Home

Wireless Local Area Network (WLAN) Security solution for Corporate and E-Government businesses

Muhammad M. Satti
Macquarie Corporate Telecommunications
IntelliCentre, Sydney Australia.
Email: msatti@macquarie.net.au

Brian J. Garner
Professor of Computing,
Deakin University, Vic. Australia
Email: brian@deakin.edu.au

Abstract

Confidence in the use of the Wireless Local Area Network (WLAN) for internal, external or corporate business communications relies on effective security, and intruder detection processes. Regrettably, the triumph of the WLAN's design for corporate and government agencies as a ubiquitous open authentication environment is at risk of being tarnished by unscrupulous and vindictive attacks. Despite the risks WLAN installation is in rise and estimated 55.9 millions nodes by the year 2006, representing a $4.5 billion market [1]. The scope of this paper is to focus on the identification of security flaws in the current protocol model and to suggest a better implementation method that includes additional security as an add-on to improve corporate confidence [2] in wireless LAN security.

Keywords: WLAN Security, Wi-Fi Security, information Security, Corporate WLAN,

I. Introduction

Despite the global economic downturn, organizations continue to deploy WLAN because of flexibility in deployment in congested downtown, and also, to increase productivity more economically than conventional wireless LANs have achieved. Emerging technologies typically focus on implementation issues first rather than security. Handheld devices are inherently insecure, and the current WLAN standards 802.11b, offers immature and inadequate security. The wireless LAN environment is deemed to require significant research work and re-structuring of the 802.11b algorithm and upgrades, endpoints, transmission techniques and mechanism, which limit the large scale deployment of this technology. The existing models of IEEE 802 algorithm combat the security problems by using shared key authentication and Wire Equivalent Privacy (WEP) [4]. Regrettably, WLAN ubiquitous entry-points undermine the security of the existing model, an urgent attention is needed to address this problem quickly and effectively. Network hacking and exploitation is now more sophisticated. Attack mechanisms are better co-ordinated and complex. Virus, worms and Trojans (Backdoor) writers, have blended their skills to subvert the security perimeters of any corporate entity or government. These non-conventional and unexpected (blended) techniques pose new challenges to researchers from academia, and to industrial research professionals, for adequate security solutions. *Code Red, Nimda* and *Bugbear* are examples of recent challenges for Security professionals.

The focus on bits in the air (WLAN) further changed crackers' habits, when networks were wired. Crackers had to dial-in or physically connect to get access, which was hard, intensive and time consuming. The "*black-hats*" spent incredible time and resources to get such access and achieve their goals. But now, instead of aiming a dialer at a phone exchange and noting the numbers when a modem answers the line, crackers have adopted a technique called "*War Driving*" Just jumping into a car with an appropriately configured wireless network client to locate and access the ("*LAN-Jack*") wireless network.

For example, recently a group of hackers called " *War Chalking*[1] " setup their laptop computer and drove through the busiest street of a major city, to find any loose nodes of a WLAN.

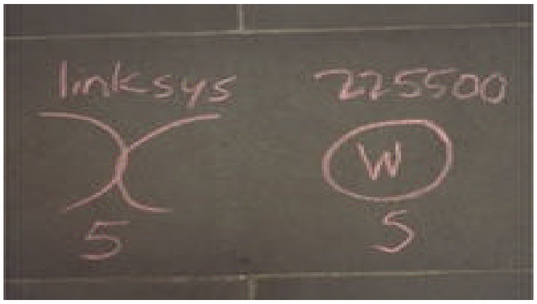


Figure1; An example of War Chalking

Wireless networks enable hackers to use their computers on the road. Hackers are equipped with laptop (*Easy-to-obtain software tools*) looking for unprotected wireless

[1] The signs are simple. If war chalker find an open Wi-Fi network they draw, in chalk two half of circles back to back. If the node is closed, the two halve Are reversed, joined into a circle. If the node is protected the circles contains a W short for Wire Equilvant Privacy (WEP). Other information is written SSID (Service Set ID) that acts as a password when a mobile device tries to connect to the network; the bandwidth available access contact and so on.

networks through which to login. Every major city of this modern world has wireless LAN also called “Wi-Fi”. It is not only to hack and access high speed free Internet and download or even steal sensitive data, but also to promote WLAN vulnerabilities for colleagues to use! Figure 1 is an example of such a malicious approach. [2]

