

國立交通大學
資訊管理研究所

博士論文

主動式無線區域網路安全防護機制之研究

The Proactive Wireless Intrusion Prevention Mechanism for Wireless LANs



研究生：謝文川

指導教授：羅濟群

中華民國九十四年七月

主動式無線區域網路安全防護機制之研究

學生：謝文川

指導教授：羅濟群 博士

國立交通大學資訊管理研究所

摘 要

隨著網際網路與可攜式裝置的普及，「無線區域網路」成爲近年來通訊市場突破性的新興應用，由於無線區域網路係以電磁波爲傳播媒介，傳輸資料完全曝露於周遭的環境中，相對於傳統有線網路透過實體線路的傳遞，其安全性更是值得堪慮。隨著無線區域網路不斷的擴張，預期將成爲新興的網路犯罪環境，讓駭客可利用此環境入侵網站，散佈病毒、竄改網頁、竊取機密、癱瘓系統的通道。

在現有無線區域網路標準的安全機制中，WEP (Wired Equivalent Privacy) 是IEEE 802.11b在發展初期時定義的安全機制，也是目前無線網路最普遍的基本防護措施，近來日益竄起的無線網路安全事件，反映了WEP加密機制極待修正的窘境。WEP其主要的功能是對在無線區域網路上所傳輸之資料進行加密，以達到無線網路能夠擁有等同於有線區域網路一般的私密性。然而WEP加密機制，其安全漏洞已被各界所證實，駭客能利用適當破解工具如AirSnort在足夠時間內破解密碼，嚴重降低無線區域網路上資料傳輸的保密性。

本研究提出『無線區域網路環境干擾式防禦安全機制』(Interference-Based Protection Mechanism; 簡稱IBPM)，以發送假冒封包的干擾的方式，藉以混淆竊聽者WEP加密金鑰還原統計演算分析結果，讓竊聽者無法從大量的假冒資料中分析出真實的金鑰，進而避免金鑰被破解，提升WEP加解密安全的防護機制，另本研究亦提出主動式無線區域網路誘陷機制，具備將網路上可疑的網路攻擊即時連線至所建構的無線區域網路誘陷系統監測，藉由觀察入侵方式。最後本研究將這兩種安全防護機制實作一『主動式無線區域網路安全防護系統』來證明其具可行性。

關鍵字：無線區域網路、有線等效保密法、連線攔劫、無線區域網路誘陷系統

The Proactive Wireless Intrusion Prevention Mechanism for Wireless LANs

Student : Wen-Chuan Hsieh

Advisor : Dr. Chi-Chun Lo

Institute of Information Management
National Chiao-Tung University

Abstract

Over the past few years, wireless networks, specifically those based on the IEEE 802.11 standard have experienced tremendous growth and been the “hot spot” of a large amount of researches discussions with respect to its security architecture and mechanism. IEEE 802.11 was initially designed to provide data confidentiality and integrity protection through Wired Equivalent Privacy (WEP). However, WEP suffers from serious security flaws which arise due to the reuse of the Initialization Vector (IV) and the deployment of an unkeyed checksum for message authentication.

This research devised an innovative solution called Interference-Based Prevention Mechanism (IBPM). The proposed method generates interference effect by injecting spoofed frames to delude the WEP cracker resulting in inaccurate statistic. This research also proposes a proactive diversion-based wireless honeypot mechanism, within which all users are closely monitored and diverted into honeypot if one’s behavior is considered to be malevolent. Under this architecture, wireless honeypot is able to capture intruders even if attacks are not targeted to the honeypot.

A prototype named as “the proactive wireless prevention system” has been developed to evaluate feasibility of those two proposed mechanisms, and the research result shows that it is effective as well as useful in enhancing the security in wireless LAN environment.

Keywords : Wireless LAN 、 WEP 、 Sesssion Hijacking 、 Wireless Honeypot

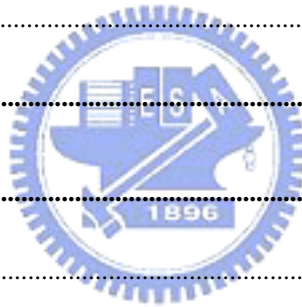
Contents

Abstract in Chinese	i
Abstract in English	ii
Contents	iv
List of Figures	vi
List of Tables	ix
CHAPTER 1	1
INTRODUCTION	1
1.1. MOTIVATION AND OBJECTIVE	1
1.2. OUTLINE OF THIS THESIS	3
CHAPTER 2	5
LITERATURE REVIEW	5
2.1. IEEE 802.11 STANDARD	5
2.2. NETWORK ARCHITECTURE	5
2.3. WIRELESS SECURITY.....	7
2.4 WLAN THREATS	8
2.4.1 <i>WarDriving</i>	8
2.4.2 <i>Encryption attacks</i>	9
2.4.3 <i>Interception and unauthorized monitoring of wireless traffic</i>	10
2.4.4 <i>Brute force attacks against access point passwords</i>	11
2.4.5 <i>Insertion attacks</i>	11
2.4.6 <i>Jamming</i>	12
2.4.7 <i>Client-to-Client attacks</i>	12
2.4.8 <i>Misconfigurations</i>	13



2.5. WIRED EQUIVALENT PRIVACY (WEP).....	13
2.5.1. WEP Vulnerability	16
CHAPTER 3	19
THE INTERFERENCE-BASED PREVENTION MECHANISM.....	19
3.1 THE PROPOSED INTERFERENCE SCHEMES	21
3.2 THE SCENARIO OF THE IBPM	23
3.3 STATISTICAL DIAGRAMS OF WEP CRACKING AND ANTI-WEP CRACKING	25
3.4 PERFORMANCE EVALUATION RESULTS	27
3.4.1 Analysis of IVs Generated by a Little Endian Counter.....	27
3.4.2 Analysis of IVs Generated by a Big Endian Counter.....	28
CHAPTER 4	30
THE PROACTIVE WIRELESS HONEYPOT	30
4.1. INTRODUCTION	30
4.2 HONEYPOT.....	30
4.2.1 Definition of Honeypot.....	30
4.2.2 The Development State of Art	31
4.3. PROACTIVE DIVERSION PROCEDURE	33
4.4. SYSTEM FRAMEWORK	36
4.4 SYSTEM PROCEDURE	38
CHAPTER 5	40
THE PROACTIVE WIRELESS INTRUSION PREVENTION SYSTEM	40
5.1. SYSTEM ARCHITECTURE AND DESIGN.....	40
5.1.1. Packet Capture Module	41
5.1.2. TCP Session Analysis Module	41

5.1.3. <i>Intrusion Reaction Module</i>	41
5.1.3.1 Anti-Wardriving	42
5.1.3.2 Anti-WEPcracking	42
5.1.3.3 MAC Authentication	43
5.1.4 <i>Honeypot Module</i>	44
5.1.5 <i>GSM Alarm Module</i>	44
5.2. SYSTEM DEMONSTRATION.....	44
5.2.1. <i>TCP Session Analysis and Reassembly</i>	44
5.2.2 <i>Anti WarDriving</i>	47
5.2.3 <i>Anti-WEP-Cracking</i>	48
5.2.4 <i>Wireless Honeypot</i>	49
5.2.5 <i>GSM messaging</i>	52
CHAPTER 6	53
CONCLUSIONS	53
6.1. SUMMARY	53
6.2. FUTURE RESEARCH DIRECTIONS	54
REFERENCES	54



List of Figures

FIG. 3 AD HOC NETWORK	7
FIG. 4 WARDRIVING MAP OF TAIPEI CITY	9
FIG. 5 SCREENSHOT OF AIRSNORT WEP CRACKING TOOL.....	10
FIG. 6 WEP ENCRYPTED FRAME FORMAT	14
FIG. 7 WEP ENCRYPTION PROCESS	15
FIG. 8 WEP DECRYPTION PROCEDURE.....	16
FIG. 9 IV PATTERN RESOLVING KEY COMBINATION	17
FIG. 10 XOR PLAINTEXT AND CIPHERTEXT TO RESOLVE KEY VALUE	17
FIG. 11 INTERFERENCE GENERATION DIAGRAM.....	20
FIG. 13 IBPM INTERFERENCE PROCEDURE.....	24
FIG. 14 K[0]~K[4] STATISTIC RESULT WITHOUT INTERFERENCE	26
FIG. 15 K[0] AND K[1] STATISTIC RESULT WITH INTERFERENCE.....	27
FIG. 16 CONNECTION PROCESS OF LEGITIMATE USERS	34
FIG. 17 DIVERTING ATTACKER INTO HONEYPOT.....	36
FIG. 18 FRAMEWORK OF THE PROPOSED WIRELESS HONEYPOT	38
FIG. 19 PROACTIVE WIRELESS IPS ARCHITECTURE	40
FIG. 20 SYSTEM MAIN INTERFACE.....	45
FIG. 21 ACTIVATING SESSION VIEW	46
FIG. 22 SELECTING A SESSION.....	46
FIG. 23 WEB PAGE RESTORED	47
FIG. 24 NETSTUMBLER DETECTED AN AP	47
FIG. 25 WAR-DRIVING WARNING MESSAGE.....	47
FIG. 26 THE RESULT OF THE CONFUSED NETSTUMBLER	48
FIG. 27 OCCURRENCES OF EACH CALCULATED WEP KEY	48
FIG. 28 WIPS INTERFERENCES WEP KEY CALCULATION	49

FIG. 29 CONCEPT DIAGRAM OF HOW WIRELESS HONEYPOT OPERATES 49

FIG. 30 SCREENSHOT OF AN ATTACKER CONNECTING TO AIRFORCE AP..... 50

FIG. 31 CURRENT CHANNEL OF THE ATTACKER..... 50

FIG. 32 WIRELESS NIC INFORMATION OF FAKEAP 51

FIG. 33 HACKER IS DIVERTED 52

FIG. 34 ALARMED SMS OVER GSM 52



List of Tables

TABLE 1 PERFORMANCE COMPARISONS OF BIG AND LITTLE ENDIAN	28
TABLE 2 MAC ADDRESS RULE.....	43



CHAPTER 1

INTRODUCTION

1.1. Motivation and Objective

Since IEEE developed the 802.11 standard to specify wireless local area networks in 1999, 802.11 related products are much common today. Wireless technology offers a more accessible and convenient means of connectivity. With the widely deployment of wireless network access around the world the requirement for a more enhanced security design emerges. The 802.11b standard for wireless networks includes a Wired Equivalent Privacy (WEP) protocol relied upon RC4 stream cipher algorithm, which is a symmetric stream cipher where both the client station and the target station share the same key for both encryption and decryption, for message confidentiality to protect link-layer communications from eavesdropping and other attacks by encrypting the data sent wirelessly. WEP keys are shared secret passwords that allow users to decode the encrypted data that travels on the wireless network. An Initialization vector (IV) is used to avoid encrypting two cipher texts with the same key stream and to produce a different RC4 key for each packet. However a lot of concerns were raised later regarding the effectiveness of WEP. However, WEP suffers from serious security flaws which arise due to the reuse of the Initialization Vector (IV).

Borisov et al. (2001) demonstrated some security flaw in WEP. They explained that WEP fails to specify how initialization vectors for RC4 are specified. They found keystreams will be reused, leading to simple cryptanalytic attacks against the cipher, and decryption of message traffic due to resetting IVs to zero when initializing the PC cards.

In 2001, Fluhrer et al. firstly showed a passive partial key exposure attack against RC4 and conjectured that their attack could be applied to WEP [1]. Later on Stubblefield et al. based on the partial key exposure vulnerability in the RC4 stream cipher discovered by Fluhrer, Mantin, and Shamir implements a practical key recovery attack on WEP [2]. Recently released tools and exploits like Airsnort and WepCrack attacked weaknesses in the 802.11 protocol and rendered these types of network highly insecure.

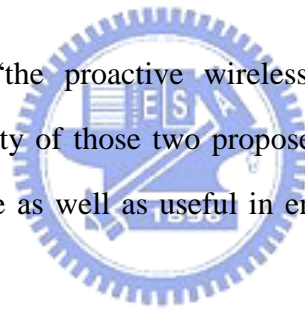
Faria et al. (2002) discussed the main wireless idiosyncrasies and the need for taking them into account when designing an access control mechanism that can be used in both wireless and wired networks. They presented the design of a mobility-aware access control mechanism suitable for both wireless and wired environments and show how the DoS attacks discussed can be prevented by implementing secure association and other essential services. Their proposed architecture proposed composed of the SIAP and SLAP protocols, uses public keys together with the RSA and AES encryption algorithms to provide a flexible service [3].

Berghel (2004) et al. assessed the extent of the security risks involved in wireless networking technology by considering three possible scenrios demonstrating vulnerabilities is discussed. The first scenario, which involves configuration WAP with SSID broadcast enabled, and no WEP enabled, is the most vulnerable case. The second scenario, which involves configuration of WAP with SSID broadcast disabled, and no WEP enabled, is the secondmost vulnerable case. The third scenario, which involves configuration of WAP with SSID broadcast disabled, and WEP enabled, is the least vulnerable case [3].

However, in it current form, WEP suffers from serious security flaws which arise due to the reuse of the Initialization Vector (IV) and the deployment of an unkeyed

checksum for message authentication. This paper attempts to enhance the security of the existing WEP protocol without changing its basic architecture. The key mechanism proposed in the paper is built on poisoning the gathering frames of attack that are deliberately tailored to generate false result. The research devised an innovative solution called Interference-Based Prevention Mechanism (IBPM). The proposed method generates interference effect by injecting spoofed frames to delude the WEP cracker resulting in inaccurate statistic. This research also proposes a proactive diversion-based wireless honeypot mechanism, within which all users are closely monitored and diverted into honeypot if one's behavior is considered to be malevolent. Under this framework, wireless honeypot is able to capture intruders even if attacks are not targeted to the honeypot.

A prototype named as “the proactive wireless prevention system” has been developed to evaluate feasibility of those two proposed mechanisms, and the research result shows that it is effective as well as useful in enhancing the security in wireless LAN environment.



