디지털산업정보학회 논문지 제11권 제3호-2015년 9월
http://dx.doi.org/10.17662/ksdim.2015.11.3.053

모바일 환경에서 개인정보 유출 방지를 위한 개선 연구*

최 희 식* · 조 양 현**

The Study of Improvement of Personal Information Leakage Prevention in Mobile Environment

Choi Heesik · Cho Yanghyun

〈Abstract〉

Recently, number of tablet or Smartphone users increased significantly in domestic and around the world. But violation of personal information such as leakage, misuse and abuse are constantly occurring by using mobile devices which is very useful in our society.

Therefore, in this paper it will talk about the problems in the network environment of the mobile environment such as tablet and Smartphone, Mobile Malware, hacking of the public key certificate, which could be potential threat to mobile environment. This thesis will research for people to use their mobile devices more reliable and safer in mobile environment from invasion and leakage of personal information.

In order to use Smartphone safely, users have to use Wi-Fi and Bluetooth carefully in the public area. This paper will research how to use App safely and characteristic of risk of worm and Malware spreading. Because of security vulnerabilities of the public key certificate, it will suggest new type of security certification.

In order to prevent from the information leakage and infect from Malware in mobile environment without knowing, this thesis will analyze the improved way to manage and use the mobile device.

Key Words : Private Information, Smartphone, Mobile Device, Haking

Ⅰ. 서론

최근 개인정보에 대한 사회적 인식이 개인정보 유출과 사이버 범죄로부터 대중들에게 알려짐으로써 그 중요성이 많이 인식되고 있다. 그러나 그 중요성을 인식하고 있는 만큼 위험으로부터 자신들의 소중한 개인정보를 안정적으로 관리하고 위험을 피할 수 있는 지식적 기반과 기술적인 보호 조치는 갖추어져 있지 않는 게 현실이다.

본 논문에서는 국민 대다수가 사용되고 있는 모바일 환경의 태블릿이나 스마트폰을 사용함으로써 위험에 처할 수 있는 개인정보의 유출·오용·남용 등

* 강원대학교 시스템경영학과 외래교수
** 삼육대학교 컴퓨터학부 교수(교신저자)

개인정보 침해 사례가 지속적으로 발생함에 따라 국민의 프라이버시 침해는 물론 명의도용, 전화사기 등 정신적·금전적 피해를 예방하고 개선하고자 한다[1]. 즉, 본 논문을 통해 모바일 환경에서의 위험 요소를 안고 있는 무선 네트워크 환경의 문제점들을 시사하고 사회적 문제로부터 모바일 기기 보급으로 인한 모바일 서비스의 활성화에 따라 개인정보 침해 및 유출의 심각성으로부터 보다 안정적으로 모바일 환경의 기기를 사용하고 경각심을 갖기 위해 본 논문에 대한 주제를 연구하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로 개인정보에 관한 내용과 특징을 확인하고, 3장에서는 모바일 환경에서 보안을 위협하는 요소에 대해서 알아보고, 4장에서는 모바일 개인정보를 좀 더 안정적인 환경에서 사용할 수 있는 개선 연구 방향을 제시, 5장에서 결론으로 마무리하고자 한다.

Ⅱ. 관련연구

2.1 개인정보

개인정보법에 따르면 개인정보란 생존하는 개인에 관한 식별정보로서 당해 정보에 포함되어 있는 성명, 주민등록번호, 이메일, 전화번호 등에 의하여 개인을 식별할 수 있는 정보를 말하며 당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 결합하여 식별할 수 있는 정보도 개인정보로 포함할 수 있다[2].

2.2 모바일 기기

모바일 기기라 함은 네트워크에 접속하여 무선 인터넷 서비스를 제공 받을 때에 사용하는 휴대용 기기로 스마트폰, 태블릿, PDA와 같은 기기를 말하며 모바일 기기를 이용하기 위해서는 사용자가 특정한 목적을 달성하기 위해 모바일 어플을 설치하여 해당 서비스를 이용할 수 있어야 한다[3].

