스마트폰용 모바일 웹페이지에 대한 취약점 분석*

곽경주, 이광우, 원동호**
성균관대학교 정보통신공학부 정보보호연구소
e-mail : {kjkwak, kwlee, dhwon}@security.re.kr

Analysis of Security Vulnerability on Mobile Webpages for Smartphone

Kyoungju Kwak, Kwangwoo Lee, Dongho Won
Information Security Group, School of Information and Communication Engineering
Sungkyunkwan University

요 약

최근 스마트폰이 빠르게 보급됨에 따라 스마트폰을 이용하여 웹페이지에 접속하는 경우가 증가하고 있다. 따라서 많은 중소사이트와 대형 포털사이트 역시 모바일에 최적화된 형태의 서비스를 제공하기 위해 추가적으로 스마트폰용 모바일 웹페이지를 개발하고 있다. 하지만 스마트폰용 모바일 웹페이지는 보안에 대한 인식이 부족하여 개인정보가 쉽게 노출될 수 있다는 문제점을 가지고 있다. 이에 본 논문에서는 현재 가장 널리 사용되고 있는 모바일 웹페이지에 대한 보안 취약점을 분석하여, 사용자의 개인정보가 노출되는지 확인하였다. 또한 모바일 웹페이지의 문제점을 개인정보 보호 관점에서 분석하였다..

1. 서 론

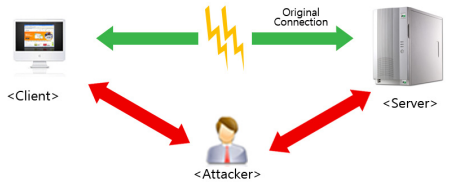
최근 한국인터넷진흥원에서 발표한 통계자료에 의하면, 2007년에서 2010년 사이에 발생한 침해사고는 발생 건수는 8,000만 건에 이르며, 2005년에서 2007년 발생한 개인정보 침해 피해규모는 총 10조7000억원으로 추정된다. 또한 2009년에 집계된 개인정보 침해사고 신고건수는 32,422건이었다[13]. 현재 개인정보 침해를 분석해보면, 점점 대형화, 지능화, 다양화되는 것을 알 수 있다. 이에 대다수의 웹사이트 업체들은 개인정보 침해를 막기 위해 많은 노력을 기울이고 있다. 하지만 최근 스마트폰용 모바일 웹페이지 구축시에는 PC 버전의 웹사이트에서 개발시 고려되고 있는 개인정보 암호화가 적용되지 않는 사이트들이 있다. 이에 본 논문에서는 최근 개발되고 있는 스마트폰용 모바일 웹페이지의 보안 취약점을 분석하고, 이에 대한 대응방안을 살펴보고자 한다.

본 논문의 구성은 다음과 같다. 우선 2장에서는 개인정보 침해에 사용되는 공격 기법과 최근 국회 본회의를 통과한 개인정보보호법에 대해 살펴보며, 모바일 웹페이지와 기존 PC 버전 웹페이지의 차이점을 알아본다. 3장에서는 최근 가장 널리 사용되고 있는 모바일 웹페이지의 취약점을 분석하고, 마지막으로 4장에서 본 논문의 결론을 맺으며 향후 연구를 기술한다.

2. 관련연구

2.1 공격기법

스니핑(Sniffing)이란 악의적인 목적을 가진 공격자가 네트워크 패킷을 훔쳐보는 것을 말한다. 그리고 스니핑을 할 수 있도록 지원하는 도구를 스니퍼(Sniffer)라고 한다. 스니퍼를 이용하여 네트워크를 스니핑하는 경우, 네트워크를 통해 전달되는 모든 패킷에 대한 도청이 가능하므로, 이러한 공격에 대응하기 위해서는 네트워크를 통해 전달되는 패킷을 암호화해야 한다. 스니핑을 응용한 대표적인 공격방법으로는 중간자 공격(Man-In-The-Middle Attack)이 있다. 중간자 공격이란, 공격자가 두 호스트간의 통신을 가로채어 송신자 또는 수신자로 위장하여 행하는 공격을 의미한다.



(그림 1) 중간자 공격

이러한 공격을 위해서는 ARP 스푸핑이 추가적으로 이용될 수 있다. ARP 프로토콜은 네트워크를 통해 데이터를 전송하기 전에 타겟 IP에 해당하는 MAC 주소를 알아내기 위해 사용된다. 하지만 ARP 요청시 상호 간의 인증 과정이 없기 때문에 악의적인 공격자에 의해 악용될 가능성이 있다. ARP 스푸핑이란, 이러한 ARP 의 특징을 이용하여 정상 사용자의 MAC 주소를 자신의 MAC 주소로 변조하는 공격기법이다.