1.2. Outline of This Thesis

This dissertation is organized into six chapters as follows. Chapter1 outlines the motivation and the research goal. In Chapter 2, the state of the art in the wireless security and the wireless threats are reviewed. Chapter 3 proposes an Interference-Based Prevention Mechanism which is proven effective in preventing adversaries from deducing WEP key based on weak key detection. Chapter 4 describes an proactive wireless honeypot. This proposed system is capable of protecting legitimate users and systems from attacks, by diverting attackers instead of passively attracting intruders, while collecting detailed information about each attack even if the attack is not targeted to the honeypot. Chapter 5 provides an overview of the proposed

Wireless Intrusion Prevention System architecture, as well as a set of generic service components, and elaborates the anti-Wardriving and anti-wepcracking functions of the WIPS. Finally, Chapter 6 summarizes the main contributions of this dissertation and discusses some remaining issues.



CHAPTER 2

LITERATURE REVIEW

This chapter of the dissertation looks at previous efforts of subsetting as related to both wireless security and wireless honeypot.

2.1. IEEE 802.11 Standard

Wireless LANs can be categorized as providing low-mobility high-speed data communications within a confined region, e.g., a campus or a large building. Coverage range from a wireless data terminal is short, tens to hundreds of feet, like cordless telephone. It is limited to within a room or to several rooms in a building. Wireless LANs have been evolving for a few years, but the situation is chaotic, with many different products being offered by many different vendors[17]. With the increasing proliferation of wireless LANs comes the need for standardization to allow interoperability for an increasing mobile workforce, several standard bodies are currently defining standards which impact wireless LAN systems. Of these, IEEE 802.11 and European Telecommunications Standards Institute(ETSI) high-performance radio LAN (HIPERLAN) are influential physical and data link layer standards[18]. This study investigates the handoff algorithm for IEEE 802.11 Wireless LANs, so this section introduces network architecture and MAC protocol defined by the IEEE 802.11 committee.

2.2. Network Architecture

As the system architecture of IEEE 802.11 illustrated in Fig. 1[18], a wireless LAN may consist of multiple Basic Service Sets(BSS), which are interconnected through a

distribution system via access points(AP), thus creating an Extended Service(ESS). In each BSS, a station can access the wireless medium after be associated with an AP. The members of the access point's cell execute the same MAC protocol and compete for access to the same shared medium. Two primary topologies are supported by the IEEE 802.11 standard: "ad hoc" and "infrastructure". In a infrastructure network, as illustrated in Fig. 2, stations access the backbone network(distribution system in 802.11 nomenclature) via access points. This topology is useful for providing wireless coverage of building or campus areas by deploying multiple access points whose radio coverage areas overlap to provide complete coverage. In an ad hoc network, as illustrated in Fig. 3, a group of stations directly establish peer-to-peer communication among themselves without the help of any infrastructure. This topology is useful for application such as file sharing in a conference room scenario[18]. The MAC protocol of the 802.11 standard was developed to allow these two types of topologies to coexist, as illustrated by the overlap in the coverage range of the ad hoc network and access point B in Fig. 1.

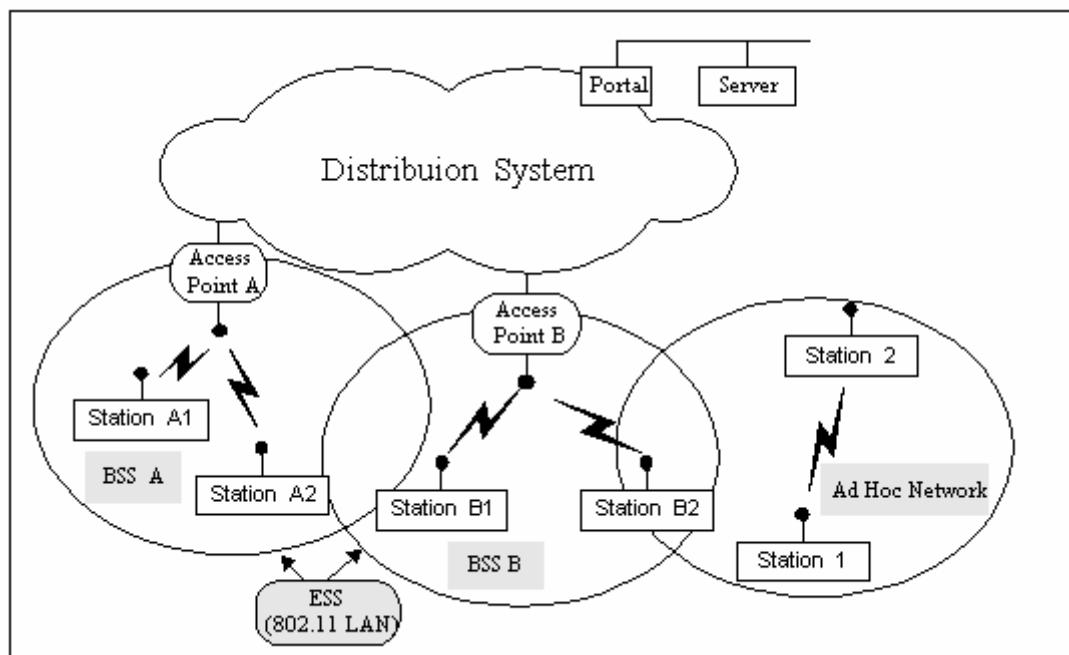


Fig. 1 System architecture of IEEE 802.11

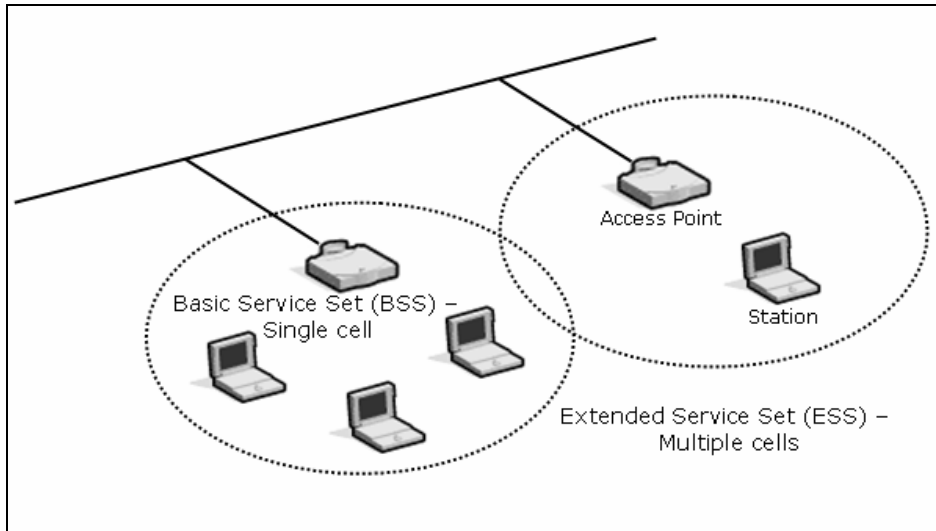


Fig. 2 Infrastructure network

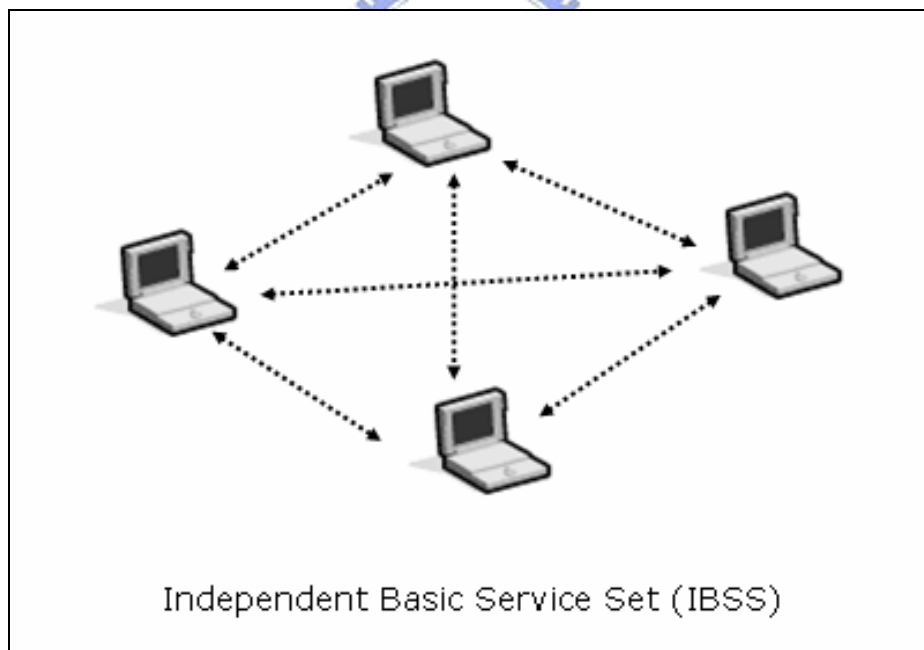


Fig. 3 Ad hoc network

2.3. Wireless security

The most prominent feature about WLAN is the absence of wires and its mobility.

As compares to the traditional network, WLAN requires no complicate configuration on its physical topology. Data transmissions are carried through radio frequency (2.4GHz spread spectrum band) between AP and its authenticated users. When data travels through air, however, it can easily be tapped by any one including unauthenticated personnel using sniffer.

As defined in IEEE 802.11b standard, WEP can be applied to encrypt data so that it becomes unreadable to the intruder. Despite the effort, WEP is now proved insecure since its key can be stolen or cracked using tools such as Aircrack-ng. In addition, most APs have their WEP setting switched off by default; and many customers usually do not spend time on reconfiguring the AP. Most APs have MAC filter as a supplementary security feature to WEP. However, keeping track of authorized MAC addresses is a time consuming and inconvenient task. Besides, some wireless cards allow users to modify its MAC address. Although the new standard 802.11i has proposed TKIP (Temporal Key Integrity Protocol) to replace WEP, majority of the users are still using 802.11b wireless card and APs. For the mean time WLAN is still considered to be vulnerable.

2.4 WLAN threats

This section is segmented in accords to each of the eight known WLAN attacks [3][10]:

2.4.1 WarDriving

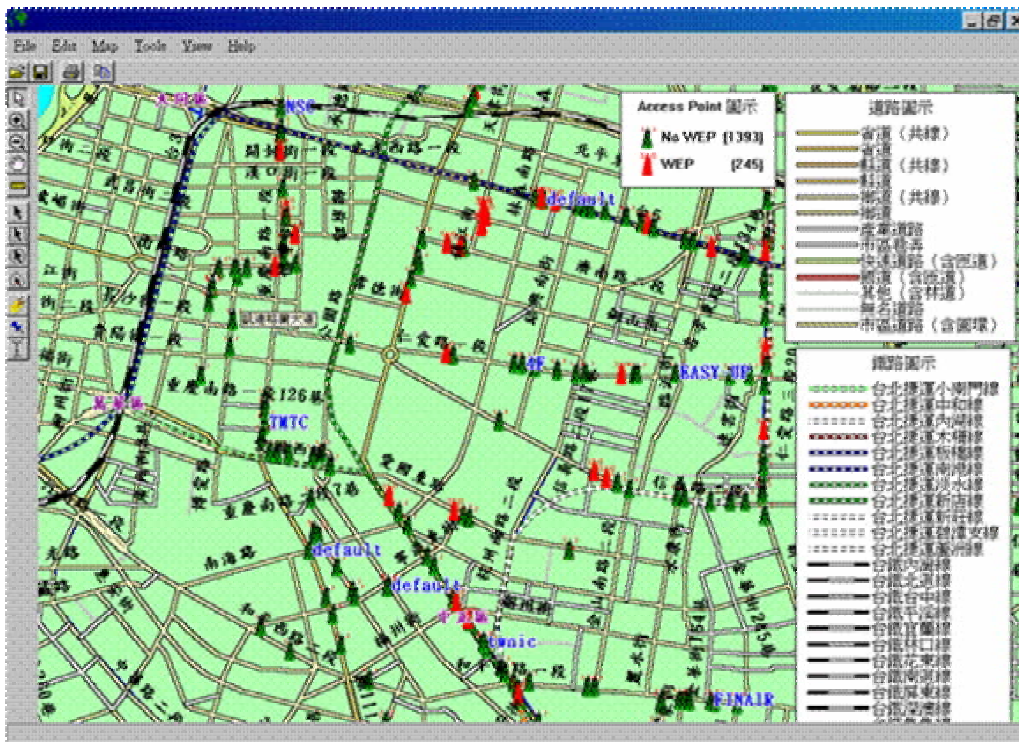


Fig. 4 Wardriving map of Taipei City

The term “Wardriving” is first coined by Pete Shipley[28]. It is an act of scanning for unsecured wireless networks with a mobile device and tools (e.g. NetStumbler & MACStumbler) that detects AP signals while driving around in a vehicle. At the same time, a GPS (Global Positioning System) device is mapping out the potential attack point (AP’s coordinates). Possible threats about War Driving include: unauthorized network access, packets sniffing, virus implanting, jamming and etc.

2.4.2 Encryption attacks

As mentioned earlier, 802.11 uses WEP to improve WLAN security. WEP is based on RC4 algorithm and serves to encrypt data. However it is recently found ineffective because skilled hackers can deduce WEP key by collecting packets that may together reveal traits about the key.

