

# Will Security and Billing issues pull Wi-Fi down?

Poongovan Ponnaivaikko, Srinivasan Rajagopalan, Gandy Tunggal

[poongovan@MobileIN.com](mailto:poongovan@MobileIN.com), [srini4\\_edu@MobileIN.com](mailto:srini4_edu@MobileIN.com), [gtunggal@MobileIN.com](mailto:gtunggal@MobileIN.com)

A capstone paper submitted as partial fulfillment of the requirements for the degree of Masters in Interdisciplinary Telecommunications at the University of Colorado, Boulder, December 12, 2002. Project directed by Dr. Frank Barnes

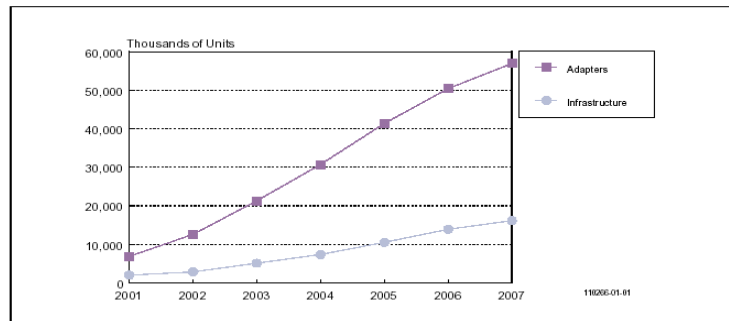
## 1. Introduction

Wi-Fi (short for wireless fidelity) is an alias for IEEE 802.11b [2]. It is a high frequency wireless local area network (WLAN), operating on unlicensed spectrum at 2.4GHz range with the area of coverage around 350 feet.

As per sextant research [10], the take rate for Wi-Fi is phenomenal. "Intel alone expects to sell 40 million Wi-Fi enabled devices in 2004. General Motors installed Wi-Fi throughout its 25 plants with about 35 to 65 access points per 80-acre plan". Wireless Developer Network [11] indicates that by 2006 analysts expect 66% of laptops and 33% of Personal Digital Assistants (PDA) to be 802.11b-enabled."This would mean an increase in the number of 802.11b enabled devices – in Europe alone – from 1 million today to 75 million in 2006". Along with the countless Wi-Fi networks at home, the currently estimated 4,100 public hotspots are expected to mushroom ten fold by 2006 [12], according to researchers at In-Stat/MDR [13].

In a recent Gartner report dated October 2<sup>nd</sup> 2002 [6], Gartner Dataquest's final wireless LAN shipment data for 2001 (as shown in Figure 1) shows total shipments of almost 9 million units worldwide, consisting of nearly 7 million adapters and about 2 million infrastructure units (primarily access points and wireless broadband gateways). This is even higher than Gartner's preliminary estimates of slightly more than 5 million adapters and 1.8 million access points, and represents a unit shipment growth over 2000 of nearly

Worldwide Wireless LAN Equipment Shipments, 2001-2007



Source: Gartner Dataquest (September 2002)

150 percent.

### **Figure 1 Worldwide WLAN Equipment Shipment**

In spite of the above favorable prediction, there is concern in some quarters that Wi-Fi could fold due to the Security holes and Billing related issues.

## **2. Goal**

The basic question that this paper would answer is, "Will Security and Billing issues pull Wi-Fi down?" This paper would discuss the evolution of wireless security, the enhancements, and available and future solutions. Also, this paper would address the billing issues related to roaming between 2.5G/3G and Wi-Fi networks and the available billing standards.

## **3. Relevance to prior work in the field**

Jesse Walker of Intel [3] published findings on the security holes of the WEP based 802.11b system in Oct 2000. Since then, Professor Arbaugh and his team have released two papers, one discussing the glaring loopholes of WEP [5] and the other discussing the vulnerabilities of 802.1X [4]. While these works are the key references for security issues discussed in this paper, this paper will also talk about the other key consideration for Wi-Fi's growth, namely billing. Thus far, the same billing standards that are currently being used for the cellular services are also being used for an integrated WLAN/Cellular service. This paper shall focus on what the alternative billing standards are, and why they are better. While the Fall 2001 Capstone Paper [25] discusses about security issues for WLAN in a public setting, this paper will lay emphasis on the impact of such issues on the growth of Wi-Fi. Also, this paper will discuss newer security standards, including the latest - Wi-Fi Protected Access (WPA).

