무선 인터넷 환경에서의 해킹/바이러스 분석 및 대응 방안 연구

김행욱*, 윤종철*, 강흥식**
*인제대학교 전산학과
**인제대학교 컴퓨터공학부
email : {hukim, pcman95, hskang}@nice.inje.ac.kr

A Research on the Counter Actions to Hacking and Virus in the Wireless Internet Environment

Haeng-Uk Kim*, Jong-Chul Yun*, Heung-Seek Kang**
*Dept of Computer Science, Inje University

요 약

현재 나와있는 무선인터넷 및 무선 랜의 보안은 아직 미약한 부분이 많이 노출되고 있으며 이에 대한 보안 역시 신속하게 이루어지지 못하고 있는 실정이다. 무선인터넷은 점점 더 많은 사용자들을 확보하고 있고 서비스 또한 다양하게 늘어가고 있는 실정이지만 그에 비례해서 많은 보안의 취약점 또한 증가되고 있는 실정이다. 이에 본 논문은 많은 무선인터넷 디바이스 상에서 이루어 질 수 있는 해킹·바이러스에 대한 취약점을 조사하고 분석하여 무선인터넷 환경에서도 좀더 신뢰성 있는 서비스가 이루어질 수 있도록 하기 위함이다.

1. 서론

"우리는 지금 무선인터넷 세상으로 간다..." 우리가 언제나 그리고 TV속에 이동 통신 사업자, 이동 통신 단말기 제조 사들이 사운을 걸고 광고하고 있는 그래서 우리는 그곳으로 간다고 우리도 모르게 당연시되고 있는 말의 요지이다.

2003년에는 세계적으로 휴대폰의 가입자가 10억이 넘으리라고 전문가들은 예상하고 있다. 이 때문에 무선 인터넷에서의 보안 역시 필연적으로 부각되어지고 있다. 국내의 경우도 이동통신가입자의 증가와 함께 무선 인터넷에 대한 수요 또한 증가하고 있으며 이에 따른 보안의 필요성이 함께 대두되고 있다.

그만큼 무선인터넷이 요즘 차지하고 있는 비중은 날로 증가하고 있는 실정이다. 무선인터넷의 사용자가 증가하고 그에 따른 서비스라든지 멀티미디어 환경 등이 커져가고 있지만 그에 비해 무선인터넷 상에서의 보안은 아직 크게 인식하고 있지 못하는 듯하다. 본 논문은 총 4장으로 구성되어 있으며 1장 서론에서는 무선 인터넷 환경에 대한 설명, 2장에서는 관련 연구로서 무선 인터넷 환경에서의 보안과 해킹 바이러스에 대한 피해 3장은 무선 인터넷 환경에서의 해킹/바이러스에 대한 대응 방안에 대하여 논하고 마지막으로 결론을 맺었다.

2. 관련 연구 및 문제점 분석

2.1 무선 인터넷 환경에서의 보안

그러면 무선 인터넷에서 보안이란 어떠한 측면에서 이해를 해야 하나부터 어떠한 기술들이 현재 사용되고 있는지 그리고 그러한 기술들을 피해서 이루어지는 해킹·바이러스 기술과 그런 취약성을 알아야 할 것이다. 또한 무선인터넷에서 보안이라는 시장이 유선 인터넷 보안 시장과 어떠한 관계를 가지고 발전해 나가고 있는지 또한 살펴봐야 할 것이다.

무선인터넷에서의 보안은 무선인터넷을 이용하여 Mobile commerce, Mobile banking, Mobile trading 등과 같은 전송되는 데이터에 대한 보안 서비스가

먼저 요구되어진다. 이러한 결과 현재 무선 인터넷의 보안이라 하면 당연히 W-PKI, M-VPN 시스템으로 대변되고 있는 실정이다.

