SOPHOS
Security made simple.

The World of WarBiking

By **James Lyne**, Global Head of Security Research

The World of Warbiking is an ambitious research project conceived to find out how our hunger to be online at all times is leaving millions of people and companies - and their sensitive data - exposed to hackers and spies. Weekly news coverage of data breaches and attacks would have the public believe nation states and unblockable super viruses are the key issue, but actually the absence of basic best practice is often too blame. Visiting cities all over the globe, Security Expert James Lyne presents the World of Warbiking,

The experiment kicked off on the famous streets of San Francisco, California, where we found some disturbing results followed by London in the UK with tours planned in Las Vegas, Vietnam and Australia shortly.

WarBiking Results Overview

Whilst the concept of Warbiking may be new, the notion of wardriving to identify wireless networks and overlay them on a map is actually rather old – so why are we talking about it now?

I have observed that often the security industry likes to talk about a security issue for a short time, before moving onto the next threat or security buzzword. For instance, it has been a good 10 years since the first major concerns over wireless security were thought to have been solved, and for many in the industry, it is a problem they considered 'cracked',

However, the explosion of connected devices in the last few years and the need for growing numbers of people to be constantly connected on the move via smartphones, tablets and laptops has seen the demand to be constantly online skyrocket. However, it is sometimes hard to identify just how well the general public and small businesses are doing in applying security best practice. Almost daily we hear news stories of widespread loss of password databases and depressingly poor password security. This would seem to support the notion that security is not always high on the agenda in the need to stay connected.

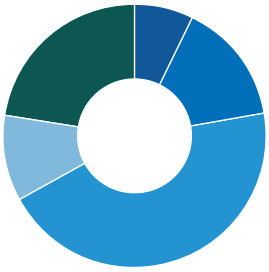
So we decided to to put it to the test. We set out to warbike San Francisco and find out just how much best practice was actually being applied and to raise awareness to the public of issues potentially not yet solved.

We will start by outlining the more obvious category of results, wireless access points, followed by user behavior and higher protocol concerns.

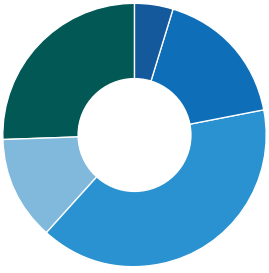
1. Network security

Whilst scanning the streets of San Francisco we aimed to identify how effectively people are securing their wireless networks. Within the confines of the law, without attacking networks, we were able to collect information about the supported security standards offered by each of the networks. The results were:

San Francisco	#	%
Total Networks:	72,312	
WEP Networks	6,869	9.5%
No Encryption	13,956	19.3%
WPA	41,704	57.7%
WPA2	9,783	13.5%
WPS	20,970	29%



London	#	%
Total Networks:	81,743	
WEP Networks	5,179	6.34%
No Encryption	18,946	23.18%
WPA	43,510	53.23%
WPA2	14,108	17.26%
WPS	27,970	34%



These broad categories show the different wireless security configurations in use. At first inspection this obviously seems bad, but to fully understand the problem we need to go in to more depth by reviewing what is in each category and the security issues associated with each.

Two brief notes on the category groupings:

1. Enterprise authentication options were grouped with WPA2 (and tiny)
2. The principle of lowest method offered was used, i.e. of WPA2+AES and WPA+TKIP was offered (typically for compatibility) the least secure was used as a category, as it is enabled and functional.

WEP Networks

WEP, or Wired Equivalent Privacy, has been understood to be severely broken since as far back as 2001. There are a number of faults that enable an attacker - equipped with readily available software and tools (even available on Amazon for a low price) - to retrieve pretty much any password combination in seconds. Take a look at this example here (HREF) where the password is recovered in next to no time at all.

Once the attacker has your password they can not only join your network and start attacking connected devices, but they can also monitor (or change) all your network communications. Your encryption becomes worthless.