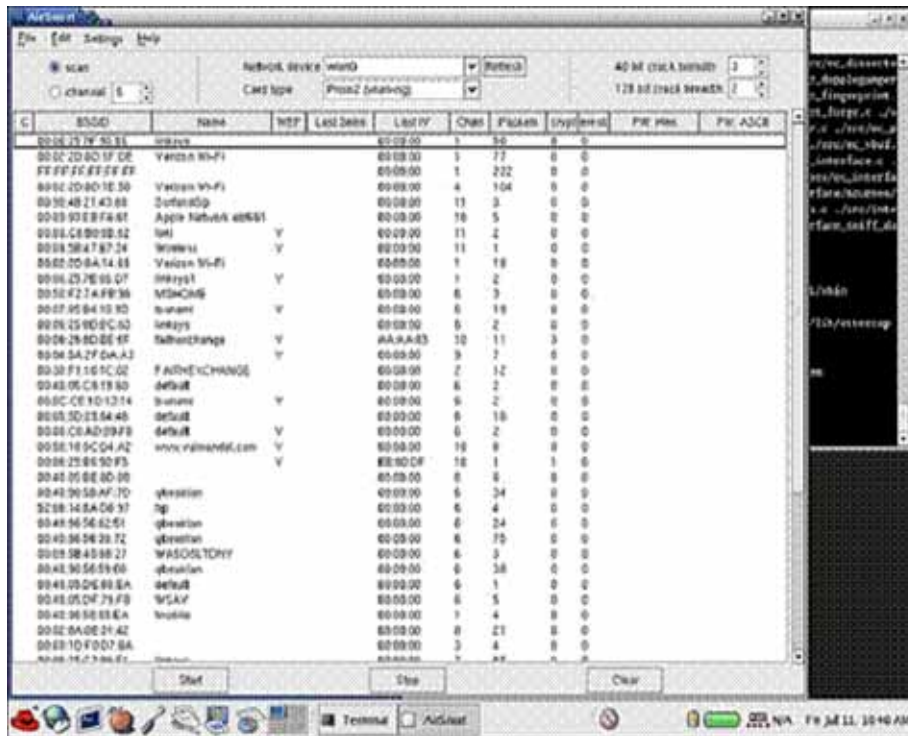


Fig. 5 Screenshot of Aircrack-ng wep cracking tool

2.4.3 Interception and unauthorized monitoring of wireless traffic

As in wired networks, it is possible to intercept and monitor network traffic across a wireless LAN. The attacker needs to be within range of an access point (approximately 300 feet for 802.11b) for this attack to work, whereas a wired attacker can be anywhere where there is a functioning network connection.

Wireless Packet Analysis: a skilled attacker captures wireless traffic using techniques similar to those employed on wired networks. Many of these tools capture the first part of the connection session, where usually includes authentication data. An intruder can then access WLAN and issue unauthorized commands in the name of the victim.

Broadcast Monitoring: from time to time, inappropriate topology significantly weakens WLAN security. If an access point is connected to a hub rather than a switch,

any network traffic across that hub are broadcasted out over the wireless network. In other words, an attacker, as one of the recipient, would be able to obtain sensitive data without even trying.

Access Point Clone (Evil Twin) Traffic Interception: an attacker deceives legitimate wireless clients into connecting to the attacker's faked AP with a stronger signal in close proximity to wireless clients. Users attempt to log into the substitute servers and unknowingly give away passwords and similar sensitive data.

2.4.4 Brute force attacks against access point passwords

Most access points use a single key or password that is shared with all connecting wireless clients. Brute force dictionary attacks attempt to compromise this key by methodically testing every possible password. The intruder gains access to the access point once the password is guessed.

In addition, passwords can be compromised through less aggressive means. A compromised client can expose the access point. Not changing the keys on a frequent basis or when employees leave the organization also opens the access point to attack. Managing a large number of access points and clients only complicates this issue, encouraging lax security practices.

2.4.5 Insertion attacks

Insertion attacks are based on deploying unauthorized devices or creating new wireless networks without going through security process and review.

Unauthorized Clients: It occurs when an attacker tries to connect a wireless client to an access point without authorization. Since WLAN does not constraint users to physical connection ports, users are able to access the AP anywhere when its security

setting is switched off.

Unauthorized or Renegade Access Points: An organization may not be aware that internal employees have deployed wireless capabilities on their network. This lack of awareness could lead to the previously described attack, with unauthorized clients gaining access to corporate resources. Organizations need to implement policy to ensure secure configuration of access points, plus an ongoing process in which the network is scanned for the presence of unauthorized devices.

2.4.6 Jamming

Jamming is considered to be a type of denial of service on WLAN. Traditional DoS attacker floods target with tremendous amount of bogus traffics to bring down its performance and keep it from operating normally. Jamming occurs when WLAN hackers corrupting the signal until the wireless network ceases to function using certain equipment and tools to flood the 2.4 GHz frequency.

In addition, any devices that operate on the 2.4 GHz band can disrupt a wireless network using this frequency. These denials of service can originate from outside the work area serviced by the access point, or can inadvertently arrive from other 802.11b devices installed in other work areas that degrade the overall signal.

2.4.7 Client-to-Client attacks

Two wireless clients can communicate directly to each other, bypassing the access point. Users therefore need to defend clients not just against an external threat but also against each other.

Wireless clients running TCP/IP services such as a Web server or file sharing are open to the same exploits and misconfigurations as any user on a wired network. A

wireless device floods other wireless client with bogus packets, creating a denial of service attack. In addition, duplicate IP or MAC addresses, both intentional and accidental, can cause disruption on the network.

2.4.8 Misconfigurations

Occasionally negligence is the main cause of assaults. Many people take convenience for granted, and actually deploy WLAN without taking security into account. For instance, organizations tend to use default settings. Also, administrator needs to configure each individual AP based on its physical location and purpose.

2.5. Wired Equivalent Privacy (WEP)

The concept of WEP is to prevent eavesdroppers by encrypting data transmitted over the WLAN from one point to another. Data encryption protects the vulnerable wireless link between clients and access points; that is, WEP does not offer end-to-end security because AP decrypts the frames before passing them to destinations that are beyond WLAN.

WEP adopts RC4 algorithm, a stream cipher, developed by RSA security. “A stream cipher operates by expanding a short key into an infinite pseudo-random key stream. The sender XORs the key stream with the plaintext to produce cipher text. The receiver has a copy of the same key, and uses it to generate identical key stream. XORing the key stream with the cipher text yields the original plaintext”[4]. In other words, RC4 is a symmetric algorithm relies on a single shared key that is used at one end to encrypt plain text into cipher text, and decrypt it at the other end [7].

Current WEP implementations support key length up to 64 bits and 128 bits; technically,

the key length of both version are shorten by 24bits due to the use of plaintext Initial Vector (IV). In this research context, a key (or key combination) is a series of ASCII bytes often presented in hexadecimal; whereas a key value is one byte (8bits) out of the total combination. Fig. 6 shows a WEP encrypted frame which consists of IV(24 bits), padding(6 bits), key index(2 bits), encrypted message and Integrity Checksum Value (ICV)(32 bits). Note that the frame is transferred with the first 32 bits in plaintext and the rest of the body encrypted. This is because a sender generates IV, either incrementally or randomly, as part of inputs to encryption process. That is, the receiver must know the exact IV to decrypt the frame.

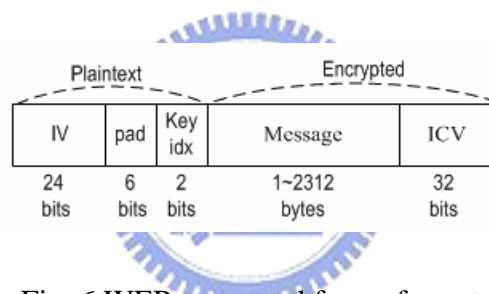


Fig. 6 WEP encrypted frame format

As indicated by the length of key index in the diagram, WEP can have up to 4 (22) keys. However, using shared static keys can be dangerous. Therefore, the purpose of constantly changing IV is to achieve the effect as if having a greater number (224) of key combinations. This gives WEP the capability of encrypting each frame with different keys (known as packet key).

Fig. 7 illustrates WEP encryption process which starts by generating IV and selecting a predefined key. Next, RC4 uses both IV and chosen key (k) as inputs to generate key stream. Then, plaintext message (M), along with its ICV, is combined with

key stream through a bitwise XOR process, which produces ciphertext (C). Upon sending the encrypted frame, WEP appends IV in clear to the front of the frame. The encryption process can be summarized as following formula.

$$C = (M, \text{crc32}(M)) \text{ XOR RC4}(IV, k)$$

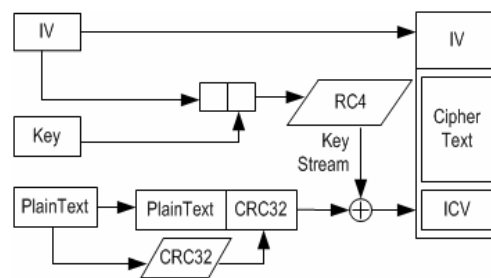


Fig. 7 WEP encryption process

To decrypt, the receiving station uses the first 32bits IV and the shared key (k) as indicated by key index bits to generate the same key stream that encrypted the frame. Next, WEP XOR key stream with ciphertext (C), along with it ICV, to retrieve the plaintext (M). Note that, plaintext has ICV attached at the end. Finally, WEP computes plaintext, without ICV, CRC32 and compares the output with the ICV.

Wireless environment is prone to interference; hence, data may be lost or damaged before reaching the destination. To ensure data integrity, sender computes CRC32 against the plaintext message and inserts the output (32 bits) at the back of the message prior to encryption. The receiver ensures data integrity by matching ICV of decrypted frame with the CRC32 result done locally with the resolved message. Frames with disconfirmed checksum will be discarded. The decryption process can be summarized as following formula based on the encryption formula.

$$(M, \text{crc32}(M)) = C \text{ XOR } \text{RC4}(\text{IV}, k)$$

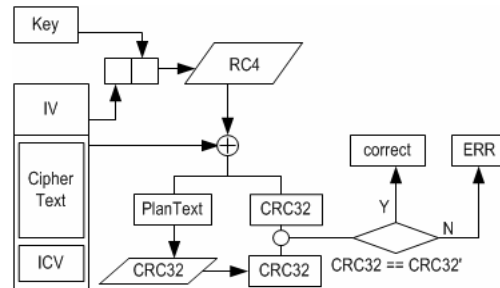


Fig. 8 WEP decryption procedure

2.5.1. WEP Vulnerability

Though combining IV into key stream computation increases key complexity so that it appears unpredictable, the reality that IV has to be transferred in clear may divulge WEP key. Such vulnerability is first discovered in a research undertaken by Fluhrer, Martin and Shamir[1] which states that IV . Specifically, frames with IV that matched (B+3, 255, X) form, where B points to the position of the key value in the combination and X can be any value between 0 and 255, may reveal key values. The probability of retrieving the right key value from the frame is 5%. Give sufficient time and traffic, one is able to obtain the WEP within hours or days. For instance, an IV (4, 255, 31) may resolve the value of the K[1], where IV (7, 255, 72) may resolve the K[4] (Fig 9). Often, attackers determine the key combinations by running statistic on all the potential key values computed from frames that matched such pattern.

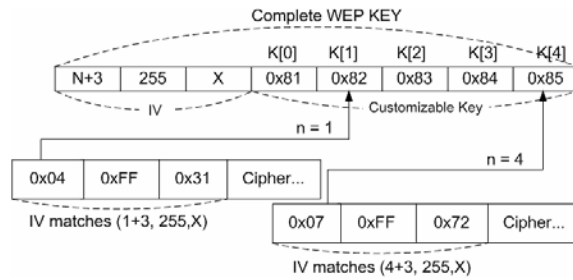


Fig. 9 IV pattern resolving key combination

Part of the key value extracting concept is based on the nature of XOR. Suppose C is the result of P XOR K, then we are able to retrieve K by XOR C with P. In the case of WEP, the idea is extended and is much complicated due to RC4 algorithm; nevertheless, the fundamental idea is the same. That is, the initial step of cracking WEP key is to obtain ciphertext with its matching plaintext, which is almost readily available. As defined in 802.11 standard, any frames of type ARP or IP has to begin with 0xAA (known as SNAP). In IPX environment, 0xFF or 0xE0 is used instead. In fact, majority of the data transferred in WALN is in either format.

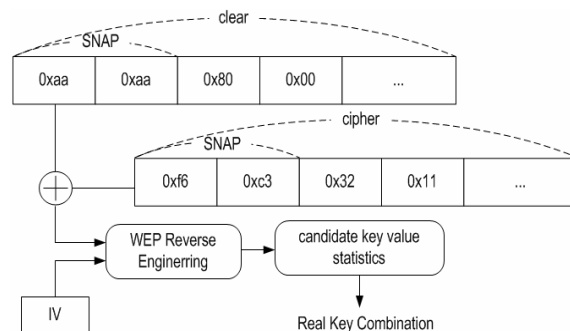


Fig. 10 XOR plaintext and ciphertext to resolve key value

All in all, to crack WEP, one must first capture as much frames that matched the specified pattern as possible. Then, for each of the captured frame, XOR the first byte of the ciphertext with 0xAA to obtain the exact key stream that were used during encryption. By reverse-engineering RC4, attacker would be able to retrieve the key value (Fig 10). Please refer to Fluhrer's study for detailed explanation on specific algorithms. Seth Fogie has published an article which describes detailed steps of WEP cracking. Also, WEP attack implementation can be found in the research done by Stubblefield et al [2].



CHAPTER 3

THE INTERFERENCE-BASED PREVENTION MECHANISM

Obviously, the major flaw that makes WEP vulnerable is the fact that attacker is able to extract key from the gathered frames. Usually, statistics is used to assists in determining the real key values from the candidates. The real key value often has the highest occurrence among all. Therefore, it is reasonable to conclude that the resulting key is based on the amount and quality of the frames. That is, the attacker is unlikely to get the right key combination if traffic is scarce or there are more frames resulted in false key values than that of the right ones.

Since it is impossible and unreasonable to prevent WLAN traffics from increasing, we propose that the alternative to prevent attacker from getting the correct key value is by poisoning the traffic with frames that are deliberately tailored to generate false result.

Based on the understanding of the frames that the attackers are interested in and the algorithms applied to retrieve the key, this research devised an innovative solution called Interference-Based Prevention Mechanism (IBPM). As implied by its name, the proposed method generates interference effect by injecting spoofed frames to delude the attacker resulting in inaccurate statistic. As a matter of fact, injecting frame increases traffic load. Present WLAN bandwidth is still limited; hence, there must be an effective and space-efficient method to poison the traffic.

