한국항행학회 논문지 제14권 제6호 2010년 12월

안전한 스마트폰 보안을 제공하기 위한 정보보호제품 인증 제도에 관한 연구

A Study on Information Security Production Certification System for Secure Smart Phone Security

박종혁*

Jong-Hyuk Park*

요 약

IT 기술이 발전함에 따라 이동 중 서비스를 제공받고자 하는 요구를 충족하기 위하여 스마트폰 보급이 급증하고 있다. 스마트폰을 사용하는 사용자들은 올바른 사용으로 유용한 정보를 획득할 수 있으나, 올바르지 않은 사용을 하는 공격자는 악의적인 목적으로 사용하기 위해 타인의 개인 정보를 노출시키고 유포하여 다양한 피해를 발생시키고 있다. 이를 해결하기 위하여 다양한 서비스들이 개발되고 있으나, 공격들이 지능화됨에 따라 보안을 제공할 수 있는 방안이 필요한 실정이다. 본 논문에서는 안전한 스마트폰을 사용하기 위해서 개발 과정부터 안전한 제품을 보증하기 위한 정보보호제품 평가 및 보안 모듈에 대한 평가 제도들에 대하여 알아보고, 안전한 스마트폰 보안을 제공할 수 있는 방안에 대하여 제안한다.

Abstract

According to IT technology has evolved, smart phone rapidly propagates for mobility. A smart phone user acquires useful information, but attackers generate various damage. For example, an attacker must distribute to expose the privacy of others. To solve this problem, various information security products are being developed. In addition, information security has been strengthened. In this paper, we propose a scheme for secure use of smart phone. For development of secure smart phone, the development processes should be secure. In addition, we propose an information security production certification system for secure smart phone security.

Key words : smart phone, certification, certification system

I. 서 론

IT 기술이 발전함에 따라 이동하면서도 서비스를 제공받을 수 있는 이동성에 대한 요구가 증가하게 되었다. 이러한 요구는 언제, 어디서나 서비스를 제공받을 수 있는 소형 디바이스 형태의 스마트폰으로 충족되고 있다. 스마트폰은 통화 및 간단한 기능만을 제공하는 일반 휴대폰에 비하여 훨씬 더 광범위한 서비스를 제공할 수 있으며, 인터넷, 이메일, 게임 등 다양한 분야에서 활용되고 있다. 하지만 PC보다 경량화된 사양의 소형 디바이스에서 다양한 서비스를 제공받는 것을 중점으로 사용되기 때문에 상대적으

* 서울과학기술대학교 컴퓨터공학과(Dept. of Computer Science and Engineering, SeoulTech)
· 제1저자 (First Author) : 박종혁
· 투고일자 : 2010년 11월 29일
· 심사(수정)일자 : 2010년 11월 29일 (수정일자 : 2010년 12월 20일)
· 게재일자 : 2010년 12월 30일

로 보안이 미흡하게 제공되고 있다. 점차 공격자들의 공격 능력이 증대되고 있어 스마트폰의 보안은 반드시 필요한 요구 사항으로 자리 잡고 있다.

이러한 스마트폰과 같이 보안이 필요하거나 보안 기능을 제공하는 개인 정보보호제품 및 기업 정보보호제품들은 사용량이 증가하고 있으나, 개방된 네트워크를 통하여 악의적인 목적의 사용자의 공격 수준도 향상되어 공격 유형이 다양해지고 피해 규모가 증대되고 있다. 이러한 피해를 줄이기 위하여 정보보호제품이 개발되는 과정부터 안전하게 개발할 수 있도록 안전한 환경이 구축되어야 한다. 안전한 정보보호제품 개발을 위해서 제품 인증뿐만 아니라 제품에 탑재되는 보안 모듈 인증 제도까지 도입되어 안전한 정보보호제품을 개발하고 개발 과정을 보증하기 위한 다양한 제도가 수행되고 있다. 하지만 점차 공격 유형이 진화하고 있기 때문에 정보보호제품의 인증제도의 중요성 및 필요성이 증대되고 있으며, 다양한 기관에서 인증을 제공하고 있기 때문에 인증에 대한 일관성을 제공해야 한다. 따라서 본 논문에서는 정보보호제품 인증 제도를 스마트폰에 적용하여 안전하게 사용할 수 있는 방안에 대하여 기술하고자 한다.

