Journal of Information Assurance and Security 1 (2006) 1-10

A Study and Testbed for the Australian Standard AS7799 Compliance and Management

Suwanna Yamsiri[1], Jennifer Seberry[2] and Willy Susilo[3]

[1]School of Information Technology and Computer Science, University of Wollongong, Wollongong, NSW 2522, Australia
sy735@uow.edu.au

[2]School of Information Technology and Computer Science, University of Wollongong, Wollongong, NSW 2522, Australia
jennie@uow.edu.au

[3]School of Information Technology and Computer Science, University of Wollongong, Wollongong, NSW 2522, Australia
wsusilo@uow.edu.au

Abstract: With AS7799 accreditation and certification schemes now firmly in place, the AS7799 standard may ultimately become a benchmark against which all organizations will be measured. In addition, the number of organizations that employ wireless technology in their businesses has significant increased in the last few years. However, there is little research about wireless security under AS7799. There are several article about the vulnerability of WEP (***W**ired **E**quivalent **P**rivacy*), a wireless protocol. This motivates us to study the wireless security compliance in the standard. In this study, we carried out experiments to test if theoretical attacks against WEP, a wireless protocol, work in the real world. We also investigated wireless protocol usage in chosen areas.

***Keywords*:** Information Security, Wireless Security, Information Standard, Australian Standard, Wireless Protocol, WEP.

1. Introduction

In 1992 the Department of Trade and Industry (DTI) in the UK published an Information Security Management Code of Practice. Later, in 1995, the first version of BS 7799 part 1 (BS7799.1) was developed and published by the UK Accreditation Service (UKAS). Subsequently, December 2000, the submission of BS7799.1 to ISO was accepted and resulted in the publication of ISO/IEC 17799. In 2002, BS7799.2 was revised to align it with ISO 17799 and to harmonize it with other management systems standards, ISO 9001 and ISO 14001, the OECD principles for security of information systems and networks.

With AS7799, BS7799 in Australia, accreditation and certification schemes now firmly in place, AS7799 may ultimately become a benchmark against which all organizations will be measured. There have been suggestions it may become mandatory. It is therefore important to understand AS7799 and determine whether it is suitable for all proposed applications, especially for wireless technology. Wireless technology has been widely used in many industries for years, and wireless LANs based on the 802.11 standard are becoming extensively prevalent in corporate environments. However, little appears to have been written regarding the wireless security compliance within AS7799. This motivates us to study wireless security compliance in the standard. We carried out experiments to test if theoretical attacks against WEP (***W**ired **E**quivalent **P**rivacy*), a wireless protocol, work in the real world. Furthermore, we are interested in which wireless protocols are actually used.

In this study, we provide a review of literature relating to AS7799 and wireless network security, especially regarding the impact of using AS7799 and the growth of wireless technology, its benefits and its insecurity. Additionally, the vulnerability of WEP will be described.

We also detail the methods used to accomplish attacks against WEP, both 64-bit and 128-bit key versions, and carry out our experiments along with surveys. Finally, conclusions and recommendations will be offered.

2. Previous works

Prior to experiments could be carried out, we reviewed literatures associated with AS7799 and Wireless LAN security. We also studied wireless security standard, its terms and definitions, Wired Equivalent Privacy (WEP), WEP weaknesses, Using the Fluhrer, Mantin and Shamir Attack to Break WEP, 802.11 Sniffer and WEP Cracking Tools.

2.1 Review of the literature

2.1.1 The AS7799 Standard

According to Office of E-Government (2005), the e-Government has developed an Information Security Management System (ISMS) implementation methodology to help agency managers implement best practice risk management and information security management based on Australian and international standards, AS/NZS 7799.2:2000.As well as Brown's research (2004), he states that information security standards including AS7799 are designed for providing guidance as to the best practice. Conversely, his research shows that the use of this

Received Feburary 2, 2006.

information security standard is still not high, only 37% of organizations used standards and only 55 % of these organizations used AS/NZS 7799.2:2003.

A possible reason could be that the information security standard, AS7799, is impractical. Dearne (2005) reports that companies need to be audited quarterly to satisfy the AS7799 information security standard therefore their current systems may need to be modified to make them easier to be audited. This contributes to compliant panic. Besides that, Allan (2003) affirmed that some security controls of AS/NZ 7799.2 are very low risk and may be not applied in practice. Likewise, Ellsmore (2003) disputes the usefulness of 7799 standard by stating that security is not a "tick-a-box" process, and 7799 compliance does not make an organization secure.

Consequently, the impact of information security standards awareness on some agencies such as information security providers would be another outcome. Kidman (2005) states that many businesses assess outsourcers by checking that they meet key standards such as AS7799 in spite of the fact that the outsourcer does not value the data as much as the owner of the data. As a result, he concludes that assumptions about what is covered may be problematic. Moreover, impact of the information security standards awareness on technology development can be found. Goh (2005) reports that ever since governments started getting tough on agencies with security, wireless adoption have slowed considerably. On the other hand, companies that hope to get the ISMS Certification or hope to comply with AS7799 are companies which probably desire to be regarded as a trusted supplier, customer or business partner. This is a goal of Bridge Point Communications that can be found in their newsletter online (2002).

In summary, AS7799, the Australian information security standard, is designed for providing guidance as to the best practice. Nevertheless, the use of this standard is still not high. Perhaps part of the problem is the standard itself; it may be impractical. Furthermore, impacts of information security standards on information security service providers would be another effect. In addition, technology developments such as wireless adoption do not go as far as they possibly could. This may be an outcome of the imposition of the standard. In contrast, some companies still seek compliance with AS7799 since they wish to be known as trusted companies.