A staggering 9.5% of networks that we found in San Francisco were making use of WEP, which is remarkable considering this standard has been known bad for so many years. You may as well put the welcome doormat down for attackers. This percentage of networks was a little higher than I have seen elsewhere (anecdotally), however there were certain areas with higher numbers of WEP APs grouped together. London on the other hand had 6.34% of networks using WEP, so a slight improvement on San Francisco. Anecdotally this figure is about half what it was in a prototype scan I conducted a little over 18 months ago - so progress has been made. That said this is still an alarmingly large number of users using standards known insecure for over 10 years!

No Encryption

Of the relatively large number of open networks, we discovered the majority looked to be open by design – that is to say they were networks with captive portals that people had to authenticate to before being able to access the network or the Internet.

A small number of networks were open and did not fit this profile (such as default named Linksys routers). Many would assume that the open by design networks are OK (they have made the decision to be open intentionally after all) but this does not necessarily follow. The lack of security when joining the network means that any information subsequently sent on the wireless network is unencrypted. Unfortunately most users do not take additional steps to encrypt their traffic and therefore any of their activities online can be easily monitored or even modified by an attacker whilst they sit at reputable 'Brand X Coffee Shop' or hotel. "A side of cyber attack with your mochaccino Sir?"

Aside from captive portals, sometimes people reject that open networks are a problem on the basis of MAC address filtering (matching your machines supposedly immutable hardware address to a predefined access list). Aside from the pain of managing such lists (which leads to limited deployment) it is trivial to bypass this restriction and for an attacker to automatically take over an existing authorized MAC address – there are even tools that will monitor the network and do it automatically. Open networks aren't necessarily bad if other mitigations are in place, but that is infrequent even in 2014 as you will see from the second stage of our test. It was also interesting to note that the number of open networks was significantly higher in London versus San Francisco with frequent occurrences of printers in default configuration as well as the more intentional free open wireless at hotels or alike.

WPA

There are a variety of different security configurations that can be used with WPA (Wi-Fi Protected Access) mode, though WPA+TKIP is the most common at 57.7% of networks detected. TKIP (Temporal Key Integrity protocol) was implemented as a quick fix to the security problems that WEP encountered and has been shown to have a number of flaws. On this basis, the Wi-Fi Alliance and the IEEE have shunned it for some time now. It is considered deprecated in the 2012 revision of the 802.11 wireless standard. In other words, while this standard certainly does not have the overt flaws that WEP (or no encryption) it is far from the recommended best practice in 2014! This was by far the largest percentage of networks identified by Warbiking San Francisco as most devices operate a WPA2+WPA mode to insure backwards compatibility.

WPA2

Only 13.5% of the networks in San Francisco used WPA2 (WPA2+AES being the majority and recommended best practice). Of course, this number of networks is a best-case scenario given that a number of these will have bad passwords. London had a higher percentage of the networks using the later security standards, that said a higher percentage of networks were using WPS potentially leaving them vulnerable to other vectors of attack as outlined below. Password cracking WPA2 is notably harder than earlier implementations, but it can still be performed at high speed with the right attack tools. Cracking the password requires a capture of the 'handshake' (or watching a device logon) after which various breaking attempts can be performed. A graphics card can be used to significantly accelerate the attack and there are readily available tools that do this.

If your password is based on a dictionary word, or a simple variation, it could be recovered and your traffic decrypted. It should be noted that other enterprise authentication mechanisms were also included in this category for simplicity, though they were not a statistically significant number.

WPS

Last, but certainly not least, WPS (Wi-Fi Protected Setup) is a convenience technology designed to enable quick connections without having to type long and complex passphrases (though long passphrases tend to be much rarer than we would all hope). It works be allowing a PIN to be entered which then authorizes the connection and allows them to connect (think of it as automatic configuration of the long passphrase based on a short, easy to type PIN).

WPS seems like a great idea but actually opens up an opportunity for attack – amongst other things, most access points do not 'throttle' the speed of PIN guesses. WPS is therefore open to an attack called 'Reaver' in which a brute force is used to recover the PIN and then the passphrase. Generally an attacker can break in to a network using this method in 4-10 hours, and by using various enhancements (such as predictions based on analysis of common WPS PIN codes) this time can be reduced significantly. Luck can also prevail, allowing an attacker to recover a PIN very quickly.

