Linux Access Point and IPSec Bridge

T. H. Tseng and F. Ye

Department of Electrical Engineering
Tamkang University
Tamsui, Taiwan, R.O.C.
E-mail: rexchen@ug.ee.tku.edu.tw

Abstract

The main idea of this paper is to present an upper-layer security solution to solve security problems of the wireless network. The IEEE 802.11 standard defines the Wired Equivalent Privacy (WEP) Protocol. The goal of WEP is to provide data privacy to the wireless network. It is generally believed that the current wireless access points have a big security problem with WEP protocol. To solve this problem, a combination of Linux-based access point and IPSec bridge has been brought up to secure the wireless network.

***Key Words*:** Linux, IPSec, Bridge, Access Point, WEP, 802.11, Security, Wireless

1. Introduction

In recent years, the surge in notebook computers and PDA has caused an increase in the aspect of people's computing. At the same time, various kinds of wireless networks have gained a great deal of popularity. As a result, wireless network security is becoming much more important than ever before. Take the application of data transmission in the radio broadcast as an example. Due to the frequency and convenience of data transmission application nowadays, it is obvious that the necessity of communication protection is gradually turning to be a must, which can be an effective interception [1].

For the safety of the internal resources, many organizations usually especially install an Internet firewall to block attacks. However, the deploy of a wireless network opens a "back door" for attacker's access to secret data by radio waves. The advantage of wireless network is that it shares the waves in free space, which almost includes locations outside the physical control of wireless network administrators, such as the company's parking lot, facilities of other floors, or nearby high-rise buildings. Under the consideration of long-distance communication and to ensure the wireless network a safety system, which is fundamentally less secure than a wired one, it has the indispensability to build a sounder network space.

2. The 802.11 Wireless Network

2.1 Wireless Network Technologies

Protocol 802.11 [2] refers to a family of WLAN (wireless LAN) specifications developed by a working group at the Institute of Electrical and Electronic Engineers (IEEE). 802.11 defines the standard for WLANs, encompassing some disparate technologies.

2.1.1 802.11e (Quality of Services)

Supplementary to the MAC layer provides QoS support for LAN applications. It will apply to 802.11 physical standards a, b, and g. The purpose is to provide classes of services with managed levels of QoS for data, voice, and video applications.

2.1.2 802.11f (Roaming)

The standard defines the registration of access points within a network and the interchange of information between access points while a user is handed over from one access point to another. 802.11f is currently working on specifying an IAPP (Inter Access Point Protocol), which provides the necessary information that access points need to exchange and to support the 802.11 distribution system functions.

2.1.3 802.11i (MAC Enhancements for Enhanced Security)

802.11i is still involved in development and approval processes. The specification might be officially released by early 2003. After it's available, 802.11i will provide replacement technology for WEP security. Initially, 802.11i will provide TKIP (Temporal Key Integrity Protocol) security that it is allowed to add to existing hardware with a firmware upgrade. In fact, TKIP is a temporary protocol for use until manufacturers implement AES at the hardware level.

2.2 The WEP Protocol Security Problem

WEP provides data confidentiality using a stream cipher called RC4 [3]. It's easy to break RC4 encryption if a second instance of encryption with a single key (a key stream reuse) can be isolated [4]. The WEP designers have been aware of this situation, so they build into WEP a so-called Initialization Vector (IV) [5], a 24-bit value that changes with each packet and is appended to the unchanging shared secret key to minimize the likelihood of "key collision" [6]. By exploiting the statistical properties of this weakness [7], an attacker can crack any message in hours [8], independently of others. AirSnort (http://airsnort.shmoo.com/) is one of the best-known WEP cracking tools, which employs this attack [9].