## **4. Scope**

This paper will address Security and Billing issues that could impact the growth of Wi-Fi in the US business and residential markets.

This paper will focus on:

- Prevalent security approaches and their loopholes
- Available and potential solutions for enhanced security
- Studying the roaming business model that is presumed to work best for an integrated mobile service provider (cellular/WLAN)
- Available billing standards
- a workable billing standard for the mobile service provider

## **5. Security in Wi-Fi networks**

### **5.1. Need for Wi-Fi Security**

WLAN has much less privacy compared to a wired LAN because of the use of Radio Frequency (RF) as a transmission medium. Anyone with compatible device can receive the RF transmission in its range and connect to the LAN server. An intruder need not physically break into a secured facility to tap into a wireless network. The potential for intrusion is more pronounced in a WLAN like Wi-Fi since it uses the free spectrum where there is no regulation, licensing or monitoring involved [5].

## 5.2. Available security measures and efficacy

Evolution of the security solutions for Wi-Fi is illustrated in Figure 2.

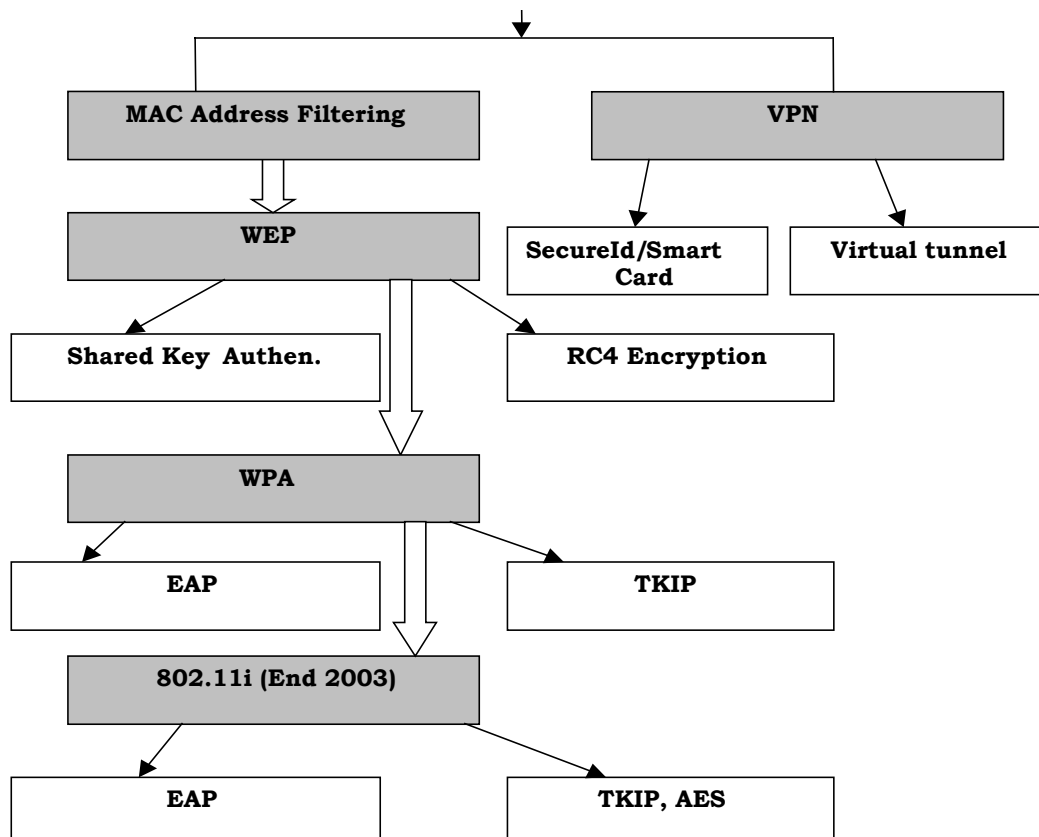
Available approaches for securing access to Wi-Fi LANs are:

- **Media Access Control (MAC) address filtering**

In this method, access to the network is restricted to client devices whose MAC addresses are configured in the access point.

