



Security PS is the Midwest's Leading Independent Application and Network Security Consulting Firm.

We offer services in the following areas:

- Web Application Security Assessments
- Network Security Assessments
- Source Code Security Reviews
- Password Compliance and Analysis
- Training
- Vulnerability Testing and Management
- Security Compliance
- And much more...

Inside this issue:

The Changing Landscape of WiFi Security	1
Webinars: PCI Compliance	3
Upcoming Training Sessions	4
How to Register for Training Sessions	4

The Changing Landscape of WiFi Security

*Steve Rodgers
President and CEO*

Growth of Wireless Networks

To say that wireless networking is ubiquitous would be an understatement. IDC predicts the worldwide market for wireless LANs, or WiFi, to reach \$3.2 billion in revenue by 2010, a 17 percent compound annual growth rate (CAGR). Anymore it's almost hard to find a coffee shop



or café that doesn't have numerous laptops accessing the Internet via wireless. Even when traveling to Puerto Vallarta, Mexico

earlier this year I was able to connect from my hotel via wireless to check e-mail, weather, sports and other information on the Internet. The growth of WiFi continues, but what about the security of the networks? Has the level of security increased, decreased, or stayed the same? Security PS set out to find the answer.

War Driving in 2002

Since starting up Security PS in early 2002 many things have changed in the last four and a half years. In 2002 use of wireless networks was just starting to rapidly grow. In December of 2003 we decided to conduct a wireless network survey. In our initial survey we drove around Johnson county, the Plaza, and downtown Kansas City. We used a laptop hooked to a high gain antenna stuck out the window of a car and were able to detect about 500 access points over a period of eight hours. At the time we felt this was a great number of access points to detect in such a short period of time, but little did we know how this would compare to our 2006 results.

Expertise and Passion

I've been flying airplanes since I was twelve years old, so warflying seemed like a natural way for me to connect my WiFi security expertise with my passion for aviation. The idea of warflying comes from wardriving -- that is driving around collecting information about wireless access points. Information such as SSID, location, encryption type, signal strength, etc.

When I first researched the idea of warflying there were at least three other groups on the

Internet that had documented their efforts to detect access points while flying over a city. During one of these flights in 2004 the warflyers were able to spot just about 4,000 access points around the Los Angeles area.

Why collect as many access points as possible in a short period of time? The answer is simple: as a security company we are interested in understanding how many of these access points could be easily compromised or hacked. We also wanted to compare current data to our findings from back in 2003.

Our Flight over the City

Our flight started at New Century Airport (KIXD) in Gardner, Kansas. We captured data on our first wireless access point while sitting in front of the hanger before we even taxied out! Before being airborne we had captured five access points just around the local airport itself.

Once airborne, things really started happening quickly. Almost immediately the computer screen started filling with wireless access points. We were using Kismet, a Linux-based program to monitor and record the access points as well as a GARMIN GPS to map the location of the signals. Kismet not only shows the access points it has found but also displays how long a signal is received from the access points. When driving on the ground it's common to receive the signal from five or six access points at any one time, but while flying over a populated area or office park we saw the entire screen light up with activity from the access points below.





Steve Rodgers, President and CEO

The Changing Landscape of WiFi Security, cont.

It was not uncommon for us to see the entire page, probably 25 or more active access points, light up at any one time.

When we initially set out to conduct this warflying experiment we felt that detecting about 5,000 access points would be a huge success. I quickly realized after ten or fifteen minutes that we would have absolutely

period of time. The FBI even demonstrated this live at a recent ISSA chapter meeting where they proved that WEP could be cracked in 3 minutes. Once WEP is cracked, the attacker may have open access to the wireless network. So considering this reality, only 10% of the access points out of a total of 6,098 would be considered strong or hardened from a security perspective. Compared to the results of our 2003 survey, the number of WEP secured access points has nearly doubled. Back in 2003 our survey showed about 28% of the access points had WEP enabled, compared to nearly 66% this year. WPA wasn't in use back then so there was no similar data to compare to this finding.

Channel Distribution

Although not security related it is interesting to note the channel distribution of the discovered wireless access points. Sixty percent (60%) of the access points are using channel six (See Figure 1.2).