WPS is extremely common and can allow an attacker to get in to a network even when a strong password is set. Unfortunately, rate throttling and Reaver attack prevention is infrequently implemented in access points even today, making WPS potentially a very nasty backdoor in to 29% of the networks we saw in the City by the Bay and 34% in London.

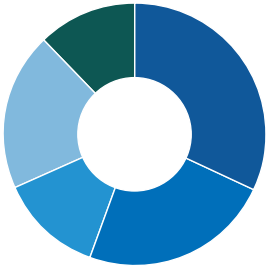
2. Users want the Internet and they don't care where they get it

Aside from the security issues of access points or hotspots, we wanted to look at another interesting issue: users simply do not care what they are connecting too to get their latest Internet fix.

To examine this, we created our very own hotspot with a captive portal page and allowed users to connect to the for free (provided by a 4G LTE modem). The captive portal page only required an acknowledgement and spelled out that we would monitor protocols (like any network running a good UTM or NGFW) but no traffic, user data or logs would be kept, only high-level statistics. Almost no users who connected to this hotspot chose not to proceed. We did not perform any manipulation, man in the middle, interception or attacks, although it would have been trivially easy to do so (a couple of extra command line switches in the tools we used). Here is an outline of the number of individuals who connected to our hotspot in a short space of time and a few choice facts about the protocols they used:

	San Francisco	London
SSIDs:	FreePublicWifi, Free Internet, DO NOT CONNECT	FreePublicWifi, Free Internet, DO NOT CONNECT
Connected users:	1512 people	2907 people
Used HTTPS:	672 people	437 people
Used HTTP:	1397 people	2901 people
Used Insecure Mail Protocols:	242 people	317 people
Used a VPN:	6% (or 94% that were open to manipulation)	2% (58 people) used a VPN
		Most requested pages: ‣ Facebook ‣ Webmail services (match OWA/Common types) ‣ Twitter ‣ Requests for Internet banking sites ‣ News sites

San Francisco	#	%
Platform	1,512	
iOS	484	32%
Android	358	23.7%
Other	194	12.8%
Windows	295	19.5%
Mac OS X	181	12%



Notes

- Only 6% of users in San Francisco and 2% of the users in London used a VPN.
- Only 27 users connected to the DO NOT CONNECT wireless network in San Francisco – it is good to see some degree of observation of security warnings.
- Unusually high number of iOS & Mac users were identified in San Francisco compared to other locations, but that is hardly surprising given the Bay area is the home of Apple.

There are a very small number of users utilizing a VPN to encrypt their traffic. This is concerning as they are on an entirely untrusted network (although, a cynical security professional might say 6% is a big improvement from years prior). This means many users exposed plain text protocols to our network. Any attacker nearby would be able to pick up the wireless traffic and read it – including 242 people who were handing over their e-mail password and e-mail contents. Only 2% of the users in London used a VPN vs 6% in San Francisco. Londoners were also more prepared to browse to sensitive sites like Internet banking than the more social media related activity we saw in San Francisco.

Of course traffic sniffing wasn't necessary as the users voluntarily connected to our network. If our network was malicious we could easily have stolen usernames/passwords, or modified web pages to insert malicious code, phishing scams or alike. Some users made use of the encrypted web browsing protocol 'HTTPS', though in many cases, if an attacker were to modify this (which generates an alert to the end user) the attacker would simply click accept to continue.

It is clear from this experiment that the default behavior of many mobile users is to find open networks, connect, test for Internet and ask questions later. This stage of the project demonstrates perhaps an even more concerning trend in that the majority of users are not taking steps to secure themselves when roaming out of the office, which is after all an increasing default. It also illustrates that aside from the technical issues of access points, we have social issues, or a requirement to educate those who would hand trust to any network offering a Facebook fix.