**Shortcomings**

- Since MAC addresses are sent as clear text, unauthorized users can sniff this. Also, most of the wireless cards have an option to configure the MAC addresses through software. This could result in an intruder gaining access into the network.
- The process of entering client's MAC addresses and updating the MAC list in all the access points of the network could be cumbersome and could prove to be infeasible for large networks.



**Figure 2. Evolution of Security Solutions in Wi-Fi networks**

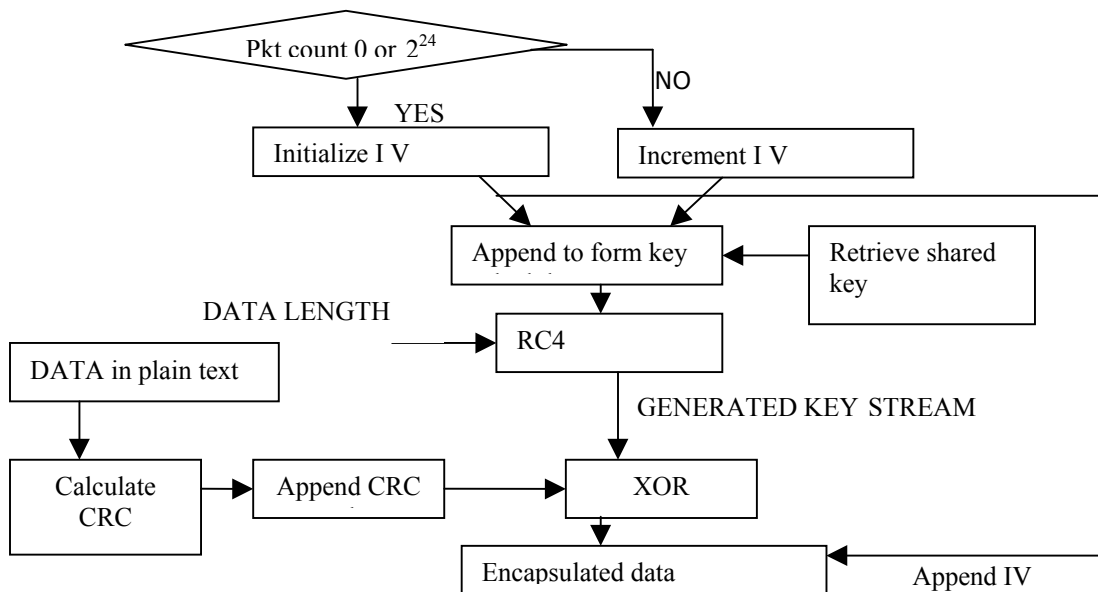
- **Wired Equivalent Privacy (WEP)**

WEP was intended to provide the same level of security as that of a Wired LAN. The primary goals of WEP include prevention of unauthorized access to the network, data security and data integrity [3]. WEP security has two subsystems: Authentication and Data Encryption. Commonly employed authentication in WEP is Shared Key Authentication. The encryption scheme of WEP uses a stream cipher known as RC4, invented by Ron Rivest of RSA (Rivest, Shamir, and Adelman) Data Security.

**WEP Authentication**

The shared key authentication employed by WEP uses an exchange of challenge and response messages between the client and the access point. The challenge text is sent in the clear to the client and is encrypted using the shared key at the client end and sent back to the access point.

**WEP Encryption**



**Figure 3. WEP encryption flowchart**

The process of key schedule generation and key stream generation is detailed in the flowchart **Figure 3**.

## Shortcomings

The limitations of WEP are:

- By sniffing one leg of the shared key authentication process, the security of the network can be compromised.
- Since Initialization Vector (IV) is reused every  $2^{24}$  packets and since IV is sent as clear text along with the encrypted packet and because most Wi-Fi installations use a few shared keys among its users and access points, data sent is decipherable thereby rendering the encryption ineffective.