2.2 모바일 웹페이지

모바일 웹페이지는 스마트폰으로 웹사이트 접속시 제한된 자원을 사용하는 스마트폰에 적합한 형태의 경량화된 웹 서비스를 제공한다. 기존 PC 버전에서 제공되는 복잡한 구조의 웹페이지가 아닌 단순한 구조의 페이지를 출력한다.

2.3 개인정보보호법

개인정보란 생존하는 개인에 관한 정보로 성명, 주민등록번호 및 영상 등을 통하여 개인을 식별할 수 있는 정보를 말한다. 이때 개인을 식별할 수 있는 정보에는 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 모든 정보를 포함한다. 올해 3월11일 개인정보보호법이 국회 본회의를 최종 통과하였다. 이 법안이 시행되면 최근 지속적으로 발생하고 있는 개인정보 침해 사고와 현행 법제 체계의 개인정보 관리상 문제점을 해결할 수 있으리라 기대된다. 따라서, 개인정보보호법이 시행될 경우, 스마트폰에서 접속되는 모든 모바일 웹페이지 역시 개인정보 보호가 필요하다. 이에 본 논문에서는 개인정보 보호법이 시행에 앞서 현재 개발되어 있는 모바일 웹페이지의 개인정보보호 실태를 분석하고자 한다.

3. 모바일 웹페이지 취약점 분석

3.1 분석 대상

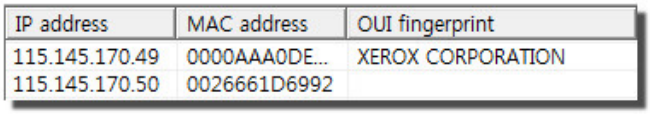
본 논문에서는 국내 대표 포털사이트 (A, B, C)과 블로깅 서비스 업체인 D 사, 마지막으로 국내에서 가장 범용적으로 사용되는 웹 개발 플랫폼인 E 가 적용된 사이트를 대상으로 하였다.

3.2 분석 방법

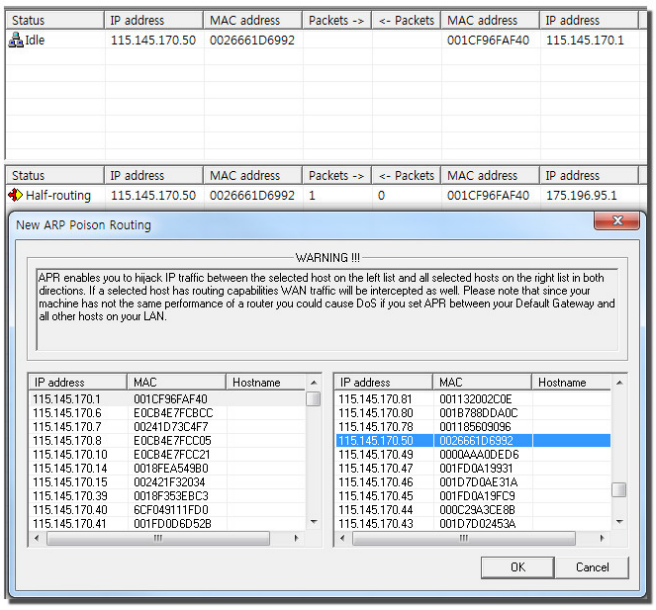
특정 Wi-Fi AP(Access Point)를 대상으로 ARP 스푸핑을 이용하여 운영체제 내에서 ARP 데이터를 기억하고 있는 ARP cache table 을 변조한다. 이후 해당 AP 를 지나는 모든 패킷을 스니핑하였다.

