



The Security Division of EMC

White paper

The Wireless Security Survey of London

7th Edition



Report Commissioned by RSA, The Security Division of EMC

October 2008

Contents

I. Executive Summary	page 1
II. Key Findings & Results	page 3
III. Summary	page 6
Appendix A – Recommended Wireless LAN Security Policy	page 7
Appendix B – Paris Survey Details & Route	page 7
Appendix C – Comparative Survey Results from London and Paris	page 8
Appendix D – Wireless Networks Background	page 9

Foreword

RSA, The Security Division of EMC, initiated its campaign to promote and improve best practices in wireless security over seven years ago – and that campaign has never been more pertinent to businesses and consumers than it is today.

Just this summer, the United States' Department of Justice indicted an international ring of hackers who had allegedly stolen more than 40 million credit card numbers from several restaurants and stores. The hackers' method for apparently perpetrating this massive theft? Wardriving, and the exploitation of those businesses' poorly-secured wireless networks. Clearly, in this era of unrelenting regulatory compliance and a sharp focus on the ability to keep sensitive proprietary and customer information properly protected, it is more important than ever to close the wireless loophole and ensure that the countless investments being made in securing networks everywhere are not undone by leaving the back-door wide-open.

First introduced in London's financial district in 2001, this year's RSA survey was conducted in London, Paris and New York. The premise for the research lies in the critical need to protect private information and to manage the identities of the people and applications sharing that information. As the use of wireless networking technology continues to explode – just take a look at this report for the picture of how adoption has ballooned in the past year alone – it is critical that network owners and administrators match that pace with sufficient security and information protection measures.

We talk in this report about 'good wireless security hygiene', and it is encouraging to note that we found that just 3% of corporate wireless access points in New York were unsecured this year... by far the best results recorded in the seven years of the survey. Additionally, in Paris we saw that 72% of all access points (excluding public hotspots) were using advanced forms of encryption. This is a good step forward – although advanced (non-WEP) encryption needs to become the norm, and rapidly. Also consider that one-in-five of all business access points in London continue to be completely unprotected by any form of wireless encryption. This was worse than our findings in London in 2007, and – embarrassingly – worse than the overall security posture of in-home networks, which we break out this year for the first time.

An increasingly savvy Internet generation is often able to take advantage of such security weaknesses. They are well aware of the abundance of WLANs and know that they will quickly find a free network with just a few minutes of roaming.

As wireless networks continue to improve in terms of speed, bandwidth and safety, this is good news for businesses and consumers alike. However, the potential consequences of unidentified users and applications accessing sensitive, private information are simply too serious to be ignored.

Sam Curry
Vice President, Identity & Access Assurance Group
RSA, The Security Division of EMC
October 2008

I. Executive Summary

Drawn from three major global cities, the results of the seventh annual wireless survey illustrate that wireless networks continue to be an increasingly-vital part of the IT infrastructure we use in our everyday work and personal lives.

This year's survey once again examined levels of wireless network technology adoption and related security practices in three major European and US cities – London, Paris and New York.

The survey's findings underscore, once again, the accelerating pervasiveness of wireless access in major metropolitan areas. In all three cities, the prevalence of wireless access points (APs) continues to rise. Unlike in previous years though, the overall posture of security and connection encryption has shifted wildly to reflect encrypted airwaves.

As expected, public hotspots continue to proliferate wherever connectivity-seeking coffee drinkers and travellers are to be found. The convenience of these public access points should be contrasted with their inherent and significant security risks – often disregarded by their ardent users.

Access Point Growth

It will come as little surprise that in all three cities the total number of wireless access points (APs) – encompassing public hotspots, home networks and corporate access points – has grown significantly. However, the largest year-on-year growth – which was recorded, by a great distance, in Paris – was simply staggering: where we found just 825 access points in our 2007 survey, this year the volume on the same route had exploded to 4,481 access points, representing growth in Paris of 543%. This dwarfs, by comparison, the significant increases once again seen in London, where access points leapt by over 72%, and in New York, which jumped 45%. London maintains its overall position of leading the way in terms of sheer volume, with 12,276 access points detected – up from 7,130 in 2007.