## Wi-Fi Protected Access (WPA)

This is the latest standard adopted by Wi-Fi alliance (WFA) [26] and is a subset of the longer term 802.11i solution. Since 802.11i is slated to be released only by the end of 2003, WFA came up with this interim solution.

### WPA Authentication

To obviate the authentication weaknesses of WEP, WPA uses 802.1x and Extensible Authentication Protocol (EAP).

IEEE802.1x standard provides port-based network access control. In this standard, a Remote Authentication Dial In User Service (RADIUS) server uses the RADIUS protocol for authentication and session key issuance. [4]

However, the authentication used in WPA is mutual as opposed to one way authentication used in 802.1x. [26]

### WPA Encryption

To reduce the decipherability of the key stream used in WEP, WPA replaces it with a newer mechanism called Temporal Key Integrity Protocol (TKIP).

TKIP [7], formerly WEP2, is intended to be an interim solution to the problems seen in WEP. Following are the steps used in this approach:

- 128-bit temporal key is shared among clients and access points
- Temporal key is combined with client's MAC address
- 128-bit Initialization Vector is added to this to produce the key for data encryption
- Temporal key will be changed every 10,000 packets
- TKIP scrambles the keys using a hashing algorithm and ensures that the keys have not been tampered with by adding integrity checking

By using a large IV and a dynamic shared key, the security of the network is enhanced. Another main advantage of employing TKIP is that the existing WEP enabled devices can be upgraded to TKIP relatively easily.

- **802.11i solution**

This is a long-term solution and is expected to be available by end of 2003.

### **802.11i Authentication**

IEEE 802.1x is a key part of 802.11i's authentication mechanism.

### **802.11i Encryption**

TKIP and Advanced Encryption Standard (AES) are combined to provide effective encryption in 802.11i. This is backward compatible with TKIP.

AES is the standard approved by [9] National Institute of Standards and Technology (NIST). The key features of AES are:

- Can generate 128, 192, and 256 bit keys. Future WLAN systems are expected to adopt the 256 bit key standard for enhanced security.
- Ready implementation of this standard is not possible because of a requirement of a coprocessor in the client devices.

- **Proprietary solutions from Equipment Vendors**

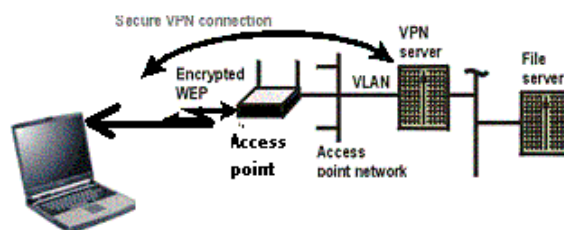
Wireless equipment manufacturers like Proxim and Cisco offer proprietary solutions to the WEP problems. Proxim's Harmony 802.11-product family offers enterprise-class security features, including 40, 128 and 152 bit WEP, VPN tunneling capabilities and per-user, per-session dynamic encryption.

Cisco's Lightweight Extensible Authentication Protocol (LEAP) overcomes the major limitations of 802.11 wireless securities by extensible authentication support to other backend directories or LEAP proxy RADIUS servers.

Such proprietary solutions however have the disadvantage of restricting product interoperability with the same level of security across networks.

- **Virtual Private Network (VPN)**

VPNs are widely used for wired networks in the enterprise sector. A VPN can be used to create a secure virtual "tunnel" from the client's device to the VPN server of Wireless Internet Service Provider (WISP) [8].



### Figure 4. VPN setup to the access point

(Courtesy: [http://www.dell.com/us/en/gen/topics/vectors\\_2001-wireless\\_security.htm](http://www.dell.com/us/en/gen/topics/vectors_2001-wireless_security.htm))

#### Shortcomings

While this solution is highly secure even for wireless LANs, it suffers from the following disadvantages:

- Use of VPN prevents multicasting on wireless networks
- Service can be disrupted when roaming between VPN servers of the WISP network or across wireless networks of different WISPs.

