

A Free Publication on Information Security from Security Horizon, Inc.

# the security journal

*"Common Sense Security for Common Businesses"*



**Keeping  
your  
critical  
information  
secure...**

*Are you thinking beyond  
your own backyard?*

**Volume 11 - Spring 2005 Edition**



5350 Tomah Drive  
Suite 3500  
Colorado Springs, CO  
80918

<http://www.securityhorizon.com>

Editor in Chief: Russ Rogers  
Layout 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](mailto:editor@securityhorizon.com).

**Interested in advertising in The Security Journal? Contact us at [editor@securityhorizon.com](mailto: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](http://www.republicofping.com)  
[design@republicofping.com](mailto:design@republicofping.com)

**For more information on Security Horizon, please visit our web site or email us at: [info@securityhorizon.com](mailto: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**  
By Russ Rogers.....p.3

**NSA IAM Course Schedule**  
.....p.5

**Blogging, Phishing and Pharming**  
By Greg Miles.....p.6

**Web Services Eco-System and SAML: Part 1**  
By David Sweigert.....p.8

**NSA IEM Course Schedule**  
.....p.11

**Book Review**  
By Brian Martin.....p.12

**Covert Channels: Part 2**  
By Russ Rogers.....p.14

**Qualification Based Selection**  
By Glenn Watt.....p.18

**Penetration Testing: Part 2**  
By Matthew Hoagberg and Ted Dykstra.....p.22

**DNS Name Prediction with Google**  
By Johnny Long.....p.24

All content used by permission or Copyright 2000-2005, Security Horizon, Inc.

# Increase Your Security Muscle



Strengthen your defenses. Train your mind. Learn the threats of tomorrow, today. Be challenged by the experts who are doing innovative work. Meet and network with thousands of your peers from all corners of the world at the Black Hat Briefings USA 2005—the only technical security event to offer you the best of all worlds.



## Black Hat®

**Briefings & Training USA 2005**

July 23-28, 2005 • Caesars Palace Las Vegas

Training: 4 days, 24 topics • Briefings: 2 days, 10 tracks, 60 speakers

[www.blackhat.com](http://www.blackhat.com)  
for updates and to register.

### sponsors



## Notes From the Editor



**Russ Rogers**  
CISSP, CISM  
Editor in Chief



### Well folks, it's happened...

We're beyond the point of no return. Have you stopped recently to take a good look around at what we call Cyber Space? I mean a really good look. The Internet isn't just about the Western world anymore; nor is it about a few Universities in other countries that might be considered third world. We're now operating globally, both in concept and reality. And before you say something like 'Yeah, duh. I already knew that,' consider what I'm really trying to say. The Internet isn't just global for businesses anymore.

We're currently on United flight 842 flying to Chicago on our way back to Denver. For the last ten days, we've been in Sao Paulo, Brazil. Greg and I were lucky enough (and honored) to be invited as keynote speakers for the Security Week 2005 conference being held in this huge South American metropolis ([www.securityweek.com.br](http://www.securityweek.com.br)). The food was great, the people were endearing, and the

lessons learned were numerous. Although, admittedly, it will likely be some time before I have a craving for a decent Rodizio.

Now, I'm not talking about anything earth shattering when I write about these lessons learned. They're more of a neglected reality that has managed to sneak up on me. In my zest to hone in on the information security front in the United States and Asia, I suppose I had forgotten that the rest of the world was rapidly catching up with us. Security Week 2005 provided me the opportunity to interact with a population (roughly 1500 over the four days) of security professionals, government officials and corporate executives from a variety of South American countries, as well as the rest of the world.

One of the best parts of this conference, for me anyway, was the direct government involvement. The Brazilian Government is aware of the growth of the Internet in their country and concerned about maintaining appropriate levels of security. Top officials even spoke at the opening ceremonies for the conference, giving it their highest endorsement. They're following our lead and learning from our mistakes.

But they're also fighting the same battles we were fighting just a few years ago. The Internet has evened the playing field in economies around the world. In Sao Paulo, we passed dozens of locations offering public Internet access. Granted, most of these were based at kiosks, but it really wasn't that long ago that we had wireless public access popping up at every coffee shop in town. To my own amusement, even our favorite fast food god, McDonalds, has entered the global market by offering visitors to the malls in Sao

## Notes From the Editor, cont.

Paulo a new menu item: McInternet.



No, I swear it's not a joke. This is reality. And it's really exciting! There was a group of students from a local University that had been granted free entrance by the organizers in an attempt to foster awareness in the next generation. I haven't enjoyed many conversations with students on the topics of information security in a long while as much as I did at the conference. But with all this growth and maturity comes a great deal of responsibility. We need to understand the new risks we face each time we conduct a transaction across the Internet.

Before you come to the mistaken conclusion that this might be another one of those 'the sky is falling' discussions, let me mention that I'm less concerned at this point about the hackers already on the Internet than I am about the plethora of new users that haven't got a clue about information security. By simply being on the Internet, new users in countries around the world are extending the battlefield exponentially. Every day, around the world, tens of thousands of new targets crop up on the Internet. And even though they might not contain useful information for an attacker, they could provide a convenient jump

point from which to launch an attack. As more and more computers hop online, the ability for an attacker to hide in the shadows grows. If today is bad for letting our guard down, consider how much worse the threat becomes with each passing day.

In this issue of *The Security Journal*, we are pleased to offer submissions from some very smart individuals in the security world. Instead of focusing on a particular theme in this issue, we've tried to provide a variety of topics. They're intended to get those mental engines in your head processing. But as you read through the selections, bear in mind what your place in the new global economy is and what you need to do to protect yourself and your organization. Even if you think you're a small fish in a big ocean, poor information security could transform you into a powerful attack platform without your knowledge.

Stay vigilant, keep learning, and thanks for reading.

Russ Rogers

### *Did you know...*

Sao Paulo, Brazil ranks among the top three largest cities in the world and is the largest in South America with over 18 million inhabitants? It generates over 30% of Brazil's GNP, which in turn accounts for more than half of that of Latin America.

**Let us hear from you!  
Send your comments and  
suggestions to  
[editor@securityhorizon.com](mailto:editor@securityhorizon.com).**



5/17 - 5/18, 2005	Dallas, TX
6/8 - 6/9, 2005	TechnoSecurty 2005 Myrtle Beach, SC
7/12 - 7/13, 2005	Boston, MA
7/23 - 7/24 or 7/25 - 7/26, 2005	Black Hat USA Las Vegas, NV
8/15 - 8/16, 2005	San Antonio, TX

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 INFOSEC assessment process. It is a high-level, non-intrusive methodology 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 further information, please contact us at:

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



## Advertisers!

Reach *THOUSANDS* of readers every quarter at an *outrageously low price!!*

The *Security Journal* is never offline, making your ad constantly available--ALL of our issues are still downloaded quarterly



Contact us at:  
[editor@securityhorizon.com](mailto:editor@securityhorizon.com)  
or  
719-488-4500

### A Sportsman's Paradise?

**Y**ou hear about it almost everyday in the news and on the net. Phishing and Pharming scams are all over the news. These scams are so new that my Microsoft Word says they are spelled wrong. (Where did the "Ph" come from anyway?).