II. Limitations of Existing (WLAN) Security

WLAN is comparatively newer then Wired LAN. The protocol explaining WLAN is 802.11X rule sets and policies. This protocol has lost its credibility due to the recent security incidents. Existing 802.11X protocol posed significant security threats to nearly all corporate enterprises and governments around the world. The risks are real and can exist even if an organization has chosen not to implement wireless devices as a corporate standard. No enterprise should ignore the potential risks posed by security compromise. Consider 802.11 protocol basics and Wire Equivalent Privacy (WEP). IEEE 802.11 [2] defines two methods of authentication service; Open system and shared Key. In open systems, authentication is essentially a null authentication algorithm. Any remote station that requests authentication with this algorithm may become authenticated if the recipient station is set to open authentication. Open system authentication is only for implementation where ease-of-use is the only issue, basically almost no security. Shared Key (SK) authentication supports authentication of stations as either a member of those who know a shared secret key or a member of those who do not. [4] The WEP algorithm is a form of electronic codebook in which a block of plain text is bit-wise Exclusive OR with a pseudorandom key sequence of equal length. Figure 2 explains basic principles of Exclusive OR and inequality comparator [3].

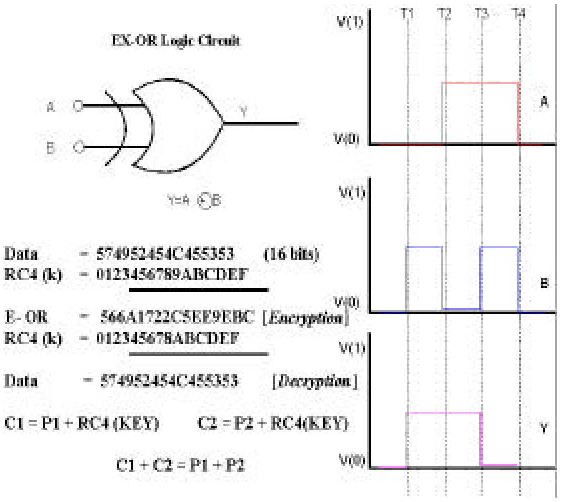

EX-OR Logic Circuit
A
B
Y
Y=A ⊕B
Data = 574952454C455353 (16 bits)
RC4 (k) = 0123456789ABCDEF
E- OR = 566A1722C5EE9EBC [Encryption]
RC4 (k) = 012345678ABCDEF
Data = 574952454C455353 [Decryption]
C1 = P1 + RC4 (KEY)
C2 = P2 + RC4(KEY)
C1 + C2 = P1 + P2
V(1)
V(0)
T1
T2
T3
T4
A
B
Y

Figure2; Basic XOR functional Diagram

The WEP algorithm generates the key sequence. This is based on RC4 algorithm, and proprietary key management. The attackers can guess the keys by sniffing a full or portion of the data packets exchanged between remote client and Access Point (AP) of WLAN network. The authentication method (using WEP) can be hard to administer since when the key changes, either because it’s been compromised, there’s a change in implementation, or the user base changes; the new key needs to be distributed to all users in a secure way [5]. Figure 3 depicts basic key exchange mechanism.

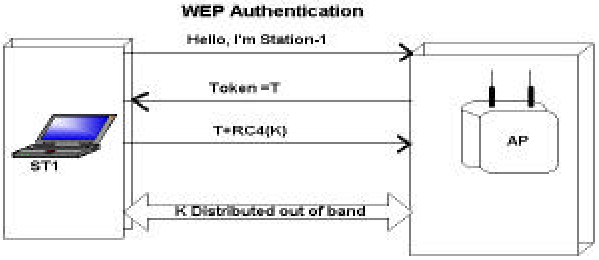
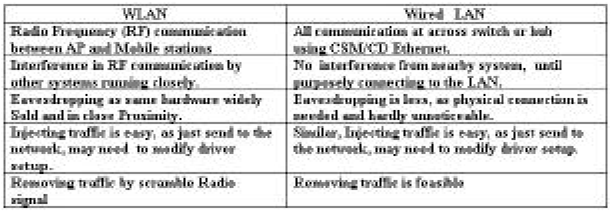


Figure 3. WLAN Key Exchange

The public/private key distribution algorithms are designed to avoid dissemination of keys between trusted users and resulting in a highly secure scheme for the wireless network with absolutely no need to distribute the keys to the end users.

A. Common Attacks in WLAN

Wireless networks becoming more prevalent, in enterprise and government use. The technology promised wired equivalent privacy and aimed to provide industry standard Privacy, Integrity and access control. Unfortunately none of these security goals were achieved and WLAN encountered numerous attacks. The weakness in WEP refers back to a key derivation problem in the standard. The WEP encryption is based on the RC4 stream Cipher, it is important each packet have a different WEP key. While the WEP standards had specified use of different keys for different data packets, the key derivation function is flawed.