Ⅱ. 관련 연구

보안 기능을 제공하는 제품은 평가 기관에서 평가를 받고 인증기관으로부터 승인을 받아야 안전한 제품으로 인증 받고, 공공기관으로 납품할 수 있다.

보안 기능을 제공하는 제품으로 분류되는 것은 아니지만 개인 프라이버시와 직접적으로 관련되어 있는 스마트폰도 품질 보증 및 검증 과정을 거쳐 안전하게 개발되어야 한다.

2-1 평가 인증제도

CC(Common Criteria)란 공통평가기준으로 CCRA(Common Criteria Recognition Arrangement) 가입국들 간에 상호 인정하여 정보보호제품을 평가하는 제도이다[2,3]. 1985년 미국이 처음으로 정보보호제품을 평가하기 위해 TCSEC(Trusted Computer System Evaluation Criteria)이라는 평가 기준을 마련하여 제품에 대한 보증을 제공하였으며, 이후 영국의 그린 북(Green Book) 시리즈, 독일의 블루-화이트 북(Blue-White Book), 프랑스의 블루-화이트-레드북(Blue-White-Red Book) 등이 계속적으로 제정되면서 1990년에 영국, 독일, 프랑스, 네덜란드가 협력하여 유럽의 공통적인 평가 기준서인 ITSEC(Information Technology Security Evaluation Criteria)을 발간하게 되었다[5,7]. 이외에도 다양한 국가에서 평가 기준을 마련하게 되었으나, 수출 및 수입 시 중복되는 평가에 따른 시간 및 비용에 대한 비효율성이 문제로 대두되게 되었다[1,4]. 따라서 이러한 문제점을 해결하기 위하여 각 나라들 간에 공통평가기준을 마련하여 평가 및 인증에 대해 상호 인정하는 제도를 도입하였다[8].

보안적합성 검증은 국가정보통신망의 보안 수준을 제고하고, 외부의 공격에 대응하기 위하여 국가 및 공공 기관이 도입하는 정보보호제품의 보안기능에 대한 안전성을 검증하는 제도이다. 국가정보원 IT 인증 사무국은 2001년 9월부터 보안적합성 검증 업무를 수행하고 있으며, 국가보안기술연구소는 보안적합성 시험을 수행하고 있다.

2-2 암호 검증

암호 검증은 CC 인증 및 보안적합성 제도와는 다르게 암호 모듈에 대한 안전성을 검증하는 제도이다. 암호 검증은 국가정보보안기본지침과 암호모듈 시험 및 검증 지침에 따라 국가 및 공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않은 중요정보의 보호를 위하여 사용되는 암호모듈의 안전성과 구현 적합성을 검증하는 제도이다. 검증 대상이 되는 암호 모듈은 소프트웨어 또는 하드웨어 형식으로 구현될 수 있다.

암호 모듈 개발 업체는 검증 대상 암호 모듈에 대한 시험 계약을 시험 기관과 체결하고 암호 검증 기준(KS X ISO/IEC 19790:2007)에 따라 암호 모듈에 대한 시험을 진행함으로써 정보보호제품에 탑재되는 암호 모듈에 대한 보증을 제공하고 있다.

2-3 스마트폰 동향

스마트폰이란 휴대전화에 인터넷 통신과 정보검색 등 컴퓨터 지원 기능을 추가한 지능형 디바이스로 사용자가 원하는 애플리케이션을 설치할 수 있으며, 이동 중 인터넷 통신, 팩스 전송 등이 가능하다. 스마트폰은 탑재된 OS(Operating System)와 네트워크 접속 기능 등 사용성 측면에서 다각화되고 있으며, 애플리케이션과 콘텐츠를 사용자 요구에 따라 무궁무진한 확장이 가능하다. MS사에서 개발한 윈도우 모바일이 가장 많은 점유율을 차지하고 있었으나, 현재 가장 많이 사용되는 운영체제는 노키아에서 개발한 심비안이며, 아이폰 OS가 급부상하고 있는 실정이다. 윈도우 모바일은 가장 많이 사용되고 왔기 때문에 OS에 대한 문제점 제기가 가장 많은 OS로 꼽히고 있다.

