근거리 무선 통신의 안전한 보안 모니터링 기법에 관한 연구

서대희, 이임영
순천향 대학교 정보기술공학부

A Study on Secure Monitoring in Short Distance Wireless Communication

Dae-Hee Seo, Im-Yeong Lee
Division of Information Technology Engineering. SoonChunHyang University

요약

무선통신 기술이 급속도로 발전하는 가운데 Mobile 기기들의 연결을 위한 근거리 무선 통신 기술이 필요하게 되었으며, 많은 연구가 진행되고 있다. 최근 국내 무선국에서는 Bluetooth와 WLAN을 국내 근거리 무선 통신기술의 표준으로 제정한바 있다. 따라서 본 논문에서는 근거리 무선 통신 기술인 WLAN에 적용한 보안 모니터링 기법을 제안함으로써 무선이라는 통신 환경에서 Mobile 기기들의 여러 가지 취약 요소들에 대한 주기적인 감시를 통해 안전한 통신이 가능하는 보안 모니터링 기법을 제안하고자 한다.

1. 서 론

최근 정보통신 산업의 급속한 발전으로 보다 자유롭고 안전하며, 신뢰성 있는 인터넷의 확장과 더불어 발전하고 있는 기술이 근거리 무선 통신 기술이라 할 수 있다.

근거리 무선 통신은 주로 사용자가 중심이 되는 Mobile 기기들간의 통신을 위해서 연구되고 있다. 따라서 사용자의 프라이버시 보호를 위해 각 Mobile 기기들의 보안 사항에 대한 주기적인 감시가 필요하다.

이러한 감시는 사용자 주변에 흩어져 있는 디바이스를 통해 사용자의 프라이버시를 안전하게 보호하기 위해 반드시 요구되는 보안 기법중의 하나라고 할 수 있다[1].

따라서 본 논문에서는 근거리 무선 통신에 적용할 수 있는 보안 모니터링 기법을 WLAN(Wireless Local Area Network)에 적용하여 제안함으로써 사용자가 사용하는 Mobile 기기들의 여러 가지 보안 사항을 주기적으로 모니터링 할 수 있는 기법을 제안하고자 한다.

2. WLAN의 개요

IEEE(Institute of Electrical and Electronics Engineers)는 사용자들의 LAN에 대한 무선 접근의 요구에 발맞추어 Mobile 장비, 랩톱, PDA, 네트워크에 선이 없이 통신이 가능한 WLAN을 802.11의 표준으로 발표하고 계속적인 연구를 지속하고 있다. IEEE는 유선 LAN과 연동되는 WLAN 장비를 지원하면서 WEP(Wired Equivalent Privacy)라 불리우는 부가적인 암호화 기능을 규정함으로써 접근제어, 프라이버시를 보호하는 기능을 제공한다.

WEP의 접근 제어는 올바른 WEP 키를 보유하고 있지 않는 사용자들이 네트워크에 대한 접근을 보호할 때 사용되며, 프라이버시는 올바른 WEP 키를 가지고 있는 사용자들에 의해서만 무선랜 구간에서 사용하는 자료들을 암호화하거나 복호화 시킬 수 있도록 하는 것이다[1].

3. WLAN의 위험 요소와 보안 대책

WLAN은 다음과 같은 4가지의 위험 요소를 분석하고 보안에 대해 살펴보고자 한다[2][3][4].

① 하드웨어 분실

WLAN을 이용하는 하드웨어의 분식의 경우 정당한 사용자 일지라도 Mobile 기기의 MAC 주소나 WEP 키를 사용하여 권한을 얻지 못하게 될 수 있다. 그렇게 때문에 이를 반드시 관리자에게

통보해야 하며 관리자는 분실된 Mobile 기기의 MAC 주소와 WEP 키를 더 이상 사용하지 못하도록 해야 한다. 따라서 WLAN에서 보안 정책을 수립하는데 있어 중요한 것은 사용자에게 독립적인 보안 정책과 동적인 키의 생성하여 사용하는 것이 그 대책이라 할 수 있다.

② 인증

WLAN에서는 단방향 인증으로 사용자를 인증하여 합법적인 사용자들에 대한 공격의 위험성을 내포하고 있다. 따라서 상호인증 체계로 부적절한 단방향 인증의 취약점을 보완해야 한다.

