보안성을 개선한 WEP 프로토콜 제안

장성렬*, 이영경†, 이경현‡
부경대학교 정보보호학과*
부경대학교 전자계산학과†
부경대학교 전자컴퓨터정보통신공학부‡

An Enhanced Protocol for WEP Security

Sung-Ryul Chang*, Young-Kyung Lee†, Kyung-Hyune Rhee‡
Interdisciplinary Program of Information Security, Pukyong Nat'l University*
Dept. of Computer Science, Pukyong Nat'l University†
Division of Electronic, Computer and Telecommunication Engineering, PKNU‡

E-Mail : jiya686@lisia21.net*, twinkel@lisia21.net†, khrhee@pknu.ac.kr‡

요 약

최근 무선 LAN을 이용한 기술과 제품들이 활발히 출시되고, 이러한 무선환경에 관한 표준 또한 활발히 제정되고 있는 실정이다. 이러한 기술의 발전과 함께 무선 LAN 환경에서의 보안문제가 관심의 대상이 되고 있다. 본 논문에서는 무선 LAN의 표준인 IEEE 802.11에서 사용하고 있는 보안 모델인 WEP과 그 개선방안인 WEP2에 대하여 고찰하고 알려진 취약점 및 개선방안을 제안한다.

1. 서론

무선 네트워크에서 사용되는 파장은 매체에 대한 한계를 가지지 않으므로 유선상에서 쓰는 물리적 보안 방식은 무선 환경에서는 적절하지 않다. 무선상으로 모든 데이터를 송·수신하기 때문에 무선 네트워킹 시스템은 유선환경과는 다른 방식의 보안상황이 고려되어야 하지만 그 보안 강도는 유선과 비슷하거나 그 이상의 효과를 지녀야 한다.

무선 LAN 보안 서비스를 제공하는 서비스 망은 무선 단말기와 AP(Access Point) 및 인증 서버로 구성된다. 무선 단말기와 AP간은 무선 접속 구간이며, 유선망에 연결되어 타 네트워크와 연동하는 브리징 기능을 수행하는 AP와 사용자 단말에게 인증 서비스를 제공하는 인증 서버는 유선 구간에 위치한다.

본 논문에서는 AP와 사용자 단말간의 무선 접속 구간의 보안을 위해 제공되는 IEEE 802.11 WEP(Wired Equivalent Privacy) 프로토콜의 취약점에 대해서만 다루기로 한다.

802.11 WEP 프로토콜은 아래와 같은 기준들에 의해 설계되었다.

첫 번째, 유선과 거의 같은 수준으로 보안상 견고해야 한다.

두 번째, 단말기는 AP가 제공하는 주파수 범위를 스스로 동기화 되어야 한다.

세 번째, 무선 단말기와 같은 소형의 디바이스에서도 WEP 프로토콜이 구현될 수 있을 만큼 계산상 효율적이어야 한다.

네 번째, 무선 LAN 제품들은 자유로이 수출·입 할 수 있게 각 국의 규정에 따라야 한다는 것이다.

마지막으로 선택적이어야 한다. WEP 프로토콜은 선택적인 사항으로써 모든 802.11 시스템의 필수 요건이 아니라, 필요 시 선택적으로 사용할 수 있어야 한다.

본 논문의 구성은 다음과 같다. 2장에서 WEP가 사용하고 있는 암호화 및 복호화 알고리즘에 대해 살펴보고, 3장에서는 WEP와 WEP2에 대한 소개와 그 취약점에 대해 분석하며, 4장에서는 그 WEP2를 개선하기 위한 방안을 제시하고, 5장에서는 결론을 맺는다.

2. WEP 프로토콜

WEP 프로토콜은 802.11 표준에서 제공하는 보안 메커니즘 중 하나로서, 무선을 사용하는 네트워크 트래픽에 기밀성(비밀성)을 제공하기 위해 디자인되었다. 서론에서 간략히 언급했듯이 인증 서버와 관련된 노드에 대한 인증에도 이 WEP 프로토콜이 시도-응답 메커니즘과 함께 사용된다. 하지만, 여기서는 WEP 알고리즘 자체의 보안성에 초점을 맞춘다.

기본적으로 WEP 알고리즘에서는 공유 비밀키를 사용하여 암호화, 복호화를 시행하며, 그 과정은 다음과 같다.

◆ WEP 암호화 과정

그림 1은 WEP 암호화 과정을 나타낸다.

(1) 40비트 RC4 비밀키를 24비트의 IV(Initialization Vector)와 연접하여 총 64비트인 seed값을 생성한다.

