

the security journal

**WOW. FALL IS HERE! ARE YOU READY
FOR A COLD, HARD WINTER?**

In this edition:

Book Review: The Art of War for Security Managers

Brute Forcing with Python

Host Compliance with Nessus

ST&E Assessment Methodology

RFID, Part 2



Your global information security experts

5350 Tomah Drive
Suite 3500
Colorado Springs, CO
80918

<http://www.securityhorizon.com>

Editor in Chief: Russ Rogers
Assistant Editor: Michele Fincher

The Security Journal is always looking for quality writers for this publication. If you're interested in submitting an article for an upcoming edition, please contact us at editor@securityhorizon.com.

Interested in advertising in The Security Journal? Contact us at editor@securityhorizon.com

Special thanks go out to Ping Look from Look Designs for the creation of the Security Horizon logo and masthead images for The Security Journal.

For more information on Look Designs:
www.republicofping.com
design@republicofping.com

For more information on Security Horizon, please visit our web site or email us at: info@securityhorizon.com.

Security Horizon, Inc. was founded in 2000 and is headquartered in Colorado Springs, Colorado. As a company, we believe that sound security services are based on education, experience, standards, ethics and unquestionable integrity.

Table of Contents

Notes from the Editor
russ rogers.....p. 3

IAM Course Schedule.....p. 4

IEM Course Schedule.....p. 4

Buffer Brute Forcing with Python
evan anderson.....p. 5

Defining the ST&E Assessment Methods
ed fuller.....p. 9

RFidiot - Why RFID isn't the Answer, Yet
jonathan younessian.....p. 13

Host Compliance with Nessus 3
russ rogers.....p. 18

Book Review:
The Art of War for Security Managers - 10 Steps to Enhance Your Organizational Effectiveness
chuck little.....p. 21



Copyright ©2007 by Security Horizon, Inc.
All rights reserved. Reproduction without permission is prohibited.



Black Hat[®]

Briefings & Training

Events for 2008

Black Hat Briefings & Training DC

Westin Washington DC City Center • Washington DC
February 18-21

Call for Papers Now Open and Registration Opens November 1.

Black Hat Briefings & Training Europe

Movenpick • Amsterdam, the Netherlands
March 25-28

Call for Papers Now Open and Registration Opens November 1.

Black Hat Briefings & Training USA

Caesars Palace • Las Vegas, NV
August 2-7

Call for Papers and Registration Opens February 1.

Notes From the Editor



Russ Rogers
CISSP
Editor in Chief

.....

This issue of the Security Journal marks the beginning of our sixth year of publication. What started out on a whim, years ago, has turned into a respectable electronic publication that has received hundreds of thousands of downloads since its inception. So, to begin this new year, I'd like to start by thanking all the readers, authors, and sponsors that have helped maintain this value resource. Thank you all for a great run so far! I'd also like to thank Michele Fincher for her continued hard work maintaining the high quality of this publication for the past few years.

When this journal started, compliance wasn't really on everyone's radar. I know, from my own perspective, that there were concerns from the programmatic aspects of information security, but compliance was just a concept still in its infancy. In fact, for historical

comparison, NIST's Federal Information Security Management Act (FISMA) was released in December of 2002, just a few months after the first Security Journal was released. You can view a brief history of the NIST documents at the NIST CSRC website: <http://csrc.nist.gov/policies/>.

Today, however, compliance has become much more prevalent in both the private and public sector. For instance, the FISMA program has grown by leaps and bounds, including programmatic guidance, technical guidance, checklists, and more. Retailers are falling into line with the Payment Card Industry's (PCI) Data Security Standard (DSS), requiring retailers to protect customer financial information related to credit cards. You can find more information on PCI here, https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm.

As we move into an election year, it will be interesting to see if the candidates in question address these security concerns while they're out on the campaign trail. With the diversity of backgrounds among the candidates, we could see any number of viewpoints on information security. But with other hot button issues demanding attention, such as healthcare, the war in Iraq, and social security, we may never know what the candidates really believe. I would be interested in hearing from you, the readers, about who you believe would be most capable of addressing information security. Who do you think would be least capable, and why?

Thanks again for all your support. Stay safe.

-Russ Rogers



- 10/23 - 10/24, 2007 Tokyo, Japan
- 10/24 - 10-25, 2007 Gaithersburg, MD
- 11/5 - 11/6, 2007 Colorado Springs
- 1/22 - 1/23, 2008 Tempe, AZ
- 1/29 - 1/30, 2008 Sierra Vista, AZ
- 2/18 - 2/19, 2008 Washington, DC

The IAM is a two-day course for experienced Information Systems Security analysts who conduct, or are interested in conducting, INFOSEC assessments of information systems using NSA's methodology. It is a high-level, non-intrusive process for identifying and correcting security weaknesses in information systems and networks.

FREE 1 Year license to the SAINT Vulnerability Scanner just for attending any of our courses!

Training so good, we teach the competition!

To register for one of these courses or to get additional information, please contact us at:

(719) 488-4500
 info@securityhorizon.com
<http://www.securityhorizon.com>



We speak CVE®!

The INFOSEC Evaluation Methodology (IEM) is NSA's hands-on process for conducting evaluations of customer networks utilizing common technical evaluation tools. Students can expect to learn an easily repeatable methodology that provides each customer a roadmap for addressing their security concerns and increasing their security posture.

- 10/26 - 10/27, 2007 Gaithersburg, MD
- 11/8 - 11/9, 2007 Colorado Springs
- 1/24 - 1/25, 2008 Tempe, AZ
- 1/31 - 2/1, 2008 Sierra Vista, AZ
- 2/18 - 2/19, 2008 Washington, DC

To register for one of these courses or to get additional information, please contact us at:

(719) 488-4500
 info@securityhorizon.com
<http://www.securityhorizon.com>



Introduction

This article is intended as an introduction to a simple brute force tool in the python language. The assumption is that you have read any of the various articles or books relating to buffer overflows: 'Smashing The Stack', 'The Shellcoder's Handbook', 'Hacking: The Art of Exploitation' to name a few. It is also assumed that you have a basic understanding of python. Check out the tutorial at <http://docs.python.org/tut>.

Why python, you may be asking? Here's a quote directly from python.org: ***"Python is a dynamic object-oriented programming language that can be used for many kinds of software development. It offers strong support for integration with other languages and tools, comes with extensive standard libraries, and can be learned in a few days."*** Basically, python is a powerful, versatile, language that is very easy to learn. One of the best features of python (especially when trying to learn a language) is the interactive interpreter. You simply type python at a prompt, and you are there.

```
$ python
<snip>
>>> print 'this is python'
this is python
>>> 8*4
32
```

For this paper, remember '\$ ' is the shell, '>>>' and '...' is python.

