



The Security Division of EMC

White paper

The Wireless Security Survey of New York City

3rd Edition



Contents

I. Executive Summary	page 1
II. Key Findings & Results	page 2
III. Summary	page 4
Appendix A – Recommended Wireless LAN Security Policy	page 5
Appendix B – New York City Survey Details & Route	page 6
Appendix C – Comparative Survey Results from London and Paris	page 7
Appendix D – Wireless Networks Background	page 8

Foreword

As part of its campaign to promote and improve best practices in wireless security, RSA, The Security Division of EMC, has commissioned annual research over the past six years. First introduced in London's financial district in 2002, the study has since incorporated additional business and financial hubs in Europe (Frankfurt, Paris and Milan) and the United States (New York City and San Francisco). This year's research 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. The concern is that the use of wireless networking technology continues to rise, yet network owners and administrators are failing to match that pace with sufficient security and information protection measures.

Wireless access is increasingly available: at home, in the office, at the airport, in hotel lobbies and on the street. Such networks are simple to install and use, bringing immediate and obvious benefits. In the workplace, however, one of the disadvantages of this simplicity is that individual departments are able to install wireless local area networks (WLANs) independently, potentially circumventing the standard – and necessary – procedural

and security checks. This has contributed to large numbers of wireless networks operating with no encryption or alternative means of protection, unwittingly identifying themselves by company name and broadcasting potentially sensitive corporate information to the outside world.

An increasingly savvy Internet generation is often able to take advantage of such security weaknesses. No longer needing to find a specific network in a particular building, users 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. All they need to do is power up, tune in and log on.

Wireless networks continue to improve in terms of speed, bandwidth and safety. This is good news for businesses and consumers alike, and will likely help to drive regulatory standards. But this progress must be matched by an equal, if not more intense, focus on security. The findings of this report are serious enough to represent a sharp wake-up call, forcing organizations to encrypt their wireless communication channels and not to rely on products' default settings. The potential consequences of unidentified users and applications accessing private information are simply too serious to be ignored.

Christopher Young
Vice President, Consumer and Access Solutions
RSA, The Security Division of EMC
June 2007

I. Executive Summary

Drawn from three major global cities, the results of the sixth annual wireless survey illustrate that wireless networks are a vital part of the IT infrastructure we use in our everyday work and personal lives. This year's survey 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 and yet the adoption of measures to secure the data on these networks lags – still. Between a quarter to a fifth of corporate wireless access points remain unsecured, wide open to anyone with a wireless device.

As expected, public hotspots continue to crop up wherever connectivity-seeking coffee drinkers and travelers are 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 – encompassing public hotspots and corporate access points – has grown significantly. London once again experienced the largest percentage increase in access points – an extraordinary 160 percent, up from 57 percent the previous year. This explosive growth to 7130 access points places London well ahead of New York City in wireless access. New York City showed a growth rate of almost 49 percent, up from 20 percent the previous year, while Paris saw a 44 percent increase.

Looking purely at the number of corporate APs, London also leads. The city saw exponential growth of 180 percent, as compared to 57 percent and 45 percent increases in New York City and Paris, respectively.

Advanced Encryption

One bright spot in this year's survey is the finding that wireless access point operators are moving away from Wired Equivalent Privacy (WEP) – which offers limited protection – and toward more advanced forms of encryption. The survey measured the use of advanced encryption as indicated by

implementation of 802.11i and WPA. Across all three cities there was a significant increase in implementation of these standards. This is an encouraging sign as the limitations of WEP have become increasingly clear. In New York City 49 percent of all secure business access points we detected had implemented advanced forms of encryption. In Paris the figure was lower at 41 percent, and London was comparable to New York at 48 percent.

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. Paris leads the way in growth, with an increase of 37 percent, followed by London at 27 percent and New York City at a modest 17 percent.

Though New York City experienced the least growth, it remains out in front in regard to its concentration of hotspots. At 15 percent, New York City is well clear of London where 6 percent of wireless access points were found to be hotspots. In Paris, a relatively small number of wireless hotspots were detected in comparison to the other cities, yet hotspots represent 11 percent of all the access points we located in the French capital.

