iPhone에서 802.11 Packet Sniffing공격과 AP분석 연구

이재현*, 박대우**

*호서대학교 벤처전문대학원 IT응용기술학과

A Study on 802.11 Packet Sniffing Attacks and AP Analysis on the iPhone

Jae-Hyun Lee*, Dea-Woo Park**

*Dept. of IT Application Technology, Hoseo Graduate School of Venture

e-mail: leejh9708@paran.com, prof1@paran.com

요 약

Smart Phone 사용자가 증가하고, Smart Phone을 통한 침해사고도 증가되고 있다. 특히 2010년 3분기 국내 Smart Phone의 31%를 차지하고 있는 iPhone은 사용자가 Jailbreak를 통하여 관리자 권한을 스스로 획득함으로서 이를 악용한다면 개인정보 탈취 등 침해사고의 위험이 있다. 본 논문에서는 Jailbreak 한 iPhone을 이용하여 주변의 802.11 Packet Sniffing공격을 실시하고 802.11 AP 취약점을 분석한다. 또한 Google Map을 이용해 주변의 무선 AP 위치를 파악하고 AP의 종류, 위치, 거리, MAC, SSID, RSSI, Channel, 보안설정 정보를 탈취한다. 본 논문을 통하여 스마트폰과 무선 인터넷 보안성 강화를 위한 기초 자료를 제공하게 될 것이다.

키워드

스마트폰(Smart Phone), 탈옥(Jailbreak), 아이폰(iPhone), 스니핑(Sniffing)

I. 서 론

Smart Phone의 활용이 증가함에 따라 Smart Phone을 이용한 침해사고가 증가하고 있다. 또한 스마트폰에서의 802.11 무선인터넷을 통한 개인정보 탈취, ID, Password 등 침해사고가 발생하고 있다.

그림 1과 같이 스마트폰에서의 WiFi 무선랜 네트워크를 통한 무선인터넷을 이용이 증가하고 있어 보안 대책이 시급한 실정이다. 따라서 WiFi 무선랜 네트워크 환경으로부터 개인정보를 보호하기 위해 AP의 보안 및 이용자 대한 정보보호 지침이 실생활 되어야 한다[1].

2010년 3분기 국내 Smart Phone의 31%를 차지하고 있는 iPhone은 사용자가 Jailbreak를 통하여 관리자 권한을 스스로 획득하여 사용자의 편리성을 도모하고 있지만, 공격자가 이를 악용한다면 개인정보 탈취 등 침해사고의 위험이 있다.

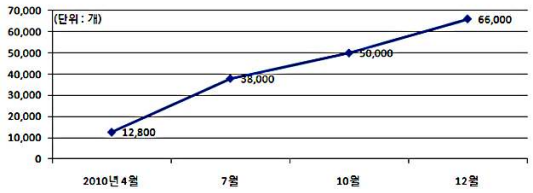

그림 1. 국내 WiFi Zone 추이

본 논문에서는 Jailbreak 한 iPhone을 이용하여 주변의 802.11 Packet Sniffing공격을 실시하고 802.11 AP 취약점을 분석한다. 또한 Google Map을 이용해 주변의 무선 AP 위치를 파악하고 AP의 종류, 위치, 거리, MAC, SSID, RSSI, Channel, 보안설정 정보를 탈취한다.

본 논문의 2장 관련연구에서는 Jailbreak iPhone과 스니핑, 패킷분석에 대해 알아보고 3장에서는 Jailbreak iPhone을 이용한 공격 대상의 AP의 정보를 확보하고 보안 설정된 AP를 해킹하여 Sniffing공격을 시도하고, 4장에서는 스마트폰 무선랜 보안 및 사용자 보안 대책을 제시하고, 5장에서 결론을 내린다.

II. 서 론

1.1 Jailbreak iPhone

iPhone OS에서 제공하지 못하는 기능을 가능하게 하도록 Root 권한을 획득하는 행위로 Jailbreak를 한다. 따라서 사용자는 유료 어플리케이션을 무료로 설치할 수 있고, 인터페이스의 변경도 가능하다. 또한 불법적으로 정보를 제공하는 어플리케이션을 이용해 악의적인 목적으로 사용할 수 있다[2].