### 5.3. Summary of security solutions

Encouragement of proprietary solutions offered by equipment vendors would result in non-uniform security fixes across different Wi-Fi networks. This has an economic dimension in terms of discouraging competition from new market entrants.

Of the other solutions, although VPN seems technically viable, guaranteeing high degree of security, it is more suited to addressing the WLAN needs of the enterprise networks. In the light of the fact that VPNs are the most sought after security mechanisms for wired enterprise networks, choice of VPNs for their wireless counterparts is only logical. But the same cannot be readily applied to the public hotspots segment of the Wi-Fi market. This stems more from an economic rather than a technical viewpoint. Deployment of VPN solution can lead to dominance by a few players, thereby encouraging non-competitive behavior.

Implementing WPA seems to have the least adverse economic impact given the backward compatibility and the security it offers.

### 5.4. Security in competing WLAN technologies

Bluetooth standard employs SAFER+ (Secure and Fast Encryption Routine) algorithm for security procedure [14]. This algorithm generates 128 bit cipher keys from an exclusive-or'd 128 bit plaintext input. The encryption engine needs four inputs, the data, the Master's Bluetooth device address, the Master's Bluetooth slot clock, and a secret key, which is shared by both devices.

HIPERLAN/2 supports both authentication and encryption [15]. Its authentication protocol allows bi-directional authentication, both the Access Point (AP) and Mobile Terminal (MT) can authenticate each other. Its connection-oriented nature allows encryption on the user traffic to protect against eavesdropping and man-in-middle attacks.

The following table summarizes it all:

802.11	802.11b	Hiperlan/2	Bluetooth	HomeRF
Use shared key authentication	Authentication uses WEP. Allows	Two way authentications allow	SAFER+ standard. Authentication	Similar to 802.11b but HomeRF claims it has a more robust security

802.11	802.11b	Hiperlan/2	Bluetooth	HomeRF
tion method (WEP) or open system. Privacy is provided by WEP.	additional layer of securities, such as, VPN, AES and TKIP.	auth. by a server. User traffic can be encrypted.	n is controlled by host. Encryption depends on shared secret key.	due to FHSS and a longer 32 bit Initialization Vector (IV)

## 6. Billing

The intent of this section of the paper is to identify any billing related issue that could pose as an impediment to the proliferation of Wi-Fi. So we shall be looking at the issue from both the user's perspective as well as from the service provider's perspective.

### 6.1. A standard for Roaming between mobile services (WLANs/Cellular)

Let us first discuss the problem from the user's perspective. In order for Wi-Fi to proliferate it must be easy for the consumer to use the service. The easier it is to use the service the faster will the technology grow.

There are two types of user, those who subscribe to Wi-Fi from a service provider and others who don't. Users, who are not subscribers, usually pay for the service either before they use the service or immediately after they use it. Hence there is not much of a billing related issue there. But there are a couple of requirements to be met, in order to make life easier for users who are subscribers. First of all, the subscriber must be able to log-on to his home ISP's account from any access point. Secondly, how many ever times he roams over to other service provider's network, at the end of the month, he must still have to deal with only one bill. This will require every service provider to have roaming agreements with each other.

We must remember that the area of coverage of Wi-Fi access points, are very limited. Hence in order to be able to provide ubiquitous Wi-Fi coverage, the number of access point required is very large. Hence it is reasonable to expect that there will be numerous players in the field. The type of service providers that we can expect to enter the field include smaller WISPs who own and operate a couple of access points, relatively larger WISP's who own and operate many access points and mobile operators who would want to make use of their existing customer base to provide Wi-Fi services, which in turn will also help the operators in reducing their operating expenditures.

There is also a need for providing an integrated billing solution for mobile operators who have added hot spots as a part of their current 2.5G/3G networks. To facilitate this integrated billing, Wi-Fi service must allow for seamless roaming between different WISP providers and between WISP and a cellular network.

In order to ensure that there every service provider is compensated for the service that he provides, there needs to be a standard for service providers to establish service agreements with each other, especially since there will be a large number of service providers. Thus from both the user's perspective as well as the service providers perspective, the main billing related issue is the lack of a standard for establishing roaming agreements.

