방송통신정책연구 11-진흥-라-07

신규 모바일 기기 정보보호 연구

(Study on Security for New Mobile Devices)

최진영/이신재/이송희/이혜리/이병희/민승욱/이형찬

2011. 12

연구기관 : 한국정보보호학회

방송통신위원회
KOREA COMMUNICATIONS COMMISSION

이 보고서는 2011년도 방송통신위원회 방송통신발전기금 방송통신정책연구사업의 연구결과로서 보고서의 내용은 연구자의 견해이며, 방송통신위원회의 공식입장과 다를 수 있습니다.

제 출 문

방송통신위원회 위원장 귀하

본 보고서를 『**신규 모바일 기기 정보보호 연구**』의 연구결과보고서로 제출합니다.

2011년 12월

연구기관 : 한국정보보호학회

총괄책임자 : 최 진 영

참여연구원 : 이 신 재

이 송 희

이 혜 리

이 병 희

민 승 욱

이 형 찬

목 차

표 목 차

그 림 목 차

요 약 문

1. 제 목

신규 모바일 기기 정보보호 연구

2. 연구 목적 및 필요성

스마트폰 보급 확산과 더불어 생활 서비스 환경이 모바일 기반으로 변화되어 가고 있다. 이에 따라 이동성, 개방성, 다양성 등이 제공되는 안전한 모바일 서비스에 대한 요구가 지속적으로 발생하고 있으며 향후에 더욱더 증가될 것으로 전망된다. 그러나 스마트폰, 스마트패드 등 신규 모바일 기기의 급속한 확산과 더불어 기존의 보안 위협뿐만 아니라 새로운 보안위협이 예상된다. 따라서 신규 모바일 단말들의 위협 현황과 전망을 통해 정보보호 이슈를 도출하고 선제적인 정책적 대응 방안 마련에 활용할 필요가 있다. 또한 안전한 모바일 기기 이용 환경 구축으로 개인, 기업, 정부 등 사회전반의 효율적인 활용 추진 방향 제시함으로 IT 강국으로서의 선도적인 경쟁력 강화할 필요가 있다.

본 연구의 목표 및 주요 내용은 다음과 같다.

- ❍ 신규 모바일 단말 확산 현황 및 전망
- ❍ 국내외 모바일 단말 활용, 위협 동향 및 정책 현황
  - 각 국의 모바일 단말 활용 현황, 위협 동향 조사 및 정보보호 대응책·정책 수립 현황 분석
- ❍ 신규 모바일 단말의 확산으로 인한 주요 보안 이슈
  - 기존 유선기기 위협의 확대 및 스마트폰, 스마트패드(태블릿PC) 등 단말의 신규 보안위협 현황 및 사례
- ❍ 안전한 모바일 단말 이용 환경 구축을 위한 보안 대책

- 스마트화 되어가는 다양한 단말기기, 네트워크, 서비스, 콘텐츠 등에 대한 보안 대책 마련
- 신규 단말 보안 강화 및 안전한 앱 유통환경 개선책 수립
- 모바일 기기 보안을 위한 법제도적 측면의 보안대책 마련
- 국내외 기업을 고려한 보안 대책 및 규제방안 마련

4. 연구 내용 및 결과

❍ 신규 모바일 단말 확산 현황 및 전망

국내 모바일 단말 보급이 점차 확산되어 스마트폰 가입자수는 2011년 7월말 기준 1,600만명으로 2011년말에는 2000만명이 넘을 것으로 예상이 되었으며, 2013년에는 국내 스마트폰 누적 가입자수는 3천만명을 돌파하고 2015년에는 4천만명을 넘어설 것으로 전망된다. 또한 스마트패드 이용자도 디지털 멀티미디어 활용 증가로 인해 2010년 18만명에서 2015년 1000만명으로 증가될 것으로 예상된다. 세계 스마트폰과 스마트패드 현황은 2015년에는 스마트폰은 10억 3천만대로 추정되며, 2011년 대비 2.1배의 성장률이 전망되며, 스마트패드는 2015년 2억 6천만대로 추정되며, 2011년 대비 4.2배로 성장할 것으로 전망된다.

❍ 국내외 모바일 단말 활용, 위협 동향 및 정책 현황

향후 신규 모바일 기기들은 이용자 맞춤형 애플리케이션이 더욱 활성화 될 것으로 전망되며 이에 따라 애플리케이션 이용은 일상생활 전반에 보다 깊숙이 침투할 것으로 예상된다. 대표적인 모바일 애플리케이션 분야에서는 LBS, AR, SNS, 근거리 통신 기술인 RFID와 NFC 등을 활용한 M2M 서비스 등의 기술들에 대한 활용이 더욱 적극적으로 추진될 전망이다.

위협동향으로는 단말기기, 네트워크, 서비스, 콘텐츠등에서의 기술적인 보안위협과 앱 유통환경 측면, 법제도적 측면, 국내외 기업 환경에서의 기술외적인 보안위협등으로 구분하여 이들의 최근 동향을 분석하였다.

방송통신위원회의는 2010년 12월 '스마트 모바일 시큐리티 종합계획'을 수립하여

2015년까지 안전한 모바일 인터넷 환경 조성을 위해 노력하고 있으며, 무선랜 정보보호 안내서, 클라우스 서비스 정보보호 안내서, 와이브로 보안기술 안내서, 스마트폰 백신 이용 안내서, 위치정보의 보호 및 이용등에 관한 법률등 신규 모바일 기기의 활성화를 위해 관련 정책 및 제도를 마련하고 있다.

❍ 안전한 모바일 단말 이용 환경 구축을 위한 보안 대책

스마트폰, 스마트패드등 스마트화 되어가는 다양한 신규 모바일 기기의 단말기, 네트워크, 서비스, 콘텐츠 등의 기술적인 보안대책을 제시하고 있으며, 신규 단말 보안 강화 및 안전한 앱 유통환경 개선책 수립, 모바일 기기 보안을 위한 법제도적 측면의 보안대책, 국내외 기업을 고려한 보안 대책 및 규제방안등에 대한 보안 대책을 제시하고 있다.

5. 정책적 활용 내용

모바일 인터넷이 활성화되면서 모바일 오피스 등 각종 신규 모바일 서비스가 등장하고 있다. 이러한 모바일 서비스에 대해 아래와 같은 보안 대책을 통해 이용자가 안심하고 이용할 수 있는 환경을 조성해야 한다.

첫째, 안전한 모바일 오피스 및 스마트워크 시스템 이용을 위한 단말, 시스템, 법적 문제 등 스마트 워크의 보안요소에 따른 정보보호 가이드라인을 개발하여 보급해야 한다. 이를 위해 모바일 오피스 사업자의 법적책임을 명확히 하고 이용자의 권익보호를 위한 관련 법제도를 개선해야 한다. 또한, 개인정보 제공 또는 위탁에 대한 통일된 법적 근거, 개인정보 유출・유실 시 배상 방안등에 대한 법적 기준을 마련하고 모바일 오피스를 구성하는 기술 및 제품의 보안성 평가 기준을 마련하는 인증제도를 개선해야 한다.

둘째, 최근 이용율이 급증하고 있는 모바일 SNS의 보안을 강화해야 한다. 위치정보 등 개인정보 유출사고 사전방지를 위해 개인정보 수집 시 개인정보 침해 위험성 사전고지 및 수집 동의 방안 등의 법제도를 마련해야 한다. 또한, 위치정보보호를 위해 개인위치정보 자기제어시스템을 구축해야 한다. 이를 통해 위치정보 사업자나 위치기반 서비스 사업자로 하여금 이용자가 위치정보 사용내역을 확인할 수 있도록 하여 이용자의

자기 위치정보 통제권을 강화할 수 있도록 해야 한다. 그리고 단축 URL을 악용한 악성코드 유포 및 피싱 사이트 유포를 예방하기 위해 국내외 단축 URL관련 정보 공유 체계를 구축해야 한다.

