

## Featured this issue: Information security without boundaries

**I**t used to be relatively easy to secure the corporate data boundary. Identifying where it lay was hardly an issue, as the distinction between internal and external network equipment was clear. Securing the boundary was largely a matter of installing point solutions such as firewalls and anti-virus protection along this boundary, and ensuring that data accessed outside this domain was at least encrypted and password-protected.

With the rise of the Internet and high-speed mobile and wireless broadband,

all that has changed. The increasing use of the Internet as a business channel, growing adoption of cloud services, high levels of third-party access to internal systems, and widespread access from remote, often unprotected, locations using a variety of devices make it virtually impossible to define the corporate network boundary, let alone secure it. Steve Durbin of ISF believes organisations need to build a new security model based on trust and which does not rely on the network for protection.

*Full story on page 4...*

## Hacking wifi the easy way

**W**ireless networking makes life easy for those that use it, but unless properly configured, it is also remarkably easy to attack. Security firm SecPoint has released a portable version of its penetration testing appliance, Penetrator, designed specifically for pen testing wireless networks.

Danny Bradbury tries out the system and along the way examines the state of wireless networking security. He

discovers that successive encryption protocols – such as WEP and WPA – have proven to be insecure. But administrators can deploy various techniques to make their networks more secure. While you can test this security using common tools available for all Linux distributions, the SecPoint product conveniently brings them all together in a single package.

*Full story on page 9...*

## The future of the firewall

**T**he humble firewall has come a long way since its origins in the 1980s. But the technology is undergoing a major change, driven by the twin impetuses of soaring bandwidth and the need to accommodate cloud computing platforms. Steve Gold looks at the firewall's future.

One of the problems is that many types of network traffic now operate via

Port 80 – originally used only for web pages. This has prompted a move away from simple traffic analysis to a pattern-matching model that identifies the applications generating or using the data packets. The cloud has an important part to play, although it isn't possible to simply move traditional firewall models into the cloud.

*Full story on page 13...*

## Contents

### NEWS

Sinister trends in cyberthreats	2
European guidelines for resilience and cyber-security	2
Zeus and SpyEye hybrid emerges	20
Waledec makes a comeback	20

### FEATURES

#### **Information security without boundaries** 4

It used to be relatively easy to secure the corporate data boundary when identifying where it lay was hardly an issue. But with the rise of the Internet and high-speed mobile and wireless broadband, all that has changed. Steve Durbin of ISF says organisations need to build a new security model based on trust.

#### **Hacking wifi the easy way** 9

Wireless networking makes life easy for those that use it, but it is remarkably easy to attack. Danny Bradbury tries out the new, portable, version of SecPoint's Penetrator penetration testing system, and examines the general state of wireless networking security.

#### **The future of the firewall** 13

The humble firewall has come a long way since its origins in the 1980s but the technology is now undergoing a major change. Steve Gold looks at the future of the firewall in this age of soaring bandwidth and cloud computing.

#### **Thinking thin: addressing the challenges of client computing** 16

Advances in technology have changed the way businesses think about the end user and IT resource allocation. David Ting of Imprivata looks at the new challenges for organisations looking to deliver a long-term and cost-effective IT strategy.

#### **Preparing for a firewall audit** 18

The two most important processes involved when undergoing a firewall audit are the review of the change process and the review of the rule base, and there are some critical technical details you need to check, says Michael Hamelin of Tufin Technologies.

### REGULARS

News in brief	3
Events	20

#### Photocopying

# Hacking wifi the easy way

Danny Bradbury, freelance journalist

**The convenience of a technology is often inversely proportional to its security. This rule works for most things, including password management, physical building access, online payments, and – unfortunately – wireless networking. So let's look at one system for testing wireless networking and, along the way, we'll examine the state of wifi security.**

Wireless networking makes life easy for those that use it. But, unless it is properly configured, it is also remarkably easy to attack. Security firm SecPoint has released a portable version of its penetration testing appliance, Penetrator, designed specifically for pen-testing wireless networks. We took a look at the system, and discovered some interesting facts along the way.

