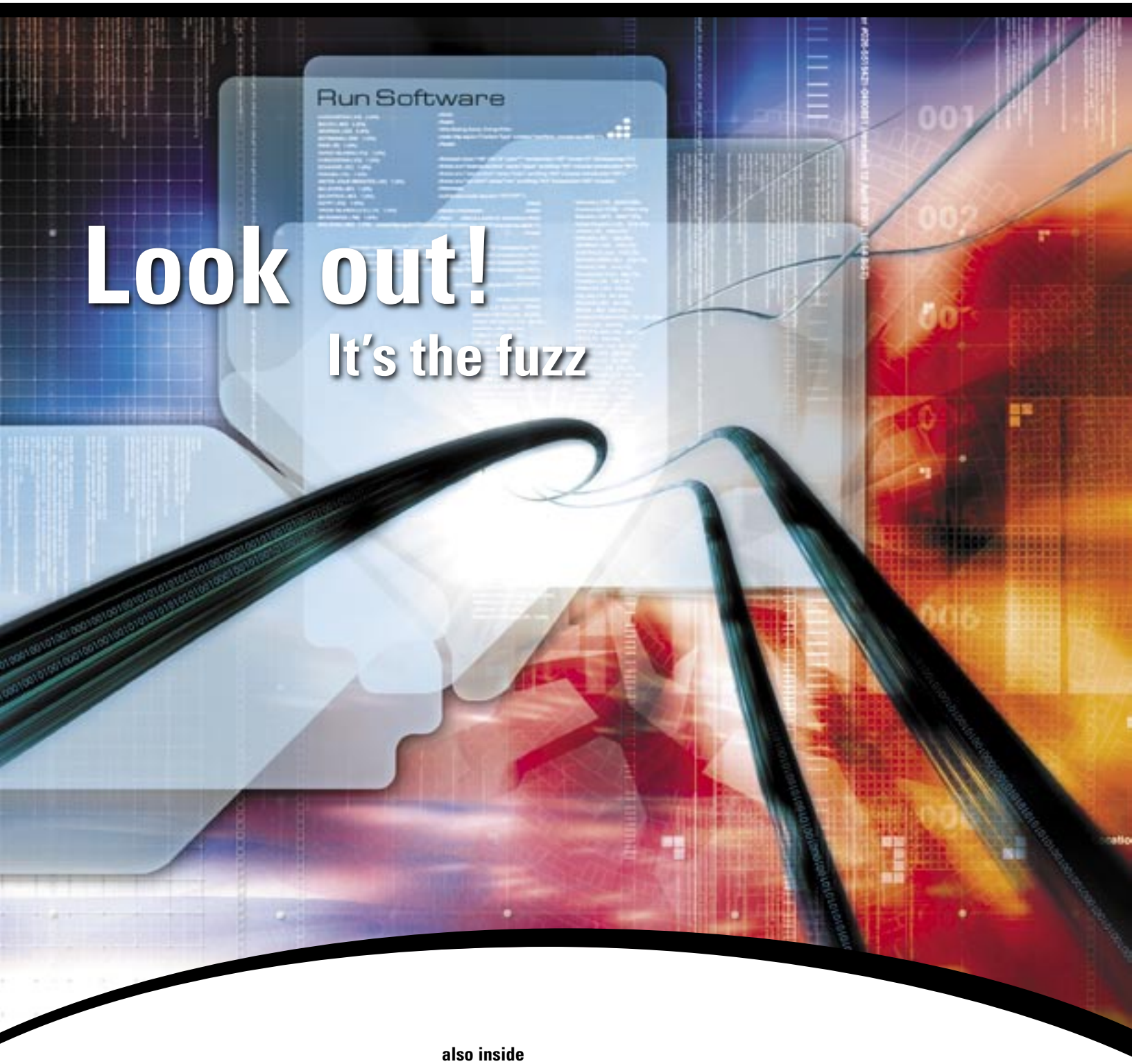
10/1

Volume 10 Number 1 • **Spring 2007**

IAnewsletter

The Newsletter for Information Assurance Technology Professionals



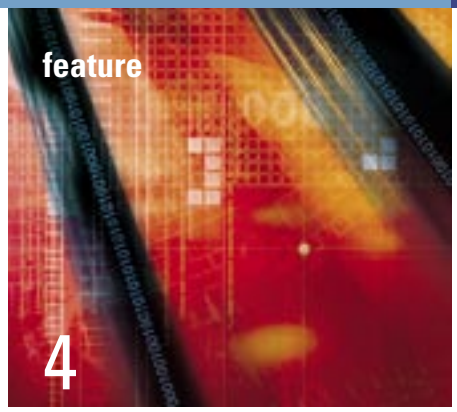
Look out!

It's the fuzz

IATAC

also inside

contents



About IATAC and the *IAnewsletter*
The *IAnewsletter* is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a Department of Defense (DoD) sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), and Director, Defense Research and Engineering (DDR&E).

Contents of the *IAnewsletter* are not necessarily the official views of or endorsed by the US Government, DoD, DTIC, or DDR&E. The mention of commercial products and/or does not imply endorsement by DoD or DDR&E.

Inquiries about IATAC capabilities, products, and services may be addressed to—

IATAC Director: Gene Tyler
Inquiry Services: Peggy O'Connor

***IAnewsletter* Staff**
Promotional Director: Christina P. McNemar
Creative Director: Ahnie Jenkins
Art Directors: Don Rowe
Copy Editor: Diane Ivone, Ahnie Jenkins
Designers: Brad Whitford, Dustin Hurt, Kacy Cummings
Editorial Board: Ronald Ritchey, Tara Shea, Gene Tyler, Buzz Walsh

***IAnewsletter* Article Submissions**
To submit your articles, notices, programs, or ideas for future issues, please visit http://iac.dtic.mil/iatac/IA_newsletter.html and download an "Article Instructions" packet.

***IAnewsletter* Address Changes/ Additions/Deletions**
To change, add, or delete your mailing or e-mail address (soft-copy receipt), please contact us at—

IATAC
Attn: Peggy O'Connor
13200 Woodland Park Road
Suite 6031
Herndon, VA 20171

Phone: 703/984-0775
Fax: 703/984-0773

E-mail: iatac@dtic.mil
URL: http://iac.dtic.mil/iatac

Deadlines for future Issues
Summer 2007 May 11th, 2007

Cover design: Dustin Hurt
Newsletter design: Bryn Farrar, Donald Rowe

in every issue

IATAC Chat

Gene Tyler, IATAC Director

2007—It's almost hard to believe it. By now, most of you are probably use to writing out the year, but for me it is still a bit of a novelty.

There was so much excitement for us in 2006, we were all eager to see what this year has in store for us in IATAC. So far, 2007 is proving to be just as, if not more, exciting than last year.

Once again, we started off the year attending the Department of Defense (DoD) Cyber Crime Conference, this year held in St. Louis, MO. This was the third consecutive year we've had the privilege to attend, exhibit, and have one of IATAC's Subject Matter Experts (SMEs) give a cyber legal presentation. Additionally, we had the opportunity to inform the community of IATAC's products and capabilities—outreach products like the *IAnewsletter*, IA Digest, IA/IO Events Scheduler, IA R&D Update, and State-of-the-Art Reports, SME database, inquiry services, Total Electronic Migration System (TEMS) database, other Information Analysis Centers (IAC), the Department of Defense, Director, Defense Research and Engineering (DDR&E) portal, and linkages to other organizations.

Our next big event in the IA community, was the 11th Annual Information Assurance Workshop (IAWS), held in Orlando, FL. Jointly hosted by DISA and NSA, it gave attendees the opportunity to discuss critical IA policies and issues facing the community today. The theme of the workshop was, "Operationalizing IA for the GIG," which brought a renewed focus on support to the warfighter. Key leaders from across DoD addressed challenges that confront today's IA professionals and also promoted cross-community collaboration to respond to those challenges. The tracks included various IA capability areas, strategic goals, and new this year was a Joint Staff hosted, warfighter track: "Operational IA: The Warfighter's Advantage." Our most recent IA event was one which was discussed in the *IAnewsletter*, Volume 9, Number 4, IATAC Chat. This Mid-Atlantic Information Security Forum was sponsored by The Institute for Applied Network Security (IANS), in conjunction with IATAC. While we have worked with the Institute in the past, this was our first, but certainly not last, opportunity to collaborate with them. Those of you who were able to attend the Forum, certainly know what an overwhelming success this collaboration effort was and that it extends IATAC's reach to the commercial world.

If you are reading this and wondering why it is you were not aware of any of these events, not to worry, our IO/IA Events Scheduler will keep you in the know. IATAC provides this calendar of events, which include both conferences and relevant training workshops, as one of our many free informational products. Plus, if you have a conference and/or workshop that you would like to be listed on our calendar, simply send an email to iatac@dtic.mil. To be added to the IA/IO Events Scheduler distribution, or to obtain any other IATAC product, you may email us, or if you prefer, an HTML version of this document is available at *http://iac.dtic.mil/iatac/IO_IA_Events_Scheduler.html.*

In addition to the numerous IA events we've participated in , we have also had several product developments as well. As you may already be aware of, the 5th edition of the *Firewalls Tools Report* was released at the end of 2006. We also have two other tools reports soon to be released; the first being the *Intrusion Detection Systems (IDS)* report, and the *Vulnerability Assessment* report. If you have not yet obtained your free copies, please email us or visit our website at *http://iac.dtic.mil/iatac/reports.html*. In addition to these tools reports, we also have State-of-the-Art-Reports (SOAR) in the works. One that is scheduled to be released in the next couple of months is the *Software Security Assurance SOAR*.

In this edition of the *IAnewsletter*, you will once again find some articles of interest. We are honored to have Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS) as our featured institution and several of CERIAS' professors as our collective SME, in this edition. The article, "Look out! It's the Fuzz!", gives the reader a basic overview of fuzzing. If you are unfamiliar with the term, this article will introduce you to fuzzing in a way that is easily understood. You will also find in this edition, another interesting article from our friends at the Air Force Institute of Technology (AFIT). "The Morphing of a Cyber Operations Curriculum at the Air Force Institute of Technology," provides a brief background of AFIT's involvement with the National Security Agency (NSA) sponsored Cyber Defense Exercise (CDX) and much more. These are just a couple of the thought provoking articles you will find in this edition of the *IAnewsletter*. ■

Look out! It's the fuzz!

by Matt Warnock

When you hear the term "fuzz," you may think of a delicious peach, or the guitar sound in early Cream or Jimi Hendrix albums, but software fuzzing is a relatively new software auditing technique responsible for finding many of the bugs and security vulnerabilities found in utilities, software applications, and network protocols. To understand what fuzzing is, we need to understand how fuzzing originated.

"It started on a dark and stormy night," is actually how the authors of the paper "An Empirical Study of the Reliability of Unix Utilities" [1] describe how they stumbled on the technique used in software fuzzing. This article is first in a series of software fuzzing papers from the University of Wisconsin over the past 15 years. The first paper tells the story of a user connecting to a server over a modem connection, and a storm causing noise on the phone line, and the noise creating random characters on the screen. This phenomenon is very understandable, but the most interesting aspect of it was that the random characters actually caused programs to crash and hang.

These four papers were instrumental in building the groundwork for software fuzzing. While these papers laid the ground work, now many research projects and utilities have been released to aid software auditors with testing. Several papers have been written on the subject, however it is still very new. The first article in the IATAC IA Digest to mention software fuzzing appeared on 6 Feb 06 entitled "The Future of Security Gets Fuzzy" [2] and shows how cutting edge this topic is.

Definition

Sending random characters to a program is the original and simplest form of software fuzzing—often called simple, or generic fuzzing. The random characters are sent via Standard Input (STDIN), in a command line utility. Characters could be standard American Standard Code for Information Interchange (ASCII), extended ASCII, control characters, null spaces, or any combination of these. When a certain combination of characters are sent, the program may crash, or exit without a proper exit code, hang, or loop indefinitely, or exit with a proper exit code. If the program crashes or hangs, the output of the fuzzer is reviewed to see exactly what combination caused the crash, and then program is analyzed to see what caused this. Simple fuzzing is very easy to perform as it does not require much prior knowledge of the application, however, it can take longer to find bugs and will not search every aspect of it. Intelligent fuzzing, usually required for advanced programs or network protocols, must take into consideration the structure of data and only fuzz certain portions, and leave the rest untouched. Things like checksums must be considered when creating random data, or the program may reject the data because it is not calculated properly. Programs that input files can also be audited by using file fuzzing, which inputs files with random data to see if they are loaded into the program. Even Application Program Interfaces (API) are vulnerable. API fuzzing sends random data to the common code used between programs to find bugs in reusable code. Also, web browsers, which accept HyperText Markup Language (HTML) data and translates it into visually understandable layouts, can be fuzzed. Malformed HTML data often leads to browser crashing.

