스마트 디바이스의 취약점 분석과 하드웨어적 해결 방안 연구

문상국

목원대학교 전자공학과

A Study on the Works of Smart Devices Weakness and Hardware Solution

Sangook Moon

Mokwon University, Department of Electronic Engineering

E-mail : smoon@mokwon.ac.kr

요 약

불의 이중성과 양날의 검의 속성을 가지는 스마트 디바이스는 편리성과 함께 구조적으로 내재한 보안의 취약점을 가지고 있으며, 아직까지는 스마트 디바이스에 대한 보안 피해사례가 크게 발생하지는 않았지만 사회적으로 상당한 영향을 끼칠수 있는 문제점을 가지고 있다. 이러한 보안에 대한 취약점은 스마트 디바이스의 운영이 소프트웨어 앱에 의존하고, 그 앱들이 하드웨어 디바이스 (카메라, 파일시스템 등등)를 권한에 구애받지 않고 사용할 수 있기 때문이다. 본 논문에서는 이러한 스마트 디바이스들에 대한 공통적이고 다양한 취약점에 대해 분석하고 그 해결 방안에 대하여 논한다.

ABSTRACT

Smart devices have the characteristics of duality of fire and the property of double-sided swords. They also both conveniency and the weakness at a time due to the structure of the devices. Although there have not been a big threat with the smart devices, but they have potential enough to destroy the network society. This is because of the fact that the devices mainly depend on the applications and the applications can abuse the devices' critical hardware sections such as camera, file system, etc.. In this contribution, we analyze the issues and the problems of the weakness of smart devices and discuss a method to solve the issues.

키워드

스마트 디바이스, 보안, 취약점

Ⅰ. 서 론

휴대 정보기기, 스마트 디바이스의 춘추전국시대이다. 스마트 디바이스의 보급으로 현대인의 생활은 유례없이 편리해졌고, 직장이나 일상 생활의 패러다임이 변화하고 있다. 여기에 클라우드 컴퓨팅의 개념이 도입됨에 따라, 개개인은 이제 웬만해서는 컴퓨터 앞에 앉을 필요조차 없어졌다 [1]. 스마트 디바이스의 도입으로 개인용 게임기의 형태가 바뀌었고, 고전적인 악기의 개념이 바뀌었으며, 스케줄관리나 홈뱅킹, 주식거래를 책상 위의 컴퓨터의 도움 없이 할 수 있게 되었고, 네비게이션이나 소셜 네트워킹도 어디를 이동하든지간에 가능하게 되었다. (그림 1)

이러한 편리성 때문에, 스마트 디바이스의 수요는 급증하고 있다. 스마트폰의 경우 2009년 4분기 5,450만대가 출하되어 전년 동기 대비 39% 성장하였으며, 전체 휴대폰 시장에서의 비중도 2009년 12.7%에서 2010년 6월 현재 15.4%로 증가하였다. 스마트패드의 경우 2010년 첫 출하 이후 1,900만대가 판매되었다 [2].

문제는, 이러한 스마트 디바이스가 급격히 발전하면서, 너무 빨리 '되는' 것들이 많아졌다는 사실이다. 아이디어 기반의 기술을 장려하면서 그에 따른 부작용를 미처 고려 못하고, 너무 편리한 '되는' 기술들이 상용화되었다. 그나마 애플 사는 iOS를 공개하고 있지 않기 때문에 아직 프로그램상의 악성코드들이 활성화하고 있지는 않지만 [3], 안드로이드 OS는 태생이 공개 OS이기 때문에 전세계에 있는 누구나가 개발할 수 있고, 경우

에 따라서는 실력있는 개발자가 나쁜 마음을 먹기만 하면 손쉽게 악성코드를 개발하여 배포할 수 있는 환경에 처해 있다고 할 수 있다 [4].