A proper penetration test of a wireless network involves a number of steps, including finding the network's access points, cracking the network key (assuming the administrator was smart enough to encrypt it in the first place), enumerating the nodes, and then analysing their vulnerabilities. SecPoint's Portable Penetrator product is designed to conduct all of these wireless hacking tasks in a single package.

The product ships on a Dell netbook as a pre-installed Linux distribution with SecPoint's own tools added. The unit also comes with an external wifi card, which plugs into the USB port of the network.

The vendor has chosen to use an external card for two reasons. Firstly, it gets around the sticky problem of wireless interface cards that don't support promiscuous mode. In promiscuous mode, an interface card will pass all of the packets it sees on the network back to the central processing unit, making it possible for analysis software to see everything that is going on. In non-promiscuous mode, which is the default for most operating systems, the only frames that get sent to the CPU are those that were addressed to the network card's particular machine.

The other advantage of using a separate card is that it enables a penetration

tester to plug in a different antenna from the one generally embedded in a laptop. This enables you to use a more powerful unit (the strength is generally measured in decibel isotropic (dBi), which is an antenna's forward gain).

## War games

In this sense, the SecPoint Portable Penetrator is a wardriver's dream. Wardriving – the act of driving around an area looking for networks to hack – was pretty sophisticated, even five or six years ago. Tools such as Netstumbler and Kismet have been used for a while to identify networks and sniff packets.

There have even been some attempts to plug this data into mapping systems. In the mid-2000, for example, wardrivers would plug a GPS unit into the serial port of a Netstumbler-enabled machine, and would then use this configuration to capture the precise locations of hackable networks. These could then be dropped into a version of Microsoft's MapPoint to produce a map

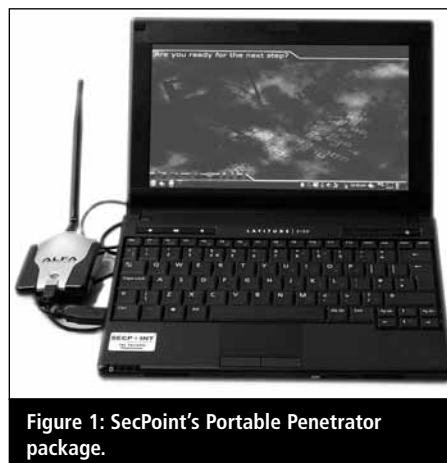


Figure 1: SecPoint's Portable Penetrator package.



Danny Bradbury

that could be referred to later. These days, things have evolved. The Wireless Geographic Logging Engine (Wigle) has emerged as a heavily used community wifi mapping service.<sup>1</sup> People upload Stumbler files with their data, or simply enter information manually.

The tools to gather data about these networks have also evolved. WigleWiFi is a mobile application that can be installed on any Android device.<sup>2</sup> It uses the mobile phone's own GPS system, along with conventional stumbling algorithms, enabling you to wardrive with something in your pocket. An iPhone version of the program was released, but Apple pulled it from the iTunes App Store.

***"A single unencrypted access point in a sea of encrypted ones can enable an attacker to compromise the whole network"***

SecPoint's Portable Penetrator is designed not so much for wardriving around a large area as for conducting penetration tests on a specific location, although it would still be perfectly usable in a campus environment, for example. Launching the unit's Wireless Audit service starts a cycle that detects wireless LANs near and far to assess their characteristics. The scanning cycle updates every 15 seconds.

## Going rogue

One of the things that the system can help a pen-tester to spot is rogue access points, which are more common than you might think. These can be installed maliciously or naively. Attackers install them covertly by plugging them into the wired infrastructure and then use them to gain access to the core network from



Figure 2: The WigleWiFi wardriving app running on an Android device.

hundreds of feet outside the building. They can also create rogue access points to conduct Man in the Middle (MitM) attacks, gathering information about users who are trying to connect to a legitimate network, before passing their packets onto that network.