Sending random characters to a program is the original and simplest form of software fuzzing—often called simple, or generic fuzzing

Fuzzing is used primarily as a software auditing technique, and is one of several auditing methods that includes reviewing source code (precompiled),

reviewing binary code (post-compiled), and reviewing API calls. Fuzzing allows an engineer to analyze software with minimal application specific knowledge. Although it is a technique that provides a capability to discover numerous bugs, it is very difficult to find every bug using this method alone. [3]

Types of Fuzzing

Unix Utilities

In their first paper, the researchers at the University of Wisconsin created the software auditing technique, and also tested their technique on several Unix command line utilities. Command line utilities usually input data through the STDIN via the Unix pipe. Their fuzzing test was run using the follow format: [1]

```
fuzz 100000 -o outfile | ptyjig vi
```

The tool that created the random data is called fuzz and the program to simulate the terminal is called ptyjig. This creates fuzzed data of maximum length 100,000 bytes, the output is saved as outfile, and the utility tested is vi, a text editor. To audit Unix command line utilities, very little needs to be known about the utility. Random data of varying characters and lengths is passed to the utility to test it. Because of this, the technique is very simple, but still very effective. The researchers implemented their auditing technique by using a tool to create random data and log it, and a tool to simulate the terminal. Also a script to automate the process was created. They tested 88 utilities in seven versions of Unix. Their techniques caused 24–33% of the utilities to crash or hang. They also tested the technique against network services, but were unable to crash any. The details of the results of their tests can be found in their original paper.

Five years after their original paper was published, researchers at the University of Wisconsin used their software auditing techniques to review the same Unix command lines with a few new operating systems, to include Linux. In this paper, "Fuzz Revisited: A re-examination of the Reliability of Unix Utilities and Services" [4] 80 utilities on nine versions of Unix were tested. Even after revealing many software bugs, the same bugs were found in the software tested five years later. In fact, on commercial versions of Unix, the 15–43% of the utilities crashed or hung. On the free versions of Unix, 9% had flaws, and GNU's Not Unix (GNU) style utilities had the lowest crash rate, at 6% of the GNU utilities tested.

Graphical User Interface (GUI)

Unix

The second University of Wisconsin paper also addressed programs for X Windows, the Graphical User Interface (GUI), for the Unix operating system. Now, in order to test X Windows applications, random data must be sent to the program via x-events, not STDIN. To do these tests, the researchers sent random, unformatted data to the X Windows programs, as well as random data sent as legal x-event streams. The random data caused 50% of X Windows applications to crash and the random data in the form of legal x-event streams caused another 25% to crash. They were not able to crash the X Server nor any network services. The details of the test results can be found in their original paper. This paper shows that fuzzing techniques are not limited to command line utilities, and now GUI applications, as well as other types of services, can be successfully audited.

Windows NT

Next in the series of papers from the University of Wisconsin is a paper [5] on using software fuzzing to test Windows NT (and Windows 2000) applications. This paper, published in 2000, details the results of testing their fuzzing techniques on Windows NT applications. Thirty GUI applications were tested including Microsoft Office 97 and 2000, Adobe Acrobat Reader, Eudora, Netscape 4.7, Visual C++ 6.0, Internet Explorer (IE) 4.0 and 5.0, as well as others. This time, valid keystroke and mouse events were simulated, as well as the Windows messages, or Win32 messages. Random Win32 messages were sent to the applica-

tion to see if they would crash or hang. The random keystroke and mouse events caused 21% of applications to crash, and 24% more hung. Also, when random Win32 events were sent to the applications, all applications hung or crashed. The researchers described this as a problem with the Win32 messaging system. The full results of their tests can be found in their original paper.

Apple Mac OS

To date, the last paper in the University of Wisconsin's series was on testing MacOS applications. [6] MacOS X is based on FreeBSD, and therefore contains many Unix-like command line tools, as well as GUI applications. In 2006, the researchers tested 135 command line tools, and 30 GUI applications, such as iChat and iTunes. They revealed that 7% of the command line tools crashed, however all but eight GUI applications crashed.

In this simple example, the first line is the original data packet. The second line is the fuzzing mask. In the mask, 0's are ignored and 1's are fuzzed. In this example, the IP source and destination are not fuzzed, the data is fuzzed, and the checksum must be recalculated. The packet is not entirely random, only portions of it.

Network fuzzing is any kind of fuzzing technique which tests software that is not on the local machine, or requires a network protocol. Fuzzing can test the network layer, such as Transmission Control Protocol/Internet Protocol (TCP/IP), or applications, such as File Transfer Protocol (FTP) servers. Leon Juranic's paper [7] details several bugs found in common FTP servers, and the techniques used to find the bugs. To test FTP, a valid network session must be created, and valid FTP commands must be sent. Other than this, random data is sent. For his tests, he uses Infigo FTPStress Fuzzer which allows you to select a valid username and password, and which FTP commands to use. While sending a valid FTP command, and a random data string, the utility was able to crash several FTP servers, such as GoldenFTPD, WarFTPD, and Argosoft FTP server. The details of the tests are available in the original paper.

Other network fuzzing attacks occur at the network layer [Internet Protocol (IP), Internet Control Message Protocol (ICMP)], and transport layer [Transmission Control Protocol (TCP), User Datagram Protocol (UDP)] and various applications (HTTP, *etc*). Other protocols, like Bluetooth can be fuzzed as well.

While the methods of finding software vulnerabilities varies greatly between the different fuzzing techniques, in the end, many of the same types of programming mistakes are found

Network Fuzzing

While "dumb fuzzing" randomly sends data to an application, intelligent fuzzing requires only certain portions of the data to be fuzzed. An example of this is when legal X-events were sent to an X application, but the data within the events is random. This type of technique is required when fuzzing network applications as well, otherwise, the packet may be rejected, and the data cannot be tested. For instance:

```
IP Source | Destination |  Checksum   | Data123456789
00000000 | 000000000 | recalculated  | 1111111111111
```

File Fuzzing

File fuzzing, or file format fuzzing, is a method of auditing software where files are opened and data is extracted. Many programs input data through files instead of STDIN, but this requires file formats to be standard or the program to be robust enough to detect and detail with anomalies. File fuzzers create files with some portions containing random data, or formats that are not exactly standard. These could be in binary format, or ASCII format. After creating the random file, they will execute the target program and open the new file in it. File fuzzing was used to find the Buffer Overrun in Joint Photographic Experts Group (JPEG) Processing (GDI+) in Microsoft Security Bulletin MS04-028. [8] It is a vulnerability found in other places, however was never exploited by a file.

Application Program Interfaces

Application Program Interfaces (API), are pieces of reusable code that is executed by many applications. Windows uses APIs, such as the Component Object Model (COM). Since APIs are reused by so many programs, they are both available to everyone, and also makes everyone susceptible if a vulnerability is found in an API. Since they are potentially vulnerable, APIs too can be fuzzed to find these vulnerabilities. API fuzzers will scan COM or ActiveX object interfaces.

Browser Crashing

Another method of fuzzing involves a form of file fuzzing called browser crashing. Web browsers, such as Firefox, Netscape, and IE, convert HTML code into viewable content. While HTML has been made standard by the World Wide Web Consortium (W3C), a web browser must be robust enough to detect and deal with non-standard and erroneous HTML input. Browser crashing creates random HTML content, which is correct enough for the browser to detect and parse it, but may contain anomalies that could crash the browser. All browsers have been susceptible to this kind of audit.

At the CanSec West Conference, H.D. Moore was able to write a simple program to mangle Cascading Style Sheets (CSS), and was able to test it and find bugs in IE at the conference. He was able to find over a dozen ways to crash the browser. In total, he's found hundreds of ways to crash IE and other browsers. [9]

Types of Bugs Found

While the methods of finding software vulnerabilities varies greatly between the different fuzzing techniques, in the end, many of the same types of programming mistakes are found. The University of Wisconsin researchers found the same bugs over and over as described below: [1]

Pointer/Array Errors

Pointer/array errors are caused when an array is created with finite length, however, the program tries to access data it thinks is in the array but actually exists outside of the array and causes the program to read unknown, and possibly malicious data. If the data after the array can be manipulated, the program could read an execute this data, causing unauthorized access. Another problem is with null pointers, where the pointer of the array is null. To make it more interesting, different systems interpret the null pointer in different ways. Some will crash, while others will incorrectly process the data.

Not Checking Return Codes

When a function is called, the function will return a value. Proper coding techniques require a check of the return code, however it is easy to assume the return value is correct and process it accordingly. If the function does return bad data, and the program assumes it to be correct, the program could crash.

Input Functions

When a program inputs data, it should check the bounds of the input string. If the function inputs data beyond the boundaries of an array, undesirable data can be read.

Sub-Processes

A program will sometimes call another program and allow access to itself. If the input from this other program contains errors or anomalies, this could cause it to crash or hang.

Signed Characters

ASCII characters are 7-bit, and are read into an array of signed 8-bit integers. If the array is not declared as signed, the value may be read as a negative number. Then a hash value will be computed differently and the index to the hash table will be out of range.

Race Conditions

A program often looks for a control command, such as the keystroke "Control-C" to break. If a program is designed to perform some other operation, such as return certain values to their original state, the program these tasks once it receives the control key. If between the "Control-C" and the cleanup process, another control key, like "Control-\" is received, the program will crash.

Undocumented Features

A network protocol follows a Request For Comment (RFC), which is a standard that the network protocol uses. If the protocol supports new or undocumented features, certain data may trigger these features creating undesired results. Also, these features may contain bugs that may not have been thoroughly tested.

Fuzzing Utilities

Open Source

- **AxMan**—A web-based ActiveX fuzzing engine
- **Blackops SMTP Fuzzing Tool**—Supports a variety of different SMTP commands and Transport Layer Security (TLS)
- **BlueTooth Stack Smasher (BSS)**—L2CAP layer fuzzer, distributed under GPL license
- **COMRaider**—COMRaider is a tool designed to fuzz COM Object Interfaces.
- **Dfuz**—A generic fuzzer
- **File Fuzz**—A graphical, Windows based file format fuzzing tool. FileFuzz was designed to automate the creation of abnormal file formats and the execution of applications handling these files. FileFuzz also has built in debugging capabilities to detect exceptions resulting from the fuzzed file formats.

- **Fuzz**—The original fuzzer developed by Dr. Barton Miller at my Alma Matter, the University of Wisconsin-Madison in 1990. Go badgers!
- **fuzzball2**—TCP/IP fuzzer
- **radius fuzzer**—C-based RADIUS fuzzer written by Thomas Biege
- **ip6sic**—Protocol stressor for IPv6
- **Mangle**—A fuzzer for generating odd HTML tags, it will also auto launch a browser.
- **PROTOS Project**—Software to fuzz Wireless Application Protocol (WAP), HTTP, Lightweight Directory Access Protocol (LDAP), Simple Network Management Protocol (SNMP), Session Initiation Protocol (SIP), and Internet Security Association and Key Management Protocol (ISAKMP)
- **Scratch**—A protocol fuzzer
- **SMUDGE**—A fault-injector for many different types of protocols and is written in the python language.
- **SPIKE**—Network protocol fuzzer
- **SPIKEFile**—Another file format fuzzer for attacking ELF (Linux) binaries from iDefense. Based off of SPIKE listed above.
- **SPIKE Proxy**—Web application fuzzer
- **Tag Brute Forcer**—Awesome fuzzer from Drew Copley at eEye for attacking all of those custom ActiveX applications. Used to find a bunch of nasty IE bugs, including some really hard to reach heap overflows.

Commercial

- **beSTORM**—Performs a comprehensive analysis, exposing security holes in your products during development and after release.
- **Hydra**—Hydra takes network fuzzing and protocol testing to the next level by corrupting traffic intercepted "on the wire," transparent to both the client and server under test.