Ⅲ. 스마트폰 보안위협

스마트폰은 경량화된 소형 단말기 하나로 여러 가지 업무를 할 수 있고 서비스를 제공받을 수 있으나, 보안을 체계적으로 대응할 수 있는 경험과 조직 체계 및 역할과 책임이 없어 알려지지 않은 해킹 발생 시 모든 관련 주체가 피해자가 될 수 있다는 문제점이 있다[10,11]. 특히 IT 기술의 진보로 인해 해킹 기술이 발전하고 있으며 공격이 점차 고도화되고 있어 보안이 반드시 필요한 요소가 되고 있다. 따라서 본 장에서는 스마트폰에서 발생할 수 있는 보안 위협에 대하여 기술하고자 한다[6].

3-1 사생활 및 개인정보 유출

스마트폰 사용자들은 스마트폰을 통해 일정관리, 메모, 인터넷 뱅킹, 이메일등의 기능을 사용하고 있으며 최근 유행하고 있는 소셜 네트워크 서비스(SNS-Social Network Service)를 사용하고 있다. 스마트폰은 자신 혼자만 사용하며 입력이 조금 번거롭다는 이유로 보안상 중요한 로그인 정보를 자동으로 처리하게 저장해 두는 경우가 많다. 또한 소셜 네트워크 서비스를 통해 자신의 일상을 기록하는 사용자들 또한 기하 급수적으로 늘어나고 있다. 하지만 이런 편리함 이면에는 사생활과 개인정보 유출이라는 부작용도 존재한다.

3-2 검증되지 않은 애플리케이션

스마트폰은 누구나 개발툴킷을 이용하여 애플리케이션을 개발하고 또 마켓을 통해 판매가 가능하다. 이를 악용한 공격자는 공격 툴이 삽입되어 있는 애플리케이션을 판매하여 무작위 사용자를 대상으로 공격을 수행할 수 있다. 사용자 몰래 스마트폰에 깔린 악성코드는 스마트폰 사용자의 개인 정보를 쉽게 획득할 수 있으며, 이를 통해 부당한 과금이 이루어지게 할 수 있다.

3-3 검증되지 않은 무선 네트워크 환경

스마트폰은 3G, Wi-Fi, Bluetooth 등 다양한 네트워크 환경을 지원한다. 이 중 Wi-Fi는 3G와는 달리 일반적으로 과금이 되지 않으므로 다른 통신 방법보다 선호하는 통신 방식이다. 그러나 비밀번호를 사용하지 않은 Wi-Fi AP(Access Point)를 개설해 놓으면 수많은 사람들이 접속하여 다른 사람의 정보를 볼 수 있다는 문제점이 있다.

3-4 보안 취약점 공격

최근 애플(Apple)사의 아이폰(iPhone)에서 내장된 사파리 웹브라우저를 사용하여 어도비(Adobe)사의 문서파일(PDF)를 처리할 때 관리자 권한을 획득할 수 있는 보안 취약점이 발견되었으며 실제 이 취약점을 활용하여 아이폰 탈옥(JailBreak)툴이 개발되고 공개 되었다.

안드로이드(Android)폰의 경우도 특정 버전에서 웹브라우저를 통해 관리자 권한을 획득하는 보안 취약점이 발견 되었다. 이런 취약점을 이용하면 단순히 웹브라우저를 통해 사이트에 접속하는 것만으로도 악성코드에 감염될 수 있다.

스마트폰은 그 특성상 감염 시 전화번호, 통화목록, 문자 메시지, 메모, 일정과 같은 개인 정보는 물론 유료 전화나 스팸 문자 메시지 발송 등 실제 금전적 피해가 발생할 가능성이 있다. 이와 같은 문제점

들은 점차 양이 증가하고 IT 기술 발전에 따라 공격 기술도 고도화되고 있다.

Ⅳ. 스마트폰 보안 제공 방안

정보보호제품은 앞에서 조사한 것과 같이 다양한 인증 제도를 통해 안전성을 검증받고 있다. 하지만 스마트폰은 보안에 대한 검증 제도가 마련되어 있지 않기 때문에 다양한 취약점이 발생할 수 있다. 따라서 검증 제도는 스마트폰 개발 및 애플리케이션 개발 단계부터 적용되어야 하며, 백신과 같이 기본 보안은 반드시 설치하여야 한다. 앱을 개발한 후에도 검증되지 않은 앱은 스마트폰에 설치될 수 없도록 해야 하며, 검증된 앱만 과금되고 사용될 수 있도록 시스템을 구축하여야 한다. 하지만 아직 해결해야 될 문제점들이 존재하기 때문에 이러한 문제점들을 보완해야 한다.