2.1.2 Wireless LANs Security

As has been shown (Foundry Networks, 2005), wireless technology has been widely used in many industries for years. Manufacturing, courier services, and retail are just some of the industries successfully using wireless for inventory control, package tracking, and pricing applications to increase productivity and streamline procedures. Furthermore, Flextronics Software Systems (2005) reports three studies associated with the growth of wireless networks; the first is a study by Ovum Research that estimates wireless networks, WLANs, could evolve into a $29 billion global market by 2006. The second study is a study by Gartner, which indicates that nearly 50% of company laptops around the world will have WLANs support by 2006. The last study is by IDC, reports that revenues from WLANs sales in Asia alone (excluding Japan) will reach US$350 million by 2005, up from US$45 million in 2000. Gralla (2004) states that worldwide revenue for WiFi hardware is up 9%, to $784.5 million, and total units were up 31% for the third quarter of 2004 compared to the same quarter of 2003. Moreover, (the United States Government Accountability Office [GAO], 2005) states that the use of wireless networks is becoming increasingly popular among personal, academic, business, and government users. Hence, it could be stated that the demand for enterprise class wireless LAN solutions is increasing quickly.

The primary reason for this increase would be the many benefits of using mobile technology. According to Foundry Networks (2005), using mobile technology can eliminate the cost of new cable plants or extensions of existing cabling. It is also easy to install and can be rapidly deployed with lower long-term costs. In addition, (GAO, 2005) also claims that wireless networks offer a wide range of benefits to federal agencies, including increased flexibility and ease of network installation.

The many benefits of wireless technology contribute to the popularity of wireless networks. However, wireless networks are widely known to be vulnerable to attack. Verton (2001) reports that in February three researchers at the University of California, Berkeley, demonstrated attacks on WEP that defeat each of the security goals. Furthermore, Ossmann (2004) states that WEP is truly dead. In addition, Ou (2005) claims that WEP cracking can be done by just a little more effort. Moreover, he states that to crack WEP has almost become a recreational sport for script kiddies and a primary tool of choice for hackers. This would be true because Cheung (2005) has provided steps to crack WEP.

In conclusion, wireless LANs based on the 802.11 standard are becoming widely prevalent in corporate environments. However, the lack of strong security in the implementations of 802.11b technology using Wired Equivalent Privacy (WEP) security should be realised.

2.2 Background

2.2.1 What is AS7799?

AS 7799.2:2003, 'Specification for Information Security Management', is the Australian Standard for information security management and contains a clear definition of comprehensive ISMS, Information Security Management System, and a detailed description of the activities required to implement it. It is also known as AS/NZS 7799.2:2003, BS7799.2:2003 in Australia and New Zealand.

The two standards are identical and are supported by ISO 17799:2001, 'Code of Practice for Information Security Management', which is an international standard providing best practice guidance on security controls that should be considered for implementation within an organization.

(a) History of the Standards

AS 7799.2 and ISO 17799 have been developed over the last 8 years by committees representing the best practice of both commercial and government organizations as the following:

- In 1992, the Department of Trade and Industry (DTI) in the UK has published an Information Security Management Code of Practice.
- In 1995, the first version of BS 7799 part 1 (BS7799.1) was developed and published by the UK Accreditation Service (UKAS).

- In 1998, the BS 7799 part 2 (BS7799.2) was published. It specified the ISMS and the methodology for selection of the controls.
- In 1999, revision of both parts were published, they aligned the controls and added some additional controls for ecommerce, mobile computing and third parties. The specific references to UK legislation were also removed and this resulted in the adoption of the standard in several other countries.
- December 2000, the submission of BS7799.1 to ISO was accepted and resulted in the publication of ISO/IEC 17799.
- In 2002, BS7799.2 was revised to align it with ISO 17799 and to harmonize it with other management systems standards, ISO 9001 and ISO 14001, the OECD principles for security of information systems and networks. It also embraced the recent drivers for Corporate Governance and the need for a continual improvement process, introducing the Plan-Do-Check-Act model.

(b) Overview of the AS7799.2

The ten control areas and sub-areas for specific controls identified in this Standard are:

1) *Security Policy*: Demonstrate management commitment to security through the issue and maintenance of an organizational Security Policy.
2) *Organizational Security*: Assign security responsibilities and set up an infrastructure for coordination and management of information security within the organization and with third parties and outsourcers.
3) *Asset Classification and Control*: Establish and implement a system for classifying and handling information assets.
4) *Personnel Security*: Reduce the risks of human error by effective screening of staff, suitable confidentiality and employee contracts and provide on-going security awareness training, including incident reporting and management.
5) Physical and Environmental Security: Prevent unauthorized access, damage, loss and interference to business premises, equipment assets and information through physical access controls and environmental protection.
6) *Communications and Operations Management*: Operational procedures and responsibilities to be established to ensure the correct and secure operation of information processing facilities. This covers areas as diverse as protection against malicious software, systems capacity planning, back-ups and logs, handling of tapes, disks, cassettes and printed reports and security of electronic mail.
7) *Access Controls*: Security mechanisms must be in place for determining and controlling access to information, information systems, networks and applications based on a documented Access Control Policy. Access to networks and systems must be monitored and logged.
8) *System Development and Maintenance*: Information systems, networks and applications must have security controls in place at all stages of development and in all operational environments to protect information assets and infrastructure. This includes cryptographic controls like encryption and digital signatures.
9) *Business Continuity Management*: Business continuity management process to be implemented to reduce to an acceptable level the disruption caused by security failures.
10) *Compliance*: Advice on compliance with relevant laws should be obtained. Reviews to check compliance with security policies and procedures to be regularly conducted.

2.2.2 Wireless LANs

(a) Terms and definitions

- 802.11 is a wireless networking standard that uses 2.4 GHz or IR and provides 1 or 2 Mbps Original wireless specification with broad support.
- 802.11a is a wireless networking standard that uses 5 GHz and provides up to 54 Mbps.
- 802.11b is a wireless networking standard that uses 2.4 GHz and provides up to 11 Mbps.
- 802.11g is a wireless networking standard that uses 2.4 GHz and provides 54 Mbps.
- 802.11i is a security protocol that provides strong authentication and encryption of wireless traffic and additional capabilities.
- 802.1X is a security protocol that supplies a framework for authentication of end devices.
- WEP, Wired Equivalent Privacy, is a security protocol that provides weak authentication and encryption of wireless traffic.
- WPA, Wi-Fi Protected Access, is a security protocol that provides authentication and encryption of wireless traffic; based on an early draft of IEEE 802.11i.