Looking purely at the number of corporate APs, however, New York has overtaken London since last year. We found 6,096 access points that could be identified as belonging to a business in New York, a greater number than the 4,927 found in London and the 3,265 in Paris.

Advanced Encryption

While the earlier editions of this survey looked simply at whether or not business wireless networks were protected by some form of encryption, as the security vulnerabilities in Wired Equivalent Privacy (WEP) have been well-documented our survey has paid close attention to the relative adoption of more advanced forms of wireless encryption. These include 802.11i-based Wi-Fi Protected Access (WPA) or WPA2, and this year we were able to comprehensively drill-down into the types of encryption being used by both businesses and home-users.

More detail follows in the charts below, but overall the adoption of advanced encryption is encouraging. Paris once again led the way, with 72% of access points (excluding public hotspots) found to be using advanced security; the numbers in New York and London were 49% and 48% respectively.

Hotspots

Public hotspots – designed to allow anyone with a wireless device to access the Internet on a pay-as-you-go or pre-paid basis – continue to grow in prevalence across all three cities. Each city's hotspot-growth accelerated significantly in 2008 compared with development in preceding years: Paris, which registered a 37%-growth in hotspots in 2007, saw the largest increase this year with a massive jump of 304%. New York's wireless hotspots grew 44% (last year, the growth in the city was a modest 17%) and London grew by 34%.

New York City remains out in front in regards to its concentration of hotspots. At 15%, New York is well clear of London where 5% of wireless access points were found to be hotspots. In Paris, hotspots represent 6% of all the access points we located in the French capital.

Security Levels

Despite the growing numbers using advanced security, it is very concerning that one-in-five of all business access points in London continue to be completely unprotected by any form of wireless encryption. This has even slightly deteriorated from 2007 when that number stood at 19%. By contrast, wireless 'hygiene' among the business community is far better in both New York (just 3% unencrypted) and Paris (6% unencrypted) – these are the best figures we have recorded since the annual survey began in 2001.

While these unprotected business networks may be requiring their users to log-in via an encrypted Virtual Private Network (VPN), not using WPA1 or WPA2 can leave the organizations involved vulnerable to whole classes of attacks against both access points and wireless client computers.

Unsecured business networks were identified as those which were clearly not hotspots, yet may offer Internet access to users connecting to them either accidentally or intentionally. Users connecting to an unsecured business network instead of a wireless hotspot, deliberately or otherwise, pose a serious risk to corporate security and data privacy. Today's mobile users expect to find wireless hotspots with ease; if they do not they may be tempted to take advantage of the access provided by corporate wireless networks. The potential consequences of unauthorised access include the theft of sensitive and confidential corporate and customer data, and the instigation of further security breaches such as undercover DOS attacks and identity theft.

In-home Wireless Networks

The development of this piece of the wireless environment has contributed greatly to the overall results. Large quantities of generic yet predictably unique networks from a couple of the large cable and satellite providers have introduced thousands of secure personal wireless networks into the streets. In London, the volume of personal wireless access points was greater even than the number of corporate ones: a total of 6,730 – or 55% of all access points detected – were identified as belonging to home-users. In New York, 18% of access points were in-home and in Paris the figure was 21%.

Surprisingly, home network users appear to be more security-savvy than their corporate counterparts: In Paris, 98% of in-home networks are encrypted – an excellent result – with New York just behind at 97% and 90% of Londoners deploying encryption at home. Additionally, the proportion of home-users who have deployed advanced encryption outpaces the business sector in Paris and New York, with the same percentages for both groups in London.

Summary

While London continues to dominate this survey in terms of the sheer volume of access points deployed, from a security standpoint it is now lagging behind both Paris and New York. New Yorkers should be proud that just 3% of their networks – in-home and business – are unsecured, a vast improvement on 2007 when 24% of the city's corporate access points were unencrypted. Clearly, the call for stronger security in wireless networks has resonated well, and it is interesting to note a shift in the alignment of the cities this year: Paris and New York are much closer in terms of trends and patterns, whereas in previous years London and Paris have typically mirrored each other.