Because access points are so cheap, and come configured to work with most networks out of the box, they are easy for employees to install – for example, in pursuit of a better signal in their office. But because these employees are rarely technologically savvy, they will often leave them unsecured. A single unencrypted access point in a sea of encrypted ones can enable an attacker to compromise the whole network. And leaving the access point's administrative interface 'protected' with the default login credentials is a classic mistake.

### When rabbit ears collide

Even if an access point has been approved, there is a number of things that could make it a relatively easy target to crack. Its antenna is a good example. Not all antennae are created equal. Companies installing wireless

access points in their buildings should consider where they are placed, and the gain used on the antenna.

Ideally, an audit would determine the rough distance necessary between the access point and the farthest client (or the edge of the building). It is difficult to calculate distance based on the access point's dBi alone, because much depends on the power of the receiving antenna. Most notebook computers will have an antenna with approximately 6dBi of gain, which gives you a rough idea. However, the antenna bundled with the SecPoint Portable Penetrator has a gain of 10 times that, giving it a far greater reach. This is evident in the number of wifi access points that show up when you put it into scanning mode.

***"You probably won't want to turn your building into a Faraday cage using wifi paint, because it plays havoc with cellphone signals"***

The other option for attackers is to use a hacked-together directional antenna (commonly called a 'cantenna'), which uses a metal can containing a probe, designed as a waveguide antenna. This bounces signals around inside the can to increase reception. Wardrivers regularly use such antennas to pick up otherwise weak signals. It would be relatively easy for an attacker to rent an apartment opposite a target's building and mount one of these by the window.

Those wishing to protect access points could themselves use different

types of antenna from the standard omnidirectional ones that you will often find with off-the-shelf units. Directional antennae are one approach, firing all of their radio signals in one direction, which can be particularly useful for site-to-site communications, or for pointing access away from a window back into a building, perhaps. You probably won't want to turn your building into a Faraday cage using wifi paint, because it plays havoc with cellphone signals.<sup>4</sup> That said, gain attenuation (which many access points will allow via their administrative interfaces) and judicious use of antenna type and placement will definitely help.

### Encryption

Once a network has been found, it may be open (in which case, gaining access is often as simple as connecting to it), or it may be encrypted. The networks highlighted in Figure 3 labelled OPN (open) are ripe for the taking. Those labelled WEP use the Wired Equivalent Privacy (WEP) protocol, which was the encryption protocol initially developed for the protection of 802.11 network data.

WEP was found to be insecure because of the way that it implemented the RC4 streaming cipher technique. A key shared between the access point and the client is used to perform an XOR function on the plaintext, producing ciphertext, which is then XORed by the recipient to obtain the original plaintext.