2.3 모바일 환경의 개인정보

이동성 기기를 선호하는 대부분의 사람들은 이동성이라는 편리함과 저장성이라는 보관된 정보를 가지고 컴퓨터 환경과 거의 흡사하게 언제 어디서나 네트워크가 지원되는 환경에서는 이동하면서 마음대로 자신이 원하는 위치에서 사용할 수 있다는 편리한 장점이 있어서 선호하게 된다. 그 대표적인 생활적인 편의가 바로 메일 확인, 소셜네트워크서비스 이용, 모바일 뱅킹이며 그 뒤를 이어 메신저, 웹페이지 검색 등에 대한 이용이다. 태블릿이나 스마트폰과 같은 이동기기를 가지고 금융서비스나 메일들을 이용하기 위해서는 사용자의 고객정보가 담긴 공인인증서나 아이디, 비밀번호와 같은 사용자 인증 과정을 거쳐야 거래가 이루어지게 되는데, 이 때 거래를 위해 저장된 개인의 모든 정보를 모바일 기기 개인정보로 포함할 수 있다.

2.4 스마트폰의 특징

2.4.1 아이폰 특징

애플은 북미에서 많이 사용하는 스마트폰으로 국내에서도 아이폰 기기를 선호하는 마니아가 점차적으로 늘고 있다. 최신 출시된 아이폰 특징으로는 자주 대화하는 사람을 더 빨리 불러낼 수 있는 유용한 기능, 뿐만 아니라 시간을 절약할 수 있는 메일 관리 기능, 클라우드와 연결된 모바일 오피스 환경 제공 등을 통해 어디서나 모든 파일 작업이 가능해졌으며,

엄격한 클라우드의 보안 서비스를 제공하고 있다.

데이터 보호 : 아이폰에서 제공하는 클라우드는 iCloud라는 이름으로 서비스되고 있는데 인터넷을 통해 데이터를 전송할 때 이를 암호화하고, 서버에 보관할 때는 암호화된 형식으로 저장하며, 보안 토큰을 사용하여 인증하는 방식으로 데이터의 보안이 유지된다. 다시 말해 데이터를 장비로 전송하는 동안과 클라우드에 저장할 때 인가된 사용자만이 저장된 데이터에 접근하도록 되어있기 때문에 무단 접근으로부터 보호받을 수 있다. iCloud는 주요 금융 기관에서 채택하는 보안 수준과 동일한 최소 128비트 AES 암호화로 암호화 키를 제3자에게 절대로 제공하지 않는다[4].

최근 출시된 아이폰은 장치내의 데이터를 보호하기 위하 AES를 활용하며, 아이폰 분실이나 도난을 고려해서 원격으로 데이터를 삭제하도록 지원, 도난당한 아이폰을 주워서 사용하기 위해 패스코드를 입력해야 하는데 암호를 지정된 횟수보다 잘못 입력하게 되면 장비가 일시적으로 비활성화 되거나 입력에 실패할 경우 로컬 내용을 삭제하는 로컬삭제 기능도 함께 제공하고 있다.

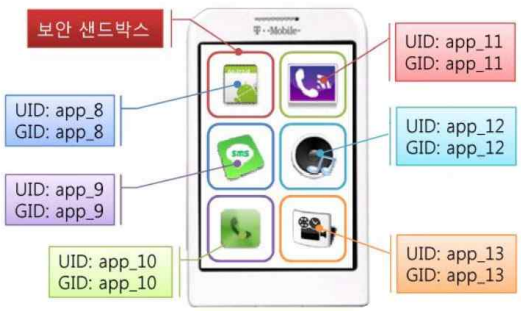
보안 플랫폼 : 개발자를 위한 어플리케이션 데이터 저장을 암호화하는데 활용할 수 있는 공통 크립토 구조를 제공, 런타임 보호, 의무적인 코드서명, AES, RC4 또는 3DES, SHA-1 등을 지원하는 공통 암호구조 등을 제공하고 있다[4].

2.4.2 안드로이드 특징

안드로이드는 구글(Google)의 모바일 기기 소프트웨어를 위한 개방형 플랫폼으로 리눅스커널을 채택함으로써 하드웨어나 주변기기에 대응이 쉽다. 안드로이드는 리눅스 기반의 OS 로서, 안드로이드사가 OS를 개발하였으며, OHA(Open Handset Alliance)에서 제작하고 지원하는 오픈소스 소프트웨어 스택으로서, 휴대폰뿐만 아니라 요구사항을 만족하기만 한다면 어떠한 기기에서도 동작이 가능하고 기기 작동이 쉽다는 것이 특징이다.