Overall, though, it is Paris that has made the most progress since our last survey. A 543% increase in access points; 304% growth in public hotspots; 94% of its business access points are secured; and 98% of its in-home networks are encrypted. Bravo, Paris!

Phil Cracknell, Konstantin Gavrilenko
and Andrew Vladimirov – Arhont Ltd (Authors of WiFio)

II. Key Findings & Results

London retains its position as the most ‘wireless city’ in our survey.

The wireless survey of London showed a massive growth rate in the number of individual access points, and an increase in public access points. In 2005, a total of 1,751 access points were detected along the route, and by 2007 this figure had risen to 7,130. The 2008 survey identified 12,276 access points which is a phenomenal 72% increase on the previous results.

The security of London’s corporate access points has seen quite a fall from grace over the last year: while New York and Paris have cleaned up their act, with just 3% and 6% of business access points unsecured respectively, London saw its numbers get slightly worse, with 20% showing no form of wireless encryption at all.

London’s home-users were also the least security-conscious: 10% have left their in-home networks unsecured, compared with 3% in New York and 2% in Paris.

Access Point Types

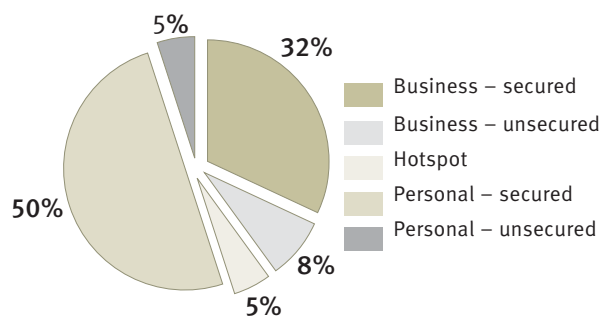
Using the characteristics of each connection we were able to accurately identify if an access point fell into the following categories:

- Business – secured/private access
- Business – unsecured
- Personal – secured/private access
- Personal – unsecured
- Hotspot – paid, public access

Security Levels

In the 2008 survey we were able to assess and ‘grade’ the different forms of security deployed by businesses and home-users, providing a revealing picture of the relative security posture that exists across the spectrum in each city.

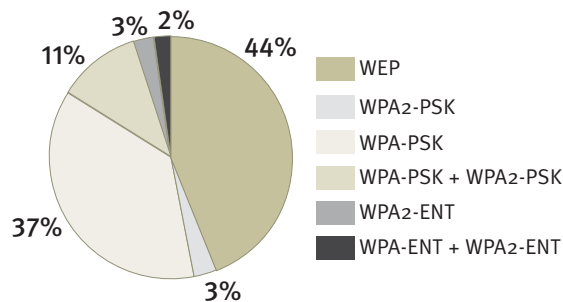
Access Point Types in London



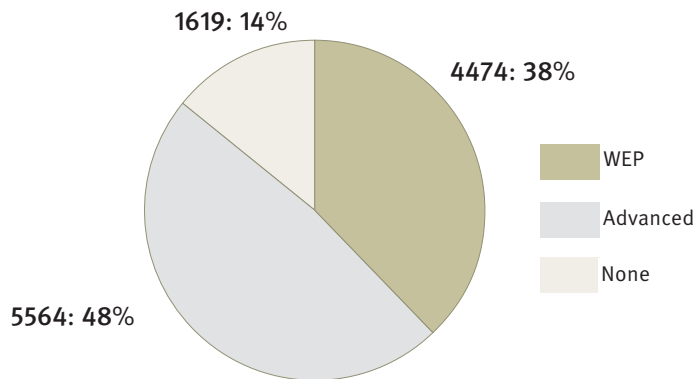
Forms of Encryption: Public hotspots aside, our recommendation is that all wireless access points should be protected with some form of encryption. With WEP now largely discredited, this year we examined how many network-owners have been wise to these vulnerabilities and started moving up to stronger forms of encryption for their wireless networks.