Vulnerabilities Found by Fuzzing

(thanks to Ilja van Sprundel)

Protos

- OmniPCX Enterprise 5.0 Lx
- Cirpack Switches software version < 4.3c
- Cisco IP Phone Model 7940/7960 running SIP images prior to 4.2
- Cisco Routers running Cisco IOS 12.2T and 12.2 'X' trains
- Cisco PIX Firewall running software versions with SIP support, beginning with version 5.2(1) and up to, but not including versions 6.2(2), 6.1(4), 6.0(4) and 5.2(9)
- Sipc (version 1.74)
- Ingate Firewall < 3.1.3
- Ingate SIParator < 3.1.3
- All versions of SIP Express Router up to 0.8.9
- Mediatrix VoIP Access Devices and Gateways firmware < SIPv2.4
- Succession Communication Server 2000 (- Compact)
- adtran ATLAS 550, ATLAS 800 (Plus), ATLAS 810Plus, ATLAS 890, DSU IV ESP, ESU 120e, Express 5110, Express 5200, Express 5210, Express 6100
- DSU IQ, IQ 710, 1st GEN, IQ Probe, TSU IQ, TSU IQ RM, TSU IQ Plus, NetVanta 3200, ADVISION, N-Form, T-Watch, OSU 300, Express 6503,
- Smart 16 Controller, TSU ESP
- AdventNet Web NMS 2.3
- ADVA AG Optical Networking: FSP 3000, FSP 2000, FSP II, FSP I, FSP 1000, FSP 500, CELL-ACE, CELLACE-
- PLUS, FSP Element Manager,
- FSP Network Manager, CELL-SCOPE
- iPlanet Directory Server, version 5.0 Beta and versions up to and including 4.13
- IBM SecureWay V3.2.1 running under Solaris and Windows 2000
- Lotus Domino R5 Servers (Enterprise, Application, and Mail), prior to 5.0.7a
- Critical Path LiveContent Directory, version 8A.3
- Critical Path InJoin Directory Server, versions 3.0, 3.1, and 4.0
- Teamware Office for Windows NT and Solaris, prior to version 5.3ed1
- Qualcomm Eudora WorldMail for Windows NT, version 2
- Microsoft Exchange 5.5 prior to Q303448 and Exchange 2000 prior to Q303450
- Network Associates PGP Keyserver 7.0, prior to Hotfix 2
- Oracle Internet Directory, versions 2.1.1.x and 3.0.1
- OpenLDAP, 1.x prior to 1.2.12 and 2.x prior to 2.0.8

Smudge

- subversion
- shoutcast
- Sambar webserver 0.6 overflow in POST
- handling
- Ratbox IRCD < 1.2.3 overflow in newline
- handling
- Unexploitable overflows in IE browser
- DoS in Helix Server < 9.0.2
- Remote Crashes in Bad Blue server
- Mailman bugs
- Cute overflow in mod_security

SPIKE

- smb stuff
- dtlogin arbitrary free()
- windows remote rdp DoS
- RealServer ../ stack overflow
- Verde
- Mdaemon
- Xeneo Web Server
- ipSwitch

Mangleme

- IE
- maxilla / Netscape / Firefox
- opera
- lynx
- links
- safari

Mangle

- libmagic (used file)
- preview (osX pdf viewer)
- xpdf (hang, not a crash ...)
- mach-o loading

- qnx elf loader
- FreeBSD elf loading
- openoffice
- amp
- osX image loading (.dmg)
- libbfd (used objdump)
- libtiff (used tiff2pdf)
- xine
- OpenBSD elf loading (3.7 on a
- sparc)
- unixware 713 elf loading
- DragonFlyBSD elf loading
- solaris 10 elf loading
- cistron-radiusd
- linux ext2fs (2.4.29) image
- loading
- linux reiserfs (2.4.29) image
- loading
- linux jfs (2.4.29) image loading
- linux xfs (2.4.29) image loading
- macromedia flash parsing
- Totem 0.99.15.1
- Gnumeric
- Quicktime
- Mplayer
- Python byte interpreter
- Realplayer (10.0.6.776)
- Dvips
- Php 5.1.1
- IE 6
- OS X WebKit (used safari)

ircfuzz

- BitchX (1.1-final)
- mIRC (6.16)
- xchat (2.4.1)
- kvirc (3.2.0)
- ircii (ircii-20040820)
- eggdrop (1.6.17)
- epic-4 (2.2)
- ninja (1.5.9pre12)
- emech (2.8.5.1)
- Virc (2.0 rc5)
- TurboIRC (6)
- leafchat (1.761)
- iRC (0.16)
- conversation (2.14)
- colloquy (2.0 (2D16))
- snak (5.0.2)
- Ircle (3.1.2)
- ircat (2.0.3)
- darkbot (7f3)
- bersirc (2.2.13)
- Scrollz (1.9.5)
- IM2
- pirch98
- trillian (3.1)
- microsoft comic chat (2.5)
- icechat (5.50)
- centericq (4.20.0)
- uirc (1.3)
- weechat (0.1.3)
- rhapsody (0.25b)
- kmyirc (0.2.9)
- bnirc (0.2.9)
- bobot++ (2.1.8)
- kwirc (0.1.0)
- nwirc (0.7.8)
- kopete (0.9.2)

isic

- Logging vulnerability in Checkpoint
- Firewall-1 4.0
- IP Stack vulnerability in Checkpoint
- Firewall-1 4.0
- Panic of Gauntlet 5.5 Beta
- Lock up Gauntlet 5.5 Beta
- Frag DOS of Gauntlet 5.5 Beta
- Lock up of Gauntlet 5.0
- Remote exploit of Raptor 6.x

Conclusion

Software auditing will always be an important processing in software assurance. While fuzzing is an easy and effective way to audit software, it is only one of many tools. Fuzzing should be implemented along with code reviews. The University of Wisconsin researchers opened up the door to this type of software auditing by creating a technique still used by many fuzzers. Also, their continued research into GUIs on specific OS showed that fuzzing can be used in many different areas. Now, network, file, and API fuzzing are important auditing techniques. Many of the vulnerabilities discovered every week are done so through fuzzing or use fuzzing to aid in the discovery. Fuzzing still has the ability to expand, improve, and analyze more complicated software. While fuzzing is not the only software auditing technique available to developers and security professionals, it is a technique that is here to stay. ■

References

1. Miller, Barton P., "An Empirical Study of the Reliability of Unix Utilities", December 1990.
2. Seltzer, Larry, "The Future of Security Gets Fuzzy", *http://www.eweek.com/article2/0,1759,1914332,00.asp*, Feb 6, 2006.
3. Van Sprundel, Ilja, "Fuzzing: Breaking software in an automated fashion", December 8, 2005.
4. Miller, Barton, David Koski, Ravi Murthy, et al. "Fuzz Revisited: A Re-examination of the Reliability of UNIX Utilities and Services",
5. Forrester, Justin E., Barton P. Miller, "An Empirical Study of Robustness of Windows NT Applications Using Random Testing", July 27, 2000.
6. Miller, Barton, P., Gregory Cooksey, et al, "An Empirical Study of the Robustness of MacOS Applications Using Random Testing", July 20, 2006.
7. Juranic, Leon, "Using fuzzing to detect security vulnerabilities", April 25, 2006.
8. Sutton, Michael, Adam Green, "The Art of File Fuzzing", Blackhat.
9. Lemos, Robert, "Browser crashers warm to data fuzzing", April 13, 2006.

About the Author

Matt Warnock, CISSP, | is an Information Assurance Specialist with the Information Assurance Technology Analysis Center (IATAC). He graduated from Pennsylvania State University with a BS in Electrical Engineering, holds an Information Security Management Certificate from the University of Virginia, and is currently enrolled in a program for the MS degree in Telecommunications at George Mason University. His background includes assignments with the Defense Logistics Agency (DLA) in firewall and border-protection support. He may be reached at iatac@dtic.mil.

ESSG

by John Palumbo

This quarter I promised to describe the DoD Enterprise-wide Information Assurance (IA) and Computer Network Defense (CND) Solutions Steering Group (ESSG) process to help the reader understand all the steps involved from taking a "good idea" to being a useful tool for the enterprise. I feel that it will be helpful for readers to understand the basic process so they may actively and constructively participate in the process. The end goal for all of us, whether we are working within the ESSG or its sub-working groups is to provide the best selection of integrated tools to help defend the enterprise.

December ESSG Updates

The ESSG held a successful meeting from 12-14 December in Miami, FL. US Southern Command (USSOUTHCOM) hosted the meeting and provided outstanding support. We had several high level participants at the meeting to include Major General Spears, Deputy Commander. USSOUTHCOM; Rear Admiral Hight, Joint Task Force–Global Network Operations; Ms. Hallihan, Global Information Assurance Portfolio national Security Agency (GIAP/NSA); Mr. Hale, DISA; and Mr. Lentz, OSD(NII). In addition to the normal routine updates the ESSG made a few key decisions to included:

- Approval for Flying Squirrel, the wireless detection tool, to move to pilot stage.
- Update on the Host Based Security System (HBSS) and decision to extend the pilot until March 2007.
- Approval to push the Insider Threat–Detection Tool Acquisition from late FY07 to early FY08.
- Accelerate antivirus and anti-spyware procurement activities.

The ESSG

I had mentioned in the previous article that I would provide information on how the ESSG works. This quarter, I provide an overview of the process to include the ESSG proper and its sub-working groups and related activities.

At the heart of the ESSG are the voting members that contribute O-6 or equivalent representatives who are empowered to speak for their organizations' IA community. The voting members on the ESSG each have a single vote and consist of US Navy, US Air Force, US Army, US Marine Corps, Defense Information Systems Agency (DISA), the Defense-wide Information Assurance Program (DIAP), Joint Staff/J6 (Representing Combatant Command Issues), National Security Agency (NSA), Defense Intelligence Agency (DIA), US Joint Forces Command (USJFCOM). US Strategic Command (USSTRATCOM) and the Joint Task Force for Global Network Operations (JTF-GNO) co-chair the ESSG and provide a single combined vote in case of ties. These twelve seats help set the course of the enterprise solutions, validate requirements and pursue funding options to bring improved defense opportunities to the Global Information Grid (GIG).

The ESSG priorities are identified from several sources to include the CND Initial Capabilities Document (ICD), the Information Operations (IO) Roadmap, and other cornerstone documents. As well as these documents, the ESSG will also consider new threats to the enterprise such as Spyware and infrastructure necessities such as demilitarized zone (DMZ) protection/upgrades as they appear.

Once the priorities have been established, the ESSG looks to acquire funding. Often a multiple pronged approach, the DIAP provides the lead for searching for funds to secure the network. The DIAP has been successful in validating the needs and over the past several years has helped establish baseline funding to provide capabilities to a broad selection of needs. Early success for the ESSG came with the utilization of funding associated with the IO Roadmap that provided a substantial boost in the funding level of several key projects. Today the ESSG continues to gain funding for identified shortfalls that require solutions. Additionally, the GIG/GIAP has made the ESSG the execution and implementation arm for enterprise products that support the CND aspects of the GIAP portfolio. This

influx of funding has allowed the ESSG to continue key enterprise efforts in protecting the network.

Sub-Working Groups

When funding has been secured for a priority, USSTRATCOM develops a high level requirements document that provides the guidance necessary to the Technical Advisory Group (TAG). The TAG has representatives across DoD that provide technical guidance on the processing of a requirement. They conduct surveys of the available technology to determine if the commercial market has a solution or solutions that could adequately address DoD needs. The TAG will often times bring solution providers into Commercial-off-the-Shelf (COTS) and Government-off-the-Shelf (GOTS) demonstration days allowing the vendors both in industry and the government to show the technical capabilities they have to address the Department's needs. After reviewing the applicable products the TAG will narrow down the technical requirements, and then make a recommendation to the whole ESSG that a solution is mature enough to enter source selection if a material solution is required.

Once the ESSG approves the material solution course of action the Acquisition Working Group (AWG) becomes involved to lead the process. The AWG is chaired by Defense Information Systems Agency Program Executive Office Information Assurance Network Operations (DISA PEO IA/NetOps) which provides program management of the entire acquisition process. They ensure that requests for proposals are filled and the government has proper personnel and equipment to conduct technical testing of the solutions from the vendors. After a testing period and performance evaluation, the AWG will make a recommendation to the ESSG on the chosen solution. Once ratified by the ESSG, the AWG will then work with the DISA Program Manager to complete the acquisition. In most cases a pilot program will be set up to assist in the development of Tactics, Techniques, and Procedures (TTPs) and to smooth implementation procedures.

Assisting in the pilot and often times the establishment of help desk activities, the DISA Field Security Office (FSO) becomes an integral part of the ESSG process. The DISA FSO ensures close coordination at the technical level, often working with the vendor and fielding activity to ensure proper installation and problem resolution.

Running in parallel to the TAG and AWG, the Concept of Operations (CONOPS) Working Group (CWG) produces a CONOPS that can be used by the local managers. The CONOPS provides the information that managers require to integrate the new enterprise-wide tool into the network and how the tool is intended to operate and support, not only their level, but support the entire enterprise. Made up of representatives from all the voting members, the CWG is co-chaired by USJFCOM and the JTF-GNO. In addition to creating and coordinating the CONOPS, the CWG provide reviews and updates as upgrades and improvements are made to the fielded tools.