It's enough to make an outdoor sportsman feel exhausted. All the phishing and pharming combined with blogging, makes it sound like some sort of exotic safari hunt.

**Blogging** (or web logging) is the act of spending your time posting to discussion forums on certain topics. Some use blogging to share information; others just use it as an opportunity to vent. Blogging can be used to discuss information security issues but otherwise has little relationship to information security, except for the social engineering that may occur during the blogging process to coerce information from fellow bloggers or to set people down the wrong path or give bad advice about information security. Remember, blogging is just like the news, just because someone says it doesn't mean it is exactly true.

Social engineering plays a big part in the rampant phishing scams that are currently purveying the Internet. These scams are focused on getting the naive and unsuspecting to do something they should not. (i.e. social engineering) We have all seen it, we call most of it spam and security professionals know better than to mess with these scams because they know it for what it is, a scam. But what about the poor

unsuspecting grandmothers, parents, and students out there that got their first computer for the holidays in 2004? Do they know any better? I personally have gotten phishing emails from eBay, PayPal, 50 of my banks (no I don't do business with 50 banks), and numerous other places I have never heard of.

Webopedia (<http://www.webopedia.com/TERM/P/phishing.html>) defines **Phishing** (pronounced fishing) as, "The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft." The Anti-Phishing Working Group ([www.antiphishing.org](http://www.antiphishing.org)) states, "Phishing attacks use both **social engineering** and **technical subterfuge** to steal consumers' personal identity data and financial account credentials." The social engineering portion should be obvious. I attempt to convince you to go to my fake website by trying to convince you that I am actually your bank, your credit card company, or some other organization you may recognize through spoofed emails. Once I get you to my fake website, I try to get credit card numbers, account usernames, passwords, and social security numbers. This will help me to steal your identity and your money. The

technical subterfuge comes from my ability to place Trojans, such as keylogger spyware, on your system. Then I can steal your credentials directly.

The *Sydney Morning Herald* reported on March 18, 2005 that a major phishing gang was arrested in Rio de Janeiro, Brazil. The gang had reportedly stolen US\$37 million from its phishing victims. The phishers depend on mass mailing and a certain percentage of people receiving the email to actually have accounts at the location its pretending to be, and that a percentage of those will actually be hooked by the scam. Reportedly, this gang sent out Trojan key-loggers to thousands of people to record their online banking passwords.

**Pharming** (pronounced farming) may soon have an even greater effect on the Internet. The Anti-Phishing Working Group ([www.antiphishing.org](http://www.antiphishing.org)) states that pharming “misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning.” Pharming attacks the DNS of a system to confuse it into going to bogus websites (which look amazingly like the real ones) and entering privacy data like social security numbers, credit card numbers etc. The end result of pharming is the same as phishing; sensitive information is stolen. It’s just a different method of getting users to go to these fake sites. The concerning part is that with pharming, you can be knowledgeable and educated on the security evils of the Internet and still be compromised.

### ***So what can be done about it?***

First and foremost is **user education**. This is the best prevention measure for phishing scams. An understanding of social engineering practices and how to avoid them will help prevent blogger and phishing manipulation. User education on email use

and misuse will help users understand the difference between legitimate emails and scam emails. Even if you think an email may be legitimate, you will want to verify it through contact information you have available from a source other than the email itself. If it is related to a bank account, find the phone number to your bank and call. If it is credit card related, call the number on the back of the credit card. Use common sense.

In order to protect against pharming, organizations must implement the **proper security protections** on their systems and networks. This is also effective against the unknown implementation of key loggers and other security-circumventing software and devices. In order to do this effectively, a security program and a security life cycle must be addressed, implemented, and enforced within the organization.

Do not procrastinate, educate. Information security is not intended to be a sports field or a sportsman’s paradise. There is not a single product, firewall rule or security policy that alone can address these issues. Information security is intended to be a systematic process that focuses on continually improving security posture by utilizing systematic, repeatable assessment and evaluation methodologies focused on identifying and resolving information security vulnerabilities. Two methodologies that help to focus on understanding security posture and implementing effective security measures are the National Security Agency’s (NSA) INFOSEC Assessment Methodology (IAM) and the INFOSEC Evaluation Methodology (IEM). More information can be found on these programs at [www.securityhorizon.com](http://www.securityhorizon.com) or [www.iatrp.com](http://www.iatrp.com).

*Greg Miles* is the President, CFO and Co-founder of Security Horizon Inc. You can contact him at [greg@securityhorizon.com](mailto:greg@securityhorizon.com).

# Understanding the burgeoning Web services eco-system with a practical illustration of the Security Assertion Markup Language

*The following is the first half of a two-part article.*

Lightweight Web-based protocols provide standardized interfaces for the exchange of information between parties. Embedded within these protocols are security services that have the capability of creating legally binding transactions, allowing access to data by business partners, empowering colloboration, etc.

New initiatives in the pharmaceutical industry (like the SAFE-Biopharma initiative<sup>1</sup>) provide a “web of trust” between trading partners based upon public key infrastructure (PKI) credentials.

The Web services eco-system has embedded security protocols that can leverage PKI credentials to facilitate the exchange of legally binding transactions. This approach to enterprise-application-integration (EAI) holds the promise of significantly streamlining interactions between trading partners, government regulatory entities, academic institutions, etc.

- A Web services ecosystem is a set of related services. A Web-based ecosystem describes an orderly arrangement of Web services within an architecture. An Ecosystem is a term to describe the horizontal nature of Web-services, as it is not necessarily a hierarchial architecture.
- The Web service technology architecture has received widespread

*acceptance amongst industry, academia and government, as it is based upon interoperable protocols. Web services are characterized by the underlying framework that defines the process of: 1) description, 2) discovery, and 3) interaction.*

## UNDERSTANDING THE WEB-SERVICES ECO-SYSTEM MODEL

The Web-services eco-system embodies standards developed by the World Wide Web Consortium (W3C)<sup>2</sup> and the Internet Engineering Task Force (IETF). The Organization for the Advancement of Structured Information Standards (OASIS)<sup>3</sup> has adopted these standards as well amongst its participating members.

The Web service protocol stack is picture in the graphic below (those services not appropriate to this discussion have been shaded out).