The sender calculates the CRC of the frame payload and appends it to the WEP encapsulated frame. It then selects a new IV (initialization vector) and appends this to the WEP shared key to form a "per-packet" key, and uses the result to generate an RC4 key schedule [10]. The IV value contains 24bits dynamic serial number. The frame then uses RC4 to generate a key stream equal to the length of the frame payload plus CRC [11]. The encrypted frame generates key stream against the plaintext payload data and CRC by XOR. The encrypted process is shown in Figure 1, and the format of the encrypted frame is shown pictorially in Figure 2 as well. To decrypt a frame protected by WEP, the receiver simply reverses the encryption process. First, the receiver extracts the IV from the frame, appends it to the WEP shared key, and generates the "pre-packet" RC4 key schedule. The receiver uses RC4 to produce a key stream. The receiver thus XOR this key stream with the packet's encrypted payload and verifies the CRC of the decrypted payload data to certify that the frame data is correctly decrypted [12].

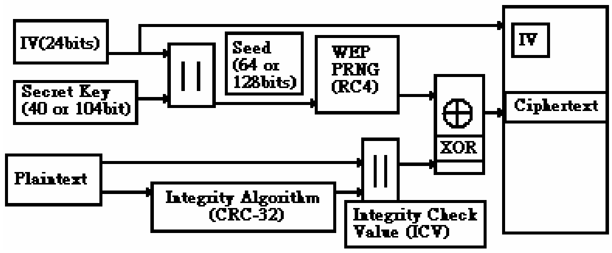

Figure 1. The encrypted process

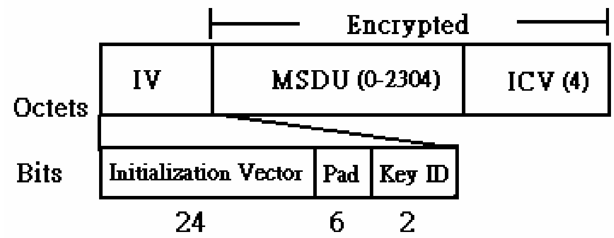

Figure 2. The format of the encrypted frame

The WEP IV is 24 bits long. Each frame transmission selects one of these 16M keys and encrypts the data under the key. The IV values can be reused, so we will get the same IV after 16M frames. Then IV database can be built to compute the WEP shared key [13].

3. IPSec Bridge System

A well-known WEP is weak, but if stronger security is needed, then upper-layer security protocols must be used. The IPSec is a common name for security extension of the IP protocol. Implementing the security on the IP layer is good because the applications won't need to be aware of it. The IPSec is very secure and has more options. The IPSec vs. WEP is shown in Table 1.

Table 1. The IPSec vs. WEP

Security Service	IPSec	WEP
Anti-Replay	Yes (IPSec seqnum)	No
Data Privacy	Yes (DES/3DES)	Yes (RC4)
Data Integrity	Yes (MD5/SHA)	Yes but weak (CRC-32)
User Authentication	Yes (XAUTH with pwd or cert)	No
Mutual Authentication	Yes (preshared key, pub/priv keys or certs)	No
Key Management	Yes (PKI)	No
Auto rekeying	Yes (SA lifetime)	No
External Users DB	Yes (RADIUS, LDAP)	No
Accounting, Monitoring	Yes (RADIUS, SNMP)	No

3.1 Build Linux Access Point

In this system, an IPSec bridge in Linux access point is built to secure the wireless network. One of the reason why choosing Linux as our operating system is that it is one of the most widely supported open source operating systems. The other reason is that we can put features in our system. Linux is not only stable but also low cost to ownership. Meanwhile, Linux makes it easy to build access point system, and port to Embedded System to make a real access point. In the experiment, we set up a computer with Linux OS and installed wireless lan card based on Intersil's Prism2 chip set. Run HostAP driver under RedHat Linux 7.3 [14]. The driver supports HostAP mode, and meantime, it takes care of IEEE 802.11 management functions in the host computer and acts as an access point. The Linux distributions have already included the bridge-utils package, and therefore, building a bridge system can be easy. The system has three network interfaces, which will be shown in Figure 3. In the chart, br0 is bridge network interface, eth0 is 10/100 network interface, and wlan0 is wireless network interface. As it shows, it can be verified these as different traffic on each interface by tcpdump software. It is feasible to test some ICMP packet from the wireless client, and monitor the two interfaces by tcpdump. The tcpdump result is the same as that shown in Figure 4. In accordance to this, the access point works correctly under Linux.