The last sub-working group of the ESSG is the CND Architecture Working Group (CAWG). The CAWG provides architecture products for the selected ESSG tools and integrates the enterprise-wide CND tools into the overall IA

> At the heart of the ESSG are the voting members that contribute O-6 or equivalent representatives who are empowered to speak for their organizations' IA community.

GIG architecture products. In addition, the CAWG leads the ESSG involvement for formulating a data strategy. This includes the development of meta-data standards and administration over their use and refinement.

Wrapping It Up

These processes have allowed the ESSG to bring several key products to bear in a relatively short period of time, not from the perspective of a single command or service, but for the entire enterprise. The true strength of the ESSG is provided by the voting members, willing to move past their traditional views to take positive actions in support of the entire enterprise. The ESSG annually conducts a realignment of the priorities for an upcoming fiscal year. These priorities are identified from several policy level documents such as the CND Initial Capabilities Document (ICD), the Information Operations (IO) Roadmap, and a multitude of Department of Defense Instructions and Manuals. In addition to the policy requirements, the ESSG voting members also look at immerging issues and threats from within their own constituency. Using these data points the voting members "rack and stack" the priorities that they will focus their efforts on in upcoming year.

ESSG email distribution should contact me for more information. Those holding a DoD Public Key Infrastructure (PKI) certificate may access the ESSG portal at *https://gesportal.DoD.mil/sites/DoD-ESSG/default.aspx*.

In the next issue of the *IAnewsletter*, I'll be bringing you a detailed report on the AWG and how they execute their ESSG responsibilities. ■

About the Author

John Palumbo | currently acts as coordinator for the ESSG. For the past 10 years he has supported both United States Strategic Command (USSTRATCOM) and United States Space Command (USSPACECOM) as an IA and Information Operations professional, both as a US Navy Officer and as a contractor. He earned his Certified Information Systems Security Professional (CISSP) certification in 2002 and holds a Master of Science in Information Technology Management from the Naval Postgraduate School, Monterey, CA

Letter to the Editor

Q ***"I've been reading several articles in your IA Digest related to "Service Oriented Architecture", could you please tell me a bit about it?"***

A While certainly not new, Service Oriented Architecture is undoubtedly one of the hottest topics for the IT professional. More commonly referred to as SOA, this is a software design approach in which an application requests one or more services from another application that provides similar services. In its most simplistic definition, a SOA is in effect a collection of services. Certainly we would all like to avoid having to recreate the wheel each time we needed a function performed; so, when a software system with similar capability already exists, SOA allows us to reuse that functionality. The intent of this architectural style is to achieve loose coupling among interacting software agents, thus requiring less interdependency. Loose coupling is the key to SOA and what distinguishes it from other architectures. The design allows internal and external business processes to be combined and recombined to support flexibility in business process execution.

A service is a specific, provided function, performed to achieve a desired result. Service Oriented Architectures must look at the technical components of service in two ways; first in term of its interoperability between the services, and secondly in the implementation of the actual service. Without both of these service oriented items acknowledged, SOA is impossible to achieve. Once the technical workings are defined, services can be combined and utilized by multiple users, all-the-while hiding the underlying implementation details. One other item to keep in mind is that the providers of these services must be able to publish information about them. This information must be accessible so consumers can look up the services they need and then retrieve the information they need about those services. For more information, please do not hesitate to contact us at iatac@dtic.mil. ■

CERIAS at Purdue University

by Ron Ritchey

CERIAS, the Center for Education and Research in Information Assurance and Security, is recognized as one of the world's foremost university centers for multidisciplinary research and education in information security. CERIAS, founded at Purdue University in 1998, addresses issues of privacy, biometrics, online trust, digital forensics, and identity management.

"Information assurance and security has never been exclusively a 'computer' problem. As other disciplines became involved it's astounding the contributions they brought to IA research," explained Dr. Eugene Spafford, [see profile, page 22] executive director and founder of the center and its predecessor, the Computer Operations, Audit and Security Technology (COAST) lab at Purdue. CERIAS has faculty from more than 20 academic disciplines involved in research and educational initiatives. CERIAS researchers combine their expertise in areas as diverse as ethics, public policy, law enforcement, digital rights management, education, linguistics, natural language processing, and economics as well as computing. Faculty members collaborate with industry and governmental agencies to conduct research into computer and network protection, e-commerce safety, cybercrime prevention and investigation, computer-based terrorism, and national defense.

There are currently more than 50 research projects being led by CERIAS faculty, staff, and graduate students. CERIAS research is conducted in eight areas of focus:

- **Incident Detection, Response, and Investigation**—How can system attacks be anticipated, identified, and mitigated? What are the appropriate technical, legal, and policy responses?
- **Cryptology and Rights Management**—How can the intended use, confidentiality, and integrity of information be assured?
- **Assurance Software and Architectures**—What tools and methods promote building software artifacts, servers, and networks that are resistant to attacks and failures?
- **Identification, Authentication, and Privacy**—Who is trying to gain access to your system and its information? What access can—and should—be allowed?
- **Risk Management, Policies, and Laws**—How do we balance investments in security and privacy to manage risk, protect assets, and promote trust?
- **Trusted Social and Human Interactions**—How does IT influence our interactions and how can more trustworthy IT affect them?
- **Security Awareness, Education, and Training**—How do we educate users, producers, designers, and purchasers of IT to choose wisely when it comes to security?

Shaping Future Policy

CERIAS faculty are among the national leaders working to establish industry standards and public policy. They serve as fellows and members of the editorial boards of most major information and computing-related organizations, including Institute of Electrical & Electronics Engineers (IEEE) and Association for Computing Machinery (ACM). Dr. Spafford also served on the President's Information Technology Advisory Committee (PITAC), which provided the President, Congress, and federal agencies with advice on maintaining the nation's preeminence in information technology.

The center partnered with MITRE to develop OVAL (Open Vulnerabilities and Assessment Language). OVAL allows users to check their systems for vulnerability, compliance, and configuration issues. OVAL currently contains more than 1,800 definitions for Windows, Linux, and Unix, all of which are free to download and implement. (See *http://oval.mitre.org/.)*

continued on page 23

CERIAS, Purdue University

by Ron Ritchey

Eighty faculty, from more than 20 different academic disciplines, conduct research with CERIAS. Here are a few of the CERIAS researchers who are making an impact in the future of IA.

Dr. Spafford
Executive Director, CERIAS
Professor, Department of Computer Science, and Electrical and Computer Engineering
Professor of Philosophy (courtesy)
Professor of Communication (courtesy)

Dr. Spafford is one of the most senior and recognized leaders in the field of computing. He has an ongoing record of accomplishments as a senior advisor and consultant on issues of security, cybercrime, and policy to a number of major companies, law enforcement organizations, and government agencies, including Microsoft, Intel, Unisys, the US Air Force, the National Security Agency, the GAO, the Federal Bureau of Investigation, the National Science Foundation, the Department of Energy, and two Presidents of the United States. He serves on a number of advisory and editorial boards, and has been honored several times for his writing, research, and teaching on issues of security and ethics.

Dr. Spafford's focus is currently on the design of forensic-friendly and secure-by-default computer systems. Additional information on Dr. Spafford and his research can be found at: *http://homes.cerias.purdue.edu/~spaf*

Edward J. Delp
The Silicon Valley Professor of Electrical and Computer Engineering and Professor of Biomedical Engineering

The falling costs and increasing availability of electronic devices has led to their widespread use by individuals, corporations, and governments. These devices, such as digital cameras, scanners, and printers, contain various sensors that generate data that is stored or transmitted to another device. Forensic techniques can be used to uniquely identify each device using the data it produces. This is different from simply securing the data because we are also authenticating the sensor that is creating the data.

Identification through forensic characterization means identifying the type of device, make, model, configuration, and other characteristics of the device based on observation of the data that the device produces. These characteristics that uniquely identify the device are called device signatures.

There are many scenarios in which it is useful to characterize a device. One use is to verify the source camera and authenticity of digital photographs in a court case. Another would be to identify a printer that was used to perform some illicit activity.

Using techniques we have developed, we can determine the source printer of a printed document. We can also determine whether a digital image was generated by a computer, digital still camera, or scanner and specifically which device in those three categories created it. Each of these techniques uses the "noise" characteristics of the device to identify the actual device used.

Additional information on Dr. Delp and his research can be found at: *http://cobweb.ecn.purdue.edu/~ace*

Mikhail "Mike" Atallah
Distinguished Professor of Computer Science
Professor of Electrical and Computer Engineering (courtesy)

Even though collaborative computing can yield substantial economic, social, and scientific benefits, a serious impediment to fully achieving that potential is a reluctance to share data, for fear of losing control over its subsequent dissemination and usage. An organization's most valuable and useful data is often proprietary/confidential, or the law may forbid its disclosure or regulate the form of that disclosure. We are developing security technologies that mitigate this problem, and that make possible the enforcement of the data owner's approved purposes for the data used in collaborative computing. These include techniques for cooperatively computing answers without revealing any private data, even though the computed answers depend on all the participants' private data. They also include computational outsourcing, where computationally weak entities use computationally powerful entities to carry out intensive computing tasks without revealing to them either their inputs or the computed answers. Our techniques do not require the use of a third party (whether trusted or untrusted), nor do they rely on any use of trusted software running on another party's machine. We have already designed protocols for doing this in the following problem domains:

- Access control and trust negotiations
- Approximate pattern matching and sequence comparisons
- Contract negotiations
- Collaborative benchmarking and forecasting
- Location-dependent query processing
- Credit checking
- Supply chain negotiations
- Electronic surveillance
- Intrusion detection
- Biometric comparisons

Additional information on Dr. Atallah and his research can be found at: *http://www.cs.purdue.edu/people/faculty/mja.*

Marcus K. Rogers
Associate Professor, Computer & Information Technology
CISSP, CCCI-Advanced
(Cyber Forensics Lab)

The cyber forensics lab at CERIAS has been very active in the development of software to assist law enforcement with contraband image investigations. The research team has released a beta version of the software that is now being used by approximately 85 agencies in six different countries. The software is designed to allow first responders to conduct a field examination in a forensically sound manner. A recent grant from the National Institute of Justice (NIJ) will allow us to add further functionality to this software.

The research team is also conducting follow-up research on iPod forensics. The study is aimed at updating previous research in this area by our team and will look at the newer versions of iPods that have been released (i.e., 5.0 & 5.5). The findings will be of interest to

law enforcement, private sector, and the intelligence community.

The third area of focus this year is in the domain of cellular phones. Several studies are underway that look at such issues as creating a national database of cellular OS characteristics, the feasibility of a hardware write blocker for cell phones, and on-scene triage tools for first responders dealing with cell phones.

Additional information on Dr. Rogers and his research can be found at: *http://homes.cerias.purdue.edu/~mkr*

Victor Raskin
Professor, English
Founder, Natural Language Processing (NLP) Laboratory

The ability for computational systems to understand natural language has become truly essential. Applications affected range from information retrieval and data mining to Internet search for question answering to advice giving, as well as monitoring terrorist and near-terrorist activities. Ingenious attempts to avoid meaning representation by using sophisticated statistical methods produce results of limited and often unacceptable accuracy.

The CERIAS Natural Language Processing research group is developing, expanding, and applying the resources of ontological semantics to a vast array of information assurance applications; some of which exist outside of natural language (i.e., watermarking or tamperproofing) and others that can be done best with natural language files (i.e., semantic forensics, where a contradiction or a lie in a text can be automatically detected and flagged to a human user).

The central resource of ontological semantics—the 8,000-concept ontology—is a tangled hierarchy, or lattice, of concepts each of which is characterized by a number of properties that are also parts of ontology. The group recognizes ontological semantics as essential for organizing domains, regularizing terminologies without policing the experts' usage, integrating knowledge across domains, and focusing research efforts. The group believes integration of ontological semantics will lead to more successful applications.

Additional information on Dr. Raskin and the research of the Natural Language Processing Laboratory can be found at: *http://omni.cc.purdue.edu/~vraskin/Raskin.html*

Elisa Bertino
Professor of Computer Science and Professor of Electrical and Computer Engineering

Digital identity management has emerged as a critical foundation for supporting successful interactions in today's globally interconnected society. It is crucial, not only for the conduct of business and government, but also for a large and growing body of electronic or online social interactions. In its broadest sense, identity management encompasses definitions and life cycle management for digital identities and profiles, and the environments for exchanging and validating such information, including anonymous and pseudonymous representations. Providing secure and efficient solutions for digital identity management is of great significance in today's world. Fighting fraud like identity theft is especially of major concern.