IBPM utilizes the same technique similar to WEP crackers. That is, IBPM monitors the

traffic and keeps computing the key values. The difference is that IBPM is implemented in a client station within a WEP protected WLAN; therefore, it is assumed that IBPM station possesses the key as a legitimate user. Having the key gives it the capability of interfering network traffic in advance. Fig. 11 shows IBPM generates spoofed frames whenever the speculated key value matches the real key value (we refer such event as weak-key occurrence). Consequently, the automated statistic program at the offense side takes those frames into account and increments false key values. What actually happened is that, IBPM pollutes attacker's statistic in a way that causes false key values to increase to prevent real key value becoming distinct. Since IBPM has disrupted the statistic long before it reveals the real key value, WEP is, therefore, secured. This chapter discusses the proposed prevention schemes, which are discussed under interference schemes section, to distribute spoofed frames that generates false key across all possible key values.

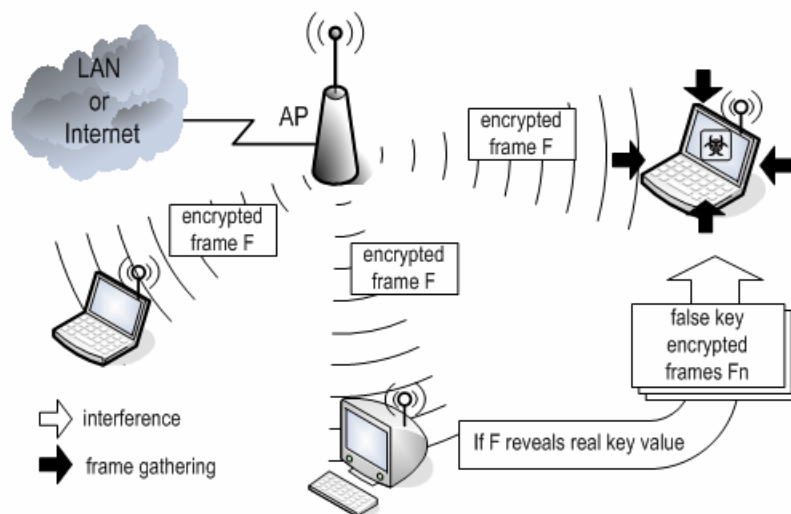


Fig. 11 Interference generation diagram

3.1 The Proposed Interference Schemes

The effect of interference is accomplished by increasing the tally of false key value whenever a weak-key is detected by IBPM. For instance, a weak-key 0xBB is detected, one may decide to increase all false-key tallies range from 0x00 to 0xFF excluding 0xBB. However, incrementing the tally arbitrarily incurs flaw that may eventually allows the attacker to discern the fixed pattern in the resulted statistic. Interference not only conceals the key, but also should prevent attackers from speculating the key based on the spoiled statistic again. The algorithm of IBPM is described as follows:

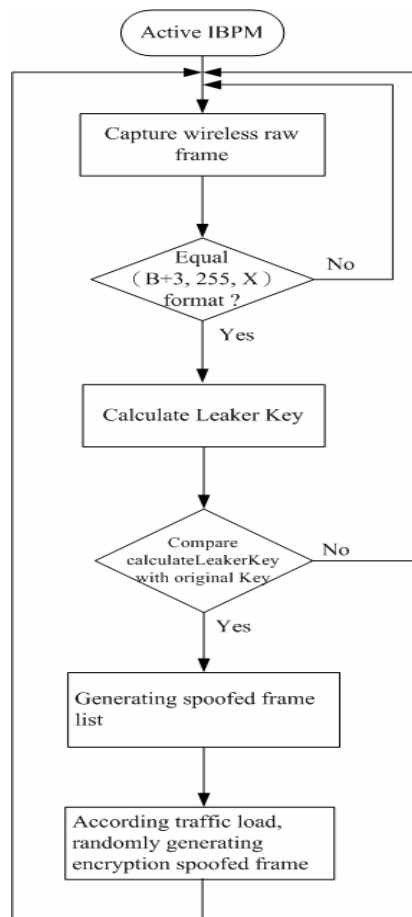


Fig. 12 IBPM Interference procedure

```

SET WEP_Key to [5 or 13]
SET Weak_IV to [3...15, 255, any]
SET WEP Key's leakers to WEP key's calculateLeakers

```

Main Procedure WEP_Interference

```

While (true)
  CALL Sniffing RETURNING Frame
  IF Frame is ENCRYPTION THEN
    CALL getInitVector with Frame RETURNING IV
    CALL getData with Frame RETURNING Data
    IF IV is Weak_IV THEN
      CALL calculateLeaker with IV, Data[0] RETURNING Leaker
      IF Leaker is WEP Key's leakers THEN
        CALL Weak_Key_Interference with Leaker
      End If
    End If
  Else
    Break
  End If
End While

```

Procedure calculateLeaker(IV, Data)

```

BEGIN
  # 802.11 SNAP Header should be 1st plaintext byte of WEP packet
  SET Text to 0xaa
  SET Range to 256
  SET Schedule_List to [0...255]
  SET tmp_Schedule to [0, 1]

  key_List[0] = IV[0]
  key_List[1] = IV[1]
  key_List[2] = IV[2]

  SET Encr to IV[3]
  SET loopIndex to 0
  SET arrayIndex to 0

  FOR loopIndex = 0 to key_List[0]
    arrayIndex = (arrayIndex + Schedule_List[loopIndex] + key_List[loopIndex]) MOD Range
    SWAP Schedule_List[loopIndex], Schedule_List[arrayIndex]
    IF loopIndex = 1 THEN
      tmp_Schedule[0] = Schedule_List[0]
      tmp_Schedule[1] = Schedule_List[1]
    END IF
  END FOR

  SET Condition to Schedule_List[1]
  SET Leaker to INTEGER
  SET XORvalue to INTEGER

  IF (Condition < key_List[0]) THEN

```



```

        IF ((Condition + Schedule_List[Condition]) = key_List[0]) THEN
            IF (Schedule_List[0] <> tmp_Schedule[0]) or (Schedule_List[1] <> tmp_Schedule[1])
THEN
                PRINT "IV error" #Initial Vector Error
            END IF
            XORvalue = int(Encr) XOR Text
            Leaker = XORvalue - arrayIndex - Schedule_List[loopIndex + 1] MOD Range
        END IF
    END IF
    RETURN Leaker
END

```

```

Procedure Weak_Key_Interference
BEGIN
    SET interfereCount to 255
    SET tmpData to ""
    FOR frame = 0 to interfereCount
        SET ram_leaker to random.randrange(0,255)
        IF ram_key <> WEP_key THEN
            CALL Scrambling with Weak_IV, ram_leaker RETURNING tmpData
            CALL send_encrypt_dataframe with socket, channel, interface, bssid, destMac, srcMac,
IV, tmpData, tmpData's Length
        END IF
    END FOR
END

```



3.2 The Scenario of the IBPM

This scheme randomly selects any amount of key values from the false set. The increment scale can also be any number. However, it is recommended to use a scale less than or equals to 3, because drastic change may ultimately cause the real key value to become the least and apparent. The scale can also be randomly assigned given a specified range.

As mentioned earlier, IBPM requires no change on the legacy network configuration and is compatible to any WEP-enabled 802.11 WLAN. The IBPM-enabled device (preferably a desktop PC) appears just like any other regular wireless clients; therefore, attackers are unlikely to realize the intension behind such deployment. As shown in IBPM system framework (Fig 12), IBPM joined the WLAN

as a member client station which issues bogus frames upon weak key occurrences. At the same time, the attacker, being unaware of the spoofed frames, keeps gathering the frames.

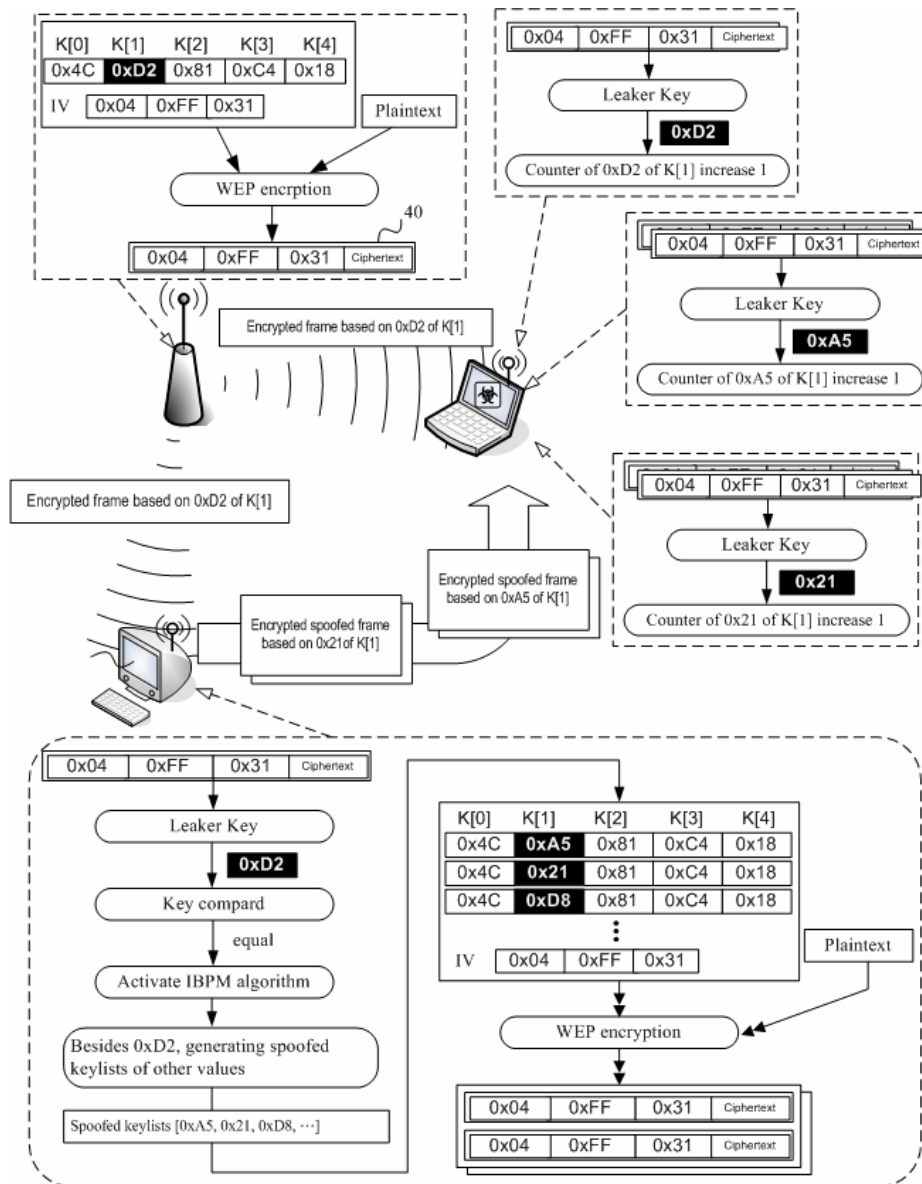


Fig. 13 IBPM Interference procedure

IBPM involves both proactive and passive activities which include traffic sniffing and injection. Presently, this research has implemented an experimental system under

Linux. Various wireless drivers are available in the open-source community [11] with each offers slightly different capabilities. This research has modified and integrated some of the drivers in achieving features to support both monitor WLAN traffics and send frames with arbitrary format, including WEP encrypted, through individual wireless network interface cards.

This research implemented IBPM using Python and C libraries under Redhat 9 Linux. The IBPM machine is equipped with two wireless network interfaces: one for sniffing frames and the other is used to inject spoofed frames whenever weak-key is detected.

3.3 Statistical Diagrams of WEP cracking and Anti-WEP cracking

To demonstrate the effectiveness of IBPM, two independent WEP attacks were launched against the experimental WLAN in the lab. At the end of each attack, the offender's statistical result is captured. This demonstration adopted perfect probability interference scheme. Since WEP-128 is as vulnerable as WEP-64 despite of its extended key length, therefore WEP-64 is applied just to illustrate the concept due to space limitation. AP is configured with WEP key setting as $K = \{76, 210, 126, 196\}$ and 24. Fig. 13 shows the result of the statistical result of the first attack without IBPM. Note that the thick line indicates the real key value.

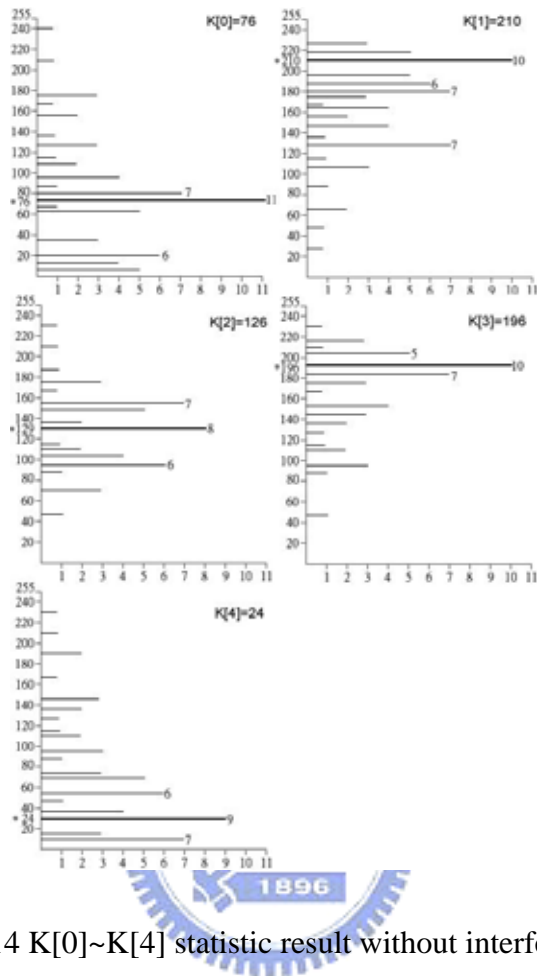


Fig. 14 K[0]~K[4] statistic result without interference

Clearly, the attacker can easily points out the real key value based on the statistical result. Evidently, each of the real key value stands out prominently. In contrasting to the previous test, the result captured in the second experiment with IBPM conceals the real key values (Fig 14). In addition, the overall distribution is almost random and there is no fixed pattern to follow. As for better observation, we deliberately thicken the line of the real key. In reality, the attackers will not be able to determine the real key value from such random formed statistical result.

