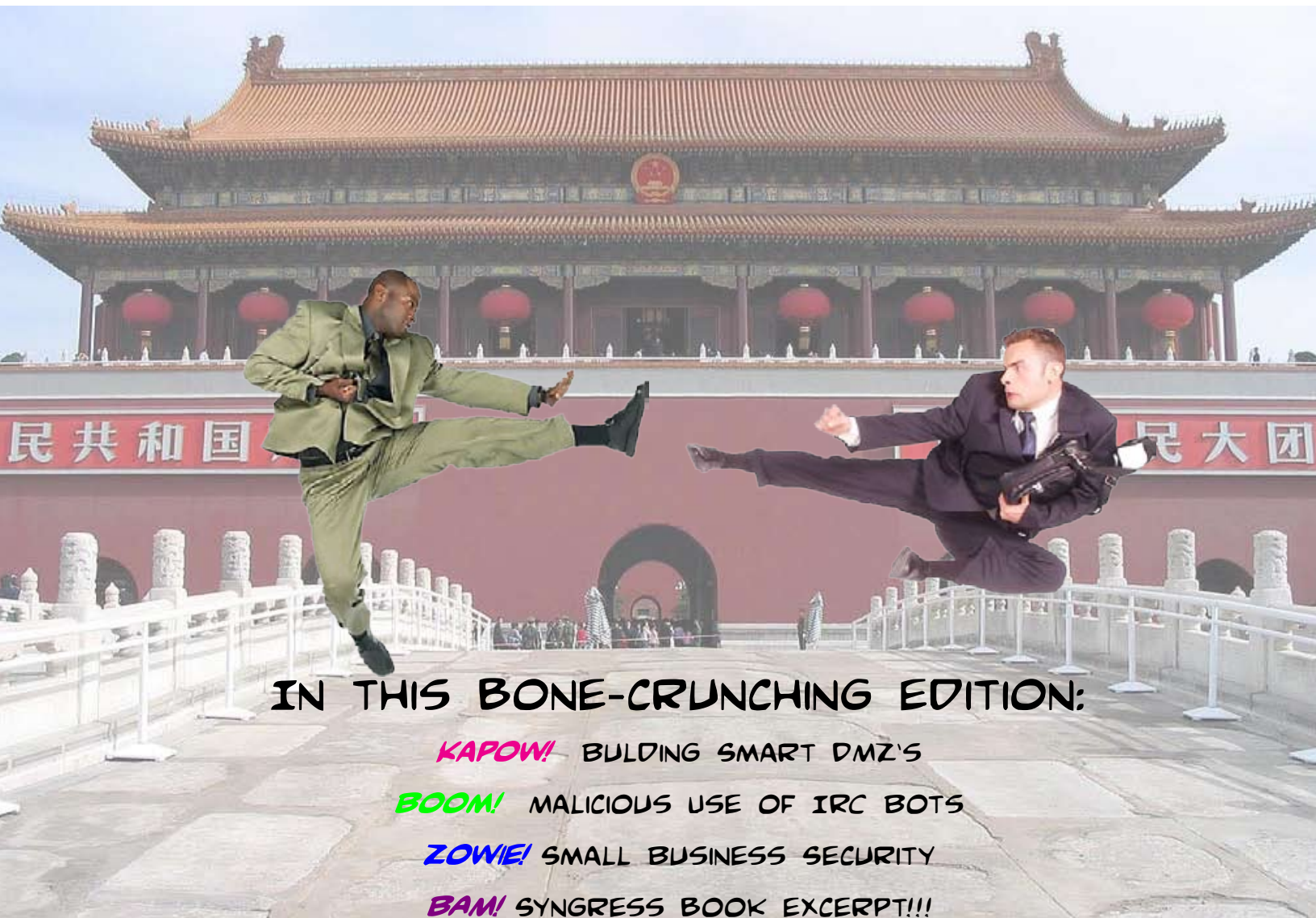


# the security journal

 **Black Belt Security:**  
Mastery through time and effort



**IN THIS BONE-CRUNCHING EDITION:**

**KAPOW!** BUILDING SMART DMZ'S

**BOOM!** MALICIOUS USE OF IRC BOTS

**ZOWIE!** SMALL BUSINESS SECURITY

**BAM!** SYNGRESS BOOK EXCERPT!!!

**Volume 19 - Spring 2007 Edition**



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](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**  
*russ rogers*.....p. 3

**IAM Course Schedule**.....p. 4

**Building Smart DMZ's**  
*timothy mullen*.....p. 5

**DenyHosts**  
*brian kirouac*.....p. 11

**IEM Course Schedule**.....p. 12

**Syngress Publishing Book Excerpt**  
*jack wiles*.....p. 13

**Malicious Use of IRC Bots**  
*patrick mcneil*.....p. 18

**Security in Small Business**  
*greg miles*.....p. 22



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

# Swim with the Best



Cyberspace is an information feeding frenzy. Stay off the menu. Black Hat USA brings together the most knowledgeable and respected figures in information and computer security to help you keep your edge.

Six days. Thirty Classes. Ninety presentations.



## Black Hat®

Briefings & Training USA 2007

July 28-August 2 • Caesars Palace Las Vegas

[www.blackhat.com](http://www.blackhat.com)

### sponsors

diamond



platinum



gold



silver



## Notes From the Editor



**Russ Rogers**  
CISSP  
Editor in Chief

### .....

## Black Belt Security

As April draws to a close and Spring really gets under way, I find myself looking at another major milestone in my life. After two years of hard work, and a genuine dose of blood, sweat, and tears; I'm finally achieving my First Degree Black Belt in Kung Fu. I started Kung Fu in April of 2005 as a way to get into shape, hang out with friends, and perhaps learn to defend myself. I stayed with it because I really enjoy it, not to mention my other goals.

It takes a lot of time and hard work to reach this point. There are 26 separate forms that have to be memorized and demonstrated effectively in order to pass this test. It's a constant exercise in

patience, dedication, and sheer will power. And now that I'm finally at this point, do you know what I've learned? I'm just getting started.

The reason I'm relating this event in my life to you is that, for me, it applies equally to the field of information security. At this point in my career, I'm absolutely positive that "security" isn't a destination. In fact, I'd hesitate to even call it a journey. It's more of an Odyssey style epic voyage that leads you past a multitude of destinations, through a variety of different paths, and finds you battling evil creatures.

Most people like to reach their goals. If you work in this industry, you may have such lofty goals as creating a useful and testable business continuity plan, or maybe you're working on creating an effective security awareness training program that people are actually interested in using. Regardless of what your project is, it probably seems quite daunting at times.