안드로이드 스마트폰에서 발생 할 수 있는 위협들에 대한 대응방안으로 다음과 같은 보안특징을 제공한다.

보안 샌드박스 : 안드로이드 보안 구조 설계의 핵심 기술은 <그림 1>의 개념도의 샌드박스(Secure Secure Sandbox)이며, 이는 외부로부터 들어온 프로그램이 보호된 영역에서 동작해 시스템이 부정하게 조작되는 것을 막는 보안 형태이다. 또한 콘텐츠 프로바이더는 기본적으로 사용자들이 대부분 이용하고 있는 연락처, 문자, 음악, 동영상, 스케줄 등과 같은 정보를 저장하여 등록하게 되므로 중요한 정보에 대해서는 각 어플마다 사용자가 보안 접근을 설정할 수 있다.



<그림 1> 안드로이드 보안 샌드박스 개념도

이는 다른 어플리케이션, OS 또는 사용자에게 영향을 줄 수 있는 동작에 대한 권한을 갖으며, 이는 Contacts, e-mail, Home Screen 등 각 어플리케이션의

Private Data를 읽고 쓰거나, 네트워크에 접근하거나, 폰을 깨어있는 상태로 유지하거나 또는 다른 어플리케이션 파일을 읽고 쓰는 것들을 포함하고 있다[4].

퍼미션 : 안드로이드 운영체제인 리눅스가 접근권한을 부여하는 방식으로 안드로이드 어플리케이션은 이러한 권한을 획득해야 사용자의 디바이스에 설치되어 제 기능을 발휘할 수 있다. 예를 들어 인터넷 권한의 획득 없이, 인터넷을 사용할 수 없고, 연락처를 읽는 권한 없이, 사용자 디바이스의 연락처를 읽어올 수 없다. 또한 전화걸기도 권한 없이 전화를 걸 수 없고, SMS 권한 없이 SMS를 다룰 수 없으므로 퍼미션은 사용자에게 있어서 안정된 권한의 보안성을 제공하고 있다. 안드로이드 OS에서 어플리케이션이 권한을 획득해야 사용자의 디바이스에 설치된 기능을 수행 할 수 있는데, 퍼미션을 주지 않았을 경우 프로그램이 강제 종료되게 된다.

Ⅲ. 모바일 환경의 보안 취약성

모바일 기기를 사용하는 환경에 있어서 개인정보를 노리는 많은 취약적인 요소를 확인하고 개인정보와 연관 있는 기기의 취약적인 요소에 대해서 알아보도록 한다.

3.1 태블릿 개인정보 취약성

최근 많은 사용자들이 휴대하기 쉬운 슬림 형태의 태블릿으로 웹 검색, 이메일, 소셜네트워킹, e북, 뉴스, 잡지, 게임, 음악, 비디오와 같은 다양한 콘텐츠 서비스를 태블릿으로 이용한다. 필요에 따라 Wi-Fi를 통한 메신저, 인터넷뱅킹을 활용하는 경우도 늘어나고 있는 추세이다. 태블릿은 얇고 휴대하기가 편해서 원하는 장소에서 이용이 편리할 수 있지만 반대로 휴대하기 편리하기 때문에 그 만큼 잃어버리거나 분실하기가 쉽다.

여기서 문제가 되는 것은 분실 시 나쁜 사람들의 손에 정보가 넘어가게 되면 저장된 정보의 탈취는 시간문제이며 저장된 개인의 프라이버시 개인정보를 침해당할 수 있는 게 더욱 큰 문제이다. 특히 태블릿과 같은 모바일 기반의 소셜네트워크서비스 및 위치기반서비스(Location Based Service, LBS)는 프라이버시 및 위치정보 관련 정보를 다루게 되므로 <표 1>과 같이 개인정보 유출에 따른 침해와 함께 보안위협에 대한 영향을 미치게 된다[9].