3. Other wireless protocols

In addition to the core wireless protocols, we also looked for other interesting signs of wireless traffic. Scanning for some of the wireless technology on our list, such as Radio Frequency Identification (RFID) and Near Field Communication (NFC) is explicitly prohibited by law in San Francisco, so in this instance we did not. We therefore focused on Bluetooth and its cousin (but very different) Bluetooth low energy.

Scanning for Bluetooth devices is notoriously difficult given challenges with rapid frequency hopping and until recently the lack of decent hardware for security professionals (compared to wireless where a $30 wireless card from Amazon works exceptionally well). There has been some fantastic work in the security industry on Bluetooth, including a number of methods of brute force detection of Bluetooth devices beyond those in discoverable mode. You can see more information on how we (or an attacker) could have gone further in our blog, but we decided to keep things very clean and only enumerate devices that were discoverable (or offering us a connection if you like).

With our polite approach to scanning we saw:

- BTLE (BlueTooth low energy) – surprising volume pulsing everywhere!
- Bluetooth - 3412 devices
  - Predominantly smart navigation or phones
  - Phones often named “James Lyne’s iPhone” or alike
  - A few vehicles, cars and systems
  - Many obvious default configuration devices

BTLE, as it turns out, is a surprisingly widely adopted technology. BlueTooth low energy is now used by a variety of different vendors. Apple for example has ‘iBeacons’ which are sent out over BTLE. Bluetooth low energy is used for device discover and for interaction with the physical world. For example, BTLE may be used in a store to allow an app on your phone to differentiate between whether you are standing by the shoes or perfume department and to change it’s behavior (advertising) based on that information. Amidst the excitement of iOS7 many missed the announcement of iBeacons. They are fully available for app developers to integrate for location-based interactions.

More broadly BLE is being explored for uses such as mobile payments too. A detailed review of BTLE and associated security mechanisms is beyond the review of this quick report, though it is well worth reading up on. Suffice to say this technology has slipped in to widespread use with the majority of people I asked about it en route having never even heard of it.

Traditional BlueTooth was also very widely used with a large number of satellite navigation, audio kits and smartphones. These devices were discoverable and awaiting connections, but will typically be protected by a PIN code. Unfortunately, a great number of devices use a default PIN such as 0000, 1234 or 9876 (a longer list can easily be used for guessing, but already I’ve probably listed a PIN one of your Bluetooth devices uses). Indeed, many of the devices such as audio kits for cars do not allow you to change the PIN (and if it does, most people have no idea how to change it). This represents an interesting opportunity for attackers to hijack such devices and perhaps inject audio in to a nearby driver’s vehicle or headset.

Measuring the active vulnerability of these devices is difficult given the law, but it is interesting to see the growing use of the protocol and a surprising number of users enabling Bluetooth on phones. Bluetooth has been around for a long time but, anecdotally, use seems to be rapidly increasing. This could be in connection to several recent features such as AirDrop on iOS 7 which uses a combination of Bluetooth and Wireless to quickly configure an ad-hoc network to exchange files. When you turn on AirDrop, notice how both Bluetooth and wireless are enabled and don’t turn themselves off again.

There are many other protocols and wireless standards we could have inspected, but the objective of this third stage was to identify if other wireless technologies were in widespread use and whether there were similar configuration challenges.

Why is this still a problem? The truth about our insatiable appetite for being connected

Issue 1 - it's 2014!

Many of the standards we found in use in San Francisco and London have been known to be totally broken for many years now – WEP being perhaps the best example. So why, 10 years since this was declared trivial to hack, is it still in relatively widespread use? There are a few issues that allow these problems to continue – the first is awareness.

Most access points allow the user to select from a number of different security standards (from open to WPA2, and these include WEP) and some of the older access points even default to bad standards such as WEP. Many users set up their access point and have never considered the need to change it. They are therefore left in a configuration where they can be attacked, but are entirely unaware of the risks. We hope that our Warbiking project helps raise awareness to the people running in this configuration.