셋째, 모바일 클라우드 보안체계를 강화해야 한다. 이기종 플랫폼간 상호운용성 확보를 위한 통합인증체계를 구축하고 사고 원인 분석을 위한 '모바일 클라우드 포렌식' 기술을 개발하는 한편, 모바일 클라우드 서비스 유형 및 정보의 민감도에 따라 차등화된 보안 서비스를 제공하기 위한 표준 가이드라인을 마련해야 하며 모바일 클라우드 서비스 제공자간 신종 위협정보 공유와 신속 대응을 위한 침해대응체계가 마련되어야 한다.

마지막으로, 스마트폰 이용자의 무선 네트워크 사용량 증가로 인해 무선 네트워크의 안전성을 확보해야 한다. 무선랜 보안 관리를 강화하기 위해 무선랜 보안 표준모델 개발, 보안인식 제고 및 무선랜 보안 법제의 개선이 필요하다. 무선랜 보안 운영 표준 모델에 기반한 공중 Wi-Fi존을 구축하는 한편 무선 AP의 초기 패스워드 변경 여부, 보안 설정 여부, 인증・암호화 지침 준수 여부를 현장 점검하는 등 사설 무선랜의 보안운영 상황을 주기적으로 점검・개선해야 한다.

6. 기대효과

신규 모바일 단말들의 위협 현황과 전망을 통해 정보보호 이슈를 도출하고 선제적인 정책적 대응 방안을 수립에 기여할 수 있다. 이를 통해 이용자들의 안전한 인터넷 사용 환경 구축과 중장기적인 정보보호 종합대책 수립에 기여할 수 있다.

SUMMARY

1. Title

Study on Security for New Mobile Devices

2. Objective and Importance of Research

The recent widespread use of smartphone has enabled advanced life style based on mobile devices. In the future, the demand for mobile services providing mobility, openness, and diversity continuously will increases. As new mobile devices diversifies, however, new mobile security threats are emerging. This leads an increasing demand on emerging mobile security technologies, solutions, and policies for use of secure mobile devices. In this study, therefore, we analyze the new mobile security threats can occur in new mobile devices and suggest strategies to establish the countermeasures to mitigate new security threats. This will help to strengthen Korea's international competitive power as a powerful country of the IT industry.

3. Contents and Scope of the Research

The detailed contents of this project are as follows:

- ❍ State of the art and future trends in new mobile devices
- ❍ Usage, threat trends, and policy of new mobile devices
- ❍ Major security issues in new mobile devices
- ❍ Security countermeasures for securing mobile devices in corporate environments.

4. Research Results

In this study, we introduce the current state of the art and future trends in new mobile devices. Especially, we focus on new security threats and security policies in new mobile devices. By analyzing the new security threats, we provide security countermeasures and policy suggestions for securing mobile devices in corporate environments.

5. Policy Suggestions for Practical Use

The result of this study can be applied to the following.

❍ Information security guideline needs to be developed and deployed for secure mobile office and smart work system

❍ Mobile SNS security needs to be strengthened

❍ Mobile cloud security system needs to be strengthened

❍ As wireless network traffic in new mobile devices increases wireless network security needs to be strengthened.

6. Expectations

By analyzing new and emerging security threats and security policies in new mobile devices, this study will help guide to identify new security issues and establish mobile security policy and security countermeasures for new mobile devices. Finally, this study will help provide secure internet environment to users and establish national information security policy in the medium and long term.

CONTENTS

제 1 장 서 론

최근 다양한 애플리케이션의 개발, 트위터 및 페이스북 등의 소셜 네트워크 서비스(SNS: Social Network Service)의 활성화, 무선인터넷 이용 증가 등으로 스마트폰, 스마트패드(혹은 태블릿PC), e-book 리더 등 다양한 신규 모바일 기기가 등장하고 활성화되고 있다. 신규 모바일 기기는 다양한 기능이 집약되어있어 이용자들이 보다 윤택하고 풍요로운 삶을 설계하도록 도와준다. 예를들어 신규 모바일 기기들은 애플리케이션을 기반으로 전화통화는 물론 이메일 확인, 지도검색, 증강현실 등의 다양한 기능들을 제공한다. 즉, 과거 일반 PC에서만 처리할 수 있었던 일들을 이제는 언제, 어디서든 이용할 수 있게 되었다.

사람들의 업무가 전산화되고 인터넷과 관련된 업무처리가 증가하면서 일반 PC 활용이 증가하고 있다. 일반 PC에 대한 수요가 많아지고 전산업무 처리의 필요성이 증가함에 따라 이용자들은 이용하여 언제, 어디서든 업무를 수행할 수 있기를 원하지만, 일반 PC는 제품의 크기가 상대적으로 크기 때문에 휴대가 불편하다. 이 같은 이유로 언제, 어디서든 인터넷을 활용하여 편의를 추구하길 원하는 이용자들의 요구를 충족시키지 못하는 측면이 있다. 반면에 스마트폰, 스마트패드(태블릿PC)등의 신규 모바일 기기는 일반 PC에 상당한 수준의 업무 처리능력을 보유하고 있고, 인터넷을 활용하여 실시간으로 정보획득이 가능하며, 일반 PC에 비해 상대적으로 디바이스(device)의 크기가 작기 때문에 이용자들의 선호가 증가하고 있다. 신규 모바일 기기 미소지자들이 신규 모바일 기기에 대하여 적극적인 구매 의사를 밝히고 있으며, 판매량도 점차 증가하고 있는 추세가 이를 반증한다. 물론 신규 모바일 기기가 지금 당장 일반 PC를 대체하기는 어렵다. 그렇지만, 일반 PC의 약점을 보완하며 주목받고 있는 만큼 빠른 시일내에 활성활 될 수 있을 것으로 전망된다.

신규 모바일 기기를 통하여 개인간 정보나 자료의 교환이 원활해지면서 긴밀한 인적 네트워크가 형성되고, 업무의 효율성이 향상되는 등 신규 모바일 기기의 확대로 긍정적인 효과가 창출되고 있다. 하지만, 신규 모바일 기기의 우수성 및 편의성 등 긍정적인 측면의 이면에는 정보보안의 문제가 있다. 유선인터넷 또는 일반 PC에 대한 정보보안

이 여전히 미흡한 상황에서 신규 모바일 기기가 도입되면서 정보보안의 새로운 위협요소로 부각되고 있다.

따라서 본 연구 보고서에서는 국내외 신규 모바일 기기의 단말 확산 동향 및 시장 전망등을 살펴보고, 신규 모바일 기기의 확산으로 인한 주요 보안 이슈를 검토함으로써 향후 신규 모바일 기기의 정보보안의 논의 방향을 제시해보고자 한다.

제 2 장 신규 모바일 단말 확산 현황 및 전망

모바일 인터넷 이용은 얼마 전까지만 해도 비싼 무선 인터넷 요금, 무선 통신 인프라 투자 부족, 모바일 단말기 보급 미흡 등으로 대중화가 되기에는 여러 가지 어려움이 있었다. 하지만, 스마트폰의 도입과 함께 무제한 무선 요금제 출시, 무선랜(Wi-Fi), 와이브로(Wibro), LTE(Long Term Evolution)등의 4세대 이동통신 인프라의 투자 및 구축 확대, 국내외 제조사로 부터의 e-북리더(e-Book Reader), 스마트패드(혹은 태블릿PC)등 다양한 모바일 단말기의 보급 증가 등으로 인해 모바일 인터넷의 이용이 크게 증가하고 있다.

제 1 절 국내 현황 및 전망

우리나라는 지난 10년간 인프라 구축 위주의 IT성장정책을 통해서 세계 최고수준의 인터넷 이용환경을 조성하여 인터넷강국의 면모를 과시해 왔으며 이를 토대로 모바일 인터넷 시대를 맞이하고 있다. 스마트폰 등 각종 모바일 기기 활용이 증가하면서 인터넷 이용도 유선 중심에서 무선 및 유·무선 통합 환경으로 이동하고 있다.