So what happens in a year or two when you've managed to finally meet your objectives? You've done it; the training program is a huge success. The work was hard. The hours were long. But management loves what you've created. You're there. *Welcome to Black Belt.*

But wait a second, I'm willing to bet money you realized along the way that there is still a lot of work left. While you were working on the business continuity plan, you may have realized that the

## Notes, cont.

organization's anti-virus solution is lacking, or perhaps your patch management program has serious issues.



The true indication that a person is a Black Belt in information security is that they realize how far they've come, but they also realize how far they have left in front of them. It's an acknowledgement of not only their current knowledge and experience, but also their deficiencies. A black belt understands how much more is left to tackle. It's a humbling thought, but you've made it this far. So roll up your sleeves and get started. People are counting on you.

~ Russ



5/7 - 5/8, 2007	Olympia, WA
5/8 - 5/9, 2007	Dallas, TX
5/15 - 5/16, 2007	Atlanta, GA
5/22 - 5/23, 2007	Boston, MA
5/30 - 5/31, 2007	Myrtle Beach, SC
6/12 - 6/13, 2007	Fairfax, VA

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 further information, please contact us at:

(719) 488-4500

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

<http://www.securityhorizon.com>



## ***...how to design and deploy DMZ structures that not only protect your assets, but that help you enforce corporate policy as well...***



***Interested in learning more from Tim? Take his class at Black Hat USA this summer and receive a \$200 discount for Security Journal readers only!***

Enter code is **BHUS7MSNBH** at the time of your online registration. It is case sensitive and **MUST** be applied at the time of registration.  
*The coupon code cannot and will not be retroactively applied.*

**Welcome** to the first installment in my series on Building Smart DMZ's. Over the next few publications, we'll discuss different topologies and methodologies you can leverage in order to build robust DMZ deployments that will dramatically increase your security posture as you publish Internet-based services. We'll outline the technical aspects of back-to-back DMZ configurations, multi-segment DMZ's, and authenticated perimeter segments. You'll learn why to use them, and what benefits you gain from each "style." But before we get to the tech that will secure your assets, I'm going to discuss a concept in DMZ design that will allow you to keep them secure over time via strict adherence to policy. I call this structure a "Multi-Segmented, Role-Based DMZ" or MS-RDB.

### **The MS-RDB: A Self-fulfilling Policy Structure**

So let's get started-- but first, we'll make sure we've defined our terms properly. There seems to be some disagreement within the security community as to what a "DMZ" actually is. Some consider a DMZ to be a network "free for all" where anything goes: a "no man's land" where systems are banished

into storms of network traffic as a sacrifice to hackers. I completely disagree with this mindset.

Like the physical zone at the Korean 38th Parallel from which the networking term "DMZ" was coined, I consider the DMZ to be a highly defined and seriously limited zone where all protocols, systems, and services are very tightly controlled. It is a zone of "least privilege" and "security in depth." Most importantly, it is a zone where said assets and services are defined by policy. Some have considered adopting the term Perimeter Network Segment to better describe this concept and to obviate confusion surrounding "DMZ," but I'm sticking with the original term. Besides, who wants to have to explain overtime hours to their boss because they had a virus outbreak in the PNS? No one does, so "DMZ" it is ;)

### **DMZ Entropy**

I've seen it a hundred times, literally. What starts off as an efficient, secure DMZ segment ends up a festering cesspool of insecurity. Initially, network engineers and security personnel properly segment off publicly assessable resources (i.e. a web server), only

allowing in HTTP(S) to just that box in the DMZ, and require internal administration be performed via a one-way RDP rule. Nice. But before you know it, a business unit determines they need an Oracle driven customer-facing application running on the web server, which then gets loaded on the DMZ web box with corresponding holes punched in the firewall allowing the DMZ application to contact the Oracle DB on the internal network. Then some admins or DBAs say the box needs to be part of the internal domain structure so that they can easily administer the DBs and perform updates. So, much to the horror of any security admin worth his salt, more ghastly firewall rules are torn open to allow intradomain and NetBIOS/CIFS traffic for authentication and “easy” administration. The vendor of the web application then decides they need VPN access into the DMZ and intranet to support their application that’s “not quite working like they expected” and another box is set up to provide RRAS or access via “PC Anywhere” so they can get to the DMZ web server as well as some internal resources.

The result is a complete breakdown of any security posture via a topology that now more resembles an extension of the internal network than it does a least privileged, protected network segment. It’s no longer a “DMZ,” but rather, just a “Z.” Why? Because even if the “front-end” of some of the services (say, the RRAS box) have security-in-depth mechanisms to gain access such as a dual-authentication RSA fob, other systems do not. If a breach occurs via some vulnerability in the web application, which by its very design is accessible anonymously over the internet, then all adjacent boxes within the DMZ are typically fair game to parallel attack since they are not protected from other resources within the DMZ itself -- they are only protected

from a “head on” attack externally. The web server itself may have no immediate path into the internal network, but the RRAS box does. It’s the three-step compromise dance: Step into the front, a step to the left, and you waltz right into the internal network.

The solution I designed for this issue is the Multi-Segmented, Role-Based DMZ (MS-RBD). In the MS-RBD, DMZ sub-segments are defined based on access types: Un-trusted, semi-trusted, and trusted. These sub-segments have a strict policy of access assigned to them that cannot change under any circumstances. For instance, the “un-trusted” segment cannot have any un-filtered in-bound ports open to the internal network from the DMZ, ever. Period. The “semi-trusted” segment can have limited internal network access, but in every case, the semi-trusted segment must require authentication to access the service in all cases. Period. The trusted segment allows for internal network access, but it must also require multi-level authentication (again, such as an RSA fob) for services for RRAS or OWA (There are some really cool techniques we’ll use to secure OWA front-ends in the following segments).

Once you have defined the access rules for the segments, you then use the “role” of the server or service to define which sub-segment the server must be located in. For instance, if a service or application allows anonymous access (like a web server app) then it MUST be located in the un-trusted DMZ. If the application requires some access to the internal network (as in the customer facing web app that must talk to an Oracle DB) then it MUST be located in the semi-trusted segment. If a user needs OWA access, which must talk to the internal network, then they MUST have at least a dual-mode authentication mechanism to gain access.