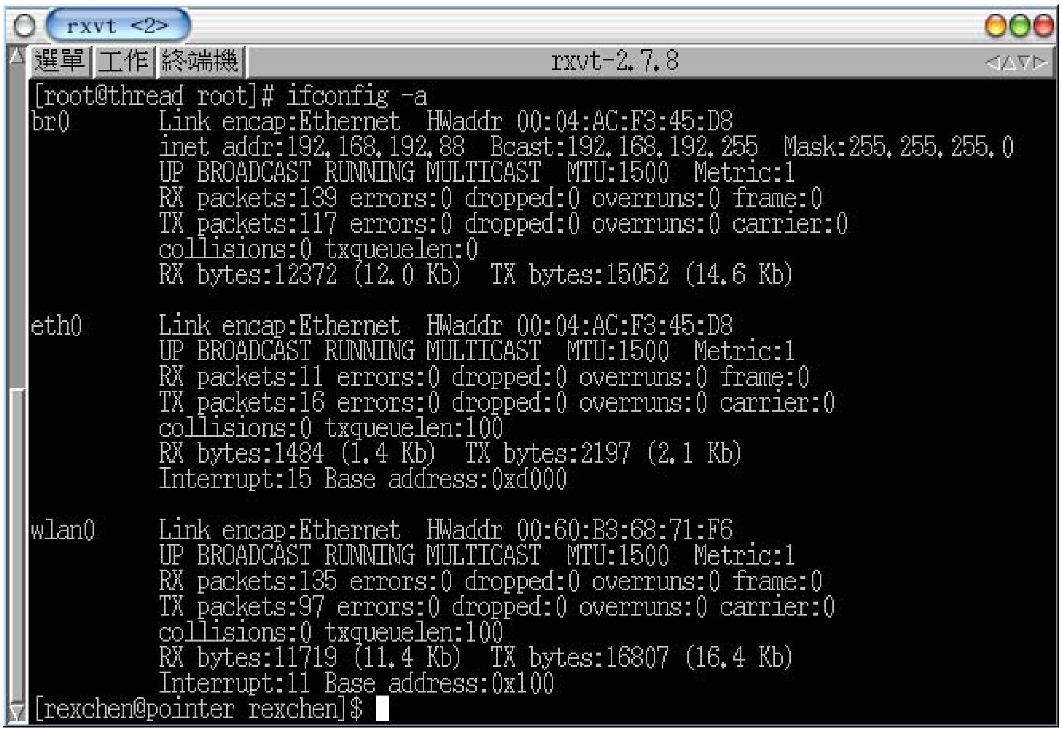

Figure 3. The Host AP's network interface

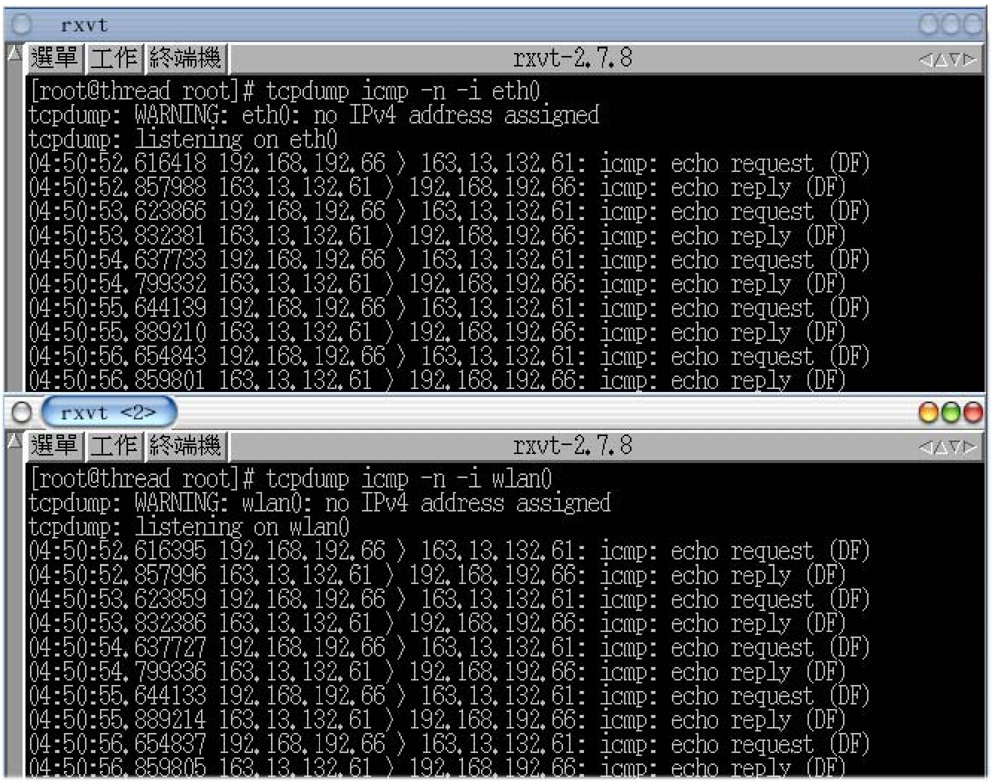

Figure 4. The tcpdump result

3.2 Build IPSec Bridge

Linux FreeS/WAN is an implementation of IPSec and IKE for Linux [15]. It can be used to secure the traffic. These services allow you to build secure tunnels through untrustful networks. This is an open source IPSec project, and as a result, it's allowed to get the source from the Internet. Then the source code of an incoming and outgoing packet sources is modified, and the packets are automatic encrypted and decrypted in the bridge interface. After that, ICMP packets are tested after set up IPSec, and comes different results with IPSec, that are shown in Figure 5. The packets response is IPSec ESP packets, so IPSec Bridge works just fine.