이에 따라 스마트폰·스마트패드(혹은 태블릿PC)·스마트TV 등을 활용한 스마트워크 및 모바일 클라우드 서비스의 등장으로 스마트라이프(Smart Life)가 가속화되고 있으며 향후 모바일 인터넷은 무선 인터넷을 근간으로 모든 사물·기기가 연결되는 사물지능통신(M2M)으로의 진화가 예상된다. 사물지능통신은 사람대 사물, 사물대 사물 간 지능통신 서비스를 언제 어디서나 안전하고 편리하게 실시간으로 이용할 수 있는 미래 융합 ICT 인프라라고 할 수 있다.

최근 아이폰 앱 스토어 시장의 성공과 안드로이드 폰의 빠른 보급 등에 힘입어 스마트폰과 스마트패드와 같은 신규 모바일 기기 시장은 양적으로나 질적으로 급속히 증가하고 있다.

<표 2-1>에 따르면 2009년 국내 스마트폰 보급대수는 80만대에서 2011년 1626만대로

2009년 대비 16배 성장한 것으로 추정된다.

〈표 2-1〉 국내 스마트폰 보급 증가 추이

(단위: 만대)

구 분	2009	2010	2011	누적	성장률
보급대수	80	722	1,626	2,428	16배

자료: ZDNet Korea, 2011

[그림 2-1]은 2009년부터 2011년 7월 기준으로 실제 스마트폰 가입자 수에 대한 증가 추이를 보여주며, 보급대수와 일치하는 것을 알 수 있다.

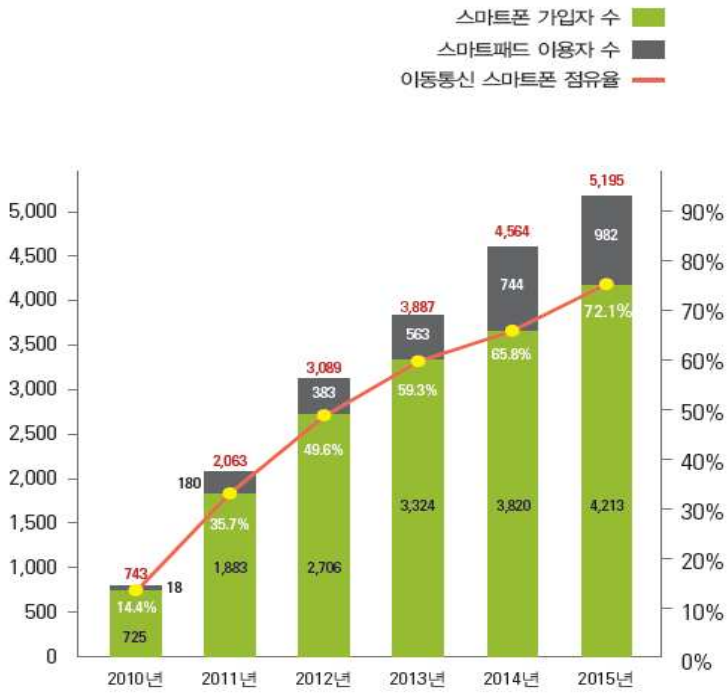
[그림 2-1] 국내 스마트폰 가입자 증가 추이

자료: 디지털타임스, 2011

[그림 2-2]는 국내 스마트폰 및 스마트패드 (누적) 보급에 대한 전망을 보여준다. 국내 모바일 단말 보급이 점차 확산되어 스마트폰 가입자수는 2010년 12월말 기준 722만명으로 전체 이동통신 가입자의 14.2%를 차지했다. 2013년에는 국내 스마트폰 누적 가입자수는 3천만명을 돌파하고 2015년에는 4천만명을 넘어설 것으로 전망된다.

또한 스마트패드 이용자도 디지털 멀티미디어 활용 증가로 인해 2010년 18만명에서 2015년 982만명으로 증가될 것으로 예상된다.

[그림 2-2] 국내 스마트폰 및 스마트패드 (누적) 보급 전망



자료: 'Mobile voice and data forecast pack: 2010-15' OVUM(2010.5월) 및 '2010 국가정보화백서(NIA, 2010.7월)' 등을 기반으로 KISDI·KCC 예측(2010.11월)

제 2 절 국외 현황 및 전망

세계의 총 인구가 70억 명을 초과한 현재, 휴대전화의 가입자도 증가를 지속하고 있어, 2011년 말의 휴대전화 가입자 수는 54억 4,270만 가입이 예상되며 선진국 등 휴대전화 이용이 인구보급률 100%를 돌파하고 있는 시장에서도 휴대전화 가입자 수의 증가는 지속적으로 증가하고 수요가 왕성한 신흥국·도상국의 일부에서는 제3세대 휴대전화(3G)의 도입이 시작되고 있다. 그 중 스마트폰과 스마트패드 현황은 <표 2-2>에 요약되어있으며 2015년에는 스마트폰은 10억 3천만대로 추정되며, 2011년 대비 2.1배의 성장률이 전망되며, 스마트패드는 2015년 2억 6천만대로 추정되며, 2011년 대비 4.2배로

성장할 것으로 전망된다.

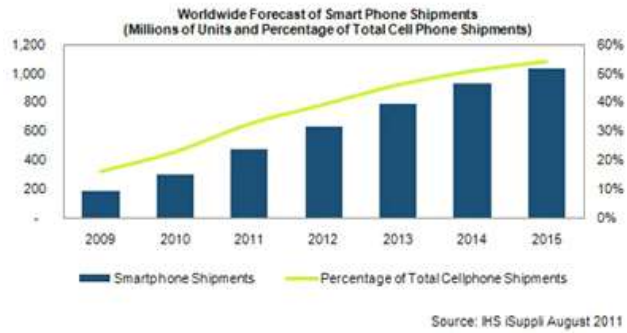
〈표 2-2〉 세계 스마트폰 및 스마트패드 현황 및 전망

스마트폰			스마트패드		
2011	2015(추정)	성장률	2011	2015	성장률
4억 8천만대	10억 3천만대	2.1배	6천만대	2억 6천만대	4.3배

자료: IHS iSuppli Research, 2011

2011년 8월 IHS iSuppli Research의 보고에 의하면 [그림 2-3]과같이 세계 스마트폰 가입자의 증가 추이가 전망되며, 2015년으로 갈수록 전체 휴대전화가입자수와 스마트폰 가입자수가 거의 일치함을 보여준다.

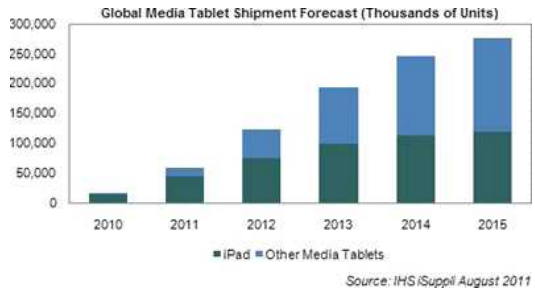
[그림 2-3] 세계 스마트폰 가입 전망



자료: IHS iSuppli Research, 2011 By 2015 smarphones will rule the mobile planet, 2011

또한 세계 스마트패드 가입자 증가 추이는 [그림 2-4]에 나타나있으며 2010년 애플사의 iPad제품이 100%를 차지하는 반면 2015년으로 갈수록 다른 스마트패드의 점유율이 더 높아지면서 다양한 스마트패드의 기기가 등장할 것으로 전망된다.

[그림 2-4] 세계 스마트패드 가입 전망



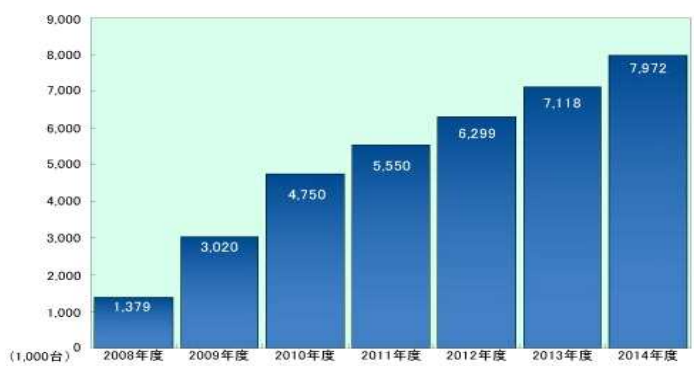
자료: HIS iSuppli Research, Media Tablet Forecast Increased as Apple's Dominance Grow, 2011

1. 일본

2009년도에 들어서 아이폰 3GS의 판매와 함께 스마트폰에 대한 인지도가 증가하여 일본 내 스마트폰 보급 시장은 전년도 대비 219%라는 고속성장과 함께 302만대에 달했다. 2010년도는 스마트폰 판매가 더욱 증가하여 475만여대에 이르렀다. 또한 2014년도에는 797만여대로 증가할 것으로 예상하고 있다.