<표 1> 위치기반 서비스 보안 위협

보안 위협	내용
개인정보 유출	- 사용자에게 전송되어야하는 위치정보를 해킹 - 서버에 저장된 사용자의 위치 유출
사회적 위협	- 악의적인 서비스 제공자가 사용자에게 잘못된 위치정보 전송

3.2 무선 네트워크 보안 위협

모바일 기기에 대한 취약점은 블루투스, Wi-Fi와 같은 공공장소의 접속 경로를 통해서 무선 네트워크 환경과 같은 취약적인 환경과 연관이 있으며 이러한 경로를 통해 바이러스 감염 및 공격대상의 경로를 제공하는 것으로, 위협적인 요소로 Wi-Fi 도청/변조와 Dos 공격 등이 있다[5].

3.3 악성코드 보안 위협

모바일 기기의 보안을 위협할 수 있는 또 다른 요소는 바로 해커에 의해 악의적인 목적으로 제작된 악성코드가 사용자의 모바일 기기에 감염되는 경우이다.

최근에는 스마트폰의 기능을 탑재한 다양한 모바

일 기기 서비스가 다양해지면서, 인터넷 연결 수단, PC 동기화, 인스턴트 메시지 등 악성코드 침입 경로 또한 다양해지고 있다[6].

악성코드 감염은 스마트폰과 같은 모바일 기기에 보내진 광고성 문자메시지 안에 숨어 있다가 사용자가 이를 열어볼 때 자동으로 이동전화기에 설치되거나 또는 특정한 어플을 수행하기 위해 어플을 설치할 때도 숨겨져 있는 경우가 많은데 이러한 원인에 의해 악성코드에 감염되기도 하며 최근에는 탈취한 사용자 메일을 통해 아는 사람인양 속여서 첨부파일에 악성코드를 포함시켜 보내는 경우도 있다.

악성코드에 감염된 이동기기는 SIM카드 표지 등의 정보를 해커가 조종하는 서버로 보낸다. 그러면 해커는 서버를 통해 공격대상 모바일 기기를 조종해 수시로 임의의 다른 이동전화 번호로 악성코드가 내장된 광고 메시지를 무작위로 대량 보내게 한다. 피해자는 매일 자신도 모르는 사이 단말기에 저장된 지인들의 번호로 광고 메시지를 재전송하게 되는 것이다. 이런 광고성 메시지를 수신한 이동전화기들도 다시 악성코드에 감염되면서 모바일 웜이 생성되게 된다. 모바일 웜에 감염된 스마트폰은 새로운 공격자가 되어 또 다른 스마트폰을 공격하는 2차적인 피해로 스마트폰을 통한 서비스 전체를 불능으로 만들 거나[7], 악성코드를 통해 사용자의 스마트폰에 저장된 임의의 데이터를 삭제하거나 설정을 변경하여 사용자에게 피해를 줄 수 있다[10]. 이러한 모바일 웜 확산의 특성은 <표 2>와 같다.

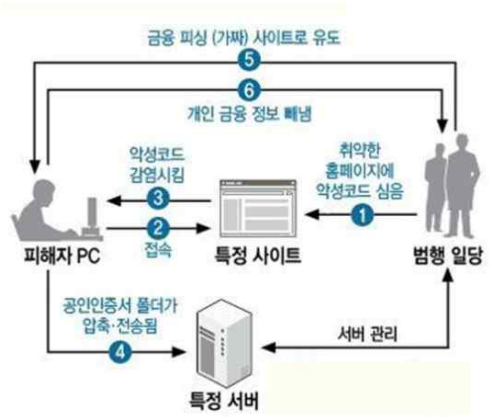
<표 2>모바일 웜 확산의 특징

종류	특성
확산의 다양성	모바일 웜은 인터넷 웜과는 달리 다양한 통신 방식을 이용하여 확산한다. Wi-Fi망 또는 3G/LTE망을 이용하고, 블루투스를 이용하기도 한다.
확산의 제한성	스마트폰은 PC보다 훨씬 더 다양한 운영체제가 사용되고 있고 특정 네트워크 기술을 활용하여 모바일 웜이 확산될 수 있으므로, 3G/LTE망이나 Wi-Fi 접속 유무에 따라 모바일 웜에 바로 감염되지 않을 수도 있다.
확산의 비효율성	인터넷 웜은 고성능 PC에서 동작하므로 최대 네트워크 속도에 근접한 확산이 가능하나, 모바일 웜은 스마트폰 성능 상의 문제로 네트워크 속도보다는 스마트폰의 처리율에 따라 확산율이 결정될 수 있다.