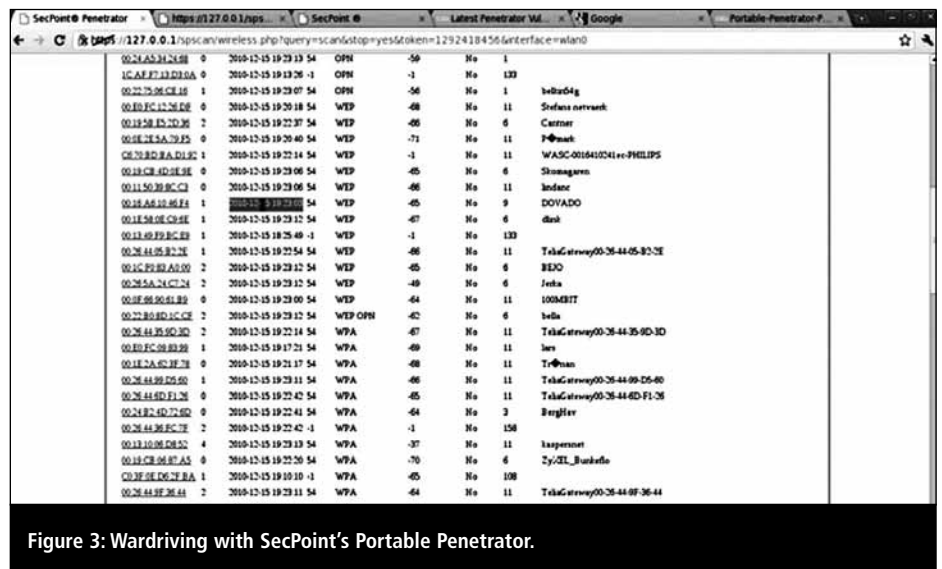


Figure 3: Wardriving with SecPoint's Portable Penetrator.

WEP implemented measures to stop the most obvious attacks on the protocol. These attacks involve flipping bits in the cipher stream and watching to see which bits are flipped in the resulting plaintext, and also decrypting ciphertexts encrypted with the same keystream. These attacks, when performed enough times, make it possible for the attacker to deduce the cipher key.

**“WPA using TKIP was subsequently shown by researchers to be crackable in 15 minutes (a window later shortened to 60 seconds)”**

Although WEP implemented defences against these attacks, it did so incorrectly, making it possible to crack a WEP key if the attacker listens to enough traffic. Consequently, the IETF 802.11 committee that defines wireless networking standards developed Wifi Protected Access (WPA), an interim protocol designed to solve some of the problems inherent in WEP. WPA was a stepping stone to the eventual ratification and deployment of 802.11i, a networking security protocol that was embodied in WPA-2, a more secure version of WPA.

Whereas WEP had embedded its 40-bit cipher key for a whole session directly into the packet stream, WPA implemented a 128-bit Temporal Key Integrity Protocol (TKIP), which changed on a per-packet basis. However, WPA using TKIP was subsequently shown by researchers to be crackable in 15 minutes (a window later shortened to 60 seconds).

WPA-2 further complicated matters for attackers by introducing 128-bit AES encryption for keys, along with a Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), which replaced TKIP with a single component for key management and message integrity checking.

**Cracking WPA**

It is, however, possible to crack both WPA- and WPA-2-based communica-

tion sessions. The irony is that, in many cases, it’s easier to do it than it is for WEP sessions. The difference is that unlike WEP sessions, which are always crackable, the outcome of a WPA crack is not guaranteed.

To gain access to a WEP network, the intruder simply has to collect enough traffic to perform a statistical analysis and obtain the key. This can be gathered in a matter of minutes, or in hours or perhaps days, depending on how busy the network is.

Conversely, WPA’s weakness lies in its handshake. When a client logs onto an access point, it exchanges the hash of the access point’s key using a four-step process, which is then used for the remainder of the session, and which is rotated on a per-packet basis. The hash is salted with the access point’s Service Set Identifier (SSID) – the name of the wireless network. If the attacker can work out the key from that hash, it is possible to retrieve the key. But how might that be done?

Enter the rainbow table. Most users (and many otherwise-savvy administrators) will fail to change the name of the SSID to something obscure. This is why so many networks retain names like ‘linksys’ (which Wigle says constitutes 6.74% of all known WiFi

networks) or ‘NETGEAR’ (the next most common, with 2.16%). Using the list of these, along with a long list of common passwords, it is possible to pre-calculate the hashes for hundreds of thousands of SSID-salted password combinations.

**“It brings together all the tools and files available across all Linux distributions in one conveniently preconfigured package”**

These pre-calculated tables, known as rainbow tables, ship with the SecPoint product, but you can also find them online. The Church of WiFi, for example, a motley collection of wireless security researchers, has compiled a list of a million passwords, salted with the top 1000 SSIDs, to produce a 40GB lookup table known as the coWPAtty table.<sup>5</sup> This, like the list provided with SecPoint’s own Penetrator, can be used to compute the key of a set of handshake packets, which are relatively easy to get. All the attacker has to do is knock a legitimate client off the network and force it to reauthenticate, in what is known as a reauthentication attack.