[그림 2-5] 일본 스마트폰 보급률 추이

(단위: 천대)

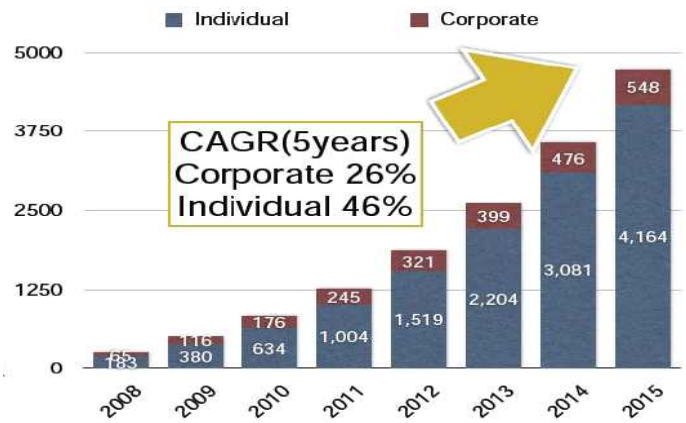


자료: 일본 MIC 경제연구소, 2010년 2월 조사자료

또한, MCPC(Mobile Computing Promotion consortium)에서는 [그림 2-6], [그림 2-7], [그림 2-8]에서 보여지는 바와같이 스마트폰과 스마트패드의 가입자 및 출하대수에 대해 개인사용자와 기업사용자로 분류하여 향후의 추이를 전망하고 있다.[그림 2-6]에서는 2010년을 기준으로 기업은 176만, 개인은 634만대의 스마트폰 가입자 수를 보여주고 있으며, 향후 2015년까지 기업은 26%, 개인은 46%의 가입자 수가 증가할 것으로 전망하고 있다.

[그림 2-6] 스마트폰 시장 전망 (가입자수)

(단위: 천만)

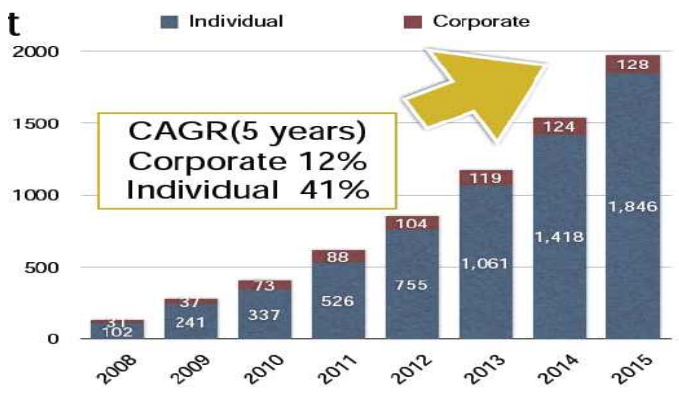


자료: MCPC/Impress R&D joint survey conducted in September 2010.

[그림 2-7]에서는 2010년을 기준으로 기업용 73만, 개인용 337만대의 스마트폰 출하대수를 보여주고 있으며, 향후 2015년까지 각각 12%, 46%로 증가할 것으로 전망하고 있다.

[그림 2-7] 스마트폰 시장 전망 (출하대수)

(단위: 천만)

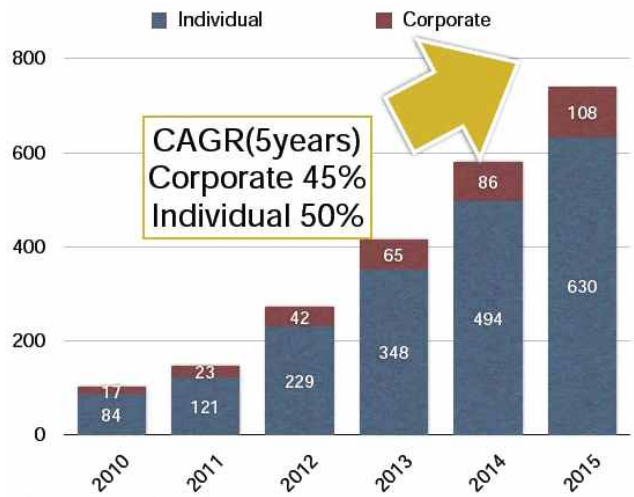


자료: MCPC/Impress R&D joint survey conducted in September 2010.

또한 [그림 2-8]에서는 2010년을 기준으로 기업용 17만, 개인용 84만대의 스마트패드 출하대수를 보여주고 있으며, 향후 2015년까지 각각 46%, 50%이상 증가할 것으로 전망하고 있다.

[그림 2-8] 스마트패드 시장 전망 (출하대수)

(단위: 천만)

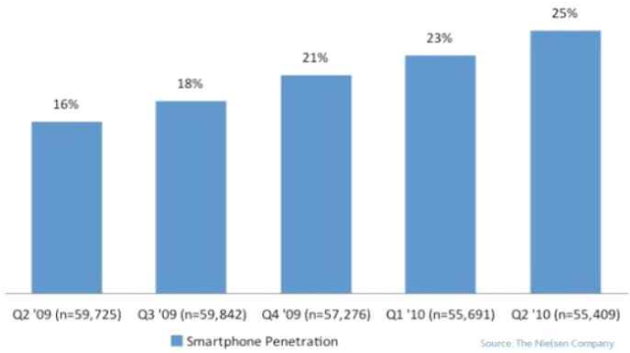


자료: MCPC/Impress R&D joint survey conducted in September 2010.

2. 미국

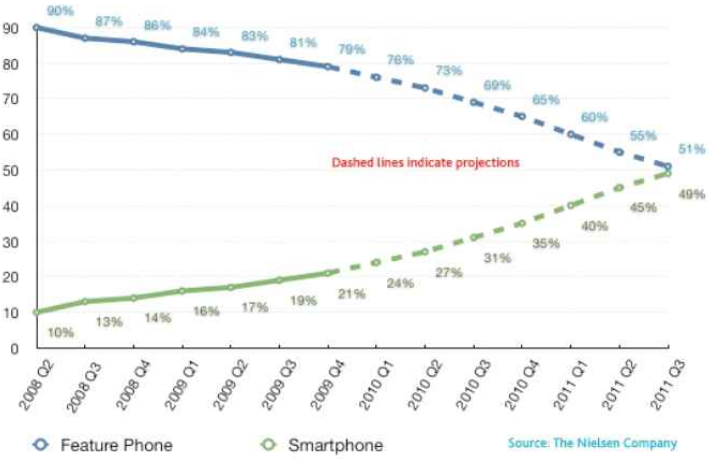
2007년부터 스마트폰 도입이 활성화됐던 미국은 전체 모바일 기기 중 스마트폰의 가입자가 2009년 2분기에 16%에서 2010년 2분기에는 25%로 증가한 것을 볼 수 있다.

[그림 2-9] 스마트폰 가입자



자료: Neilsen Company, 2010

[그림 2-10] 스마트폰 가입 현황 및 전망



자료: Neilsen Company, 2010

또한 향후에는 기존이 피쳐본 가입자 2008년 2분기 90%에서 2011년 3분기에는 51%로 대폭 감소하고 스마트폰 사용자는 2008년 2분기 10%에서 2011년 3분기에는 49%로 대폭 증가할 것으로 전망된다.