(b) Wired Equivalent Privacy

The IEEE 802.11b standard defines two mechanisms for providing access control and privacy: Service Set Identifier (SSID) and Wired Equivalent Privacy (WEP). SSID is a 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS, a group of any number of stations. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet it does not supply any security to the network.

The WEP security protocol was ratified in September 1999. It provides encrypted communication between the client and an access point (AP). It provides a shared key authentication mechanism, where a static, manually preset WEP key on both the AP and the clients is used for authentication. The WEP protocol also uses the stream cipher RC4 for confidentiality and the CRC-32 checksum, integrity check value or ICV, for integrity.

(c) WEP Weaknesses

As discovered by three researchers, Fluhrer, Mantin, and Shamir , WEP can be cracked by anyone with a *sniffer*, which is the name given to the hardware device or software that can capture data as it flies through the air. Hence, WEP is an obsolete scheme to secure wireless networks.

WEP can be cracked because of a number of weaknesses. The weaknesses are the following: there is no specified key

management in the WEP standard and the twenty-four bits IV is too small. In addition, the ICV algorithm that is based on CRC-32 is not appropriate since CRC-32 is an excellent checksum for detecting errors, but an awful choice for a cryptographic hash. Moreover, WEP's use of RC4 is weak. RC4 in its implementation in WEP has been found to have weak keys that are described by the three researchers in their paper "Weakness in the Key Scheduling Algorithm of RC4".

(d) Using the Fluhrer, Mantin, and Shamir Attack to Break WEP

The Fluhrer, Mantin, and Shamir Attack (or in short, FMS attack) is a passive attack to break WEP based on statistical analysis. This attack exploits the design failure of RC4, a stream cipher. It is initialised with the IV and key (64 bits or 128 bits together). The output of the cipher is XORed with the payload/ICV to produce the cipher text.

To break WEP is to guess the first byte of a plain text payload. A plain text payload is an IP header followed by a TCP header, and lastly a data payload. Since IP headers tend to remain constant, guessing the first byte of plain text is considerably reduced. When the IV and the first byte of a plain text are known, information about encryption key can sometimes be obtained. An IV that meets this condition is called a weak IV. Three steps to break WEP by using FMS attack are the following:

- Simulating the Attack
- Capturing the Packets
- Cracking the Key

(e) 802.11 Sniffer and WEP Cracking Tools

Tools for breaking 802.11 WEP keys can classify to two kinds of program as the following:

- A program for capturing packets in order to collecting IVs
- A program for cracking WEP

3. Methodology

To study the need for wireless security compliance in standards such as AS7799, we carried out experiments to test if theoretical attack against WEP work in the real world. Furthermore, we are interested in how cheaply and easily the attack could be launched. We divide our methodology into four parts; system requirements, installations, experiments carried out and surveys.

3.1 System Requirements

There are four required systems in this study. These are hardware, operating systems, device drivers and software. Hardware is divided into a client, a sniffer machine and an access point. A client in this study is the Dell Desktop including with WLAN USB adaptor 54 Mbps. The sniffer machine is IBM Laptop R50e with internal wireless device, Centrino IPW2200. The access point is Wireless Network Access point 802.11b 11Mbps, BELKIN.

Operating Systems are used in this study are Microsoft Windows 2000 and Linux which is Fedora Core 4 or FC4. Furthermore, Device drivers are utilized for WLAN USB adaptor and IPW2200, wireless device, which needs three parts: 1). Firmware: ipw2200-firmware-2.3-6.at.noarch.rpm 2). Driver Kernel: ipw2200-kmdl-2.6.12-1398_FC4-1.0.4-30.rhfc4.at.i686.rpm and 3). Driver: ipw2200-1.0.6.tgz.

Software are employed in this study are the Belkin wireless access point manager, Kernel packages which are Kernel-2.6.12-1.1389_FC4.i686.rpm, Kernel-devel-2.6.12-1.1389_FC4.i686.rpm.

Additionally, Kismet-3.0.1-3.200506r1.2fc4.rf.i386.rpm, Aircrack-2.1-1.2.fc4.rf.1386.rpm and Airsnort-0.2.7e.tar.gz are used as sniffing and cracking tools.

3.2 Installations

Installations are divided into four steps. The first step is a step to install an access point. Secondly, it is to install driver of wireless device that is used as client. Next step is a step to install laptop that has wireless device that supports raw monitoring (rfmon) mode in order to be a sniffer. The last step is a step to install collecting IVs and cracking tools.

Firstly, we installed the Belkin wireless access point manager on Dell Desktop that has installed Microsoft Windows' 2000. Figure 1 is shown its icon after setting up.

Figure 1. Belkin Wireless Access Point Manager

Secondly, we installed WLAN USB adaptor driver on Dell Desktop in order to send packet to AP.

Next step is the significant step; we installed Fedora Core 4(FC4), kernel version 2.6.11-1.1369_FC4 on an i686, on IBM Laptop. This is because sniffer tools and cracking tool which we needed to use for WEP cracking are run on Linux. According to Fedora Project (2005), Fedora Core 4 is something like Red Hat Linux 13. However, we still could not install IPW2200 driver. Since IPW2200 firmware which provides monitor mode supporting are compatible with kernel version 2.6.11-1.1389_FC4 but IPW2200 firmware on kernel 2.6.11-1.1369_FC4 does not provide monitor mode. Hence, we then upgraded kernel of FC4 from version 2.6.11-1.1369_FC4 to kernel version 2.6.12-1.1389_FC4 that is needed for activating monitor mode of IPW2200 as explained.

We then installed IPW2200 driver on FC4 by doing the following: installed the firmware, *ipw2200-firmware-2.3-6.at.noarch.rpm*. Additionally, we installed *ipw2200-kmdl-2.6.12-1398_FC4-1.0.4-30.rhfc4.at.i686.rpm.* At last, we installed driver ipw2200-*1.0.6.tgz*.

Finally, we then installed WEP cracking tools which we used in our experiments that are Airsnort, Aircrack and Kismet as the following:

- Install *Airsnort-0.2.7e.tar.gz*
- Install *Aircrack -2.1-1.2.fc4.rf.i386.rpm*.
- Install *Kismet-3.0.1-3.200506r1.2fc4.rf.i386.rpm*.