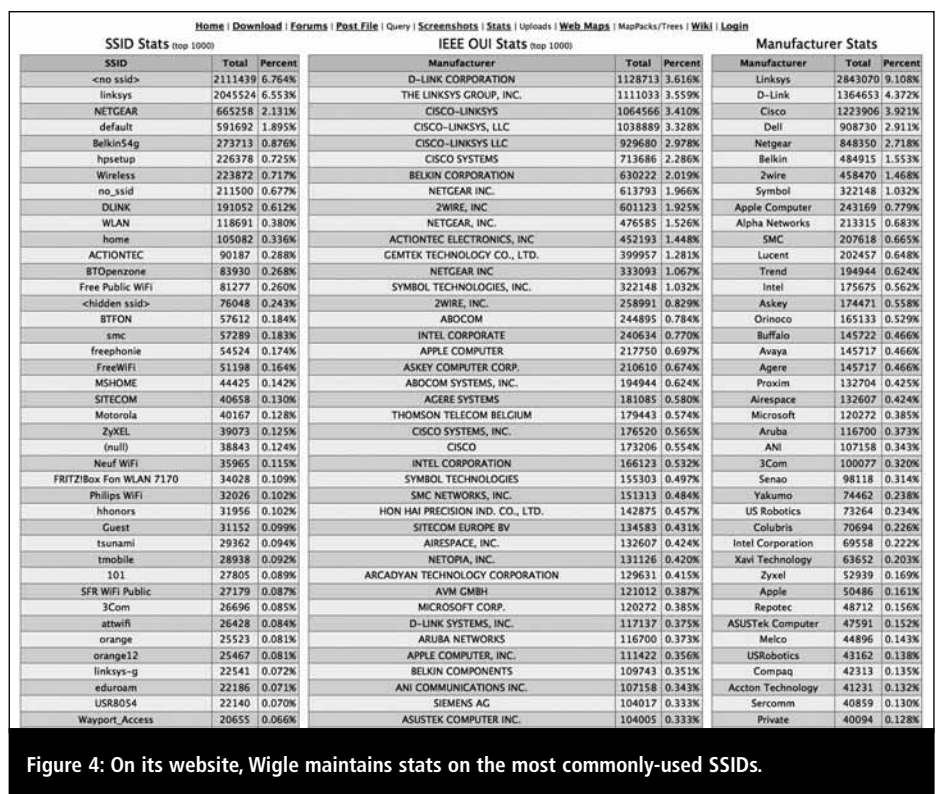


Figure 4: On its website, Wigle maintains stats on the most commonly-used SSIDs.

WPA-2, the final, ratified version of 802.11i with CCMP capabilities, can also be hacked. All coWPATy versions 4 and upwards support WPA-2, but there are other ways to crack that protocol. In 2010, Airtight Networks published details of a vulnerability that it called Hole 196, in which a malicious client can spoof packets from the access point.<sup>6</sup> By doing so, it effectively impersonates the access point, enabling it to sniff traffic on the network or disrupt service.

SecPoint's Portable Penetrator includes the ability to mount such reauthentication attacks as part of its workflow. Its main value proposition is that it brings together all the tools and files available across all Linux distributions in one conveniently preconfigured package. However, it is perfectly feasible to wardrive a selection of likely access points using established tools such as Kismet in other versions of Linux. GISKismet can even be used to produce database files that can be viewed in SQL, or exported to KML files for visualisation in Google Earth or Google Map.

## Rolling your own wardriving kit

Using your preferred Linux distro, tools such as AirmonNG can be used for troublesome tasks, such as putting your wireless network interface card into monitor mode (wireless sniffing tools won't use wireless NICs that are run in normal mode). Monitor mode is slightly different from promiscuous mode, in that it doesn't require the client doing the scanning to associate with a particular access point first, which is particularly useful when monitoring traffic on a wireless network. And Aeroplay-ng is a utility that forces a client to reauthenticate. (This, incidentally, can also be useful if mounting a MitM attack using a rogue access point, by forcing the client to automatically connect to the SSID with the greatest gain.)