The research team has addressed various aspects related to digital identity management. An approached was developed to support the strong verification of identity information. The approach is based on a privacy-preserving multi-factor verification of such information achieved by the development of a new cryptographic primitive. Such primitive uses aggregate signatures on commitments that are then used in aggregate zero-knowledge proof protocols. The resultant signatures are very short and the zero-knowledge proofs are succinct and efficient.

This cryptographic scheme is superior in terms of the performance, flexibility, and storage requirements to the existing efficient zero-knowledge proof protocol techniques that may be used to prove, under zero-knowledge, the knowledge of multiple secrets. Thus, it is suitable also for small devices. The research group extended this scheme to the support of biometrics and developed a new approach to the generation of biometric-derived keys.

The team also analyzed the life cycle of digital identity information and identified relevant classes of policies dealing with various aspects of the management of this information. As part of this work, the group developed a notion of authentication service and developed an XML-based authentication language, supporting the specification of quality-based authentication policies.

Additional information on Dr. Bertino and her research can be found at: *http://www.cs.purdue.edu/homes/bertino*

CERIAS

The Center includes personnel throughout academia, but also works closely with researchers in private industries and government agencies. The broad foundation of the Center allows us to draw from faculty in more than 20 different departments. For additional information on CERIAS research, faculty and academic partners visit *http://www.cerias.purdue.edu/about/people*. ■

IANetSec

by Jack Phillips

Useable Authentication

With the recent year-end deadline for Federal Financial Institutions Examination Council (FFIEC) [1] guidance compliance within the commercial sector, two related topics have consistently been hitting our inbox, both of which have been well debated within the federal IA community.

First, commercial sector security teams are searching for two-factor authentication solutions that don't require end-user hardware distribution (*e.g.*, SecureID tokens), and are not viewed as too cumbersome by both internal users and customers. Second, integration of logical authentication schemes with physical access control systems continues to be high on most Information Technology (IT) security priority lists for 2007.

Finding secure, yet useable, authentication solutions is a top priority right now for many commercial security teams. Compliance with regulation aimed at safeguarding customer financial data is driving adoption from the outside, and the growing insider threat and reliance on remote access among employees is driving the need from the inside. However, the optimal solution seems to lie somewhere between single factor authentication (username/password) and two-factor authentication. One security leader at a major financial institution recently put it this way:

"Essentially, we're looking for 1.5 factor authentication. Our employees and customers tend to lose (or don't understand) the mainstream token-based authentication devices. But one-factor authentication is simply not enough. Is there technology that lies somewhere in the middle?"

We have been following a interesting group of vendor companies who offer biometric authentication on unique characteristics such at keystroke/typing patterns and voice recognition. Another growing area in the mobile device area is generation of a one-time-password from a server on the corporate internet which is then sent to a user's mobile device via SMS or email to allow authentication.

These technologies are more easily adopted, but (conceptually) provide the same quality of authentication. Added to this, guidance for authentication requirements provided by FFIEC is vague. [2] It provides nowhere near the specificity of NIST's FIPS 201 which translated HSPD-12 into an action plan for government agencies. Most commercial organizations are, therefore, applying varying levels of authentication based on the value of the data, employees or customers accessing the data, and different network environments.

The next issue that will be tackled in 2007 is the integration of logical and physical access control. While the mandate of Common Access Cards (CAC) solved this issue for the Department of Defense, the organizational separation of logical and physical security inside most commercial organizations has led to the emergence of two separate and distinct solutions—one for physical access and one for systems access.

Broadly, we see a trend toward information security being integrated into a central risk function in many commercial organizations. This trend should lead to a CAC approach within the commercial sector, but incorporating more user-friendly authentication techniques.

Centralized decision-making coupled with specific, mandated requirements present within the IA community have been sorely lacking within the commercial sector. [3] This has led to a patchwork of authentication solutions and methods being deployed without real certainty of solid security, or compliance with regulations. ■

References

1. Federal Financial Institutions Examination Council. Guidance on the risks and risk management controls necessary to authenticate the identity of customers accessing Internet-based financial services. The guidance, Authentication in an Internet Banking Environment, was issued to reflect the many significant legal and technological changes with respect to the protection of customer information, increasing incidents of identity theft and fraud, and the introduction of improved authentication technologies and other risk mitigation strategies.
2. See *http://www.ffiec.gov/press/pr101205.htm.* "The agencies consider single-factor authentication, as the only control mechanism, to be inadequate in the case of high-risk transactions involving access to customer information or the movement of funds to other parties."
3. HSPD-12 and FIPS 201.

A Snapshot of Some Current CERIAS Research

by Dr. Gene Spafford and Randy Bond

There are over 80 faculty associated with the Purdue University CERIAS (Center for Education and Research in Information Assurance and Security). It isn't feasible to describe all of (or even most of) the activities of this large group, so we are providing a small "snapshot" of a sampling of current research efforts.

CERIAS functions with a consortium model—companies and government agencies provide a yearly contribution to fund core center activities and to gain preferential access to CERIAS services and products. CERIAS partners also provide technical and managerial advice, real-world data, and often provide cooperation in the R&D efforts conducted by our researchers. CERIAS students and graduates are regularly hired as interns and full-time employees of our partner organizations, and faculty often act as consultants.

More information on our research and education programs (including many not listed here), as well as information about the partner program, may be found on our WWW site—*http://www.cerias.purdue.edu/* or by contacting *info@cerias.pudue.edu*.

Section I—Technical Research Areas Overview

Security for Network and Computing Infrastructures

Wireless

Ad hoc wireless networks are attractive because they can be deployed without prior infrastructure. As sensor networks, they hold the promise of providing ubiquitous sensing and intelligence embedded in the physical environment. A key challenge is devising protocols that are robust in the face of compromise of a subset of the nodes. The protocols cannot rely on a reachable trusted authority at all times. The protocols may also need to operate under the constraints of energy and limited bandwidth, especially for sensor networks. The initial research has resulted in a practical toolset for detecting and diagnosing a large class of control and data attacks. The outcome of the research is a toolset for building a robust and secure environment of mixed ad hoc and sensor nodes.

VoIP

Voice over IP (VoIP) systems are gaining in popularity as technology. As the popularity of VoIP systems increases, they are being subjected to different kinds of intrusions some of which are specific to such systems and some of which follow a general pattern targeted at IP networks. VoIP systems pose several new challenges for Intrusion Detection System (IDS). First, these systems employ multiple protocols for call management (*e.g.*, SIP), data delivery (*e.g.*, RTP), and connection monitoring (*e.g.*, ICMP). Second, the systems employ distributed clients, servers and proxies. Third, the attacks to such systems span a large class, from denial of service to billing fraud attacks. Finally, the systems are heterogeneous and typically under several different administrative domains. Our effort has built an IDS specific to VoIP environments using two powerful primitives—stateful detection and cross protocol detection. The system is validated through a suite of attacks specialized for a VoIP application.

Grid Computing

The research focuses on two topics. One topic is related to the problem of managing identities in grid computing systems. The main issue addressed here is how to allow users to access remote resources in a grid computing system without having to re-authenticate. Research in this area is in the context of the TeraGrid project; extensions to the Shibboleth approach are being investigated. The second topic is related to access control for resources on a grid, with special focus on the data grid. Initial results include organizing local access control policies by using the virtual organization approach and integrating access control with resource scheduling.

Alternative Architectures
The Poly2 Project is an information assurance project in security architecture. The goal of this project is to secure critical network while also providing reliability and redundancy. The initial design incorporates separation of network services onto multiple computing systems and strict control of the information flow between the systems and networks Additionally, we are creating minimized, customized operating systems tailored for the applications each system. The operating systems will only provide the minimum set of needed services and resources to support a specific application or network service. This customization will increase the difficulty in attacking and compromising the system. To manage the individual systems and services in this design, a platform management system will allow administrators to provision additional network services. The research will also develop metrics that will allow objective comparison of the vulnerabilities and benefits of the resultant system against architectures that are more conventional.

Digital Forensics

Sensor Watermarking
We are developing techniques that will allow observation of the output of a sensor and determination of which sensor produced it. Question of whether the sensor can be "trusted" or whether the device has been comprised are of prime interest. The ultimate goal is to develop a signature of each sensor. This requires modeling the sensor and its associated devices. We are developing both intrinsic and extrinsic signatures. We have developed techniques for various types of sensors including printers, scanners, digital cameras, sensor nodes, and Radio Frequency (RF) devices.

Small Scale Digital Devices
We are identifying the best tools and techniques to use in the applied forensics of small-scale digital devices (cellular phones, PDAs, flash drives, and other sources of digital evidence). We are compiling a comprehensive database with the cooperation of vendors and investigators. Information can then be found for future investigations, as well as for the improvement of forensic techniques and technologies. We are also designing a digital device forensic tool for fast triage (acquisition and analysis) forensics of other small-scale digital devices.

Psychological Digital Crime Scene Analysis
We are focusing on a behavioral analysis model that will assist law enforcement with the investigation of digital/electronic crimes. The study is determining the efficacy of reusing "traditional" psychological crime scene analysis models and concepts with primarily technological crimes. The goal is to map analogous crime scene elements between traditional physical crime scenes and their digital equivalent. A crime scene analysis elements matrix has been published as a step in the development of our final model.

Contraband Images Investigative Tool
This research involves development of an open source forensic application that will allow investigators to analyze large volumes of evidence when searching for contraband images, while ensuring the forensic soundness and admissibility of derived evidence. A prototype has been developed and is currently in use by over 35 state and local law enforcement agencies focused on child pornography investigations.

Computer Criminal Taxonomy
Our objective is to develop a taxonomy of individuals involved in deviant/criminal computer behavior. This taxonomy will allow for the identification of discriminating characteristics (*e.g.*, personality traits, demographics) and the development of predictive risk models of behaviors. This research is fundamental to developing a clearer picture of the human side of computer crime and information risk. We hope to apply this to early identification of at-risk individuals.

Digital Forensics Friendly Construction
We are examining methods of structuring digital forensics investigations

such that appropriate evidence is generated and stored to support effective investigation after an incident. Effective forensics is more than keeping highly detailed audit trails, especially if those trails can be altered by intruders, easily deleted, or exfiltrated to expose sensitive information. The challenges include how to appropriately generate, collect, and store necessary information without impacting execution efficiency, storage capacity, security, or privacy.

Database Systems

Privacy

Several topics related to high assurance secure and privacy-preserving Database Management System (DBMS) are being investigated. The first topic is related to the extension of DBMS architectures with metadata related to privacy. We have devised a method supporting the labeling of items with information concerning the intended purposes of the data. Query modification techniques are used to enforce compliance of use; experimental results have shown that the technique is very efficient. The second topic deals with data anonymization; in particular, the use of clustering techniques from machine learning is being investigated. Experimental results show that our approach is quite efficient and reduces information loss. The third topic is intrusion detection systems specifically tailored to address insider threats. Our proposed approach allows one to generate user profiles that include representation of user activities at different granularity levels. Anomaly detection is then efficiently performed on these profiles.

Privacy-Preserving Data Integration, Fusion, and Sharing

Integrating and sharing data from multiple sources has been a long-standing challenge in databases. This problem is crucial in numerous contexts, including data integration for enterprises and organizations, data sharing on the Internet, collaboration among government agencies, and the exchange of scientific data. Many applications of national importance, such as emergency preparedness and response, as well as research, require integrating and sharing data among participants.

Data integration is seriously hampered by an inability to ensure privacy. For example, without a privacy framework, sources are reluctant to share their data about people. The problem is that to merge data, we must know which individual the data is about—disclosing this violates privacy constraints stating that only anonymous data can be revealed. In collaboration with researchers at other institutions, we are developing techniques to solve problems of schema matching, record linkage, and query mapping without violating constraints on privacy of the source data.

Digital Identity Management

We are working on two topics in federated digital identity management. The first is related to the problem of identity theft. An initial solution has been developed that is based on three techniques: multi-factor authentication, zero-knowledge proof protocols, and distributed hash tables. The second topic involves the integration of digital identity management with trust negotiation techniques to allow a resource owner to specify policies in terms of conditions against user credentials. The goal is to develop trust negotiation systems that are able to use identity information already available in federations.

Section II—Selected Currently Funded Research Projects

Homeland Security

A Survivable Information Infrastructure for National Civilian Biodefense

This project focuses on the theoretical foundation and the protocols that facilitate a survivable information infrastructure that meets the critical requirements of a national emergency response system. Specifically, the project is addressing: (1) expansion of existing theoretical frameworks to analyze the behavior of malicious and colluding participants; (2) design and construction of a scalable survivable messaging system that operates correctly under a strong adversarial model; (3) design and construction of information access protocols that protect against compromised database servers providing incorrect data; and (4) prevention of malicious users learning unauthorized information. The domain of application for this work is the Clinicians' Biodefense Network (CBN), a nationwide Internet-based information exchange system designed to provide clinicians with critical information in the aftermath of a bioterrorist attack.