Of the systems that were encrypted, the diagram below shows a breakdown of the encryption methods used. We would consider ‘Advanced Security Levels’ to incorporate all non-WEP forms of encryption and authentication. These forms include 802.11i-based WPA1 and WPA2 in both SOHO and Enterprise configurations. (As a rule of a thumb, correctly set-up and managed WPA1/2 Enterprise is significantly more secure than WPA1/2 SOHO, but is also more difficult and expensive to maintain. While WPA1 was designed as a temporary replacement for WEP until WPA2 arrived, it would be incorrect to state that its security level is inferior to that of WPA2: Over the years of practical use, no exploitable WPA1-specific vulnerabilities have been discovered that are not present within WPA2.)

In London, 56% of all secured access points were found to be using advanced forms of encryption. In this respect, the English capital was ahead of New York (52%) but some distance behind Paris, which is setting the pace here with its advanced security figure of 76%.



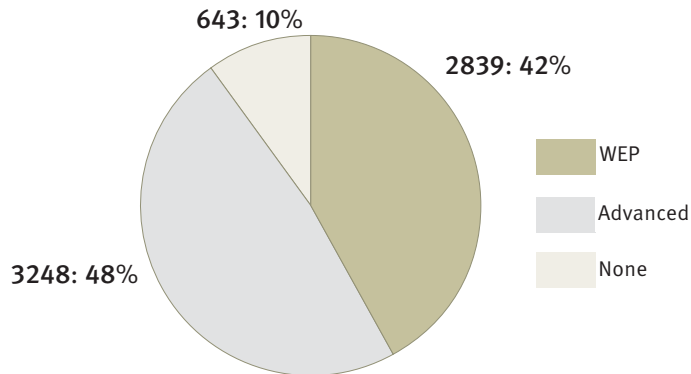
Advanced Security Levels



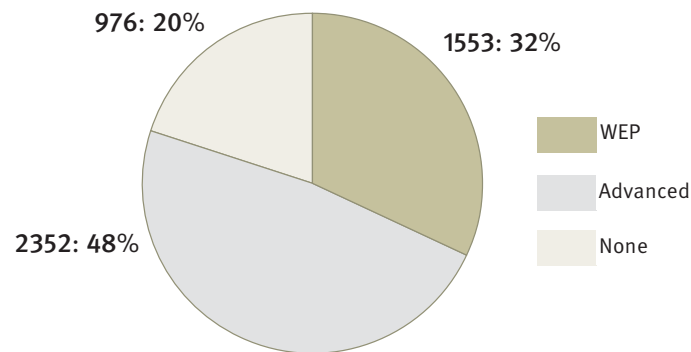
Encryption Breakdown in London – Overall

A split of almost 50/50 between those using advanced encryption and those using WEP or nothing at all is quite worrying. Note that this chart excludes systems that should be open (public hotspots).

52% of wireless access-point owners should be looking to improve their security posture. As mentioned earlier, while any unprotected business networks may be requiring their users to log-in via an encrypted Virtual Private Network (VPN), leaving the network itself unencrypted can leave the organizations involved vulnerable to various wireless-specific attacks.



Encryption Breakdown – In-home Networks in London



Encryption Breakdown – Business Networks in London

As the two detailed breakdowns of security in London's in-home and business access points show in the charts on the previous page, personal users appear to be leading the way: similar proportions in each group are using advanced encryption, and just 10% of in-home networks use no encryption at all, compared with a stunning 20% of the business community.

Hotspots

Wireless hotspots are growing in prevalence across all three cities. In the 2007 survey we detected 461 on the route around London; this year we detected 619 hotspots on the same route, representing an increase of 34%.

Hotspots account for 5% of all wireless access points in London. This number puts London behind both New York City – where 15% of all access points are publicly-available – and Paris, where the percentage is 6%.