3.4 모바일 공인인증서 위협

이동성 모바일 기기에서 빈번하게 2차적 피해를 입을 수 있는 것이 금융서비스를 사용하기 위해 개인의 소중한 정보를 스마트기기와 같은 메모리장치에 공인인증서를 탑재하면서 개인 인증을 실시하게 되는데 있다.

해커는 이러한 중요한 인증 정보를 탈취하게 위해 [3.3절]에서 설명한 악성코드를 통해 접근을 시도하게 된다. 유일한 본인 인증 안전 수단으로 사용되고 있는 공인인증서가 PC로부터 스마트폰과 같은 모바일 기기로 확대되어 저장되면서 최근 <그림 2>과 같이 해커에 의해 공인인증서를 불법 수집하는 악성코드 등으로 사용자들은 몸살을 앓고 있다.



<그림 2> 공인인증서 불법 수집

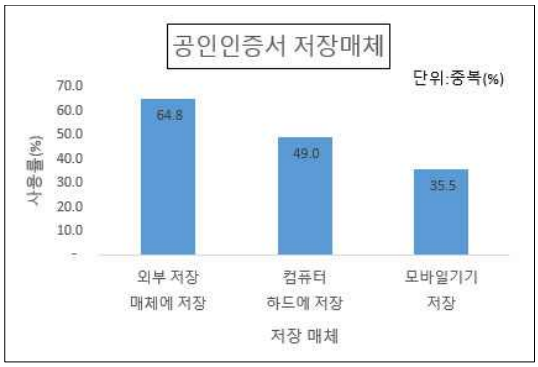
한국인터넷진흥원(KISA)이 2014년 11월 3일부터

17일까지 15일 동안 만 14세부터 59세 중 최근 1개월 이내 인터넷 사용자 및 스마트폰 보유자 1,203명을 대상으로 <표 3>과 같이 '개인정보보호수준 실태조사'를 실시한 결과에 따르면 안전한 저장방식으로 공인인증서를 USB 메모리와 같은 외부 저장매체에 저장하는 비율이 가장 높은 것으로 <그림 3>과 같이 드러났으며, 인터넷 사이트나 금융기관에서 신분 대조용으로 본인인증 수단에도 공인인증서를 이용 가장 많이 이용하는 것으로 확인되었다.

또한 전체 조사 대상 중 92.1%는 공인인증서를 발급받았고 88.6%는 공인인증서를 사용하고 있는 것으로 조사되었다. 특히 20대부터 40대까지는 대부분 공인인증서를 발급받아 사용하고 있는 것으로 나타났다[4].

<표 3> 공인인증서 저장 매체

저장 매체		외부저장 매체에 저장	컴퓨터 하드에 저장	모바일기기 저장
성별	남	66.2	48.3	34.7
	여	63.4	49.7	36.2
연령	10대	49.8	49.4	30.6
	20대	65.3	47.3	42.1
	30대	65.4	51.2	46.5
	40대	72.9	48	28.5
	50대	56.2	49	22.6



<그림 3>공인인증서 저장 매체

그렇기 때문에 공인인증서가 탑재된 개인의 스마트폰을 분실할 경우 돌이킬 수 없는 피해를 입을 수도 있다.

예를 들어 공인인증서를 이용한 모바일뱅킹 서비스나 증권 서비스와 같은 서비스를 이용하여 계좌이체, 증권 거래까지 가능하기 때문이다. 이러한 중요한 정보들이 스마트폰에 고스란히 저장되어 있을 경우 고정된 형태로 물리적인 보호를 받으면서 이용할 수 있는 PC와는 다르게 휴대의 편리성으로 인해 사고로 이어질 경우에는 위험적인 요소가 너무도 크다[8].

Ⅵ. 개인정보 위협 개선 방안

4장에서는 3장에서 살펴본 모바일 기기가 안고 있는 개인정보의 취약적, 위협적인 사용 형태로부터 벗어나서 좀 더 보호적인 측면에서 위협적인 요소에 대한 개선 방향을 제시하고자 한다. 본 논문에서 제시하는 방향 점과 개시된 내용들을 주지시킴으로써 모바일 기기 사용자들은 기본적이지만 훨씬 더 안정적인 모바일 기기환경을 만나볼 수 있을 것으로 기대한다.