Bruting

See, python is pretty cool, but lets move along and do some actual exploiting shall we? We are going to need some code to exploit. Let's look at the classic example of a buffer overflow. First things first, let's compile the

program and use python to figure out how much data is needed to overflow the buffer.

```
$ cat vulnerable.c
#include <stdio.h>
#include <string.h>

int main(int argc, char *argv[]) {
    char buffer[512];

    if (argc > 1)
        strcpy(buffer,argv[1]);
}
$ gcc -o vulnerable{,.c}
```

```
>>> import os
>>> for num in xrange(500, 550):
...     input = 'A'*num
...     retcode = os.system('%s %s' % ('./vulnerable', input))
...     if retcode == 11:
...         print num, retcode, 'Seg Fault! \m/ \m/'
...
512 11 Seg Fault! \m/\m/
513 11 Seg Fault! \m/\m/
514 11 Seg Fault! \m/\m/
<snip>
```

Let's break that down and look at what we did.

```
>>> import os
```

The first line imports the 'os' module, this lets the program know that we intend to use the module in this program. The 'os' module has standard OS routines for Mac, NT and Postfix. To get more information about the 'os' module, or any other module, you can use the built in help function in python, or the pydoc command. Both of these will return documentation similar to a man page.

```
>>> for num in xrange(500, 550):
```

The next line is the start of a for loop, using xrange as the iterator. In human, for every number in 500 through 550, do the following.

```
...     input = 'A'*num
```

This line creates the 'input' variable by repeating the character "A" a specified number of times. Note the '...' means that we are in the "for" statement, and thus we need a tab as python does interpret white space.

```
...     retcode = os.system('%s %s' % ('./vulnerable', input))
```

Continuing we use os.system (the 'system' method from the 'os' module) to run the vulnerable program with the input variable. We save the return code to the variable 'retcode'.

```
...     if retcode == 11:
...         print num, retcode, 'Seg Fault! \n/
\n/'
```

Following that is an "if" statement that checks to see if the return code was 11. If a return code of 11 is found, print the number used, the return code and a message.

So that is pretty simple, but it still isn't a script. We've only verified the logic. Luckily converting from the interpreter to a script is as easy as copy and paste. Were going to add some user input and sanity checking, then we are done.

Here is what the finished product looks like, saved to the file brute.py.

```
$ cat brute.py
#!/usr/bin/env python
```

```
import sys, os
```

```
def usage():
    print 'Usage: %s <program> [beg] [end]'
% sys.argv[0]
    sys.exit(0)
```

```
if len(sys.argv) - 1 < 1:
    usage()
```

```
try:
    program = sys.argv[1]
    beg = int(sys.argv[2])
    end = int(sys.argv[3]) + 1
```

```
except:
    print 'Using default range 1 100'
    beg = 1
    end = 101
```

```
if (os.access(program, os.X_OK)) != 1:
    print '%s does not exist' % program
    usage()
```

```
for x in xrange(beg, end):
    input = "A"*x
    retcode = os.system('%s %s' %
(program, input))
    if retcode == 11:
        print num, retcode, 'Seg Fault!
\n\n/'
```

Some of this should look very familiar. Let's step through the new parts.

```
#!/usr/bin/env python
```

This invokes python to run the rest of the script.

```
def usage():
    print 'Usage: %s <program> [lower]
[higher]' % sys.argv[0]
    sys.exit(0)
```

This is the definition of a function named

Buffer Brute Forcing with Python, cont.

evan anderson

'usage', this will tell the user what type of input the program is expecting. In this case the script needs to know the target program, the beginning length of the input and the ending length of the input.

```
if len(sys.argv) - 1 < 1:  
    usage()
```

This checks to verify there is at least one input from the user. We subtract 1 from the length of sys.argv because the script name is the first argument. If no input is given, call the usage function.

```
try:  
    program = sys.argv[1]  
    beg = int(sys.argv[2])  
    end = int(sys.argv[3]) + 1  
except:  
    print 'Using default range 1 100'  
    beg = 1  
    end = 101
```

This try/except statement tells python to attempt to set the variable, if the user doesn't specify a buffer range, a default of 1 to 101 is used. Note, xrange actually stops on the given number so 0-101 would actually stop at 100.

```
if (os.access(program, os.X_OK)) != 1:  
    print '%s does not exist' % program  
    usage()
```

This is the last check of our program. Using the 'access' method of the 'os' module to verify that we have execute privileges on the given program, printing a helpful statement and the usage if there is a problem.

The rest of the program should look familiar. Now save the file, make sure it is executable and you are good to go. If all is right you should get output similar to this.

```
$ ./brute.py ./vulnerable 510 515  
512 11 Segmentation fault \m\m/  
513 11 Segmentation fault \m\m/
```

Hopefully this simple example has shown how powerful python can be, and how python can simplify finding and testing for buffer overflows. Have fun.



Evan Anderson, GCIH, CISSP is a security consultant specializing in Linux and Open Source technologies. You may contact him at evan@regextech.com



SOLARWINDS

Network Management Simplified



**DESIGNED BY NETWORK ENGINEERS
FOR NETWORK ENGINEERS.**

You won't find any shelf-ware at SolarWinds. Our affordable, easy-to-use network management products install in minutes & deliver robust, scalable functionality.

See why more than 45,000 customers trust SolarWinds products to manage their networks.

DOWNLOAD FREE 30-DAY EVALUATION VERSIONS TODAY AT SOLARWINDS.COM



49 Desktop Applications for Finding and Fixing Network Issues

Engineer's Toolset delivers the powerful network management, monitoring, and troubleshooting tools you need to easily and effectively manage your network right from your desktop — all in one extremely affordable package.

from \$1390



Scalable Performance Management for Complex Networks

Providing extensive visibility into the health of network devices, servers, and applications, Orion ensures that you have the real-time information you need to keep your systems running at peak performance all the time.

from \$2475



Change & Configuration Management Made Easy & Affordable

Cirrus is an affordable, easy-to-use network change and configuration management solution that automates device configuration and change management across multi-vendor network infrastructures.

from \$1245



Learn More Today:

**www.solarwinds.com
866.530.8100**



SOLARWINDS

For some time now I have been asked about and had several discussions about testing requirements for government certification and accreditation (C&A). Most of these questions have been from people that are just getting into the C&A work, although there have been several from individuals that are responsible for C&A oversight. While I normally point to all the different instructions that should be read before I start discussions about what is required, I thought I would give some overviews and examples based on NIST SP 800-53A. Most of this material can easily be obtained by reading NIST SP 800-53A and this article draws heavily from that source. Specifically I want to talk about the three assessment methods; interview, examination, and testing.

