Auditing the Data Confidentiality of Wireless Local Area Networks

Peter Clutterbuck, Terry Rowlands and Owen Seamons
Business School, University of Queensland, Brisbane, Australia
p.clutterbuck@business.uq.edu.au
t.rowlands@business.uq.edu.au
o.seamons@business.uq.edu.au

Abstract: Wireless Local Area Networks (WLANs) provide many significant advantages to the contemporary business enterprise. WLANs also provide considerable security challenges for network administrators and users. Data confidentiality (ie, unauthorised access to data) breaches are the major security vulnerability within WLANs. To date, the major IT security standards from the International Standards Organisation (the ISO/IEC 17799) and the National Institute of Standards and Technology (the NIST Special Publication or 'SP' suite) have only a superficial coverage of WLAN security controls and compliance certification strategies. The clear responsibility for WLAN managers is to provide network users with best practice security strategies to mitigate the real risk of unauthorised data access. The clear responsibility for IT auditors is to ensure that best practice security practices are in place and that operational compliance is consistently achieved. This paper describes a newly researched software auditing artefact for the evaluation of the data confidentiality levels of WLAN transmissions – and therefore by extension for the evaluation of existing security controls to mitigate the risk of WLAN confidentiality breaches. The paper describes how the software auditing artefact has been evolved via a design science research methodology, and pivots upon the real time passive sampling of data packets as they are transmitted between mobile users and mobile transmission access points. The paper describes how the software auditing artefact uses these sampled data packets to produce a very detailed evaluation of the levels of data confidentiality in effect across the WLAN. This detailed evaluation includes specific identification (for network managers) of the types of software services operating across the WLAN that are not supported with the appropriate data confidentiality controls. The paper concludes by presenting an analysis of the results achieved during beta testing of the auditing artefact within a university production WLAN environment, together with a brief description of WLAN best practice security.

Keywords: Security, WLAN, confidentiality, auditing, 802.11.

1. Introduction

The use of computing and telecommunication technologies has revolutionised the design of business practices over the past two decades. Amongst these computing and telecommunication technologies wireless local area networks (WLANs) are increasingly providing significant advantages to the contemporary enterprise. The WLAN concept allows any data entry/retrieval device to be moved to any location within a mobile cell (defined as that geographical area in which the strength of the mobile signal ensures its easy recognition and consistent integrity). WLANs facilitate ready deployment, simplification of office infrastructure requirements, and adoption of mobile and nomadic work patterns. WLANs enable roaming employees to have access to applications and information on demand. WLANs also directly encourage the design of more streamlined business processes. The sales function can unfold at any location throughout the store via wireless connections between multiple point-of-sales machines linking with centralised order-processing servers (Dennis 2002). The sales function is also evolving via wireless networks to focus on the nomadic customer (Sabat 2002). The stocktaking function becomes more efficient when the relevant personnel are mobilised within warehouses and supermarkets and operate bar-coding devices to update centralised inventory lists via wireless connections. Many more examples of such efficiencies provided by WLANs are outlined in (Sabat 2002). All of these business process redesigns allow a more flexible customer-staff relationship and provide the basis for the rapidly emerging business paradigm of M-Commerce, defined as "any transaction with a monetary value either direct or indirect that is conducted over a wireless telecommunications network" (Sabat 2002). The business drivers outlined above have caused WLANs to become more pervasive (Tsalgatidou 2001). The Information Systems Audit and Control Association (ISACA) has stated that the use of Personal Digital Assistants (PDAs) is widespread and is likely to increase. Garner Dataquest has recorded that worldwide PDA shipments were 11.4 billion units in 2004. These demand trends in turn have caused the cost of WLAN adoption to drop by significant margins. Indeed costs have reached such a level where many Small to Medium Enterprises (SMEs) are incorporating WLANs into their business strategies.

Confidentiality is an essential network security quality of service parameter. Confidentiality is defined in ISO/IEC 27001 as "*the property that*

ISSN 1566-6379

Reference this paper as:
Clutterbuck P, Rowlands T and Seamons O (2007) "Auditing the Data Confidentiality of Wireless Local Area Networks" *The Electronic Journal Information Systems Evaluation* Volume 10 Issue 1, pp 45 - 56, available online at www.ejise.com

information is not made available or disclosed to unauthorised individuals, entities, or processes." ISO/IEC 27001 and (Garfinkel 2002) state that confidentiality must be assured (where relevant) for all network transmissions. WLANs pose a confidentiality vulnerability not usually encountered with guided (ie, wired) networks. This vulnerability occurs because wireless signal spread is physically dictated by the cell concept and not necessarily by the architectural design of business accommodation or the availability of wired access points. Consequently a wireless signal can 'leak' past the physical perimeter of a business enterprise and into public airway space. This same signal leakage may also occur within the sizable public contact areas provided by many businesses within their infrastructure perimeter. This scenario offers significant opportunity for the unauthorised and non-detectable introduction of wireless devices within the wireless cell space of an enterprise. These wireless devices are then the launching pad for confidentiality attacks on the business network. These attacks, known as "*Drive by Hacking*" are well described in (Hinde 2001).

The motivation for the research described in this paper is the design and testing of an innovative software auditing artefact that evaluates the data confidentiality levels of WLAN transmissions – and therefore by extension mitigates the risk of WLAN confidentiality breaches. The paper describes how the software auditing artefact has been prototyped via a design science research methodology (Hevner 2004), and operationally pivots upon the real time passive sampling of data packets as they are transmitted between mobile users and mobile transmission access points. The software auditing artefact uses these sampled data packets to produce a very detailed evaluation of the levels of data confidentiality in effect across the WLAN. This detailed evaluation includes specific identification (for network managers) of the types of software services operating across the WLAN that are not supported with the appropriate data confidentiality controls. This paper unfolds in the following format. Section two discusses WLAN protocol design and describes why this design proves to be problematic in terms of data confidentiality. Section three discusses the design science research methodology and the conceptual design of the software auditing artefact produced via the methodology. Section four presents an analysis of the results achieved during beta testing of the auditing artefact within a university production WLAN environment. Section five describes best practice security solutions for a WLAN environment. Section six concludes the paper.

