Names Functions Strings

IDA View-A

```
.text:08049339 loc_8049339: ; CODE XREF  
.text:08049339 sub_8049339  
.text:08049339 cmp [ebp+var_2A], 0  
.text:08049339 jnz short loc_8049342  
.text:08049340 jmp short loc_8049398  
.text:08049342  
.text:08049342 loc_8049342: movzx eax, [ebp+var_2A] ; CODE XREF  
.text:08049342 sub_8049342  
.text:08049344 cmp eax, 0FFFFFFh  
.text:08049344 jz short loc_804934E  
.text:0804934C jmp short loc_8049339  
.text:0804934E  
.text:0804934E loc_804934E: lea eax, [ebp+var_28] ; CODE XREF  
.text:0804934E sub_804934E  
.text:08049351 mov mov [esp+48h+var_48], eax  
.text:08049354 call sub_80493EE  
.text:08049359  
.text:08049359 loc_8049359: lea eax, [ebp+var_28] ; CODE XREF  
.text:08049359 sub_8049359  
.text:08049364 mov mov [esp+48h+var_48], eax  
.text:08049364 call sub_804934E  
.text:08049366 cmp [ebp+var_850] = dwd  
.text:08049366 jz short var_83C = dwd  
.text:08049366 lea eax, var_838 = dwd  
.text:0804936F mov [esp+var_828] = dwd  
.text:08049372 call sub_8var_818 = dwd  
.text:08049374 jmp short var_18 = dwd  
.text:0804937C mov [ebp+arg_0] = dwd  
.text:0804937C push mov
```

Strings window

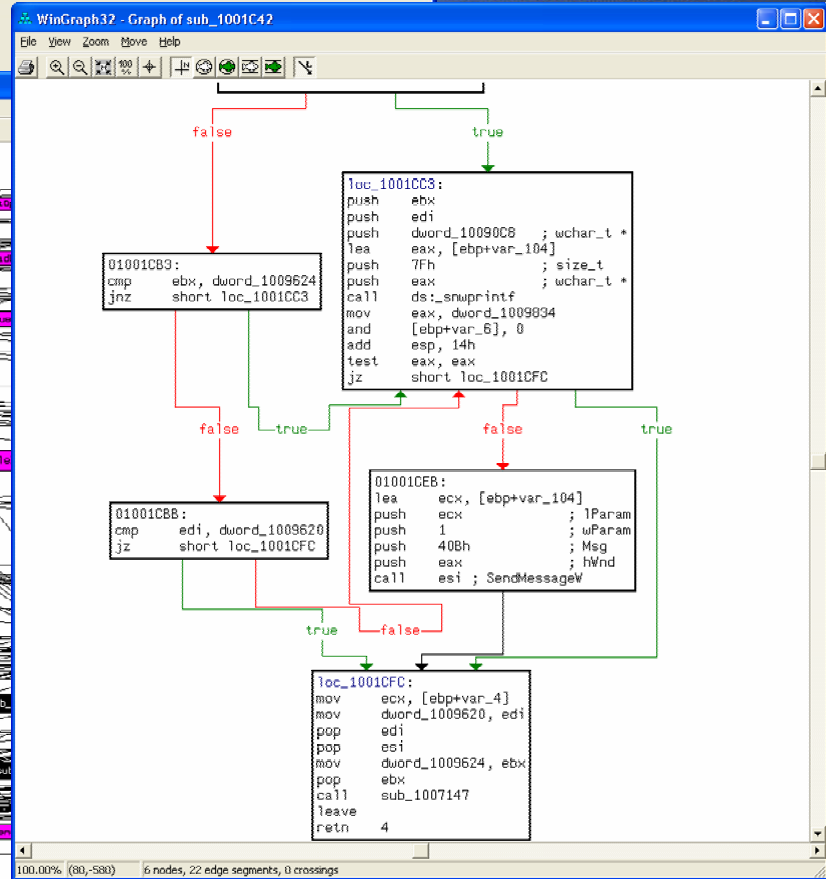
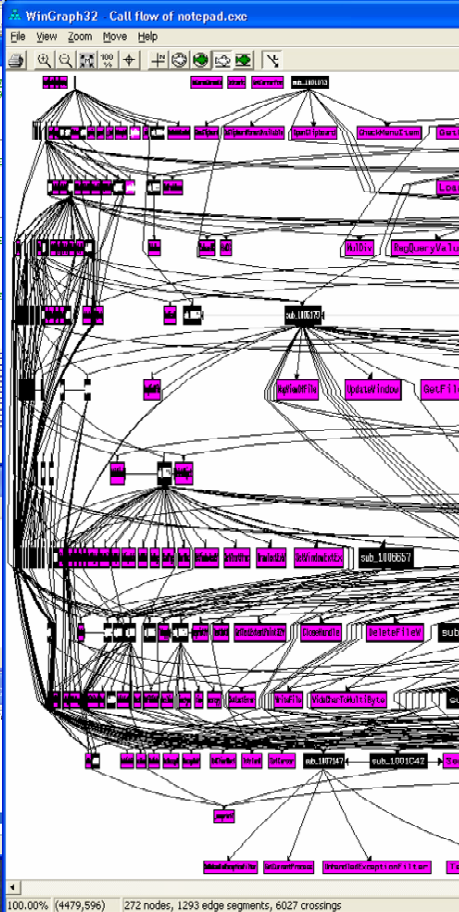
Address	Length	T...	String
..rodata...	0000000D	C	Equation :
..rodata...	0000000D	C	Processing:
..rodata...	0000000C	C	Processing:
..rodata...	00000027	C	Division by zero, setting factor to 1!
..rodata...	00000036	C	The following operation has not been implemented yet.
..rodata...	0000000D	C	Result :
..rodata...	00000023	C	You have entered a wrong infix equation!