Near these hotspots are significant numbers of unprotected business networks that are clearly not hotspots but still offer access to those who might accidentally or intentionally connect to them. This has added a new and worrying dimension to the wireless security problem; the massive growth of hotspots for mobile users means that there are large numbers of mobile users who are frequently seeking connections throughout their travels. This introduces an even greater threat to regular business users of wireless networks who are operating them with little or no security. Fueled by the availability and profusion of hotspots, mobile users expect to find wireless networks – and know how to connect to them.

Security Levels

Surprisingly, while one city made significant gains in the security of business wireless networks, in two of the cities security levels remained nearly flat. 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.

London leads in the adoption of security measures, with 19 percent of corporate wireless access points unsecured and open to misuse, as compared to 26 percent in the previous year. Paris made a very slight improvement, with 20 percent of business access points unsecured, down from 22 percent last year. Wireless security remained almost flat in New York City, with 24 percent of business wireless access points unsecured, down just slightly from 25 percent in 2006.

These numbers tell us that between one-quarter and one-fifth of business wireless access points in three of the world's largest business centers are wide open. This statistic seems at odds with the increase in awareness – among both companies and consumers – of the scope and severity of security threats.

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 unauthorized access include the theft of sensitive and confidential corporate and customer data, and the instigation of further security breaches such as undercover denial of service attacks and identity theft.

Rogue Hotspots

As highlighted in previous surveys, a further potential security issue is the presence of rogue hotspots in the major financial districts of the world. These fake hotspots – designed to look like the real thing – are created to attract connections and capture important security information from unsuspecting users. It is impossible to know exactly how many rogue hotspots are in existence as they are transitory in nature.

Summary

In summary, London leads the way – both in the pervasiveness of wireless access and in the implementation of security measures to protect the enterprises and consumers who use that access. However, all three cities have much progress to make as the rise of wireless network use continues to outpace the adoption of wireless security measures.

Phil Cracknell, FBCS, CISSP, MIRM
President, Information Systems Security Association, UK

II. Key Findings & Results

The wireless survey of New York City revealed another year of substantial growth in wireless network systems. In 2006 we identified 4280 individual access points along the route of the survey; a year later we found 6371 access points on the same route – an increase of 49 percent, following a 20 percent increase the previous year.

This year, New York City was – for the first time – surpassed by London, which made a huge leap in number of access points to 7130, a 160 percent year-over-year increase.

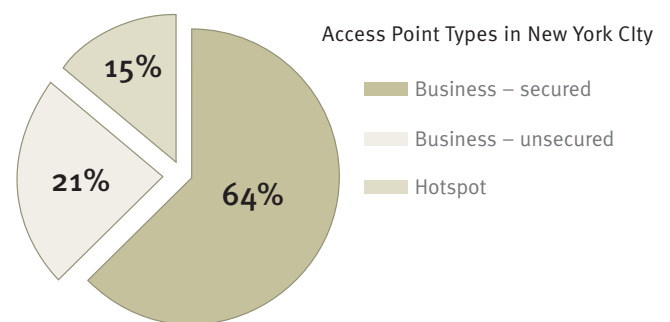
New York City once again saw more growth than Paris, which experienced a 44 percent increase in number of access points.

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
- Hotspot – paid, public access

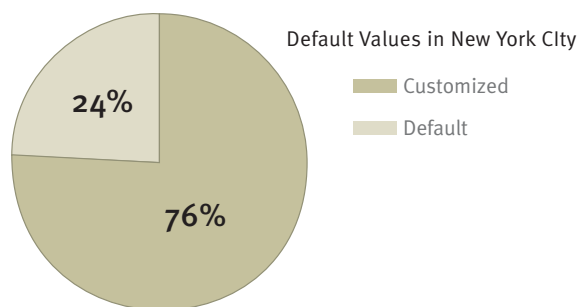
Access Point Types



Security Levels

Surprisingly, security levels in New York City remained nearly flat over the last year. In 2007, we found that 24 percent of wireless access points were unsecured and open to misuse, down just slightly from 25 percent in 2006. New York City trailed London and Paris, at 19 percent and 20 percent respectively.