2. WLAN overview

The major wireless standards are published by the *Institute of Electrical and Electronics Engineers* (IEEE). IEEE802.11 (WLAN) has become more popular than other protocols (eg the European Telecommunications Standards Institute's High Performance Radio Local Area Network) defined within an overall WLAN context (Frankel 2006). The IEEE 802 wireless suite also defines a range of protocols for other wireless network topologies. The Wireless Personal Area Networks (WPAN) topology describes small-scale wireless networks that require little or no infrastructure (Sabat 2002). A WPAN is typically used by a few devices in a single room (eg, print service, keyboard or mouse connectivity). WPAN standards include 802.15.1 (Bluetooth), 802.15.3a (Ultrawideband) and 802.15.4 (ZigBee). The Wireless Metropolitan Area Network (WMAN) topology provides connectivity to users located in multiple facilities that are generally within a few miles of each other. IEEE 802.16 (better known as WiMAX) is a WMAN standard. IEEE 802.11 is well suited for most intra-office wireless networking scenarios and has become dominant within the WLAN market (Gast 2005). IEEE 802.11 is the WLAN protocol under analysis in this research. This section will firstly present an overview of 802.11, and then analyse the 802.11 security focus.

2.1 IEEE 802.11 overview

The initial IEEE 802.11 standard (also know as Wireless Fidelity or Wi-Fi) was published in 1997. That standard has since been updated in 1999 and 2003. The current standard has been accepted by the *American National Standards Institute* (ANSI) and has also been adopted by the *International Organisation for Standardisation* (ISO) as ISO/IEC 8802-11:2003. The IEEE 802.11 standard uses the Media Access Control (MAC) protocol *Carrier Sense Multiple Access with Collision Avoidance*. An overview 802.11 bandwidths, frequency spectrums, and release timetables is shown in Table 1.

Table 1: Summary of IEEE 802.11 WLAN technologies

.IEEE Standard	Maximum Data Rate	Typical Range	Frequency Band	Comments
802.11	2 Mbps	50-100 metres	2.4 GHz	
802.11a	54 Mbps	50-100 metres	5 GHz	Not compatible with 802.11b; more expensive to implement than 802.11b
802.11b	11 Mbps	50-100 metres	2.4 GHz	Equipment based on 802.11b has been the dominant technology
802.11g	54 Mbps	50-100 metres	2.4 or 5 GHz	Backward compatible with 802.11b

Table 1 does not include all current and pending 802.11 amendments. For example, in November 2005, IEEE ratified IEEE 802.11e, which provides quality of service enhancements to IEEE 802.11 that improve the delivery of multimedia content. The IEEE 802.11n project is also currently considering four proposals for IEEE 802.11 enhancements that will enable data throughput of at least 100 Mbps.

2.2 802.11 security

The IEEE 802.11 variants listed in Table 1 all include a security architecture known as Wired Equivalent Privacy (WEP). The fundamental goal of WEP was to provide a level of security comparable to that of wired LANs. The design of WEP assumed the major categories of threats facing the WLAN paradigm were identical to those posed to guided (ie, wired) LAN networks. Consequently the design of WEP focused upon providing authentication, confidentiality, and integrity controls for all transmissions between a wireless user and a WLAN access point. It should be noted that the designers of the original 802.11 standard only ever intended WEP to make it difficult to break into a WLAN – the designers did not intend WEP to provide military levels of access. Section 8.2.2 of the 1999 IEEE 802.11 standard states the following in relation to 802.11 WEP design objectives (quoted verbatim):

- It is reasonably strong: The security afforded by the algorithm relies on the difficulty of discovering the secret key through a brute-force attack. This in turn is related to the length of the secret key and the frequency of changing the keys. WEP allows for the changing of the key (K) and frequent changing of the Initialisation Vector (IV).
- It is self synchronising: WEP is self-synchronising for each message. This property is critical for a data-link-level encryption algorithm, where “*best effort*” delivery is assumed and packet loss rates may be high.
- It is efficient: The WEP algorithm is efficient and may be implemented in either hardware or software.
- It may be exportable: Every effort has been made to design the WEP system operation so as to maximise the chances of approval, by the U.S. Department of Commerce, of export from the U.S. of products containing a WEP implementation. However, due to the legal and political climate toward cryptography at the time of publication, no guarantee can be made that any specific IEEE 802.11 implementations that use WEP will be exportable from the USA.
- It is optional: The implementation and use of WEP is an IEEE 802.11 option.

In retrospect, the designers’ goal of a “*reasonable*” level of security was a mistake (it should be noted that the work “*reasonable*” was dropped in the marketing campaign for the initial promotion of IEEE 802.11 – and WEP was simply described as “*secure*”). The contemporary security community promotes only two types of security: *strong security* and *no security* (sometimes described as *open security*). The WEP design proved to be inadequate for one main reason: the relative ease of intercepting WLAN transmissions (and also inserting spoofed transmissions into the transmission stream). This relative ease of interception is caused by the omni-directional transmission propagation of a WLAN as contrasted with the constrained/guided transmission propagation of a traditional LAN. This means that an attacker in a WLAN simply needs to be within range of the WLAN infrastructure (ie, a wireless sender or receiver), whilst in the wired LAN an attacker would need to gain physical access to the LAN (ie, physical access to a wired connection point). The security consequence is clear: a WLAN is more vulnerable to confidentiality breaches (eg, eavesdropping) than a traditional guided/wired LAN.