Line 9 of 66

Exports Imports

File 'C:\Documents and Settings\My Documents\Projects\Software Assurance Tools and Techniques\calculator.exe'
Compiling file 'C:\Program Files\IDA\idc\onload.idc'...
EXECUTING FUNCTION 'main'...
Compiling file 'C:\Program Files\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analyzing the input file...
You may start to explore the input file right now.
The initial autoanalysis is finished.
.text:0804934F: Can't find name (hint: use manual arg)
.text:0804934F: Can't find name (hint: use manual arg)

AU: idle Down Disk: 46GB 0000137A 0804937A: sub_80491C4+1B6





Extraction/Inspection

untitled cfgvgraph2

Graph Edit Queries Go Tools Window Help

untitled...

src/ftpd.c

```
File Edit Functions Queries Go T
ftpd.c in.h access.c domain.c timeout.c
(void) signal(SIGALRM, dr
alarm(timeout data);
socket_ In Function send_data
}
transflag =
if (ferror
goto fi
goto da
draconian_F
alarm(0);
reply(226, "transrer complete
#ifdef TRANSFER_COUNT
if (retrieve_is_data) {
file_count_total++;
file_count_out++;
}
xfer_count_total++;
```

Path Explorer - wu-ftp-2.6(1)

Path Search Elision Navigation Help

Elide Unelide All

Skip to Next actual-in Step Mode Visible

Seq #	D	R	I	State	Kind	Program Point
2230	3			s1	exit	getpid exit
2236	3			s1	entry	... fctl entry point
2248	3			s1	exit	... fctl exit
2249	2			s1	actual-out	Return value : fctl\$result72
2250	2			s1	control-point	fctl\$result72 == -1
2251	2			s1	control-point	RootDirectory != (void *)0
2252	2			s1	call-site	initialize_dns()
2253	2			s1	actual-in	\$param_1 = &his_addr in call initialize_dr
2254	3		✓	s1	entry	initialize_dns entry point

Ready

Control Predecessors: >

Control Successors: >

CFG Predecessors: >

CFG Successors: >



Extraction/Inspection

The screenshot displays a security analysis tool interface with three main panels:

- Top Panel (Vulnerability Assessment):** Shows a table of vulnerabilities for 'Project WebStore'.