Issue 2 – regulatory infrastructure

The second issue is that whilst there are bodies focused on wireless (such as the WiFi Alliance) they are consortium standards not black letter law enforcements to change. Globally, there is relatively poor infrastructure for regulation of technology and to drive quality standards. In the US this infrastructure is all but non-existent and the only approach would be a legal obligation through legislation that would impact those that use blacklisted standards (of which the likes of WEP should certainly be included).

In Europe we do have a formalized standardization infrastructure but there is presently no policy consideration of wireless security. Some other vertical specific standards have moved to blacklist WEP, for example PCI (https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf) has guidelines that prohibit the use of WEP after 2010. This is appreciably still many years after the original flaws were found and do note the paper does not make reference to the flaws with WPS (Wi-Fi Protected Setup).

Issue 3 – old standards, new threats

Another issue is one that teaches us an interesting lesson about the mass of 'Internet of Things' devices being adopted. A large number of the access points serving up wireless are likely older access points that were acquired some time ago and will dutifully sit in service until they break. A smooth transition to newer standards is not trivial, but there are flaws that could have been addressed which just aren't in the present ecosystem.

Unlike the mainstream laptop, these devices have very poor updating infrastructure and few means to be enhanced or fixed without significant user intervention. It is not expected that wireless providers make changes to their devices to prevent Reaver WPS attacks and then deploy this to their customer base, they can just post it and people can download it "if they choose". This of course assumes that a fix is issued at all, which you might find unlikely if you followed the news about the plethora of home routers with gaping security flaws over 2013.

Many of these new Internet of Things devices are in the same box – they are considered black boxes (not computers) and do not receive the same security concerns, configuration checks or even attitudes towards quality and updatability. The abysmal failure to eliminate the use of standards known to be completely compromised since 2001 should be a warning to future developers of such infrastructure.

It is impossible to know how long a security standard or cryptographic method will be trusted and, as much as possible, products should be designed with updatability in mind, such that over time quality issues can be addressed without the dependence on the user to download and install firmware patches to their devices. This issue will only worsen as more black box devices enter our homes and businesses, so we should learn the lesson before it is too late.

Issue 4 – Lack of awareness

Lastly we need to address the issue of users connecting to untrusted wireless and using protocols with a lack of integrity checking and security. There are good mitigations available to these issues, but again awareness is a key factor. We have also observed that many of the security concerns users had with the 'traditional PCs' do not register as concerns on a mobile device (which are wrongly assumed 100% secure).

Small businesses should insure they have controls in place for roaming users and mobile devices, while user education should again become a key focus. As our experiment shows, too many users are still prepared to click first, think later and failing to protect their information in transit.

What should I do about it?

As our exercise in the first stop in the World of Warbiking tour has proven, serious issues exist with wireless security – issues that could put people, companies and their data at risk.

To help, we have put together some very simple tips at http://www.sophos.com/tips. These are designed to be shared with those with less technical expertise and use fairly plain speaking. The most important thing you can do is to make sure you are not part of the problemYou can also find a video we made about the exercise at http://www.sophos.com/warbiking which we hope you will share with others to help educate family, friends and colleagues about these issues.

If you are a small business, the age-old principle of defense in depth is a good one to apply here. Of course, you should be using best practice encryption and authentication for your wireless network, but you should check this at any branch offices too. Laptops and mobile devices can be configured with a VPN to be protected when using less trustworthy networks, and of course you should use use up to date, modern protocols to access key services like email to provide an additional layer of encryption and integrity.

You can find more information about secure wireless, network security (including VPN) and mobile device management at http://www.sophos.com/en-us/products/unified-threat-management.aspx.

Good luck and thank you for helping to secure the world's wireless networks, one access point and device at a time!

Sophos UTM

Get a free trial at sophos.com/try-utm

More than 100 million users in 150 countries rely on Sophos as the best protection against complex threats and data loss. Sophos is committed to providing complete security solutions that are simple to deploy, manage, and use that deliver the industry's lowest total cost of ownership. Sophos offers award winning encryption, endpoint security, web, email, mobile, server and network security backed by SophosLabs—a global network of threat intelligence centers. Read more at www.sophos.com/products.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

1155-04.14DD.wpna.simple

SOPHOS