③ 전력 & 프로세싱

Mobile 기기에 대한 계속적인 활성화 전력 사용을 유도함으로써 기가 자체를 일시적으로 사용하지 못하도록 하는 전력 소모 공격을 들 수 있다. 따라서 현재 진행중인 프로세싱과 접속 요구 요청에 따라 이를 감시하고 처리할 수 있는 주기적인 관리체계가 필요하다.

④ 중앙 집중적인 보안 관리 체계

사용자를 중심으로 분산되어 있는 Mobile 기기들간의 강력한 수준의 이용 가능한 보안 수준을 제공하여 중앙 집중적인 효율적인 보안 관리체계를 보장하는 것이다.

4. 제안 방식

본 논문에서는 WPKI 기반의 WLAN 환경에서 Mobile 기기에 내장된 기지 Agent를 이용하여 AP(Access Pointer)와 유선으로 연결된 중앙 서버의 보안 모니터링을 통해 현재 사용자 주변의 Mobile 기기의 보안 사항을 모니터링 함으로써 공격자로 의심되는 제 3자로부터의 안전한 근거리 통신이 가능한 방식을 제안한다.

4.1 시스템 계수

WLAN에 적용한 보안 모니터링을 위한 시스템 계수이다.

* (중앙서버 : D, AP : P, Agent : A, Mobile 기기 : M)

$*_p, *_q$: *의 공개키, 개인키

ID_* : *의 시스템 메시지

m_* : *의 이벤트 메시지

$Cert_*$: *의 공개키 인증서

r_* : *에서 생성한 의사난수

T_* : *의 타임 스탬프

Sig_* : *의 공개키 서명값

$H()$: 안전한 해쉬 함수

g, n : 공개된 시스템 계수

4.2 프로토콜 진행 단계

[단계 1] 이벤트 발생 및 통보 단계

Mobile 기기내에 활성화 된 기지 Agent에서 보안 정책에 위배된 이벤트가 발생했을 경우 이를 Mobile 기기에 통보하고 중앙 서버의 이벤트 응답 메시지를 대기하는 단계이다.

① Mobile 기기에 포함된 기지 Agent는 Mobile 기기 자체의 보안 정책에 위배되는 이벤트가 발생했을 경우 이를 Mobile 기기에 전송한다.

② 이벤트 발생을 통보 받은 Mobile 기기는 다음을 계산한다. X_M, e_M, C_M을 계산한 뒤 $(ID_A \| X_M \| m_M \| C_M \| g^{r_{M_1}})$, $Cert_M$, T_M를 AP에 전송한다.

$$X_M = (g^{r_{M_1}} \times r_{M_2} \bmod n)$$

$$e_M = H(X_M \| m_M)$$

$$C_M = H(ID_M \| e_M) \oplus H(g^{r_{M_2}} \times P_{M_p}) \bmod n$$

[단계 2] 중앙 관리 서버와 통신단계

단계 2는 Mobile 기기에서 발생한 보안 이벤트에 대한 중앙 관리 서버의 보안 정책의 수정과 이벤트에 대한 보안 대처방안을 Mobile 기기에게 안전하게 전송하는 단계이다.

① Access Pointer는 전송받은 $(ID_A \| X_M \| m_M \| C_M \| g^{r_{M_1}})$, $Cert_M$, T_M을 중앙 서버의 공개키로 암호화 한 뒤 자신의 공개키 인증서와 함께 $(V_{P_D} \| Cert_P)$를 전송한다.

$$V_{P\_D} = E_{D_p}(ID_A \| X_M \| m_M \| C_M \| g^{r_{M_1}})$$

② 중앙서버는 전송받은 $Cert_P$를 확인한 뒤 V_{P_D}를 자신의 개인키로 복호화 하여 다음을 계산하여 무결성을 검증한다.