Classification	Severity	Type	Method
Vulnerability	High	Injection SQL	rbp.webs
Vulnerability	High	Injection SQL	rbp.webs
Vulnerability	High	Validation.EncodingRequired	rbp.webs
Vulnerability	High	Validation.EncodingRequired	rbp.webs
Vulnerability	High	Validation.Required	rbp.webs
Vulnerability	High	Validation.Required	rbp.webs
Vulnerability	High	Validation.Required	rbp.webs
Vulnerability	High	Validation.Required	rbp.webs
Vulnerability	High	Validation.Required	rbp.webs
Vulnerability	High	Validation.Required	rbp.webs
- Bottom Left Panel (Smart Trace):** Shows the execution flow of a request. The **Input Stack** includes 'WebStore.jsp.cart.Checkout_jsp_jspService'. The **Output Stack** includes 'WebStore.jsp.cart.Checkout_jsp_jspService', 'WebStore.orders.Orders.insert', and 'nbp.webstore.orders.Order.insert'. The **Data Flow** section shows code snippets like 'new java.lang.StringBuffer.append(insertSQL)' and 'insertSQL = new java.lang.StringBuffer.append(insertSQL)'.
- Right Panel (inSight Architect):** Displays a class hierarchy diagram for 'CLASS BootLoader'. The diagram shows relationships between various classes, including 'ARCH_LIST', 'ARCH_PA_RISC', 'ARCH_PPC', 'ARCH_SPARC', 'ARCH_X86', 'OS_AIX', 'OS_HPUX', 'OS_LINUX', 'OS_LIST', 'OS_MACOSX', 'OS_QNX', 'OS_SOLARIS', 'OS_UNKNOWN', 'OS_WIN32', 'PI_BOOT', 'WS_CARBON', 'WS_GTK', 'WS_LIST', 'WS_MACOS', 'WS_PHOTO...', 'getCommand...', 'getOSArch', 'getWS', 'knownOSAr...', 'knownOSVa...', 'shutdown', and 'startup'. A context menu is open over the 'BootLoader' class, showing options like 'Show Flowchart', 'Show Definition', 'Show Usage', 'Show Messaging', 'Show Inheritance', 'Show Superclass', 'Show Attributes', and 'Show Annotations'.



Extraction/Inspection

RSM Wizard 1.10

File Edit Action Help

Guided Process Steps

? Free 1 - Load or Name Solution 2 - Choose or Modify Files 3 - Load or Name Output File 4 - Select/Create Reports 5 - Execute RSM

Selection Tree of Path or Files

Acquisition Mode Path

C:\Project Release 1.1

h,c,cpp,java

temp,tmp,test

Set Path Path To List Acquire Files

C:\Project Release 1.1

- LongContextBlock.c
- Remove1LineComment.c
- RemoveFunction.c
- add1LineComment.c
- AddFunction.c
- blockmove.c
- ContextLocComment.c
- LineSwap.c

RSM Input File List

Count 9 Append ? Load

File List Baseline 1.1.lst

C:\Project Release 1.1\LongContextBlock.c

C:\Project Release 1.1\Remove1LineComment.c

C:\Project Release 1.1\RemoveFunction.c

C:\Project Release 1.1\add1LineComment.c

C:\Project Release 1.1\AddFunction.c

C:\Project Release 1.1\blockmove.c

C:\Project Release 1.1\ContextLocComment.c

C:\Project Release 1.1\LineSwap.c

C:\Project Release 1.1\HTTPSoapClient.java

RSM Command Line

Auto -H -O'F:\Documents and Settings\m2.M2SHAR

Dependency Walker - [notepad.exe]