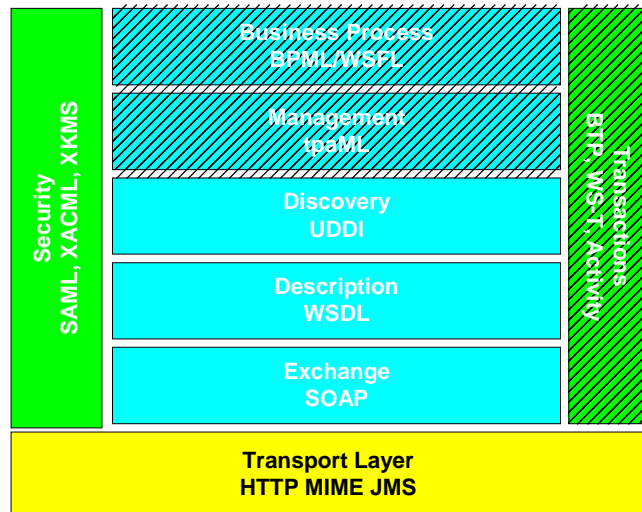


Figure 1. Web services architecture

<sup>2</sup> <http://www.w3.org/>

<sup>3</sup> <http://www.oasis-open.org/>

<sup>1</sup> <http://www.safe-biopharma.org>

### **BURGEONING PROTOCOLS WITHIN THIS NEW MODEL**

#### **TRANSPORT LAYER**

This layer represents the basic protocol stack to move “messaging” amongst systems. These “messaging” protocols must be lightweight and support interoperability. The transport protocols recommended for Web-services transport are: Hyper-text Transport Protocol (HTTP), Multipurpose Internet Mail Extensions (MIME), and Java Messaging Service (JMS). These protocols, or very similar instantiations, represent the current best practices in defining a loosely coupled architecture that supports a messaging “bus” framework.

#### **EXCHANGE LAYER**

The underlying communication mechanism in the Web services architecture is Simple Object Access Protocol (SOAP). SOAP is a lightweight protocol for exchange of information in a decentralized, distributed environment. It is an eXtensible Markup Language (XML) based protocol that consists of three parts: 1) an envelope that defines a framework for describing what is in a message and how to process it, 2) a set of encoding rules for expressing instances of application-defined data-types, and 3) a convention for representing remote procedure calls and responses. See graphic below.

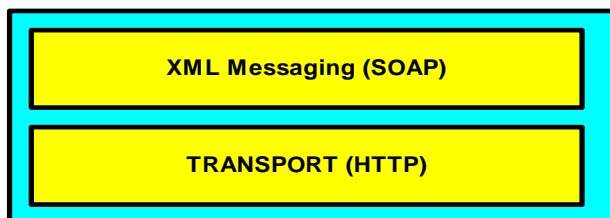


Figure 2. SOAP over HTTP

SOAP offers a lightweight protocol that has been designed for efficiency in communicating between different platforms; e.g., a Java 2 Enterprise Edition (J2EE) platform communicating with a Microsoft .NET platform. HTTP is the common communications protocol that enables this transport interoperability between platforms. A major advantage of SOAP is that a SOAP/HTTP can be allowed through port 80 (HTTP) of an enterprise firewall, this flexibility enables extra-net communications capability (if needed at a later time for inter-enterprise communications; e.g., between business partners).

Therefore, SOAP provides two distinct advantages as a protocol: 1) interoperability, and 2) firewall transversal.

#### **DESCRIPTION LAYER**

Web Services Definition Language (WSDL). WSDL is a protocol designed to support the communication of what a Web service can do. WSDL supports service description capabilities within the Web services architecture. WSDL uses XML-based grammar to describe primarily SOAP-based services to a calling application.

#### **DISCOVERY LAYER**

Universal Description, Discovery, and Integration (UDDI)<sup>4</sup>. UDDI is built around a relational data model to retrieve information. A UDDI register can be likened to a white pages or yellow pages directory service. Many commercial vendors — Sun Microsystems, Novell, and BEA Systems — are mapping their LDAP repositories to UDDI to enable a Web services interface to the traditional directory.

<sup>4</sup><http://www.uddi.org>

The information that an organization can register includes several kinds of simple data that help others determine the answers to the questions “who, what, where and how”. UDDI enables simple information about an organization – information such as names, contact information, etc., to be registered in a systematic manner.

### SECURITY LAYER

The **Security Assertion Markup Language (SAML)** is a XML-based framework for exchanging security information. This security information is expressed in the form of assertions about subjects, where a subject is an entity (either human or computer) that has an identity in some security domain.

The eXtensible Access Control Markup Language (XACML) is used to define a core schema and corresponding namespace for the expression of authorization policies in XML against objects that are themselves identified in XML.

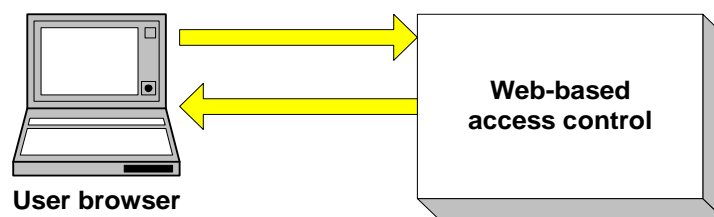
XML Key Management Specification (XKMS) defines protocols for distributing and registering public keys, suitable for use in conjunction with the proposed standard for XML Signatures (XML-SIG).

### SUPPORTING INTEROPERABILITY

Prior to Web-based authentication and the use of HTTP as a transport protocol, there have been local area network (LAN) centric protocols that bind clients and servers, employing the Distributed Component Object Model (DCOM) and Component Object Model (COM). DCOM/COM essentially binds objects and machines within a client-server framework suitable for a LAN. The fact that Microsoft has now embedded Web-based services, like XML and SOAP (see .NET), within their latest OS release is significant in terms of interoperability. This has created, by default, a DCOM/COM-to-.NET interoperability platform. This is helpful when considering interoperability with those applications currently deployed within a DCOM/COM environment.

### WEB BASED ACCESS CONTROL AND AUTHORIZATION METHODOLOGIES

Browser-based thin-client authentication represents a common denominator to the authentication and authorization process (as contrasted to an enterprise-centric framework like a DCOM/COM object LAN environment). In a thin-client authentication/authorization model a challenge/response process is used for the authentication of users (like submission of a username/password).



**Thin-client authentication  
(challenge/response)**

Figure 3. Challenge-response system

## Web Services Eco-System and SAML, cont. By: David Sweigert

Thin-client access via a uniform user interface (UI) is a common and supported process by nearly a dozen software vendors. Thin-client UI provides a baseline to users and a lightweight development environment. Therefore, it is instructive to note the trends of several such vendors, as their support, and subsequent product releases, create economies of scale for authentication/ authorization.

.....

*Look for Part 2 of this article in our Summer 2005 edition.*



David Sweigert, CISSP, PMP, is the Director of Information Assurance for Data Systems Analysts, Inc. He is the former State IT Security Policy Officer for the State of Ohio and a U.S. Air Force veteran. He may be contacted at [sweigertd@dsainc.com](mailto:sweigertd@dsainc.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.

**5/19 - 5/20, 2005 Dallas, TX**

**5/23 - 5/24, 2005 Black Hat  
Seattle, WA**

**6/10 - 6/11, 2005 TechnoSecurity  
Myrtle Beach, SC**

**7/14 - 7/15, 2005 Boston, MA**

**7/23 - 7/24 or  
7/25 - 7/26, 2005 Black Hat  
Las Vegas, NV**

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

(719) 488-4500

[info@securityhorizon.com](mailto:info@securityhorizon.com)

<http://www.securityhorizon.com>



***Computer Security for the Home and Small Office***

Thomas C. Greene

Paperback - 405 pages (2004)

Apress ISBN: 1-59059-316-2

*[Full Disclosure: I have been quoted by Greene for past articles in a friendly/professional capacity. He has also written articles that were accusatory to me and attrition.org in the past. Translated: I owe him nothing.]*

The first and most obvious question that will come to some people is where an alleged hack from The Register [1] gets off writing a book on computer security. After reading the entire book, you'll understand that his last five years covering computer security and playing Windows solitaire has paid off. Just as he writes his news material in an "irreverent editorial style", so shall I in this quippy review.

ins and outs of firewalls or other security technology. Some books came out to address this issue but ended up being dull, covering the absolute basics while ignoring serious issues, or contained more errors than facts. After all this time, one book seems to be ideal for the everyday user, and read to educate them on more than configuring a Windows machine or personal router.