According to the NIST SP 800-53A these assessment methods are the processing component of the System Test & Evaluation (ST&E) framework. The interview method of assessment is the process of conducting focused discussions with individuals, or groups of individuals, within an organization to facilitate your understanding, achieve clarification, or obtain evidence. The examination method of assessment is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment security and operational controls. Similar to the interview method, the primary purpose of the examination method is to facilitate assessor understanding, achieve clarification, or obtain evidence. The test method of assessment is the process of exercising one or more security or operational controls under specified conditions to compare actual with expected results. In all situations where the assessment methods are employed, the results are used to support the determination of overall security or operational control effectiveness. Each of the assessment methods described above has a set of

associated attributes which help define the extent, rigor, and level of intensity of the assessment process.

Interviews

Typical interviews will include agency heads, chief information officers, senior agency information security officers, authorizing officials, information owners, information system owners, information system security officers, information system security managers, personnel officers, human resource managers, facilities managers, training officers, information system operators, network and system administrators, site managers, physical security officers, and users. Basically you will need to include all three levels of an organization to get the entire picture. How you conduct the interview defines the rigor and level of detail covered during the interview. There are three depths possible; generalized, focused, and comprehensive.

Generalized interviews consist of broad high-level discussions with selected organizational personnel on particular topics relating to the security controls being assessed. This type of interview is typically conducted using a set of generalized, high-level questions and is intended to capture a broad, general understanding of the fundamental concepts associated with specifications, mechanisms, or activities. This is commonly how the first interviews are conducted.

Focused interviews consist of broad, high-level discussions and more detailed discussions in specific areas with selected organizational personnel on particular topics relating to the security controls being assessed. This type of interview is typically started by using a set of generalized, high-level questions and a set of more detailed

questions in specific areas where responses indicate a need for more detailed investigation and is intended to capture the specific understanding of the fundamental concepts associated with specifications, mechanisms, or activities.

Comprehensive interviews that consist of broad, high-level discussions and more detailed, probing discussions in specific areas with selected organizational personnel on particular topics relating to the security controls being assessed. This type of interview is typically conducted using a set of generalized, high-level questions and a set of more detailed, probing questions in specific areas where responses indicate a need for more detailed investigation, or where assessment evidence allows and is intended to capture the specific understanding of the fundamental concepts and implementation details associated with specifications, mechanisms, or activities.

Another aspect of the interview is the coverage that addresses the categories of individuals to be interviewed, usually based on organizational roles and associated responsibilities, and the number of individuals to be interviewed by topic. Consider that there may be over 75 people in an organization. Do you really want to try to interview all of those people on all topics? That would be an intensive workload that is probably not really needed. You should coordinate with your customer organization to determine the specific topics and numbers of individuals to be interviewed.

Examination

Normally this is the review of documentation, visual inspection of equipment, and observation of activities. Typical actions may include; reviewing information security policies, plans, and procedures; analyzing system design documentation and interface specifications; observing system backup operations, reviewing and analyzing the results of contingency plan exercises or drills; observing incident response operations or activities; checking security configuration settings; or studying technical manuals and user/administrator guides. During examinations certain artifacts, such as records, logs, reports, and previous test / evaluation / audit results should also be reviewed.

Does this sound like a review? One thing you should keep in mind to

reduce the level of effort is to the maximum extent possible, reuse examination results and evidence from previous security control reviews or examinations. Caveat to this is there has to be no significant changes to the information system since the previous results were obtained. I also recommend that you consider the time that has elapsed since the results were obtained. I usually recommend you re-test anything older than 6 months. Again, there are three levels of rigor when doing examinations; generalized, focused, and comprehensive.

Generalized examinations consist of brief, high-level reviews, observations, or inspections of security controls using a limited level of knowledge or review of



documentation. These types of examinations are typically conducted using functional-level descriptions of specifications, mechanisms, or activities.

Focused examinations consist of detailed analyses of security controls using a substantial level of knowledge of the functional aspects of the control and in depth understanding of the system documentation. These types of examinations are typically conducted using functional-level descriptions of specifications, mechanisms, or activities and appropriate high-level design information.

Comprehensive examinations consist of detailed and thorough analyses of security controls using an extensive level of knowledge and extensive body of evidence, or documentation. These types of examinations are typically conducted using functional-level descriptions of specifications, mechanisms, or activities, and where appropriate, high-level design, low-level design, and implementation-related information such as source code.

The other aspect of examination is the coverage. This aspect addresses the topics and number of the component or system specifications, mechanisms, or actions to be examined. Think about a server farm, more than 100 servers. If through the interview portion you have identified that all 100 servers were purchased at the same time and have same hardware and OS configuration, do you really need to inspect each server? Probably not, it may be more effective to do a sampling. Just like in the interview process, you and your customer organization should come to an agreement on specific topics for examination and if sampling is appropriate.

Testing

Testing is the process of exercising one or

more assessment objects under specified conditions to compare actual with expected behavior. Testing is typically used to determine if security controls meet a set of pre-defined specifications. Testing can also include controlled demonstrations of specific mechanisms or activities by individuals, or groups of individuals, within the organization to provide assessors with evidence of security control effectiveness. Normal actions will include structural testing of the logical access control and encryption mechanisms; functional testing of the identification/authentication and audit mechanisms; functional testing of the security configuration settings; functional testing of the physical access control devices; penetration testing of the information system and its key components; functional testing of the information system backup operations; and functional testing of the incident response/contingency planning capability. Understand that, when testing, you will normally be testing multiple assessment objects of different topics. The number and topics of assessment objects is a function of the particular control, specifically its composition, design, and implementation. During the process of testing, certain artifacts associated with those tests, such as records, logs, reports, test / evaluation / audit results should also be reviewed. To reduce the work load in testing, you should reuse test results and evidence from previous security control assessments (when appropriate as previously discussed). Like the other two methods, interview and examination, there are three levels to the rigor of testing; functional testing, penetration testing, and structural testing.

Functional testing is a test methodology that assumes knowledge of the functional specifications, high-level design, and operating specifications of the item under assessment; also known as “black box” testing.

Penetration testing is a test methodology in which assessors, using all available documentation, such as system design, source code, and manuals and using pre-defined constraints, attempt to circumvent the security features of an information system security control.

Structural testing is a test methodology that assumes at least some explicit knowledge of the internal structure of the control to be tested. Also known as “gray box” or “white box” testing.

The other aspect of testing is the coverage attribute addresses the topics to be tested and the number of mechanisms or activities to be tested by category. One consideration you will need to understand through interviews and examinations how effective the configuration management is for your customer organization. Besides running tools to test applications and vulnerability scanners to test multiple controls there are manual tests and scripts that will require you to consider whether you need to test all system components. If there is a standard configuration management process then it can be more effective to do sampling. Again, this is based on how effective the configuration management process is, without effective configuration management you will need to test all of the components.