Steward: Scalability, Accountability and Instant Information Access for Network-Centric Warfare

Network-centric warfare calls for survivable command control communication and intelligence (C3I) systems that are resilient to a broad range of attacks. The focus of this project is to construct a realistic solution for the broad malicious attack problem where part of the C3I system is compromised. The project targets three main limitations with current solutions:

1. they are not scalable to high latency wide area networks underlying C3I systems;
2. they have no protection against malicious clients providing incorrect input that is within their authority;
3. they often unnecessarily delay applying updates, withholding important information from clients until updates can be globally ordered.

Ad Hoc Networks

SWAN: Survivable Wireless Ad hoc Networks

Survivable protocols are protocols able to provide service in the presence of attacks and failures. The strongest attacks that protocols can experience are attacks where adversaries have full control of a number of nodes that behave arbitrarily to disrupt the network.

In such a case, authentication and integrity mechanisms are not enough to guarantee correct service, because once an adversary compromises a node he has full control over all cryptographic keys stored on that node. The project focuses on providing routing survivability under an adversarial model where any intermediate node or group of nodes can perform Byzantine attacks such as creating routing loops, misrouting packets on non-optimal paths, or selectively dropping packets. In addition, the project examines defense mechanisms against wireless specific attacks such as wormholes and flood rushing attacks.

Cellular-Aided Mobile ad hoc Networks Integrating ad hoc and cellular networks can enhance wireless communication and support for services. Mobile ad hoc networks have limited wireless bandwidth, low throughput, large delays, and poor authentication and security. This research proposes a cellular-aided mobile ad hoc network (CAMA) architecture. Research includes identifying strategies for routing with global positioning knowledge, security, and radio resource allocation for data transmission. Research problems in moving from integrated networks with a "flat" ad hoc network component to integrated networks with a "hierarchical" ad hoc network component are included.

Digital Identity

Design and Use of Digital Identities

Digital identity management (DIM) has emerged as a critical foundation for supporting successful interactions in networks. It is crucial for not only the conduct of business and government but also for a large and growing body of electronic or online social interactions. In its broadest sense, identity management encompasses definitions and life cycle management for digital identities and profiles, and the environments for exchanging and validating such information, including anonymous and pseudonymous representations. The project is developing a Flexible, Multiple and Dependable Digital Identity (FMDDI) technology supporting multiple forms of identity, including nyms, partial identities, and a variety of user properties, credentials, and roles. Relevant research thrusts in the project include: identity schemes and representation formats; use of ontology and issues related to identity interoperability; anonymity, dependability, accountability, and forensic-friendly identification schemes; psychological and social aspects related to the use of digital identities.

Compilers are an important part of today's computational infrastructure as software is ever-increasingly written in high-level programming languages.

Incident Detection, Response, and Investigation

Development of a Safe, Virtual Imaging Instrument for Logically Destructive Experiments

We are developing a networked system to allow safe and rapid analysis of network security and vulnerabilities with respect to worms, viruses, and other malicious conduct. This reconfigurable facility, named ReASSURE, allows efficient reproducible, controlled, and safely contained experiments with emphasis on information assurance and security. This new instrument integrates functionalities in a manner that will enable high levels of safety and efficiency in manipulating, testing, and developing potentially dangerous experimental networking and virtual machine software while providing computational power to remote users. Advancing the study of virtual machine (VM) technology, the activity offers settings where potentially dangerous experimentation with networking and VM technologies can be performed safely. Providing a testbed networking facility, the infrastructure supports projects that require "self-contained" computing environments in computer science (including security), computer technology, forensics, and information warfare.

Assurable Software and Architectures

Self-Management of Distributed Virtual Environments

This project is investigating management and autonomic operational issues in running distributed virtual private environments. The proposal calls this environment a "VP-Grid"; organic in function, a VP-Grid acts as an overlay on existing grid resources and dynamically adjusts at runtime in response to resource and network conditions in emulating a virtual grid environment. Specifically, the research tasks include: explore application-specific administration policy specification and enforcement through instantiation of self-management agents within the virtual VP-Grid; investigate effectiveness of orchestration methods (scaling, relocation and topology adjustment) by application-driven conditions and demands; and perform a system emulation based on a real Internet worm code.

Foundations of ILP-Based Static Analysis

Compilers are an important part of today's computational infrastructure as software is ever-increasingly written in high-level programming languages. Compiler correctness is generally desirable but essential for embedded systems such as sensor networks, medical implants, and fly-by-wire/drive-by-wire systems. Many commonly used compiler techniques lack proven foundations despite substantial advances in the field of proving compiler correctness. This project will focus on the foundations of static analysis based on integer linear programming (ILP), a technique commonly used by compilers for

embedded systems. This project will investigate key correctness properties of ILP-based analyses, including:

1. **Soundness**—is the analysis sound with respect to a formal semantics?
2. **Preservation**—is the analysis preserved after program transformations?
3. **Composition**—can analyses be combined in ways that preserve basic properties of the program?

Scalable Edge Router for Differentiated Services Networks
This research studies and designs coordinated traffic conditioning, network monitoring, flow control, and provisions the network properly to meet the demands for data and multimedia traffic in various applications. An edge router component to monitor a large network for service level agreement (SLA) violations and bandwidth theft attacks is developed. Our network monitoring scheme involves only edge routers. A scalable edge router cannot use excessive per-flow information and cannot involve core routers. The researchers follow this principle in designing edge routers to achieve scalability.

Assured Software Composition For Real-Time Systems
This project investigates fundamental issues involved in the construction of scalable, reconfigurable, real-time embedded systems. The work focuses on application of object-oriented technologies and, in particular, the Real-time Specification for Java (RTSJ) to the domain of mission critical embedded software systems. The specific outcomes of this projects are:

- Configurable Real-Time Java Framework: The technical foundation for the project is a new framework for real-time Java execution environments called Ovm. The Ovm framework allows domain experts to configure a real-time virtual machines to the operational requirements of a particular mission, *e.g.* tune footprint or predictability characteristics.
- Automatic Configuration of Component Families: Automatic techniques for adapting part of an embedded system in response to changes in its environment, such as, hotswapping bug fixes are studied. Behavior adaption is based on a combination of plugging and reflective object techniques.
- Integrated Testing and Verification: Software composition requires strong assurance about the behavior of individual components and the system as a whole. This project includes development of compliance tests for real-time embedded systems with reference to functional and non-functional aspects.

Section III—Some Additional Project Titles
In addition to the above-described research, what follows are titles of some other, representative research efforts being conducted with external funding.

System Architecture
- Security of Large Scale Systems
- Network Loss Tomography
- Protecting TCP Congestion Control: Tools for Design, Analysis, and Emulation
- Tolerating Malicious and Natural Failures in Distributed Applications Through Non-Intrusive Mechanisms
- Rugged: Resilient Distributed Java Over Heterogeneous Platforms

Forensics
- Printed and Sensor Forensics

Biometrics
- Dyna-Sig Signature/Sig Testing Phase I
- Hand Geometry Testing
- Automated Trust Negotiation in Open Systems

Reliable Wireless
- Reliable Wireless Communication
- Networks with High Mobility

Embedded Systems
- Remote Examination and Manipulation of Electric and Electronic Devices Using Inverse Evaluation of Scattering (Remedies)
- Resource-Efficient Monitoring, Diagnosis, and Programming Support for Reliable Networked Embedded Systems

Data Assurance
- Watermarking Relational Databases (Prabhakar, Atallah)

Intrusion Detection
- Benchmarks for Distributed Denial of Service (DDOS) Defense Evaluation ■

About the Authors

Dr. Gene Spafford | is Professor of CS and ECE at Purdue University, and the Executive Director of CERIAS. He is a senior advisor and consultant on issues of security, cybercrime and policy to a number of major companies, law enforcement organizations, and government agencies, including Microsoft, Intel, Unisys, the US Air Force, the NSA, the GAO, the FBI, the NSF, the DoE, and Presidents Clinton and Bush.

Randy Bond | has been the Managing Director for CERIAS since 2002. Prior to coming to CERIAS, he served five years as the Computing Facilities Manager for his alma mater, the Purdue Computer Sciences Department. He also spent 13 years as a software engineer and is the holder of two patents. He has a B.S. in Computer Science and an M.B.A.

6th Annual Department of Defense (DoD) Cyber Crime Conference

The sixth annual Department of Defense (DoD) Cyber Crime Conference was held from 21-26 January, 2007 at the Renaissance Grand Hotel in St. Louis, MO. This highly informative event was jointly sponsored by the DoD Cyber Crime Center (DoD CCC) and the Joint Task Force-Global Network Operations (JTF-GNO).

This years conference was once again open to all federal, state, and local law enforcement officials, as well as their contractors. The conference started off with two days of optional training, two days of expositions, followed by four days of track sessions. Because of the wide range of individuals involved, the tracks were widely varied to include: law enforcement, information assurance (IA), legal, forensics, and research and development (R&D).

As in years past, the conference is the only one that brings together digital forensics, legal, information technology, investigative, and forensic R&D personnel in an open and interactive forum, facilitating information sharing and team building on issues facing DoD as well as federal and state governments within the cyber crime arena. The goal of the conference was to address today's new cyber crimes and those of the future, with presentations from leaders in the discipline of cyber crime prevention. This year, the conference focused on numerous aspects of computer crime including: intrusion investigations, cyber crime law, digital forensics, and IA as well as the research, development, testing, and evaluation of digital forensic tools. Specific briefing topics included: peer to peer applications, forensics of fringe devices, cyber crime investigative and incident reporting methodology, protecting and storing digital evidence equipment, network security and security tools, wireless security, cryptography, open source analysis, Microsoft Vista security concerns, charging computer crimes, and many, many more.

For information on how to obtain specifics on the conference or particular briefings, please contact IATAC by email iatac@dtic.mil or visit *http://www.DoDCyberCrime.com.* ■

continued from page 13, "CERIAS at Purdue University"

CERIAS Industry Partnership Program

CERIAS has an established industry and agency partnership program. The program facilitates meaningful, two-way communication between CERIAS and industry or agency leaders. The program provides early access for partners to CERIAS research, technology and graduate students. The partnership program works to provides organizations with a mechanism to keep abreast of emerging developments. *http://www.cerias.purdue.edu/partners*

Academic Partnerships

CERIAS continues to establish a community environment among organizations that provide research-based education at the graduate level. The Academic Partner Program is intended to enhance collaboration and synergy among CERIAS faculty and select research centers and programs around the world through:

- Shared research and scarce resources
- Cross-institutional proposal and research teams
- Large-scale test beds and data interchange
- Faculty capacity-building and curriculum development
- Increased opportunities for professional growth and education
- Wider variety of education and training opportunities for students

http://www.cerias.purdue.edu/partners/affiliates ■

An IATAC/DACS State-of-the-Art-Report on Software Security Assurance

by Karen Goertzel

The era of asymmetric warfare is well underway. Nation-state adversaries, terrorists, and criminals have joined malicious and "recreational" attackers in targeting this growing multiplicity of software-intensive systems. These new threat agents are both better resourced and highly motivated to discover and exploit vulnerabilities in software. The National Institute of Standards and Technology (NIST)'s Special Publication 800-42, Guideline on Network Security Testing sums up the problem: "Many successful attacks exploit errors ('bugs') in the software code used on computers and networks."

Software assurance is the "justifiable confidence"—or trust—that software will consistently demonstrate its required properties, such as quality, reliability, correctness, dependability, usability, interoperability, safety, fault tolerance, and security. Software security assurance, then, is the assurance of security as a consistently demonstrated property in software.

In practical terms, "secure software" is software that is as free as possible of faults and weaknesses that could be exploited to subvert or sabotage the software's required properties, and which is able resist or tolerate and rapidly recover from attacks that attempt to exploit any faults/weaknesses that could not be eliminated.

"Secure Software" is software that is as free as possible of faults and weaknesses that could be exploited to subvert or sabotage the software's required properties, and which is able resist or tolerate and rapidly recover from attacks that attempt to exploit any faults/weaknesses that could not be eliminated

As Gary McGraw states in his book *Software Security—Building Security In*, "We must first agree that software security is not security software." What this means is that the ability to assure the security of the software itself is unrelated to whether that software performs security functions or implements security mechanisms. Software performs many more non-security functions than security functions—non-security functions that are mission critical, and thus require the same high level confidence in their dependability and other required properties.