A hotspot will typically broadcast its presence by advertising a recognizable ESSID, which is often the name of the establishment in which the hotspot is located, or a commonly-known provider (look for ESSIDs containing 'Free', 'Guest', 'Hotel', 'Cafeteria', etc.). Visible signs will be in place informing customers of the hotspot and in many cases there will be leaflets telling them how to connect.

Generally neither WEP nor WPA is in use as they would require the client system to be a party to the encryption key or certificate. Finally, both DHCP (Dynamic Host Configuration Protocol) and browser redirection will be active, and so a user's system should be assigned an IP address and once this is established the hotspot's homepage will appear. This homepage will contain details of how to buy access or how to login if you have already bought access.

Usually, access to any service is not permitted until the user has connected to the hotspot homepage and registered or logged in. However, attackers can always disconnect a legitimate user with a denial of service attack and take his or her place by spoofing both MAC and IP addresses. This provides a good avenue for online identity faking and hiding.

- Hotspots can pose a serious threat to businesses using wireless networks in a number of ways. Initially, they are responsible for more people searching for accessible networks; unlike in the earlier years of the survey, if you have a WLAN today, it is likely to be found and used.
- Secondly – focusing more on the mobile business users of hotspots – there is at present no formal recognition of a hotspot owner and no true indication of its legitimacy at the network layer. The industry is lacking a method of identifying that a particular hotspot belongs to a licensed or registered hotspot provider. Considering the information that could be gathered simply by installing a rogue hotspot (bogus access points designed to look like genuine hotspots and to capture important private information from users) in the vicinity of valid access points, this risk must be considered extremely high.

Rogue Hotspots

A rogue hotspot is a temporary wireless access point designed to look like a genuine hotspot and established to capture important security information from users who inadvertently log on to it. Rogue hotspots can efficiently exploit vulnerabilities in network discovery algorithms used by client devices and present a variety of fake capture portals, as well as launching client-side exploits, typically against web browsers.

The number of rogue hotspots in existence is extremely difficult to estimate - they exist for relatively short periods of time in order to avoid detection, and are very simple to implement. There is also little need to maintain a rogue hotspot, as they rapidly yield valuable information.

It has also recently been proved that it is possible to build a test system on a laptop which emulates a commonly seen hotspot. In private tests, devices have connected to test 'rogue' hotspots rather than the genuine article, as the rogue hotspot is indistinguishable from the real thing. Such fake hotspots can even process credit card details and allow Internet access. This simple configuration could potentially be the next big thing in identity theft as it has a greater capacity – and yields more accurate results - than current phishing attacks. It is feasible that identities could be stolen using a system like this.

III. Summary

It is safe to say that wireless technology has been widely-adopted and accepted in most cities globally. Over its seven years, this survey has seen trends develop and security fluctuate: we have seen a variety of new security issues introduced, addressed and superseded.

As always there seems to be a new and significant threat or development wrapped up in each survey, and the major security concern we have at the moment is that users appear to be working with a false sense of security in two areas:

1. There is a belief that ANY type of encryption will suffice; and
2. Equally, people believe that the advanced encryption options are invulnerable.

WEP is not secure by any means, but both WPA1 and WPA2, in SOHO and Enterprise configurations, must be properly set-up and maintained if they are to offer the high level of security that is built into these countermeasures.

Now that the network media is more secure, the focus shifts to the client systems and how they can be ‘easily’ compromised. A client compromise can lead to a more lateral type of attack against a corporate environment because it is harder to detect; it can go on over a longer period of time; and, generally, it has more “permission” to traverse the target network because it is accessing it as an authorised user! The majority of client-side attacks are launched employing rogue access points specifically configured to lure, associate and exploit vulnerable client devices. Such exploitation can be related to the access point search algorithms, weak client device security settings and even buffer and input validation flaws within the wireless client device drivers.