4.1 태블릿 개인정보 개선 방향 설정

우선적으로 태블릿을 안정하게 사용하기 위해서는 비밀번호를 설정해야 하는 것인데 비밀번호 설정은 해커가 추측하기 쉽고 알아내기 쉬운 숫자나 패턴 이미지 비밀설정 보다는 지문인식으로 설정하는 것이 좋다. 최근에 출시된 스마트 기기는 대부분 지문인식을 지원하고 있기 때문이다.

만약 구형 스마트 기기를 가지고 있는 사용자의 경우는 추측이 어려운 형태의 특수문자를 포함한 비밀번호로 자주 변경해서 사용하는 것을 적극 권장한다.

태블릿의 비밀번호 설정이 완료한 후에는 태블릿을 안전하게 사용하기 위해 몇 가지 간과해서는 안 될 내용들을 반드시 숙지하도록 하는 것이 좋다.

① 자동적으로 최신의 어플과 기능이 업그레이드되도록 설정하는 것이 중요하다.
② 태블릿에 돈을 지불하고 유료화된 어플을 설치하기 싫어서 탈옥을 하는 경우가 많은데 절대로 탈옥하여 공짜 어플을 깔지 않도록 한다. 공짜 어플을 설치하기 위해서 태블릿에 많은 보안 기능들이 우회되고 무력화되기 때문에 해킹 공격으로부터 취약하게 만드는 원인을 제공하기 때문이다.
③ 어플 다운로드는 구글 플레이스토어나 아이튠즈의 애플스토어와 같은 신뢰 있는 사이트로부터 어플을 다운로드하여 설치하도록 한다. 보통 이러한 사이트들에서는 어플들이 공개되기 전에 검증을 한 후, 업로드하기 때문에 악성코드로부터 신뢰성을 얻을 수 있기 때문에 좋다.
④ 공짜 어플이라고 해서 무작정 다운로드 하는 것은 그다지 좋은 습관과 방법이 아니므로 어플이 필요 없거나 불필요하다고 생각되는 것은 삭제하여 깨끗한 태블릿 환경이 되도록 한다.
⑤ 새로운 어플을 설치 시에는, 새로운 태블릿을 구성할 때 한 것처럼 개인정보 접근 옵션을 설정하도록 한다.
즉, 새로운 어플이 어떤 정보에 접근할 수 있도록 할 지, 어플이 그 정보로 인해 어떠한 연관성을 가지고 접근하는지에 관심을 가지고 개인정보 접근성에 대해서 관심을 가지고 선택을 하도록 한다.
⑥ 태블릿이 분실될 경우를 대비해서 원격으로 추적, 잠금 또는 삭제할 수 있는 어플을 설치하거나 태블릿 하드웨어 분실기기 찾는 옵션을 설정하는 것이 중요하다.
⑦ 실시간으로 사용자의 위치추적을 알아내는 기능을 모두 비활성화로 설정하도록 한다. 태블릿을 이용하여 실시간 위치 정보를 사용하는 경우가 아니라면 위치추적 기능을 비활성화하고 필요에 따라서 네비게이션과 같은 필요 기능을 이용할 때만 활성화하여 사용하는 것이 바람직하다.

4.2 무선 네트워크 개선 방향

많은 사람들이 태블릿이나 스마트폰과 같은 모바일 기기를 통해 무선 네트워크 서비스를 활용하고 있다. 공격자는 무선 네트워크 환경과 같은 보안의 취약성이 약한 Wi-Fi 영역을 노려서 타인의 무단 접속으로 인해 개인정보를 탈취하고자하는 악성코드 유포 가능성을 높이고자 한다. 이러한 위협에 대해서는 사용자들이 해킹의 위험적인 요소에 대해서는 걱정들은 하지만 실제상으로는 무선 네트워크에서의 보안기능 강화와 무선 네트워크 환경에서의 위험 상황과 보안 상식이 그다지 높지가 않다.

무선 네트워크 환경에서 안전한 기기 사용을 위해 우선적으로 평상시 사용하지 않는 모바일 기기에 대해서는 블루투스 기능을 Off하여 사용 설정을 하지 않는 것이 좋으며, Wi-Fi 역시 사용하지 않을 경우에는 에어플레인 모드로 설정하여 공공장소에서 자동적으로 무선 랜이 인식되지 않도록 설정해 두는 것이 좋다.