The software security assurance community is interested in policies, activities, practices, methods, standards, technologies, and tools that can contribute to achieving that high level of confidence, regardless of whether the software performs security functions or not. The subject of this State-of-the-Art-Report (SOAR) is what the software security assurance community has done, is doing, and is planning to do to further the cause of software security assurance.

Specific questions to be addressed in this SOAR include:

- What are current definitions and implications of the terms "software assurance," "software security," and "secure software"?
- What is the relationship of software security to software dependability?
- How does software security assurance differ from, complement, and overlap with information assurance, information systems security, and application security?

- Why does software security matter? What are the threats to software throughout its lifetime? What characteristics of software make it uniquely vulnerable to these threats?
- What impact do offshoring, outsourcing, and the use of Software Of Unknown Pedigree (SOUP) have on the ability to assure the security of software?
- What is the relationship between how software is engineered and its ability to resist threats? How does secure software engineering differ from, complement, and overlap with secure systems engineering?
- What current standards, process improvement models, and development methodologies have been demonstrated to improve the likelihood that software life cycle processes will result in secure software?
- How can development and deployment technologies and tools be used in ways that improve software's security?
- What unique security challenges are posed by component-based development?
- What is the relationship between information system risk management and software assurance? Do Common Criteria evaluation and C&A contribute to the assurance of software security?
- What are the emerging standards and methodologies for building and verifying software assurance cases?
- What security criteria and evaluations should acquisition personnel require for commercial and open source software products and development contractors?
- What current software security assurance programs, initiatives, and activities are underway in DoD and the Intelligence Community, in other Federal agencies, in foreign governments, industry, and academia, in the US and abroad? What R&D and S&T is being done to help improve the security of software?
- What resources are available to help readers learn more about software security assurance? What constitutes the software security assurance "community"—who are the recognized subject matter experts (SME)? Are there firms that specialize in software security assurance? Are their organizations devoted to the discipline? What workforce awareness, education, and training resources are available? ■

About the Authors

Karen Goertzel, CISSP, | is a subject matter expert in software security assurance and information assurance, particularly multilevel secure systems and cross-domain information sharing. She supports the Department of Homeland Security Software Assurance Program and the National Security Agency's Center for Assured Software, and was lead technologist for three years on DISA's Application Security Program. Ms. Goertzel is currently lead author of a report on the state of the art in software security assurance, and has also led in the creation of state of the art reports for the Department of Defense on information assurance and computer network defense technologies and research, and was involved in requirements elicitation and architectural design of several high-assurance trusted guard and trusted server applications for the defense departments of the U.S., Canada, and Australia, for NATO, and for the U.S. Departments of State and Energy, the Internal Revenue Service, and the Federal Bureau of Investigation.

The Morphing of a Cyber Operations Curriculum at AFIT

by Timothy Lacey, Robert Mills, Barry Mullins, and Richard Raines

Cyberspace has become a formidable abstraction, offering countless new capabilities, services, and avenues for adversaries to cause harm. The US Air Force recognizes the significance of this new domain and recently added "Cyberspace" to its mission statement. [1] Education and training plays a pivotal role in creating cyber warriors to support this new mission with the Cyber Defense Exercise (CDX), sponsored by the National Security Agency (NSA), providing invaluable real-world experience.

This article provides a brief background of the involvement of the Air Force Institute of Technology (AFIT) with the CDX, introduces our supporting Cyber Operations (CO) curriculum, and discusses how we changed our course format to better use student time in and out of the lab. We also discuss how we found a workable balance between class time and lab time. In the end, we found that students thrive on the hands-on competition and attribute a large percentage of their Information Assurance (IA) education to the exercise itself. The article concludes with a brief discussion of our CO short course plans.

Background

AFIT is the Air Force's graduate school and home to the Center for Information Security Education and Research (CISER). The National Security Agency (NSA) and Department of Homeland Security have designated AFIT as a Center of Academic Excellence in Information Assurance Education. The CDX is conducted under the auspices of CISER.

To weave the CDX into our courses, AFIT's CO curriculum has undergone a metamorphosis since 2002. The CDX is an annual competition that provides students the opportunity to learn and demonstrate best practices in defensive cyber operations. The fundamental objective of the CDX is to design and implement a network to provide specified Information Technology (IT) services and defend it against an onslaught of cyber attacks and natural events. [2, 3] CDX participants include Blue Forces (defensive operations—students at military service schools), Red Forces (attackers), and a White Cell that serves as both referee and director of the exercise. Red Forces are comprised of highly-trained DoD cyber practitioners. Figure 1 illustrates the relationships among the participants.

Schools (students) are responsible for designing their security posture and methods of securing their networks. This design typically includes the use of firewalls, an intrusion detection system (IDS), encryption, defense-in-depth and breadth, and disaster recovery. Students are also required to plan for the following operational design requirements: functionality and usability, physical security, vulnerability assessment, forensics, and reporting. The ultimate goal is to keep all services operational during cyber attacks. Penalty points are assessed against a school for disrupted services or compromised machines.

Preconceived scenarios are used to mimic real-world events to test the students' ability to maintain a viable network despite unexpected events. The team with the highest score (fewest penalty points) is declared the winner and awarded the NSA Information Assurance Director's Trophy. As a graduate school, AFIT does not compete directly with the service academies but is scored in the same manner. Based on our observations of the 2001 exercise, we decided to leverage the competitive nature of our students and integrate the competition into our curriculum.

AFIT's CO Curriculum

AFIT's CO curriculum and student interest has steadily grown since 1996 with the inception of our first CO courses. This growth presented challenges to our faculty such as course timing relative to the CDX and too much material for just two courses. As a result, we moved course offerings and doubled our CO curriculum to accommodate the CDX [4]—a testament to our belief in the hands-on experience. The core courses in our cyber operations curriculum now consists of the following five courses:

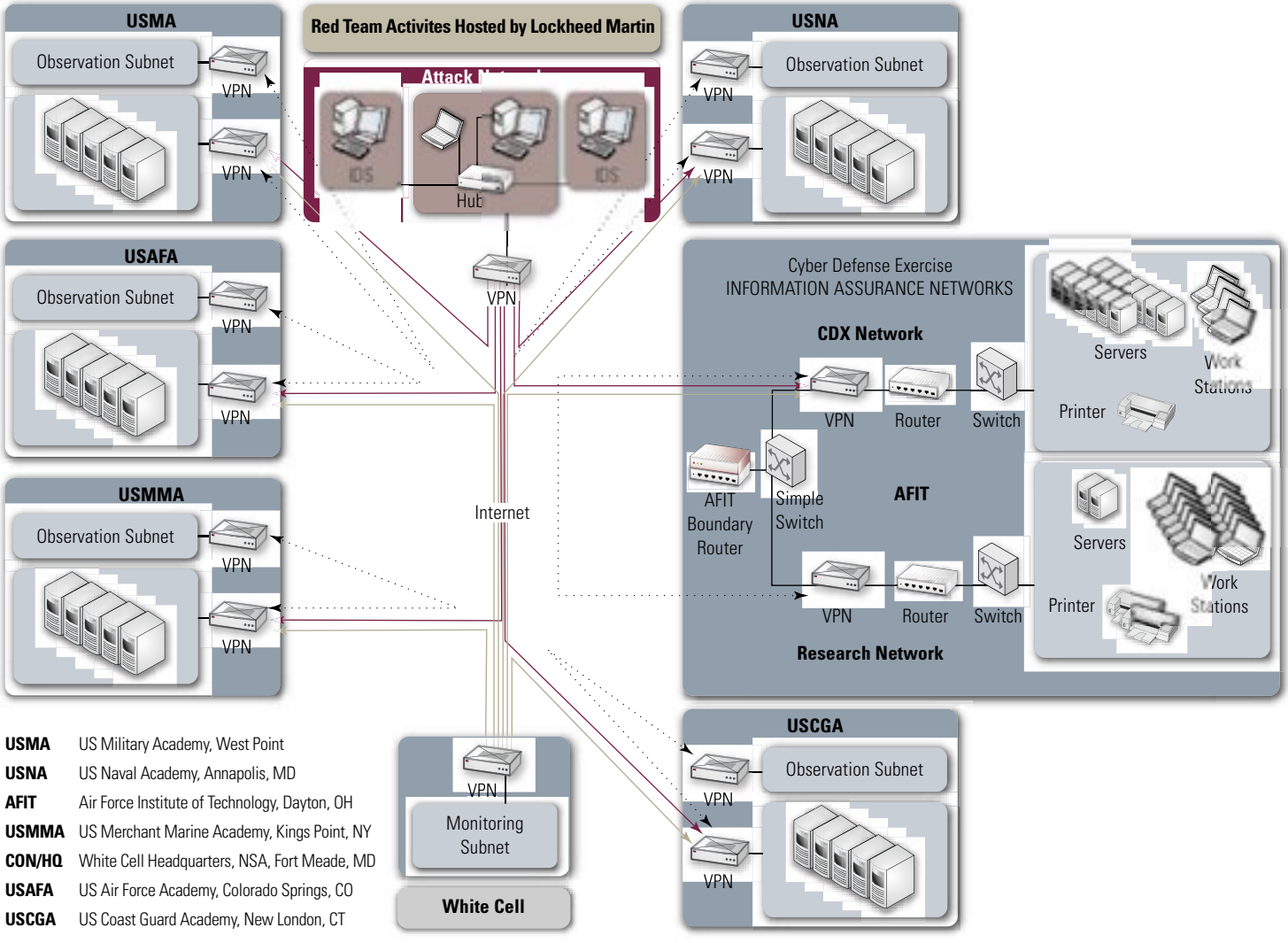


Figure 1. CDX architecture highlighting AFIT's configuration

1. **CSCE 525** Introduction to Information Warfare (Fall, Spring)
2. **CSCE 528** Cyber Defense and Exploitation I (Winter)
3. **CSCE 625** Information Systems Security, Assurance, and Analysis I (Winter)
4. **CSCE 628** Cyber Defense and Exploitation II (Spring)
5. **CSCE 725** Information Systems Security, Assurance, and Analysis II (Spring)

CSCE 525, Introduction to Information Warfare, covers a very broad list of topics associated with cyber warfare, Information Warfare (IW), Information Operations (IO), and IA. We emphasize a systems-oriented viewpoint in examining Air Force, DoD, and national information infrastructures, their vulnerabilities, interdependencies, threats, and opportunities for exploitation. The course provides a foundational understanding of IO doctrine, including traditional concepts such as Electronic Warfare (EW); influence operations; and command and control warfare (C2W). We also explore computer network operations, including defense and attack. Because of the breadth of topics, we emphasize exposure rather than depth in any single topic. There are no prerequisites for the class, and while an understanding of computer networking and communications systems is helpful, it is not required.

Week	Course Title
Week 1	Configure Cisco Router and Switch
Week 2	Configure Firewall and Intrusion Detection System using Fedora Core
Week 3	Configure Windows Server 2003 Domain Controller, Active Directory, and Domain Name Service
Week 4	Configure Exchange Server 2003
Week 5	Configure Windows XP Professional Laptops, Client E-mail, Video Teleconference, and Vulnerability Scanner
Week 6	Configure Internet Information System Web Server and MySQL Database Server
Week 7	Configure File Shares using Server Message Block
Week 8	Configure Incident Response Machine and Analyze Images
Week 9	Configure Internet Protocol Security (IPSEC)
Week 10	Reserved for Special Topics

Table 1. CSCE 528 course topics

The timing of the remaining four courses is orchestrated to provide a synergistic relationship between courses in the same quarter: CSCE 625/725 students learn the theory behind most of the concepts they employ in CSCE 528/628.

CSCE 528, Cyber Defense and Exploitation I, teaches the various aspects of network operations and defense. It focuses on the hardware and software tools of cyber operations and on protection and exploitation techniques. Topics are introduced to address the CDX functional areas (see Table 1). The course is grounded in DoD and Air Force policy, doctrine, and tools. The CDX directive and common "best practices" for securing a network dictate the course material; in place of a text, the course uses a collection of information derived from various sources including The SANS Institute, the NSA, Microsoft Corporation, and Cisco Systems, Inc.

CSCE 625 uses the text, *Computer Security: Art and Science*, by Matt Bishop. It examines the more theoretical aspect of computer security and provides students with an understanding of threats and countermeasures. Propositional and predicate logic are used to explore underlying principles of security. Topics include access-control matrices, protection models, confidentiality, integrity, representing identity, flow and confinement, and malicious logic and intrusion detection.