After installed Airsnort, we used command "airsnort" on the command line to execute it. Airsnort screen is shown by Figure 2.

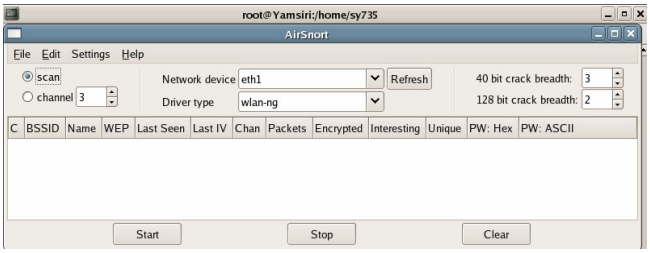

Figure 2. Airsnort Screen

In our experiments, we can use either “aircrack –e TestPuzzle –n <key length> <.cap file(s)>” or “aircrack –e TestPuzzle –n <key length> -k 1 –f 4 <.cap file(s)>” to crack WEP key. By adding option “–k 1” and “–f 4”, it can improve cracking as shown in our experiments afterwards.

For Kismet setup, it is necessary to change its configuration in file /etc/kismet.conf after installation. There are two parameters needed to be changed which are suiduser and source. We placed suiduser to be sy735 and source type to be ipw2200. Moreover, interface was replaced with eth1 and source name was substituted by TestPuzzle. This alter is shown by Figure 3.

kismet.conf

```
# Kismet config file
# Most of the "static" configs have been moved to here -- the command line
# config was getting way too crowded and cryptic.  We want functionality,
# not continually reading --help!

# Version of Kismet config
version=2005.06.R1

# Name of server (Purely for organizational purposes)
servername=Kismet

# User to setid to (should be your normal user)
#suiduser=your_user_here
suiduser=sy735

# Sources are defined as:
# source=sourcetype,interface,name[,initialchannel]
# Source types and required drivers are listed in the README under the
# CAPTURE SOURCES section.
# The initial channel is optional, if hopping is not enabled it can be used
# to set the channel the interface listens on.
# YOU MUST CHANGE THIS TO BE THE SOURCE YOU WANT TO USE
#source=none,none,addme
#source=ipw2200,eth1,najanet
#source=ipw2200,eth1,any
source=ipw2200,eth1,TestPuzzle

# Comma-separated list of sources to enable.  This is only needed if you defined
# multiple sources and only want to enable some of them.  By default, all defined
# sources are enabled.
# For example:
# enablesources=prismsource,ciscosource

# Do we channelhop?
channelhop=true
```

Figure 3: kismet.conf

It is important to execute Kismet by using command as kismet with login as root but on home path of suiduser. In our experiment, we used command, kismet, on home directory of sy735 as shown by Figure 4 and Figure 5 is a Kismet screen. Otherwise; an error was shown by Figure 6.

```
[root@Yamsiri /]# cd ~sy735
[root@Yamsiri sy735]# kismet
```

Figure 4: Kismet command

Figure 5: Kismet screen

```
[root@Yamsiri scripts]#
[root@Yamsiri scripts]# kismet
Server options:  none
Client options:  none
Starting server...
Waiting for server to start before starting UI...
Will drop privs to sy735 (500) gid 0
No specific sources given to be enabled, all will be enabled.
Enabling channel hopping.
Enabling channel splitting.
Source 0 (TestPuzzle): Enabling monitor mode for ipw2200 source interface eth1 channel 6...
Source 0 (TestPuzzle): Opening ipw2200 source interface eth1...
Spawned channelc control process 3464
Dropped privs to sy735 (500) gid 0
Allowing clients to fetch WEP keys.
Logging networks to Kismet-Oct-18-2005-1.network
Logging networks in CSV format to Kismet-Oct-18-2005-1.csv
Logging networks in XML format to Kismet-Oct-18-2005-1.xml
Logging cryptographically weak packets to Kismet-Oct-18-2005-1.weak
Logging cisco product information to Kismet-Oct-18-2005-1.cisco
Logging gps coordinates to Kismet-Oct-18-2005-1.gps
Logging data to Kismet-Oct-18-2005-1.dump
Writing data files to disk every 300 seconds.
Mangling encrypted and fuzzy data packets.
Tracking probe responses and associating probe networks.
Reading AP manufacturer data and defaults from /etc/ap_manuf
Reading client manufacturer data and defaults from /etc/client_manuf
Using network-classifier based data encryption detection
FATAL: Dump file error: Unable to open dump file Kismet-Oct-18-2005-1.dump (Permission denied)
Sending termination request to channel control child 3464...
WARNING: Sometimes cards don't always come out of monitor mode
         cleanly.  If your card is not fully working, you may need to
         restart or reconfigure it for normal operation.
Waiting for channel control child 3464 to exit...
Kismet exiting.
[root@Yamsiri scripts]#
```

Figure 6: Kismet error screen

3.3 Experiments Carried Out

Our experiments are divided into two parts. The first part is 40-bit WEP key or 64-bit secret key cracking. The second part is 104-bit WEP key or 128-bit secret key cracking.

3.3.1 64-bit key cracking

After system installation, we set the configuration of the AP by getting its IP address and its name from the manual. We got 192.168.0.254/255.255.255.0 as the IP address and subclass of our AP. Then we set an IP address and subclass of our WLAN USB adaptor on Dell Desktop to be 192.168.0.1/255.255.255.0 in order to communicate with the AP. We then changed the AP configuration by changing SSID name from its default, WLAN, to “TestPuzzle”. Additionally, we enabled an encryption key. Lastly, we set 64-bit encryption for the first testing with a note of 40-bit key for verifying later. It is referred as a 64-bit key in short.

When the AP was ready to be used, secondly, we needed to change the configuration of WLAN USB adaptor by adding the WEP key that we had noted during AP setting.

Consequently, we were able to make a connection to the AP with the 64-bit key.