(2) 이 seed값을 RC4를 기반으로 한 WEP PRNG (Pseudo Random Number Generator)를 이용하여 의사난수 키 시퀀스를 생성한다.

(3) 데이터 무결성을 위해 평문에 무결성 알고리즘(CRC-32 checksum)을 사용하여 ICV(Integrity Check Value)를 생성하고 이를 평문과 연접한다.

(4) 평문과 (3)에서 만들어진 ICV를 연접한 값에 (2)에서 출력된 키 시퀀스(키 스트림)를 XOR하여 암호문을 생성한다.

(5) 암호문과 함께 4바이트의 확장된 데이터를 추가하여 전송된다.

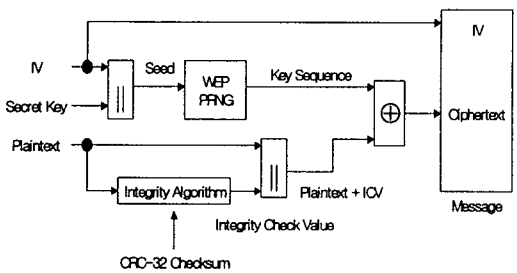

그림 1. WEP 암호화 과정

여기서 4바이트의 확장된 데이터란 암호문에 추가된 3바이트의 IV와 키 시퀀스 ID 2비트와 padding 6비트로 구성된다. WEP 데이터 프레임은 그림 2와 같이 구성된다.

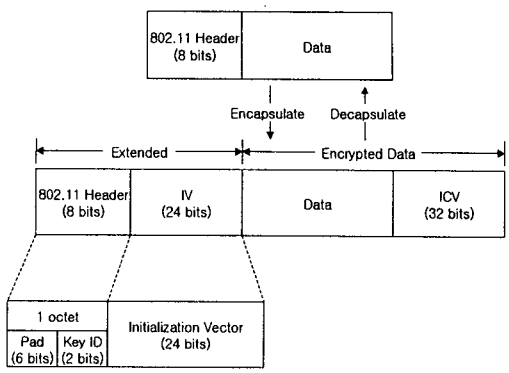

그림 2. WEP 캡슐화 및 데이터 프레임

◆ WEP 복호화 과정

그림 3은 WEP의 복호화 과정을 보여준다.

(1) 전송받은 메시지에서 3바이트의 IV는 암호화와 마찬가지로 수신자의 RC4 비밀키와 연접하여 WEP PRNG에 입력할 seed값을 생성한다.

(2) WEP PRNG는 조합된 키와 IV가 연접된 seed값을 이용하여 RC4 키 시퀀스를 생성한다.

(3) 전송받은 메시지에서 암호문을 (2)에서 생성한 키 시퀀스와 XOR 연산을 수행한다.

(4) 전송된 데이터의 무결성 검사를 위해, 생성된 평문을 암호화 시 사용하였던 CRC-32 checksum을 사용하여 ICV"을 생성한다.

(5) 메시지에 대한 무결성 체크는 (3)에서 출력된 ICV와 (4)에서 생성된 ICV"을 비교하여 수행할 수 있다.

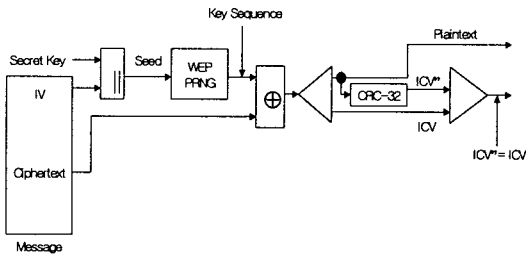

그림 2. WEP 복호화 과정

3. WEP 취약점과 WEP2

WEP에 대한 많은 취약점이 알려져 있으며, WEP의 취약점은 크게 3 가지로 나눠볼 수 있다.

◆ WEP 프로토콜의 취약점

첫 번째, RC4라는 스트림 암호의 특성상 발견되는 취약성이라고 할 수 있겠다. 스트림 암호는 같은 키를 두 번 사용하기에 안전하지 않다. 그래서 이 속성을

물려받은 WEP 프로토콜 또한 안전하다고 할 수 없다.