WEP uses the well regarded RC4 symmetric encryption algorithm to mitigate the confidentiality risk inherent in WLAN transmissions. The WEP standard specifies that the symmetric key used within WEP-implemented RC4 should include a 24-bit value known as an initialisation vector (IV). It is this value that has caused much of the security concern that has since been documented about WEP. As early as 2001 (Fluhrer 2001) showed via experiment that an eavesdropper could deduce the base RC4 key by obtaining a relatively small number of packets within a WLAN communication session. Shortly after (Stubblefield 2002) reported that the experimental approach of (Fluhrer 2001) had been used to mount a successful attack against a production WLAN system. Many more successful WEP attacks have been since described (Airmagnet 2004). (Cam-Winget 2003) summarised the security community's assessment of WEP by stating: "*The security goal of WEP is data confidentiality equivalent to that of a wired LAN. WEP falls short of this objective…*". The vulnerabilities within WEP are further exposed by the emergence of a suite of open source WEP-cracking software tools (Ossman 2004).

The IEEE response to the WEP vulnerabilities was the formation of the 802.11i (Security) group, a body charged with the total overhaul of security within 802.11. The 802.11i group's security review, however, would prove to be a long term project over several years. As an interim security measure, a non-profit industry consortium of WLAN equipment and software vendors (the Wi-Fi Alliance) began work on a more robust WLAN security specification in 2002. In October 2002 the Wi-Fi Alliance released the first specification of the interim WLAN security specification: Wi-Fi Protected Access (WPA). WPA proved to be much stronger than WEP, but did ultimately exhibit some vulnerabilities in the areas of authentication and key exchange (Moskowitz 2003).

In June 2004 the IEEE finalised the 802.11i standard – specifying security components that work in conjunction with all Table 1 standards. The IEEE 802.111i standard includes many security enhancements that leverage existing mature and proven security protocols. The 802.11i standard introduces the concept of a Robust Security Network (RSN), which is defined as a communication association/session between two WLAN entities that fully implement 802.11i. An RSN provides verifiably strong security in the areas of confidentiality, integrity, availability, and access control. The 802.11i standard takes a two-track approach to addressing the security weaknesses that had existed within WEP. Its major components are two new link-layer encryption protocols. The first, the Temporal Key Integrity Protocol (TKIP) was designed to bolster security to the greatest extent possible on pre-802.11i hardware. The second, Counter Mode with CBC-MAC Protocol (CCMP) is a new encryption protocol designed from the ground up to offer the greatest level of security. The 802.11i standard is industry-accepted as strong security (Gast 2005). In conjunction with the ratification of 802.11i, the Wi-Fi Alliance specified WPA2 in September 2004 to completely comply with the IEEE 802.11 standard as amended by IEEE 802.11i. Official support for WPA2 in Microsoft Windows XP was rolled out on 1st May 2005 (some driver upgrades for network cards may be required). As from March 13, 2006, WPA2 certification is mandatory for all new devices wishing to be Wi-Fi certified.

3. Research experiment overview

The motivation for the research experiment described in this paper is the design and testing of a software auditing artefact that evaluates the data confidentiality levels of WLAN transmissions. This section will firstly discuss the design science framework that has been adopted as the research methodology for this experiment. The section will then describe the logical design and network positioning of the software audit artefact that was prototyped during the experiment.

3.1 Research methodology

Design science is one of the two paradigms (the other being behavioural science) that characterise much of the research in the Information Systems discipline (Hevner 2004). In the design science paradigm, knowledge and understanding of a problem domain and its solution are achieved in the building, application, and evaluation of a designed artefact. (Hevner 2004) differentiates design science from routine design by stating: "*The difference is in the nature of the problems and solutions. Routine design is the application of existing knowledge to organisational problems… On the other hand, design-science research addresses important unsolved problems in unique and innovative ways or solved problems in more effective or efficient ways. The key differentiator between routine design and design research is the clear identification of a contribution to the archival knowledge base of foundations and methodologies.*" In addition to the crucial differentiation between routine design and design research, (Hevner 2004) proposes the following heuristics to assist the research community in understanding the requirements for effective design science research:

- Design science research requires the creation of a purposeful artefact for a specified problem domain.
- The artefact is represented in a structured form that may vary from software, formal logic, and rigorous mathematics to informal natural language descriptions.
- The artefact must yield utility for the specified problem, and this utility must be evaluated. The artefact must be innovative – solving a heretofore unsolved problem or solving a known problem is a more effective way.
- The artefact must be rigorously defined, formally represented, coherent, and internally consistent.
- The design process should comprise a 'build-and-evaluate' loop that is typically iterated a number of times before the final artefact is generated.
- The research results must be communicated effectively.

Design science – and all heuristics outlined above – have been used to produce the audit software artefact described in the next section.

3.2 Audit software artefact logical design and network positioning

The audit software artefact produced within this research is designed to evaluate the data confidentiality levels of WLAN (802.11) transmissions. The network positioning of the artefact and its logical design is now discussed with reference to Figure 1.