Then we were ready to simulate the attack by creating a ping-flood. We flooded the AP with ping command as “ping 192.168.0.254 –t” (which we will refer to as the ping-t command) from the Dell Desktop. We did not only execute one command, we executed sixty commands for this flood.

Finally, we were ready to begin capturing packets. We then ran an Airodump, which is a tool of the AirCrack package, with the command “airodump eth1 airodump 11” where the second airodump is an output file. At the same time, we also ran Aircrack in order to crack a 64-bit key in real time until the key was found. Subsequently, we terminated Airodump and Aircrack. This parallel run let us know a possible minimum number of unique IVs that can be cracked as shown in Figure 7.

```
                                aircrack 2.2

                        [00:51:31] Tested 186149166 keys (got 41989 IVs)

   KB    depth   byte(vote)
    0    0/  6   49(   5) 9D(   5) DB(   5) 91(   4) BF(   3) FC(   3) 00(   0) 01(   0)
    1    4/  9   77(   3) 84(   3) 8D(   3) B7(   3) CD(   3) 00(   0) 01(   0) 04(   0)
    2    0/  2   4B(  34) 84(   8) 3A(   5) 9C(   5) AF(   5) 05(   3) 11(   3) 62(   3)

                            KEY FOUND! [ 49:77:4B:69:2D ] (IwKi-)

You have new mail in /var/spool/mail/root
```

Figure 7: 64-bit key Capturing and Cracking.

The experiment result shows that only fifty-one minutes or around one hour was needed for IVs collecting. But we also wanted to know what the result of cracking in passive mode is. Hence, we cracked again in passive mode and we got a result that is shown in Figure 8. Figure 8 shows a 64-bit key can be cracked in only four seconds by analysing forty thousand unique IVs from approximately two hundred thousand captured packets.

```
[root@Yamsiri save]# aircrack -e TestPuzzle -n 64 -k 1 -f 4 airodump.cap.1Sep12H30
Opening airodump.cap.1Sep12H30
Read 220659 packets.

                                aircrack 2.2


                        [00:00:04] Tested 289070 keys (got 42848 IVs)

   KB    depth   byte(vote)
    0    0/  5   49(   5) 9D(   5) DB(   5) 91(   4) BF(   3) 00(   0) 01(   0) 03(   0)
    1    4/  9   77(   3) 84(   3) 8D(   3) B7(   3) CD(   3) 00(   0) 01(   0) 04(   0)
    2    0/  2   4B(  34) 84(   8) 3A(   5) 9C(   5) AF(   5) 05(   3) 11(   3) 62(   3)

                        KEY FOUND! [ 49:77:4B:69:2D ] (IwKi-)

[root@Yamsiri save]#
```

Figure 8: 64-bit WEP key cracking in passive mode

3.3.2 128-bit key cracking

In order to crack a 128-bit key, we needed to change a WEP key on the AP and then changed a WEP key on WLAN USB adaptor on Dell Desktop. After that we made a ping-flood in the same way as we did for 64-bit key cracking.

For a 128-bit key cracking, we did not only use Airodump to capture packets. We also used Kismet in order to compare their efficiencies. This is because in our review of the literature we found that Cheung (2005) states that Airodump is better than Kismet in the context of WEP cracking. For this reason, we ran Airodump and Kismet at the same time for this study. Since this attack is a passive attack, we do not need to run Aircrack in parallel.

In addition, in our experiments, Kismet stores captured packets in a defined-format as "Kismet-MMM-DD-YYYY-nn.dump" for each run. On the other hand, Airodump stores captured packets in an output file specified in the executed command as "airodump interface *output- file channel*". This means that Airodump can append captured packets in the same file as before. We were unsure that this difference contributes a different efficiency or not.

As a result, we found that Kismet stores captured packets into each file on each run but Airodump does not; we determine their efficiency with the number of unique IVs. Their efficiencies are shown in Figure 9 and we also include Airsnort in the study of efficiencies.

at hr.	Kismet	Airodump	Airsnort
	Kismet-IVs	Airodump-IVs	Airsnort-IVs
1	7318	7309	7299
2	11335	11348	11344
3	12465	12467	12483
4			
5			
6			
7			23108
8			
9	38366	38346	
10	45243	45218	
11	52416	52394	
12	59548	59532	
13	66730	66706	
14	73860	73802	
15			
16			
17			
18			
19			
20			
21			
22			
23	135750	135703	

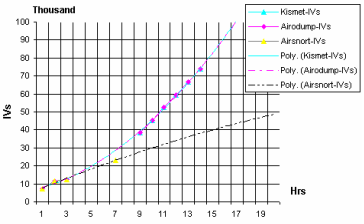

Figure 9: Collecting IVs by three capturing tools

Figure 9 shows that the number of unique IVS of Kismet and Airodump are nearly equivalent, but Airsnort can collect less unique IVs than the both tools.

Let us examine the question of whether Airodump is better than Kismet or not. We state that the efficiency of both tools to capture packets in a WEP key cracking is not quite different. Although, the difference of the both which are more provided information, more users friendly and more features of Kismet might contribute Kismet is better than Airodump. However, we maintain that Airodump is better than Kismet in the context of cracking WEP. Our reason is that Airodump is a capturing tool of the Aircrack package, and we need to use Aircrack for cracking WEP even if we use Kismet to capture packets. In addition, Airodump is easily installed but Kismet configuration must be changed after installation.

During the process of capturing packets and cracking the WEP key in passive mode, we wondered if it was necessary to capture packets continuously. To answer this question, we have written a graph in Figure 10 composed of the number of IVs and capturing time in hours.

at hr	ivs
1	10000
2	
3	
4	
5	
6	36000
7	
8	
9	
10	
11	
12	
13	49365
14	49641
15	49641
16	49641
17	49641
18	49641
19	49641
20	49641

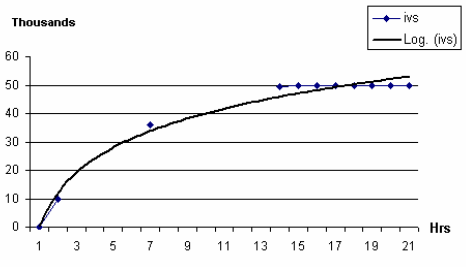

Figure 10: Duplicated IVs are generated continuously

The graph in Figure 10 shows that the number of unique IVs may tend to remain constant in some situations such as in our experiment. A possible reason would be the loaded AP. Earlier in our experiment we made a flood-ping with sixty executions of ping-t command, we increased the ping-t command to ninety executions in the hope that we were able to break the WEP key quicker. As we know the AP generates IVs; if the AP is too loaded, it is possible that duplicated IVs are generated continuously. Accordingly, we still did not know it is necessary to capture packets continuously or not. Nevertheless, we know that too much execution of ping-t command is not good.