The logic of “the role defines the segment” and “the segment defines the rules” within an access policy gives your security people a leg to stand on when it comes to business units dictating application deployment in the DMZ. But the policy **MUST** be obeyed for it to be successful. There can be no exceptions. If an anonymous-access web portal gets deployed, it goes in the un-trusted segment which can't get to the internal network. If a vendor needs access to the internal network, they can access it through the trusted segment, but they'll have to use dual-authentication. If the web app gets hacked, the hacker is limited in access. They have no direct access to the internal network, and they can't piggy-back onto the RRAS server for access since it's not an adjacent server anymore - it's in a different segment that they can't hit. In most cases, vendor application support or data-driven web apps already require some sort of authentication (you must log on to gain access to the application) so they could possibly go into the semi-trusted segment, giving you a far more secure posture than allowing the vendor VPN access. It all depends on the access method and how you choose to authenticate. And remember, just because a user authenticates themselves, it doesn't mean that they are trusted. I require authentication for some users to gain access to privileged information, but that doesn't mean they get to live in the semi-trusted segment that has some, albeit limited, access to my internal network.

The diagram on the following page illustrates the MS-RBD.

So, there we have it. A DMZ design that not only secures your assets in a least privileged, security-in-depth environment, but one that also, by merit of policy enforcement, keeps assets where they belong by assigning roles

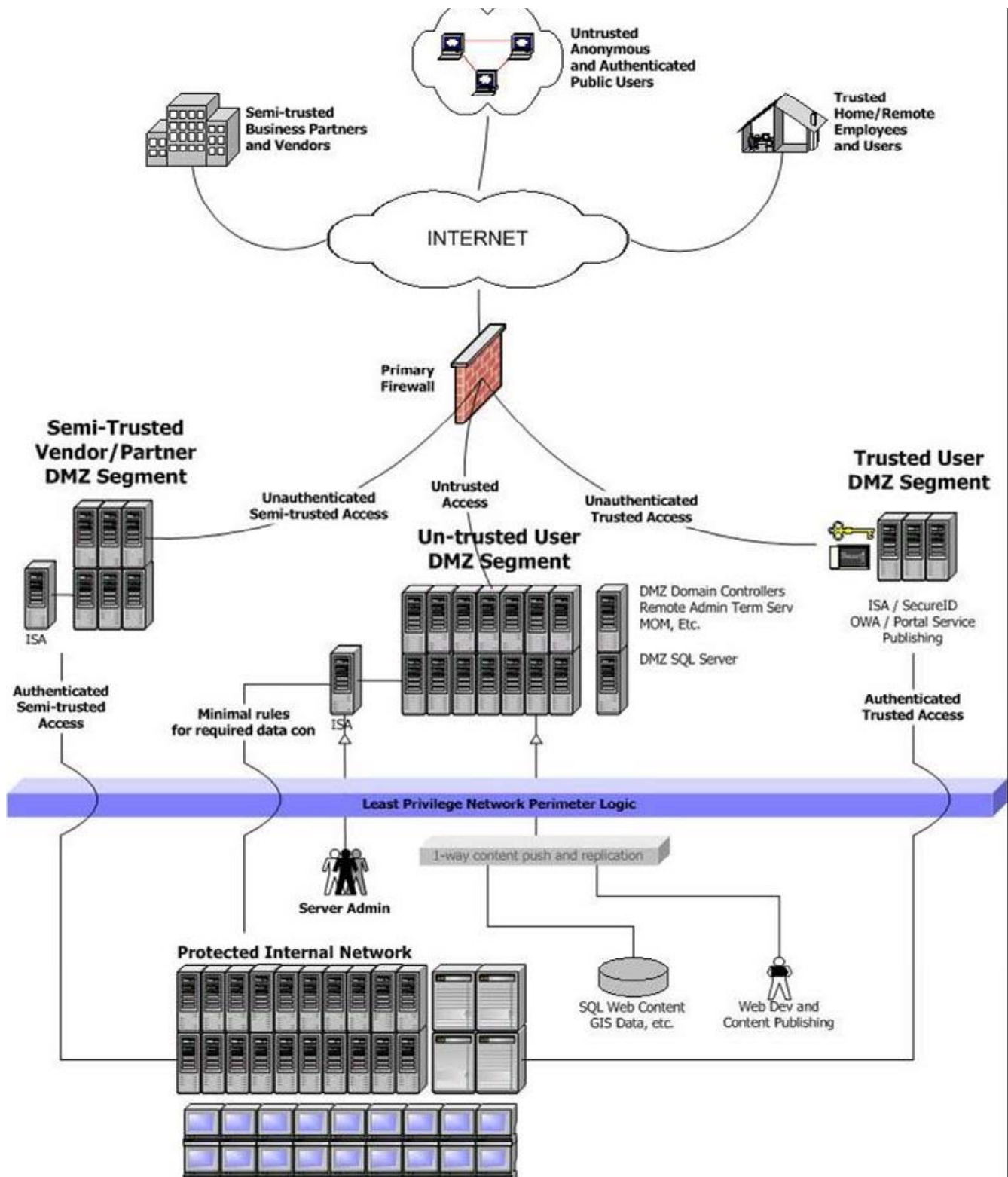
to them.

### **The Hard Part**

But what happens when there isn't a perfect match of role-to-segment-to-rules? What happens when there is an exception to the rule? The first service that probably springs to mind is mail.

Your SMTP server must accept anonymous connections in order to accept mail. That mail then needs to be delivered to the internal network. You may be prone to locate an SMTP gateway in the semi-trusted segment, but you can't: remember, anonymous access means that the SMTP gateway **MUST** go into the un-trusted segment. But the un-trusted segment cannot have an unfiltered, direct path to the internet network? What do you do?

That's where the keyword “unfiltered” comes in. In the case of SMTP, externally sourced inbound connections to your SMTP gateway box are made anonymously. After your gateway verifies the mail and checks it for viruses and against your SPAM policy, it will need to connect up to your internal Exchange server for intra-domain delivery. If you refer to the diagram, you'll see an ISA server with a “Minimal rules for required data con” connection object to the internal network. Here, we use the “SMTP Application Filter” to act as a connection gateway between the SMTP gateway and the internal network. The SMTP gateway accepts the mail item, which is then smart-hosted to the ISA box. The SMTP Filter actually checks the application level content of the connection, and verifies that it is actual SMTP content and that the SMTP commands are supported (we'll get into this in more detail in the next couple of articles). Once the content is verified, the ISA box will connect up to the



Exchange SMTP connection (and only to the Exchange box on TCP port 25) to make the final delivery.