또한 무엇보다 공공장소에서의 개인정보를 요구하는 금융서비스, 인증서비스를 요구하는 사이트에 접근을 자제하여 사용하지 않도록 한다.

4.3 스마트폰의 개인정보 개선 방향

대부분의 스마트폰에는 개인정보를 비롯 업무와 관련된 중요한 정보가 저장되어 있는 경우가 많다.

혹시라도 스마트폰 도난 또는 분실 시에는 정보유출과 관련 프라이버시 침해 또는 기업에 손실을 불러일으킬 수 있다.

또한 스마트폰의 운영체제가 가지는 버그, PIN 보안 등의 취약성으로 인해 시스템이 일시 중단되거나, 취약한 PIN을 통한 보안 유지로 인해서 정보유출이 발생할 수 있다. 이에, 스마트폰 시스템 접근에 대한 사용자 식별, 인증, 접근제어, 객체 식별 기능이 제공되도록 보안 강화를 설정하여야 하며 스마트폰이 분실, 도난 시에도 인가되지 않은 사용자가 정보에 접근하지 못하도록 해야 하며 시스템 사용의 안정화를 위한 가용성 제공을 위한 개발 어플리케이션에 대한 소프트에어 관리 규정이 제공되어야함을 제안한다.

4.4 모바일 공인인증서 개선 방향

금융권을 비롯하여 본인인증의 유일한 수단으로 제공되던 공인인증서의 해킹으로 인해 사용자들은 패닉상태로 접어들면서 더 이상 안전한 본인인증 대체수단을 찾지 못하고 있다.

지금까지 공인인증서는 메모리방식으로 저장되고 있었으므로 해킹에 취약적인 부분이 있었는데, 개선된 공인인증서 방식은 스마트폰에 삽입할 수 있는 USIM 칩을 활용하여 인증수단으로 활용하면 좀 더 안정적인 본인 인증수단 매체로 적용할 수 있다.

PC의 경우에서도 고정 장치에 공인인증서를 저장하지 말라는 주의사항은 금융 사이트를 통해서도 많이 홍보되어 익히 알려져 있으므로 대부분 외장 저장매체인 USB메모리를 이용하여 개인 인터넷 뱅킹에 사용되어 안정성을 찾은 것과 같은 원리로 볼 수 있다.

USIM 칩을 이용한 인증 방식은 각 사용자의 통신사에 맞는 어플을 먼저 다운로드 받은 후, 스마트폰 USIM 칩에 공인인증서를 저장하고 스마트폰을 통해 전자서명 함으로써 공인인증서를 외장 메모리와 같이 안전하게 보관하고 이용할 수 있다. 사용자들은 USIM 칩을 안전하게 잘 관리하고 활용할 수 있는 노력이 필요하다.

4.5 보안 위협 요소 제안

아래 <표 6>는 본 논문에서 제시한 개선되어야할 현행 보안 위협 요소에 대한 부분을 좀 더 안정적인 차원에서 보완하여 정리하여 제시하고 있다.

<표 6> 보안 위협 비교 분석

	현행	개선 방향
비밀번호	주기적인 비밀번호 설정으로만 안정성 강조	- 새로운 기기에서는 반드시 지문인식으로 설정 - 구 기기에 대해서는 특수문자를 포함한 12자 이상의 비밀번호 설정
어플 사용	무작위 어플 다운로드 사용으로 인한 개인정보 위협	- 필요한 어플만 다운로드 - 다운로드는 인증된 플레이스토어나 애플스토어를 이용 - 불필요한 어플은 모두 삭제하여 깨끗한 환경 유지
무선 네트워크 서비스	커피숍, 공공 장소에서의 Wi-Fi 환경에서의 안전대책없는 모바일 서비스 이용	- 공공 Wi-Fi 영역에서 사용하지 않는 블루투스 기능 끄기 - 자동으로 Wi-Fi가 자동으로 잡히지 않도록 에어플레인 모드 설정 -공공 Wi-Fi 영역에서는 금융서비스 사용하지 않기
사용자 인증	기본적인 개인 식별 기능으로만 사용	- 사용자 식별, 인증, 접근제어, 객체 식별에 대한 강력한 보안 기능 설정
공인인증서	메모리방식	- 스마트폰 USIM 칩을 보안 토큰으로 권장 사용

Ⅴ. 결론

본 논문에서 모바일 환경에서 흔히들 발생할 수 있는 개인정보 유출에 대한 심각성을 인식하고 사회적 현상으로 도출되어진 사고에 대비하기 위해 본 논문을 통해 간과하기 쉽고 놓칠 수 있는 모바일 기기 환

경을 개선하기 위해 위협적인 사례 중심에 대한 개선 방향을 제시하였다.