<표 1> 분석 도구

도구이름	용 도	참고 사이트
Cain&Abel	ARP Spoofing	http://www.oxit.it
Wireshark	네트워크 패킷 분석	http://wireshark.org



(그림 2) Cain&Abel MAC 주소 스캔



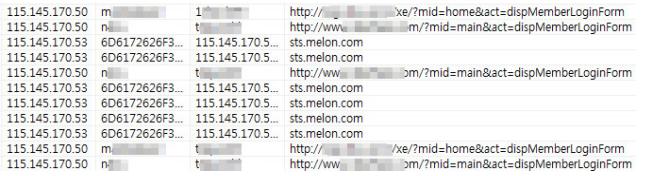
(그림 3) Cain&Abel 분석 대상 선택

3.3 분석 결과

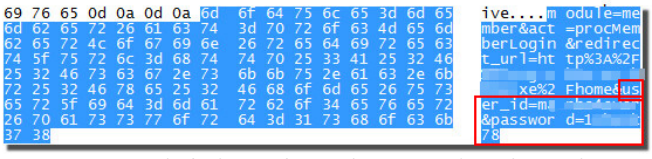
D 와 E 사의 공식 모바일용 웹페이지 등에서 사용자 정보를 암호화하지 않는 취약점이 있었다. 이러한 과정을 통해 취득된 정보는 해당 사이트에 타인으로 위장하여 접속을 하는데 악용될 수 있다.

<표 2> 취약점 분석 결과

대상 사이트	사이트 주소	사용자 정보 암호화	
		PC 용 웹페이지	모바일 웹페이지
A	http://m.xxxxx.com	O	O
B	http://m.xxxx.com	O	O
C	http://m.xxxx.com	O	O
D	http:// xxxxxxx.com	O	X
E	http://xxx.xxxx.xxx	O	X



(그림 4) 개인정보 평문 전송



(그림 5) 개인정보 평문 전송 - 네트워크 패킷

4. 결론 및 향후연구

현재 많은 사용자들이 스마트폰을 이용하여 웹사이

트에 접속하고 있다. 스마트폰은 자원이 제한적이므로 스마트폰용 모바일 웹페이지에 대한 요구가 발생하게 되었다. 이에 따라 대형 포털사이트, 블로그 서비스 업체 및 웹 개발 플랫폼 서비스 제공 업체 등이 앞다투어 모바일 웹페이지 서비스를 개시하였다. 하지만 분석 결과, 기존 PC 버전의 웹 페이지에서 적용되던 개인정보(아이디 및 패스워드) 암호화 전송이 모바일 웹페이지에서는 제대로 구현되어 있지 않다. 이는 서울중앙지법 2006. 4. 28. 선고 2005가단24005【손해배상(기)】, 참조법령: 민법 제750조, 제751조, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제49조에서 알 수 있듯이, 개인정보에 대한 심각한 위협이 될 수 있다. 웹 비즈니스가 보편화되면서 고객정보 등 다량의 개인정보가 수집되어 이용되고 있는 오늘날, 사용자의 개인정보를 보호하기 위해 다양한 관점에서의 정보보호 노력이 요청된다. 이와 함께, 기존의 공공기관 웹사이트를 대상으로 발간된 개인정보 노출방지 가이드라인[15]을 민간 및 스마트폰용 모바일 웹사이트에 대한 가이드라인으로 확대, 적용할 필요가 있다.

ACKNOWLEDGMENT

* “본 연구는 지식경제부 및 정보통신산업진흥원의 “대학 IT연구센터 육성• 지원사업”의 연구결과로 수행되었음” (NIPA-2011-C1090-1001-0004).
** 교신저자, dhwon@security.re.kr

참고문헌

[1] S. Garfinkel, Web Security and Commerce. O'Reilly & Associates, Cambridge, 1997.
[2] V. Ramachandran and S. Nandi, "Detecting ARP spoofing: An active technique," Lecture Notes in Computer Science, vol.3803, pp.239-250, 2005.
[3] Eric Rescorla, "SSL and TLS Designing and Building Secure Systems ", Addison-Wesley, 2001.
[4] Dafydd Stuttard, “Web Application Hacker’s Handbook”, Wiley Publishing, 2008.
[5] Rails, "Ruby on Rails Guides: Ruby On Rails Security Guide", MIT, 2010.
[6] Cain&Abel, "http://www.oxit.it"
[7] Wireshark, "http://www.wireshark.org"
[8] libpcap, "http://www.tcpdump.org"
[9] Wikipedia, "http://www.wikipedia.org"
[10] Burp suit, "http://portswigger.net"
[11] Lawnb, “http://www.lawnb.com”
[12] 법제처, “http://moleg.go.kr”
[13] 의안정보시스템, “http://likms.assembly.go.kr”
[14] 행정안전위원장, 개인정보 보호법안(대안), 의안번호 11087
[15] 행정안전부, “공공기관 개인정보 노출방지 가이드라인 2차 개정판”, 2008