암호를 생성하기 위한 키 스트림 비트를 $k_1\ k_2\ k_3$이라 가정하고, 송신자(encryptor)는 이 키 스트림을 평문 스트림인 $p_1\ p_2\ p_3$ 와 XOR 연산을 하여 암호문 스트림 $c_1\ c_2\ c_3$ 을 생성한다.

$$c_i = p_i \oplus k_i \quad \text{for} \quad i = 1, 2, 3, \cdots$$

반대로 수신자(decryptor)는 암호문 스트림 $c_1\ c_2\ c_3$와 키 스트림 $k_1\ k_2\ k_3$ 를 XOR하여 평문 스트림 $p_1\ p_2\ p_3$를 복호한다.

$$p_i = c_i \oplus k_i \quad \text{for} \quad i = 1, 2, 3, \cdots$$

악의적인 도청자가 전체의 스트림을 도청해서 기록할 수 있다고 가정하자. 만약 도청자가 i 번째 비트의 평문 값을 알아냈다고 가정하면 암호문 스트림은 아래의 식에 의해 i 번째 비트의 키 값을 알아낼 수 있을 것이다.

$$k_i = c_i \oplus p_i$$

두 번째, 키 스트림의 재생공격에 대한 취약성이다. 서로 다른 두 개의 메시지에 대하여 모두 같은 키와 IV 쌍으로 이루어진 키 스트림을 사용하기에 관찰된 두 메시지로부터 정보를 아래와 같이 얻어 낼 수 있다.

$$Cipher_1 \oplus Cipher_2$$
$$= \{Plain_1 \oplus (IV, k)\} \oplus \{Plain_2 \oplus (IV, k)\}$$
$$= Plain_1 \oplus Plain_2$$

세 번째, IV의 크기가 매우 작아서 키 재생공격으로부터 보호되지 못한다. IV는 24비트의 길이를 가지고 있다. 이는 한 패킷 당 2^{24}개의 키 중에 하나를 선택하여 전송하고, 계속 재생한다면 초당 11M 비트를 전송하는 802.11b 무선 LAN 제품에서는 아래와 같은 계산 시간 내에 키가 깨어질 수 있다.

$$\frac{1500\,bytes}{packet} \times \frac{8\,bits}{1\,byte} \times \frac{1\,\text{sec}}{11\,Mbits} \times \frac{1\,Mbits}{10^6\,bits} \times 2^{24}\ packets$$

$$\approx 18.300\,\text{sec} \approx 5\,hours$$

◈ WEP2 프로토콜과 그 취약점

현재까지의 무선 LAN에서 데이터에 대한 보안을 위해서는 기존의 WEP보다 개선된 WEP2 프로토콜의 사용을 권고하고 있다. WEP2 프로토콜은 무선 LAN 사용자에게 데이터의 보안성을 제공하기 위한 암호화 기법으로써 데이터의 암호화, 복호화에 동일키를 사용하는 스트림 암호 방식이다. AP의 서비스를 받는 모든 단말기는 128비트 크기의 비밀키를 미리 공유하고 있다.

WEP2 프로토콜은 128비트의 비밀키와 128비트의 IV를 결합하여 이를 RC4 기반의 PRNG에 입력시켜 난수 키 시퀀스를 생성하고, 이를 이용해 평문을 암호화하여 전송한다. 그 이외의 과정들은 WEP 프로토콜의 암호화, 복호화 과정과 동일하다.

WEP2 프로토콜은 비밀키와 IV 크기를 늘려 기존의 WEP보다 보안성이 강화된 것은 사실이다. 하지만, 키와 IV 크기가 늘어나서 악의적인 공격에 대한 해독 시간만을 늘렸을 뿐 기존의 스트림 암호방식이 가지고 있는 취약성과 여전히 키와 IV 쌍으로 전송하기 때문에 두 개의 암호문을 도청하여 그 값을 XOR 연산함으로 평문이 노출되는 재생공격의 가능성은 여전히 남아있다.

4. WEP2를 보완하기 위한 제안

WEP는 스트림 암호의 특성으로 인한 취약점 및 재생공격 그리고 24비트의 작은 IV 크기로 인해 모든 키가 크랙 당할 위험 등이 존재했으며, WEP2는 이러한 점을 보완하여 키와 IV 크기를 128비트로 늘려 크랙 당할 시간적 위험으로부터는 조금 벗어났지만 여전히 재생공격의 위험은 남아있음을 알 수 있다.

본 논문에서는 이러한 취약점을 개선하기 위한 방안을 제안한다. 제안된 방안에서는 IV에 랜덤한 타임스탬프를 추가하여 전송한다. 제안 방안은 매 세션마다 IV가 달라지기 때문에 모든 메시지마다 동일한 IV를 사용하는 기존의 WEP2가 가지고 있는 재생공격으로부터 안전할 수 있다.