4-1 인증제도 도입

보안 기능을 제공하는 제품들이 CC 인증이나 보안 적합성 제도 등을 통해서 인증을 받는 것과 동일하게 스마트폰을 개발하는 과정에서 스마트폰을 검증할 수 있는 제도들을 도입하여 시행해야 한다. 개발 단계부터 제품 검증 제도를 도입했을 경우 초기에 문제점을 해결할 수 있어 비용 및 시간이 절약될 수 있으며, 심각한 취약점을 수정할 기간이 길어짐에 따라 더욱 안정화 된 제품을 개발할 수 있다.

검증하는 과정에서는 취약성에 대한 검토가 반드시 이루어 져야 할 것이며, 정보보호 취약성은 CVE(Common Vulnerabilities and Exposures)에 정의된 취약성을 기반으로 시험을 수행해야 하며, 취약성이 발견되었을 경우 이를 보완하여 스마트폰을 개발해야 한다.

이러한 시험을 수행하기 위해서는 소프트웨어, 펌웨어 시험 도구뿐만 아니라 하드웨어를 시험할 수 있는 도구들을 국내 평가기관에서 보유하고 있어야 한다. 하지만 현재 국내에서는 하드웨어에 대한 개발이 미비하고 활성화되어 있지 않아 시험 도구가 부족한 실정이다. 이러한 문제를 극복하기 위해서는 충분한 교육을 통하여 국내 평가 스킬을 향상시키고 시험 도구들을 보유할 수 있는 환경이 구축되어야 할 것이다.

또한 스마트폰 개발뿐만 아니라 스마트폰에 설치되는 애플리케이션의 경우 검증되지 않은 애플리케이션을 통해서 부당한 과금이 발생하거나 개인 정보가 유출될 수 있기 때문에 마켓에서 검증할 수 있는 절차가 필요하며, 검증된 애플리케이션만을 사용자가 설치하고 사용할 수 있도록 해야 한다. 또한 PC와 유사한 환경이기 때문에 백신은 반드시 설치하여 안전한 환경을 구축하여야 한다.

4-2 스마트폰 보안 수칙 준수

스마트폰 보안 위협 요소들이 발생하며, 스마트폰 보편화의 걸림돌이 되고 있다. 특히 스마트폰을 분실했을 경우 발생하는 개인 정보 노출, 프라이버시 침해 문제는 심각한 수준이다. 또한 최근 스마트폰에서 폰뱅킹과 인터넷 뱅킹 해킹 문제가 실질적으로 발생하여 앞으로 스마트폰에 대한 보안 위협이 점차 다양해질 것으로 예상되고 있다. 따라서 이러한 문제들을 개선하고 스마트폰 보안 문제가 발생하지 않도록 예방하기 위해서는 다음과 같이 스마트폰 보안 수칙을 준수해야 한다[9].

표 1. 스마트폰 보안 수칙
Table 1. Security rule of smart phone

번호	스마트폰 보안 수칙
1	애플리케이션을 설치하거나 이상한 파일을 다운로드 한 경우에는 반드시 악성코드 검사를 한다.
2	게임 등 애플리케이션을 다운로드할 때는 신중하게 다른 사람이 올린 평판 정보를 먼저 확인한다.
3	브라우저나 애플리케이션으로 인터넷에 연결 시 이메일이나 문자 메시지에 있는 URL은 신중하게 클릭한다.
4	PC로부터 파일을 전송 받을 경우 악성코드 여부를 꼭 확인한다.
5	백신의 패치 여부를 확인해서 최신 백신 엔진을 유지한다.
6	스마트폰의 잠금 기능[암호 설정]을 이용해서 다른 사용자의 접근을 막는다. 잠금 기능에 사용한 비밀번호를 수시로 변경한다.
7	블루투스 기능을 켜놓으면 자동 감염되므로 필요할 때만 켜놓는다.
8	ID, 패스워드 등을 스마트폰에 저장하지 않는다.
9	백업을 주기적으로 받아서 분실 시 정보의 공백이 생기지 않도록 한다.
10	임의로 개조하거나 복사방지 등을 풀어서 사용하지 않는다.