Default Values



Of the 6371 access points discovered in New York, 1501 – 24 percent – were using default network settings, down slightly from 28 percent the previous year.

One example of how an SSID (Service Set Identifier) default value is noted: if a network administrator has not configured an optional name for the company's network, the manufacturer's software will usually default to the name of the manufacturer and MAC address or other information, which might be valuable to a hacker in finding ways to penetrate the network. Another example of a default value could be the default operation channel (which can cause performance problems and conflicts), beacon rates and other settings which come with that particular vendor's hardware.

One default value which was not tested for was the use of default passwords to control access points. If other settings are left default, this is something that may also be found to be unchanged during installation.

Hotspots

Wireless hotspots are growing in prevalence across all three cities. In the latest survey we detected 987 on the route around New York, compared to last year's figure of 847 – an increase of 17 percent. Hotspots account for 15 percent of all access points in the city, down from 20 percent the previous year. New York's hotspot growth was outpaced by both London and Paris – which saw 27 percent and 37 percent increases, respectively.

Hotspots – well-known to city dwellers and travelers alike – are access points provided for visitors to an establishment. They have cropped in many coffee shops, hotels, and airports over the last few years.

A hotspot will typically broadcast its presence by advertising a recognizable SSID, which is often the name of the establishment in which the hotspot is located, or a commonly known provider. 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 WEP is not in use as it would require the client system to be a party to the encryption key.

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 home page will appear. This home page 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 home page and registered or logged in.

- 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. 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 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.

III. Summary

The rapid rise in the number of public hotspots and corporate wireless access points has permanently altered how people in European and U.S. cities connect to networks.

As we evolve toward a "wireless everywhere" world we are witnessing enormous leaps in wireless connectivity, as underlined by London's explosive growth in access points over the course of the last year.

Continued education for both businesses and consumers regarding security considerations, best practices, and the potential for corporate disruption, is essential. The dangers are obvious: unauthorized users can and do access unprotected or poorly protected WLANs. In addition, consumers also risk compromising their own wireless devices should they unwittingly connect to a virus-infected network, for example.

What these users do once they are connected is entirely up to them. The potential effects that a data security breach can have on an organization may include:

- Direct or indirect financial loss
- Loss of customer confidence
- Damage to brand and reputation
- Messy litigation or even government regulatory action
- Loss of competitive advantage

The estimated proliferation of rogue hotspots and their potential to facilitate identity theft should also be a concern. With fraudsters continually looking for new ways to collect personal information, it is possible that rogue hotspots will be deployed precisely for this purpose. This would be a worrying development for businesses and consumers alike.

A look back at the early years of the Internet should remind us all that addressing security issues from the start can spare us much pain and money down the road. RSA's recommended best practices for wireless security follow in Appendix A.

Appendix A – Recommended Wireless LAN 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 Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with the computer security team and where possible enabled for access using MAC address control on the access points
- Lost or stolen cards should be reported immediately
- All wireless LAN access must use corporate-approved vendor products and security configurations
- All computers with wireless LAN devices must utilize a corporate-approved Virtual Private Network (VPN) for communication across the wireless link. The VPN will authenticate users and encrypt all network traffic
- Wireless Access Points / Base Stations 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 Service Set Identifier (SSID) should be vague and defined by the security department
- Assess the benefits and technical challenges of disabling broadcasts of your SSID
- WEP may be used to identify users, but only together with a stronger authentication and/or VPN solution
- 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
- Consider VPNs as a means of securing your data rather than proprietary methods which are hardware specific. The rapid changes in hardware speeds, frequencies and interoperability issues may tie you into unsuitable access points for longer than you desire. The added benefit of a VPN is that it can also span your wired networks giving a ubiquitous, consistent level of protection
- Ensure all mobile users are educated in the use of public WLANs (Hotspots), 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 could be eavesdropped.

Appendix B – New York Survey Details

The wireless survey of New York was conducted as part of an ongoing study of major cities to identify wireless use and the security of such networks and businesses. This time we specifically attempted to identify hotspots as well as private business networks (secured or otherwise).

Route

The survey followed an identical route to the 2006 study, covering the Midtown and Downtown districts of New York City, with some coverage of areas Uptown.