In setting up access points one must consider the channel that is used so the access point is not receiving interference from other access points nearby. After conducting this warflying test and also looking at our data from wardriving, the majority of users and organizations are leaving these devices on the default channel 6. Simply changing the channel to something other than six will reduce signal interference and increase the reliability of your connection.

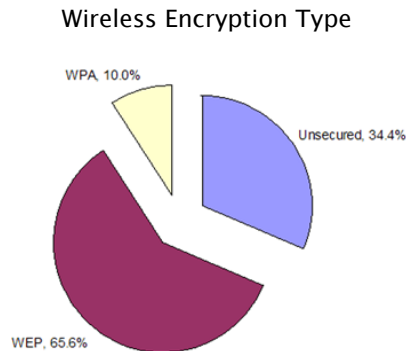


Figure 1.1

no problem exceeding this target.

In the end, we captured data from 6,098 unique access points in a 45 minute period and only covered about 10-15% of the greater Kansas City area. It certainly makes you wonder how many access points are really in the entire city.

Security Statistics

So what did we discover about the security of the access points? The statistics are quite interesting—out of 6,098 access points, 34% of them were completely unsecured. This means that a technology savvy neighbor or a criminal hacker could easily access these open connections to the Internet or corporate networks.

Of those access points that were secured, about 66% of them had Wired Equivalent Privacy (WEP) enabled, but only 10% had Wi-Fi Protected Access (WPA) or better enabled (See Figure 1.1). Note: the percentages won't add up to 100% because some of the access points had both WEP and WPA enabled, so they were not mutually exclusive.

For those who know about wireless network security, WEP in its strongest form of 128-bit encryption can be cracked in a very brief

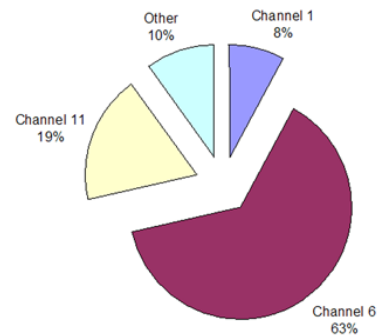


Figure 1.2

Secure the Endpoints

So what do these findings really mean? While the number of access points using encryption appear to be increasing, choices of the type and strength of the encryption aren't keeping up with technology options and the threat of attacks.

“We captured data from 6,098 unique access points in a 45 minute period and only covered about 10-15% of the greater Kansas City area.”

“...out of 6,098 access points, 34% of them were completely unsecured.”

The Changing Landscape of WiFi Security, cont.

Since WEP is easy to crack, you should use something stronger on your network. Unless, of course, you're managing a purposefully open network for personal or business reasons. In the majority of cases, you'll want to keep unauthorized users off your wireless network. Several great "Top 10" lists on securing your access point are out there, but I'll give you my short list of the most important recommendations:

1. **Turn on encryption using WPA or WPA2, and turn off WEP.** This enhances the encryption and prevents an attacker from cracking WEP and getting on your network.
2. **Update your access point(s) with the most recent version of firmware.** Access points that haven't been updated recently may not provide you with the latest security settings and enhancements, so be sure you're running a current firmware version.
3. **Enable an authentication mechanism.** In an enterprise environment use WPA2 and a strong form of 802.1X authentication such as EAP-TLS. For home users, set up pre-shared Keys using AES and turn on MAC address control.
4. **Turn off access point SSID broadcasting.** While this isn't a fail-safe security practice, it does add one more layer of security protection by obfuscating the SSID.

5. **Remember to address the security of the end-points.** The security of the end-points is also a critical and often overlooked factor. Ensure your mobile device has personal firewall, anti-virus, and spyware applications installed. Also, make sure you use a VPN client to connect back into your office or home network to avoid transferring sensitive information over the WiFi network. And last, but not least, ensure your operating system and application software is patched and up to date with the latest security fixes.

The Future of WiFi Security

With its constantly expanding use, WiFi will certainly continue playing a key role in home and enterprise networks alike. This growth will add complexity to the overall Internet infrastructure, and complexity always increases security risks.