Then you can complement these tools with others, such as Wireshark, which analyses the packets being captured by

sniffers such as Kismet. These tools allow you to tease out the handshake packets in any communication for processing.

At that point, tools such as Aircrack-ng can be deployed to crack WEP or WPA-PSK keys locally. Alternatively, if a penetration tester needs a faster crack, WPACracker, a cloud-based service launched by renowned hacker Moxie Marlinspike, will distribute the processing load to return the result in an average of 20 minutes, for a cost of \$17.<sup>7</sup> The advantage of Marlinspike's service, he says, is that it uses a dictionary an order of magnitude larger than that provided by cowPATy, allowing for SSIDs that fall outside the standard most-popular list.

The SecPoint Portable Penetrator handles all of this invisibly under a wireless audit process accessible via a locally hosted browser-based interface. The other advantage of the service is that it will also handle brute-force attacks on handshake packets for WLANs that have been configured with strong (alphanumeric gibberish or passphrase-based) passwords and/or non-standard SSIDs. These brute-force attacks will take a while, but it features the ability to use graphical processing units (GPUs) to help speed up the processing. This concept, which has been pioneered by Russian password-cracking firm Elcomsoft, uses the floating-point capabilities of graphics cards to speed up the number-crunching capabilities of password matchers.

Once you have cracked the network key and enumerated the different clients operating on the system, you can begin scanning the network for vulnerabilities. Users of BackTrack or some other Linux configured for penetration testing, might want to try Metasploit, HD Moore's vulnerability testing toolkit, for this purpose. SecPoint wrote its own tools to accomplish the same ends.

In short, then, SecPoint's device is well-configured and easy to use. Alternatively, those well-schooled in Linux will be able to cobble together their own system for wifi penetration testing in a relatively short time, with-

out the associated licensing overhead. However, the tools available to report network weaknesses clearly and succinctly to clients may require some scripting if you don't opt for the wifi-hacker-in-a-box approach.

## About the author

*Danny Bradbury is a freelance technology writer who has written regularly for titles including The Guardian, Financial Times, National Post, and Backbone magazine in addition to editing several security and software development titles. He specialises in security and technology writing, but is also a documentary film maker and is currently working on a non-fiction book project.*

## References

1. Wireless Geographic Logging Engine (Wigle). Accessed Jan 2011. <<http://wigle.net/>>.
2. WigleWiFi app. Accessed Jan 2011. <<http://www.androlib.com/android.application.net-wigle-wigleandroid-Axjt.aspx>>.
3. 'WPA2 Hole 196'. Airtight Networks, August 2010. Accessed Jan 2011. <<http://www.airtightnetworks.com/WPA2-Hole196>>.
4. Jowitt, Tom Jowitt. 'Block wifi Intruders with a Secure Paint Job'. PC World, January 2009. Accessed Jan 2011. <[http://www.pcworld.com/businesscenter/article/158288/block\\_wifi\\_intruders\\_with\\_a\\_secure\\_paint\\_job.html](http://www.pcworld.com/businesscenter/article/158288/block_wifi_intruders_with_a_secure_paint_job.html)>.
5. 'COWPATY – attacking WPA/WPA2-PSK exchanges'. Will Hack for Sushi, 20 March 2008. Accessed Jan 2011. <<http://www.willhackforsushi.com/Cowpatty.html>>.
6. Ohigasji, Toshihiro; Morii, Masakatu. 'A Practical Message Falsification Attack on WPA'. Hiroshima University and Kobe University, August 2009. Accessed Jan 2011. <<http://jwis2009.nsysu.edu.tw/location/paper/A%20Practical%20Message%20Falsification%20Attack%20on%20WPA.pdf>>.
7. Marlinspike, Moxie. WPACracker, 2009 <<http://www.wpacracker.com/>>.