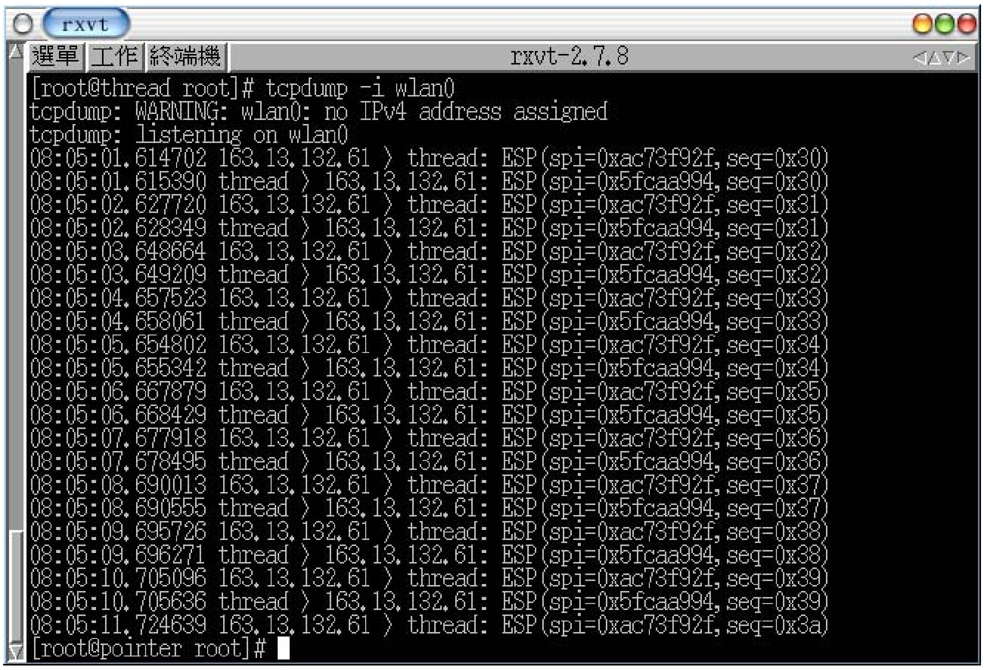

Figure 5. The IPSec ESP packets response

3.3 IPSec Bridge Infrastructure Network

The novel thing about IPSec Bridge is how it secures the wireless network between the client notebook and IPSec Bridge. In many networks, we use IPSec tunnel to secure our network between the client notebook and IPSec gateway. It has the necessity to change the router, which is quite expensive. From above description, the IPSec tunnel Infrastructure network can be constructed as shown in Figure 6. The IPSec Bridge is built in access point, and the IPSec tunnel is only between client notebook and access point on air. In local networks, we have firewall to protect Internet, thus there's no need of IPSec router. It only needs to secure the wireless network by IPSec access point that is shown in Figure 7.

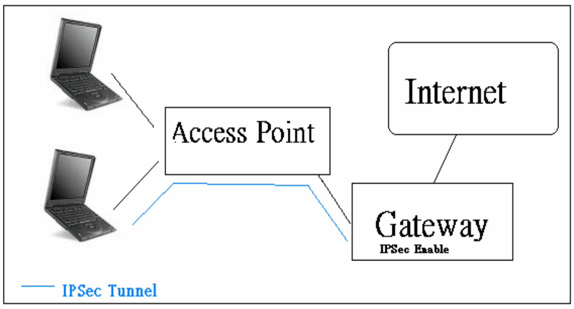

Figure 6. IPSec Tunnel

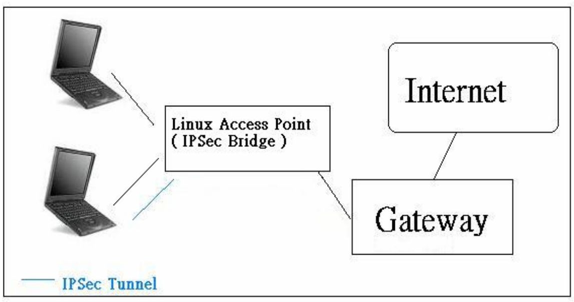

Figure 7. IPSec Bridge

4. Performance

It is for certain to lose some performance by using WEP. Linux tests the performance about the impacts of WEP with Lucent Gold wireless card [16]. The test machine is Pentium III-600 with 320MB ram. This will generate a 4MB file, and try to send file by any rate and WEP. This test is a measure of how fast data moves between a wireless client and access point. The tests