Overall, the book favors the end Windows user in time spent explaining the gritty details of basic security. However, neophyte Linux users will be able to learn some of the basics as applies to them, as Greene considers both platforms when dealing out information. Using plain wording unencumbered by superfluous jargon, the lessons you need are easy to understand, well organized and well written. Fortunately for you, the book was technically reviewed by Robert Slade [2] before hitting the shelves, and it shows. It's a pleasant

***"It's a pleasant change of pace reading a book without sighing in disgust every few pages when the author typically proves they are better off working at McDonalds."***

Computer security isn't just for hackers or professionals, it's something every computer owner and operator should be aware of. When we read about the worm-of-the-week, it is infecting and compromising tens of thousands of machines, often owned by you, the end user. How are the average computer user expected to protect their home systems when security is a discipline and career? In the past, they were expected to read web sites, trust Microsoft and possibly struggle through an overly technical book detailing the

change of pace reading a book without sighing in disgust every few pages when the author typically proves they are better off working at McDonalds. The Greene/Slade combination is definitely worthy of Subway.

The last third of the book moves beyond configuring your computer and delves into the single most important aspect of computer security: Common Sense and Awareness. Rather than continue on with tech tips, Greene opts to educate the end user about the

security industry, which is a blessing in disguise. Later chapters warn you on FUD (Fear, Uncertainty and Doubt), how to avoid industry charlatans, and how to apply common sense toward keeping unwanted people out of your system.

Greene also delves into some of the great debates of our time, like open vs. closed operating systems (Windows vs. Linux). His journalistic experience shines through here and Greene delivers perhaps the single best summary of why Linux may be a better option for you than Windows. He dispels the myth that it is too complex, that it doesn't run the programs you want, and the shortcomings of Windows.

The last section covers a wide variety of topics that move beyond the personal computer and into daily life, as computers may affect you. This is a nice touch, as a large part of the population doesn't follow technology news despite the drastic effects it can have on your life. By understanding what is looming around the corner, you can better prepare for changes that affect the Internet, your computer, and your security.



No review is complete without a little criticism! The biggest complaint I can direct at this book is the practice of lengthy and largely worthless Appendix. Starting on page 297 (Appendix B) and ending on page 392 (Appendix C), about half of the material would have been better left on Greene's new website [3]. Giving us long lists of trojan port numbers for example, isn't the most helpful thing you could have filled those pages with.

All in all, if you are an average Joe when it comes to computers and security, grab a copy of this book. It *will* help you learn what you need to know, and it will make you realize that security is more than tweaking options on a computer configuration screen. That lesson is still hard to teach to some so-called security professionals, but one you will learn rapidly with this book.

[1] <http://www.theregister.com/>

[2] <http://victoria.tc.ca/int-grps/books/techrev/mnbk.htm>

[3] <http://www.basicsec.org/>

.....

**Brian Martin** is a member of Attrition.org (<http://www.attrition.org>), a computer security Web site dedicated to the collection, dissemination and distribution of information about the industry for anyone interested in the subject.

*The following is the second of a four-part series on Covert Channels.*

---

---

**I**n my last article, I concentrated more on the general aspects of Covert Channels; explaining more of what they were than delving into the specifics of each one. This edition, however, will begin a more in depth analysis of Covert Channels by covering the first topic, **Steganography**.

Steganography has been around for thousands of years, in one form or another. The word comes from the Greek words “steganos”, which means *covered*, and “graphie”, which means *writing*. There are tons of historic examples of how steganography has been used through the years, including the wax tablet example I used in the last article. But the concept has evolved and now takes on a slightly different meaning as we look at it in a technological sense.

The Internet has created a massive marketplace where anyone in the world can post their information or opinions. There are personal websites that are nothing more than electronic slideshows of family vacations. You can find thousands of sites dedicated to just chatting, or blogging. Aside from just the web though, you can find areas for file sharing, streaming music or video, and even online gaming. Each one of these has the potential to store or transmit hidden information.

So what does that mean for steganography? If we take the literal meaning of covered writing,



then we're talking strictly about mechanisms for hiding information that use a *cover*. The most popular forms of this utilize digital image files and digital audio files. These are binary files into which we can hide a payload of information. For the purposes of this series of articles, we'll be using this more technically based definition.

These types of files, image and audio files, are considered by many to be relatively benign and are often immune to the security policies of the organization. In many organizations, employees are allowed to store or email these types of files without restriction, which could cause a grave concern to the organization.

As an example, look at the two images in Figure 1. One of them is the original image, while the other has a text file hidden within it. Can you see the difference? In our example below, the image on the right is the one with the payload hidden inside, while the one on the left is the original image.



Figure 1

I used an application known as S-Tools 4 to hide a text file in the original image. But there are literally hundreds of tools available for creating similar types of steganography. For a quick glimpse of these tools, check out [www.stegoarchive.com](http://www.stegoarchive.com).

So how do we currently detect when steganography is in use? In some cases, if the user tries to hide too much information, we'll be able to see or hear distortion in the file we're dealing with. In most cases, hiding much more than 25% will likely result in this type of distortion. Other times, we can look for various signatures within the file that can tell us that information may be hidden there. When we're looking for signatures, we're looking for items that are out of the ordinary. As an example, if you look at the two images in Figure 2, you'll see the hex output of two digital images. The first one is the original file, unmodified. The second is the one in which I have hidden a Microsoft Word document.