Ⅴ. 결 론

최근 시간과 공간에 구애받지 않고 서비스를 제공받기 위한 요구가 증가됨에 따라 스마트폰 보급율이 급증하고 있다. 스마트폰은 다양한 서비스를 제공받을 수 있고 사용 방법이 간단하여 사용 범위가 확대되고 있으나, 소형 디바이스에서 제공할 수 있는 보안의 범위가 경량화 되어 다양한 위험에 노출되고 있다. 특히 애플리케이션의 경우 검증되지 않은 애플리케이션들이 마켓에서 판매되고 있어 불법 과금이 이루어질 수 있으며, 악의적인 목적의 애플리케이션들로 인해 스마트폰 사용자의 개인 정보 및 사생활이 노출될 수 있다. 이러한 문제점을 해결하고, 안전한 스마트폰을 사용하기 위해서는 인증뿐만 아니라 탑재되는 보안 모듈에 대한 검증도 수행해야 하기 때문에 CC 인증, 보안적합성 검증, 암호 모듈 검증 등 인증 제도를 통해 스마트폰을 보증 받도록 해야 한다. 하지만 평가 기관이 증가하고 보유 툴 및 지식이 동일하지 않으므로, 인증의 일관성이 제공될 수 있도록 해야 할 것이다. 또한 공격자의 수준 및 공격 유형이 다각화되고 있는 요즘, 기존에 발생하고 있는 취약점뿐만 아니라 실시간으로 업데이트 되고 있는 취약점, 경험으로 발견되는 취약점 등 모든 취약점이 스마트폰에 존재하는지 시험해야 한다. 이러한 항목들이 개선된다면 더욱 안전한 스마트폰을 개발하고 검증된 애플리케이션을 개발할 수 있을 것이며, 급변하고 있는 공격 유형에 대응할 수 있는 안전한 환경이 구축될 것이라 사료된다.

참 고 문 헌

[1] Canadian Trusted Computer Product Evaluation criteria(CTCPEC), Version 3.0, Canadian System Security Centre, *Communications Security Establishment, Government of Canada*, Jan.1993

[2] Common Criteria for Information Technology Security Evaluation, Version 3.0, 2005.07 (http://www.commoncriteriaportal.org/public/expert)

[3] Common Criteria for Information Technology Security Evaluation, Version 3.1, 2006.09 (http://www.commoncriteriaportal.org/public/expert)

[4] Federal Criteria for Information Technology Security(FC), Draft Version 1.0, jointly published by the NIST and NSA, US Government, Jan.1993

[5] Information Security Evaluation Criteria(ITSEC), *Version 1.2, Office for Official publications of European Commnunities*, Jun.1991

[6] Soo-Young Kang, Jong Hyuk Park, Muhammad Khurram Khan, Jin Kwak, “Study on the common criteria methodology for secure ubiquitous environment construction”, *Journal of Intelligent Manufacturing*, 2009.11

[7] Trusted Computer System Evaluation Criteria(TCSEC), US DoD5200.28-STD, DEC.1985

[8] 최락만, 송영기, 인소란, “보안 평가 기술 : Common Critetia를 중심으로”, *전자통신동향분석, 제 12권 제 5호*, 1997.10

[9] http://www.ahnlab.com, *안철수연구소 스마트폰 보안수칙 10계명*

[10] KISA, "모바일 악성코드 침해 대응 가이드", 2009

[11] KISA, "인터넷 & 시큐리티 이슈", 2010.03

박 종 혁 (朴鍾爀)

2002년 2월 순천향대학교 컴퓨터공학부 학사
2004년 2월 고려대학교 정보보호대학원 석사
2007년 7월 고려대학교 정보보호대학원 박사
2007년 9월 경남대학교 컴퓨터 학부 전임강사
2009년 9월 서울과학기술대학교 컴퓨터공학과 조교수
관심분야 : 정보보증, 디지털 포렌식, 멀티미디어 보안, 보안 프로토콜, 상황 인식, 스마트 홈, 유비쿼터스 컴퓨팅 및 보안