$$e_M' = H(X_M \| m_M)$$

$$C_M' = H(ID_A \| e_M) \oplus H(g^{r_{M_2}} \times p_M)$$

$e_M' = e_M$ 이고 $C_M' \stackrel{?}{=} C_M$ 이면 Mobile 기기의 공개키 인증서를 확인하고 전송된 이벤트

메시지 m_M에 해당되는 응답 메시지 m_{res}과 함께 다음을 계산한 뒤 Access Pointer에게 V_{D_P}, $Cert_D$, T_D를 전송한다

$$X_D = (g^{r_{D_1}} \times r_{D_2} \bmod n)$$

$$e_D = h(X_D \| m_{res})$$

$$C_D = H(ID_D \| e_D) \oplus H(g^{r_{D_1}} \times p_D) \bmod n$$

$$V_{D\_P} = E_{D_P}(ID_D \| X_D \| m_{res} \| C_D \| g^{r_{D_1}})$$

③ Access Pointer는 전송받은 V_{D_P}, $Cert_D$, T_D에서 중앙서버의 공개키 인증서와 타임 스탬프를 확인하고 V_{D_P}와 자신의 공개키 인증서 $Cert_P$를 Mobile 기기에 전송한다.

$$(V_{D\_P} \| Cert_P)$$

④ Mobile 기기는 전송받은 $(V_{D_P} \| Cert_P)$에서 Access Pointer의 공개키 인증서를 확인하고 자신의 개인키로 V_{D_P}를 복호화 한 뒤

$$e_D' = H(X_D \| m_{res})$$

$$C_D' = H(ID_D \| e_D) \oplus H(g^{r_{D_1}} \times P_{D_p})$$

$e_D' = e_D$ 이고 $C_D' \stackrel{?}{=} C_D$ 이면 중앙서버의 m_{res}를 기지 Agent에 ID_M과 함께 전송한다.

$$(m_{res}, ID_M)$$

[단계 3] 세션키 설정 단계

기지 Agent는 중앙 서버의 이벤트 응답 메시지에 맞는 보안의 재설정과 Mobile 기기의 계속적인 보안 모니터링을 위한 세션키 설정 단계이다.

① 중앙 서버로부터 전송된 보안 정책에 따라 기지 Agent는 Mobile 기기는 보안 업데이트를 통해 보안 정책을 수정하고 계속적인 보안 모니터링을 위해 사용자의 PIN번호를 이용하여 Z를 생성한 뒤 Mobile 기기에 전송한다.

$$Z = H(PIN \| r_{M_1})$$

$$(r_{M_1} \| Z \| T_A)$$

② Mobile 기기는 전송 받은 $(r_{M_1} \| Z \| T_A)$를 자신의 공개키 서명값과 암호화 된 V_{M_P}, T_M를 Access Pointer에 전송한다.

$$S_M = Sig_{M_q}(ID_M \| T_M)$$

$$V_{M\_P} = E_{D_p}(r_{M_1} \| Z \| T_A)$$

③ Access Pointer는 전송된 S_M, V_{M_P}, T_M을 자신의 개인키로 암호화 하여 S_P를 계산하여 중앙서버에 전송한다.

$$S_P = Sig_{P_p}(S_D \| V_{M\_P})$$

$$(S_P, T_P)$$

④ 중앙 서버는 전송된 (S_P, T_P)를 Access Pointer의 공개키로 서명을 확인 한 후에 자신의 개인키로 V_{M_P}를 복호화 한 뒤 $(r_{M_1} \| Z \| T_A)$를 확인하고 다음을 계산하여 Access Pointer에 V_{D_P}, S_D, T_D를 전송한다.

$$Z' = H(Z \| r_{D_1})$$

$$S_D = Sig_{D_q}(ID_D \| T_D)$$

$$V_{D\_M} = E_{M_p}(r_{D_1} \| K' \| T_D)$$

⑤ Access Pointer는 전송된 S_{D_q}를 중앙 서버의 공개키로 복호화 하여 ID_D, T_D를 확인한 뒤 V_{D_M}를 자신의 개인키로 서명하여 S_P, T_P를 Mobile 기기에 전송한다.

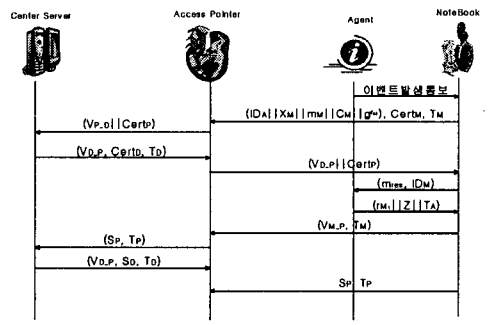
$$S_P = Sig_{P_q}(V_{D\_M})$$

⑥ Mobile 기기는 전송된 S_P를 Access Pointer의 공개키로 서명을 확인한 뒤 V_{D_M}를 자신의 개인키로 복호화 하여 r_{D_1}, Z'를 확인한다.