### **But what if...**

OK. I know things aren't always that easy. So let's roll with an example of dealing with another potential "real world" issue. In our un-trusted DMZ segment, we've got our SMTP gateway, and the web server we originally talked about. There are no "static" ports open to the internal network (with the only possible exception being SMTP delivery- but that goes through a robust application level filter). So along come the business unit guys (hey, they're just doing their job, right?) who now want to bolt on that customer facing application we talked about that needs access to an internal DB. Internal users update article information that anonymous visitors need to read. The app is designed to pull the data right from the database, but here we go again: since the app accepts anonymous connections, it must go in the un-trusted DMZ which can't make a direct internal connection. Enter the "DMZ SQL" box. Again, we'll cover the specific technical aspects of this later, but for now, consider that we will configure a SQL box in the DMZ itself for the purposes of warehousing this article data. The apps need only talk to the SQL box in the same protected segment, and not to a back-end database within the internal network. Data on the server can easily and instantly be replicated via a replication scheme that is sourced from internal network and delivered via a "one-way replication rule" that can only go from the internal network to the DMZ, and not the other way around. The result is an up-to-date collection of data delivered to the DMZ where there is no static port available for abuse when the DMZ box is compromised. There are added benefits as well: For one, only a small sub-section of the data on the main server is replication, thus reducing possible

unauthorized access, and secondly, there are no "shared credentials" in the DMZ that can be used to access internal assets. The internal box will specify credentials that only exist in the DMZ to perform the replication. A breach of this segment greatly limits an attacker's options and thus dramatically increases your security posture. But know that no technology is bulletproof- it is possible for an attacker to leverage the "established" channel used for data replication from the internal network to the DMZ to possibly compromise the SQL server, but it would require a highly skilled attacker to do this. In fact, the only people I know who can pull this off work for NGS Software, but that doesn't mean others can't. Regardless, the deployment of an MS-RBD still greatly increases your security and severely limits the actions of an attacker.

This is the power of a MS-RBD deployment. But remember, you've got to have a policy that is backed by management and given some teeth in order for it to be successful.

Look for our next installment when we actually get under the hood and address the technical aspects of Building Smart DMZ's.



*Tim Mullen* is Vice President of Consulting Services at NGS Software. You may contact him at [thor@hammerofgod.com](mailto:thor@hammerofgod.com)



THE  
**TECHNO  
SECURITY  
CONFERENCE**

• MYRTLE BEACH, SOUTH CAROLINA •

## Life is a Beach, hope to see you there at Techno Security 2007

Now in our ninth year, the Techno Security Conference promises to be our most incredible event ever with seven concurrent tracks covering the latest headline making security and digital forensics topics. Over 1,000 attendees will again make their way to one of the most beautiful locations in the world for three and one half days of non-stop education and networking and just as important, fun for you and your family.

Here are just a few of the highlights for this year's exciting conference:

- Keynote addresses by Johnny Long and Ray Semko, aka the DiceMan.
- New this year, "Techno Investigators Track" Stay tuned for more information on this.
- Several exciting new pre-conference classes are available with a FREE admission ticket to the conference, a \$1200 value....
- Hands on Digital Forensics Labs from Access Data and Paraben
- Others topics include Incident Response, Web Hacking, legal issues, wireless, threats and countermeasures, risk management, intrusion detection and prevention and so much more
- Stop by and play with the latest Intel based Apple Computers.
- Attendee can earn up to 32 credit continuing professional Education (CPE) credits

There are still some excellent exhibit and sponsorship opportunities available. Call 410.703.0332 for more details...



[www.Techno2007.com](http://www.Techno2007.com)

Techno Security Conference 2007

June 3 - 6

Myrtle Beach, South Carolina

**On July 07, 2004** the SANS Internet Storm Center published an entry titled “Brute Force PW Scans” (1). This was one of the first notices to watch for scans against SSH servers. Nearly three years later it is routine to find daily many failed login attempts in the logfiles of your Internet exposed SSH servers. On my machines the entries in my logfiles became very annoying. I first ran my SSH servers on a non-standard port. I ran into problems accessing the non-standard port from some sites, so I had to move back to port 22. About 6 months ago I ran across a project that has solved my problems.

If an attempt to login as the root account from a non-trusted machine is probably a malicious threat. The same can be said for many application accounts; mysql, postgres, shutdown, ssh, games... Should machines trying to access these accounts have further access to your system? My answer is NO. By adding these IP address to my tcp\_wrappers(3) deny file most of my Internet facing services will deny any connection attempts from these IPs.

In February of 2005 Phil Schwartz registered his new project, DenyHosts, with SourceForge (2). It was designed for linux systems that have Internet facing SSH services. It has since been ported to other Unix and unix-like operating systems.

By looking for failed logins with-in the servers logfiles it can identify what machines are trying to brute force the SSH service. When an IP has been identified it will add this IP to your tcp\_wrappers deny file. DenyHosts can purge hosts after a configurable time. You



can also configure how many times a host will be purged before it being left in the deny file forever.

DenyHosts, a python application, was initially designed to be used by a single machine. As the project grew the ability to use a central server to keep multiple machines in sync was added. At this point there are over 13000 hosts contributing data points to the central server (4). These combined hosts have now blocked over 65000 unique hosts with an average around 1000 hosts per day. You do not have to opt for this ability. If you do, you have the choice of uploading and/or downloading the data for use with your local servers.

The configuration of DenyHosts is very easy and well thought out. The main configuration file is denyhosts.conf. The example configuration file that comes with the distribution has most of the options available and documented. The projects FAQ has additional information that expands on the inline documentation (5).

The ability to set your own thresholds is important. How many times can a host attempt to login with an invalid account prior to being blacklisted? How many times can a host attempt to login with a valid account? What about your system accounts? All of these thresholds are configurable.

There are hosts that I do not want to be blocked. DenyHosts gives you the ability to lists hosts or networks that should never be blocked. This does eliminate the denial of service attacks spoofing your trusted hosts and networks.

This simple freeware program can improve the security of your system. Check it out.

- (1): <http://isc.sans.org/diary.html?storyid=258>
- (2): <http://sourceforge.net/projects/denyhosts/>
- (3): <ftp://ftp.porcupine.org/pub/security/index.html>
- (4): <http://stats.denyhosts.net/stats.html>
- (5): <http://denyhosts.sourceforge.net/faq.html>



*Brian Kirouac* is the CTO and a Principal Security Consultant for Security Horizon, Inc. You may contact him at [brian@securityhorizon.com](mailto:brian@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.