Many of the client attack countermeasures are administrative, rather than technical, and require a lot of work on the policy and enforcement side, so that the client hosts only associate to highly-secure networks and their wireless profiles are regularly cleaned. This must be supplemented by deploying distributed wireless IDS/IPS to monitor the airwaves for malicious access points, and by ensuring that the client device drivers are fully updated and patched. The old adage – ‘defence in depth’, or ‘layered security’ – has never been more relevant. A client VPN with some type of strong, two-factor authentication (and all VPN-unprotected traffic banned) should counter many client-targeted attacks.

We’ve pulled up the drawbridge and manned the castle turrets but we have left the outrider, galloping towards the fort, somewhat exposed while we sit inside feeling secure! At the same time, that outrider usually has the keys to the main gates.

Appendix A – Recommended WLAN Security Policy

This wireless LAN security policy has been developed from industry best practices and general information security common sense.

- All wireless access points / base stations connected to the corporate network should be approved by the computer security department
- All wireless client devices used in corporate laptop or desktop computers must be registered with the computer security team and where applicable enabled for access using MAC address control on the access points
- Lost or stolen wireless-enabled computers should be reported immediately
- All wireless LAN access must use corporate-approved vendor products and security configurations
- WPA Enterprise must be used to protect corporate networks. The use of WPA SOHO is acceptable for small businesses, where regular strong shared key generation and change routines must be observed. The use of WEP for protecting any wireless connections must be explicitly prohibited.
- EAP-TLS is the most secure EAP type to employ as a part of your WPA Enterprise-based defensive scheme, for as long as you use client host certificates protected with strong passwords. You will need to deploy industry-grade Certification Authority (CA) to create, distribute and manage these certificates efficiently. Also, configure end hosts to validate certificates and connect to approved authentication servers only.
- Avoid using EAP-MD5, EAP-LEAP and the "anonymous mode" of EAP-FAST. Use strong MS-CHAPv2 passwords with EAP-PEAP and EAP-TTLS.
- In highly-secure environments, all computers with wireless LAN devices should utilise a corporate-approved Virtual Private Network (VPN) for communication across the wireless link. The VPN will authenticate users and encrypt all network traffic in addition to WPA-based defences. The end hosts must be configured not to send any traffic across connections not protected by the VPN, thus eliminating many wireless client-side attack risks.
- If a VPN is in use, wireless access points must be deployed so that all wireless traffic is directed through a VPN device before entering the corporate network. The VPN device should be configured to drop all unauthenticated and unencrypted traffic
- The wireless Extended Service Set Identifier (ESSID) should be vague and defined by the security department
- The transmit power for access points / base stations near a building's perimeter (such as near exterior walls or top floors) should be turned down. Alternatively, wireless systems in these areas could use directional antennas to control signal emanation.
- Regular auditing of the wireless environment should take place. This especially applies to businesses that do not use wireless and wish to keep their environment that way. Monitor the area for unauthorized access points and client devices (including ad-hoc nodes), wireless intrusion attempts and denial-of-service (DoS) attacks.
- Ensure all mobile users are educated in the use of public WLANs (hotspots), and in particular the risks of connecting to a rogue hotspot. Email usernames/passwords should not be sent over an unencrypted link. During browser sessions the user should be aware that all data input not protected with SSL/TLS could be eavesdropped.

Appendix B – London Survey Details

The wireless survey of London was conducted as part of an ongoing study of major cities to identify wireless use and the security of such networks. This time we specifically attempted to identify hotspots, private business networks (secured or otherwise), and in-home networks (secured or otherwise).

Route

The survey followed an identical route to that used in the 2007 study, and indeed in all previous years. It covered the following districts of London:

Holborn

Clerkenwell

Shoreditch

City (Moorgate, St. Paul's, Bank, Fenchurch & Liverpool Streets)

St Luke's

Finsbury

Spitalfields

Canary Wharf and Docklands

Equipment

The survey was carried out using an IBM ThinkPad T61 with an inbuilt antenna.

When devices were detected the software once again identified the channel, ESSID and other network information before moving on from that source. The software had no way of capturing or retaining the data content of sessions detected.

