The Wireless Security Survey of London

Final Report Commissioned by RSA Security, Inc.

One year on from our first survey of wireless network (WLAN) security in the heart of London, we revisited the same locations to discover whether corporations have heeded the warnings and taken steps to protect their investments and the integrity of their IT infrastructures.
The results of this survey demonstrate two things: that while the use of wireless networks has accelerated dramatically in line with industry predictions, the level of unencrypted traffic — incredibly — has not decreased at all.

Some considerable time has passed since the inadequacies of wireless network security were first highlighted, yet network managers still appear to be leaving their wireless LANs wide open to potential hackers. As demonstrated 12 months ago, CEOs, CIOs and IT Managers must understand that any investments they have made in securing their infrastructure can be swiftly negated if the backdoor is left open through the introduction of wireless LANs.

A key finding is that the biggest growth area for wireless LANs is in the financial district, the City of London, where the number of systems discovered almost trebled from 48 in 2001 to 142 in 2002. Of these, only just over one third were using encryption to protect their data. There is no doubt that the benefits of WLAN technology have fuelled significant usage; however security seems to have been overlooked in a rush to implement wireless solutions. This situation needs immediate attention if serious breaches are to be avoided.

Tim Pickard
Strategic Marketing Director, EMEA
RSA Security Inc.
January 2003

RSA SECURITY®

The Wireless Security Survey of London – 2002

Table of Contents

Introduction

One year on from the original RSA survey which first raised the issue of Drive-by Hacking in the UK we can reveal a dramatic growth of Wireless networks in London.

UK-based companies have firmly embraced wireless technology, choosing to ignore or mitigate the risks from drive-by hacking and electronic eavesdropping in order to reap the massive benefits to their business through cost savings, mobility and flexibility.

Wireless audit technology has advanced as rapidly as WiFi itself and we are now able to detect and record client devices. The number of client systems with WiFi enabled was incredible. On the train, in the street and even in a rucksack on the bus wireless cards were enabled and offering direct access to the laptop in which they were installed! I am sure that many such devices were not even supposed to be enabled and would tend to blame factory defaults or more intelligent operating systems which see the hardware, load the drivers, configure the device and enable its use — all automatically.

There was little improvement in the use of WiFi's own security (WEP) since last year. I would actually expect to see the use of WEP, as is, to decrease in favor of third party, more secure VPNs. WEP has fundamental design flaws and can create a false sense of security.

Phil Cracknell, CISSP, M.INSTIS
Independent Security Specialist

I. Executive Summary

The contents of this report are intended for security managers, infrastructure and business management, and anyone responsible for risk management, data protection and business continuity.

Substantially more access points were discovered in this survey than one year previously. As detailed, a huge volume of client systems were detected and most were associated with one of the access points.

On analysis of the results it was found that more companies now have three or four access points spanning one site which clearly indicates a greater reliance on WiFi as their staff roam the building while still connected.

There was also a more varied use of WiFi in the City. During the survey many devices were found to be operating in traditional access mode but also a growing number of wireless devices were being used for peer-to-peer networking and even to bridge a wired network from building to building.

The greatest danger in the City right now is the device operating as a client (i.e. a laptop with a wireless card). These devices are often unprotected and many have shared drives configured that are instantly accessible to the remote wireless device. It is common to fail to disable the device before travelling and so some devices were even detected on trains.

The dynamic wireless network now seems to be offering IP addresses via DHCP for speed and convenience. We would argue that if a passing wireless client is 'offered' an IP address by your network then you would find it hard to subsequently challenge the rights of that individual to access your network; after all, you invited them!

Terms

The following definitions will be helpful in understanding WLAN technology and the findings in this report:

Wireless Network SSID. The Service Set Identifier (SSID) is an identifier attached to the packets sent over a wireless network. This identifier functions as a "password" for joining a particular wireless network. All clients and access points within the same wireless network must use the same SSID, or their packets will be ignored. Much like a password, the network's administrator usually chooses the SSID to be used. SSIDs may therefore be apparently meaningless strings, or, quite commonly, instantly recognizable strings such as a company name.

Wireless Network Name. The definition is obvious but it is important to understand that the name given the network is the one transmitted with the SSID. Most system administrators give the network the name of the company inadvertently providing targeting information to potential hackers. The network administrator may also configure an optional network name. If one is not assigned, 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.

Wireless Signals. To determine the location (and owner) of a WLAN, a hacker using a WiFi PSM network card, wireless driver and some freeware (listed below) can roam until he identifies a random signal and by analyzing its strength, alter his geographic coordinates until he finds the source.

Physical card address screening was not used widely and yet serves as a robust screen to unwanted access. As such a mechanism requires the MAC addresses of all valid cards to be entered in an administrator screen it is suggested that this is too much of a management overhead for most wireless administrators.

Overall, other than the huge volume of new networks, the expansion of existing networks from development to production quality it seems that the most common mistake of identifying your organization or address when naming the wireless networks is still widespread. Almost one third of network names identified the organization.

II. Background to Wireless Networks

The IEEE 802.11b specification is a link layer (layer 2 — OSI model) protocol. 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.