5/9 - 5/10, 2007	Olympia, WA
5/10 - 5/11, 2007	Dallas, TX
5/17 - 5/18, 2007	Atlanta, GA
5/24 - 5/25, 2007	Boston, MA
6/1 - 6/2, 2007	Myrtle Beach, SC
6/14 - 6/15, 2007	Fairfax, VA

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>



## Book Excerpt: Syngress Publishing



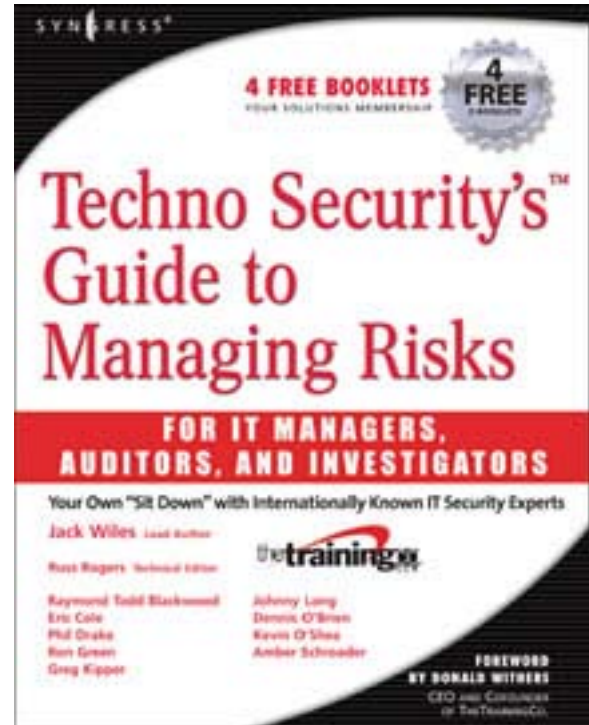
The following is an excerpt from:  
*Techno Security's Guide to  
Managing Risks*  
by Jack Wiles, et al.  
ISBN: 1597491381



### Introduction

Some of the things I will discuss in this chapter have been on my mind since the mid-1980s. I believe it's time I put them in writing and present my thoughts on what I believe could be the most effective and dangerous threat to any security plan: social engineering! This age-old threat has taken on a new meaning as what I collectively call "bad guys" have continued to use the art of the con to gain access to intellectual property and, if necessary, the buildings that house it.

This chapter isn't meant to be read as a complete story from beginning to end. Social engineering and ways to prevent it are subjects with many meanings. This will be more of a potpourri of tips, tricks, vulnerabilities, and lessons learned from 30-plus years of dealing with these issues. As an inside penetration team leader, I used every exploit I could to conduct a successful inside penetration test. It was during those years that I gained most of my social engineering experience. These skills helped me eventually hang up my dumpster-diving penetration team clothes and retire from the tiger team world UNDETECTED! Although I came close several times, I was never stopped or reported to security as a possible burglar or corporate espionage agent, even though that's what I effectively was while I had our



teams inside their buildings.

If you think this chapter has a strong risk management flavor, it was intentional. Just about every area of concern with security today is a risk management issue. This chapter, and most of the others in this book, are chock full of what I like to call Techno Tidbits of useful risk management countermeasures. Hopefully, many of them will be topics you might not have considered in the past as you put together your security plan. External, internal, and information system auditors should pick up a few ideas for things that should be added to their audit process.

### How Easy Is It?

Way back in 1988, I was part of an internal security team for a large corporation. On several occasions, I had the opportunity to hear some of the conversations that went on when a cracker (bad guy hacker) group targeted a victim by calling them on the phone. They were using social engineering

## Book Excerpt: Syngress Publishing, cont.

skills to gain access to proprietary information, including passwords. I'll never forget what I heard one experienced cracker say to a cracker-in-training: "Social engineering is the easiest way to break into a system." He then followed up that comment by saying "The stupidity of the average system administrator amazes me."

That was almost 20 years ago and it was the first time I had heard the words social engineering. Why do I think of it as a tool that could be used by any "bad guy" from a cracker to a terrorist? Social engineering is what I believe could be the most effective and dangerous outsider-insider threat to any security plan.

Over the past 15 years, I have learned firsthand just how easy it is to be an effective con man as I lead several inside penetration teams into clients' buildings who hired us to test their vulnerabilities. Not one time did we fail or get caught as we roamed their buildings pretending to be employees. Everyone we encountered while doing our thing thought we belonged there.

### **Human Nature: Human Weakness**

This is certainly not the first time anyone has written about the effects of social engineering. It doesn't take much searching on the Internet to find material on the subject, and in almost every article you will note a common thread. In each case, the social engineer turns our normal human nature of wanting to be kind, helpful, and sympathetic into a weakness they can exploit.

If we looked at this through the eyes of a risk manager performing a risk assessment, our untrained and unaware human nature could be considered a major vulnerability, threatening just about everything important to our company. We'll talk about possible countermeasures to these threats throughout of the rest of the chapter.

The reason I digressed into a full discussion about a risk assessment of the threat of social engineering is because I don't think many people have performed a detailed risk analysis. Since social engineering is a truly formidable threat, you need to know how vulnerable you are (at work and home) and what you can do to reduce those risks.

Any risk assessment needs to consider at least four things: risks, threats, vulnerabilities, and countermeasures.

### **Risk Management:**

#### **Performing a Mini Risk Assessment**

I recently had the opportunity to purchase my first boat. It's not huge, but it is just big enough for me to use as a floating mini-office a couple of days a week when the weather is nice. Just for fun, let's do a mini risk assessment of some of the risks, threats, vulnerabilities, and countermeasures associated with my new floating office. This isn't intended to be extensive (I'm sure you will think of things I didn't mention here). I just wanted to give us practice using terms most associated with risk assessments and risk management.

#### **What Do I Have at Risk?**

Being out on the water all day, my life is the first thing that comes to mind as a risk. The boat itself is also at risk, though I have passed some of the financial risk along to an insurance company, which is what we do with a lot of risks where it makes sense. Any equipment on the boat is at risk of not only sinking but of possibly being dropped overboard, or being soaked by a large wave. A sudden thunderstorm could cause problems. Depending on lake conditions, too many other boats could cause a problem. The battery in the boat could die causing me to lose all power and even strand me on the lake. As you can see, when you consider what you have a risk, you will immediately start to

## Book Excerpt: Syngress Publishing, cont.

consider some of the threats that could possibly increase your risks. What I have at risk on the boat is everything I could lose if something bad happened. Let's call all the bad things that could happen "possible threats."

### What Are Some Possible Threats?

We've already mentioned a few possible threats, which are different than those surrounding my home office. Weather could certainly be a threat, as could simply hitting something as I was moving from one place to another on the lake. The threat of a sudden thunderstorm, or of being hit by another boat, always exists. There isn't much risk of being hit by a car (hopefully), or suffering from a commercial power outage while I'm aboard. The possible threat of theft should be small as long as I keep an eye on my equipment while I'm launching the boat. Overall, the threats, which could possibly hinder my ability to conduct business from my boat, would be lower than most places. (Am I looking for reasons to work from my boat or what?)