The survey was conducted by bus, car, on foot and in horse-drawn carriage around the edges of Central Park; this latter leg of the journey yielded some significant access points around Central Park West.

The Downtown leg of the survey took us around Little Italy, SoHo, Chinatown, Greenwich Village, past the World Trade Center site, onto Broad Street, Wall Street, Liberty Street and then down towards Battery Park, and up through the East Village.

Centrally, we covered all streets from 14th Street – touching upon areas including the Rockefeller Center, Trump Towers, Madison Square Garden and The Empire State Building, all the way up to 58/59th Avenue, and the start of Central Park.

Uptown, we went through Harlem and as far up as 125th Street and briefly around the Cloisters.

In short, the entire area of Manhattan was covered including the Brooklyn, Manhattan, and Williamsburg Bridges.

Equipment

The survey was carried out using a laptop running a special version of Airtight Networks probe which is normally deployed to detect malicious corporate activity.

The device was built into a laptop rucksack and two omni-antennas were used to give even coverage of both sides of the street. We were able to detect 802.11a, b and g WiFi devices and a variety of security configurations.

When devices were detected the software once again identified the channel, SSID and other network information before disconnecting 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:

Service Set ID (SSID)

Channel (1-11)

WEP or other security method

Advanced encryption

Signal strength (for exact location purposes)

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

MAC Address

Hardware vendor

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

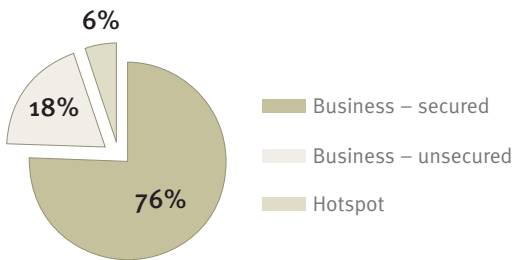
The laptop and software scanner again detected both broadcasting and non-broadcasting APs in the 802.11a, b and g frequencies.

Appendix C – Comparative Survey Results from London and Paris

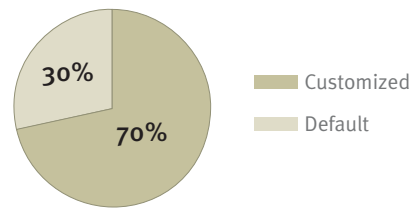
Access Point Types

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

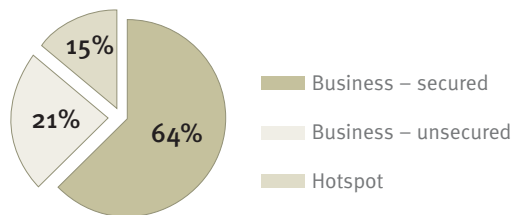
- Business – secured/private access
- Business – unsecured
- Hotspot – paid, public access



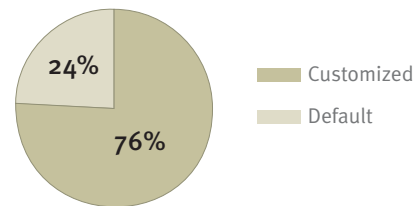
London – Access Point Types



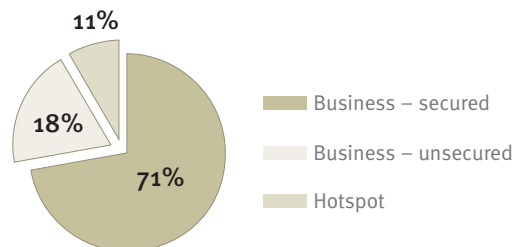
London – Default Values



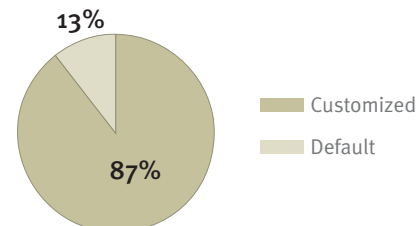
New York – Access Point Types



New York – Default Values



Paris – Access Point Types



Paris – Default Values

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 802.11x.

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. ©2006-2007 RSA Security Inc. All rights reserved.

WLANNY WP 0607