CSCE 628, Cyber Defense and Exploitation II, does not use a text. It provides ample lab time to prepare the network before the exercise begins in mid-April, or about halfway through our quarter. Before the exercise, students are engrossed in building their secure network design, checking configurations, scanning for vulnerabilities, increasing security, and ensuring that all services work as expected. Backup and contingency plans are also practiced and perfected in anticipation of system failures. Students are given unstructured time during the weeks following the exercise to explore various aspects of their network and research incidents, attacks, and exploits that were seen during the exercise. Students are able to conduct "what if" scenarios

AFIT's approach to the exercise—and the basic tenet of our CO curriculum—is to teach students CO techniques and tool fundamentals and to provide them with the opportunity to become experts on a network service, meticulously plan for contingencies, and keep all aspects of the exercise as simple as possible

and to investigate how the CDX exercised their assigned area of responsibility. Students can also learn more about the other functional areas.

CSCE 725 uses the text, *Reversing: Secrets of Reverse Engineering*, by Eldad Eilam and is fundamentally a continuation of CSCE 625. This course emphasizes offensive IW techniques such as information attack, offensive counterinformation, and automated retaliatory strikes.

CDX Course Format

Before the 2005–2006 academic year, CSCE 528 was taught with four hours per week of lecture and at least two hours per week of lab time. Students received lectures on the fundamentals of computer and network configuration and administration. They also received requisite security education and exposure to numerous vulnerabilities and exploits associated with both Windows and Linux operating systems. Although two hours per week were allocated to lab, in reality, students typically spent more than ten hours per week in the lab primarily because of their interest in the topics. Although their intellectual curiosity and work ethic were laudable, the students were falling behind in other courses.

We changed the CSCE 528 course format in 2006 to strike a balance between lab time and the number of topics presented in class. We abandoned the stereotypical classroom mindset during which an instructor lectures out of a text for the majority of contact time. There simply was not enough time to adequately lecture on all topics and design a robust network.

Most structured classroom lecture time from previous years has now been converted to lab time. The class meets twice a week for two hours. Each class begins in the classroom for 30–45 minutes. The instructor lectures briefly on the most pertinent material and then requires the student teams to present their respective functional areas. Teams interact with each other to ensure systems are interoperable. Occasionally, an idea from one team initiates a discussion on various design options. The instructor then lectures on the pros and cons of one approach over another. When necessary, the instructor lectures on the specific technologies and how one method of defense is better than another. The goal is to give the students the flexibility to choose implementation details and to help them avoid serious design flaws.

The remainder of the two-hour class is spent in the lab. This allows students to learn their functional area by getting their hands on the network components. The lab atmosphere is very eclectic, and topics are covered as they manifest themselves during the network design process.

A disadvantage of this method of instruction is that students are asked to become experts in one area at the expense of breadth. A series of lectures could provide the breadth, but then the students would not have the depth required to successfully design the network. Finding the right balance between classroom lecture and lab time continues to be the instructor's mission. Confirmation of the value of this new course format is seen in the following quote from a CDX student:

I personally learned more from this CDX than the one at [name removed] through the more open environment. At [name removed] we did have lectures for the first half of the semester before we really started working in the labs. Overall, I did not think this really added much to the class, as most of the learning came through the actual exercise itself.

Results

The reinforcement of instruction with hands-on labs and competition results in a thorough understanding of network operations and system security. We submit that the best way to teach network and system security is to explain the objectives, give basic instruction, and then get the students on the machines as quickly as possible. Once students begin to configure machines and services, they will have a myriad of questions that can then be addressed to the benefit of the entire class. Instead of teaching vague concepts, precise instruction in the lab is given, which is immediately reinforced through hands-on application.

We find that students genuinely enjoyed, and responded well to, the hands-on, active-learning environment of the CDX and would rather spend their time in the lab, learning by doing. In fact, feedback from students in 2006 included a unanimous recommendation to continue the "hands-on" experience and the suggestion of adding more injects, as these were seen as valuable learning opportunities. Students consistently indicate the cyber defense courses are among their favorites, and the lessons learned are internalized. Moreover, student surveys conducted by the NSA across all schools have shown that students believed about 45% of their IA knowledge came from participating in the CDX. [5]

AFIT's approach to the exercise—and the basic tenet of our CO curriculum—is to teach students CO techniques and tool fundamentals and to provide them with the opportunity to become experts on a network service, meticulously plan for contingencies, and keep all aspects of the exercise as simple as possible. This approach falls in line with NSA's best practices:

- Understand the network
- Block unnecessary ports
- Remove all unnecessary services and accounts
- Plan for contingencies

Conclusions

The CDX has proven itself an extremely powerful motivator and education tool for cyber operations. This paper describes a successful cyber operations curriculum through which students not only learn concepts, but they apply them in a real-time operational environment. The exercise provides all participants with an opportunity to test their best practices by demonstrating the skills acquired through the supporting curriculum. AFIT's goal is to arm the students with a solid understanding of how to plan for and solve problems, and the curriculum has proven to be extremely effective at teaching cyber operations.

As a result of the success of our cyber operations curriculum, we developed a one-week short course derived from CSCE 525, Introduction to Information Warfare, and presented it to the 67th Network Warfare Wing, which is the USAF's operational arm for cyber warfare. Student feedback from our inaugural offering was outstanding. We are also considering the development of a one-week short course based on the concepts taught in our other four CO courses. We envision taking these short courses to organizations interested in learning more about secure networking and network defense.

Acknowledgments

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the US Air Force, DoD, or the US Government. ■

References

1 M. Gettle, "Air Force releases new mission statement," Air Force Print News, *http://www.af.mil/news/story.asp? storyID=123013440*, last accessed 12 October 2006.

2 R. C. Dodge and D. J. Ragsdale, "Technology Education at the US Military Academy," IEEE Security and Privacy, vol. 3, no. 2, March/April 2005, pp. 49-53.

3 W. J. Schepens and J. R. James, "Architecture of a Cyber Defense Competition," IEEE International Conference on Systems, Man & Cybernetics, 2003, pp. 4300-4305.

4 G. H. Gunsch, R. A. Raines, and T. H. Lacey, "Integrating CDX into the Graduate Program," IEEE International Conference on Systems, Man and Cybernetics, 2003, pp. 4306-4310.

5 T. Augustine and R. C. Dodge, "Cyber Defense Exercise: Meeting Learning Objectives thru Competition," Proceedings of the 10th Colloquium for Information Systems Security Education, University of Maryland, University College, Adelphi, MD June 5-8, 2006, pp. 61-67.

About the Authors

Mr. Timothy "Tim" Lacey | is an instructor of Computer Science in the Department of Electrical and Computer Engineering at AFIT. Mr. Lacey received a BS in Computer Science/Management of Computer Information Systems (magna cum laude) from Park College and an MS in Computer Systems from AFIT. He has several professional certifications to include Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and Microsoft Certified Systems Engineer (MCSE). He teaches and conducts research in both network and software security.

Dr. Robert "Bob" Mills | is an assistant professor of Electrical Engineering in the Department of Electrical and Computer Engineering at AFIT. Dr. Mills received a BS degree in Electrical Engineering with highest honors from Montana State University, an MS degree in Electrical Engineering from AFIT, and a PhD in Electrical Engineering from the University of Kansas. His research interests include digital and spread spectrum communications; low-probability-of-intercept and anti-jam communications and networks; signal detection and exploitation; and mobile communication networks and security.

Dr. Barry Mullins | is an assistant professor of Computer Engineering in the Department of Electrical and Computer Engineering at AFIT. Dr. Mullins received a BS in Computer Engineering (cum laude) from the University of Evansville, an MS in Computer Engineering from AFIT, and a PhD in Electrical Engineering from Virginia Polytechnic Institute and State University. His research interests include computer communication networks, embedded (sensor) and wireless networking, cyber operations, and reconfigurable computing systems.

Dr. Richard "Rick" Raines | is the Director of the Center for Information Security Education and Research (CISER) at AFIT. Dr. Raines received a BS degree in Electrical Engineering from the Florida State University, an MS degree in Computer Engineering from AFIT, and a PhD in Electrical Engineering from Virginia Polytechnic Institute and State University. He teaches and conducts research in information security and global communications.

FREE Products Order Form

Instructions: All IATAC LIMITED DISTRIBUTION reports are distributed through DTIC. If you are not registered DTIC user, you must do so prior to ordering any IATAC products (unless you are DoD or Government personnel). To register On-line: *http://www.dtic.mil/dtic/registration*. The *IAnewsletter* is UNLIMITED DISTRIBUTION and may be requested directly from IATAC.

Name _____ DTIC User Code _____

Organization _____ Ofc. Symbol _____

Address _____ Phone _____

_____ E-mail _____

_____ Fax _____

Please check one: ☐ USA ☐ USMC ☐ USN ☐ USAF ☐ DoD
☐ Industry ☐ Academia ☐ Government ☐ Other

Please list the Government Program(s)/Project(s) that the product(s) will be used to support: _____

_____

LIMITED DISTRIBUTION

IA Tools Reports (softcopy only)
☐ Firewalls ☐ Intrusion Detection ☐ Vulnerability Analysis

Critical Review and Technology Assessment (CR/TA) Reports
☐ Biometrics (soft copy only) ☐ Configuration Management ☐ Defense in Depth (soft copy only)
☐ Data Mining (soft copy only) ☐ IA Metrics (soft copy only) ☐ Network Centric Warfare (soft copy only)
☐ Wireless Wide Area Network (WWAN) Security ☐ Exploring Biotechnology (soft copy only)
☐ Computer Forensics* (soft copy only. DTIC user code MUST be supplied before these reports will be shipped)

State-of-the-Art Reports (SOARs)
☐ Data Embedding for IA (soft copy only) ☐ IO/IA Visualization Technologies (soft copy only)
☐ Modeling & Simulation for IA (soft copy only) ☐ Malicious Code (soft copy only)
☐ A Comprehensive Review of Common Needs and Capability Gaps

UNLIMITED DISTRIBUTION

IAnewsletters Hardcopies are available to order. The list below represents current stock.
Softcopy back issues are available for download at *http://iac.dtic.mil/iatac/IA_newsletter.html*

Volumes 4		☐ No. 2	☐ No. 3	☐ No. 4
Volumes 5	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 6	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 7	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 8	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 9	☐ No. 1	☐ No. 2	☐ No. 3	☐ No. 4
Volumes 10	☐ No. 1			

Fax completed form to IATAC at 703/984-0773

Calendar

MAY

Global INFOSEC Partnership Conference
1-3 May
Fort Huachuca, AZ
http://www.fbcinc.com/gipc/default.asp

18th Annual National OPSEC Conference
7-11 May
Orlando, FL
http://www.ioss.gov/conf/noce.html

INSCOM IM/IT Conference
8 May
Fort Belvoir, VA
http://www.fbcinc.com/event aspx?eventid=Q6UJ9A00CSNZ

Global Threats...Global Opportunities
8-9 May
Washington, DC
http://www.ttivanguard.com/conference/2007/washingtondc.html

52nd Joint Electronic Warfare Conference
8-10 May
Nellis Air Force Base, Las Vegas, NV
http://www.fbcinc.com/jewc

2007 IEEE Conference on Technologies for Homeland Security
16-18 May
Woburn, MA
http://www.ieeehomelandsecurity2007.org

June

Techno Security Conference
3-6 June
Myrtle Beach, SC
http://www.techsec.com/html/Techno2007.html

The Sixth Workshop on the Economics of Information Security (WEIS 2007)
7-8 June
Pittsburgh, PA
http://weis2007.econinfosec.org

CSI NetSec 2007
11-13 June
Scottsdale, AZ
http://www.gocsi.com

Network Centric Homeland Security - Aligning Policy, Strategy & Technology
26-28 June
Washington, DC
http://www.iqpc.com/cgi-bin/templates/singlecell.html?topic=221&event=12804

July

Bay Area Information Security Forum
Late July
San Francisco, CA

21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security
8-11 July
Redondo Beach, CA
http://www.dcs.kcl.ac.uk/staff/steve/ifip07/index.html

Heartland Security Conference & Exhibition
9-11 July
Minneapolis, MN
http://www.ndia.org/Template.cfm?Section=7790

Symposium On Usable Privacy and Security
18-20 July
Pittsburgh, PA
http://cups.cs.cmu.edu/soups/2007/

IATAC
Information Assurance Technology Analysis Center
13200 Woodland Park Road, Suite 6031
Herndon, VA 20171

To change, add, or delete your mailing or e-mail address (soft-copy receipt), please contact us at the address above or call us at: 703/984-0775, fax us at: 703/984-0773 , or send us a message at: iatac@dtic.mil