본 논문을 통해 살펴본 바와 같이 소홀해질 수 있는 위기 상황에 따라 언제든지 사용자도 모르는 사이 개인정보가 유출될 수 있는 위험상황에 대처하기 위해 예방차원에서 고무된 내용을 주지하여 개선된 방향으로 모바일 기기를 관리하고 사용할 수 있도록 개선 방향을 비교 분석하여 제시하였다. 앞으로 모바일 기기 사용자가 더 증가될 추세로 보아 기술적인 면에서 사용자들을 위한 보안 모듈이 더 개발되어야하고 사용자들도 개인정보에 대한 경각심을 가지고 사회적 문제점으로 피해자들이 더 이상 나오지 않도록 정부 및 공공 단체 개인정보처리 담당자들이 개인정보의 중요성에 대한 홍보와 관리적 대책 마련이 꾸준히 필요할 것으로 본다.

참고문헌

[1] 서우석, 전문석, “개인정보 보호를 위한 조직구성과 관리체계에 관한 표준화 모델링,” 디지털산업정보학회 논문지, 제8권, 제3호, 2012년, p. 33.

[2] 조성규, 전문석, “개인정보보호를 위한 개인정보 유출 모니터링 시스템의 설계,” 정보보호학회논문지, 제22호, 제1권, 2012, p. 100.

[3] http://www.law.go.kr/, “모바일 애플리케이션 접근성 지침”.

[4] http://www.boannews.com/media/view.asp?idx=45468

[5] 김기연, 조성재, “스마트폰 보안 취약점 동향,” 정보통신산업진흥원, 가을 학술발표논문집, 제37권, 3호, 2010, p. 93.

[6] 장기헌, 최상명, 염흥열, “스마트폰 DDoS 공격 동향,” 정보과학회지, 제21권, 제5호, 2011, pp. 68-69.

[7] 신원, “스마트폰 환경에서 무선 모바일 웜 확산 방식 연구,” 한국정보통신학회논문지, 제17권, 제5호, 2013, p. 1156.

[8] 최은혁, “악성코드 동향으로 살펴본 스마트 기기의 보안 위협,” 정보보호학회지, 제21권, 제3호, 2011, p. 8.

[9] 최진영, 이신재, 이송희, 이혜리, 이병희, 민승욱, 이형찬, “신규 모바일 기기 정보보호 연구,” 방송통신위원회, 2011, p. 39.

[10] 김지연, 전응렬, 이영숙, 김미주, 정현철, 원동호, “안전한 스마트폰 애플리케이션 개발을 위한 보안 고려사항 및 국산암호알고리즘 적용 방안 연구,” 디지털산업정보학회 논문지, 제7권, 제1호, 2011, p. 54.

■ 저자소개 ■

최 희 식
Choi Heesik

2012년 9월~현재 강원대학교 시스템경영학과 외래교수
2002년 2월 숭실대학교 컴퓨터학과(공학박사)
2006년 2월 숭실대학교 컴퓨터공학과 (공학석사)

관심분야 : 정보보안, 클라우딩컴퓨터, 유비쿼터스, DRM
E-mail : dali3054@ssu.ac.kr

조 양 현
Cho Yanghyun

1997년 9월~현재 삼육대학교 컴퓨터학부 교수
2011년 2월 광운대학교 전자통신학과 (공학박사)
1985년 2월 광운대학교 전자통신학과 (공학석사)
1982년 2월 광운대학교 전자통신학과(공학사)

관심분야 : 컴퓨터네트워크, 통신망(BcN), GMPLS
E-mail : yhcho@syu.ac.kr

논문접수일: 2015년 8월 17일
수 정 일: 2015년 8월 28일
게재확정일: 2015년 8월 31일