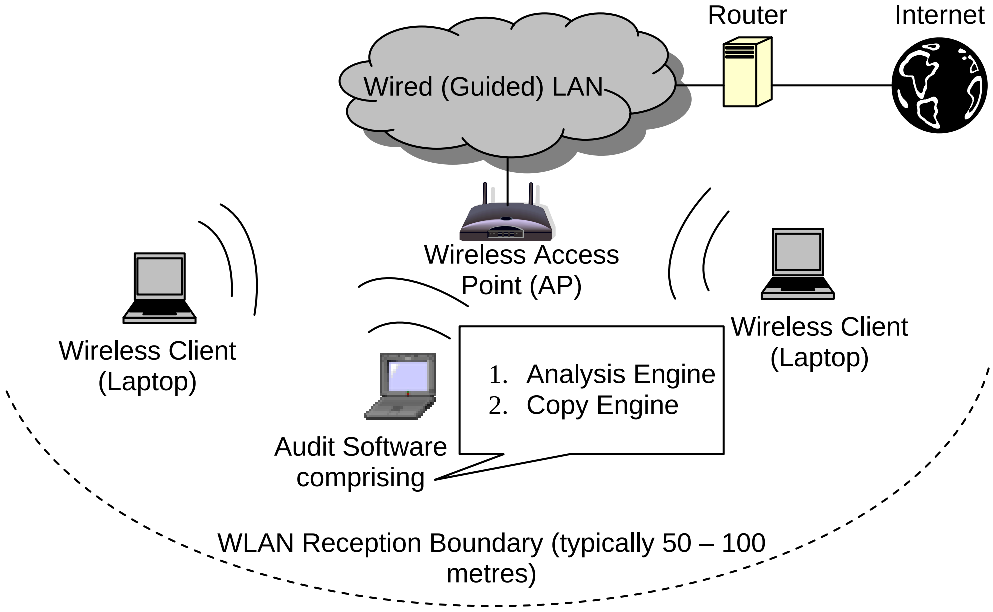

Figure 1: Audit software tool – Network positioning and logical architecture

Figure 1 shows a typical WLAN within an overall context of a wired (guided) LAN and Internet connectivity. The WLAN comprises one or more wireless access points (APs) which in turn wire back to the wired LAN backbone. The wired LAN backbone itself connects to the Internet via one or more routers. The WLAN reception boundary (from each AP) is within the range 50 – 100 metres. The only positioning requirement for the audit software is that its host (routinely a wireless enabled laptop) is within the reception boundary of a targeted AP. All mainstream operating systems (eg, Windows XP) routinely report WLAN signal strength to the nearest AP – this is a ready guide to the appropriate positioning of the audit tool.

The overall logical design of the audit tool comprises a low level Copy Engine and a higher level Analysis Engine. The Copy Engine places the wireless network card of the host into *RFMON* mode – thereby ensuring the network card captures all WLAN packets (i.e. *control*, *management*, and *data* packets) as they are transmitted between mobile users and mobile transmission access point. The Copy Engine is a Win32 Open Source port of *libpcap* – a widely used network programming Application Programming Interface (API) for capturing/imaging network packets (within wireless and wired networks). The Copy Engine may be configured to operate on a temporal sessional basis (ie, copying packets for a defined time period) or on a packet count sessional basis (ie, copying packets until a defined count is reached). The captured network packets are then saved to file storage for subsequent processing by the Analysis Engine. The Analysis Engine comprises three main categories of software: a *read* module (the input of data from file storage), a suite of *protocol analysers*, and a *logger* module (the output of data to file storage). The heart of the Analysis Engine is the suite of *protocol analysers* which process the captured network packets (imaged by the Copy Engine) with a logic and sequence which is now described with the assistance of Figure 2.

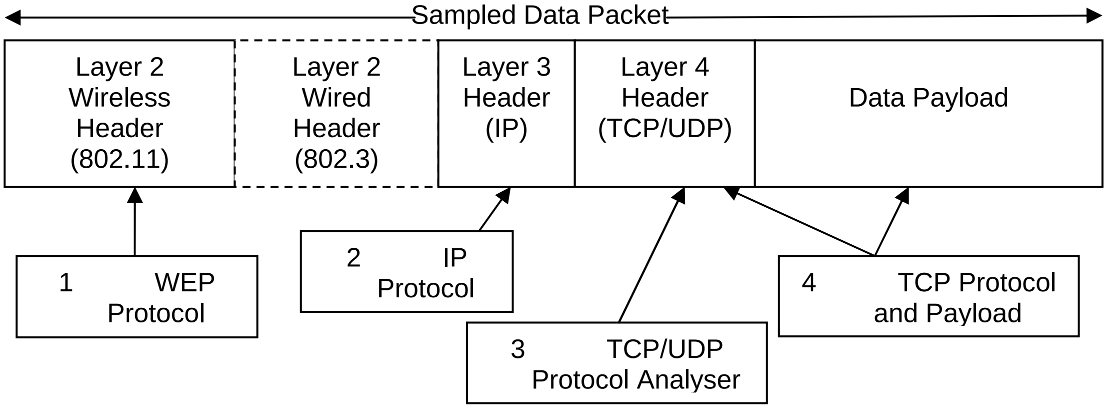
Sampled Data Packet
Layer 2 Wireless Header (802.11)
Layer 2 Wired Header (802.3)
Layer 3 Header (IP)
Layer 4 Header (TCP/UDP)
Data Payload
1 WEP Protocol
2 IP Protocol
3 TCP/UDP Protocol Analyser
4 TCP Protocol and Payload

Figure 2: Packet structure and protocol analysers

Figure 2 shows the structure of the generic data packet which is of most interest to the audit tool of this research. The audit tool views each packet as a bit stream comprising a series of headers and data payload. This structure follows the Open Systems Interconnection (OSI) model from the International Standards Organisation (ISO). The 802.3 Ethernet header is not always present – it only occurs where the wireless transmission forms a 'bridge' between wired (Ethernet) LANs (the audit tool however must allow for this possibility). The Analysis Engine uses each protocol analyser in two ways: (1) to test certain bit/byte values in the appropriate header; and (2) to search for the occurrence of certain *string* (ie, text) values within the data payload. A highly abstracted algorithmic description of the operation of the Analysis Engine and each *protocol analyser* is as follows:

INITIALISATION: Set all global count variables uses in statistically reporting this set of WLAN transmissions to 0. The global count variables are as follows:

TOTAL: The total number of packets analysed in this sample.

OPEN-HTTP-AUTHENTICATION: Indicates Basic Authentication (part of the HTTP protocol) has been used. Basic Authentication effectively transmits passwords in plain text and is therefore breaches confidentiality best practice.

OPEN-HTTP : Indicates HTTP is carrying plain text (or MIME encoded) payload.

WEAK: Indicates WEP encryption (ie, static keys) has been used.

STRONG-IPSEC : Indicates Encapsulating Security Payload (ESP) – the encryption protocol of IPSec (IP Security). The dominant protocol used within Virtual Private Networks (VPNs)

STRONG-KERBEROS: Major authentication protocol – all credentials are strongly encrypted.