Wireless Ethernet Compatibility Alliance (**WECA**) is currently working on establishing one such a roaming standard. In this paper we would like to discuss three aspects of such a roaming standard, viz., the roaming platform model, a standard for the AAA protocol and a standard for the billing records.

## **6.2. Business Model for Roaming**

Establishing a standard for roaming agreements is not new. It has been used in the past for dialups as well as for GSM. But both the above standards do not allow for characterization or individualization of the service. For example a when a dialup user roams to a different network, he cannot expect the same kind of service as he would have got if he had logged onto his home ISP directly from the Home ISP's network. The roaming agreement standard for Wi-Fi must not make the same mistake. As we shall discuss in the following sections, this can be taken care of, by using flexible AAA protocols.

The dialup's roaming model allows for the service providers to sell the access minutes in wholesale to roaming brokers who in turn sell the minutes to service providers whose members roam to the area serviced by the broker. This model does not allow service providers to set agreements for service delivery quality. Hence this model can be ruled out for Wi-Fi. In the GSM's roaming model, every service provider has a bilateral roaming agreement with every other service provider. The clearing house only implements the settlement based on the bilateral roaming agreements. Such a model will also not work for Wi-Fi, because of the number of service providers involved.

Because of the magnitude of the number of bilateral roaming agreements that would be required for a ubiquitous coverage, one of the roaming business models that will work for the WLAN market is that of a multilateral roaming platform. That involves a centralized and independent clearinghouse which will have bilateral agreements with every service provider. In the bilateral agreement with the service providers, the clearing house should allow the service providers to set expectations for the quality of service delivery and should also allow the service providers to set the roaming tariffs for other service providers whose members roam in the service provider's network.

### **6.2.1. Current Players**

A small but growing group of companies has recognized WISP roaming as a business opportunity and are targeting the WISP market with clearing and brokering/aggregation

service offerings that will lower the transaction costs for WISPs who want to achieve roaming with other WISPs. Ipass ([www.ipass.com](http://www.ipass.com)), GRIC communications ([www.gric.com](http://www.gric.com)), Excilan ([www.excilan.com](http://www.excilan.com)) and t-net ([www.weroam.com](http://www.weroam.com)) are all examples of such companies.

### **6.2.2. Available Billing/Accounting Standards for an integrated service provider Accounting protocol standards**

The AAA protocol for Wi-Fi should be able to send more user related information than just the user profile. This requirement will help in implementing service characterization. For example, if the user has subscribed to gold or platinum service from the service provider, it should be possible to transmit such information too using the AAA protocol. The current version of RADIUS does not allow that. Moreover since the current version of RADIUS was built specifically for Dialups, it works only on top of PPP or SLIP. It has to be enhanced to allow for use over PPPoE. Thus an enhanced version of RADIUS (IETF RFC 2138) could be used for authentication and accounting. Other alternatives include Terminal Access Controller Access Control System (TACACS+). Another option would be to use a DIAMETER Authentication Authorization and Accounting (AAA) server. The DIAMETER protocol defines a policy protocol used by clients to perform Policy, AAA as well as Resource Control. It allows for transmitting more information than just the user profile and also allows for use over PPPoE. Thus DIAMETER would be a good choice for AAA protocol standard.

### **6.2.3. Available Billing Record Standards:**

The CIBERNET Cellular Inter-carrier Billing Exchange Roamer Record™ or CIBER is the roaming record used by all carriers employing AMPS analog, CDMA and TDMA air-interfaces, regardless of frequency [21]. CIBER is a set of proprietary protocols for the exchange of billing information among wireless telecommunications companies, billing vendors, clearinghouses, clearing banks and CIBERNET, developed, maintained and updated by CIBERNET.

The TAP or Transferred Account Procedure is the roamer billing standard used in GSM. CIBER is the equivalent for TAP in the IS-41 world [22]. TAP was originally designed to support the European community, and then its use spread to other continents. Because of this, roaming only occurred when traveling to another country until GSM was adopted in the United States. There are multiple TAP standards in use. TAP 2+ is the defacto standard for most of the world. Conversion ‘between’ TAP and CIBER is also done by data clearinghouses as well as by some billing vendors and operators.