Using the three methods discussed in this article you can provide your customers with the rigor and depth needed to meet their security needs during the ST&E portion of C&A. In order to apply these methods you will need to know which topics apply and what level rigor is needed. These are topics of discussion that I am not going into for this article, but I will recommend that you read and understand how to do system and data categorization along to determine which

controls apply. The best sources if you are doing a ST&E would be FIP 199, NIST SP 800-60, and NIST SP 800-53 Rev 1.

References:

FIPS 199, dtd Feb 2004, Standards for Security Categorization of Federal Information and Information Systems
<http://csrc.nist.gov/publications/PubsFIPS.html>

NIST SP 800-53 Rev. 1, dtd Dec 2006, Recommended Security Controls for Federal Information Systems - Revision 1
<http://csrc.nist.gov/publications/PubsSPs.html>

SP 800-53 A, dtd Jun 4, 2007, Guide for Assessing the Security Controls in Federal Information Systems (third public draft)
<http://csrc.nist.gov/publications/PubsSPs.html>



Ed Fuller is the Chief Operating Officer and Senior VP of Security Horizon. He has over 30 years of experience in Operations, Communications, Computer Information Systems and Security. He is the primary lead for INFOSEC Assessments, Appraisals and Training for Security Horizon. He may be reached at ed@securityhorizon.com.

The following is the second half of a two-part article on RFID.

Implementations – Personnel ID

While RFID fits easily into property protection and tracking, a more dynamic field presses at civil liberty and personal privacy laws within the next few years. This all comes down to personnel identification. Previously, the field of biometrics attempts to control access to areas and information through the irrefutable verification of personnel by comparing anatomy, chemical, or physical measurements unique to the individual.

Now through RFID, organizations and governments can control access by proximity. Whether transponders are simply attached to identification cards or implanted directly under the flesh, RFID allows an organization to verify the identification of a subject through digital information stored on a transponder.

Speculative military applications include the identification of ranking officers in various national governments such as the United Kingdom and the United States of America (Laurie). While specific information cannot be confirmed for security reasons, RFID transponders would be implanted under the skin of ranking officers as a secondary measure of identification. The major weakness to this system is the reliance on unique RFID transponders.

Medical facilities in the United Kingdom are using RFID transponders to track mental patients that are at risk of hurting themselves or others (Laurie). This method is performed similarly to the above mentioned; a transponder is implanted under the skin with information about the patient and what medical center is in charge of their health. If the patient leaves the campus, a quick scan will inform officials of the patient's residence and any medical conditions critical at that moment. While this system appears to be quite effective, there are not currently any plans to implement this system in the United States of America due to human rights issues.



In the private sector, RFID tracking is being offered as a theft prevention measure in tourist areas, frequented clubs, and discos throughout Europe. Most venues are treating RFID tracking as a "quick pass" to allow frequent customers with

implanted RFID transponders to skip the queue and use RFID tracking to verify their age and identity (Graham-Rowe). Beaches in Spain are working with local store locations to use a common RFID tracking system that would allow tourist to register their credit information and utilize a unique RFID transponder to reference their stored information (Laurie). The goal is to prevent loss or theft of credit cards while tourists enjoy the waters and entertainment, relying on their RFID transponders to pay for the experience without worry. The major weakness to this system is the sole reliance on unique RFID transponders.

National Identification

Perhaps the most significant implementation of a modern radio frequency identification system is the United States of America's "Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief of 2005," otherwise referred to as the Real ID Act added later (Library of Congress: H.R.418). The Real ID Act will require all states in the Union to issue state driver's license with RFID transponders built into the cards themselves. The object is to replace the already widely used magnetic strips found on current drivers' licenses in the states with RFID transponders. Transponders will contain common machine-readable technology with minimum defined data elements.

The details of what data elements will be required are not spelled out, but left to the Secretary of Homeland Security and the Secretary of Transportation to regulate (Wikipedia: Radio Frequency Identification). Because the Real ID Act establishes a national standard for the state issued IDs to adhere to, many critics view this as the first implementation of a national ID card. The act even calls for check points at various locations including airports, court houses, and even random check-points established by United States Border Patrol. The major weakness to this system is the reliance on unique RFID transponders, though each state will control the impact of this vulnerability.

International Identification

While the Real ID Act is still undergoing revisions and progressing through stages, Electronic Passports, or ePassports, have been in distribution since September of 2006. The ePassport consists of paper and electronic identity verification that uses both RFID transponders and biometrics to

authenticate the citizenship of travelers. The International Civil Aviation Organization, or ICAO, defines the biometric standards to be facial recognition, fingerprint recognition, or iris scans, though they have no plans to implement retinal scanning at airports. The reader interfaces follow the standard ISO/IEC 14443-4:2001 (ISO: 1443). The major weakness to this system is the reliance on unique RFID transponders, which are not so unique anymore. With the aid of biometrics, RFID transponders are not the only measure to identify the ePassport holder.

Vulnerable Identity

Although ePassports implement a measure of defense to identity theft through biometrics, the data used to compare to the anatomy of the subject is literally handed over by the subject itself. Because of this, there is a large dependence on the uniqueness of the transponder used in the identification process. This system, as well as many of the previous examples, assumes that the information on the RFID transponder has been unaltered and cannot be duplicated. This assumption is wrong.

Adam Laurie is the non-executive director of The Bunker, a security consultation firm in the United Kingdom. His most recent work has been with British journalist Steve Boggan, from The Guardian, to prove to the world that ePassports are not secure (Boggan). It was at the 2007 ShmooCon, a white-hat and black-hat hacker convention in Washington D.C., that Laurie revealed the full process in which he was able to replicate the information stored in a UK ePassport still sealed in the envelope.

In his speech, Laurie discusses a huge vulnerability to ePassports; "They rely entirely on the uniqueness of the ID." According to

Laurie, the industry defense to the duplication process of RFID transponder is, “clones do not have the same form factor and therefore not true clones.” In essence, because a clone of the transponder does not have the exact same appearance and electronic composition, they are not true clones. However, Laurie mentions that, “the reader can’t see the form factor of the device, so [...] as far as the reader is concerned the chip equals the clone.”

In the case of ePassports, the subject is identified by comparing biometric information contained on the RFID transponder. Using Laurie’s methods, the information can be

“The information stored on ePassports is all the information you need to produce a fake passport”

obtained by setting a reader to the correct bit rate and modulation to receive the data. This data, although encrypted, took only 4 hours to brute force with his equipment on hand; a laptop and an RFID reader. Laurie mentioned that, “I have to be within 3 or 4 inches. What I have, I have built a blue-tooth version of the reader so I can have it on my person.” With a laptop in a backpack and his blue-tooth scanner in hand, it will not be hard to obtain information from an unknowing target with a subtle slip of the hand without ever making contact.