STRONG-TLS/SSL: SSL (Secure Socket Layer) is the major security protocol – used heavily with HTTP. TLS (Transport Layer Security) is the IETF standardised version of SSL.

STRONG-S/MIME: S/MIME (Secure MIME) is the dominant protocol for email security. S/MIME uses a specifically defined mime type ("*pkcs7-mime*") to carry encrypted data.

OPEN-MS-FILE-TRANSFER: Indicates the presence of a Microsoft File System transfer via Server Message Block (SMB) over NetBios and TCP.

LOOP: For the next packet imaged by the Copy Engine do the following:

- Step 1: Is the packet a *data* frame (ie, not a WLAN *control* or *management* frame).

  NO - increment TOTAL by 1 and return to LOOP.

  YES – is the *protected* bit set?

  - o YES - increment WEAK-WEP and TOTAL counts by 1.

Discard the packet and return to LOOP.

- NO - continue to next step.

- Step 2a: Does the packet contain an IP header? NO, increment the TOTAL global count by 1. Discard the packet and return to LOOP (the audit is not interested in non-IP protocol packets – these cannot carry user data (eg, protocols such as ICMP, IGMP, ARP). YES – continue to next step.
- Step 2b: Does the IP header show the *protocol* field is set to IPSec encryption? That is, *protocol* field is set to 50 indicating Encapsulating Security Payload (ESP)? YES, increment STRONG-IPSec and TOTAL by 1. Discard the packet and return to LOOP. NO – continue to next step.
- Step 3: Does the TCP/UDP header show the *port* field contains any one of the following values:

  88 (Kerberos authentication port) – increment STRONG-Kerberos and TOTAL by one – return to LOOP.

  443 (HTTP over TLS/SSL) – increment STRONG-TLS/SSL and TOTAL by one – return to LOOP.

  NO – continue to next step.
- Step 4: Does the TCP header show the *port* field contains any of the following values:

  25 (SMTP email) – does the data payload contain the string "pkcs7-mime"?

  YES - increment STRONG-SMIME and TOTAL by one – return to LOOP.

  NO – increment OPEN-SENDING-EMAIL and TOTAL by one – return to LOOP.

  80 (HTTP) – does the (HTTP) data payload contain the string "Basic"?

  YES – increment OPEN-HTTP-AUTHENTICATION and TOTAL by one – return to LOOP.

  NO – increment OPEN-HTTP and TOTAL by one – return to LOOP.

  110 (POP email) – does the data payload contain the string "pkcs7-mime"?

  YES – increment STRONG-SMIME by one – return to LOOP.

  NO – increment OPEN-RECEIVING-EMAIL by one – return to LOOP.

  139 (NetBios) – does the data payload contain the string "Session Message"?

  YES – increment OPEN-MS-FILE-TRANSFER and TOTAL – return to LOOP.

  NO – (indicating a NetBios control message) – increment TOTAL and return to LOOP.

END LOOP – all packets have been analysed – call the *logger* module to output results.

The logger will output two audit reports that will be discussed in the next section.

4. Research evaluation

The overall evaluation of the software audit tool is made against two critical success factors: *innovation* and *utility*.

4.1 Innovation

The discussion of Section 3 presented innovation as a major criterion in classifying good design science research. (Hevner) outlined innovation as follows:

> *"design-science research addresses important unsolved problems in unique and innovative ways or solved problems in more effective or efficient ways. The key differentiator between routine design and design research is the clear identification of a contribution to the archival knowledge base of foundations and methodologies".*

The problem domain (confidentiality within WLANs) for this research is not new. Confidentiality is considered historically as a fundamental focus (with authentication and integrity) within IT security (Garfinkel 2002). Section 2 has also described the evolution over several years of WLAN confidentiality controls. The literature review conducted with this research, however, has verified that no existing confidentiality audit compliance controls for WLANs have been based on software-automated real time packet analysis. (The heavily used packet monitoring tools *Ethereal* and *tcpdump* are very much designed for network administrator manual analysis of packet characteristics). Indeed the increasing influential ISO/IEC 17799 (the Information Security policy control instrument) and ISO/IEC 27001 (the Information Security compliance certification instrument) still exhibit only very superficial coverage of WLAN security compliance. It is also noted that the real time packet analysis methodology of this research fits very well with IS security audit best practice as described in ISO/IEC 27001. That is, the audit methodology within this research is *non-intrusive* to network productivity/bandwidth, *resistant* to attack, and *active* in identifying control weaknesses (as contrasted with a *reactive* audit strategy whereby the absence of attacks – not the absence of weaknesses – is reported).

4.2 Utility

The utility of this research will be discussed in terms of the results returned via the beta testing of the audit tool within a university WLAN environment. The results from the audit tool comprise two main reports: (1) a statistical overview of confidentiality levels (Table 2); and (2) a detailed report of those transmissions where non-secured user data has been detected (Table 3).

Table 2: Statistical overview of WLAN confidentiality levels

Confidentiality Level (1, 2, or 3)		Total Packets	Comments				
1	Open system (no encryption)	93897	NetBios and SMB	HTTP Authentication	HTTP Plain	SMTP Email	POP/IMAP Email
			792	1897	20125	187	897
2	Weak Encryption	8345	Wired Equivalent Privacy (WEP)				
			8345				
3	Strong Encryption	57945	IPSec (Layer 3)	SSL/TLS (Layer 4)	Kerberos (Layer 7)	S/MIME (Layer 7)	
			40328	13762	3610	245	
Total Sample Size		160187					

Table 2 shows the overall results of beta testing the audit tool over twenty-four sampling sessions (each session of 30 minutes). A total of 160187 transmissions were sampled of which nearly 59% (93897) were open transmissions. Within the ‘open’ category there were 792 network file system transfers, and a total of 1084 email transfers. Perhaps of most concern were the 1897 passwords transferred unsecured via HTTP Authentication. The dominant form of strong encryption was via IPSec (most likely across a VPN).