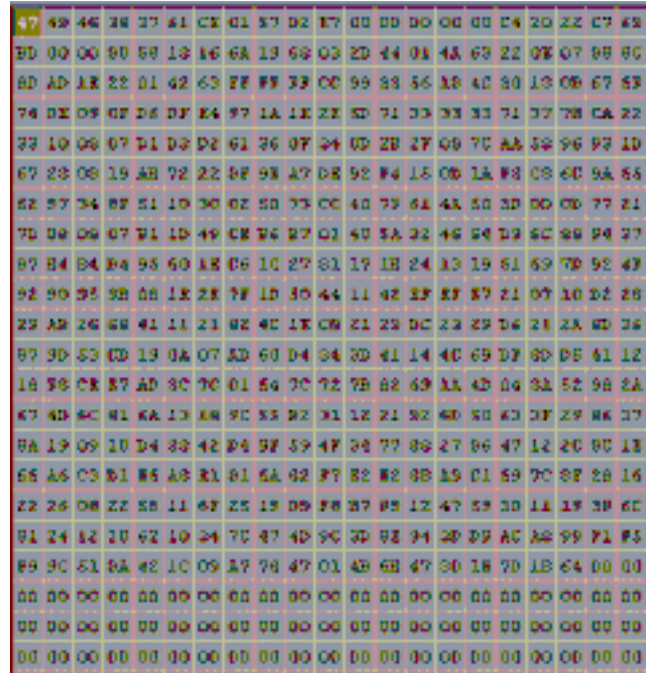
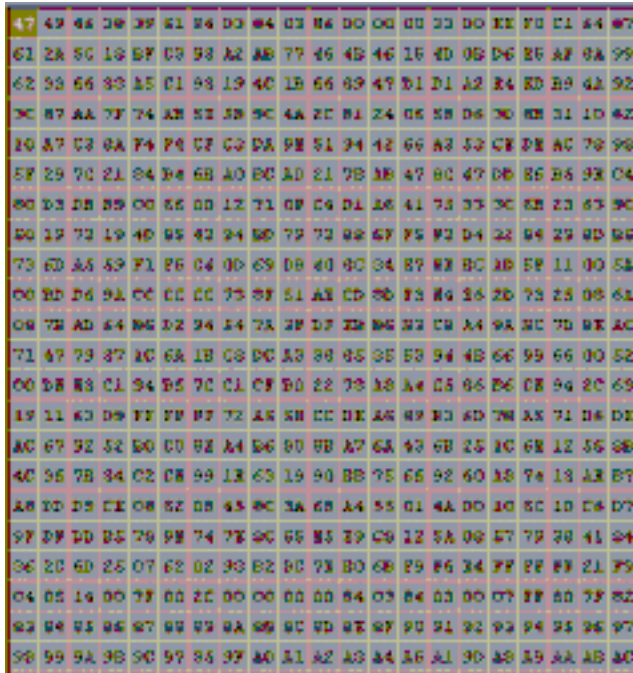


Figure 2

The thing to notice is the long string of null characters, identified by the “00”, at the end of the screenshot. I’ve obviously shortened the output so that the images would fit within the Journal, but you should get the idea. It’s unnatural to have a long string of null characters. Each application could potentially leave behind its own signatures. In essence, signature based stego-detection becomes very similar to anti-virus protection. The signature databases will need to be maintained and updated.

There are other means to detect steganography, but it requires more space than I really have here. Suffice it to say that this is still a very young area. Detection of these types of activities is lagging years behind the technology that creates them. But understanding that these types of things exist will help you start thinking of methods to counter them and protect your critical information. The best places to start are to limit access, in a least privilege fashion, to all your users. If they’re not allowed to install non-

work related applications on to their computers, you’re helping limit your risk. Also, consider periodic checks of organizational computers and servers, looking for applications that can be used to hide information. Understanding that your information could be leaking out of your organization without your knowledge is the first step in addressing the risk.

For more information on the topic, consider reading my new book, “*Hacking a Terror Network*” or Eric Cole’s “*Hiding in Plain Sight*”. Both are available from most major book dealers or online.

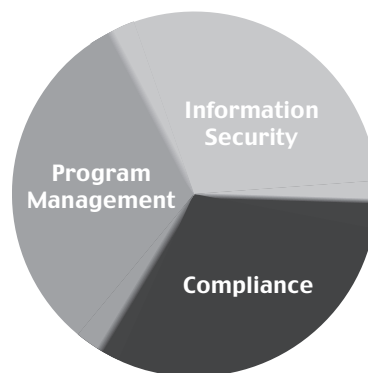
*Look for Part 3 of this article in our Summer 2005 edition.*

Russ Rogers is the CEO and CTO of Security Horizon. He is the Editor in Chief of the Security Journal and can be reached at [russ@securityhorizon.com](mailto:russ@securityhorizon.com).



# Give Us Your Poor, Your Troubled, Your Wretched, IT Projects...

DSA is the only company that blends project management, information security and regulatory compliance to deliver strategic, secure and mission-critical IT solutions.



## **DSA**

**PMI** Project  
Management  
**R.E.P.** Institute

Eight Neshaminy Interplex, Suite 209  
Trevose, PA 19053-6980  
(215) 245-4800 • (215) 245-4375 fax  
[www.dsainc.com](http://www.dsainc.com)

## Qualification Based Selection for the Procurement of Cyber Security Engineering Services



Selecting the right cyber security firm to provide computer network security is as important as selecting the right doctor. You really want a well-trained, credentialed, and experienced firm with whom you can share your most confidential information. Security engineering firms aren't as regulated as other engineering professionals are -- so how can you tell if you've hired the best firm to help with your particular needs? I turn to a method used in other engineering disciplines, *Qualification Based Selection*

### DEFINING QBS?

*Qualification Based Selection* is the process recommended for most other engineering disciplines and is superior to *Value Selection* as the most objective method of selecting a security-engineering firm. Compelling evidence from the Information Technology industry indicates that in selecting the services of a cyber security-engineering firm, the qualification and capability to meet a client's specific objectives should be the primary consideration. Correct selection will have a major bearing on the quality, cost, and success of the project.

### SELECTION

Selection of the optimum firm will have a major bearing on ROI in terms of quality, cost, and performance. Using QBS, the choice is made on standardized set of criteria and a fee is negotiated after the optimum firm has been selected. Figure 1 illustrates the process.