send a file from client to client, measures how much time it takes, and calculates the result in Mbps. The result is shown in Table 2. As we can see, the transmission has 10% loss with 128bits WEP and 5% loss with 40bits WEP in 11 Mbps. The WEP performance depends on wireless network card's chip, because the network card’s chip has hardware-based WEP options. And the IPSec bridge performance depends on access point's CPU. In this system, the Linux access point suffers slight loss in performance.

Table 2. WEP and IPSec Performance test result

Without WEP	Wihout WEP	With 40bits WEP	With 128bits WEP	IPSec Enabled
1 Mbps	1,183,441 bps	1,142,451 bps	1,175,440 bps	1,182,314 bps
2 Mbps	2,127,334 bps	2,123,123 bps	2,116,332 bps	2,125,443 bps
5.5 Mbps	3,650,111 bps	3,651,332 bps	3,551,871 bps	3,700,011 bps
11 Mbps	4,524,322 bps	4,300,121 bps	4,082,889 bps	4,511,998 bps

5. Conclusions

It will improve the security, secrecy and managerial convenience of wireless networks constructed by IPSec Bridge. We don't change any network gateway to support it. IPSec Bridge developed on Linux environment can be ported to embedded system to manufacture the Access Point series products. We can use the board—WL11000 SA-N combined with AMD Eln-SC400 (CPU)—to produce Access Point as shown in Figure 8. The embedded system is better than personal computers.