### What Are Some of the Possible Vulnerabilities?

I would be much more vulnerable to severe weather changes out on the lake than in my home office. I would also be vulnerable to lake conditions in general at any given time. (This is a large lake about 20 miles long.) For a few days following a heavy rain, hundreds of semi-submerged items float down stream. I would certainly be vulnerable to someone losing control of his or her boat and crashing into mine. If I didn't know the depth of the water I was in, I could possibly run aground or hit something in water that was shallower than I thought it was. It would most likely just be an inconvenience, but as in any vehicle, I could run out of fuel. I mentioned not being affected by commercial power failures, but I could easily run my only battery down to where I couldn't start the engine to return to the

marina. In addition, though I am always very careful, I could possibly fall overboard—a difficult problem when you're on the water alone.

### What about My Countermeasures?

I really enjoy talking about countermeasures. The word even sounds cool. You have all of these things that you have identified as yours and they could be at risk out there in the boat. You have considered the possible threats and how vulnerable you might be as you encounter them. Now, what can you do to lower your risk and decrease your vulnerability? I've learned a lot during the few months I have had this new floating mini-office. Some of my newfound countermeasures are:

- I only try to be on the lake when most other boaters aren't out there.
- I check the weather forecast every time before I head to the lake.
- I will install a second marine battery to insure I always have power.
- I have made sure special waterproof cases are used for my computer and cell phone.
- I carry a small inverter onboard to provide me with 110 volts AC from the boat battery.
- I make sure the marina and my family are always notified of where I will be, and when I expect to return.
- I always carry a small marina radio onboard.
- All data on my computer and cell phone have backup copies on shore.
- I wear a self-inflating life vest at all times.

I'm sure many more issues could be addressed in this mini-assessment, but the point is we all need to at least be familiar with, and understand, our risks at home and work. Included in this book is a detailed chapter titled "Personal, Workforce, and Family

## Book Excerpt: Syngress Publishing, cont.

Preparedness,” which contains a wealth of information for lowering your risk in some of the most important areas of your life.

### Outsider–Insider Threats

For my definition here, let’s consider the outside threats as those coming at you from the Internet or dial-up modem (You do know where all of your dial-up modems are; don’t you?), or a simple phone call from a total stranger. The reason I mention dial-up modems is because there are still many of them out there. Many maintenance ports on older PBXs, building environmental controls, air handling systems, and access control systems still use them and probably will continue to rely on them well into the future.

I’m not considering insider (current employee) activity in this chapter. Even though malicious insiders can use social engineering in a number of ways, the countermeasures for that kind of activity can be much different. For this discussion, let’s consider outsider–insider threats as people who never were employees and didn’t belong in the building.

This would be the category my inside penetration team would fit into. When we roamed through buildings unchallenged, we definitely didn’t belong there (other than being hired to try to get there). Someone checking out your building for possible espionage or future terrorist activities would also fit in this category. In theory, some employee inside the building should eventually figure out that there is a “Trojan horse” in the camp. Someone who has gotten past whatever security there is at the perimeter where entry was gained. There is a good chance they used some form of social engineering to get there.

Here’s why I keep preaching about this subject and the subject of knowing who is in your building at all times. For more than three decades now, I have observed what I

believe is a lack of awareness of this concern. Over the years, I have seen comparatively few articles address this silent but formidable threat. Remember, when I spent those years doing this for a living, we were hired expecting to get caught in an attack that was designed to become bolder the longer I had the team in a building. Toward the end of just about every job, we were openly walking around like we worked there, almost hoping to get caught by someone. We never did!

We were good, but I suspect there are many “bad guys” out there who are much better at it than we were, and they won’t try to get caught in the end like we did. We were also working under a few self-imposed rules that the real bad guys could care less about. Using forced entry, like a crow bar to get through doors or windows, was a no-no for us. Our main tools were a cool head and our social engineering skills whenever it made sense to use them.



*Printed with permission from Syngress, a division of Elsevier. “Techno Security’s Guide to Managing Risks” by Jack Wiles, et al. Copyright 2007. For more information about this title or other similar books, please visit [www.syngress.com](http://www.syngress.com).*

Syngress Publishing ([www.syngress.com](http://www.syngress.com)), headquartered in Rockland, Massachusetts, is an independent publisher of print and electronic reference materials for Information Technology professionals seeking skill enhancement and career advancement. For more information on Syngress products, contact Amy Pedersen at 781-681-5151 or email [amy@syngress.com](mailto:amy@syngress.com).



# 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](http://www.saintcorporation.com)  
or contact Billy Austin at 1-800-596-2006 ext. 0119 or [austin@saintcorporation.com](mailto:austin@saintcorporation.com).

**Internet Relay Chat** (IRC) provides users with the ability to hold interactive conversations with other users in real time across world. IRC has a distributed architecture that will be described at a high level. IRC bots provide enhanced capabilities to the IRC network and provide valuable features that would not be available without their use. However, there is a dark side to the IRC bots that allows for malicious activities. An example of a recent IRC bot based worm will be discussed along with potential defenses against these types of attacks.

on the server from a published list (retrievable via direct query to the server) or create their own channel (assuming they have sufficient permissions). There is also the option to create hidden channels (channels that are not reported when the server is queried for the list of channels). IRC servers can be connected together forming IRC networks. The servers are configured to replicate the chat traffic between each of the servers allowing the network (and channel) to support a virtually unlimited number of users. In addition to providing scalability, the IRC networks allow