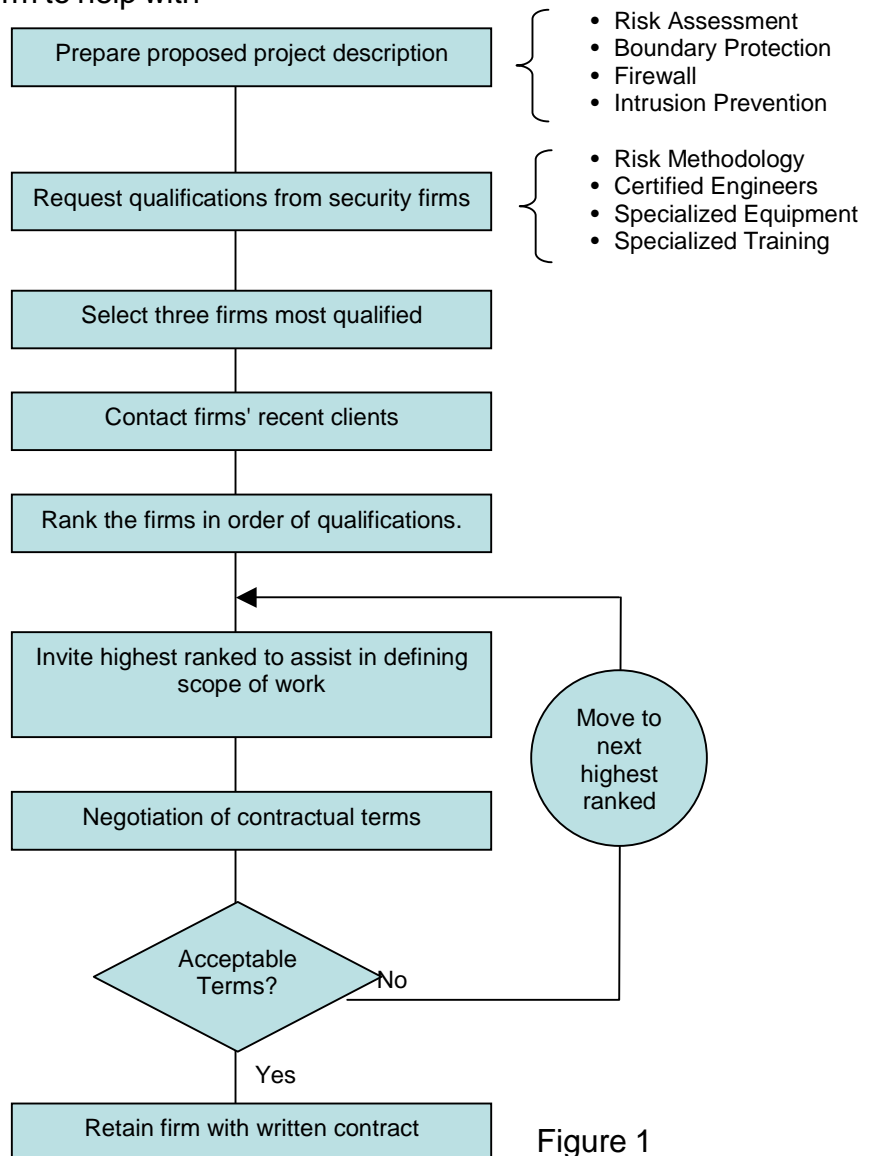


Figure 1

The central areas of focus for the remainder of this article are the six key qualification factors in the selection of a cyber security-engineering firm:

- Skills and qualifications of personnel
- Technical competence
- Reputation
- Experience on similar projects
- Capacity to undertake the project
- Understanding and commitment to the client's interests.

### Skills and qualifications of the personnel

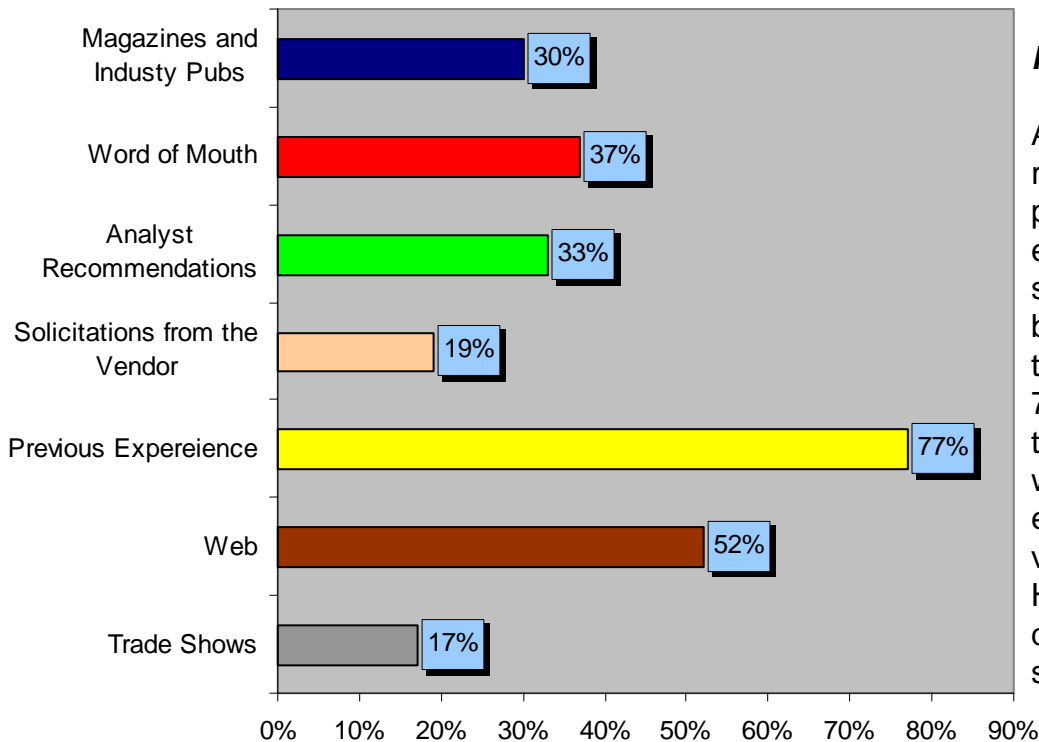
A crucial factor in the selection process is the quality of the individual engineers. Fortunately, the International Information Systems Security Certification Consortium or (ISC)<sup>2</sup> has some excellent certifications to measure an individual's quality. (ISC)<sup>2</sup> is recognized around the world for its information security certifications, including the Certified Information Systems Security

Professional (CISSP<sup>®</sup>), considered the Gold Standard among security professionals. Other certifications, like HIPAA or Sarbanes-Oxley may also be important depending on your industry.

### Technical competence

Overall technical competence of a cyber security firm can be evaluated through the methodology they use. Look for a firm that uses a recognized methodology.

Methodologies worth considering include the National Security Agency's, Information Assurance Methodology (IAM), Carnegie Mellon's Operationally Critical Threat, Asset and Vulnerability Evaluation<sup>SM</sup> (OCTAVE), and the ISO 17799 / BS7799. NSA has a formal evaluation process for security firms that have adopted their methodology. The NSA evaluates and rates these firms before giving them a capability rating. NSA's list of evaluated firms is at <http://www.iatrp.com/companies.cfm>.



### Reputation

A company's reputation is a vital part of the selection equation. In a survey conducted by Tech Republic,<sup>1</sup> the method used 77 percent of time to rate reputation was previous experience with the vendor's products. However, if you're dealing with cyber security for the first

Source: Tech Republic Survey

<sup>1</sup> Beth Blakely, "Consultants choose vendors based on experience", *Tech Republic*, 2 February, 2002

time, some other metrics are needed to quantify reputation. The survey helps again, by illustrating that researching a firm's web site and collecting word of mouth recommendations accounted for next most used methods.

Ultimately, the reputation that you're most interested in is the quality of the product or service as well as the post contract support you can expect.

### ***Experience on similar projects***

Past performance about a security-engineering firm's experience is a major criterion for selecting a quality supplier. Congress identified past performance information as an evaluation factor for Federal acquisition streamlining.<sup>2</sup> Without considering past performance, a firm could easily write a winning proposal, without having any experience to back it up. Security-engineering companies with significantly better performance records might be overlooked

### ***Capacity to undertake the project***

The capacity to undertake the project provides a general prediction of capability to deliver. This step will prevent a situation where the security-engineering consultants, and possibly your staff, make heroic attempts to achieve success against the odds. Don't be fooled by the size of a firm! Larger firms have no better chance of success than small well-run businesses. In fact, a small business comprised primarily of trained and certified security engineers can often do as much or more than a larger firm. Three crucial questions when evaluating capacity are: 1) what's the profile (servers, workstations, and

architecture) of largest client you've successfully completed; 2) how many experienced and certified engineers are available for this contract, and 3) what type of project management system do you have in place.