When the WEP key was still not cracked even ninety executions of the ping command were created and the duplicated IVs were generated continuously. We terminated Airodump and Kismet at 49,641 IVs. We then performed another experiment using sixty executions of the ping-t command to crack a WEP key in passive mode by let Aircrack read multiple files. After we tested, we found three interested files which these files can not be individually cracked even ran in two hours as shown in Figure 11(a), 11(b) and 11(c) and Table 1.

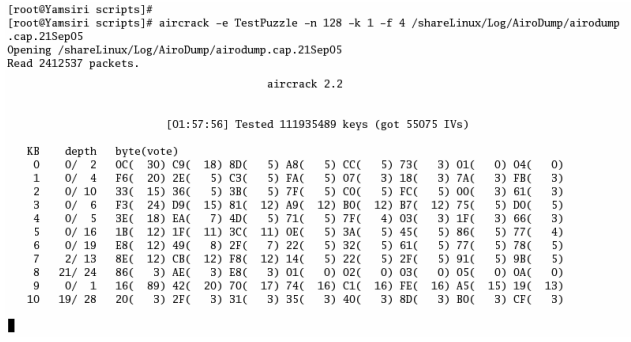

Figure 11(a): The result of cracking airodump.cap.21Sep05.

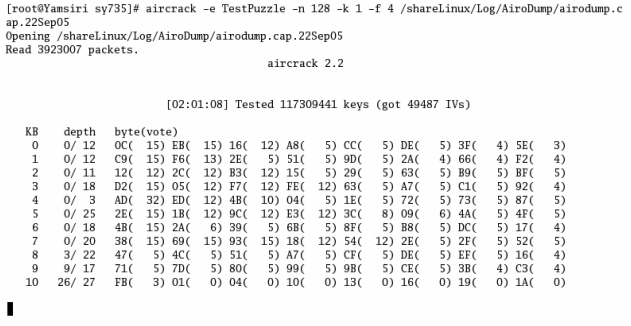

Figure 11(b): The result of cracking airodump.cap.22Sep05.

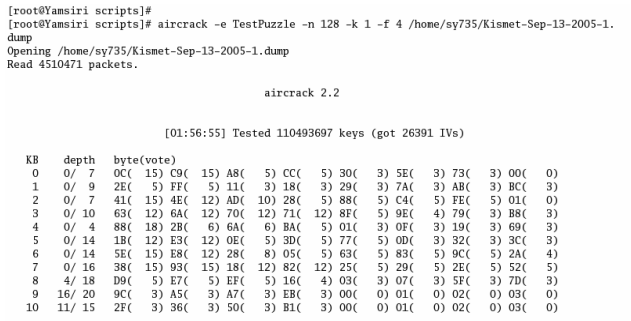

Figure 11(c): The result of cracking kismet-Sep-13-2005-1.dump.

File Name	Unique IVs	Packets (Millions)	Hrs
Airodump.cap.21Sep05	55,057	2.41	9
Airodump.cap.22Sep05	49,487	3.92	20
Kismet-Sep-13-2005-1.dump	26,391	4.51	5

Table 1: Three files are all together reading to be cracked.

However, luckily; we found the key when we cracked by reading the three files together. The key was recovered when the numbers of unique IVs was 81,339 as shown in the Figure 12 although the total unique IVs of these three files were 130,935. Therefore, it can be stated that it is not necessary to capture packets continuously. On the other hand, to capture packets for collecting unique IVs in different situations would be better because of duplicated IVs avoidance.

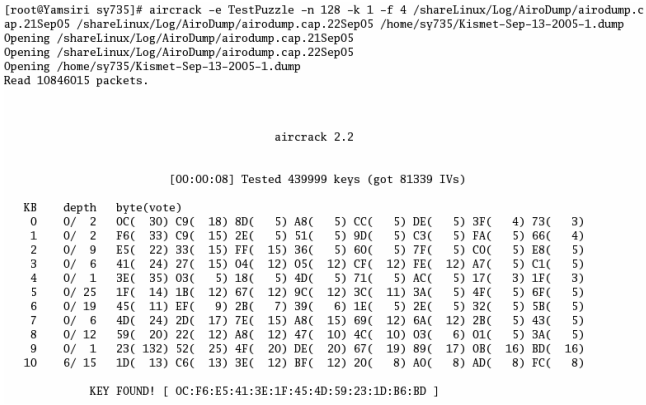

Figure 12: The result of cracking the three files.

Given details, we are able to crack the WEP key by capturing approximately ten million packets which are stored in three files in thirty-four hours. The achievement requires roughly eighty thousand unique IVs to be collected and only eight seconds cracking. After we cracked a 104-bit WEP key, we then conducted another experiment in order to study whether it is better to have more IVs or fewer IVs. We afterwards got the “more IVs” file and cracked it. As a result, a file of 136,038 unique IVs still could not be cracked in two hours, as shown in Figure 13.

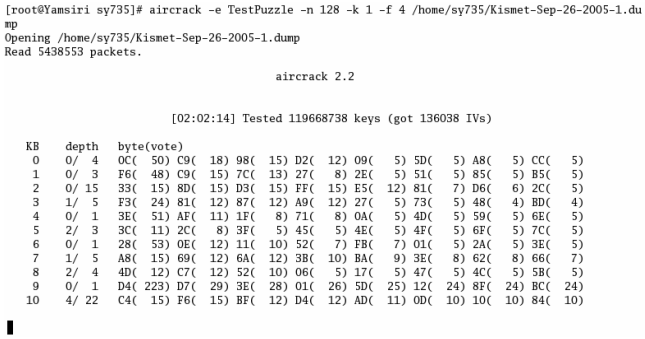

Figure 13: The result of cracking Kismet-Sep-26-2005-1.dump.