또한 무선인터넷의 보안이 비단 Mobile에 국한되어 있는 것은 아니다. 유선인터넷의 경우에는 서버와 클라이언트라는 각각의 다른 보안 환경을 가지고 있다. 예를 들어 서버의 경우에는 Linux, Unix, Windows NT 환경으로 나누어지고 클라이언트 환경에서는 대부분의 환경이 windows로 되어있다. 하지만 무선 환경에서는 Mobile 뿐만 아니라 PDA의 경우에도 Palm, WinCE Pokect Pc, WinCE Hand Held PC, Cellvic 등 수많은 시스템들이 존재한다. 그에 따라 각각의 시스템에 맞는 무선인터넷의 보안이 필요하다. 또한 공중 무선랜 환경에서 보안이 문제되는 이유에 대해서 알아보면, 무선랜 표준인 802.11b에서 규정한 보안 솔루션이 소규모의 사설 무선랜을 대상으로 설계됐기 때문에 현재 서비스되고 있는 공중 무선랜 환경이나 일정규모 이상의 사설 무선랜 환경에서의 보안 요구사항을 충족시켜주지 못하기 때문이다.

2.2 무선 인터넷 환경에서의 해킹/바이러스 피해

무선 인터넷 또한 유선 인터넷과 마찬가지로 해킹의 대상이 되어가고 있는 실정이다. 바이러스, 웜(worm), 트로이 목마 등 악의적인 프로그램들이 파괴활동을 수행하기 위해서는 희생물이 되는 장비가 일정 정도의 프로세싱 성능을 보유하고 있어야 한다. 트로이 목마는 번식력이 없지만 호스트 상의 정보를 염탐할 수 있는 성능을 보유하고 있다. 또한 악의적인 소프트웨어는 소프트웨어 또는 데이터를 공격한다. 따라서 컴퓨팅 자원을 거의 보유하고 있지 않은 장비는 본질적으로 침입에 대한 면역성을 지니고 있다고 할 수 있다. 따라서 성능이 증가할수록 위험도 증가하게 되는 것이다.

현재 전화는 비록 트로이 목마를 호스트할 수 있지만 바이러스 또는 웜을 배양할 만큼 충분한 성능을 가지고 있지 않다. 가장 큰 위험은 트로이 목마가 데이터를 수집하는데 이용되어 해커가 희생자의 비용으로 전화 통화를 하게 되는 문제일 것이다. 그러나 모바일 폰은 기업 IT 시스템에 액세스하기 위한 터미널로서 널리 보급되고 있기 때문에, 트로이 목마가 기밀 데이터를 수집 및 재전송할 수 있는 가능성이 있다. 또한 바이러스는 전파를 위한 수단을 필요로 하고, 그러나 감염은 대규모 사용자에게 급속히 확산된다. 인간 상황에서와 마찬가지로 널리 분산되어 있는 소규모 사용자의 경우 바이러스가 확산될 환경을 조성하지는 않는다. 특정 운영체계를 사용하는 특정 종류의 하드웨어 장비를 감염시키기 위해 작성된 바이러스는 여타 종류의 장비 또는 상이한 소프트웨어를 운영하는 장비에 감염되는 경우가 거의 없다.

2.3 무선 디바이스에 대한 위협 유형 분석

모바일 폰과 같은 무선 디바이스에 대한 위협은 다음과 같다. WAP 폰과 같은 모바일 기술에서 푸시(push) 기능의 역할이다. 이는 소프트웨어가 사용자의 참여 없이도 전화로 다운로드 되도록 한다. 모바일 네트워크의 구성 요소인 음성 메일 시스템은 모바일 폰이 언제나 효과적으로 온라인 상태를 유지한다는 것을 의미한다. 해커는 이러한 액세스 용이성을 자동 전화 걸기 기능과 함께 이용해 콘텐츠가 그 스스로를 복제할 필요도 없이 악의적인 콘텐츠를 널리 확산시킬 수 있다. 따라서 시스템 관리자는 이러한 기능이 악의적인 콘텐츠를 다운로드 하는데 이용되는 것을 방지하기 위한 조치를 취해야 한다. WAP 폰은 WML이라는 특수 마크업 언어를 사용하고 있으며, 이는 HTML의 서브셋에 해당하는 기능을 제공하는 XML 애플리케이션이다. WML 브라우저는 스크립트 언어, 즉 자바스크립트인 WML 스크립트를 지원한다. WAP 폰은 최근 들어 유일하게 높은 인지도를 얻기 시작했으며 아직 해커들의 타깃이 되고 있지는 않다. 따라서 WML 스크립트 언어가 HTML 기반 브라우저 상에서 오용된 것과 동일한 방식으로 악의적인 콘텐츠의 매개 수단이 될 것인지를 평가하기에는 아직 시기상조라고 할 수 있다. 하지만 그러한 부분까지도 염두해 두어야 될 것이라고 생각한다.