Be suspicious of any firm that can't describe their project management tools and processes. Firms that can crisply set down what they are promising to produce are the ones most capable of undertaking the project. Remember that clients don't care about how you're going to satisfy the contract - they care about the results (promises). A phrase that I try to live by is: "*Under Promise and Over Deliver*".

### ***Understanding and commitment to the client's interests.***

The final area of consideration is an understanding of the client's core competencies. If you want to do business with a client, you need to know their mission and understand their responsibilities. Too often, corporate people will say, "I have this tool that does this" or "We can install a system that does that." However, if it doesn't address a client's priorities, it is just of casual interest to the client. The security-engineering firm must place the client's interests before anything else.

### **HOW DOES QBS PROVIDE THE BEST ROI?**

When both parties focus on scope, project details, and defining their respective responsibilities, the security firm can develop a more accurate scope of work and associated cost. With QBS, the client has selected the best firm and can then negotiate the scope and bottom-line cost, thereby achieving the highest return on investment.

<sup>2</sup> Federal Acquisition Streamlining Act (FASA), signed into law October 13, 1994 (P.L. 103-355)

Cost-based selection processes, often undermine the anticipated return on investment with fuzzy Request for Proposal (RFP) language. The responding firms' interpretations of that language results in poorly defined or understood statements of work needed to complete the project on time and within budget. Consider the following example:

*A healthcare facility issues an RFP containing a scope of work and a request for a firm-fixed price estimate. Four firms respond with prices ranging from \$35,000 to \$350,000. The \$35,000 firm seems like a bargain, but the large range of estimates indicates a poor understanding of the project between the client and the bidding firms. Deciding a winner based on cost means additional charges are inevitable that will probably surface mid project. At this point, clients, and contractors cease being partners and turn into adversaries.*

## CONCLUSION

Security Engineering is a new and often ill-defined area that can leave many wondering how to select the correct firm to handle the task. Qualifications Based Selection for security-engineering firms, may be the answer to avoid the pitfalls. Using an established methodology of selection based on objective criteria, a best-of-breed decision can be determined before cost even enters the picture. Moreover, by adhering to the decision criterion along the way, a firm can be sure that a well-qualified, accredited, and capable firm is going to assess the security of their cyber resources.



Glenn Watt is the President, & CEO of Backbone Security.Com. He can be reached at [glenn.watt@backbonesecurity.com](mailto:glenn.watt@backbonesecurity.com) or at 888-805-4331.



*The following is the conclusion of a two-part series on Penetration Testing.*

.....

*Editor's Note: If you downloaded an early version of last edition's Journal, please note the following changes to this article:*

*- Bullet 1, first paragraph, "...Black Box Testing or Red Teaming" should have been White Box Testing.*

*- Bullet 2, first paragraph, "...White Box Testing or Blue Teaming" should have been Black Box Testing.*

*We apologize for any confusion.*

***The last edition covered the basics of penetration testing up through planning. We now continue through the process...***

## Exploitation

Once the plan is in place, it's time for what most people consider "the fun stuff". Actual weaknesses and how to exploit them will be left to the plethora of books and articles detailing the exploitation of systems and services. Rather, we will focus on the one subject often ignored and usually left out.

The key to pen-testing a customer is documentation. Each and every step of an exploit should be documented. How the weakness was discovered, the code or actions taken to exploit it, the actions taken after the exploit, the EXACT nature of any data modification or access, the success or failure of each exploit attempt, etc. All of this information will be needed by the customer and sets apart the actions of the hired guns from the unwanted attacker. Even such basic information such as directory and permissions listings should be kept for detail



in the final report.

The exploitation itself will follow the agreed upon rules or scenarios described early in the engagement, and continue until the goal or defined timeline is reached.

## Reporting

Once the exploitation process is complete, a final report should be readied including all

evidence collected during the project. This include research documentation (informing the customer of possible unwanted information leaks) as well as any retrieved files or locations of modified data.

Often, the testing will end after only one or two weaknesses are exploited, as the goal has been reached. Of great benefit to the customer however is the planning documentation created including all possible weaknesses discovered. Just because some may not have been tested do not mean they are not vulnerable. This allows the customer to perform additional investigation internally.

A clean-up section should include detailed instructions for repairing any damage done to the system (installed rootkits, modified routes and ACLs, edited permissions tables or firewall rule sets, etc.). Also, a map to modified data files or tables should be made including the original information and the new

# Penetration Testing

By: Matthew Hoagberg and Ted Dykstra

information. During the exploitation, copies should have been made of any originals and their modified counterparts. At the end should come a recommendation list for mitigating all discovered weakness, whether exploited or not.

## Expectations

Penetration testing will uncover technical vulnerabilities as well as flaws in your security policy and procedures. After the test you should receive a report that not only lists the findings or vulnerabilities found, but whether it is a high, medium, or low threat to your organization. Also included should be ideas on how to correct or remediate the vulnerabilities to your organization.

## Conclusion

Penetration testing can:

- Increase the awareness and importance of IT security
- Justify funding for IT Security and allow you to plan for an IT Security budget
- Provide due diligence and help maintain industry standards
- Allow you to resolve the weaknesses or vulnerabilities within your organization after being discovered by the testing team
- Be able to see the return on your investment when you consider the cost to your organization if you are unable to access your information, if your information has lost its integrity, or sensitive/classified information becomes available to individuals outside your organization

For more information on the subject of penetration testing, please take a look at some of the following books:

### **Hack I.T.: Security Through Penetration Testing** (Addison-Wesley)

A good introductory guide to the concepts and goals of penetration testing

### The **Hacking Exposed** Series (McGraw-Hill)

Several good books in a series on detailed technical exploits across multiple platforms

### **Hacking: The Art of Exploitation** (No Starch)

An interesting text discussing technical exploits (programming experience recommended)

### **Google Hacking for Penetration Testers** (Syngress)

A great text on how to use Google as a security-testing tool

### **The Shellcoder's Handbook: Discovering and Exploiting Security Holes** (John Wiley & Sons)

An excellent book detailing exploitation through coding (programming experience recommended)

### **WarDriving: Drive, Detect, Defend, A Guide to Wireless Security** (Syngress)

A detailed discussion of 802.11 wireless weakness and protections



*Matthew Hoagberg and Ted Dykstra are Security Consultants for Security Horizon.*

They may be contacted at  
matt@securityhorizon.com and  
ted@securityhorizon.com

*The following is the first half of a two part article.*



## *Introduction*

As discussed in “Google Hacking for Penetration Testers” from Syngress publishing<sup>1</sup>, there are many different ways to perform network reconnaissance using Google. Since the publication of that text, many different ideas and techniques have come to light. This document addresses one

In most cases the quality of the target list often depends on the sheer volume of traffic and the amount of time and effort the attacker is willing to expend on the exercise. From the defender’s standpoint, a flood of mapping traffic is often easy to detect, and most intrusion monitoring tools are well equipped to detect these common signatures. If an attacker is willing to offload some of these tasks to Google, less packets are passed to the target, and the attacker can rely on some of Google’s strengths, in this particular case the ability to group hosts by domain name, and the ability to perform intelligent language

*If you’re evil, stop reading this and go work out some aggression on a sack-o-potatoes or something.*

interesting technique, which we’ll call DNS name<sup>2</sup> prediction. This document assumes you have some knowledge of basic network recon, and is not intended as a hand-holding approach to hacking. If you’re evil, stop reading this and go work out some aggression on a sack-o-potatoes or something.