Conclusion, a 128-bit key can be cracked in eight seconds with only thirty-four hours’ capturing. Moreover, we found that WEP cracking can be done intermittently by using either Airodump or Kismet as IVs collecting tools. The “more IVs” file is not regularly better than the “less IVs” file. The only thing that can assist cracking a WEP key is testing. This is because this attack is a passive attack based on statistical analysis. Ultimately, it can be concluded that it is easy to attack a WEP key whether it is a 64 bit key or a 128 bit key.

3.4 Surveys

We also surveyed three locations to investigate wireless encryption key use in the real world. This survey is wireless packets detection in University of Wollongong at the Security Lab (referred to as ‘University’) in Wollongong City and in Sydney at the Entertainment Complex (referred to as ‘Sydney’). Table 2 and Figure 14 provide a comparison of the use of encryption keys in these three locations.

Location	# Stations	None		Open		WEP		WPA		No data - WEP or WPA		Unknown	
UOW (Security Lab)	17	2	12%	2	12%	9	53%	4	24%	0	0%	0	0%
Wollongong City	27	13	48%	0	0%	3	11%	0	0%	11	41%	0	0%
Sydney (Entertainment Complex)	129	50	39%	0	0%	18	14%	1	1%	53	41%	7	5%

Table 2: A comparison of the use of encryption keys in these three locations.

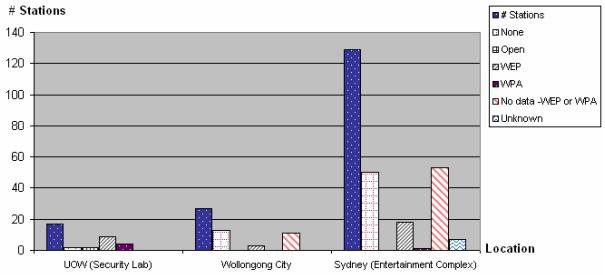

Figure 14: A comparison of the use of encryption keys in these three locations.

As illustrated in Table 2 and Figure 14, the number of stations in the University that do not use wireless encryption key is not much(only twelve percent), but in Wollongong City and Sydney the numbers are higher (forty-eight and thirty-nine percent respectively). It is shown that about fifty percent of non-academic users utilize wireless network without employing any encryption key. Furthermore, there are about fifty percent of stations in University still use WEP keys as their encryption keys. Some stations in Wollongong City and Sydney had no detected data they may use either WEP or WPA; hence we can only conclude that WEP keys are still used in both cities. Moreover, we also study the percentages of wireless access point names, shown in Table 3 and Figure 15 respectively.

Location	# Stations	No Name		"default"		Brand Name		Corp. Name		Defined Name	
UOW (Security Lab)	17	6	35%	0	0%	0	0%	1	6%	10	59%
Wollongong City	27	6	22%	1	4%	3	11%	8	30%	9	33%
Sydney (Entertainment Complex)	129	37	29%	8	6%	17	13%	26	20%	41	32%

Table 3: A comparison of three locations with their wireless accesses point names.

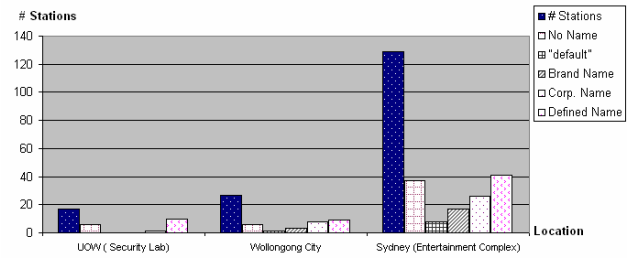

Figure 15: A comparison of three locations with their wireless accesses point names.

Table 3 and Figure 15 demonstrate that most stations in University indicate their APs with defined names—excluding corporate names and AP brand names —which seem to be good names because it means attackers are not able to guess their locations. In contrast, the AP names that are based on their AP brand names or their corporate names seem to be bad names. This kind of name is found in Wollongong City in forty-one percent and in thirty-three percent in Sydney. The percentage of bad names is marginally more than the percentage of good names in both cities.

3.5 A summary of experiments and Surveys

Our experiment has shown that it is possible, easy and cheap to recover a WEP key that is designed to have authentication and integrity. In addition, cracking a WEP key by collecting packets intermittently can increase the possibility of recovering a key. Moreover, our survey has shown that although the weakness of WEP keys has been known since 2001, current wireless users do not recognize or even do not know how to secure their wireless networks. As a result, an information security standard is essential.

4. Conclusion

We carried out experiments to study the need for wireless security compliance in standards such as AS7799. We conclude that the Australian Standard AS7799 should include wireless security compliance. If AS7799 includes wireless security compliance, companies adopting the standard will ensure that wireless networks are secured. Additionally, our experiments show that it is possible, easy and cheap to recover a WEP key. Therefore, we suggest that AS7799 ought to be state that the proven weak wireless protocol should not be used in wireless networks. If the control is stated as above, WPA or WPA2 are suitable encryption protocols for wireless network at the moment. Furthermore, we argue that companies need to be audited quarterly to satisfy the AS7799 information security standard. Nevertheless, we maintain that the AS7799 information security standard is suitable for corporations to ensure their information is secured. On the other hand, we also recommend that the standard itself should be reviewed at least once a year owing to rapid technological development. Moreover, standards which harmonize AS7799 and IEEE 802.11 need to be developed for wireless LANS.