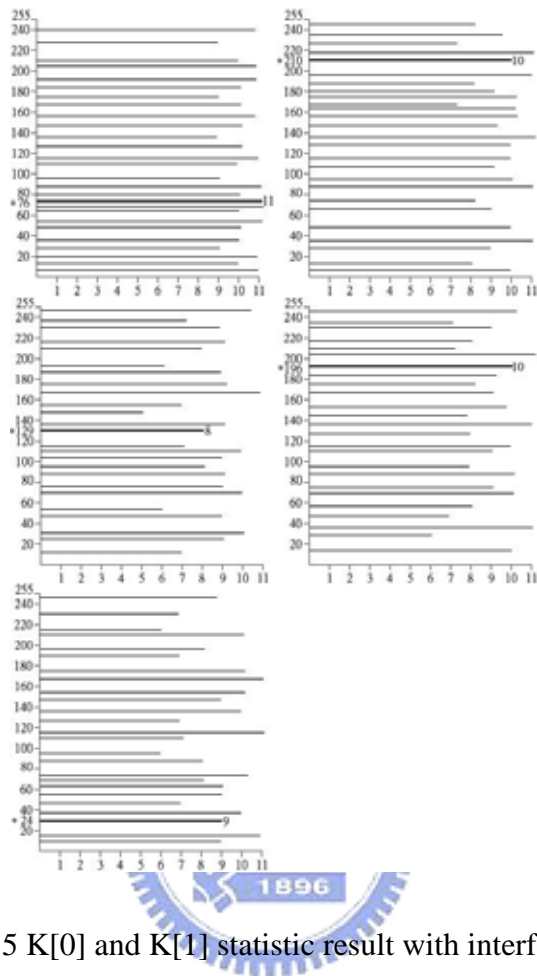


Fig. 15 K[0] and K[1] statistic result with interference

3.4 Performance Evaluation Results

In this section, the impact of key parameters on the actual interference performance of wireless LAN is discussed. The major two parameters considered in our discussion included the endian of IVs and the encrypted key length of WEP.

3.4.1 Analysis of IVs Generated by a Little Endian Counter

If the IVs are generated by a multibyte counter in little endian order (IV[0] the first byte of the IV increments the fastest), then the attacker must collect IVs of the form (N,255,X) for $2 < B < 16$. If he collected these for 60 different values of N, then he can

derive the secret key with little. This requires approximately 4,000,000 ($60 \times 256 \times 256 = 3,932,160$) packets. The influenced traffic load depends on the key length of WEP secret key. If the length of key is 5 bytes, the number of generated interference raw frame counts for $60 \times 5 \times 5 \times 255 = 3285$ packets. Otherwise if the length of key is 13 bytes, the number of generated interference raw frames counts for $60 \times 5 \times 13 \times 255 = 9945$ packets.

3.4.2 Analysis of IVs Generated by a Big Endian Counter

If the IVs are generated by a multibyte counter in Big endian order (IV[2] the first byte of the IV increments the fastest), then the attacker must collect IVs of the form (N, 255, X) for $2 < B < 16$. If he collected more than 60 different values of N, then he can derive the secret key with little. This requires approximately 4,000,000 ($16 \times 256 \times 256 = 1,048,576$) packets. If the length of key is 5 bytes, the number of generated interference raw frame counts for $256 \times 5 \times 5 \times 255 = 16,320$ packets. Otherwise if the length of key is 13 bytes, the number of generated interference raw frames counts for $256 \times 5 \times 13 \times 255 = 42,432$ packets.

Table 1 Performance Comparisons of Big and Little Endian

IVs generated counter	Little endian counter	Big endian counter
Required number of captured packets	Approximately 4,000,000 ($60 \times 256 \times 256 = 3,932,160$) packets	Approximately 1,000,000 ($16 \times 256 \times 256 = 1,048,576$) packets

Raw frame capture time(traffic average 200 packets/s)	Approximately 55.6 hours	Approximately 13.9 hours
Generated interference packets	$60 * 5\% * 5 * 255 = 3825$ $60 * 5\% * 13 * 255 = 9945$	$256 * 5\% * 5 * 255 = 16,320$ $256 * 5\% * 13 * 255 = 42,432$



CHAPTER 4

THE PROACTIVE WIRELESS HONEYPOT

4.1. Introduction

Unlike other protection mechanism (such as firewall and IDS), honeypot is capable of both protecting systems by means of diverting attackers into a non-production system and collecting information about their habitats, intentions, potential targets and tools used. Presently, majority of the prior honeypot researches are concentrating on traditional wired network environment. With the increasing need of mobile communication and public acceptance on adopting wireless technology, it is necessary to extend the concept over WLAN (Wireless Local Area Network). In contrasting to traditional wired network, WLAN transmit data over radio frequency which can incur security problems due to data exposure. However, without additional protection, any AP (access point) can become an open gate to attackers. To further enhance security measures, much has to be learnt from the attackers. Therefore, the purpose of this research is to design and implement an active wireless honeypot under 802.11b standard. This proposed system is capable of protecting legitimate users and systems from attacks, by diverting attackers instead of passively attracting intruders, while collecting detailed information about each attack even if the attack is not targeted to the honeypot.

4.2 Honeypot

4.2.1 Definition of Honeypot

Researches and technologies related to Honeypots have attracted public's attention in recently years. As Lance Spitzner defined, a honeypot is expected to get probed, attacked and potentially exploited. Honeypots do not fix anything. They provide us with additional, valuable information. The capability of collecting direct, concise and observable information is the greatest advantage honeypots have over other information gathering techniques. A honeypot can be actual computers with actual services or service simulators designed to mimic vulnerable systems, as entrapments. In fact, a honeypot can be regarded as deceptive device and information collector.

Honeypot does not work along; like any other production systems, it is always recommended to have firewall and IDS installed. Firewall provides protection and data control while IDS is mainly designed to detect known signatures and anomalies to reduce manual analysis. Both technologies are capable of gathering information through packet sniffing and events logging. These additional data can help security officers to draw a better picture of the attacks.

4.2.2 The Development State of Art

In fact, the idea of honeypot has been realized for some time and several products are available in the market. However, each of them has advantages and disadvantages. This section lists some of the commercial honeypots with each followed by a short description on its features.

- CyberCop Sting: CyberCop Sting, a product from Network Associates Inc., is a collection of security tools which includes CyberCop Monitor and

CyberCop Scanner. Sting can simulate a realistic network environment and its consisting components such as Windows NT server, Unix server and routers. It is capable of both detecting and logging attack events.

- NFR Back Officer Friendly[12]: Known as a "honeypot" for its ability to attract and trap hackers, Back Officer Friendly (BOF) is free and downloadable from NFR Security, Inc. BOF was once a tool used to detect scan attempts against targeted machines using Back Orifice. Presently, it supports several service traps such as Telnet, FTP, SMTP, POP3 and IMAP2. Traps are nothing but port listeners that responds upon receiving requests. When BOF receives a request for service, it will fake replies to the hopeful hacker. The primary goal is to distract attacker's attention from the actual production system.
- Deception Toolkit:Deception Toolkit is a customizable vulnerability simulation bundle developed by Fred Cohen. In times of port scanning, a machine running DTK can appear to attackers as if the system has a large number of widely known vulnerabilities. That is, DTK can waste the attacker significant amount of time on just trying to find out which ones are real. For well protected system, there can be none. The purpose is to discourage the adversaries.
- Specter:Specter is a commercially supported product, developed and sold

by a Swiss company Netsec. Specter is classified as low-interaction honeypot with no actual operation system involved. It supports both traps and service simulation. Specter offers service simulation that provides basic interactive environment for the attackers.

The honeypots listed above are all low-involvement, which may certainly reduce risk. However, it also means little information can be gathered from interactions. With the exception of CyberCop Sting, these honeypots provides little or no interactive features that may encourage more interactions from the attacker. Most importantly, all of them do not support WLAN, which has becoming an essential part of any organizations.



4.3. Proactive Diversion Procedure

Within 802.11 WLAN, connections between clients and servers are established by AP. In an opened network, whereby AP accepts all connections, once AP recognizes clients' SSID no further authentication is required. However, in a closed network, WEP key exchange is a compulsory procedure during authentication stage to verify user identity. For simplicity, the following section omitted concepts and details concerning WEP key exchange.

Fig. 15 is an over view of connection process of a user accessing network through an AP. Basically, these processes can be grouped into two stages. In stage 1, client broadcasts probe request frame in querying for an available neighboring AP. Upon

receiving probe request, AP would first verify the user by examining whether its SSID matches with that of the current setting. Once matched, AP would regard the user as one of the WLAN member. Next, AP replies the requester with probe response frame to notify the user about its existence. Probe response frame header includes source, destination and currently occupied channel. Before establishing a connection, AP requires further identity verification, whereby authentication frames are exchanged between the user and AP. At last, user associates with AP.

In stage 2, after association frame exchange, user is then able to access network resources through AP. The association is sustained until client or AP issues disassociation frame.

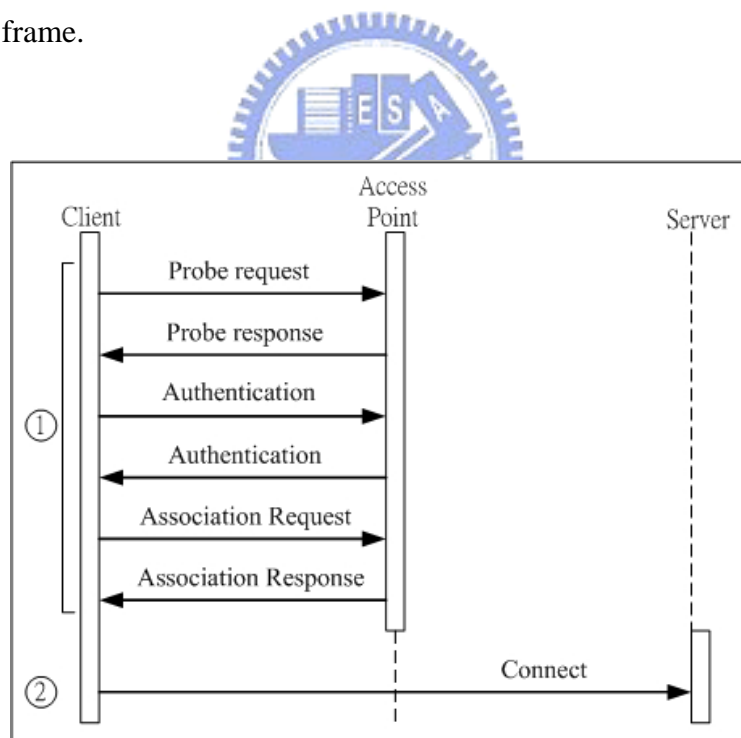


Fig. 16 connection process of legitimate users

Fig. 16 shows an attacker being diverted into honeypot. The diverting process of

the proposed wireless honeypot involves client(attacker) 、 server(destination) 、 AP 、 WIPS 、 FakeAP and honeypot. Note that WIPS is a device within WLAN that monitors wireless traffics for known attacks (signatures). Similar to the legitimate user in figure 1, client needs to go through discover, authentication and association processes before connecting to server (stage 1, 2).

Next, client launches attacking server at stage 3. As soon as WIPS discerns unusual events, it starts sending disassociation frame to the attacker and prevents it from reconnecting with the AP. At the same time, WIPS activates FakeAP in preparing for processes that follows (stage 4).

At stage 5, when client encounters interference that forces it to disconnect from AP, it would automatically begin searching for a new AP by broadcasting probe request frames using another channel. FakeAP replies the attacker with a faked probe response to make it into believe that it has found a real AP when in fact this FakeAP will not actually deliver its request to the destination but honeypot. The process of redirecting attacker from real target to honeypot is defined as “active diversion”.

Finally, attacker would be diverted into honeypot whereby all events will be recorded and all damages do not affect production system.