3. 예방 및 대응기술 연구

3.1 WAP 기반에서의 보안 프로토콜

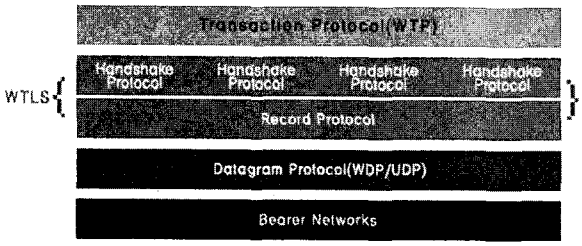
WTLS는 예전에 SSL(Secure Sockets Layer)라고 알려진 산업계 표준인 TLS(Transport Layer Security)에 기반을 둔 보안 프로토콜로써, WAP에서의 WTP와 함께 사용하도록 저대역폭 통신을 위해 최적화되었다. WTLS는 통신개체간의 보안이 필수인 경우에 사용되며, 무선 통신망의 특성과 요구수준에 따라 어플리케이션에서 WTLS 특성을 제어

할 수 있다. WTLS는 다음과 같은 특성을 갖는다.

- 데이타 무결성(Data Integrity) : 단말기와 어플리케이션 서버사이에 전송된 데이타의 변질 혹은 오염되지 않았음을 보장한다.
- 비밀유지(Privacy) : 단말기와 어플리케이션 서버 사이에 전송된 데이타에 대한 비밀을 보장한다. 즉, 도청이 불가하다.
- 인증(Authentication) : 단말기와 어플리케이션 서버에 대한 인증절차를 거친다.
- Denial-of-service protection : 입증되지 않거나 재시도되는 데이타를 감지하여 거절하는 기능을 가진다.

<그림1 WTLS 프로토콜 구조>

위 그림은 WTLS 프로토콜의 구조이다. WTLS를 사용하는 구간에서는 기밀성, 무결성, 사용자 인증의 보안 문제를 해결할 수 있으나, 무선 단말과 유선



인터넷의 웹 서버가 통신을 위해서는 WAP Gateway에서 WTLS와 SSL간 상호 프로토콜 변환이 이루어지는데 여기에서 데이터의 원본이 노출되는 보안의 문제가 발생한다.

<그림2. WAP에서의 보안>

위와 같은 문제는 WAP 게이트웨이가 무선인터넷 서비스 제공자에 종속되어 있는 한 별다른 해결방법

은 없으며, WAP 게이트웨이와 웹 서버의 통합, 응용 계층의 비표준 보안 방식 적용 등을 통해서 해결이 가능합니다. WAP Forum에서는 End-To-End 보안을 해결하기 위해 규격을 보완하는 작업을 수행하고 있으며, 국내에서는 WAP 방식의 WTLS를 사용한 보안 제품을 사용하기 보다는 응용계층에서 데이터 부분만 암호화하여 이를 전송하는 비표준방식으로 End-To-End 보안을 제공하고 있는 실정이다.

3.2 무선 PKI 기술

PKI(Public Key Infrastructure)는 사용자와 프로그램, 시스템간의 디지털 인증과 암호 키를 관리하는 서비스 하부구조로, 인증발급 주체(CA), 키와 인증이 저장되는 곳(repository), 관리기능 등으로 구성되어 있다. 무선 PKI를 구현하기 위해서는 가입자 전자 서명키 생성 기술이 필요, WAP이나 ME에서는 RSA를 사용하고 있다. 무선 이동 단말기들은 유선 장비에 비해 통신 대역폭, CPU 및 메모리의 제한, 배터리 수명, 사용자 인터페이스 등 많은 차이와 제약점을 가진다. 보안에 있어서도 마찬가지로 유선 장비와는 다르므로 무선 이동특성을 고려해 무선 보안을 구현해야 한다. 현재 ECC라는 새로운 공개키 암호 알고리즘이 주목받고 있는 상황으로 이는 RSA와 같은 기능을 수행하지만 적은 CPU 자원을 요구하며 통신 및 저장에 적은 데이터가 사용된다. 그외 인증서 규격의 제정이 필요한데 인증서 규격 표준, 프로파일, 인코딩/디코딩 방식을 고려하여야 한다. 인증서의 유효성을 확인하기 위해 인증서의 상태를 확인해야 하는데 무선의 특성상 매우 중요한 부분으로 인증서 상태에 대한 검증 방식에 대해서도 많은 고려를 해야 하며 인증서에 대한 공고방식을 확보하여야 한다. 해외 무선 보안 서비스 업체들로는 이사인, 베리사인, 소네라, 엔트러스트 등이 있다.