802.11a and 802.11g should see a variety of improvements including better security, less congested frequency use and faster speeds.

The fundamental operation of wireless networks introduces a new risk over a wired network, in that traditionally a network manager can physically control access to the network, 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.

III. Survey Details

The survey was conducted to revisit the October 2001 RSA survey, visit the same districts of London and record the amount of wireless network traffic from the pavement, road and public areas.

When networks were detected the handheld scanner identified the channel, SSID and other network information before disconnecting from that source. The type of data on these networks was not examined.

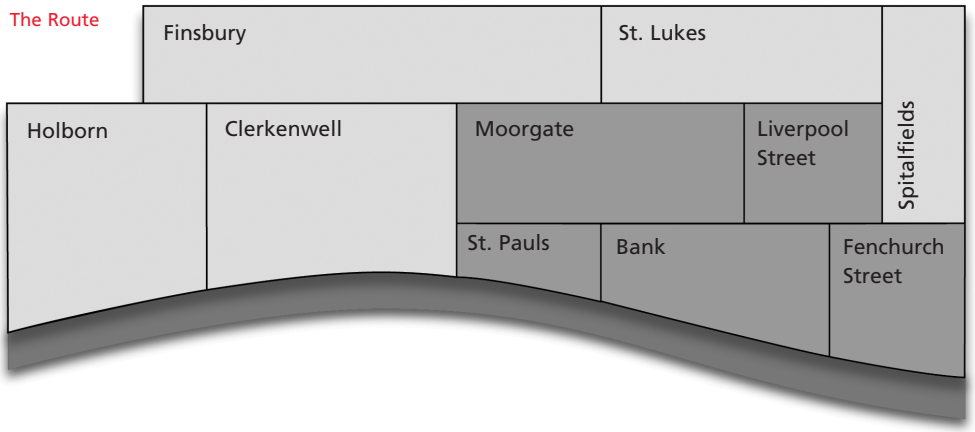
The information gathered from each brief connection enabled offline analysis of the networks to identify any of the following where available:

- Server Set ID (SSID)
- Channel (1-11)
- Signal strength (For exact location purposes)
- Mode of operation (Ad-hoc, station, access point, infrastructure)
- MAC Address
- Hardware vendor

The survey was intended to demonstrate the increase in the use of wireless technology in the City of London. No corporate data was extracted and the names of organizations that were identified in any of the information above have been protected.

The handheld scanner detected both broadcasting and non-broadcasting APs, which identifies far more than previous scans have been able to. Preventing an AP from broadcasting its SSID is seen as a security measure against drive-by hacking.

The Route



The survey followed the seven districts of London previously covered in October 2001.

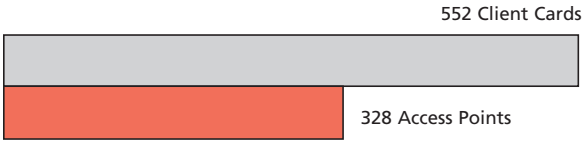
Holborn
Clerkenwell
City (Moorgate, St. Paul's, Bank, Fenchurch & Liverpool Streets)
St Luke's
Finsbury
Spitalfields
Canary Wharf (not pictured)

IV. Results

Our scanner detected 328 access points in the 2002 Wireless Security Survey of London. These devices were operating as wireless network hubs allowing connection from client devices. 552 client wireless devices were found and many were operating with the access points.

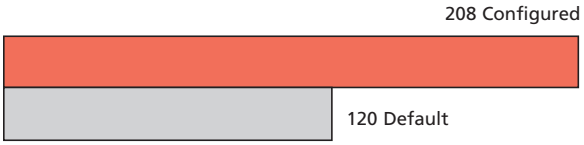
264 unique networks were detected. Some of the larger installations had as many as 11 access points in one site for complete coverage.

Ratio of Access Points to Client Cards



Of the 328 access points discovered only just over a third were using WiFi's own encryption (WEP). 120 devices had default values, and would be high on the target list for an attacker as many of these were also the systems not using WEP. Of the total, 100 devices identified the organization to which they belonged by name or location.

Ratio of Configured to Default Access Points



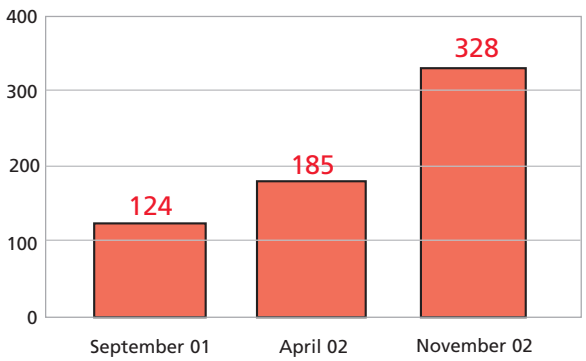
V. Wireless Growth in the City

Below is an illustration showing the last three surveys. In September 2001 RSA conducted a survey in the City that showed 124 access points. In April 2002 Phil Cracknell, on behalf of the Institute of Information Security (INSTIS) carried out a six monthly review that found 185 access points. The most recent result of 328 access points is an incredible increase and starts to show a trend towards wireless networking in the City.