Nowadays there are more and more developments of Linux Access Point evolving various functions, such as the well performance of RADIUS (Remote Access Dial In User Service) Protocol, Firewall, or supports of QoS. It is feasible to adopt these given programs to design Access Point which are matched our demands.

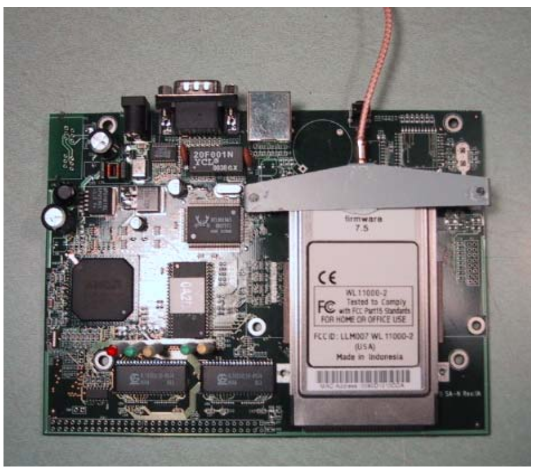

Figure 8. WL11000 SA-N combined AMD Eln-SC400

References

[1] Borisov, N., Goldberg, I. and Wagner, D., "Intercepting Mobile Communications: The Insecurity of 802.11," http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

[2] "LAN MAN Standards of the IEEE Computer Society. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification. IEEE Standard 802.11, 1997 Edition", *IEEE Standard 802.11*, 1997.

[3] Rivest, R. L. *The RC4 Encryption Algorithm*, March 1992.

[4] Mantin, I., "Analysis of the Stream Cipher RC4," *Master's Thesis*, Weizmann Institute of Science, 2001.

[5] Fluhrer, S., Mantin, I. and Shamir, A., "Weaknesses in the Key Scheduling Algorithm of RC4," *Proceedings of SAC '01*, 2001.

[6] Fluhrer, S., Mantin, I. and Shamir, A., "Attacks on RC4 and WEP," *Cryptobytes*, 2002.

[7] Golic, J., "Linear Statistical Weakness of Alleged RC4 Key Stream Generator," *Proceedings of EUROCRYPT '97*, 1997.

[8] Mantin, I. and Shamir, A., "A Practical Attack on Broadcast RC4," *Proceedings of Fast Software Encryption '01*, 2001.

[9] AirSnort Project, http://airsnort.shmoo.com/.

[10] Fluhrer, S. R. and McGrew, D. A., "Statistical Analysis of the Alleged RC4 Key Stream Generator," *Proceedings of Fast Software Encryption '00*, 2000.

[11] Knudsen, L. R., Meier, W., Preneel, B., Rijmen, V. and Verdoolaege, S., "Analysis Methods for (Alleged) RC4," *Proceedings of ASIACRYPT '98*, 1998.

[12] Dawson, E. and Nielsen, L., "Automated Cryptanalysis of XOR Plaintext Strings," *Cryptologia*, pp. 165-181, April 1996.

[13] Walker, J., "Unsafe at Any Key Size: An Analysis of the WEP Encapsulation," Intel Corporation, November 2000.

[14] HostAP Driver for Intersil Prism2/2.5/3, http://hostap.epitest.fi/

[15] FreeS/WAN Project, http://www.freeswan.org/ .

[16] Lucent Orinoco, *User's Guide for the ORINOCO Manager's Suite*, November 2000.

Manuscript Received: Feb. 21, 2003
and Accepted: Apr. 21, 2003