Table 3: Detailed transmission report of non-secured user data

Date	Time	Vulnerability Type	Client Address (IP:Port)	Server Address (IP:Port)
3 May 06	12.56pm	HTTP Auth.	192.168.12.87:12389	192.168.2.3:80
3 May 06	12.59pm	SMTP	192.168.12.87:13567	192.168.2.4:25
3 May 06	1.43pm	SMTP	192.168.12.87:13568	192.168.2.4:25
3 May 06	1.51pm	POP	192.168.12.68:11324	192.168.2.5:110

Table 3 shows a small sample of four entries from the detailed transmission report of non-secured data. The report identifies the vulnerability type and also the client/server addresses (both IP and port). This detailed transmission report provides (at least) one main security purpose. The report identifies the server that is involved in creating the vulnerability. For example, entry 1 in Table 3 shows that a web server is still serving web pages under HTTP Authentication (ie, plain text exchange of passwords). This should not occur in a secure production environment – the preferred strategy is to always request authentication within an SSL session. It is also apparent that the detailed report provides very useful trend information.

5. Best practice

The previous sections of this paper have highlighted the chequered development of WLAN security. Whilst the most recent 802.11i/WPA2 security specification is considered strong (Gast 2005), it is also clear that the take-up of this specification requires the upgrading of network card hardware. Additionally, 802.11i is a complex specification and its full adoption within any network requires a system administrator to focus upon design issues at several levels (i.e., the data link layer, network layer, transport layer, and the application layer). This complexity is clearly a significant challenge to administrators and network owners. Within this context of relatively slow transitional progress to full 802.11i / WPA2 adoption, this section will now focus on best practice in the two main areas of WLAN deployment: (1) public wireless hotspots and (2) corporate networks (offering WLANs).

5.1 Public wireless hotspots

WLAN technology was developed about the same time that the Internet was expanding rapidly. It is not surprising that the two technologies have become closely linked. A pubic wireless hotspot is any location (e.g. airport, hotel, coffee shop) where any person with 802.11 hardware capability can legitimately connect to an access point (possibly for a paid fee) and receive broader network/Internet connectivity. Whilst this may prove to be a rich service delivery model in the near future (in principle it means that 802.11 could compete with the existing cellular phone infrastructure), the service model adoption has proven to be problematic for two main reasons (Edney 2004): the fax machine problem (i.e. a lack of user 'critical mass') and also the multiparty barrier problem (i.e. multiple stake holders combining to deliver the service and each/every stakeholder requiring healthy financial returns). Notwithstanding the service model growth challenges, it is important to appreciate the organisation of public wireless hotspots – and the consequential security implications. The logical organisation of public wireless hotspots is shown in Figure 3.

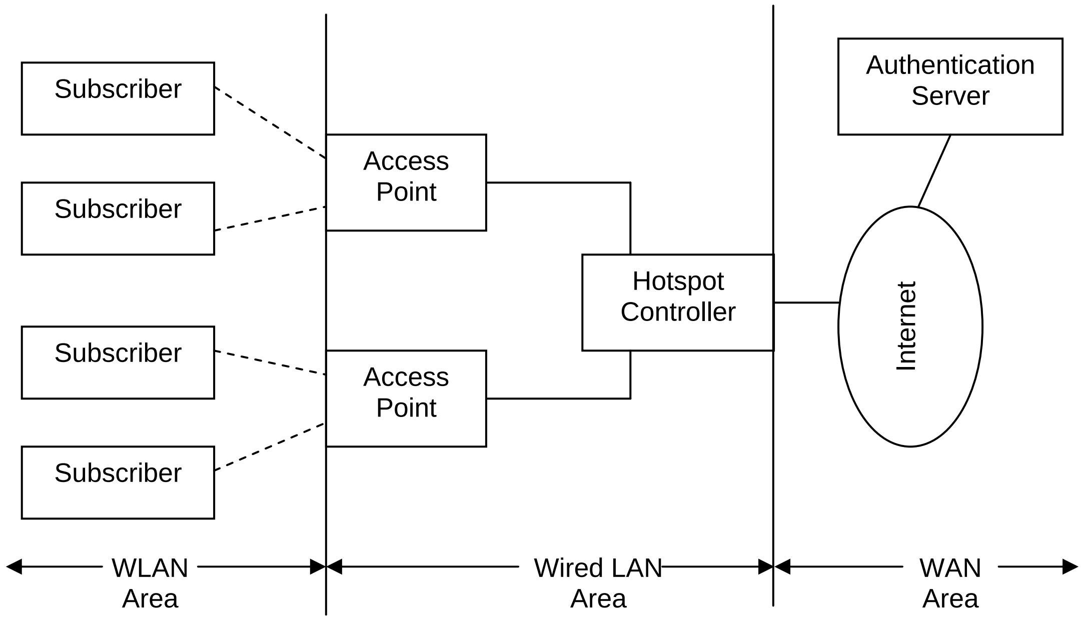

Figure 3: WLAN hot spot organisation

The subscribers and access point equipment shown in Figure 3 are standardised IEEE 802.11 equipment. This means that the hot spot organisation is based very much upon a "*no new hardware/software*" paradigm – hot spot users/subscribers are most reluctant to use any hotspot service that requires specialised hardware installation or software downloads (Edney 2004). Typically the subscribers and access points do not use any data link layer encryption (i.e. no WEP or RSN/WPA2 security). The hotspot controller of Figure 3 is the critical infrastructure in the overall WLAN hotspot operation. Typically the hotspot controller will perform the following functions:

- Coordinate user authentication
- Collection of account and billing information
- Collation of usage time and subscription time statistics
- Provision of local IP addresses
- Access to World Wide Web services
- Access to Domain Name Services