3.3 대응 기술

무선인터넷을 바라보는 시각은 이미 많은 사람들이 유선인터넷과 무선 인터넷을 구분지어 생각하지 않고 있으며, 통합 환경에서의 서비스 제공을 당연한 것으로 받아들이고 있다. 그에따라서 각종 무선과관련된 해킹/바이러스에 대한 대응기술에 대해서 알아볼것이며 가장 적합한 대응기술에 대한 연구또한 이루어져야 할 것이다.

- 대칭키 기반과 공개키 기반 시스템의 연구.
- WPKI 와 M-VPN 비교 및 전망에대한 연구.
- WTLS를 이용한 보안솔루션이 갖고있는 가장 큰문제점인 종단간 (End-to-End)보안문제 연구.
- 아직까지 핸드폰 상에서의 바이러스에 대한 위험은 크지 않지만 PDA 나 팜OS에서와 같은 경우에는 바이러스에 좀더 취약하다. 일반 PC보다는 바이러스가 좀더 제한적이긴 하나 이에 대한 확실한 방안

또한 연구되어야 할 것이다.

또한 단기적 측면에서는 모바일 장비의 낮은 대역폭, 느린 스위칭 속도 및 소형 화면이 그 사용을 제한함으로써 그 자체의 안전한 Application 확보한다. 하지만 이들의 성능이 향상되면 취약성을 고려할 수 있는 수준까지 이들 성능의 활용을 억제하는 것도 중요하다. 그리고 장기적 측면에서, 훌륭한 설계 즉, 처음부터 엑세스 보안 제어 기능을 모든 시스템 및 어플리케이션에 포함시켜 설계를 할 수 있어야 한다.

4. 결론

어차피 보안 솔루션은 필요한 응용분야와 적용되는 인프라에 종속적인 것이기 때문에 시작점이 틀린 것은 당연한 결과일지도 모른다. 그러나 시장과 사용자의 요구에 따라 그리고 인프라의 발전에 따라 기존의 인프라와 자연스럽게 연동될 수 있도록 융합되는 과정을 거치는 것 역시 당연한 결과일 것이다.
향후에는 보안솔루션 뿐만이 아니라 모든 솔루션들이 유무선 인터넷을 통합해 나갈것이며, 그에따른 각종 서비스 또한 활발히 진행되어질 것이다.

본 논문은 확산되어가고 있는 무선인터넷 상에서의 보안 취약점 및 해킹/바이러스에 대한 자료로서 무선 플랫폼 상에서의 개발자나 무선 Device를 사용하는 유저에게 좀더 신뢰성 있는 무선 인터넷 환경을 조성해줄 것이다. 또한 무선 인터넷상에서의 각종 해킹/바이러스에 대한 정보를 DB화 하여 관련 사고에 대해 신속히 대응할수 있는 체계를 만들어줄수 있을 것이다.

급증하고 있는 모바일 해킹 시도의 효과적인 방어를 위해 가장 요구되는, 해킹 기술 자체를 분석하고 대응기술을 개발할수 있도록 한다. 분석 대상이 되는 해킹 기술들은 현존하는 해킹 기술뿐만 아니라 앞으로 발생 가능한 해킹 기술도 포함되며, 이를 위해 발생 가능한 해킹 기술을 사전에 예측하고 분석 가능할수 있을 것이다.

참고문헌

[1]http://cesec.ajou.ac.kr
[2]http://home.ahnlab.com
[3]http://www.wapforum.org
[4]http://ns1.icom21.co.kr
[5]http://www.certcc.or.kr.
[6]김건우 외 2, "이동통신에서의 정보보호기술", Telecommunication Review, 제10권 3호, 2000년 5월.
[7]http://www.kisa.or.kr
[8]http://ns.imgweb.co.k