제 3 장 국내외 신규 모바일 기기 현황 분석

제 1 절 신규 모바일 기기 정의 및 활용 동향

1. 신규 모바일 기기의 정의

최근 모바일 시장은 다양한 신규 모바일 기기의 확산과 차세대 이동통신망의 도입을 바탕으로 급속히 발전하고 있다. 이로 인해 언제 어디서든지 온라인에 접속할 수 있는 모바일 인터넷 시대가 본격화되었으며 업무처리, 학습, 의료진료 등 사회 전반에 스마트 기술이 활용되는 '스마트사이어티(Smartciety)' 시대가 도래 하고 있다. 이러한 패러다임의 변화에 가장 주도적인 역할을 한 것은 단연 스마트폰이다. 2007년 애플(Apple)사의 아이폰(iPhone) 등장 이후 단순히 업무용 개인 단말기로 여겨지던 스마트폰에 대한 인식이 획기적으로 바뀌면서 산업, 사회, 문화 전반에 걸친 거대한 변화가 촉발된 것이다.

아이폰의 성공을 필두로 하여 모바일 시장의 주도권을 차지하기 위해 다양한 모바일 기기들이 등장하였는데 이러한 신규 모바일 기기는 기존의 모바일 기기와 확연히 다른 몇 가지의 특징이 있다.

첫 번째 특징은 다양한 기능을 제공하기 위한 고성능의 하드웨어를 기본으로 한다는 점이다. 스마트폰의 경우 전화와 문자를 주고받는 기존의 단순한 기능을 벗어나 웹브라우저를 통한 인터넷 망으로의 접속, 문서작업, GPS를 사용한 위치기반 서비스와 증강현실 서비스, 모바일 게임 등 다양한 기능을 제공하고 있다. 따라서 이러한 기능들을 수행하기 위한 고성능의 APU(Application Processing Unit)와 대용량의 메모리가 필수적으로 탑재된다.

신규 모바일 기기의 두 번째 특징은 개방형 모바일 소프트웨어 플랫폼을 기반으로 작동한다는 것이다. 애플사의 iOS와 구글(Google)사의 안드로이드(Android)가 신규 모바일 기기에 탑재되는 대표적인 개방형 플랫폼이다. 플랫폼 제공업체의 정책에 따라 개방의 범위가 다르지만 일반적으로 제공업체들은 시장 선점을 위해 애플리케이션 개

발용 SDK나 API를 개방하여 개발자들로 하여금 다양한 애플리케이션을 개발하도록 유도하고 있다.

마지막으로 신규 모바일 기기는 차세대 이동통신망이나 Wi-fi망 등을 통하여 인터넷에 접속할 수 있다. 따라서 이러한 특징을 활용하여 웹서핑, 이메일 송수신 등이 가능하고 더 나아가 최근 화두가 되고 있는 클라우드 컴퓨팅과의 융합으로 스마트워크의 실현을 앞당기고 있다. 이밖에 신규 모바일 기기들은 다양한 방식의 센서를 내장한 인터페이스를 지원하고 다양한 애플리케이션을 다운로드하여 설치할 수 있다는 특징도 가지고 있다.

이와 같은 기존의 모바일 기기와 차별화 되는 특징들을 고려하여 신규 모바일 기기를 정의내리면 '고성능의 하드웨어와 개방형 모바일 소프트웨어 플랫폼을 기반으로 하여 인터넷 망에 접속 가능한 휴대형 기기'라고 할 수 있으며 이러한 정의에 적합한 모바일 기기에는 대표적으로 스마트폰과 스마트패드가 있다. 신규 모바일 기기는 [그림 3-1]과 같이 구성된다.

[그림 3-1] 신규 모바일 기기의 구성

가. 스마트폰(Smart Phone)

스마트폰은 기존의 휴대전화 기능에 PDA(개인휴대단말기)의 기능이 합쳐져 데스크

톱 환경과 유사한 다양한 애플리케이션을 제공할 수 있는 모바일 기기를 말한다. 스마트폰에는 범용 운영체제 기반의 모바일 소프트웨어 플랫폼이 탑재되는데 어떤 플랫폼이 탑재되느냐에 따라서 설치 가능한 애플리케이션과 사용자경험이 결정된다. 따라서 기기에 탑재된 모바일 소프트웨어 플랫폼을 기준으로 스마트폰의 세부적인 분류가 가능하다.

1) iOS(iPhone OS)

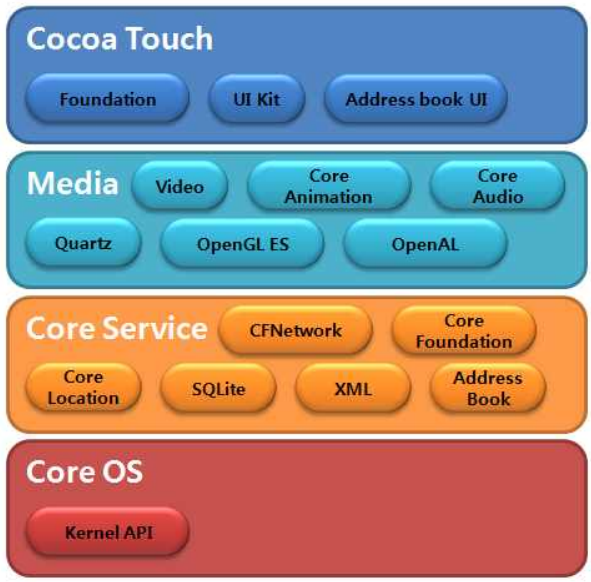
애플사에서 MAC OS X를 기반으로 개발한 모바일 소프트웨어 플랫폼으로써 아이폰, 아이팟, 아이패드 등 자사의 다양한 모바일 기기에 탑재되어있다. 애플은 iOS 기반의 애플리케이션 개발을 유도하기 위해 API나 SDK를 공급하고 있으며 결과적으로 수많은 애플리케이션이 개발되어 하드웨어 중심의 기존 모바일 시장 구조를 소프트웨어 및 콘텐츠 중심의 시장구조로 바꾸는데 큰 영향을 미쳤다.

iOS는 <표 3-1>과 같은 특징을 가지며 [그림 3-1]와 같은 구조로 이루어져 있다. [그림 3-2]는 iOS가 탑재된 대표적인 스마트폰 제품을 보여준다.

〈표 3−1〉 iOS의 플랫폼의 특징

기반 커널	MAC OS X
최신 버전	iOS 4.3.3
구조	Core OS, Core Service, Medeia, Cocoa Touch
특징	Objective-C 기반의 개발환경 기존 버전 설치 제품과의 높은 호환성
적용 모바일 기기	iOS 기반 스마트폰, 스마트패드

[그림 3-2] iOS의 구조



[그림 3-3] iOS 탑재 스마트폰

2) 안드로이드(Android)

구글에서 iOS에 대항하기 위해 개발한 모바일 소프트웨어 플랫폼으로서 운영체제, 미들웨어, 자바(Java)언어로 개발되는 애플리케이션들을 포함한다. 구글은 모바일 기기 제조사들로 하여금 안드로이드 플랫폼을 로열티 없이 사용할 수 있도록 허가하여 시장에 빠른 속도로 보급되고 있다.

<표 3-2>는 안드로이드의 특징을 보여주며 [그림 3-4]와 [그림 3-5]는 각각 안드로이

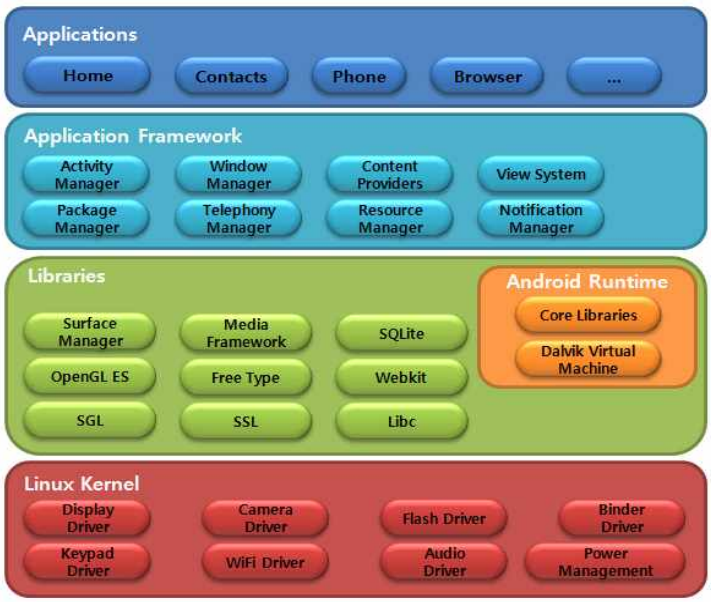
드가 탑재된 스마트폰 기기와 안드로이드 플랫폼의 구조를 보여준다.