File Edit View Options Profile Window Help

NOTEPAD.EXE

- COMPLG32.DLL
- SHLWAPI.DLL
- MSWRT.DLL
- GD32.DLL
- KERNEL32.DLL
- USER32.DLL
- ADVAPI32.DLL
- OLE32.DLL
- APPHELP.DLL
- NTDLL.DLL
- KERNEL32.DLL
- SHLWAPI.DLL
- USER32.DLL
- YESHONUI.DLL
- HLANG.DLL
- MSWRT.DLL
- KERNEL32.DLL
- USER32.DLL
- GD32.DLL
- ADVAPI32.DLL
- OLE32.DLL

Pt	Ordinal	Hint	Function	Entry Point
	N/A	3 (0x0003)	ChooseFontW	0x763CC4A9
	N/A	4 (0x0004)	CommDlgExtendedError	0x763C00CE
	N/A	6 (0x0006)	FindTextW	0x763C0B96
	N/A	8 (0x0008)	GetFileTitleW	0x763B1986
	N/A	10 (0x000A)	GetOpenFileNameW	0x763C7C65
	N/A	12 (0x000C)	GetSaveFileNameW	0x763C7CF3
	N/A	15 (0x000F)	PageSetupDlgW	0x763D40D6
	N/A	18 (0x0012)	PrintDlgExW	0x763D9D29
	N/A	21 (0x0015)	ReplaceTextW	0x763C86CA

F	Ordinal	Hint	Function	Entry Point
	100 (0x0064)	N/A	N/A	0x0001BCE0
	101 (0x0065)	0 (0x0000)	ChooseColorA	0x0000E0EE
	102 (0x0066)	1 (0x0001)	ChooseColorW	0x0000FF7F
	103 (0x0067)	2 (0x0002)	ChooseFontA	0x0001C289
	104 (0x0068)	3 (0x0003)	ChooseFontW	0x0001C4A9
	105 (0x0069)	4 (0x0004)	CommDlgExtendedError	0x000100CE
	106 (0x006A)	5 (0x0005)	FindTextA	0x0001067C
	107 (0x006B)	6 (0x0006)	FindTextW	0x00010896
	108 (0x006C)	7 (0x0007)	GetFileTitleA	0x00002533
	109 (0x006D)	8 (0x0008)	GetFileTitleW	0x00001986