IPDR stands for the Internet Protocol Detail Record [23], the name comes from the traditional telecom term Call Detail Record (CDR), used to record information about usage activity within the telecom infrastructure (such as a call completion).

MXP, Mobile Xchange Protocol [24], designed by CIBERNET to permit the wireless industry to bill for non-traditional (i.e. non-voice) services. MXP is designed to support revenue-sharing business models and facilitate the exchange of wholesale billing details for wireless m-commerce, messaging, voice and data across CDMA, TDMA, GSM, iDEN and 3G air interface technologies.

#### **6.2.4. Apt Billing Standard for a Cellular and Wireless LAN mobile operator**

CIBER and TAP are similar in terms of the functionality, architecture and the features they provide. Both the above standards are designed specifically for a particular network architecture namely IS-41 and GSP respectively. That being the case the above standards cannot be scaled to handle wholesale relationships. For example mobile operators in general support more than one air interface and more than one network architecture (E.g. Cellular & WLAN). In such a case the billing standards need to be able to implement and maintain multiple billing exchange protocols. CIBER and TAP hence are not best suited, when compared to other available standards.

MXP is similar to the Internet Protocol Detail Record (IPDR). Both protocols harmonize on a “technology-independent” approach to billing and settlements. Both protocols allow for real-time record exchange. Both protocols allow for XML based definition of the data structure and format of the records. One thing that differentiates MXP from IPDR is that, MXP has a billing-centric design and IPDR has a network-centric design. While IPDR is focused on Wireless technologies, IPDR has to cater to the requirements of Cable as well as Fixed line billing requirements.

### **7. Conclusion**

#### **Security**

Based on the above research on Security following is a summary of conclusions:

- In the enterprise sector, use of VPNs or WPA provide the much needed security
- In the residential market, stopgap measures like WPA bolster Wi-Fi's security.
- The frenetic pace at which IEEE task forces are proactively working to find a lasting solution like 802.11i make the outlook optimistic for Wi-Fi security.

#### **Billing**

Based on the above research on billing, this paper postulates that the mobile service providers would lean towards the following:

- A multilateral roaming platform
- An enhanced version of RADIUS (Ex. DIAMETER) for authentication and accounting
- MXP Billing standard

After a slow start, the Wi-Fi community has addressed the problems associated with security and billing proactively. Hence, this paper concludes that Security and Billing are, at best, minor concerns and do NOT have the potential to impede the proliferation of Wi-Fi in the coming years.