WLAN	Wired LAN
Radio Frequency (RF) communication between AP and Mobile stations	All communication at across switch or hub using CSM/CD Ethernet.
Interference in RF communication by other systems running closely.	No interference from nearby system, until purposely connecting to the LAN.
Eavesdropping as same hardware widely Sold and in close Proximity.	Eavesdropping is less, as physical connection is needed and hardly unnoticeable.
Injecting traffic is easy, as just send to the network, may need to modify driver setup.	Similar, Injecting traffic is easy, as just send to the network, may need to modify driver setup.
Removing traffic by scramble Radio signal	Removing traffic is feasible

Table 1. Security in LAN and in WLAN.

Top

Table.1 explains the Wired LAN and Wireless LAN security issues in general terms, focusing on a comparison of two network technologies.

B. Initialization Vectors (IV) Collision

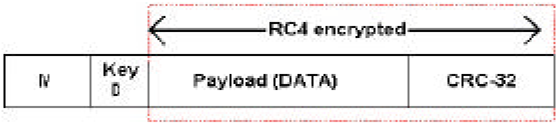
If encrypting two messages C1 and C2 with the same part of RC4 Key stream, if any part of Key stream is known then the second message can be easily decrypted. e.g.

C1 = P1 XOR RC4 (Key)

C2 = P2 XOR RC4 (Key)

C1 XOR C2 = P1 XOR P2

Hence the Keystream will cancel out, if P1 is known, P2 is immediately available.



When three or more packets collide, the hacker can use the collision to analyse the stream ciphers for useful information.

C. Decryption Dictionary Attack

Once a packet is successfully decrypted, one can discover the key stream easily and can use known Initialization Vectors (IV) sequence to guess the secret key.

RC4 (k, IV) = P XOR C

It can be used to decrypt packets with same IV. The IV is limited to 2^{24} and with existing high-powered CPU can easily decrypt the combination of WLAN shared key.

D. Linear Checksum and Packet Modification

With the present encryption in WEP the CRC-32 is used to check the data integrity. It may be suitable for normal communication for random errors, but not providing due diligence and granularity in WEP. The Linearity of the CRC-32 allows intruders to change bits in the packet. The hacker can modify the active stream and then bypass the access control system.

CRC (X + Y) = CRC (X) + CRC (y)

RC4 (k, X + Y) = RC4 (k,X) + Y

RC4 {k, CRC (X + y)} =

RC4 { k,CRC(X) } + CRC(y)

In order to modify the bits in the packet the partial knowledge is sufficient and only known portion's modification can leads to breaking of whole key management.

E. Redirection and Reaction Attack

Another common dirty trick is to re-direct the traffic from legitimate remote station to malicious machine, without violation of the checksum process at AP.

Suppose someone can guess destination IP in encrypted packet. It can flip the bits to change IP (Internet Protocol) to any non-authorized user. AP would assume legitimate user and will communicate as normal. Therefore the *MAC* (Message Authentication Control) address of any remote station should be the part of authentication rather then simple TCP checksum. Authors are suggesting a state-full firewalls to address these problems as stated bellow.

There are few common issues with existing WLAN protocol, which required further investigation and improvement to mitigate the risk.

i. Single key shared by all WLAN station, and it is easy to Guess.

ii. Key length is not appropriate, as 40 bits is most commonly used and 128 bits is available but practically delivers 104 bits.

iii. Unauthorized access is possible by altering packets.

iv. Eavesdropping (sniffing)

v. Attacks from authorized users

vi. Interference in RF communications by card-less phones and other systems.

vii. High Signal to Noise ratio due to the narrow bandwidth limit.

viii. Cross talk effects from other's UHF communication bands.

The attacks against WEP are not a result of a weakness of the algorithm, but instead a weakness in WEP key derivation, that produced weak RC4 keys that were very similar for different data packets. RC4 is the popular algorithm protecting the millions of users who access secure web pages and send data via the SSL/TSL protocol.

It is observed that even the advent of new keying algorithm of *Fast Packet Keying* (FPK) adopted by IEEE 802.11i dose not guarantee the WLAN security. The un-resolved issues arguably opening the door of other technologies to secure the transmission and improve the model of authentication. The add-on technologies are more

Top

secure and resilient and can facilitate highly protected environment.