1.2 스니핑(Sniffing)

한대의 컴퓨터나 다름없는 Smart Phone의 등장으로 인해 PC, 노트북에서 사용되던 해커들의 Sniffing 공격이 Smart Phone에서도 사용되어지고 있다[3].

1.3 패킷분석

수집한 Wireless 패킷을 분석하기 위해 사용되는 도구로서 네트워크의 취약점을 보안하기 위해 사용된다. 하지만 악의적인 목적의 공격자는 외부 또는 내부에서 네트워크를 통해 전송되는 패킷들을 불법적으로 수집하여 데이터를 분석하기 위해 프로그램을 사용한다. 따라서 개인정보 및 E-mail의 ID, Password 등을 탈취한다. 그림 2와 같이 패킷을 수집한다[4][5].

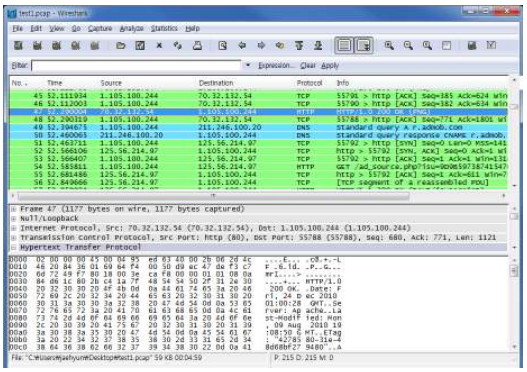

그림 2. Wireshark 패킷분석

III. iPhone을 이용한 Sniffing공격

3.1 실험환경

■ 시스템
- Jailbreak iPhone 4G(v4.1)

■ iPhone Tool
- WiFiFoFum
- iWep Pro
- Aircrack
- Tcpdump
- MobileTerminal

■ 분석도구
- Cain&abel

■ 실험 AP
- SSID : 305
- Security : WEP

■ 실험내용 : iPhone을 이용하여 WEP 보안설정 무선AP에 불법적으로 접근하여 네트워크 Packet을 Sniffing하여 데이터를 분석하여 무선인터넷 사용에 대한 취약점을 분석하고 보안방안을 제시한다.

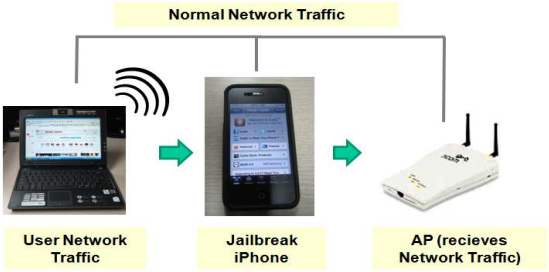

그림 3 iPhone Sniffing 공격 경로

그림 3과 같이 네트워크 환경이 구성하였다.

무선인터넷 연결된 노트북을 이용하여 E-mail에 접속을 시도할 경우 트래픽은 iPhone을 거쳐 AP로 전달되게 된다. 이 방법으로 Wireless 패킷을 탈취하여 사용자의 개인정보, ID, Password 등 정보를 확인한다[6].

3.2 AP 정보수집

iPhone의 Jailbreak를 통해 공격자인 해커는 대상 AP정보를 악의적인 목적으로 Sniffing한다. AP의 정보를 제공하는 어플리케이션을 통해 그림 4와 같이 공격 대상의 AP의 위치, 주변 AP정보, 현재 위치에서 대상 AP와의 거리를 확인할 수 있다.