The authentication server of Figure 3 is typically accessed and facilitated via Web protocols. The most common approach to date is to require user login via a Web page. This approach requires the subscriber to connect/associate with an access point and start his/her Web browser. The first Web request initiated from the browser will be directed by the hotspot controller to the authentication server. The authentication server will complete the necessary login process – and from this point on (subject to certain subscription time settings) each user web request will then be routed to the appropriate destination service by the hotspot controller. The security implications for WLAN hotspot users centre very much upon the confidentiality risks posed by open security (i.e. no data link layer encryption) IEEE 802.11 deployment. The most direct confidentially risk is the passive viewing of private or commercially sensitive data during transmission across the (hotspot) WLAN – this has been evidenced within our audit tool beta testing described in Section 4 of this paper. A second important risk shown up within our research is the active attack against the shared file system of a WLAN user. Many popular operating systems (including Windows XP) provide default share directories. The operating system will '*advertise*' the shared directory via network broadcasts and this strategy provides a most popular method of sharing data for small businesses and home users. These network advertisements pose a serious security risk when a subscriber commences a WLAN hotspot session without firstly '*unsharing*' the shared data repository. The WLAN hotspot security risks outlined above are best mitigated at the present time via personal firewalls and virtual private networks (VPNs) – and in the future via the deployment of IEEE 802.11i. A personal firewall operating on a subscriber's computer can easily be configured to allow only TCP/IP packets to exit/enter the subscriber's computer. This protocol suite is required for Internet/Web use – but does not routinely facilitate LAN based computer-to-computer communication (which includes directory sharing). This should manage the risks posed via shared file systems. A VPN creates an encrypted tunnel through any network that is considered to be unsecured (i.e. the Internet). A typical use for a VPN tunnel is to connect an employee to their company's intranet. The VPN encrypts all TCP/IP communications whilst those communications are traversing the unsecured network(s). The VPN concept is most useful when a subscriber wishes to communicate with only one destination (e.g. the corporate network) – but is problematic if communication is required concurrently with several destination networks. The most comprehensive (but still a future focused) solution for hotspot WLANs will be the broad-based adoption of IEEE 802.11i. This solution will leverage built-in operating system support to allow the subscriber to choose the most suitable form of user-authentication and data link layer encryption – and thereby mitigate the confidentiality risks to within acceptable levels.

5.2 Corporate networks WLAN deployment

The best practice deployment of a WLAN within (onto) a corporate network requires two conceptual steps to ensure a professional level of protection:

- Isolate (potentially) hostile traffic from all sensitive corporate traffic and canalise (i.e. force traffic down a well defined route) this traffic through a small set of well protected and comprehensively logged fixed entry points.
- Deploy *defence in depth* via (1) the authentication of all traffic using an access point and (2) the strong encryption of all data transferred between each WLAN client and each access point.

The ultimate implementation of the above points would also create a firewall within each WLAN access point. However this solution does not scale well – and may mean an unsupportable level of work within the context of a corporate network. A more scalable solution is now discussed with respect to Figure 4.

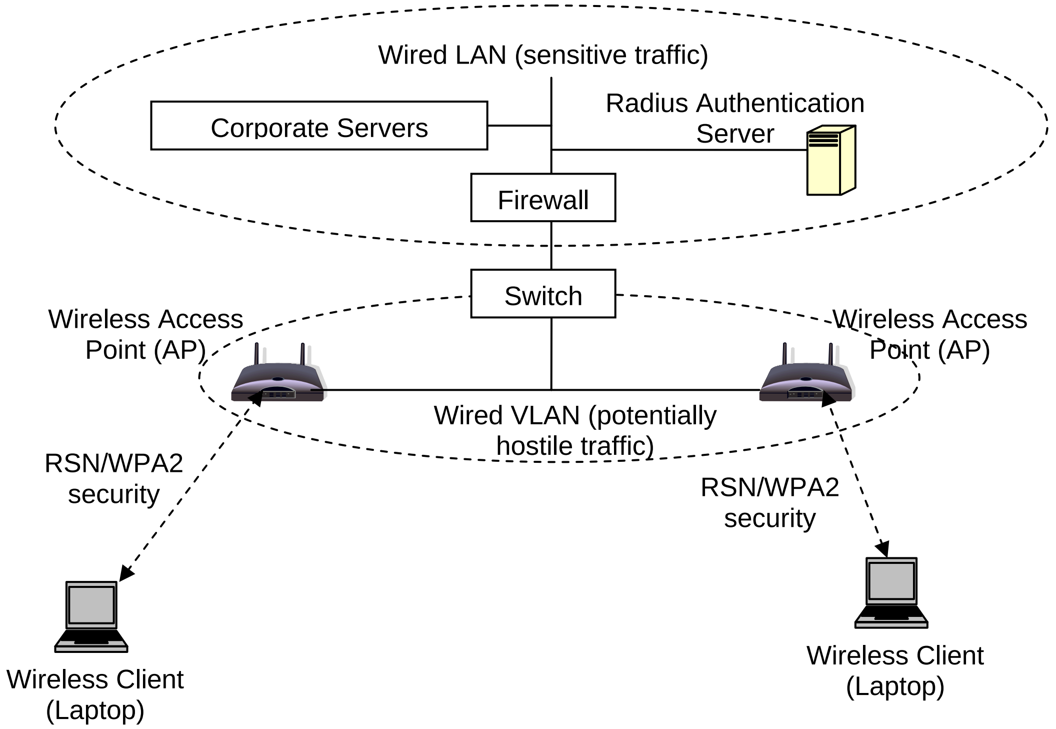
Wired LAN (sensitive traffic)
Corporate Servers
Radius Authentication Server
Firewall
Switch
Wireless Access Point (AP)
Wireless Access Point (AP)
Wired VLAN (potentially hostile traffic)
RSN/WPA2 security
RSN/WPA2 security
Wireless Client (Laptop)
Wireless Client (Laptop)