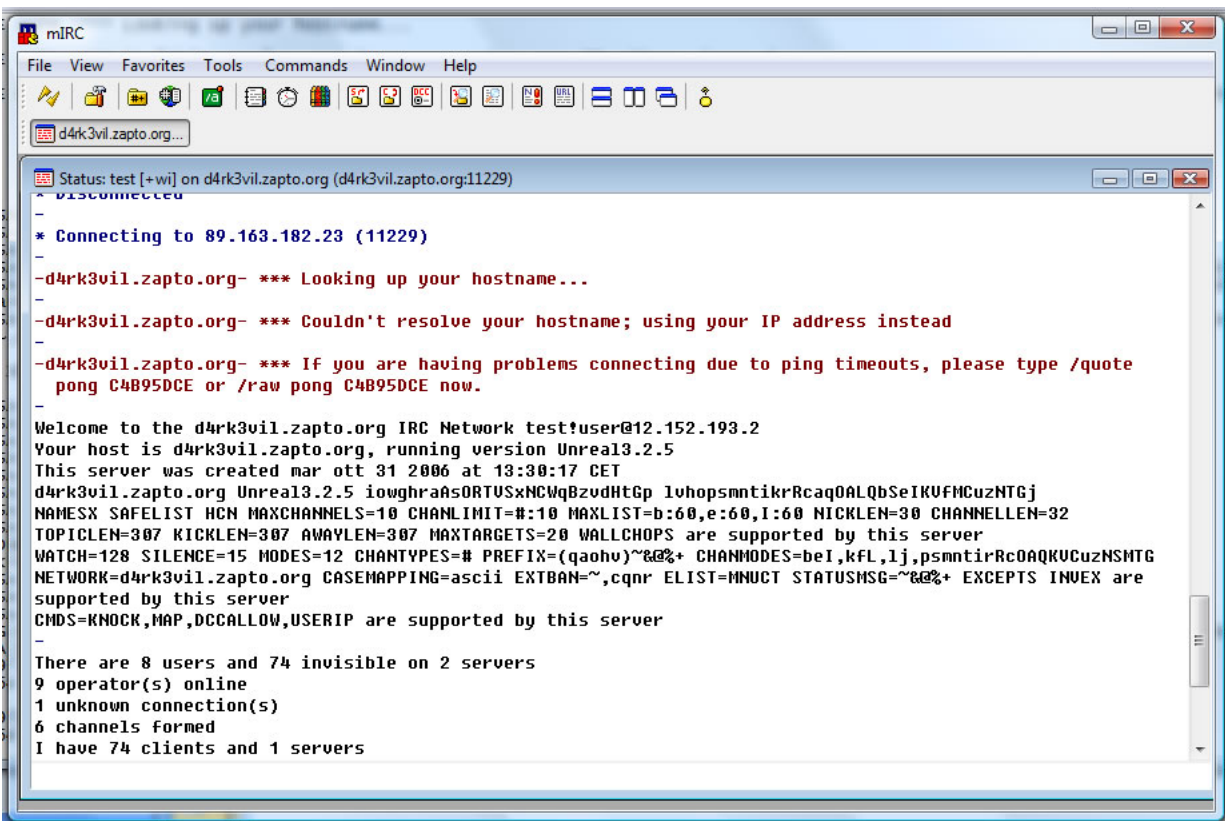


Figure 1 – The mIRC IRC client connecting to an IRC Server

Internet Relay Chat (IRC) is a set of programs and protocols designed to give users an interactive (primarily text based) conversation with other Internet users. IRC users use client software to connect to the IRC servers across the Internet. Once connected to the IRC server, the user can select different channels

for localized control and additional security. By distributing the servers in different regions of the world, the networks also enable additional anonymity. The anonymity is achieved by the clients connecting to servers that are in different legal jurisdictions, making the job of obtaining connection logs much

more time consuming and expensive for law enforcement agencies. In addition, some jurisdictions may not recognize or require the logs or other data be turned over to the foreign law enforcement authorities.

The IRC initial system design was to enable users to hold real time interactive chats with each other being distributed in different locations. One of the ideas is to enable collaboration on projects and brainstorming between members of a team. Because of this collaboration feature, users on the channel can send binary files to each other, not just text. The files are encoded and then sent as a text and decoded by the remote users. Another early use of IRC is customer support. Companies would setup an IRC server (connected to a web site for example) and allow their support members to work interactively with customers on their issues. This is similar to the standard telephone support model. Because primarily technology enthusiasts initially used the IRC network, the idea of an IRC automatic responder was created. The IRC automatic responder became known as an IRC bot (short for IRC robot).

These IRC bots are simply applications or scripts that would perform some automatic functions when specific input was received. For example, a company with an IRC server may enable an IRC bot to search the database for common errors to help a customer fix an issue before an actual person was involved. In this case, a person may send a message to the IRC channel asking for help on error number 12345. The IRC bot could recognize the question and error number, do a search in the internal company support database, and respond to the user with information on how to fix the problem.

Other uses for IRC bots were more nefarious.

These included watching channels for key words and inserting advertisements into the conversation. In this case, the IRC bot watch for one of the keywords (blackberry for example) and would then respond with an advertisement such as "I got my new blackberry from <http://www.advertisersite.com/> and got the best deal on the Internet". The IRC bots are designed to look like humans responding (as opposed to traditional advertisements) in hopes of getting users to believe that another person is responding (not just a commercial advertisement).

Another use of the IRC bots and advertisements involve two or more IRC bots having what appears to be conversation about certain products or servers. In this case, several IRC bots would log on to a channel as different users. The IRC bots would wait for specific events and begin what would appear to be a standard human conversation with the other bots. For example, one IRC bot may wait for one of the other bots to log on and then send a message like "hello bot2" (but they typically would not use such obvious names for the other bots). The second bot, would then respond in kind ("Hey, bot1"). They would then begin their conversation (or could continue with idle chitchat for a bit first). The conversations between the IRC bots centered around products (such as "do you know of a product to do X" or "I got a great deal on X from this retailer"). The conversation is a scripted set of responses to simulate a real conversation. Additional responses may be implemented to attempt to interact with other real humans on the channel to make the users seem less like IRC bots and more like standard humans.

Technology enthusiasts have used IRC networks since the initial conception of the IRC servers. In addition, black hat hackers and software pirates have used the IRC

networks as a way to distribute malicious code, ideas for new exploits and to discuss (or brag) about their accomplishments. Due to the distributed nature of the IRC networks, it is difficult for law enforcement to gain access to the server logs and track down users of the network. More recently, virus and worm writers have begun incorporating IRC bot code into their malicious software as a means to control and update their software.

By implementing a connection to an IRC network, the virus and worm writers can send updates to get around any bugs that may have been discovered in their code, update the code to get around anti-virus signatures (to avoid detection) and to add new features to the code. In addition, with the advent of the distributed denial of service (DDOS) attacks and SPAM bot networks (where large numbers of infected computers are infected with a virus for the purpose of sending unsolicited email) the virus or worm writer can send commands to attack a specific host or send out a new set of email with new content.

A search on Google reveals a number of example source codes in both Perl and VBScript for creating your own IRC bot. These are generic and harmless examples of how to connect to an IRC server, perform generic send commands (or messages), and retrieve messages from the IRC channel. Researching on the Internet (source is undisclosed because for security reasons), there are virus and worm kits already available where a new hacker can pick the modules to include and create their own custom virus. In one of the kits found during the research phase, the kit included code for sending SPAM, implementing ping sweeps, implementing a TCP port scan of a host, performing a DOS attack (essentially connect to a web site and request a given URL as fast as the system can), report back the results of

any scans, search files for key words, send files to the network and execute shell commands on the host (command from the command line or via Windows API calls). In addition, there is sample code for implementing exploits for various software packages. The exploits allow a virus writer to essentially execute the exploit (a buffer overrun for example) and then execute arbitrary code. The arbitrary code is generally used to install the other malicious software from the virus writer.

In the second half of the article, I will discuss the events of an IRCBot attack observed and captured in the wild. This was during a security consulting engagement with one of my customers. The IRCBot effects on the systems and network will be analyzed. In addition, the basic steps analyzing the behavior of the IRCBot and the first part of tracking down the people behind the IRCbot will be discussed.