The process of replication is simple after that; “The information stored on ePassports is all the information you need to produce a fake passport” (Laurie). By creating a clone, the information can then be altered to contain different biometric information to allow the ePassport holder to pass without conflict of information—successfully defeating the entire purpose of RFID transponders in the identification process.

Cryptic Solutions

While the transponders themselves contain the ability to encrypt information, there is no way to track how many failed attempts have been made, allowing brute force attacks to go unchallenged. Because current RFID chips are passive they only turn on when being used. Once they return to the passive state, there is no evidence that a read has been initiated. In order to allow transponders to block brute force attacks, the transponders would have to be redesigned to allow for an RFID chip to record how many failed attempts have been made, which is unforeseeable (Laurie).

Asymmetric encryption would offer the extra measure of encryption necessary. Asymmetric encryption is a process that uses two keys to encrypt and decrypt a message. By using a private key to encrypt the information contained on any given RFID transponder, a database of public keys can then be used to decrypt the information when called upon. This database would have to be common to every check point that would need resource to the public and private keys required to decrypt the information necessary for authorization. World wide implementation will be quite expensive, but continued reliance on RFID transponders that simply spit out a number for verification will result in a drop in the security standard and will give easier access to sensitive information for identity theft.

Digital Fortress

Security measures are always implemented when there is information or material sensitive

to the nature of an entity. Especially in the recent trend of ultimate security recourse, technology, as always, takes the front-line to the protection of data and resources. With the addition of Radio Frequency Identification to the arsenal, the United States and various allies have taken steps forward in the verification of it's citizens identity. RFID is implement in great strides in the private sector, returning pet's to their owner and allowing ease of access to properly secured vehicles or homes. However, as Adam Laurie responds to questions asked at his ShmooCon presentation, "unless there is a bilateral agreement in place between my country and your country, yes you can enter with a false ID." There are a lot of questions that need to be asked about the government implementation of RFID transponders in state issued and federal issued identification. It will not be long before every American holds in their hands their very own digital flag to defend. The industry must seek every avenue to provide a digital fortress in defense.

Resources

Boggan, Steve. (17 Nov 2006) Cracked it! <<http://www.guardian.co.uk/idcards/story/0,,1950226,00.html>>

Ciampa, Mark. (2005) Security + Guide to Network Security Fundamentals. 2nd Ed. Thomson Course Technology.

Graham-Rowe, D. (2004) Clubbers chose chip implants to jump queues. NewScientist.com <<http://www.newscientist.com/article.ns?id=dn5022>>

International Civil Aviation Organization. (2007) Flight Safety Information Exchange. <<http://www.icao.int/fsix/>>

International Organization of Standards. (2004) ISO/IEC 18000-6:2004. <<http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=34117>>

International Organization of Standards. (2001) ISO/IEC 14443-4:2001. <<http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=31425>>

Laurie, Adam. (March 2007) RFIDiots – Exploration of Technology. Speech presented at ShmooCon, Wardman Park Marriott Hotel, Washington D.C. <<http://www.shmoocon.org>>

Library of Congress: THOMAS. (2007) H.R.418. <<http://thomas.loc.gov/cgi-bin/bdquery/z?d109:HR00418:>>

National Highway Traffic Safety Administration (2000) Tread Act. <http://www.nhtsa.gov/cars/rules/rulings/index_treadact.html>

Wikipedia. (2006) Radio Frequency Identification. <<http://en.wikipedia.org/wiki/RFID>>

Wikipedia. (2006) Biometrics. <<http://en.wikipedia.org/wiki/Biometric>>

World Small Animal Veterinary Association. (2002) ISO Technical Working Group Electronic Animal Identification. <<http://www.wsava.org/microchip1102.htm>>



Jonathan Younessian is a current student of the University of Advancing Technology and can be contacted through this Journal.



Examine, expose, and exploit
your vulnerabilities before an attacker does.



SAINT® offers the only integrated vulnerability assessment and penetration testing tools available. The SAINT® product suite offers you a complete solution to evaluate all of the threats to your network.

Examine your network with the SAINT® vulnerability scanner, and **expose** the areas where an attacker could breach your network. Then, go to a higher level of visibility and **exploit** the vulnerability to prove its existence without a doubt. SAINT's remote management console also enables enterprise-wide vulnerability scanning for large organizations.

Extreme Network Security

To learn more, visit www.saintcorporation.com
or contact Billy Austin at 1-800-596-2006 ext. 0119 or austin@saintcorporation.com.

Compliance has become a hot button issue over the last year or so, and if you work in an organization that has literally hundreds or thousands of computers, you know what a headache it can be to monitor the settings on all those hosts. Regardless of what regulations you're trying to adhere to, you know there are sometimes hundreds of settings that need to be watched. NIST, NSA, DISA, CERT, and CIS all have their own ideas about what's important, not to mention the various military branches and Federal or State agencies.

Most applications for this type of work can cost the organization many thousands of dollars. Creating this functionality in-house could be even more expensive once you add time and resource costs for development and maintenance. The alternative is to utilize a freely available or less expensive alternative; enter Nessus 3.

Nessus 3 is the latest relative in the long line of Nessus vulnerability scanners. The features of the application are much improved over past versions and the speed of Nessus 3 over its predecessors is dramatic. But even if you've used it in the past, maybe you weren't aware of its ability to help you control host configurations, as well. This article will serve as an introduction to these capabilities, but I encourage you to do some research on your own to determine if this works for your organization. You can find more information at <http://www.tenablesecurity.com>.

The first thing you should understand is that the compliance testing functionality is an additional product from Tenable Network

Security, the owner of Nessus 3. It can be purchased through either their Direct Feed product or their Security Center product. Depending on the product you purchase, the means for running compliance checks is slightly different. For example, with Direct Feed, you would run a compliance check on a host in much the same way you would run a normal vulnerability scan from Nessus. If you're using the Nessus 3 Security Center, the compliance scans can be run directly against assets that you've entered into the application. The good news is if you're already paying for the immediate updates through Direct Feed, this functionality is already in place.

NOTE: If you've used Nessus for a while, then you're probably familiar with the NASL scripts used to provide signatures and checks to Nessus. The compliance auditing functionality is added to Nessus 3 through two separate .nbin files, which are basically compiled NASL scripts. These files use .audit files as input for what configuration settings Nessus 3 will check when you run the compliance check.

The .audit files are specially formatted text files that you can create yourself or download from tenablesecurity.com, in the Support Portal. If you're currently using the Microsoft .inf files to check compliance (maybe via the CIS scripts), Tenable offers the i2a.exe application to automatically convert .inf files to .audit files. You also have the option to use a separate Nessus Policy Creator to create a .audit file from the configuration of a known good server.