〈표 3−2〉 안드로이드 플랫폼의 특징

기반 커널	리눅스 커널
최신 버전	Android 2.3(스마트폰용) / Android 3.2(스마트패드용)
구조	Linux Kernel, Library, Android Runtime Library, Application Framework, Applications
특징	자체 자바 가상 머신을 통한 편리한 개발환경 제공 개방성을 바탕으로 여러 제조사의 제품에 탑재
적용 모바일 기기	안드로이드 기반 스마트폰, 스마트패드

[그림 3−4] 안드로이드 탑재 스마트폰

[그림 3-5] 안드로이드 플랫폼의 구조



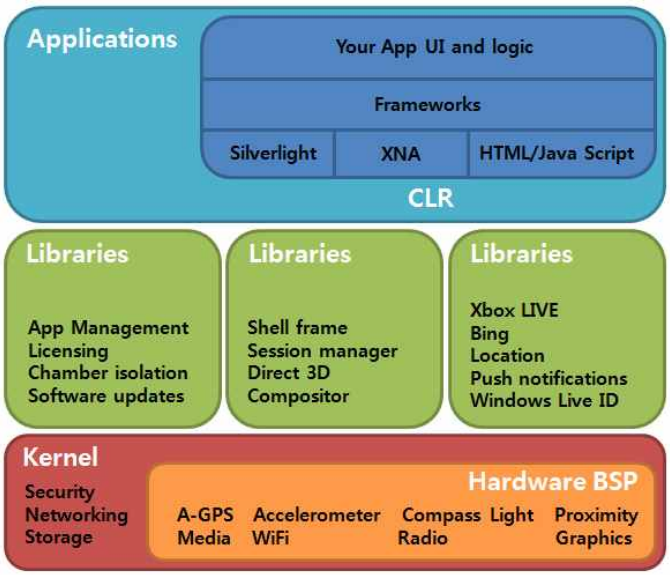
3) 윈도우폰(Windows Phone) 7

마이크로소프트(Microsoft)사에서 기존의 윈도우 모바일(Windows Mobile)의 단점을 개선시켜 개발한 플랫폼이다. 윈도우폰7은 기존 PC의 윈도우 운영체제를 기반으로 개발된 업무용 소프트웨어와 높은 호환성을 가진다는 특징이 있다. 시장 점유율에서 아직 iOS나 안드로이드에 비해 두드러지는 모습을 보이지 못하고 있지만 최근 노키아(Nokia)사와의 제휴를 약진의 발판으로 삼아 급격한 성장세를 보일 것이라는 예측이 나오고 있다. <표 3-3>은 윈도우폰7 플랫폼의 특징을 나타내며 [그림 3-6]과 [그림 3-7]은 각각 윈도우폰7 내부 소프트웨어의 구조와 탑재 스마트폰을 보여준다.

〈표 3-3〉 윈도우폰7 플랫폼의 특징

기반 커널	Windows Embedded CE
최신 버전	Windows Phone 7 Mango
구조	Windows embedded CE Kernel, OEM Adaptation Layer, Board Support Package, Application Platforms
특징	실버라이트와 닷넷 언어를 사용한 개발환경 XNA 기반 고속 프레임워크 지원 최소 하드웨어 사양 지정으로 균일한 성능 보장
적용 모바일 기기	윈도우폰7 기반 스마트폰

[그림 3-6] 윈도우폰7 소프트웨어 구조



[그림 3-7] 윈도우폰7 탑재 스마트폰

4) 블랙베리(Blackberry)

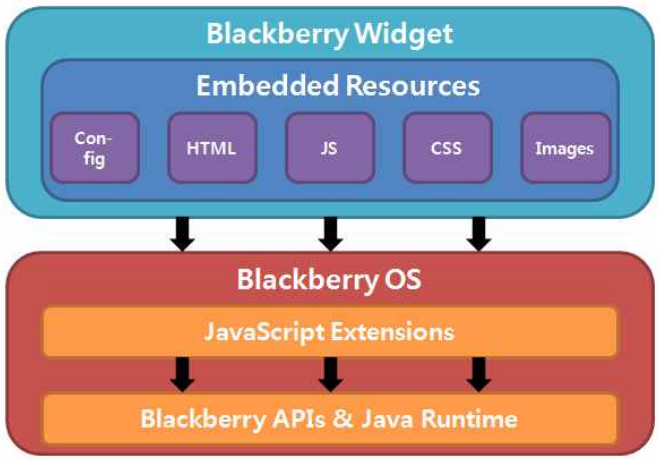
림(Rim)사에서 자체적으로 개발한 플랫폼으로 자사의 스마트폰에 탑재된다. 마이크로소프트사의 익스체인저 서버와 로터스(Lotus)사의 이메일 시스템등과의 동기화를 지원하여 업무처리에 최적화되어 있으며 자바를 지원하고 위젯(Widget) SDK를 제공하여 개발자들이 애플리케이션을 개발할 수 있도록 지원하고 있다.

<표 3-4>는 블랙베리 플랫폼의 특징을 보여주며 [그림 3-8]과 [그림 3-9]는 각각 블랙베리 플랫폼 OS와 위젯의 구조, 그리고 블랙베리 탑재 스마트폰 제품을 보여준다.

〈표 3−4〉 블랙베리 플랫폼의 특징

기반 커널	RIM 자체개발 커널
최신 버전	Blackberry OS 7
구조	Blackberry OS, APIs, Java Runtime, Blackberry Widget
특징	HTML, CSS, Javascript 등의 개발 환경 지원 멀티태스킹, MIDP, WAP 지원 자사의 모바일 기기에만 탑재
적용 모바일 기기	블랙베리 기반 스마트폰, 스마트패드

[그림 3-8] 블랙베리 OS, 위젯 구조



[그림 3-9] 블랙베리 탑재 스마트폰

5) 바다(bada)

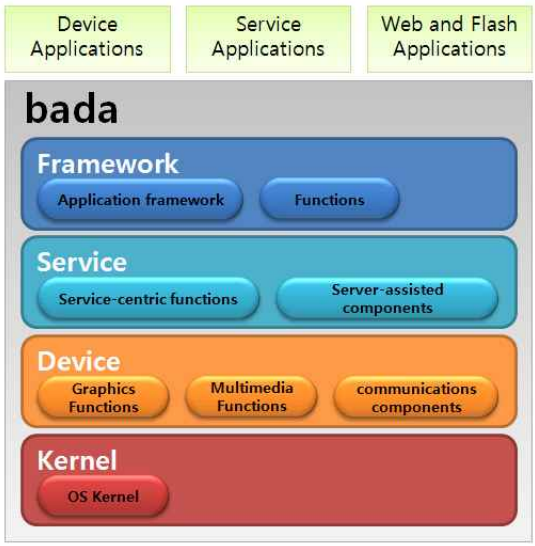
바다는 삼성전자가 스마트폰에 탑재하기 위하여 개발한 모바일 플랫폼이다. 바다 OS는 RTOS를 기반으로 하여, OS 커널을 분리한 미들웨어 형태로 탑재되어있다. 애플리케이션 개발을 위한 IDE, 컴파일러, 에뮬레이터가 공개되어있으며 개발 언어는 C++를 사용한다. 현재 바다 플랫폼은 삼성전자의 스마트폰에만 탑재되고 있으나 오픈소스가 기본 방침으로 타 업체의 사용도 가능해질 전망이다.

<표 3-5>는 바다 플랫폼의 특징을 보여주며 [그림 3-10]과 [그림 3-11]은 바다 플랫폼의 구조, 그리고 바다 플랫폼 탑재 스마트폰 제품을 보여준다.