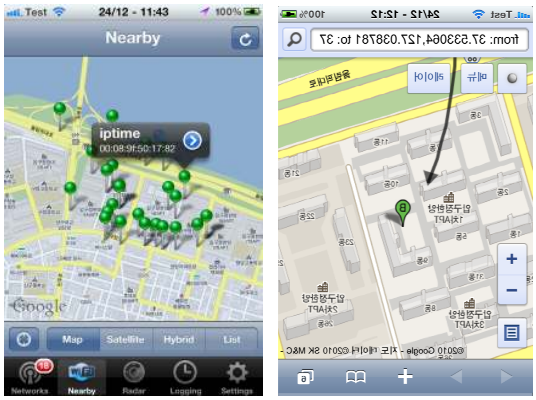

그림 4. iPhone을 이용한 AP 정보수집

또한 그림 5와 같이 AP의 MAC, SSID, RSSI, Channel, Security 등 민감한 정보들을 Jailbreak iPhone을 통해 확인할 수 있다.

그림 5. iPhone을 이용한 AP 정보수집

3.2 AP 공격

사용자들은 편의를 위해 AP의 보안을 사용하지 않거나 Password를 짧고 간단하게 하는 경우가 있다. 해커는 보안수준이 낮은 AP를 대상으로 수집한 정보를 이용해 대상의 AP의 공격을 시도한다. Jailbreak iPhone의 MobileTerminal을 실행시켜 무선랜 구인 Aircrack으로 그림 6과 같이 AP를 공격한다.

공격은 WEP의 약점을 이용한 초기화벡터(IV)를 수집하는 방식으로 동작한다. 따라서 네트워크상에 암호화된 패킷을 Sniffing하여 WEP Key를 해킹한다.

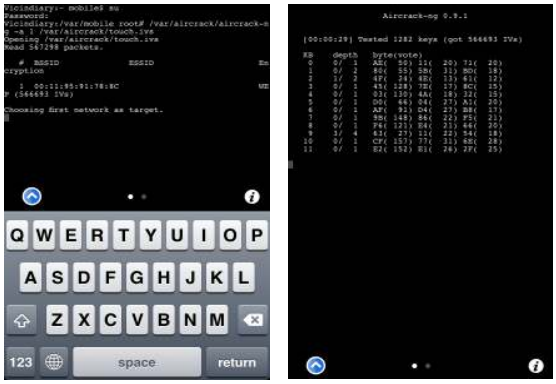

그림 6. Aircrack 공격

그림 7은 수집한 IV를 이용해 WEP Key를 획득하는 그림이다. WEP Key를 이용하여 해커는 보안이 설정되어 있는 AP의 Password를 입력하여 불법적으로 접근하게 된다.

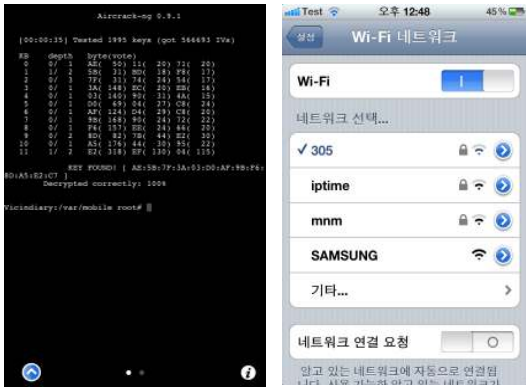

그림 7. iPhone을 이용한 AP 정보수집

그림 8과 같이 해킹한 AP의 접근해 Wireless 패킷을 수집하기 위해 MobileTerminal을 이용해 tcpdump를 동작시킨다.

그림 8. iPhone 패킷 스니핑

공격자가 무선랜 Packet을 Sniffing하는 동안 그림 9와 같이 사용자는 무선랜을 이용해 Google에 ID, Password를 입력시켜 로그인을 시도한다. 이때 Packet은 Jailbreak iPhone의 의해 Sniffing되게 된다.