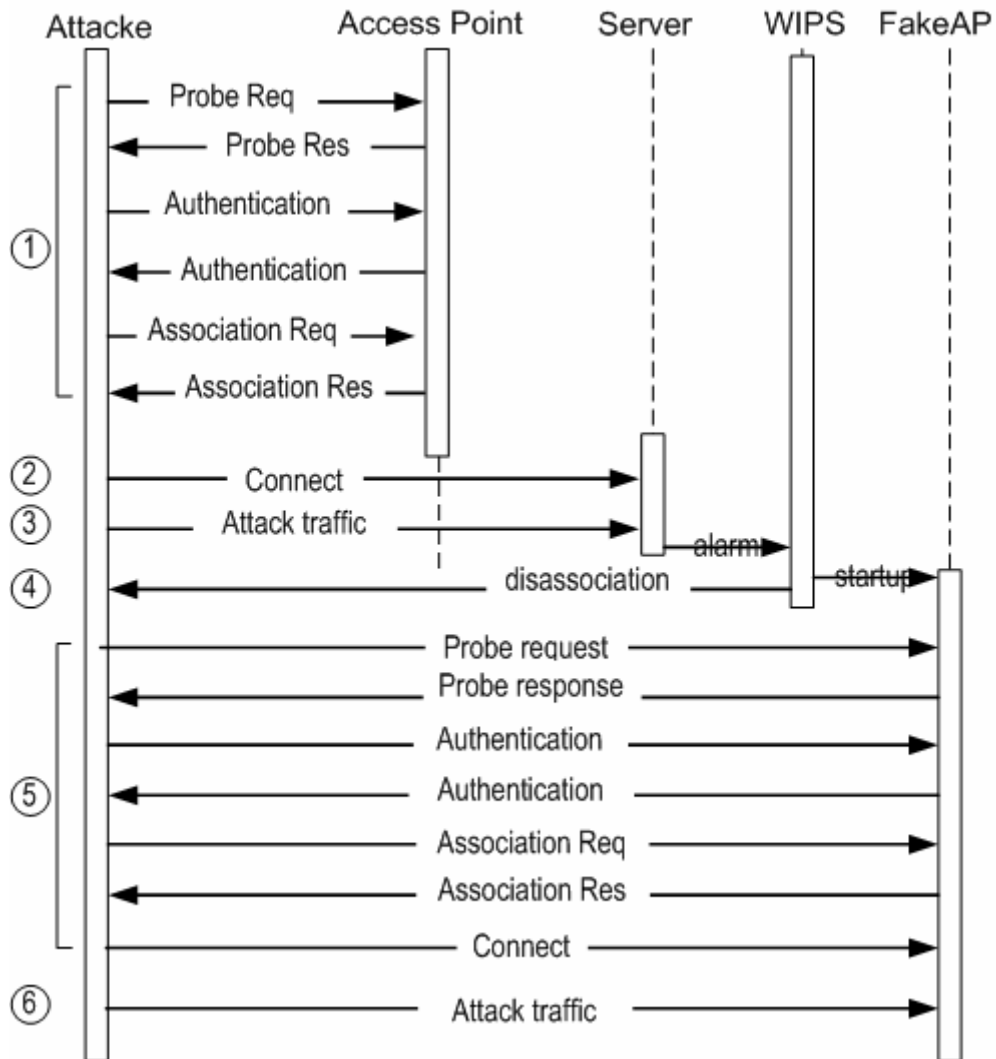


Fig. 17 diverting attacker into honeypot

4.4. System Framework

In contrast to simulation-based honeypot, this research attempts to build a high-involvement wireless honeypot equipped with real operation system and services utilizing VMware.

VMware is software that is capable of creating working environment for various types of operating systems on a single host despite of its platform. Currently, it

supports Windows, Linux, FreeBSD, Solaris and Mackintosh; therefore, it has become a convenient alternative for implementing honeypot. However, the host running virtual machine must allocate large memory and disk space and works fast enough to efficiently handle the operations from both the VMs and the host itself.

There are several advantages on using VMs as honeypots. First of all, one can have several honeypots on just a single machine without additional spending. Secondly, different types of operating system can be switched and replaced easily. Third, VMs are stored as files on the host machine; which means backups can be made. Fourth, when a virtual honeypot is compromised, it can be recovered by simply replacing with its backup file. Most importantly, it is difficult for a hacker to differentiate an actual machine and a virtual machine.

Wireless honeypot consists of WIPS (Wireless Intrusion Prevention System) , FakeAP and a honeypot (built by VM). The overall activities are: (a) monitoring, (b) divertsion and (c) logging.

WIPS is responsible for monitoring unusual events and activating redirection procedure. FakeAP, as implied by the name, is a temporal special purpose AP that specifically designed to divert attacker's traffic into honeypot. Honeypot is the device/environment that interacts with the intruder while recording every single event that occurred.

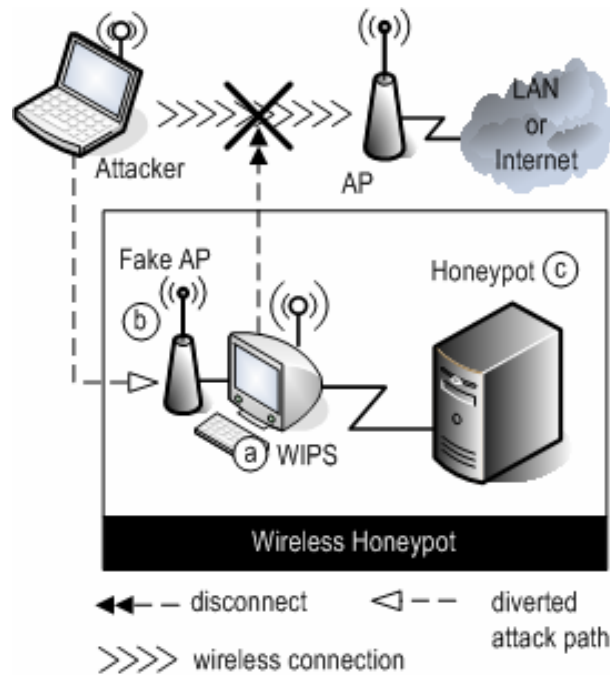


Fig. 18 framework of the proposed wireless honeypot

4.4 System Procedure

The overall operation of the proposed wireless honeypot is as follows:

1. Once attack is detected, WIPS terminates the connection between the offender and the AP through which illegal activities were carried out. To prevent the attacker from reconnecting with the AP, WIPS keeps sending disassociation frames until it gives up trying.
2. At the same time, WIPS activates FakeAP on a different channel with the same SSID that used by the original authentic AP. To prevent legitimate user from entering honeypot, FakeAP is configured so that it only accepts connections from the detected hackers.
3. The fact that FakeAP using same SSID as the original AP makes attacker into believe that he/she is still connecting through the same AP. Often, wireless

network card tend to look for new AP when disconnected or interfered. In such case, attackers are unlikely to find out the difference even after been forced to disconnect from the AP.

4. Finally, FakeAP diverts attacker into honeypot whereby any movements made will be logged. These collected information provides details, such as intruder techniques used, habitats, interested targets, that serve as learning material and crucial evidence.



CHAPTER 5

THE PROACTIVE WIRELESS INTRUSION PREVENTION SYSTEM

5.1. System Architecture and Design

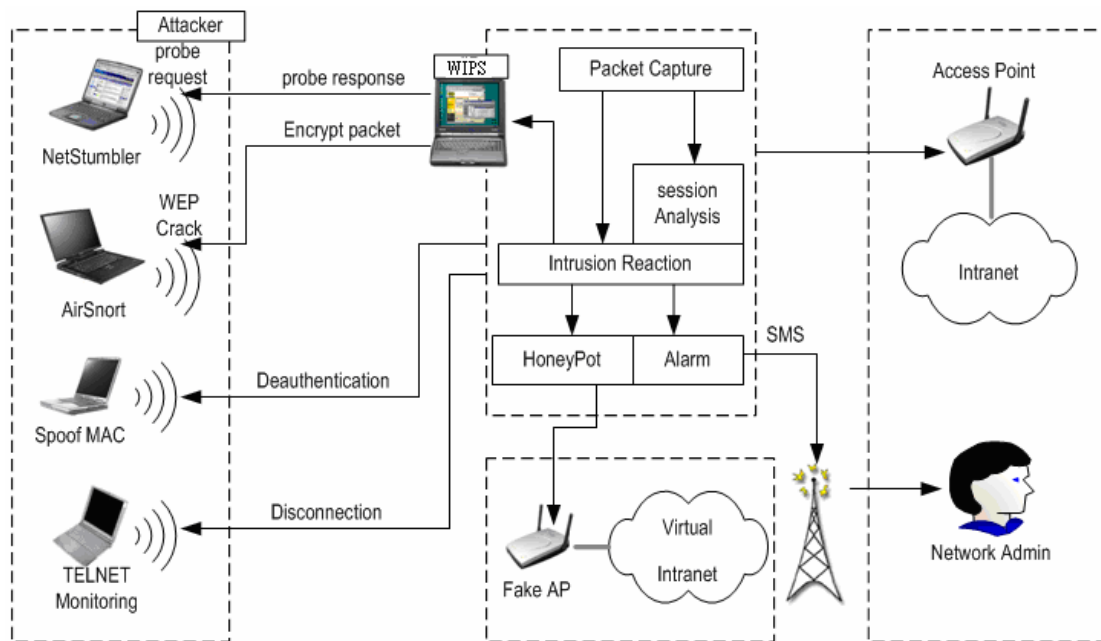


Fig. 19 proactive wireless IPS architecture

As shown in the system framework (Fig. 18), the proposed WIPS is able to protect network from Wardriving and WEP cracking attacks. Also, with each different types of attack, a proper response mechanism is designed to prevent protected-users on Intranet from further damage. This system component consists of five modules: packet capture, session analysis, intrusion reaction, honeypot and alarm module. Packet capture module collects and stores wireless packets for future analysis and reference. Session analysis module sorts packets into logical order in accords to its protocol and session. Intrusion reaction module monitors traffics and responds to offensive behaviors. Honeypot module is a mechanism designed to redirect intruder into a faked AP so that

risk is shifted to a non-production network. Alarm module takes charge of informing network administrator through GSM message service in times of attack.

5.1.1. Packet Capture Module

This module collects wireless frames using Airjack library and stores them into an audit file if requested. Airjack is an open-source library, that supports Prism 2 chip network cards, provides frame capture and injection interfaces. The gathered frames will then be utilized by session analysis module or intrusion reaction module.

5.1.2. TCP Session Analysis Module

Traditional packet analyzer focuses solely on its structure and characteristics. Consequently, the result is usually a list of raw packets sorted by its collected time; therefore, no distinct relationship is established between them. Hence network administrator would not be able to utilize this information efficiently. In order to overcome this obstacle, it is necessary to design an algorithm to rearrange the packets into individual session groups. TCP session analysis module is specifically designed to serve that purpose. As defined in IEEE 802.11 standard, there are three types of frames that must be recognized in WLAN:

- Management Frames: WLAN uses these frames to perform authorization and establish connections between AP and clients.
- Control Frames: they are responsible for media access control.
- Data Frames: they are used to deliver data.

5.1.3. Intrusion Reaction Module

It is crucial to respond to the offensive activities immediately after they are detected

by the system. Intrusion reaction module takes such role in handling procedures to prevent further damage. The service type and functions provided by this module include:

5.1.3.1 Anti-Wardriving

Before connecting to a WLAN, client device must first find an AP either by listening for AP's beacon or broadcasting probe requests consecutively. As stated in 802.11, AP must reply a probe response, as to inform its existence, to the client that issues the request to establish connection. War-Driving takes the advantage of such vulnerability to scan every AP within reach by broadcasting probe request frames. Two indicators are used in War-Driving detection:

NetStumbler is the most popular tool for War-Driving. However, it is possible to detect NetStumbler, because it always sends out a special packet whenever an AP is detected. This packet contains a unique value that can be used to identify NetStumbler.

Probe Response traffic: War-Driving forces AP to generate probe response frames and is likely to increase the traffic of these frames. Such abnormal increase in traffic can be revealed by monitoring probe response frames. However, legitimate users may also request for AP response. Therefore, detailed analysis is required to determine the main cause of the increased traffic.

5.1.3.2 Anti-WEPcracking

The core of WEP is RC4 stream cipher, which XORs key-stream with plaintext to generate encrypted cipher-text. To crack WEP, attacker reverses encryption procedure to retrieve the key. WEP key vulnerability is first discovered in a research undertaken by Fluhrer, Martin and Shamir[1] which states that IV transferred in clear may divulge WEP key. Obviously, the major flaw that makes WEP vulnerable is the fact that

attacker is able to extract key from the gathered frames. Usually, statistics is used to assists in determining the real key values from the candidates. The real key value often has the highest occurrence among all. Therefore, it is reasonable to conclude that the resulting key is based on the amount and quality of the frames.

That is, the attacker is unlikely to get the right key combination if traffic is scarce or there are more frames resulted in false key values than that of the right ones. WIPS adopted a interference-based mechanism of by poisoning the traffic with frames that are deliberately tailored to generate false result to prevent attacker from getting the correct key value.

5.1.3.3 MAC Authentication

This function is used to determine whether faked MAC address is being used in WLAN. Any users with a faked MAC address will be redirected into honeypot. A rule is set and binds network card manufacturer for a specific MAC pattern. As shown in table 1, MAC address the first 3 bytes of network cards from a producer will always be the same. In other words, it is possible to find out the potential attacker by checking its MAC address pattern.

Table 2 MAC Address rule

Wireless NIC Manufacturer	First 3 bytes of MAC
3COM	00-02-9C
Toshiba	00-08-0D
Cisco	00-0B-45
SierraCom	00-02-12
Oxygnet	00-0B-50
OmniWerks	00-0B-7F
Telcomm	00-04-3E
IBM	00-50-76

5.1.4 Honeypot Module

A honeypot is a security resource whose value lies in being probed, attacked or compromised. This means, that a honeypot is expected to get probed, attacked and potentially exploited. In fact, honeypot provides additional and valuable information about the hacker.

WIPS incorporates a basic honeypot feature, which diverts attacker into a faked AP (honeypot) where he/she is quarantined from the actual WLAN. With the target being deceived, it starts to record every single move made by it. Hopefully, these records can be used as a learning material and reference.

5.1.5 GSM Alarm Module

Although IDS should be designed to handle attacks automatically, there are times whereby manual procedure or decision making is required by administrator. Therefore, as with any IDS, severe attacks must be reported efficiently to administrator. Traditionally, alarms are delivered through email or other network message services. To be more efficient, WIPS employs SMS (Short Message Service) as a mean to enable immediate reporting.

5.2. System Demonstration

Presently, this WIPS system leveraging resources from Open-Source community was developed by Python, wxPython and executed on the Linux OS Environment (Red Hat 9.0).

5.2.1. TCP Session Analysis and Reassembly

As shown in figure 19, the proposed system support two operating mode real-time capture and off-line. Real-time mode collects frames that travel through the air; while off-line retrieve historical frame data from audit file previously created.

Section A is a list of captured frames with their information labeled: packet number, time stamp, source MAC, destination MAC, protocol used and payload summary. It gives analyst a quick view of network events that occurred within a certain period of time. Also, it reveals traces that are crucial evidence in computer forensics when determining the identity of the attacker. Section B shows full detail about the selected frame in section A. For better presentation, frame information is transformed into a tree data structure in accords to its protocol. Section C shows the raw data of the selected frame in hex for advanced users.