Figure 4: Corporate WLAN best practice deployment

Figure 4 shows that the isolation of (potentially) hostile traffic is achieved via the use of corporate switches to create a Virtual Local Area Network (or VLAN) as per IEEE 802.10. The alternative to a VLAN is to run new LAN cables to all access points and create a single new LAN – however this solution is not optimal in terms of time and cost. Whilst the VLAN solution is still vulnerable to several attack vectors (including ARP spoofing), it is still clearly preferable to allowing traffic from access points to intermix with other corporate traffic. The canalisation of (potentially) hostile traffic is then achieved (as shown in Figure 4) via the deployment of a firewall at the point at which VLAN (and therefore WLAN) traffic enters the corporate wired LAN. The second conceptual step for strong security is the creation of defence in depth – comprising data link layer strong encryption (for confidentiality) and access control. The strong encryption is implemented via RSN/WPA2 security operating between each wireless access client and each access point. The access control is achieved using the IEEE (access control) 802.1X and suitably constructed X.509 digital certificates operating across each wireless client, each access point, and a corporate Radius server.

Conclusions

The clear responsibility for WLAN administrators is to provide network users with best practice security strategies to mitigate the real risk of unauthorised data access. The clear responsibility for IT auditors is to ensure that best practice security strategies are in place and that operational compliance is consistently achieved. WLAN security is complicated by the open nature of the wireless signal propagation which in turn creates a confidentiality vulnerability. The development of WLAN protocols with robust confidentiality controls (ie, encryption) has been problematic. Indeed it is only very recently that a verifiably robust solution has been specified (802.11i) – and this solution will take time to roll out across WLAN services and users. Best practice security strategies for WLANs are routinely agreed within the IT industry (Garfinkel 2002) to comprise strong data encryption of transmitted packets. In the general WLAN transmission case, this strong encryption may be provided by 802.11i (layer 2) or VPNs based on IPSec (layer 3). Higher level (ie, layer 4 and above) more specific encryption solutions centre upon SSL/TLS for HTTP, Kerberos for secure authentication, and S/MIME for secure email. It remains very unclear within the IT industry, however, as to how the level of WLAN operational compliance with these best practice methods may be gauged and reported. This research has developed a software audit tool to analyse the level of confidentiality within a production WLAN system. The audit tool is innovative, non-intrusive on network productivity/bandwidth, controlled against attack, and active in its analysis and reporting of security vulnerabilities.

Clutterbuck P, Rowlands T and Seamons O (2007) “Auditing the Data Confidentiality of Wireless Local Area Networks” *The Electronic Journal Information Systems Evaluation* Volume 10 Issue 1, pp 45 - 56, available online at www.ejise.com

References

Airmagnet (2004) “Best Practices For Securing Your WLAN”, [online], Airmagnet Inc, http://www.net-security.org/dl/articles/WLAN_Security_Best_Practices.pdf.

Dennis, A. (2002) “*Networking in the Internet Age”*, John Wiley and Sons. New York.

du Preez, G. T., Pistorius, C. W. I. (2003) “*Technological Forecasting and Social Change*”, Vol. 70, pp1-20.

Edney, J, Arbaugh, W. (2004) “*Real 802.11 Security*”, Pearson Education, Inc.

Fluhrer, S., Mantin, I., Shamir, A. (2001) “*A Weakness in the Key Schedule Algorithm of RC4*”. Proceedings of the 4th Annual Workshop on Selected Areas of Cryptography.

Frankel, S., Eydt, B., Owens, L., Kent, K. (2006) ”*Guide to IEEE 802.11i: Establishing Robust Security Networks*”, National Institute of Standards and Technology. Special Publication 800-97 (Draft).

Garfinkel, S., Spafford, G. (2002) ”*Web Security, Privacy, and Commerce*”, 2nd Edition. O’Reilly and Associates.

Gast, M. S., (2005) “*802.11 Wireless Networks The Definitive Guide*”, 2nd Edition. O’Reilly and Associates.

Hevner, A. R., March, S. T., Park, J. (2004) “*Design Science in Information Systems Research*”, MIS Quarterly. Vol. 28, No. 1, pp. 75-105.

Hinde, S. (2001) “*The Weakest Link*”, *Computers and Security*, vol. 20, no. 4, pp. 295-301.

Hinde, S. (2002) “*Compsec 2002: the complete security circle*”, Computers and Security, vol. 21, no. 8, pp. 689-93.

Moskowitz, R., Fleishman, G. (2003) “*Weakness in Passphrase Choice in WPA Interface”,* WNN Wi-Fi Net News, http://wifinetnews.com/archives/002452.html.

Ossman, M. (2004) “*WEP: Dead Again, Part 1”*, Security Focus, viewed 15/5/2006, http://www.securityfocus.com/infocus/1814.

Sabat, H. K. (2002) “*The evolving mobile wireless value chain and market structure*”, Telecommunications Policy, vol. 26, no. 9-10, pp. 505-35.

Stubblefield, A., Ioannidis, J., Rubin, A. D. (2001) “*Using the Fluhrer, Mantin, and Shamir Attack to Break WEP”*, ATandT Labs Technical Report TD-4ZCPZZ Revison 2.

Stallings, W. (2003) “*Network Security Essentials Applications and Standards”*, 2nd edition, Pearson Education International, New Jersey.

Tsalgatidou, A., Pitoura, E. (2001) “*Wireless Innovations*”, Computer Networks, Vol. 37, pp. 221-236

Cam-Winget, N., Housley, R., Wagner, D., Walker, J. (2003) “*Security Flaws in 802.11 Data Link Protocols*”, Communications of the ACM. May 2003. Vol. 46, No. 5. pp 35-39.

Reference this paper as:

Clutterbuck P, Rowlands T and Seamons O (2007) “Auditing the Data Confidentiality of Wireless Local Area Networks” *The Electronic Journal Information Systems Evaluation* Volume 10 Issue 1, pp 45 - 56, available online at www.ejise.com