References

[1] Allan, A. (2003). *Impact of in-house electronic security standards on projects such as eDRS* [Online]. Available URL: http://www.ciap.health.nsw.gov.au/project/gp/downloads/secure/Implementation_Group/Meetings/2003/papers/Impact_ofEIS_on_eDRS.doc [Accessed 1 March 2005]

[2] Bridge Point Communications. (2002). *Bridge Point Going for AS 7799.2:2000 Information Security Management System Certification* [Online]. Available URL: http://www.bridgepoint.com.au/news/2002/NewsletterDec02.htm [Accessed 1 March 2005]

[3] Bowman, B.(2005). *How to Secure Your Wireless Home Network with Windows XP* [Online]. Available URL: http://www.microsoft.com/windowsxp/using/networking/learnmore/bowman_05february10.mspx [Accessed 2 October 2005]

[4] Brown, L. (2004). *Security Risk Management Overview* [Online]. Available URL:

http://www.unsw.adfa.edu.au/~lpb/seminars/auugsec04.html [Accessed 1 March 2005]

[5] Cheung, H.(2005). *How To Crack WEP – Part 1: Setup & Network Recon* [Online]. Available URL: http://www.tomsnetworking.com/Sections-article118.php [Accessed 2 October 2005]

[6] Dearne, K. (2005). *Stricter corporate rules create compliance panic* [Online]. Available URL: http://australianit.news.com.au/comment/0,10190,12154632%5E24170%5E%5Enbv%5E24169,00.html [Accessed 1 March 2005]

[7] Devine, C. (2005). *Aircrack Documentation* [Online]. Available URL: http://www.cr0.net:8040/code/network/aircrack/ [Accessed 1 October 2005]

[8] Ellsmore, N. (2003). *BS7799 Adoption "Appalling", AS7799 Even Worse* [Online]. Available URL: http://sift.com.au/press_room.asp?data=050801044D01050502074B7043545D4E4849455742436C475B5A5A454B [Accessed 27 March 2005]

[9] Fedora Project. (2005). *The Unofficaial Fedora FAQ* [Online]. Available URL: http://www.fedorafaq.org/ [Accessed 1 September 2005]

[10] Flextronics Software Systems. (2005). *Wireless LANs: Security, Reliability and Scalability Issues* [Online]. Available URL: http://www.hssworld.com/whitepapers/whitepaper_pdf/Wireless_LAN.pdf [Accessed 2 October 2005]

[11] Foundry Networks (2005). *The Evolution of Wireless* [Online]. Available URL: http://www.foundrynet.com/solutions/wireless/ [Accessed 2 October 2005]

[12] Goh, C. (2005). *On the Net with Chris Goh: Year in Review* [Online]. Available URL: http://www.echonews.com/1104/computing.html [Accessed 27 March 2005]

[13] Gralla, P. (2004). *WiFi Hardware Sales Jump 9% Over Last Year* [Online]. Available URL: http://informationweek.com/story/showArticle.jhtml?articleID=54200184 [Accessed 1 October 2005]

[14] IEEE. (2004). *THE IEEE Wireless Standard : Overview*[Online]. Available URL:http://standards.ieee.org/wireless/overview.html#802.11 [Accessed 2 July 2005]

[15] Intelligraphics.(2005). *Introduction to IEEE 802.11* [Online]. Available URL: http://www.intelligraphics.com/articles/80211_article.html [Accessed 8 July 2005]

[16] Internet Security Systems. (2001). *802.11b and Corporate Networks* [Online]. Available URL: http://documents.iss.net/whitepapers/wireless_LAN_security.pdf [Accessed 3 October 2005]

[17] Kidman, A. (2005). *Security concerns as jobs go offshore* [Online]. Available URL: http://www.openoutsource.com/resource-dated18377-Security%20concerns%20as%20jobs%20go%20offshore.phtml [Accessed 27 March 2005]

[18] Kershaw, M. (2005). *Kismet* [Online]. Available URL: http://www.kismetwireless.net [Accessed 1 October 2005]

[19] McCabe, K. (2005). *THE IEEE 802® LAN/MAN STANDARDS COMMITTEE, Networking Standards For Advanced Telecommunication* [Online]. Available URL: http://standards.ieee.org/announcements/bkgnd_802stds.html [Accessed 2 July 2005]

[20] Office of E-Government. (2005). *Step up to a more secure environment for your information* (Home Page) [Online]. Available URL: http://www.govsecure.wa.gov.au [Accessed 27 March 2005]

[21] Ossmann, M.(2004). *WEP: Dead Again, Part 1*[Online]. Available URL: http://securityfocus.com/infocus/1814[Accessed 1 October 2005]

[22] Ou, M.(2005). *WEP cracking for dummies* [Online]. Available URL: http://blogs.zdnet.com/Ou/?m=200505[Accessed 3 October 2005]

[23] Pollard, A. (2003).*Developing an AS/NZS 7799.2 and ISO 17799 Compliant Information Security Management System* [Online].Available URL: http://www.bridgepoint.com.au/Documents/7799paper.pdf [Accessed 1 July 2005]

[24] Rager, AT. (2001). *Wepcrack* [Online]. Available URL: http://wepcrack.sourceforge.net/[Accessed 1 October 2005]

[25] Rice University.(2001). *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP* [Online]. Available URL: http://www.isoc.org/isoc/conferences/ndss/02/proceedings/papers/stubbl.pdf [Accessed 1 October 2005]

[26] Symbol Technologies (2005). *Securing Enterprise:Understanding and achieving next-generation wireless* [Online]. Available URL: http://www.symbol.com/assets/files/SecureEntAirWP.pdf [Accessed 1 October 2005]

[27] United States Government Accountability Office. (2005). *Federal Agencies Need to Improve Controls over Wireless Networks* [Online]. Available URL: http://www.gao.gov/new.items/d05383.pdf [Accessed 1 October 2005]

[28] Verton, D. (2001). *Black Hat: Users warned about wireless LAN holes* [Online]. Available URL: http://www.computerworld.com/networkingtopics/networking/story/0,10801,62144,00.html [Accessed 1 October 2005]

[29] Wikipedia. (2005). *IEEE 802.11i* [Online]. Available URL: http://en.wikipedia.org/wiki/802.11i [Accessed 8 July 2005]

[30] Wikipedia. (2005). *WEP* [Online]. Available URL: http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy [Accessed 2 October 2005]

[31] Wincom Technology Corp. (2005). *Wireless Networking Tutorial* [Online]. Available URL: http://www.winncom.com/html/wireless.shtml [Accessed 1 July 2005]