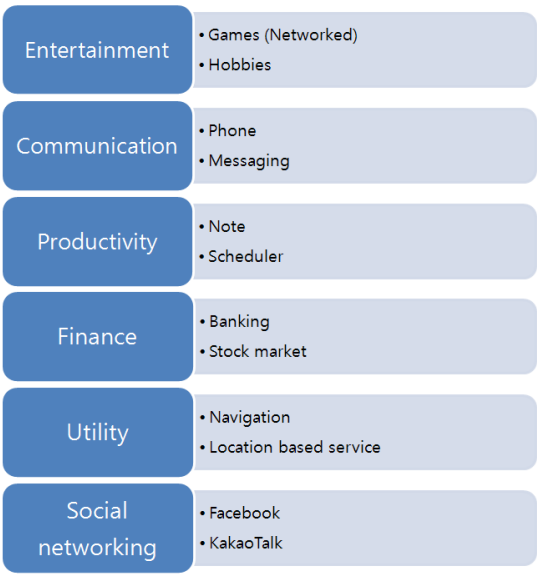

그림 1. 스마트 디바이스로 인한 편리성

II. 다양한 스마트 디바이스 공격 기법

스마트 디바이스는 너무 빠른 속도로 발전하여 왔기 때문에 그 자체의 유용성이 함정이 되는 경우가 많다. 인류의 가장 위대한 발명인 '불'이나 '칼'이 문명 발달에 막대한 영향을 끼쳤지만, 반대로 잘못 사용하면 부작용이 생기는 경우와 마찬가지라고 할 수 있다. 아래 몇 가지 스마트 디바이스에 대한 공격의 형태를 보인다.

1) 바코드를 이용한 인젝션

그림 2에 보이듯이 스마트 디바이스에서 사진을 찍어, 바코드를 해석하여 주소록을 등록할 수 있는 매우 편리한 애플리케이션 (이하 앱)이 이런 경우에 해당한다. 바코드를 인식하여 내부 코드를 실행하기때문에, 악성 피싱 공격에서 피싱 서버로 사용자의 정보를 빼낸다든지 개인정보를 유출 할 수 있는 특성을 가지고 있다. 최근들어 스마트 디바이스의 바코드 인식을 이용한 주문결제 또는 쇠고기의 국산 여부, 인터넷 최저가 확인 등 다양한 서비스를 제공하는 업체가 증가하는 추세이며, 점차 범위를 넓혀나가고 있어서 큰 문제점을 가지고 있다.

그림 2. 바코드 인식을 통한 공격

2) 무선 인터넷 중계기를 사용한 공격

모 통신사 광고를 보면 점원의 설명에 아랑곳 하지 않고 '와이파이 잘 떠요?' 라는 질문만 계속 하는 구매자를 볼 수가 있다. 인터넷 통신료를 절감하기 위한 소비자가 그만큼 많다는 이야기이다. 따라서 스마트 디바이스 이용자들은 장소를 옮길 때 무선 인터넷이 되는 지를 고려하는 사람들도 많다. 스마트 디바이스를 이용하여 인터넷에 접속하기 위해서는 AP (무선 인터넷 중계기)를 통해 접속해야 하는데, 대부분의 AP는 가능하면 모든 자원을 활용해서 네트웍의 트래픽을 많이 중계할 수 있도록 세팅이 되어있기 때문에 보안에 매우 취약하다. 한 예로, 커피숍에서 누군가가 자신의 노트북의 무선랜 기능을 사용하여 AP를 제공할 수 있다. 이 때, AP의 이름을 누구나 알 수 있는 대기업 통신사 (Nes***, IPt***, MyLG***, Qook*** 등등)의 이름을 등록해도 아무런 문제가 없는 것이다. 이를 와이파이 피싱이라고 하는데, 위험을 모르는 사용자에게는 대단한 위협이 되는 것이다.

그림 3. 와이파이 피싱 (phishing)

III. 하드웨어 기반의 보안기술 제안

2003년 인텔은 간단한 하드웨어를 도입하여 자사 칩의 불법 오버클록킹을 방지할 수 있는 특허를 취득하였다. (그림 4) 이는 보다시피 허용 주파수의 최대값과 허용 주파수의 최소값을 롬 테이블에 저장하고, 오버클록킹 되었다고 가정된 클록을 비교기에 넣어 주파수가 그 범위를 초과하면 오버클록킹을 진단하는 간단한 하드웨어로 구

성되어 있다.