III. Authentication model for secure communications by WLAN

Wireless LANs (WLANs) are attractive due to their ease of deployment and reconfiguration. In addition, they support roaming hosts, and flexibility to communicate with nearby offices [6]. Enterprise and global aspects of this technology is not yet explored by industry due to the lack of security confidence in existing technologies. This paper is suggesting some common industrial recommendations and secures implementation of WLAN with state-of-arts security and encryption tools. This solution could serve better security for WLAN implementation until IEEE 802.11X algorithm addresses its security related flaws .The following suggested design is well suited to guarantee a corporate /Government level of trust and information security.

A. Enhanced WLAN Security Model

An enterprise or in Government network giving remote access to the employees or contractors by the central directory system, which is compatible with all operating systems is Lightweight Directory Access Protocol (LDAP) and RADIUS servers. This is the best password authentication model, but in WLAN environment where the login is remote, authentication is not enough. The problem arises with remote users issuing a fake identification, which subverts the authentication server by providing access. By implementing perimeter Firewalls at the front, and a Virtual Private Network (VPN) for secure connection, the product is more resilient and trustful for corporate business as compared to IEEE 802.11b, or other similar algorithms.

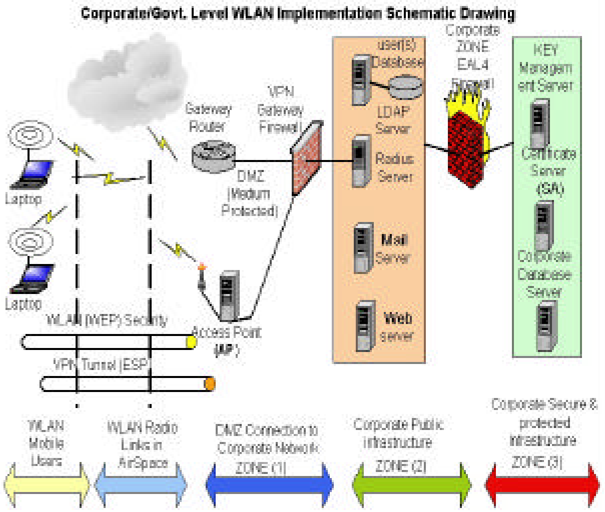

Corporate/Govt. Level WLAN Implementation Schematic Drawing
Laptop
Laptop
Gateway Router
VPN Gateway Firewall
DMZ (Medium Protected)
Access Point (AP)
WLAN (WEP) Security
VPN Tunnel (ESP)
user(s) Database
LDAP Server
Radius Server
Mail Server
Web server
Corporate ZONE EAL4 Firewall
KEY Managem ent Server
Certificate Server (SA)
Corporate Database Server
WLAN Mobile Users
WLAN Radio Links in AirSpace
DMZ Connection to Corporate Network ZONE (1)
Corporate Public infrastructure ZONE (2)
Corporate Secure & protected infrastructure ZONE (3)

Figure 4; The Enhanced Security model for corporate WLAN.

VPN, the remote access choice for a growing number of enterprises, is arguably the best way to thwart intrusions via wireless transmissions. Using a VPN and deploying wireless Access Points in a de-militarized zone, DMZ effectively segregates the WLAN and assures that only authorized wireless traffic can access the network [7].

In this architecture, the VPN gateway is placed behind the wireless access points. This offers the same level of security as VPNs can provide for any remote user who uses a dial-up or high speed, wired connection. A Remote Access Dial-In User Service (RADIUS) server is added in this design, to authenticate wireless access points before they are passed to the VPN!

B. Remote Authentication Method

A WLAN deployment network can be created as an extension of an existing corporate network, or it can be a completely separate physical network and system infrastructure located at a carrier collocation facility.

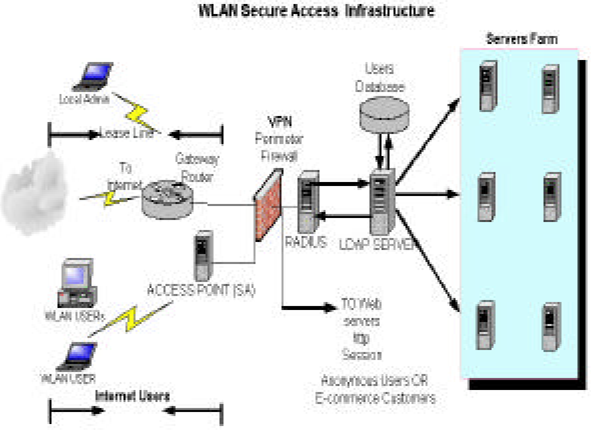


Figure 5. WLAN Access Control System

In a case where the new WLAN infrastructure is created as an extension within an existing corporate network, the simple and secure way to connect the corporate network and WLAN system is to build a dedicated WLAN on the core corporate infrastructure switch and restrict traffic by applying Access Control Lists (ACLs) on the router and Switches (Layer 3), where all servers are connected [8]. However without a VPN tunnel, the security can be compromised by "*sniffers*" sniffing packets from the air and gaining access into the networks. Therefore, for more secure scenarios a firewall (as shown in Figure. 4) should be considered between the highly protected network and the Corporate WLAN infrastructure.