The information gathered from each brief connection enabled offline analysis of the networks to identify any of the following where available:

Extended Service Set ID (ESSID)

Channel (1-11)

WEP or other security method

Advanced encryption

Mode of operation (Ad-hoc, station, access point, infrastructure)

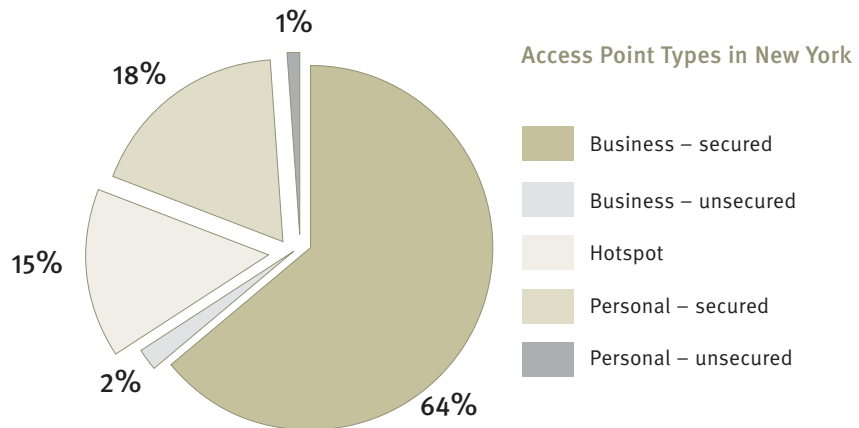
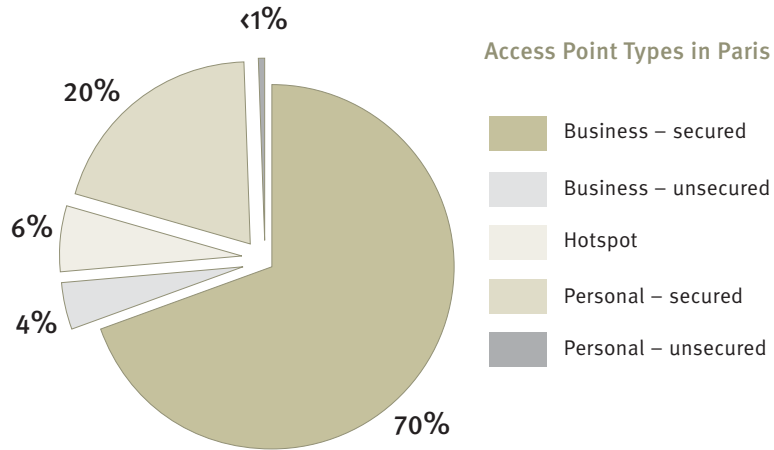
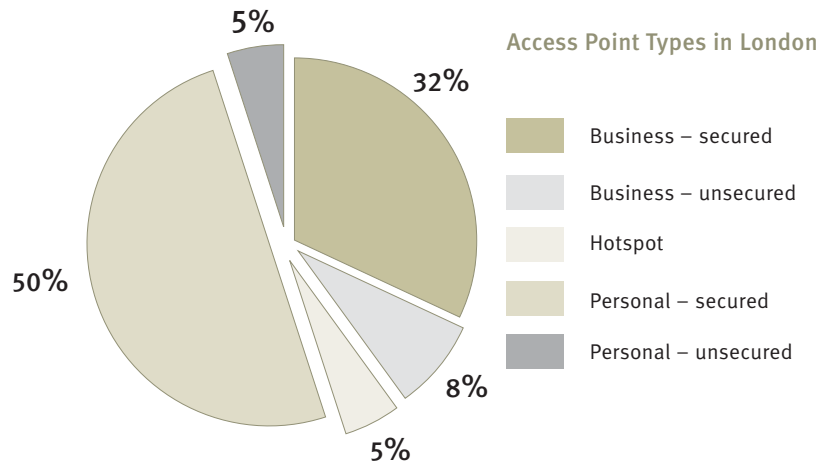
MAC Address

Hardware vendor

The nature of the AP response, security levels, ESSID values, broadcasting, physical location and presence of other APs with the same ESSID enabled us to deduce which were public access systems and which were private business systems which a high degree of accuracy.