In Figure 1, you can see the open file dialog

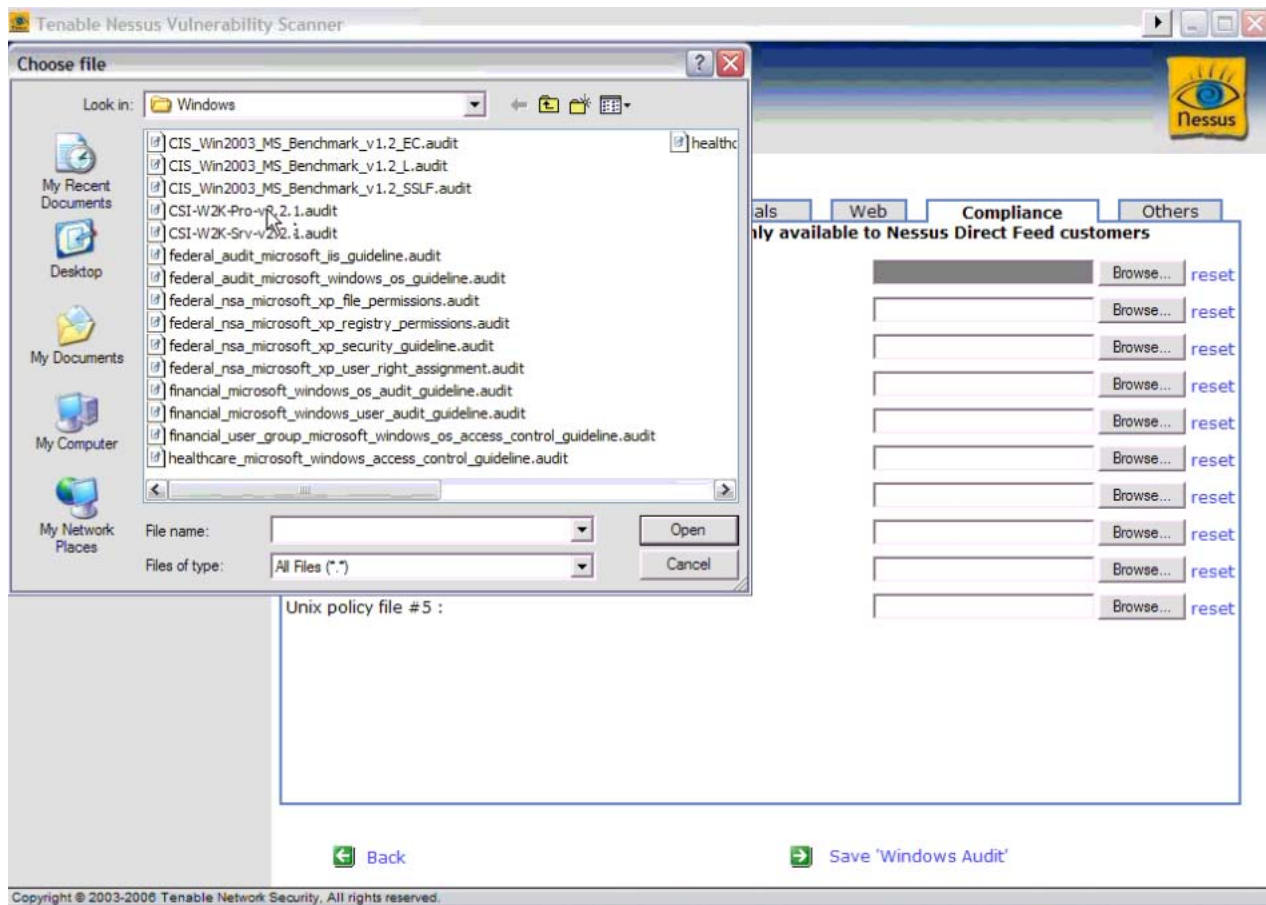


FIGURE 1 – Audit Files

where you choose the .audit file that you'll use to check your configuration. This file is chosen from the Compliance tab of the Nessus 3 window. Again, please bear in mind that this functionality is only available if you've purchased the Direct Feed or Security Center products.

Once the compliance scan is complete, you can view your results. They should look similar to what you're used to from the Nessus 3 vulnerability scans. An example has been provided in Figure 2. One thing you'll need to understand is that, although the results are still rated as HOLE, WARNING, and INFO, their interpretation may be slightly different. For example, if a configuration

comes back as meeting the required criteria, that result will be reported as INFO (PASSED). Should a setting be located that does not meet the required criteria, it will come back as a HOLE (FAILED).

If you're interested in learning more about these compliance capabilities of Nessus 3, I recommend you check out the tenablesecurity.com web site. Specifically, Ron Gula, the CTO of Tenable has provided an online web demo of how the compliance portion of the application operates, including reporting, the conversion of audit files, and examples of how to use the application most efficiently. They've also provided an extensive white paper on their site that provides detailed information

192.168.20.16 general/tcp	✔ "Audit account logon events" : [PASSED]
192.168.20.16 general/tcp	✘ "Audit account management" : [FAILED] Remote value: "no auditing" Policy value: success, failure
192.168.20.16 general/tcp	✔ "Audit directory service access" : [PASSED]
192.168.20.16 general/tcp	✔ "Audit logon events" : [PASSED]
192.168.20.16 general/tcp	✔ "Audit object access" : [PASSED]
192.168.20.16 general/tcp	✘ "Audit policy change" : [FAILED] Remote value: "no auditing" Policy value: success, failure

FIGURE 2 – Sample Compliance Results

on compliance auditing with the Nessus 3 application.

So if you've used Nessus in the past for your vulnerability scanning and you've been looking for an application to help with compliance checks, it may be worth your while to look into the extended capabilities of the Nessus 3 software. The ability to not only run these tests, but to record and track them, makes this a powerful tool in the continuous security process.



Russ Rogers is the Editor in Chief of The Security Journal, author, and professional penetration tester. You may contact Russ at russr@securityhorizon.com.

THE ART OF WAR FOR SECURITY MANAGERS – 10 STEPS TO ENHANCE YOUR ORGANIZATIONAL EFFECTIVENESS



I've (finally) come to the realization that if I want to stay in the Information Security field, I need to expand and enhance my non-technical skill set(s). It is inevitable and unavoidable if I wish to advance my INFOSEC career. In other words, I need to learn how to be a manager. Now, as you can probably imagine, this realization shook up my quaint little world, where I am pretty much purely a technical person. Many questions came to mind, all of which I had no answers to. In cases like this (where there are more questions than answers), I usually turn to Google to help guide me on my way. But, being a person who loves to read and enjoys books; I saw this as a prime opportunity to visit the book store (and there was much rejoicing). While perusing the aisles of books, one caught my eye: *The Art of War for Security Managers – 10 steps to enhance your organizational effectiveness*. Wow... spot on for the type of book I was looking for. Given that I am a fan of Sun Tzu's work, I like to see how people apply *The Art of War* to so many different topics. I bet Sun Tzu's descendants wish he had gotten a (better) publisher and contract so they could still be receiving residuals!