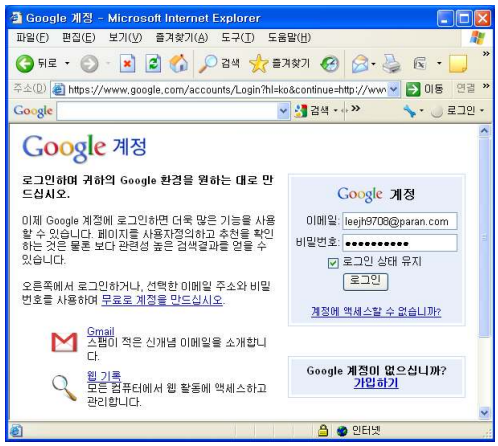

그림 9. 구글 로그인

3.2 분석결과

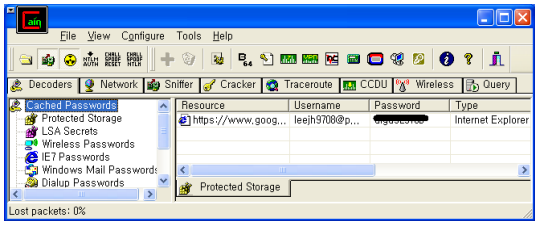

그림 10. 패킷분석 결과

Jailbreak iPhone으로 수집한 Packet을 Cain&abel 툴을 이용해서 분석한 결과 그림 9와 같이 Google계정의 ID, Password가 들어난 것을 볼 수 있다.

IV. 스마트폰 무선랜 보안 및 사용자 보안

- 개인 AP 사용 시에는 외부사용자가 무단으로 이용할 수 없도록 암호화/인증 등에 대한 보안을 설정해야 하며 장비에서 제공하는 가장 높은 보안강도를 선택하고 Key를 주기적으로 변경한다.
- 공공장소에서 무료로 제공하는 AP에 대해서는 개인정보가 쉽게 유출되지 쉽다. 따라서 AP 사용 시 금융거래, 메신저, 이메일, 등 개인정보 포함된 서비스는 하지 않는 것이 좋다.
- 공격자의 악의적 어플리케이션 사용으로 AP의 위치, 정보 등이 확인될 수 있다. 따라서 공격자의 접근을 막기 위해 무선공유기의 SSID를 변경하고 숨김 기능을 설정한다.

V. 결 론

국내 WiFi 무선랜 시장 규모는 지속적으로 증가하고 있으나 신뢰할 수 있는 AP의를 찾기란 쉽지 않다. Smart Phone의 Sniffing 공격에 대한 보안을 위해서는 AP의 보안도 중요하지만 개개인의 정보보호가 중요하다. 사용자는 기존적인 보안 기능 및 정책에 대해서 숙지하고 WiFi 무선랜 사용 시 불필요한 웹사이트, 메신저, 등 서비스 활동은 하지 않는 것이 개인정보를 보호하는 방안이라 할 수 있다.

향후 연구에서는 Smart Phone 침해사고에 대한 네트워크 메신저 환경에서의 실시간 Sniffing 및 해킹을 당하였을 경우 IP 역추적 실시에 대한 기술과 포렌식 방법론에 대한 연구에 기여할 것이다.

참고문헌

[1] Jong Hyun Baek and Young Jun Choi, "Study on analysis of wireless internet service market and plans for activation", Korean Society for Internet Information, pp.281-285, June, 2010.

[2] Apple, http://developer.apple.com/, 'code signing guide', 2009.10.13

[3] Woo-Sung Chun, Dea-Woo Park, "A Study of Forensic on Eavesdropping from VoIP and Messenger through WiBro Network," Korea Society of Computer and Information Transaction, Vol 12, No 3, pp.195-201, May 2009.

[4] Dea-Woo Park, "A Study of Packet Analysis regarding a DoS Attack in WiBro Environments", International Journal of Computer Science and Network Security, IJCSNS (1738-7906), December 2008.

[5] Chang-ki Hong, Chul-ho Kang and Yong-jin Jeong, "Design of the security module for IEEE 802.11i WLAN," The Institute of Electronics Engineers of Korea, pp.288-291, May 2009.

[6] Lee. Sungryoul, Kang. Jimyung, Moon. Hogun, Lee. Myungsoo and Kim. Chong-Kwon, "Per Packet Authentication Scheme Using One-bit in 802.11 Wireless LAN," ScientificCommons, 2008.