The laptop and software scanner again detected both broadcasting and non-broadcasting APs in the 802.11a, b, g and n hardware.

Appendix C – Comparative Survey Results from Paris and New York City



Appendix D – Wireless Networks: Background

The IEEE 802.11b specification was the first layer 2 (OSI model) protocol to enjoy wide acceptance in 2000/2001. It is designed to allow Ethernet connectivity between two radio devices operating in the currently unlicensed 2.4GHz spectrum.

Such configurations can be used for peer-to-peer connectivity but where WiFi is concerned the more typical configuration is a radio device configured as the network card for each client and a radio device configured as a central hub on the network known as an “access point” (AP). The standard was designed as a replacement technology for data cables, becoming the entire LAN cabling in the case of peer-to-peer or the last 100 feet in the case of multiple clients connected to an access point.

The traffic between the client(s) and the access point travels ‘in the air’ and so an encryption method to protect the transmitted data from being eavesdropped was introduced. The initial (and commonly implemented) standard today is WEP (Wired Equivalent Privacy), but recent discoveries about the inherent weakness in the design have led to rapid efforts to introduce stronger encryption technology as part of the standard 802.1x.

The fundamental operation of wireless networks introduces new risks over the wired network: traditionally a network manager can control access to the network physically but with wireless it is not as easy to do so.

In addition, access points are being installed throughout the network, inside the firewall, often without the knowledge of the network manager. For these reasons it is critical to introduce authentication before any network access can occur.

IEEE 802.11

IEEE 802.11 refers to a family of specifications developed by the IEEE for wireless technology. 802.11 specifies an over-the-air communication between wireless units (client/AP, AP/AP, client/client). The IEEE accepted the specification in 1997.

There are several components of the 802.11 specification:

- 802.11 – applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either FHSS or DSSS.
- 802.11a – an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.
- 802.11b – an extension to 802.11 that applies to wireless LANs and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.
- 802.11d – a wireless communications specification for use in countries where systems using other standards in the 802.11 family are not allowed to operate. The 802.11d standard is well suited for the systems that want to provide global roaming because although it is like 802.11b in many aspects, the MAC layer configuration allows it to comply with the rules of the country in which the network is being used.
- 802.11e – a proposed enhancement to the 11a/b specifications to offer Quality of Service (QoS) through prioritization of protocols such as voice, video and data.
- 802.11g – applies to wireless LANs and provides 20+ Mbps in the 2.4 GHz band.
- 802.11i – a standard for wireless LANs that provides improved encryption for networks that use the 11a, b and g standards at present. The new protocols, namely TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) are required in any such 11i implementation. The standard was officially ratified in June 2004. The new enhancements actually satisfy many of the defined requirements for governments to use wireless networks, although AES requires a dedicated chip for processing and as such may result in hardware upgrades for current networks to conform to the standard.
- 802.11x – refers to a group of evolving WLAN standards being developed but as yet not formally approved. This includes:
 - 802.11e – Adds Quality of Service (QoS) features to existing 802.11 family specifications
 - 802.11f – Adds Access Point Interoperability to existing 802.11 family specifications
 - 802.11h – Resolves interference issues with existing 802.11 family specifications
 - 802.11j – Japanese regulatory extensions to 802.11 family specifications
 - 802.11k – Radio resource measurement for 802.11 specifications so that a wireless network can be used more efficiently
 - 802.11m – Enhanced maintenance features, improvements, and amendments to existing 802.11 family specifications
 - 802.11n – Next generation of 802.11 family specifications, with throughput in excess of 100 Mbps



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

RSA and RSA Security are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products or services mentioned are trademarks of their respective owners. ©2006-2008 RSA Security Inc. All rights reserved.

WLANLN WP 1008