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size	Load Order	File Ver	Product Ver	Image Ver
RASMAN.DLL	08/03/2004 11:56p	08/04/2004 2:56a	61,440	A	0x0001A747	0x0001A747	x86	GUI	CV	0x76E90000	Unknown	0x00012000	Not Loaded	5.1.2600.2180	5.1.2600.2180	5.1
REGAPI.DLL	08/03/2004 11:56p	08/04/2004 2:56a	49,664	A	0x00018E28	0x00018E28	x86	Console	CV	0x76B0C000	Unknown	0x0000F000	Not Loaded	5.1.2600.2180	5.1.2600.2180	5.1
RTLUTILS.DLL	08/03/2004 11:56p	08/04/2004 2:56a	44,032	A	0x000121E6	0x000121E6	x86	Console	CV	0x76E00000	Unknown	0x0000E000	Not Loaded	5.1.2600.2180	5.1.2600.2180	5.1
SAMLIB.DLL	08/03/2004 11:56p	08/04/2004 2:56a	64,000	A	0x00019C51	0x00019C51	x86	Console	CV	0x718F0000	Unknown	0x00013000	Not Loaded	5.1.2600.2180	5.1.2600.2180	5.1
SECCL.DLL	08/03/2004 11:56p	08/04/2004 2:56a	180,224	A	0x0003281D	0x0003281D	x86	Console	CV	0x74410000	Unknown	0x0002E000	Not Loaded	5.1.2600.2180	5.1.2600.2180	5.1
SECUR32.DLL	08/03/2004 11:56p	08/04/2004 2:56a	55,808	A	0x0001A281	0x0001A281	x86	Console	CV	0x77FE0000	Unknown	0x00011000	Not Loaded	5.1.2600.2180	5.1.2600.2180	5.1
SETUIWAPI.DLL	08/03/2004 11:56p	08/04/2004 2:56a	983,552	A	0x000F5968	0x000F5968	x86	GUI	CV	0x77920000	Unknown	0x000F3000	Not Loaded	5.1.2600.2180	5.1.2600.2180	5.1
SHDOCVW.DLL	08/03/2004 11:56p	08/04/2004 2:56a	1,403,264	A	0x0016F41D	0x0016F41D	x86	GUI	CV	0x77760000	Unknown	0x0016C000	Not Loaded	6.0.2900.2180	6.0.2900.2180	5.1
SHSVC.SYS	08/03/2004 11:56p	08/04/2004 2:56a	134,656	A	0x00025718	0x00025718	x86	GUI	CV	0x776E0000	Unknown	0x00023000	Not Loaded	6.0.2900.2180	6.0.2900.2180	5.1
TAPI32.DLL	08/03/2004 11:56p	08/04/2004 2:56a	181,760	A	0x0003736D	0x0003736D	x86	GUI	CV	0x76E80000	Unknown	0x0002F000	Not Loaded	5.1.2600.2180	5.1.2600.2180	5.1
URLMON.DLL	08/03/2004 11:56p	08/04/2004 2:56a	601,088	A	0x0009E7C8	0x0009E7C8	x86	GUI	CV	0x77260000	Unknown	0x0009C000	Not Loaded	6.0.2900.2180	6.0.2900.2180	5.1
USERENV.DLL	08/03/2004 11:56p	08/04/2004 2:56a	723,456	A	0x000867EA	0x000867EA	x86	GUI	CV	0x769C0000	Unknown	0x000B3000	Not Loaded	5.1.2600.2180	5.1.2600.2180	5.1
USP10.DLL	08/03/2004 11:56p	08/04/2004 2:56a	406,528	A	0x000656C9	0x000656C9	x86	GUI	CV	0x74D90000	Unknown	0x00058000	Not Loaded	1.420.2600.2180	1.420.2600.2180	5.1
UTILDL.DLL	03/19/2004 5:44p	08/18/2001 12:36a	25,600	A	0x0000D091	0x0000D091	x86	Console	PDB	0x5AD80000	Unknown	0x00000000	Not Loaded	5.1.2600.0	5.1.2600.0	5.1
VERSION.DLL	08/03/2004 11:56p	08/04/2004 2:56a	218,240	A	0x0003E638	0x0003E638	x86	GUI	CV	0x5AD70000	Unknown	0x00038000	Not Loaded	6.0.2900.2180	6.0.2900.2180	5.1
UXTHROW.DLL	08/03/2004 11:56p	08/04/2004 2:56a	18,944	A	0x00011078	0x00011078	x86	GUI	CV	0x77C00000	Unknown	0x00000000	Not Loaded	5.1.2600.2180	5.1.2600.2180	5.1
WS2TQPL.DLL	03/19/2004 5:44p	08/18/2001 12:33a	22,016	A	0x00014769	0x00014769	x86	Console	PDB	0x71F40000	Unknown	0x00009000	Not Loaded	5.1.2600.0	5.1.2600.0	5.1
WINHTTP.DLL	08/03/2004 11:56p	08/04/2004 2:57a	351,232	A	0x00055D26	0x00055D26	x86	GUI	CV	0x4D4F0000	Unknown	0x00058000	Not Loaded	5.1.2600.2180	5.1.2600.2180	5.1
WININET.DLL	08/03/2004 11:56p	08/04/2004 2:57a	656,384	A	0x000A248D	0x000A248D	x86	GUI	CV	0x71800000	Unknown	0x000A6000	Not Loaded	6.0.2900.2180	6.0.2900.2180	5.1
WINSRV.DLL	08/03/2004 11:56p	08/04/2004 2:57a	372,128	A	0x0003200A	0x0003200A	x86	GUI	CV	0x76E00000	Unknown	0x00030000	Not Loaded	5.1.2600.2180	5.1.2600.2180	5.1

Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

For Help, press F1



Measuring Software Assurance

Phase Report Card:

- C+** • **Acceptance**
- B+** • **Extraction/Inspection**
- **Analysis**
- **Meta-Analysis**
- **Reporting**

CAS: Identify and fill capability gaps

CAS: Foster integration and promote further research



Analysis

- Apply tools and techniques that query the metadata for properties or indicators of assurance
 - Existence of Buffer Overflows
 - Improper Memory Management/Object Reuse
 - Insecure Storage of Cryptographic Keys
 - Lack of Authentication
 - Race conditions
 - Covert Channels
 - Unexpected Functionality



Analysis

- Existing analytical tools:
 - Relatively primitive
 - Typically tailored to a specific sets of bugs
 - Not easily modified to address new questions
 - Typically highly coupled to a particular extraction/inspection tool
 - Simple analytic capability carries with it the cost of sophisticated tool
 - Lots and lots of false positives



Analysis

- Analysts typically create small programs on the fly to answer specific questions
 - Custom tools generally aren't refined to cover all relevant cases
 - Limited distribution and support of tool
 - Tools themselves are not well-engineered or extensible
 - No integration into an overall evaluation methodology



Measuring Software Assurance

Phase Report Card:

- C+** • **Acceptance**
- B+** • **Extraction/Inspection**
- C-** • **Analysis**
- **Meta-Analysis**
- **Reporting**

CAS: Identify and fill capability gaps

CAS: Foster integration and promote further research

CAS: Generate quality tools, reduce false positives



Meta-Analysis

- Integrate output from multiple analytical tools and techniques to discern higher-order assurance indicators
 - Some tools may increase the confidence in the results from another tool
 - Use one tool to focus the analysis of a following tool or filter the results of a preceding tool
 - Independent indicators help rank results
 - Perform analytical tests not within the capability of any one tool



Meta-Analysis

- **No technological methodology currently exists that:**
 - **Leverages the strengths of multiple tools**
 - **Contains the technological “glue” to connect tools from different vendors**
 - **Models software assurance through a diverse set of direct and indirect indicators**
 - **Is repeatable, scalable, and well-documented**



Measuring Software Assurance

Phase Report Card:

- C+** • **Acceptance**
- B+** • **Extraction/Inspection**
- C-** • **Analysis**
- I** • **Meta-Analysis**
- **Reporting**

CAS: Identify and fill capability gaps

CAS: Foster integration and promote further research

CAS: Generate quality tools, reduce false positives

CAS: Weave tools into a scalable methodology



Reporting

- **Transform analytical results into comprehensible reports**
 - Ranked “raw” data for follow-on deep analysis
 - Comparative results for systems design decisions
 - Summary results linked to standardized evaluation criteria for use as part of a larger evaluation process
 - Formal evaluation report for technology-only evaluations
- Report formats are not currently defined



Measuring Software Assurance

Phase Report Card:

- C+** • **Acceptance**
- B+** • **Extraction/Inspection**
- C-** • **Analysis**
- I** • **Meta-Analysis**
- I** • **Reporting**

CAS: Identify and fill capability gaps

CAS: Foster integration and promote further research

CAS: Generate quality tools, reduce false positives

CAS: Weave tools into a scalable methodology

CAS: Define customer-focused report formats



Center for Assured Software

Kris Britton

TD, NSA Center for Assured Software

rkbritt@missi.ncsc.mil

410-854-4543