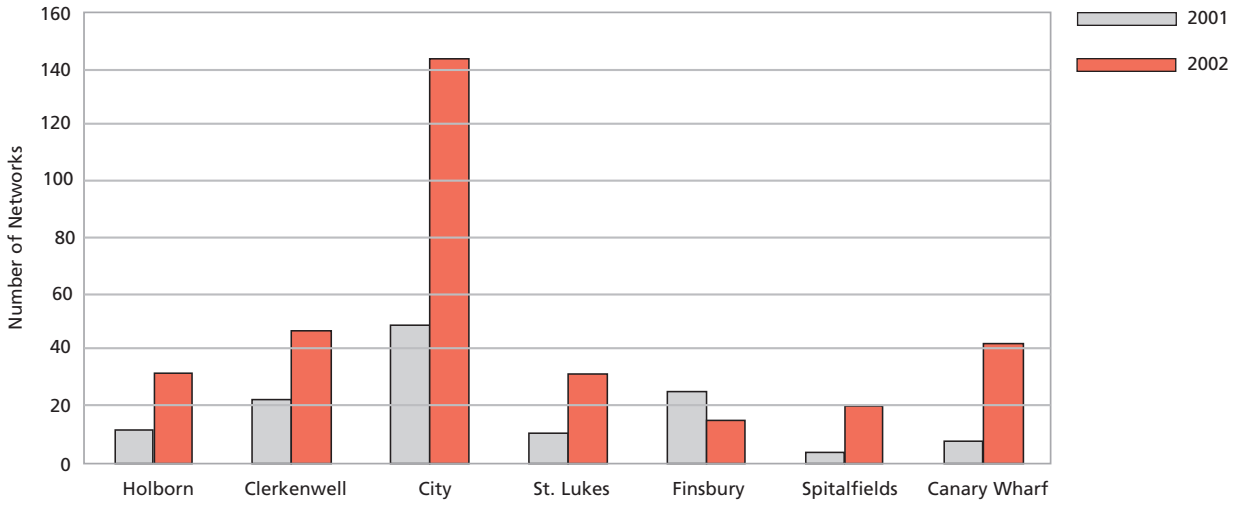
The breakdown of networks found in each location is as follows. The number of networks detected in the October 2001 survey is included in brackets.

Holborn — 33 (12)
Clerkenwell — 46 (21)
City — 142 (48)
St Luke's — 31 (9)
Finsbury — 16 (26)
Spitalfields — 19 (2)
Canary Wharf — 41 (6)

Access Point Growth



Growth in Wireless Networks 2001 – 2002



VI. Wireless Security

In general one in three wireless network access points is not secure, either because it has default configuration, no WEP or because it identifies the organization. Many devices had all three faults!

The 552 client devices represented a laptop, PDA or desktop computer with a wireless card configured to connect to an access point or another client device (peer-to-peer).

VII. Summary

The 2002 Wireless Security Survey of London has confirmed many suspicions and actually reinforced many predictions from the industry.

Despite growing concerns about wireless security the benefits outweigh the risk to business, or so it seems.

There is still a great uncertainty about just how much wireless network hacking takes place, what the networks are used (or misused) for and who the perpetrators are.

The survey has shown that the City has embraced wireless technology but there is still some way to go in the industry before transmission standards, security and best practice is fully agreed. In such circumstances organizations should enter into the wireless market with a guarded approach.

VIII. 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.
- 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.
- It is also recommended that two-factor authentication methods should be used in conjunction with any VPN.
- 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.
- WEP may be used to identify users, but only together with a 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.

About RSA Security

With more than 9,000 customers around the globe, RSA Security (NASDAQ: RSAS) is recognized as the strategic e-security partner to many of the largest and most successful companies leveraging the Internet to grow their businesses and improve their bottom line.

RSA Security's comprehensive portfolio of e-security solutions — including authentication, Web access management and developer toolkits — helps organizations fully realize revenue opportunities while helping protect critical information against unauthorized access and other forms of malicious intent.

RSA Security's strong reputation is built on its history of innovation and leadership, award-winning solutions and long-standing relationships with more than 1,000 technology partners.

For more information on RSA Security, please visit www.rsasecurity.com.

About Z/Yen Limited

Z/Yen improves performance by enabling organizations to make better choices. We apply our Risk/Reward approach to people, strategy, systems and markets. Z/Yen believes that by intelligently managing risks, the activities of an organization can be expanded and thus performance increased.

Typical projects:

- Governance review and process improvement.
- Establishing a risk-based project management team for a major government agency.
- Board level mentoring to improve decision-making.
- Customer research insights that improve sales & marketing productivity.
- Systems/process analysis that enables competitive cost improvement.
- Performance measurement providing evidence of organizational value.
- Providing experts to deliver time-critical projects.

For more information on Z/Yen Limited, please visit www.zyen.com.

RSA Security Inc.
www.rsasecurity.com

RSA Security Ireland Limited
www.rsasecurity.ie

CLWS WP 0203