As I was flipping through the book to see how applicable it would be to my current scenario, one phrase on the very 1st page immediately grabbed my attention, and pretty much guaranteed its place in my "stack o' books to buy." And that phrase is: "Accept that conflict is both inevitable and necessary." As I read that statement, I thought to myself, if the

author can help me understand and deal with conflict in the INFOSEC realm, then the book is well worth it (to me). That wasn't the only phrase/concept that sold me on the book, but it is the one that sticks out most prominently. I've always had difficulties concerning conflict, and that one concept seemed to settle in-place in my mind, and things started fitting together quite nicely for me. But I digress, this article is about the book "The Art of War for Security Managers;" and here's a summary of the book, as well as my thoughts regarding the content.

The book is approximately 179 pages (not including the index, preface, and acknowledgments; so it's not an exceptionally long book; which suits me just fine, considering this book seems aimed at providing you with the concepts and tools for INFOSEC management, rather than providing you with a "cookbook" approach. The "cookbook" style of writing is handy, and proper in the correct situations, but I don't believe this is one of them (situations); plus "cookbook" style books tend to become outdated quickly – at least in my opinion.

There are 12 chapters in the book (the original *Art of War* by Sun Tzu had 13 chapters in case you were curious). An introduction chapter, a chapter for each of the 10 steps, and a chapter entitled "The Art of War and Homeland Security." Additionally the author provides an appendix which contains "...an overview of the tools, tactics, and strategies..." from the chapters in which he

discussed the 10 steps. I like the format of the book/chapters as well; The author opens each chapter with a quote from Sun Tzu that applies to the chapter material, next is an executive summary of material being covered, followed by the actual chapter content, and finishing off with discussion questions. It made for an easy, yet valuable, read and helped me apply the 10 steps more quickly with a better understanding. I bet you are asking yourself, "Chuck, what **are** these 10 steps of which you speak?" Ask and ye shall receive, my friends!

Summary of the 10 Steps

1. Continually develop and exercise leadership.
2. Accept that conflict is both inevitable and necessary.
3. Endeavor to understand your own behavior and that of your adversary.
4. Assess your situation.
5. Keep the mission in focus.
6. Strike when the odds of success are the best.
7. Be able to change positions quickly in order to gain the advantage.
8. Adapt to change.
9. Don't be predictable.
10. Continually collect, analyze, and apply information.

Just when you thought you could skip to the chapters about the 10 steps, the author keeps your attention in the next section, which is titled "Today's Threat Environment." How he keeps your attention is by listing and briefly explaining the greatest enemies Security Managers face. If you've been paying attention, you will notice that this directly applies to step #3, endeavor to understand your own behavior and that of your **adversary**. Here's the author's list of Security Manager enemies (a.k.a scourge of the INFOSEC community):

- Enemy #1: Emotionalism
- Enemy #2: The Environment
- Enemy #3: Unrealistic Expectations of Oneself
- Enemy #4: Lack of Understanding
- Enemy #5: Ineffective Organizational Structures
- Enemy #6: Lack of Leadership
- Enemy #7: Poor Timing
- Enemy #8: Poor Execution
- Enemy #9: Predictability
- Enemy #10: Lack of Intelligence Capability

Hmmm..... there are 10 steps, and 10 enemies. Coincidence? I think not! If I'm not mistaken, you can begin to see how well the concepts are covered and tied together in this book. Not everyone will agree completely with the author's list of our common enemies, but I believe we can all attest to the fact that each of the enemies listed are indeed threats in some way, and need to be understood as well as mitigated.

I don't want to ruin the book for you; I want you to read it! And keeping with that sentiment, I will provide a brief summary of each of the chapters. I'm not going to re-write the book here, but provide just enough detail to give you an idea of what's going on; key concepts and whatnot. Sound good? Excellent. Now onward!

I've already discussed chapter 1, the *Introduction* (you just read it). So let's jump to chapter 2, *Be a Leader*. This chapter looks at what it takes to be a leader, how to tell the difference between a good leader and bad leader, and answers the question of whether there are rules for leadership. The author asks, and answers fundamental questions regarding leadership, but it all boils down to the first section title in this chapter: Who would you follow into battle? To emphasize this point he discusses the battle of

Thermopylae (e.g. The recent movie – 300), and pulls out four lessons from this battle that can be applied to security management:

- Leaders must understand what is supremely important.
- What is supremely important to your organization?
- Leaders must exhibit courageous integrity.
- Can you (the leader) be bought?
- Leaders must utilize their resources to the best of their ability.
- Are you (the leader) effectively using the resources at your disposal?
- Leaders must make a commitment to training.
- How important do you (the leader) consider training?



The battle of Manassas Junction (Gen. Stonewall Jackson) is discussed next, but I'll let you read that one. I can't do all the work for you!

Chapter 3 is about conflict, entitled *Accept the Inevitability of Conflict*. This is the chapter that addresses the phrase/statement that initially sparked my interest in the book. In other words, this is an important chapter to me. In summary, the author states that business related conflicts involve one or more of the following causes, and goes on to list three steps to understanding conflict:

Conflict causes (business related):

1. Differing objectives.
2. Limited resources
3. Position and influence
4. Interpersonal matters

Steps to understanding conflict:

1. Accept the inevitability of conflict.

2. Understand that conflict is not necessarily bad.
3. Make a systematic study of conflict typologies and decide how they apply to the operational environment.

It's a short chapter, but it made a lot of sense, and I am already utilizing the concepts and steps the author listed. They have helped me; perhaps they will help you (the reader) as well.

Chapter 4 is *Know Yourself and Know Your Enemy*. I couldn't state it better than the author did when he summarized the chapter thusly: "This chapter provides a general overview of both external and internal adversaries commonly faced by today's security professional." The chapter is exactly that. I

can't summarize it very well here, so I will leave it an exercise for the reader. You didn't think you were going to get any homework out of this article, did you? That's just me addressing Enemy #3: Don't be predictable. <insert evil laugh> The author has provided an adversary checklist in the appendix, so don't forget to check it out. Check out the checklist. I'm easily amused and found it to be humorous.