## *Why Google?*

If an attacker is willing to throw tons of packets at a target network, he can develop a fairly decent list of targets in very short order.

analysis. In an extreme case, it’s even possible for an attacker to get a decent list of targets without communicating with those targets at all, instead relying only on information from Google. If the attacker is willing to use additional techniques such as standard DNS lookups in addition to Google queries, the attacker can maintain a relatively low profile while building a very decent target footprint. Security professional can also use this technique help protect their clients from undue exposure.

## *Grabbing Hosts*

The first step in compiling a target list is to decide on a top-level target. As a security professional, this is almost certainly dictated in the form of a customer’s network holdings, their domain name, IP range, or some combination of these. If the target is an IP

<sup>1</sup> <http://www.syngress.com/catalog/?pid=3150>

<sup>2</sup> It’s worth mentioning that there is a distinct difference between the terms “hostname” or “DNS name” and “subdomain” although these terms are often used interchangeably. We use the term ‘DNS name’ to refer to any resolvable address, so if a subdomain resolves... we call it the wrong thing. Sorry.

## DNS Name Prediction with Google, cont. By: Johnny Long

range, the security tester is very limited in what can be discovered and in most cases the tester will often skip the target discovery phase, instead beginning the assessment by feeding that IP range into some type of industrial grade vulnerability scanner. If the client has supplied a domain name or has authorized a “carte blanche” scan of all it’s network holdings, the tester has more discovery leverage and will most likely begin the testing with a fairly robust target discovery phase, in which the techniques discussed here can be used fully.

Several techniques for host detection have already been discussed in other places, so

for this purpose is `google_miner.pl`<sup>3</sup> by Roelof Temmingh of `sensepost.com`. This tool automates various (*site* operator-based) Google queries aimed at a domain name. Figure 1 shows the output of this tool when aimed at `sdsu.edu`.

This type of scan produces a decent list of what appears to be host names, although further investigation reveals they are actually subdomains.

*Expansion: Using Google To Manually Determine Word Relationships*

Next, we will try to intelligently expand the list



```
Terminal — sh — 79x23
Subdomains:
-----
math.sdsu.edu
biologylessons.sdsu.edu
serg.sdsu.edu
geology.sdsu.edu
foundation.sdsu.edu
scec.sdsu.edu
dr-jamesollis.sdsu.edu
music.sdsu.edu
eli.sdsu.edu
bio.sdsu.edu
cs.sdsu.edu
scl.sdsu.edu
edcenter.sdsu.edu
so.sdsu.edu
chemistry.sdsu.edu
csrc.sdsu.edu
ces.sdsu.edu
physics.sdsu.edu
tvcampus.sdsu.edu
borderecweb.sdsu.edu
root#
```

Figure 1: `google_miner.pl` results for `sdsu.edu`

for the purposes of this document we’ll assume an attacker has collected hosts with Google queries. For example, an attacker might begin a footprint for `sdsu.edu` with a query like `site:sdsu.edu`. Although host and subdomain names can be gathered with simple Google queries (using the `site:` operator, for example) in many cases, automation is needed to quickly parse through the results. One tool that can be used

of targets. When reviewing this list, it becomes relatively obvious that some of the subdomains (specifically *math*, *geology*, *chemistry* and *physics*) are named for college disciplines. An attacker could easily expand this search by performing WHOIS or forward DNS queries for other similarly

<sup>3</sup> `google_miner` available from the `sensepost.com` website, perhaps as a different name

## DNS Name Prediction with Google, cont. By: Johnny Long

named subdomains or hosts like *history.sdsu.edu* or *geography.sdsu.edu*. This technique works well as long as the word pattern is recognized, but this requires human intervention or some relatively heavy lifting by a program. In cases where a pattern is not relatively evident, or in cases where word relationships need to be determined programmatically, our old friend Google once again comes to the rescue. Google provides a relatively easy mechanism for determining whether or not words are related. Let's take a look at a few examples. First, consider the words *cat*, *dog*, and *pickle*. Anyone can plainly see that only two of the three words are related (*cat* and *dog*, both domesticated house pets) and even a poorly contrived computer program would have little trouble figuring this out, but for the sake of example, let's have Google give us an idea of the relative association of these words. We can do this in three queries, as shown in Table 1.

Google Query	Google Results
cat dog	11,000,000
pickle dog	341,000
pickle cat	255,000

Table 1: Google comparison of cat, dog, and pickle.

According to Google, the words *cat* and *dog* are referenced together on the web much more than either *pickle* and *cat* or *pickle* and *dog*. This gives *cat* and *dog* a stronger relative association. This is a simple example, but let's take a look at a slightly more complex example. Consider the three words *cat*, *dog* and *horse*. As anyone can tell you, these three words are all related (they all refer to animals, specifically mammals, and to some extent *domesticated* animals) but a

computer program would have some degree of difficulty determining that only two of the three words refer to domesticated *house pets*, thus making those two words more closely related. Even a child would describe cats and dogs as more related than cats and horses or dogs and horses, even if the child couldn't accurately describe *why* those two words are more related. Once again, let's turn to Google to determine which pair of words floats to the top.

Google Query	Google Results
cat dog	13,600,000
horse dog	9,520,000
horse cat	8,760,000

Table 2: Google comparison of cat, dog, and horse.

As shown in Table 2, the terms *cat* and *dog* again float to the top even though all the words are fairly closely associated. The point here, is that Google offers a relatively simplistic mechanism for an attacker to determine relationships between entire lists of words, and as we'll see in the next step, word relationships can play a key role in DNS name prediction. Let's focus again on our example scan of *sdsu.edu*, which as an aside is an excellent institution and my use of their domain is in no way a statement about their overall security posture. Have I said enough to keep myself in SDSU's good graces? =)

### *Expansion: Automating Google Word Relationship Determination*

When we last left *sdsu.edu*, we had a list of subdomain names and had determined that there was some sort of pattern to the naming convention they were using. Using the Google query techniques we just explored, we could



## DNS Name Prediction with Google, cont. By: Johnny Long

the next most relevant words as shown in Figure 3.



**Figure 3: Basic set expansion with Google Sets**

This small set of 15 predicted terms could be expanded to a large set very easily, although the strength of the word associations suffers once more results are presented.

Applied to our SDSU names, Google Sets expands the words *chemistry* and *physics* to the following small set:

- PHYSICS
- CHEMISTRY
- BIOLOGY
- Mathematics
- Geology
- Astronomy
- Psychology
- Engineering

- English
- Geography
- Economics
- History
- Statistics

Armed with this list, forward DNS queries could be made for each of these words, followed by the sdsu.edu domain name.



.....

*Look for Part 2 of this article in our Summer 2005 edition.*

Johnny Long can be reached at  
[johnny@ihackstuff.com](mailto:johnny@ihackstuff.com)  
<http://johnny.ihackstuff.com>