While the use of WEP increased dramatically from one survey to another, this recent Security PS survey also demonstrated the majority of WiFi networks aren't keeping up with what is considered "secure" from a best practices perspective. As the security technologies used to secure WiFi continue to evolve, it will be increasingly important to implement the latest security enhancements into the overall network architecture. And certainly don't overlook to the importance of securing the end-points themselves.

"...only 10% of the access points out of a total of 6,098 would be considered strong or hardened from a security perspective."

Security PS Webinars

PCI Compliance: Staying Ahead of the Curve

The rise of identity theft has the major credit card companies clamping down hard on merchants and processors alike. Join presenter Bill Witbrod, Director of Security Compliance, for an informative session that will cover the recent changes to the PCI requirements and how your organization can stay ahead of the curve by assessing your PCI posture and securing your customers credit card information.

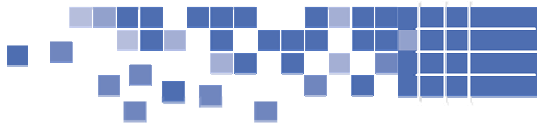
Learn about the changes to the PCI 1.1 Standards as well as how to leverage resources and implement best practices into the PCI compliance process.

To Register for this event go to:
<http://www.securityps.com/training/webinar-pci-2006.html>

Date:	Thursday, Dec. 7, 2006
Start Time:	10:00AM (CST)
Cost:	FREE



Bill Witbrod
 CISSP CISA CISM



SECURITY PS

STRATEGIC INFORMATION SECURITY

Security PS

7300 College Blvd, Suite 175
Overland Park, Kansas 66210
USA

Phone: +1 (913) 888-2111
Toll Free +1 (877) 9 SPS INC
Fax: +1 (913) 888-2120

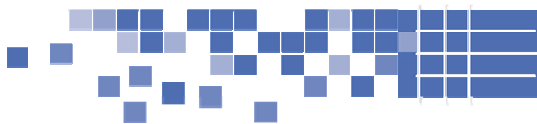
Prefer a hardcopy of the InfoSec Advisor?

If you would like to receive this newsletter in hardcopy, please email us a quick note along with your mailing address to: info@securityps.com

Visit our Web site at www.securityps.com

Coming Next...

In an upcoming issue of *InfoSec Advisor*, the Security PS newsletter, we'll provide an overview of ISO17799 and share some insights we've learned in our upcoming article "Application Pen tests vs. Code Reviews."



Training from Security PS

Upcoming Training:

Hands-on Attacking and Defending Web Applications	February 6 & 7
Information Security Foundations	February 27
In-Depth Web Application Security	March 13
Hands-on WebInspect™ Training & Certification	March 14 & 15

Hands-on Attacking and Defending Web Applications is a course that will allow Attendees to get hands on experience and gain a solid understanding of top web application vulnerabilities such as session fixation, cross site scripting, SQL injection, XPath injection, privilege escalation, bypassing authentication and access controls, weak use of cryptography, and gathering information from the application that enables attackers to worm past defenses. Each module will explain and demonstrate modern attacks, common pitfalls, and proven best practices for building defenses as they apply to modern web applications and important technologies such as Web Services and AJAX.

Information Security Foundations is a survey course aimed at system administrators and others charged with supporting IT security. The course addresses both hardware and software

In-Depth Web Applications Security provides the attacks, demonstrations,

principles and best practices of web application security by the experts in the industry. Up-to-date and designed to impact the security of your on-line applications for the long term, managers, developers and security staff will benefit from this course.

Hands-on WebInspect™ Training & Certification teaches manual and automated assessment techniques using SPI Dynamics' WebInspect™ product.

For more information on all Security PS Training offerings, visit our Web site at www.securityps.com.

Three Easy Ways to Register for Training:

- Complete and fax registration form available at: <http://www.securityps.com/training>
- E-mail us at training@securityps.com
- Call toll free +1 (877) 977-7467 and ask for the Training Coordinator

Remember, early registration discount ends 4 weeks prior to event date. Register now!

For further information on classes and locations, please visit our Web site: <http://www.securityps.com/training>