그림 4는 본 논문에서 제안하는 WEP2 암호화 과정을 나타낸다. 제안 방안은 IV를 128비트에서 64비트로 감소시키고 64비트의 타임스탬프를 연접시켜 WEP2 PRNG에 입력한다. IV가 줄어들어 IV로부터 키를 계산해 내는 시간은 감소하였지만, 키 값을 알아낸다고 하더라도 매 세션마다 타임스탬프가 포함된 다른 IV가 전송되기 때문에 키를 알아내기 위한 노력은 의미가 없게 된다. 또한 기존의 WEP2에서 사용한 비트와 동일한 비트 수를 사용함으로써 WEP2의 계산시간과 동일한 계산시간을 얻을 수 있다.

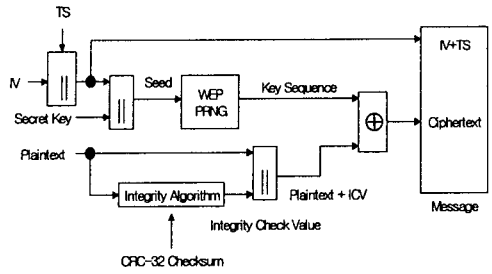

그림 4. 제안한 WEP 암호화 과정

그림 5의 복호화 과정도 타임스태프가 추가된 것만 다를 뿐 그림 3과 동일하게 이루어진다.

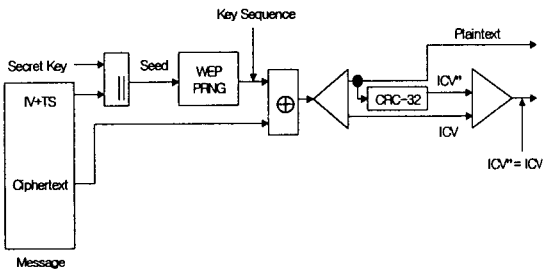

그림 5. 제안한 WEP 복호화 과정

따라서 아래 식과 같이 서로 다른 2개의 암호문을 도청한다 하더라도 키와 IV가 매 세션마다 다르기 때문에 그로부터 평문을 도출해 낼 수 없게 된다.

$$Cipher_1 \oplus Cipher_2$$
$$= \{Plain_1 \oplus (IV+TS, k)\} \oplus \{Plain_2 \oplus (IV+TS', k)\}$$
$$= Plain_1 \oplus Plain_2 \quad (X)$$

5. 결론

WEP는 무선 LAN의 데이터 링크계층(단말기와 AP) 상의 보안에 관여하기에 소형 단말기와 같은 하드웨어에 이보다 더 강한 보안기법을 사용한다면 보안 측면에서는 우수하지만 효율성은 어떻게 될지 미지수여서 무선 제품의 가장 큰 장점을 감소시킨다. 이런 이유로 WEP에서는 보안강도는 다소 약하지만 대칭형 암호보다 약 10배정도 빠른 RC4 스트림 암호 기법을 사용하고 있다.

따라서 WEP는 보안상 많은 공격들에 노출되어 있으며, 이를 보완하기 위한 방안으로 WEP2의 사용을 권고하고 있으나 이 또한 키와 IV 크기를 증가함으로써 계산 복잡도를 증가했을 뿐 보안적인 측면에서는 개선된 점이 없다고 할 수 있다. 본 논문에서는 IV에 랜덤한 타임스탬프를 추가하는 방안을 제안하여 WEP2의 약점인 재생공격으로부터 안전성을 보장하여 데이터 전송을 수행할 수 있게끔 하였다.

[참고문헌]

[1] 김상철 "무선랜보안", 한국정보보호진흥원/기반보호사업단 해킹바이러스상담지원센터

[2] 김신효, 강유성, 정병호, 조현숙, 정교일 "무선 LAN 정보보호 기술 표준화 동향", 정보보호학회지, 2002. 08

[3] 박창섭 "암호이론과 보안", 대영사, pp.221~224, 2001. 08

[4] Jesse Walker "Unsafe at any key size; An analysis of the WEP encapsulation" Tech Rep. 03628E, IEEE 802.11 committee, 2000. 03, http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip

[5] Jesse Walker "Overview of 802.11 Security", jesse.walker@intel.com

[6] Princy C. Mehta "Wired Equivalent Privacy Vulnerability", 2001. 04

[7] RSA Loboratories "WEP Fix using RC4 Fast Packet Keying", tech note, http://www.rsasecurity.com/rsalabs/technotes/wep-fix.html

[8] Sultan Weatherspoon, Network Communications Group, Intel Corporation "Overview of IEEE 802.11b Security", Intel Technology Journal Q2, 2000

[9] William A. Arbaugh "An Inductive Chosen Plaintext Attack against WEP/WEP2", University of Maryland, College Park

[10] William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan "Your 802.11 Wireless Network has No Clothes" University of Maryland, 2001. 05

[11] 802.11 working group, "http://grouper.ieee.org/groups/802/11/index.html"