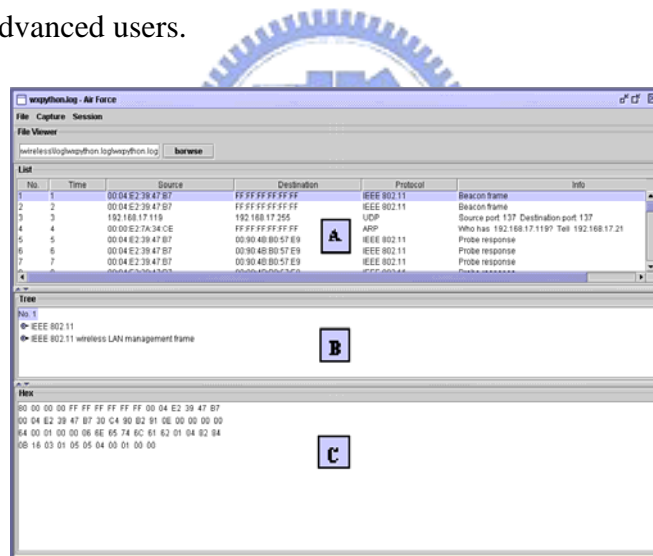


Fig. 20 system main interface

In addition to the basic frame browsing method, this system provides user with a much convenient interface called session view. As shown in figure 20, user can activate session view by clicking on the menu item “session”.

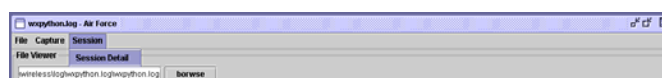


Fig. 21 activating session view

As shown in figure 21, the session list on the left is a current session list generated from the collected frames with first session [prot1315,3128] selected. Detail section on the right displays the constituting frames of the chosen session and each summarized frame information. In this case, the selected session is between hosts 192.168.17.197 and 210.71.23.110 according to the information provided.

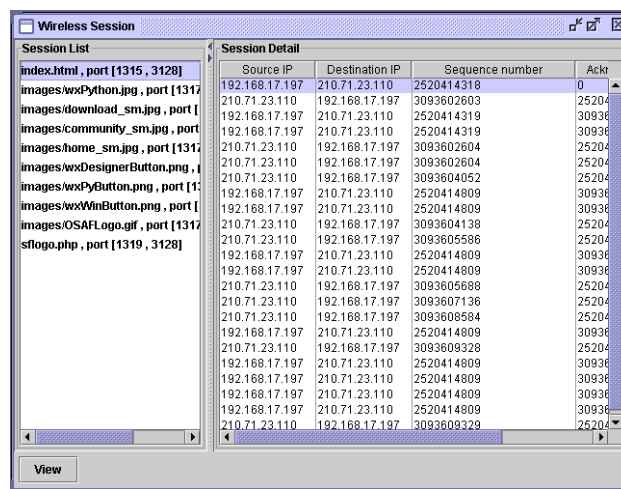


Fig. 22 selecting a session

In addition to session analysis, WIPS even has the ability to reassemble the frames and reconstruct the fragmented data back to its original file form. By clicking the button “view” located at bottom-left, the file reconstructed from the session will be shown. Figure 22 displays a result of web page being restored.



Fig. 23 web page restored

5.2.2 Anti WarDriving

To simulate War-Driving attack, a laptop with NetStumbler installed is used in this case. First, NetStumbler is started to probe for AP. Fig. 23 shows the search result with an AP being detected using channel 5.



Fig. 24 NetStumbler detected an AP

Immediately after NetStumbler found an AP, WIPS also detected the presence of the attacker. Fig. 24 is the system generated war-driving warning sign which indicates that the attack source MAC address was 00:05:5d:f1:de:30. Next, GSM alarm module sent a message through SMS to report the current situation to network administrator.



Fig. 25 War-Driving warning message

At the same time, WIPS starts to generate false probe request frames, which contain faked AP information, to confuse the attacker. Fig. 25 is the result of NetStumbler when war-driving is detected by WIPS. In this case, there are five faked APs.

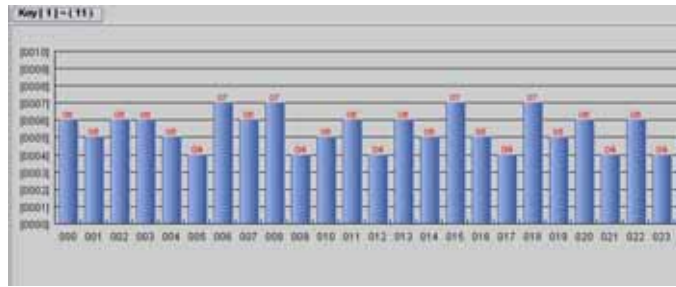


Fig. 28 WIPS interferences WEP key calculation

5.2.4 Wireless Honeypot

It is difficult to demonstrate how wireless honeypot works by just showing output screens of each stage. Therefore, to enhance the comprehensibility, details of each stage will be described accompanied with Fig. 28.

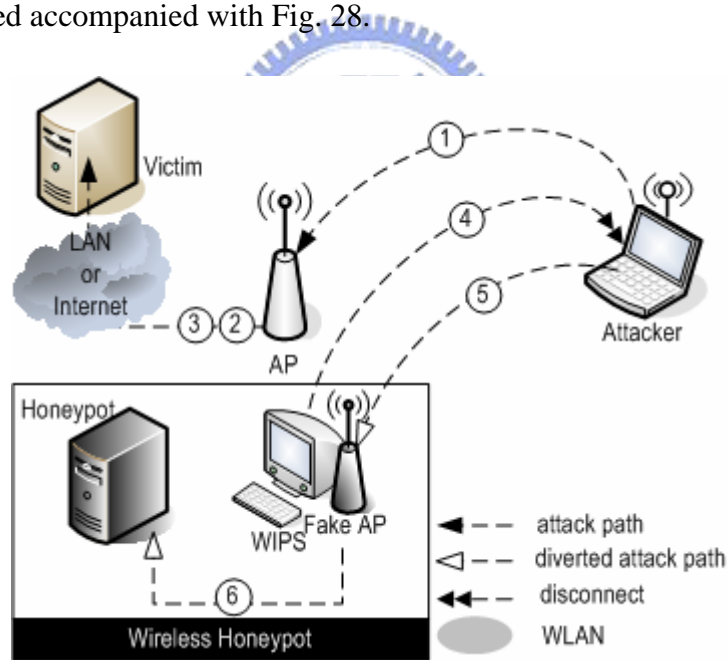


Fig. 29 concept diagram of how wireless honeypot operates

Step 1 and 2 (Fig. 28.) show that attacker has successfully connects to the target server through AP. The framed section in Fig. 29 shows information about attacker's wireless NIC and the associated AP. Currently, the attacker is connecting using SSID AirFore on channel 5.

```

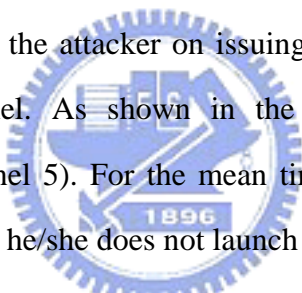
Mode:Master Frequency:2.422GHz Access Point: 00:11:11:11:11:11
Bit Rate:11Mb/s Tx-Power:-13 dBm Sensitivity=1/3
Retry min limit:8 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality:0 Signal level:0 Noise level:0
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:53 Missed beacon:0

[root@localhost /]# iwconfig wlan0 mode managed
[root@localhost /]# iwconfig wlan0 essid "AirForce"
[root@localhost /]# iwconfig wlan0 channel 5
[root@localhost /]# iwconfig wlan0
wlan0 IEEE 802.11b ESSID:"AirForce"
Mode:Managed Frequency:2.432GHz Access Point: 00:05:5D:DA:48:7E
Bit Rate:2Mb/s Tx-Power:-12 dBm Sensitivity=1/3
Retry min limit:8 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality:74/92 Signal level:-56 dBm Noise level:-100 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:62 Missed beacon:0

```

Fig. 30 screenshot of an attacker connecting to AirForce AP

Fig. 30 is output screen of the attacker on issuing “iwlist” command to query the present communication channel. As shown in the diagram, current frequency is 2.432GHz (equivalent to channel 5). For the mean time, this person can still interact with the target server as long as he/she does not launch attack.



```

root@localhost:/
檔案(F) 編輯(E) 顯示(V) 終端機(T) 移至(G) 求助(H)
[root@localhost /]# iwconfig wlan0
wlan0 IEEE 802.11b ESSID:"AirForce"
Mode:Managed Frequency:2.432GHz Access Point: 00:05:5D:DA:48:7E
Bit Rate:2Mb/s Tx-Power:-12 dBm Sensitivity=1/3
Retry min limit:8 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality:78/92 Signal level:-55 dBm Noise level:-100 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:63 Missed beacon:0

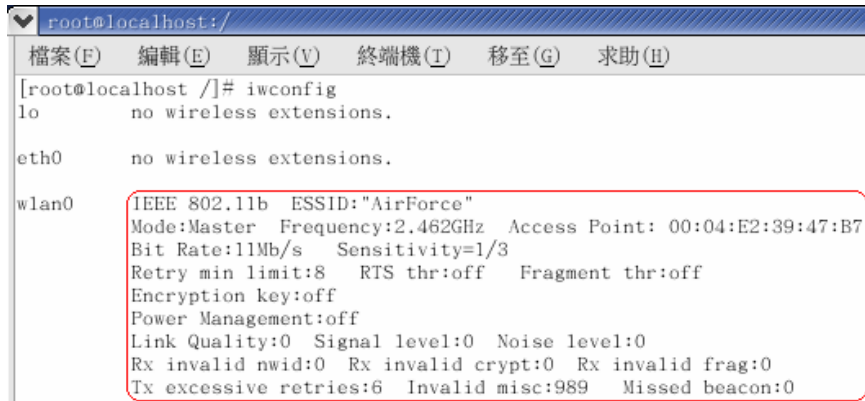
[root@localhost /]# iwlist wlan0 channel
wlan0 14 channels in total; available frequencies :
Channel 01 : 2.412 GHz
Channel 02 : 2.417 GHz
Channel 03 : 2.422 GHz
Channel 04 : 2.427 GHz
Channel 05 : 2.432 GHz
Channel 06 : 2.437 GHz
Channel 07 : 2.442 GHz
Channel 08 : 2.447 GHz
Channel 09 : 2.452 GHz
Channel 10 : 2.457 GHz
Channel 11 : 2.462 GHz
Current Frequency:2.432GHz (channel 05)

[root@localhost /]# █

```

Fig. 31 current channel of the attacker

At step 3 (Fig. 28) shows the intruder has launched attacks on the target server. Meanwhile, WIPS detected this event and start the diversion procedure (step 4). Figure 31 describes FakeAP network information. Notice that FakeAP is using the exact SSID that the real AP is using. The purpose of faking the real AP is to deceive the attacker.



```
root@localhost: /
檔案(F) 編輯(E) 顯示(V) 終端機(T) 移至(G) 求助(H)
[root@localhost /]# iwconfig
lo          no wireless extensions.

eth0       no wireless extensions.

wlan0      IEEE 802.11b  ESSID:"AirForce"
           Mode:Master  Frequency:2.462GHz  Access Point: 00:04:E2:39:47:B7
           Bit Rate:11Mb/s  Sensitivity=1/3
           Retry min limit:8  RTS thr:off  Fragment thr:off
           Encryption key:off
           Power Management:off
           Link Quality:0  Signal level:0  Noise level:0
           Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
           Tx excessive retries:6  Invalid misc:989  Missed beacon:0
```

Fig. 32 wireless NIC information of FakeAP

Step 5 and 6 (Fig. 28) show that the attacker has been redirected into honeypot (VM). Fig. 32 shows the wireless NIC information of the attacker after diversion. Note that the attacker is unlikely to discern the difference between real AP and faked one by observing SSID. In the case where attacker finds out the change in MAC address or channel, it would as well be misinterpreted as normal situation whereby AP suffered interference. Hence, FakeAP may be regarded as another potential target.

```

[root@localhost /]# iwconfig wlan0
wlan0 IEEE 802.11b ESSID:"AirForce"
Mode:Managed Frequency:2.462GHz Access Point: 00:04:E2:39:47:B7
Bit Rate:11Mb/s Tx-Power:-12 dBm Sensitivity=1/3
Retry min limit:8 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality:74/92 Signal level:-56 dBm Noise level:-100 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:193 Missed beacon:0

[root@localhost /]# iwlist wlan0 channel
wlan0 14 channels in total; available frequencies :
Channel 01 : 2.412 GHz
Channel 02 : 2.417 GHz
Channel 03 : 2.422 GHz
Channel 04 : 2.427 GHz
Channel 05 : 2.432 GHz
Channel 06 : 2.437 GHz
Channel 07 : 2.442 GHz
Channel 08 : 2.447 GHz
Channel 09 : 2.452 GHz
Channel 10 : 2.457 GHz
Channel 11 : 2.462 GHz
Current Frequency:2.462GHz (channel 11)

```

Fig. 33 hacker is diverted

5.2.5 GSM messaging

When WIPS detects War-Driving, WEP cracking, MAC faking or other similar attacks, it is necessary to inform network administrator efficiently before its condition becomes critical. Fig. 33 shows a short message sent by WIPS when WLAN under malicious attack.



Fig. 34 alarmed SMS over GSM

CHAPTER 6

CONCLUSIONS

6.1. Summary

With rapid growth of Internet and mobile device user population, Wireless Local Network (WLAN) is increasingly used in offices and home because of its convenient deployment and management. Comparing to traditional wired network, wireless environment does not constraint hacker in physical topology which sometimes protects network from direct attack. The fact that WLAN using radio frequency as the transmission media introduces new threats into network due to data exposure. That is, WLAN is prone to attacks. Hackers are exploiting these weaknesses in the field, from distances of a mile or more.