*Patrick McNeil* is an experienced security consultant for Alexander Open Systems. He holds many certifications include CISSP #84805 and CCIE - Security #14432. Patrick has over 15 years of experience in the network and security consulting business. You may contact him at [patrickm@aos5.com](mailto:patrickm@aos5.com).

As a small business owner or operator, you have many priorities that take up your time, billing, inventory, payroll, customer service, etc; but what about physical and information security? You can't afford to ignore all the publicity about information security incidents. Some of the most recent ones may have even affected you. For example, if you have shopped at Marshalls or TJ Max recently, you may be one of the 45 million people whose personal information has been stolen by malicious hackers. For the small business owner, an incident like this could very well be the end of you company's operation.

***... YOU MAY BE ONE OF THE 45 MILLION PEOPLE WHOSE PERSONAL INFORMATION HAS BEEN STOLEN BY MALICIOUS HACKERS...***

Many people think of security as an alarm system, a locked door, security cameras, or being in a building that has security officers that patrol the area. This is part of the overall layered security model and of course is known as physical security. An often overlooked aspect of security in small business is information security. Information security is related to the security of systems that process, store, and transmit data. These systems can be technology based (computers) or manual (pen and paper).  
Information Security:

- Protects the data and information that resides in a computer
- Keeps unauthorized individuals from accessing confidential data
- Ensures proper authentication: (Are you who you say you are?)
- Ensures Authorization: (Are you supposed to have access to the system?)
- Access Control: (What data are you allowed to access on this computer system?)

- Reinforces confidence in the integrity of data stored on the computer system

There is no such "animal" as 100% effective security. The idea is to balance the risk to your data with the cost of implementing protective measures. Never spend more on security measures than the data itself is worth.

### **Start with the Basics**

If you are just realizing that security is important for your small business, or you are just now able to address security, consider starting with some basic implementations. If

you don't have a background with information security, seek professional assistance. Poor security implementation can often create more problems than it helps. In small business, there is a fine line between your personal and professional lives. So for the basics, we will look at protecting yourself and protecting your business.

### **Protect Yourself**

Is your home computer up to date? Do you have a good password on your system? Does the system have virus protection and a personal firewall? These are the first things you should consider for protection yourself.

What about your habits on the internet? Anybody that has used the Internet has been asked the question, "Would you like us to remember your password?" or "Would you like us to remember your credit card information for next time?" What do you answer?

What you are trying to prevent is identify theft. The federal government has recognized

the issue and passed the “Identity Theft and Assumption Deterrence Act of 1998”. This act makes it a federal crime when someone: “knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.” The Act defines “means of identification” to include names, SSN, credit card numbers, or other information that can be used to specifically identify an individual. So how do you prevent it? There is no 100% solution, but be vigilant and smart about where and how you give out your personal information.

### **Remembering**

#### **passwords on your computer:**

Although extremely convenient, saving passwords on your computer creates a loss of accountability that someone can use your identity to log on to websites, sign up for unwanted services, or spend your money. If you save the password for your online banking and someone else uses your computer, they can easily access your information. Get in the habit of saying no.

**Recommendation: When asked, always select NO or NEVER FOR THIS SITE**

#### **Remembering Credit Card information**

**on e-commerce websites:** If you have ever purchased something from Amazon, Travelocity, Expedia, or other e-commerce websites, you may have been asked the question whether you want them to remember your credit card information for the next time you “stop in” to spend some money. Some of these e-commerce sites have done a very

good job of putting mechanisms into place to help protect their databases and your information. Others have not. The challenge is knowing which have or have not done a good job at implementing security. The other challenge is that there is no such thing as 100% security, and a very secure website might get hacked. Don’t do it, take the extra 10 seconds to enter your card number.

**Recommendation: When asked, always select NO**

**Keep your computer up to date:** Keep your personal computer up-to-date with the latest patches and hotfixes. One of the easiest



ways for a malicious hacker to take control of your computer system is to exploit a known vulnerability that could have easily been protected against with current patches and hotfixes. This approach applies to your operating system (for most of you that is probably a version of Microsoft Windows). Your Start Menu has a link to Windows Update or Microsoft Update. Staying up-to-date also applies to your applications. This may require monitoring of the application provider to see when patches and hotfixes come out for the applications. You also have to make decisions on the appropriate time to buy newer versions of your operating systems or applications as they may eventually

become unsupported.

**Recommendation: Keep operating systems and applications up-to-date**

I have been in the security business for almost two decades and I have been a victim of credit card and identity theft. It can happen to anybody and does happen to many people every day. Reduce the number of opportunities that criminals have to get your information. Don't save passwords on your system and don't save credit card information on websites.

### **Protect Your Business**

Business owners and operators are responsible to provide a level of due diligence when it comes to information security and protection of customer privacy data. Your customers and the courts won't accept ignorance of this responsibility as an excuse. Many of you are driven by legal/regulatory requirements such as: Sarbanes-Oxley, Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and many more. If you don't know if you fall under a particular legal/regulatory requirement, then you should consider consulting with a professional security firm and/or your legal counsel.

### **Layered Security**

The most effective way to address security within your business is to take into account the layered security model. This model addresses multiple security implementations that should be considered for inclusion in your security program. These layers may include technology (firewalls, intrusion detection/prevention, and operating system security), policy/procedure, training/education, physical security, etc. By taking into account multiple implementations for protecting your critical data, the likelihood of a successful attack on your data is reduced. But even with layered

security, you must take steps to assure currency and accuracy of the security implementation. Just having security technology is not enough. It must also be properly configured, managed and monitored.

In small business, protecting your key assets also means protecting yourself. Take security seriously and put basic security practices in place within your organization. Making security awareness and security considerations a part of both your personal and professional life will assist in a quality overall security posture for your organization.



*Greg Miles* is the President of Security Horizon, Inc. and a professor with the University of Advancing Technology. (www.uat.edu) You may contact him at [greg@securityhorizon.com](mailto:greg@securityhorizon.com).

# The Future

Brought To You By Inspiration—and Coffee

The University of Advancing Technology (UAT) provides students a diverse, exhilarating environment where the best elements of a college education collide with an unrivaled passion for advancing technology. It's an innovative educational model that gives talented individuals an opportunity to create the future with a complete immersion in the rapidly expanding technological universe. We need the very best professors/instructors to continue this vision. If you are committed to expanding the field of technology (online or on-campus) through research and sharing of knowledge—challenging, educating and empowering students, we invite you to explore the teaching opportunities at UAT.



**Learn more.**

[www.uat.edu](http://www.uat.edu) or email Dave Bolman,  
Provost at [dbolman@uat.edu](mailto:dbolman@uat.edu)