〈표 3-5〉 바다 플랫폼의 특징

기반 커널	Nucleus RTOS
최신 버전	bada OS 2.0
구조	bada OS Kernel, Device Layer, Service Layer, Framework Layer, Application
특징	Eclipse 기반 IDE 지원 저성능의 하드웨어에 적합하게 설계
적용 모바일 기기	바다 기반 스마트폰

[그림 3-10] 바다 플랫폼 구조



[그림 3-11] 바다 탑재 스마트폰

나. 스마트패드(Smart Pad)

스마트패드는 앞서 기술한 신규 모바일 기기의 특징들을 만족시키는 개인용 휴대단말기로서 스마트폰과 유사한 하드웨어, 소프트웨어 구성을 가진다. 제품에 따라서는 스마트폰과 같이 차세대 이동통신망을 통한 음성통화가 가능한 경우도 있다. 스마트패드와 스마트폰의 가장 뚜렷한 차이점은 화면크기의 차이에서 오는 기기 크기의 차이점, 그리고 적합한 활용분야의 차이점이다. 스마트패드와 비슷한 제품으로 노트북에서 분화된 태블릿PC가 있으나 운영체제, 입력장치, 네트워크 연결 등에서 차이점을 보인다. 스마트패드는 일반적으로 7인치~10인치 사이의 화면크기를 가지며 터치스크린 방식의 인터페이스를 지원한다. 따라서 단순 업무 생산성 향상뿐만 아니라 전자책, 웹서핑, 게임 등의 활용분야에서 강점을 가진다.

스마트패드는 스마트폰용으로 개발된 모바일 소프트웨어 플랫폼을 탑재하고 있으므로 스마트폰과 마찬가지로 탑재된 플랫폼에 따라 분류가 가능하다. <표 3-6>은 탑재된 모바일 소프트웨어 플랫폼을 기준으로 분류한 스마트패드의 종류를 나타낸다.

〈표 3-6〉 스마트패드의 분류

플랫폼	제조사	제품명	제품 사진
iOS	Apple	iPad	
Android	Samsung	Galaxy tab	
	HTC	Flyer	
	Motorola	Zoom	
Blackberry	RIM	Playbook	
WebOS	HP	TouchPad	

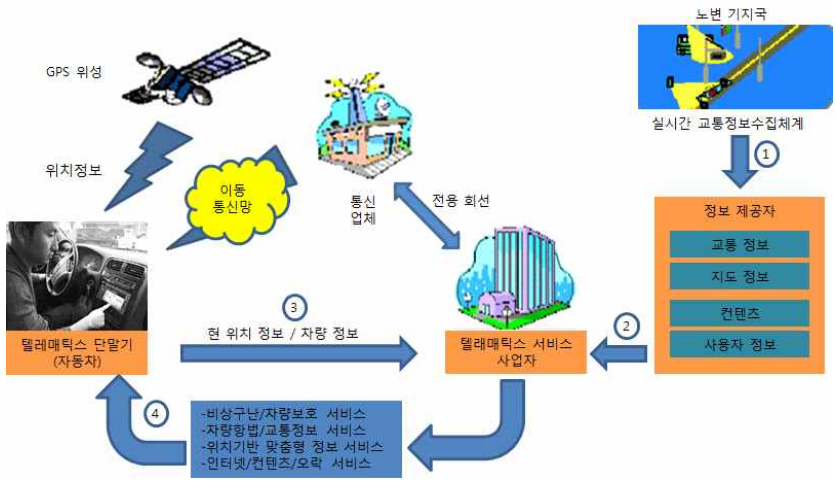
다. 무선 통신을 이용한 신규 스마트기기

1) 차량 기술

- 텔레매틱스(Telematics)

텔레매틱스란 자동차와 무선통신을 결합한 새로운 개념의 차량 무선인터넷 서비스이다. 자동차 안에서 이메일을 주고받고, 인터넷을 통해 각종 정보도 검색할 수 있는 오토(auto) PC를 이용한다는 점에서 오토모티브 텔레매틱스라고도 부른다. 운전자가 무선 네트워크를 통해 차량을 원격 진단하고, 무선모뎀을 장착한 오토 PC로 교통 및 생활 정보, 긴급구난 등 각종 정보를 이용할 수 있다. 또한 사무실과 친구들에게 전화 메시지를 전할 수 있음은 물론, 음성 이메일을 주고받을 수도 있고, 오디오북을 다운받을 수도 있다.

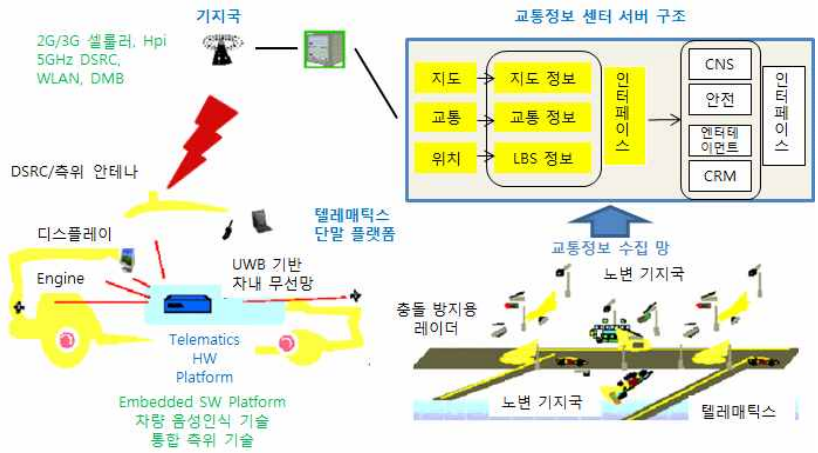
[그림 3-12] 텔레매틱스 개념도



텔레매틱스는 미국의 제너럴 모터스(GM)와 모토로라의 합작회사인 온스타(On-Star)가 이미 GPS 위성을 이용해 서비스를 제공하고 있는 한편 포드-퀄컴, 벤츠-도이치텔레콤 등 자동차 메이커와 이동통신 전문업체간의 합작이 활발하게 이루어지고 있다. 국내에서도 텔레매틱스 서비스 개발을 위해 자동차 회사와 이동통신업체 간의 협력이 활발하다. 서비스 형태에 따라 뉴스수신, 주식투자, 전자상거래, 금융거래, 호텔예약, 팩시밀리 송수신, 게임, 차량 사고 및 도난 등 다양한 서비스가 가능하다. 특히 자동차가 주행

중에 고장이 나면 무선통신으로 서비스센터에 연결되고, 엔진 속에 내장된 컴퓨터가 자동차 주요 부분의 상태를 알려주어 언제든지 정비사에게 정확한 차의 고장 위치와 원인을 알려준다. 또한 블랙박스와 연결된 카메라를 이용해 주행간의 영상을 기록하여, 사고시 비디오 파일을 참조할 수 있다.

[그림 3-13] 텔레매틱스의 기술 구성도



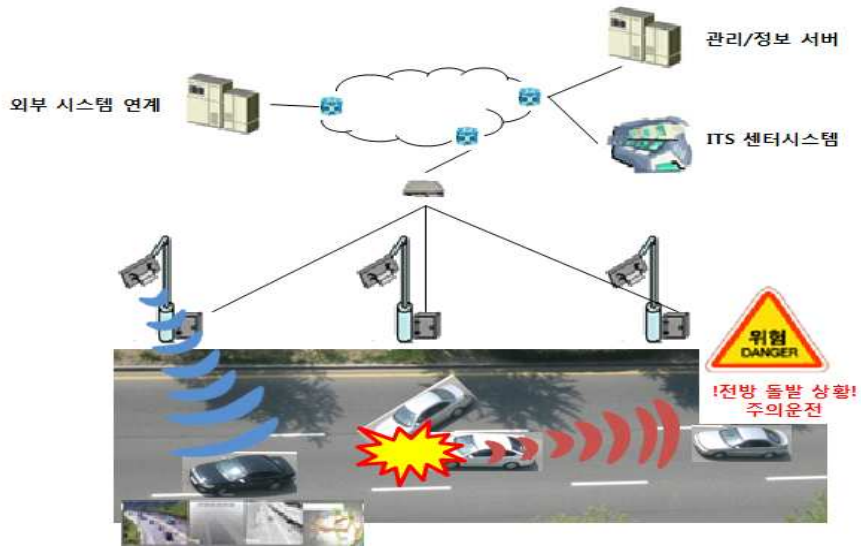
-VMC(멀티홉 방식의 차량간 통신 기술)

한국전자통신연구원(ETRI)은 교통사고를 줄이고 목적지에 빨리 도달하게 하는 스마트 하이웨이(Smart Highway) 시스템의 핵심기술로써 VMC를 개발했다. 이는 차량간 실시간 무선통신을 통해 앞차의 사고 등 돌발 상황이 뒤따라 오는 차에 직접 전달돼 연쇄추돌을 방지한다. 그리고 네비게이션과 연동시 교통정체 없는 빠른 길 안내, 차량 고장 원격점검 등에 활용할 수 있다.