Chapter 5 is *Conduct Strategic Assessments*. "Strategy requires an alignment of resources, tactics, and objectives"¹ for the organization. Again, I couldn't have put it better than the author did. Sun Tzu listed five criteria for assessing the capabilities of an adversary, which the author details in the book. They are:

- The Way

- Weather
- Terrain
- Leadership
- Discipline

The author relates each of these criteria to modern day organizations rather well, and provides an “interpretation” of the criteria into modern day terminology and concepts. For example, Weather for Sun Tzu was exactly that, weather or seasons. In the *Art of War for Security Managers*, Weather refers to “external conditions that influence the behavior of an organization and/or its adversaries.” This refers to such topics as market conditions, regulatory conditions/ climate, public relations issues, and external political, religious, and other controversial issues. Those issues affect the “weather” in an organization’s environment.

Chapter 6 is entitled *Remember What is Really Important*. The quote that the author provides from Sun Tzu is especially applicable in my opinion. The quote is “So the important thing in a military operation is victory, not persistence.” How often have you heard, “that’s how it’s always been done,” or some similar comment? Many times a project will “live on” just because someone is persistent, or they don’t want to change. Or cumbersome and outdated processes continue to be followed/utilized even when they are no longer applicable to the current business model. All the processes, business models, and personnel should be focusing their efforts on what is important to the organization; and concentrate on supporting the organization and its priorities. Chapter 6 is a reminder that we are there for, and because of, the organization; and our efforts need to reflect that.

Chapter 7 is *Engage the Enemy*. This chapter details and examines the key factors necessary to engage and prevail in battle (paraphrase of author’s text). Those key factors are:

1. Solid preparation
2. Skill assessments
3. Creation of “invincibility” in oneself and one’s organization
4. Discovery of the vulnerability of one’s

- adversary
5. Understanding of the battle equation
6. The judicious application of force against weakness

Factor #3 caught my eye because it brings to mind the very question the author asks in the text: “who can truly be invincible?”² Invincibility is not referred to in absolutes, at least not by Sun Tzu and not in the context of this book. It’s really interesting how invincibility is defined by Sun Tzu, but I won’t ruin it for you, check it out on pg 80 in the book. The author discusses the battle equation and battle strategies next, as well as providing input on choosing a basic battle strategy. Which battle strategy is right for you?

Chapter 8, *Maneuver Your Army*. This chapter discusses terrain that the general (security manager) must understand in order to maneuver his or her forces best and most effectively. The types of terrain described in Sun Tzu’s *Art of War* include:

1. Easily passable terrain
2. Hung-up terrain
3. Standoff terrain
4. Narrow terrain
5. Steep terrain
6. Wide-open terrain

The author goes on to explain each of the terrain types, and how they relate to modern day security manager situations/issues. I liked how the author accomplished this task, and how easily I was able to relate scenarios I have encountered (or endured) to the types of terrain the author describes. The chapter goes into quite a bit more detail on each terrain type, how to maneuver on such terrain, and the problems associated with each (both terrain and movement types).

Are you still with me? Excellent! Chapter 9 is next, and is about how to *Adapt to the Battlefield*. Immediately this quote comes to mind: “No battle plan survives contact with the enemy” (quote by Field Marshall Helmuth Karl Bernhard Graf von Moltke). If you cannot adapt, you cannot survive; it’s as simple as that. Understanding and accepting the inevitability of change is not only required,

but also liberating. By liberating I mean you get to exercise your creativity, get to meld the conventional and unconventional (S. Watson), see the unorthodox give rise to the orthodox (S. Tzu). These are key concepts for this chapter on adaptability, and they must be embraced to survive in the harsh, unforgiving, Internet-connected world.

Chapter 10 is entitled *Avoid Predictability*. This chapter is kind of like the opposite of Chapter 9. This chapter emphasizes the reduction of your organization's predictability, and making it more difficult to anticipate your actions, and thus adaptable to by the enemy (they read chapter 9 as well). The author discusses predictability, whether it is ultimately an advantage or a detriment. He discusses how to find a balance between avoiding predictability, and maintaining some sort of order within the organization. The author even provides 30 suggestions for how to make your organization less predictable, without completely throwing order "out the window."

Chapter 11 is about how to *Collect Intelligence*. This isn't a chapter about super spies or anything like that, but about common sense intelligence gathering. This chapter discusses the importance of intelligence, intelligence vs. information, the steps in the intelligence cycle, sources of intelligence, and evaluation of an organization's intelligence capabilities. Foremost, everyone should follow step #1 of the intelligence process: Obey laws and ethical principles. Don't sacrifice your ethics or principles for the sake of finding out something. It's not worth it. There are several more steps in the intelligence process, but again you will have to read the chapter to find them out!

This brings us to the final chapter, #12, which is about *The Art of War and Homeland Security*. In this chapter the author brings it all together and applies the steps and concepts to our modern day situation. I refer to the United State's increased/enhanced security posture, post Sept 11, 2001. The world was changed forever on that day, and information security has been affected just as much, if not more, since then. The author provides us with what he views as "The

Wrong Question", and "The Right Questions." My favorite part of this chapter is the section titled: "Sun Tzu and the War on Terrorism." I enjoyed reading how Sun Tzu may have broken down a strategic assessment of the war on terrorism ("The Way", "The Weather", "The Terrain", "Leadership", and "Discipline").

The appendix, a.k.a. The Armory, is where the author provides you with various job aids, checklists, and tools, to assist us in the INFOSEC battle. It is basically the concepts from the previous chapters, in checklist or plain list format. It is handy to have the concepts and steps listed as such, succinctly, and quick to reference. There is quite a bit of material in there, so don't forget to check it out.

The author ties this book together (concept-wise, etc.) very well, and leaves one with very few unanswered or unanswerable questions; at least in regards to the Art of War and Information Security. I enjoyed reading it, and I got quite a bit out of the book. I would definitely recommend it to a friend, a friend that's an INFOSEC professional, obviously.

Footnotes:

1. Art of War for Security Managers, Chapter 5, pg 48, fig 5-1.
2. Art of War for Security Managers, chapter 7, pg 80.

References and Credits:

Watson, Scott A. *The Art of War for Security Managers – 10 Steps to Enhance Your Organizational Effectiveness*. Burlington, MA: Elsevier, Syngress is an imprint of Elsevier, 2007.
ISBN: 978-0-7506-7985-5

[AOWFSM]



Chuck Little is a Security Consultant with Security Horizon, Inc. You may contact him at clittle@securityhorizon.com.

Master the ghost in the machine.

Some may dream in code. We program the dreams. Gain comprehensive knowledge of application development, object oriented graphical programming. Conjure your calling as an innovator in the realm with a Bachelor of Science in Software Engineering degree.



Discover yourself and make the software spirits dance. UAT.edu/majors

Artificial Life Programming > Technology Management > Computer Forensics > Game Programming > Network Engineering > Network Security > Software Engineering > Web Architecture > Robotics and Embedded Systems > Digital Animation > Digital Art and Design > Digital Video > Game Design > Game Art and Animation