## References

- [1] Cryptography and Network Security, by William Stallings, Prentice Hall, 1999.
- [2] IEEE Std 802.11b-1999 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band
- [3] IEEE P802.11 Wireless LANs doc.:IEEE 802.11-00/362 - "Unsafe at any key size; An analysis of the WEP encapsulation" Oct 27,2000, Jesse R. Walker, Intel Corporation
- [4] "An Initial Security Analysis of the IEEE 802.1X Standard" - Feb 6 2002, Arunesh Mishra and William A. Arbaugh, University of Maryland
- [5] "Your 802.11 Wireless Network has no Clothes" - March 30, 2001, William A. Arbaugh, Narendar Shankar and Y.C.Justin Wan, University of Maryland
- [6] Gartner DataQuest Perspective - Wireless LAN Equipment Market: Strong Growth Set to Continue - Published 2 Oct 2002
- [7] "Better than WEP" - 1 February 2002, Internet.com, Lisa Phifer, [http://www.isp-planet.com/fixe\\_d\\_wireless/technology/2002/better\\_than\\_wep.html](http://www.isp-planet.com/fixe_d_wireless/technology/2002/better_than_wep.html) Website Accessed on 10/24/02
- [8] Vector Technology Brief, 802.11 Wireless security in business networks, September 2001, [http://www.dell.com/us/en/gen/topics/vectors\\_2001-wireless\\_security.htm](http://www.dell.com/us/en/gen/topics/vectors_2001-wireless_security.htm) web site accessed 25 October 2002
- [9] <http://www.nist.gov/speeches/rk-aes.html> REMARKS BY RAY KAMMER Director, National Institute of Standards and Technology Advanced Encryption Standard announcement Monday, October 2, 2000, Website accessed 24 October 2002
- [10] <http://www.autofieldguide.com/columns/martin/0902it.html> Automotive, Design and Production, Column The Next Big Thing: Wi-Fi By Martin Piszczalski, Sextant Research, Sep 2002, website accessed on 20<sup>th</sup> Oct 2002.
- [11] <http://www.wirelessdevnet.com/news/2002/238/news1.html> - Wireless Developer Network, "RoamAD Announces 802.11b Breakthrough with Metropolitan-Wide Wi-Fi Network", August 27, 2002, website accessed on Oct 20<sup>th</sup> 2002
- [12] <http://www.80211-planet.com/columns/article.php/1434601> "The WLAN Roaming "Standard" By [Ed Sutherland](#) , July 29, 2002, website accessed on Oct 22<sup>nd</sup> 2002
- [13] [www.instat.com](http://www.instat.com), website accessed on Oct 19<sup>th</sup> 2002
- [14] Bluetooth, connect without cables, Jennifer Bray and Charles F. Sturman, Prentice Hall PTR, 2001
- [15] HiperLAN2–The Broadband Radio Transmission Technology Operating in the 5 GHz Frequency Band, Martin Johnsson, H2GF White paper, 2001
- [16] <http://www.nwfusion.com/wifi/2002/main.html> Wi-Fi World, "What if Wireless Ethernet becomes as ubiquitous as cell service" By Joanie Wexler, Network World, 03/25/02, website accessed on 10/19/02
- [17] [http://www.servicefactory.se/whitepapers/roaming/#4\\_3\\_4](http://www.servicefactory.se/whitepapers/roaming/#4_3_4) "Roaming between Wireless ISPs", By Gunnar Almgren, website accessed on Oct 24<sup>th</sup> 2002
- [18] <http://www.wayport.net/press/75> Wayport Joins New Industry Organization As Founding Member To Develop Global Wi-Fi Roaming Standard, Press Release 30 Apr 2002, website accessed on 10/24/02
- [19] <http://www.nwfusion.com/news/2001/0528wispr.html> "Effort afoot to provide wireless roaming" By John Cox, Network World, 05/28/01, website accessed on Oct 18<sup>th</sup> 2002
- [20] [http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed\\_cr/secur\\_c/scprtl/scaa.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprtl/scaa.htm) Cisco Systems Documentation of AAA, website accessed on Oct 20<sup>th</sup> 2002
- [21] [http://www.cibernet.com/product\\_descriptions/product\\_ciber.cfm](http://www.cibernet.com/product_descriptions/product_ciber.cfm) Product Description of CIBER RECORD, website accessed on Oct 24<sup>th</sup> 2002
- [22] [http://www.ifast.org/files/IFAST15\\_011\\_Int'l%20Roaming%20Guide%20V3.doc](http://www.ifast.org/files/IFAST15_011_Int'l%20Roaming%20Guide%20V3.doc) International Roaming Guide from IFAST (International Forum on ANSI-41 Standards Technology), Jan 2001, website accessed on Oct 24<sup>th</sup> 2002
- [23] <http://www.ipdr.org/technical-work/FAQ.htm> Frequently Asked Questions, website accessed on Oct 24<sup>th</sup> 2002
- [24] <http://www.billingworld.com/archive-detail.cfm?archiveId=5723&hl> Standards Watch: Cibernet Releases MXP standard for MobileIP Revenue settlement, August, 2002, website accessed on 10/24/02
- [25] "Security of an 802.11b Wireless LAN in a Public Setting" - Capstone paper presented in Fall 2001 in University of Colorado By Dan DeKalb, Kylene Merritt, William Schultes, Jessica Wiest
- [26] [http://www.weca.net/OpenSection/pdf/Wi-Fi\\_Protected\\_Access\\_Overview.pdf](http://www.weca.net/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf) Over view of Wi-Fi Protected access : Wi-Fi alliance Rev dated 10/31/2002