⑦ Mobile 기기와 중앙관리 서버는 다음을 공통으로 계산하여 새로운 보안 이벤트가 발생하기 전까지 보안 모니터링을 위한 세션키 K를 계산한다.

$$K = H(r_{D_1} \| Z) \oplus H(r_{M_1} \| Z')$$

이상의 내용은 그림 1과 같이 요약해 볼 수 있다.



(그림 1) WLAN에 적용 가능한 보안 모니터링

5. WLAN에 적용 가능한 보안 모니터링 분석

본 논문에서는 근거리 무선 통신중에서도 최근 많은 연구가 진행중에 있는 WLAN에 적용 가능한 보안 모니터링 기법을 제안하였다.

① 하드웨어 분실

WLAN을 이용하는 정상적인 사용자가 하드웨어 기기를 분실했을 경우 사용자의 PIN번호가 없이는 계속적인 중앙서버의 정책을 수행할 수 없으며, 세션키를 생성하는데 의사난수를 이용함으로써 보안 정책과 동적인 세션키를 이용하여 하드웨어 분실에 대한 보완방법이라 할 수 있다.

② 인증

WLAN에서는 단방향 인증으로 사용자를 인증하여 합법적인 사용자들에 대한 공격의 위험성을 내포하고 있지만 제안 방식은 공개키 인증을 이용하여 각 객체간 상호인증 방식으로 단방향 인증의 취약점을 보완하였다.

③ 전력 & 프로세싱

제안 방식은 Mobile 기기의 기지 Agent를 이용하여 현재 프로세싱 뿐만 아니라 전력 사항까지 주기적인 감시와 처리를 통해 Mobile 환경에서 보안 이외의 사항까지를 중앙 관리체계를 통해 안전하게 관리 방식이다.

④ 중앙 집중적인 보안 관리 체계

제안 방식은 사용자를 중심으로 분산되어 있는 WLAN을 사용하는 Mobile 기기들간의 강력한 수준의 이용 가능한 보안 수준을 제공하여 중앙 집중적인 효율적인 보안 관리체계를 보장한다.

6. 결론

본 논문에서는 근거리 무선 통신의 표준중의 하나인 WLAN에 적용한 보안 모니터링 기법을 제안하였다. 그러나 사용자의 안전성을 고려한 보안 뿐만 아니라 Mobile 기기에 대한 무선이라는 특수한 환경에 적합한 보안에 적합한 중앙 감시 모델이 필요하다.

제안 방식은 근거리 무선 통신을 기반으로 이루어지므로 향후 일반화 모델을 제시하고 WLAN 뿐만 아니라 최근 많은 연구가 진행되어 가고 있는 Bluetooth에도 이를 적용해 안전한 보안 모니터링 기법에 대해 적용이 가능하리라 사료된다.

7. 참고 문헌

[1]. http://www.cisco.com (시스코)

[2]. 김희선, 백준상, 이병천, 김광조, "대리서명을 이용한 모바일 에이전트의 안전성 강화 방법 (Enhancing Security of Mobile Agent using Proxy Signature)", KIISC 종합학술발표회(CISC2000), 종합학술발표 논문집 Vol. 10 No. 1, pp.424~437, 성균관대학교, 2000. 11.

[3]. M. Abdalla, W. Cirne, L. Franklin, A. Sterrett, and K. Marzullo, Chimichanga: A Fault-tolerant Asynchronous Communication Infrastructure for Mobile Agents, March 1998.

[4]. http://www.kisa.or.kr (정보보호진흥원)

[5]. 최용락, 소우영, 이재광, 이임영 "통신망 정보 보호", 도서출판 그린, 1997.2.

[6]. 이만영, 김지홍, 류재철, 송유진, 염흥렬, 이임영 "전자상거래 보안 기술", 생능출판사 1999.8.

[7]. 최용락, 소우영, 이재광, 이임영 "컴퓨터 통신 보안", 도서출판 그린, 2001.2.

[8]. Alfred J. Menezes, Paul C.van Oorschot, Scott A. Vanstone "HANDBOOK of APPLIED CRYPTOGRAPHY", CRC, 1996.11.