이러한 개념을 응용하면, 이론상으로는 간단하게 통신사의 고유식별번호나 프로그램의 integrity value를 사용하여 피싱이나 악성 코드를 원천적으로 차단시킬 수가 있다 [5].

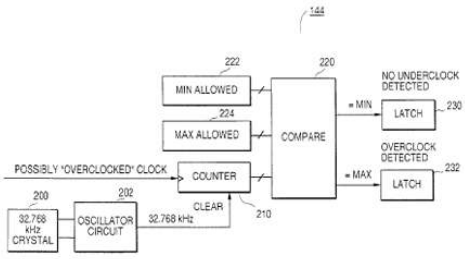

그림 4. 인텔의 오버클록킹 방지 회로

1) 무선 AP 공격 방지 개념

CPU 레지스터 이외의 공간에 신뢰할 수 있는 통신사 혹은 AP의 SSID 고유값을 저장할 수 있는 저장공간을 마련하고 무선랜이나 블루투스가 연결될때마다 신뢰할 수 있는 값과 비교하는 개념이다.

2) 악성 코드 실행 차단 개념

텍스트 메시지나 웹사이트 방문 시에 접할 수 있는 악성 코드 외에, 하드웨어와 연동된 코드를 실행시키면서 공격당하는 방법은 지금까지는 알려진 바가 없으며, 근원적인 대책이 필요하다. 일단 문제점은 프로그램에 너무 많은 권한을 주었다는 점이다. 일단 이점은 기본적으로 OS에서 보완해주어야 하며, OS에서 보완해주지 못한다면, 몇 가지 방법을 생각해 볼 수 있다. 그중 한 가지 아이디어는 이러한 앱들은 자체적으로 수정되지 않는 코드들이다. (self-modifying) 이러한 앱들이 메모리에 로드되어 실행될 때마다, 프로그램의 순정값 (integrity value)을 해쉬하여 실행되는 값과 비교하여 공격 여부를 판단하는 것이다. 이를 위하여 하드웨어적으로는 정보저장공간과 해쉬연산 블록 (SHA-2), 비교기를 설계하여 구현한다.

IV. 결 론

불의 이중성과 양날의 검의 속성을 가지는 스마트 디바이스는 편리성과 함께 구조적으로 내재한 보안의 취약점을 가지고 있으며, 아직까지는 스마트 디바이스에 대한 보안 피해사례가 크게 발생하지는 않았지만 위의 설명에 보이듯이 대단히 깊은 문제점을 가지고 있다. 이러한 보안에 대한 취약점은 스마트 디바이스의 운영이 소프트웨어 앱에 의존하고, 그 앱들이 하드웨어 디바이스(카메라, 파일시스템 등등)를 권한에 구애받지 않고 사용할 수 있기 때문이다.

이러한 보안에 대한 취약점은 쉽게 알려져 있는것들도 있지만, 앱이 기하급수적으로 발전함에 따라, 근원적인 보안에 대한 취약점의 분석과 해결방법이 필요하다. 지난 2003년 전세계적으로 비메모리반도체를 독점하다시피 했던 인텔에서는 사용자의 불법 오버클럭킹을 방지하기 위하여 간단한 하드웨어를 도입하여 오버클럭킹을 방지하는 특허를 제출하여 오버클럭킹을 원천적으로 봉쇄하였던 바가 있다. 본 고에서는 소프트웨어가 주도하는 스마트 디바이스에 눈에 보이지 않는 하드웨어 장치를 추가하여 개개인의 정보를 보호하면서 스마트 디바이스의 편리성이 해가 되지 않도록 하는 기술에 대하여 제안하였다.

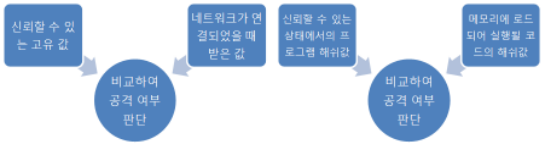

그림 5. 하드웨어 기반의 스마트 디바이스 보안 기술 개념

참고문헌

[1] http://www.google.com
[2] http://open-tube.com/smart-phone-market-share-iphone-and-android-are-battling-symbian-rim-are-down/
[3] http://www.apple.com
[4] http://www.android.com
[5] http://www.intel.com