This research has discussed WLAN vulnerabilities and threats it faces presently. Also, with concepts and techniques of different attack scheme as foundation, a proactive wireless intrusion prevention system is developed. Finally, the proposed WIPS is experimented and proved to be effective in detecting and preventing WEP cracking, MAC spoofing, War Driving and content violation

Honeytrap protects internal network from adversaries while collecting valuable information for post analysis. As people's desire on mobility grows, wireless LAN gradually replaces part of the wired network. However, the most popular 802.11b standard lacks a secure protection mechanism that can prevent WLAN from becoming a threat to internal network. This research implements a wireless honeytrap that functions

similar to traditional honeypot, but with additional WIPS support and active diversion. The proposed system proves to be effective in preventing wireless attacks and gathering crucial evidence.

6.2. Future Research Directions

Nevertheless, wireless honeypot is still in its infancy, much effort should be invested. For instance, further research should focus on performance, cross-platform issue and multiple standard supports including the latest IEEE 802.11a.

Several modules of WIPS still require further elaboration. For example, it is possible to extend intrusion detection module's function by incorporating known signatures from other IDS. Also, installing simulation of client interactions or services may improve honeypot's attraction to the hacker. Presently, the proposed system has been only tested on Linux platform. Further research should consider implement a cross-platform system in the future.

REFERENCES

1. Borisov, N., Goldberg, I., and Wagner, D. (2001) 'Intercepting mobile communications: The insecurity of 802.11', in the Annual International Conference on Mobile Computing and Networking, pp. 180 188
2. Fluhrer, S., Mantin, I. and Shamir, A. (2001) "Weaknesses in the key scheduling algorithm of RC4", in the Eighth Annual Workshop on Selected Areas in Cryptography, pp. 33 35
3. Faria, D. B., Cheriton, D. R. "DoS and authentication in wireless public access networks" in the Workshop on Wireless Security, 2002, pp. 47 56
4. Stubblefield, A., Ioannidis, J., and Rubin, A. D. (2004) 'A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP)', ACM Transactions on Information and System Security, Vol. 7, No. 2, pp. 319 332.
5. Berghel, H, Uecker, J. (2004) 'Wireless infidelity II: Airjacking' Communications of the ACM, Vol. 47, no. 12, pp. 15 20.
6. Yang, H., Xie L., and Sun, J. (2004) 'Intrusion detection for wireless local area network', in the 2004 Canadian Conference on Electrical and Computer

- Engineering, pp. 1949 1952.
7. Lim, Y.-X., Yer, T.S., Levine, J., Owen, H.L., (2003) 'Wireless intrusion detection and response', in the Information Assurance Workshop of IEEE Systems, Man and Cybernetics Society, pp. 68 75.
 8. Schmoyer, T.R., Yu Xi Lim, Owen, H.L. (2004) 'Wireless intrusion detection and response: a classic study using main-in-the-middle attack', in the IEEE Wireless Communications and Networking Conference, pp. 883 888.
 9. Yang . H., Xie L., Sun, J. (2004) 'Intrusion detection solution to WLANs', in the IEEE 6th Circuits and Systems Symposium on Emerging Technologies: Frontiers of Mobile and Wireless Communication, pp. 553 556
 10. Ren, Q., Liang Q. (2004) 'Secure media access control (MAC) in wireless sensor networks: intrusion detections and countermeasures', in the 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 3025 – 3029.
 11. Chandran, N. and Sampath, D. (2004) 'Strengthening WEP protocol for wireless networks using block chaining algorithm with variable encrypting function mechanism', in 2004 IEEE Sarnoff Symposium on Advances in Wired and Wireless Communication, pp. 141 143.
 12. Welch, D. and Lathrop, S. (2003) 'Wireless security threat taxonomy', in 2003. IEEE Systems, Man and Cybernetics Society, pp. 76 83.
 13. Ding, P.Q., Holliday J.N, and Celik A. (2004) 'Improving the security of wireless LANs by managing 802.1x disassociation', in First IEEE Consumer Communications and Networking Conference, pp. 53 58.
 14. Wang, S., Tao R., Wang, Y. and Zhang, J. (2003) 'WLAN and it's security problem', the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. :241 244.
 15. Carli, M., Rosetti, A., and Neri, A. (2003) ' Integrated security architecture for WLAN', in the 10th International Conference on Telecommunications, pp. 943 947/
 16. Barken, L. (2003) 'WEP vulnerabilities: Wired equivalent privacy?', Computer Security Journal, Vol. 19, No, 3, pp. 31 36.
 17. Goth, G. (2003) 'Will the white house take on Wi-Fi?', IEEE Distributed Systems Online, Vol. 4, No. 2, 7p
 18. Potter, B. (2003) 'Wireless security's future', IEEE Security and Privacy, Vol. 1, no. 4, pp. 68 72.
 19. Bakirdan, A., Qaddour, J., Jalozie, I.K. (2003) 'Security Algorithms in Wireless LAN: Proprietary or Non-Proprietary', in the 2003 IEEE Global Telecommunications Conference, pp. 1425 1429.
 20. Varshnez, U., Malloy, A., Ahluwalia, P., and Jain, R. (2004) 'Wireless in the enterprise: requirements, solutions and research directions', *Int. J. Mobile Communications*, Vol. 2, No. 4, pp.354 367.
 21. Abuelyaman, E. and Wen, H.J. (2004) 'An efficient wireless transmission method for m-commerce', *Int. J. Mobile Communications*, Vol. 2, No. 4, pp.405 417.
 22. Maunuksela, A. J. and Nieminen M. (2005) 'Micromobility supported WLAN networks: an empirical study of new IP protocol to support mobility and connection handovers', *Int. J. Mobile Communications*, Vol. 3, No. 4, pp.127 137

23. Tsaur, W. J. and Ho, C. H. (2005) 'A mobile agent protected scheme using pairing-based cryptosystems', *Int. J. Mobile Communications*, Vol. 3, No. 4, pp.183 196
24. Lu, J., Yu, C.S., Liu, C. and Ku, C. Y.F. (2004) 'Wireless trust: conceptual and operational definition', *Int. J. Mobile Communications*, Vol. 2, No. 1, pp.38 50
25. Lu, J., Hayes, L.A., Yu, C.S. and Liu, C. (2003) 'Conceptual and operational definition of system complexity in the domain of Wireless Internet via Mobile Technology', *Int. J. Mobile Communications*, Vol. 1, No. 1, pp.360 371
26. Banitsas, K. A., Song, Y.H., and Owens, T. J. (2004) 'OFDM over IEEE 802.11b hardware for telemedical applications', *Int. J. Mobile Communications*, Vol. 2, No. 3, pp.310 327
27. Jamshaid, K., You, L. (2003) 'Performance evaluation of technologies for securing 802.11 Enterprise wireless networks', in the International Conference on Communication, Network, and Information Security, pp. 15 19.
28. Adelstein, F., Alla, P., Joyce, R., Richard III, G. (2004) 'Physically locating wireless intruders', in the International Conference on Information Technology: Coding Computing, pp. 482 489.
29. Virendra, M., Upadhyaya, S., (2004) 'SWAN: a secure wireless LAN architecture', in the 29th Annual IEEE International Conference on Local Computer Networks, pp. 216 223.
30. Flickenger, R. (2003) 'Building Community Networks', O'Reilly & Associates Inc.
31. Raynal, F., Berthier, Y., Biondi, P., Kaminsky, D, (2004) 'Honey-pot forensics part 1: analyzing the network' *IEEE Security & Privacy Magazine* , Vol. 2, no. 4, pp. 72 78.
32. Raynal, F., Berthier, Y., Biondi, P., Kaminsky, D, (2004) 'Honey-pot forensics part II: analyzing the compromised host' *IEEE Security & Privacy Magazine* , Vol. 2, no. 5, pp. 77 80.
33. Raynal, F., Berthier, Y., Biondi, P., Kaminsky, D, (2004) 'Honey-pot forensics' in the the Fifth Annual IEEE System, Man and Cybernetics Information Assurance Workshop, pp. 22 29.
34. Borsc M, Shinde H. (2005) 'Wireless security & privacy' in the 2005 IEEE International Conference on Personal Wireless Communications, pp.424 428.
35. Peltier, J. (2005) 'Testing wireless security cryptosystems for speed', *Computer Security Journal*, Vol. 2, no. 1, pp. 1 20.
36. Sharp, Kevin R. (2005) 'Wireless security and management', *Supply Chain Systems Magazine*, Vol. 25, no. 4, pp. 32 34.
37. Chen, J. C., Jiang, M. C., Liu, Y. W. (2005) 'Wireless LAN security and IEEE 802.11i', *IEEE Wireless Communications*, Vol. 12, no. 1, pp. 27 36.
38. Carr, J.(2005) 'Configuring wireless security' *Network Magazine*, Vol. 20, no. 2, pp. 58 60.
39. Wu, L., Shi, L. (2005) 'Construction of security wireless LAN based on VPN' *Jisuanji Gongcheng/Computer Engineering*, Vol. 31, no. 4, pp. 169 171.
40. Held, G. (2005) 'Focus on firetide HotPoint wireless mesh routers' *International Journal of Network Management*, Vol. 15, no. 1, pp. 67 71
41. Beyah, R., Kangude, S., Yu, G., Strickland, B., Copeland, J. (2004) 'Rogue access point detection using temporal traffic characteristics' in the IEEE Global

- Telecommunications Conference, Vol. 4, pp. 2271-2275
42. Jagetia, M., Kocak, T. (2004) 'A novel scrambling algorithm for a robust WEP implementation' in the IEEE 59th Vehicular Technology Conference, Vol. 59, no. 5, pp. 2487-2491
 43. Sorman, M., Kovac, T., Maurovic, D. (2004) 'Implementing improved WLAN security' in the 46th International Symposium Electronics in Marine, pp. 229-234.
 44. Mishra, A. Petroni Jr., Nick L.; Arbaugh, W. A., Fraser, T. (2004) "Security issues in IEEE 802.11 wireless local area networks: A survey" *Wireless Communications and Mobile Computing*, Vol. 4, no. 8, pp. 821-833.
 45. Diaz, J. A. P., Del Valle Torres, G. (2004) 'Vulnerabilities in 802.11b wireless local area networks' in the International Conference on Security and Management, pp. 118-124.
 46. Larson, M. (2004) 'The SecureScout Wi-Fi security and monitoring framework' *Dr. Dobb's Journal*, Vol. 29, no. 11, pp. 34-39.
 47. Namadurai, E., Qaddour, J., Doss, D. (2004) 'Wireless LAN: Security problems, solutions and challenges', in the 5th World Wireless Congress, pp. 719-722.
 48. Ahuja, S. P., Dendukuri, K. (2004) 'Security problems in 802.11 based wireless networks' in the Third IASTED International Conference on Communications, Internet, and Information Technology, pp. 195-200.
 49. Boland, H., Mousavi, H. (2004) 'Security issues of the IEEE 802.11B wireless LAN' in the Canadian Conference on Electrical and Computer Engineering, Vol. 1, pp. 0333-0336.
 50. Erten, Y. M., Tomur, E. (2004) 'A layered security architecture for corporate 802.11 wireless networks' in the 2004 Wireless Telecommunications Symposium, pp. 123-128.
 51. Karir, M., Baras, J. S. (2004) 'Data dependent keying for wireless networks' in the 2003 IEEE 58th Vehicular Technology Conference, Vol. 58, no. 3, pp. 2098-2102.
 52. Yan, H., He, C. (2004) 'Security analysis and improvement of wired equivalent privacy' *Journal of Shanghai Jiaotong University*, Vol. 38, no. 5, pp. 693-696+700
 53. Chandran, N., Sampath, D. (2004) 'Strengthening WEP protocol for wireless networks using block chaining algorithm with variable encrypting function mechanism' in the IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communication, pp. 141-143.
 54. Ding, P., Holliday, J., Celik, A. (2004) 'Improving the security of Wireless LANs by managing 802.1x disassociation' in the 2004 IEEE Consumer Communications and Networking Conference, pp. 53-58.
 55. Komori, T., Saito, T., (2004) 'A secure wireless LAN system retaining privacy' in the 18th International Conference on Advanced Information Networking and Applications, Vol.2, pp.370-375.
 56. Cheung, D. (2004) 'WLAN security and Wi-Fi protected access' *Dr. Dobb's Journal*, Vol. 29, no. 6, pp. 45-47.
 57. Majstor, F.; (2003) 'WLAN security threats & solutions' in the 28th Annual IEEE International Conference on Local Computer Networks, pp. 650.
 58. Potter, B. (2003) 'Wireless security's future' *IEEE Security and Privacy*, Vol. 1, no. 4, pp. 68-72.

59. Goth, G. (2003) 'Will the white house take on Wi-Fi?' IEEE Distributed Systems Online, Vol. 4, no. 2, 7p.
60. Jha, N., Sengupta, I. (2003) 'A new scheme to improve the security of the WEP protocol' in the Intl. Conference on Communication, Network and Information Security , pp.1 6.
61. Cam-Winget, N., Housley, R., Wagner, D., Walker, J. (2003) 'Security flaws in 802.11 data link protocols' Communications of the ACM, Vol. 46, no. 5, pp. 35 39.
62. Salgarelli, L., Buddhikot, M., Garay, J., Patel, S., Miller, S. (2003) 'Emerging authentication and key distribution in wireless IP networks' IEEE Wireless Communications, Vol. 10, no. 6, pp. 52 61.
63. Bakirdan, A., Qaddour, J., Jalozie, I.K., (2003) 'Security algorithms in wireless LAN: proprietary or nonproprietary' in the IEEE Global Telecommunications Conference, Vol. 3, pp.1425 1429.
64. Potter, B. (2004) 'Fixing wireless security' Network Security, Vol.4, no.6, pp. 4 5.
65. Zahariadis, T. (2004) 'Evolution of the Wireless PAN and LAN standards' Computer Standards and Interfaces, Vol. 26, no. 3, pp. 175 185.
66. Hassan, H.R., Challal, Y. (2005) 'Enhanced WEP: an efficient solution to WEP threats' in the Second IFIP International Conference on Wireless and Optical Communications Networks, pp. 594 599
67. Chandran, N., Bhavana, K.R., (2005) 'Enhancing RC4 algorithm for WEP protocol using fake character insertions and compression technique (FCICT)' in the Second IFIP International Conference on Wireless and Optical Communications Networks, pp. 80 83.