Top

C. Key Management

The proposed model incorporates digital certificates supported by advanced key management. If an enterprise offers on-line business in which WLAN users are relying on their login for financial transactions, or dealing with a critical database, the transactions require highly protected (HP) security solutions. However if the WLAN is deployed for dedicated corporate users and the does Business not require a high level of protection, than a digital certificate requirement can be removed from the above model, but key management will remain, as in WEP, in the protected security zone. In order to provide a uniform framework for key distribution and to manage key groups reflecting *need-to-know* categories, we chose to implement PKI (*Public Key Infrastructur*e) style key generation and authorization as a centralized function. The basic structure of any PKI requires at least 2 functional blocks. Firstly, certificates must be created and destroyed (revoked) somewhere within the system, and secondly, certificates must be stored and made available to the clients [9]. The Certification Authority (CA) provides all the required services of the former, and the Certificate Server (CS) the latter.

Since trust in a PKI system resides within the certificates themselves, the CA must be a trusted entity, but no such requirement need be placed on the CS. The CS receives Certificates and CRLs from the CA and stores these items in the corresponding database. The database server is also at Zone-3 (Ref. Figure 4) to maintain a highly protected portal. The CS provides several other interfaces to clients within the local domain as well as an inter-domain interface. Clients may contact the CS requesting certificates by subject name or serial number. They may also request CRLs from the CRS interface. Inter-domain clients may access the same facilities through the local CS. The CS may reside in corporate zone-2 and need not be trusted, as it merely stores certificates in which the trust is inherent.

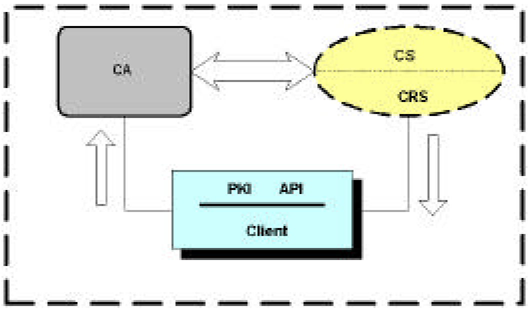


Figure 6. Key management

IV. Conclusion

The security model presented in this paper can achieve most of its goals by implementing add-on technologies and proven techniques of deployment in realistic corporate models. Wireless equipment continues to evolve. The IEEE is on notice to address known vulnerabilities, but whether to use WLAN for its convenience is a vexatious issue for IT managers at present, as the wireless LAN environment is not secure. Without significant security enhancements to IEEE 802.11X, endpoints and transmission are regrettably, wide open to compromise. Handheld devices are not designed for, nor capable of, sophisticated security. Personal Digital Assistants (PDAs) and their wireless access points (AP s) are currently deployed outside the information security control framework. IEEE 802.11X protocols are inadequate, to meet anything but minimal security requirements. The Wired Equivalent Privacy (WEP), 802.11b is a very low-grade encryption mechanism, has proved easy to break, and is hamstrung by its lack of a key management scheme. In the corporate scenarios discussed, the suggested framework extension is believed to address all current vulnerabilities. The WLAN could then be utilized as a corporate solution in most environments. Cost-effectiveness is still an open question justifying future research. The tradeoff for Information Technology (IT) managers is the traditional cost/security balance!

V. References

1. Dale,G. "*Wireless Insecurities*" Information Security Magazine January 2002(USA) .
2. Garry,B. Technology editor of The Age, " *X marks the Spot for Hackers*" July 8, 2002.
3. Millman,J. and Grabel,A. " Microelectronics " 2nd Edition pp-215 McGraw -Hill 1988.
4. Draft International Standards, ISO/IEC 8802-11. IEEE P802.11/D10, 14 January 1999.
5. William, S. Cryptography and Network Security: "*Principles and Practice*", Prentice Hall, July 1998.
6. Muller N.J, "Wireless data Networking," Artech. House, 1995, USA.
7. Prasad A R, Moelard H, Krugs J. "Security Architecture for wireles s LANs , IEEE 2000.
8. Park S.H , Ganz. A, " Robust re-Authentication and Key exchange protocol for IEEE 802.11 Wireless LANs Oct. 1998 Boston, USA.
9. Rivest, A.S., Adleman, R & L : A Method for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 1978.

Top