기존 차량에서 사용 가능한 무선통신 기술인 이동통신, 무선랜, 하이패스 등은 모두 도로변에 설치된 기지국을 통해 정보를 주고받는데 비해 차량간 직접 통신이 가능하다. 이에 따라 통신비용이 저렴하고 응답시간이 100ms 이내로 짧아 차량 안전과 첨단 교통시스템 구축에 필요한 기술로 평가받고 있다. 또한, 시속 200km의 고속 이동중에도 교신이 가능하며 1km까지 통신이 가능하다. VMC 기술은 현재 상용화 수준에 가까운 통

신칩 개발까지 이루어졌다.

[그림 3-14] VMC 기술 개념도



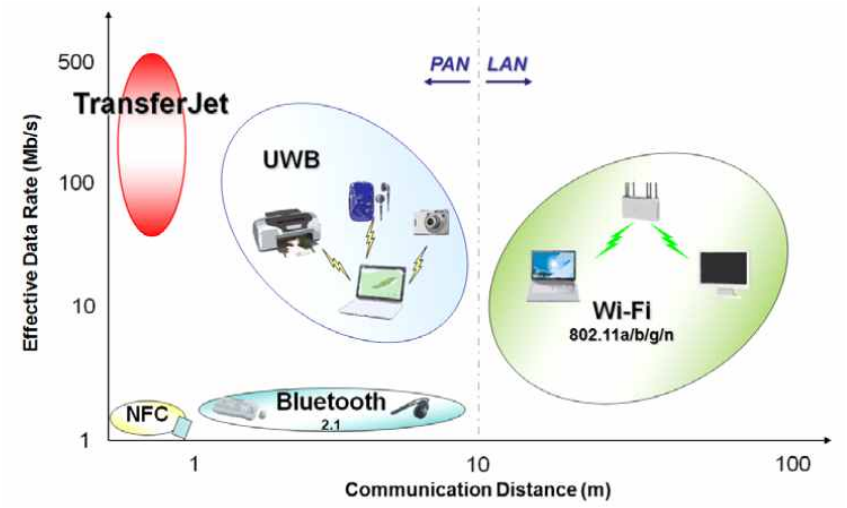
2) 무선 사진 전송 카메라

무선 사진 전송 카메라는 근거리 무선통신 기술을 이용한 카메라로써, 일반적으로는 블루투스, 지그비 또는 Wi-fi를 이용하여 사진이나 동영상 파일을 자동으로 전송한다. 이는 모두 10~20m안에서 이루어지는 근거리 무선 통신 방식을 사용한다. 사용자가 10~20m 근방에 카메라를 위치시키면 자동적으로 카메라에 저장되어있는 사진 파일을 PC로 전송시키는 방식이다. Sony의 경우에는 독자적인 근거리 무선통신 기술인 트랜스퍼젯(Transfer Jet)을 개발하여 상용화에 성공했다. 그리고 캐논은 s95 모델에 Eye-Fi 카드를 삽입하여 이미지들을 무선으로 PC로 자동 전송하거나 웹사이트에 업로드할 수 있도록 하였다.

이러한 근거리 무선 통신의 주목할 점은 짧은 전송거리를 통해 데이터 유출의 위험을 최소화할 수 있다는 점이다. 그 이유는 트랜스퍼젯의 경우 장치를 통해 연결될 수 있는 기기를 제한할 수 있도록 보안 설정을 할 수 있기 때문이다. 그리고 이러한 근거리 무선 통신은 데이터 전송속도가 빨라 스마트폰, 스마트패드 등 대부분의 모바일기기

에서 사용된다.

[그림 3-15] 트랜스퍼젯 기술의 포지셔닝



2. 신규 모바일 기기의 활용 동향

신규 모바일 기기는 앱스토어나 오픈 마켓을 통해 필요한 기능을 추가하고 변화시킬 수 있는‘ 사용자 중심(user-centric)’의 장치로 인간적, 지능적 감지 기능을 통해 다양한 형태의 정보를 취득하고 소비할 수 있는 특성으로 인해 패러다임 변화를 주도하고 있다. 또한, 사람과 정보를 연결하면서 SNS(Social Networking Service)와 같은 입체적인 의사 소통을 제공하고 있으며, 사업적으로는 이동통신사와 단말제조사가 독점하던 시장에서 소프트웨어 플랫폼 중심으로 이동함에 따라 수직적 구조에서 상호 Win-Win하는 수평적 구조로 재편되고 있다.

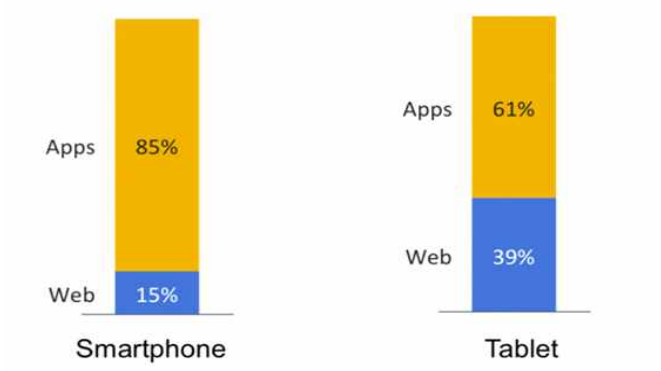
[그림 3-16]은 대표적인 신규 모바일 기기로서 스마트폰, 스마트패드, 스마트TV로 분류하고 이들의 네트워크/인프라 환경, 제공되는 서비스와 콘텐츠, 제공되어야하는 정보보안 요소들에 대해 보여주고 있다.

[그림 3-16] 신규 모바일 기기

구 분	네트워크/인프라	서비스/콘텐츠			보안/윤리
스마트폰	무선 네트워크	모바일 앱	상황인식	비즈니스/지식 인텔리전스	정보보호
태블릿 PC	사물지능통신	오픈 마켓	분석기술	3D	개인정보
스마트 TV	사물인터넷	소셜네트워크 /미디어	가상화	스마트워크	통합보안
	미래인터넷	증강현실	클라우드	그린 IT	인터넷 윤리
	오픈 플랫폼	위치기반 서비스	융합/컨버전스		

스마트폰과 스마트패드와 같은 모바일 기기는 서비스를 제공하기위해 애플리케이션을 제공하는데, [그림 3-17]을 보면 스마트폰에서는 사용시간의 85%를 모바일 애플리케이션을 이용하고, 스마트패드에서는 61%를 이용하고 있으며, 웹 애플리케이션의 이용도는 각각 15%, 35%이다. Zokem'의 연구팀의 보고에 의하면, 이는 스마트패드와 같이 더 큰화면과 더 나은 사용자 환경에서는 상대적으로 웹브라우징을 선호하고, 반면 작은 화면과 간단한 사용자 환경을 가지고 있는 스마트폰에서는 모바일 애플리케이션의 이용을 선호한다.

[그림 3-17] 스마트폰과 스마트패드 이용 비율



자료: Zokem LTD., 2010

신규 모바일 기기는 강력한 하드웨어 성능과 다양한 애플리케이션, 인터넷과의 결합으로 기존의 모바일 기기가 가지지 못했던 여러 가지 기능을 제공한다. 따라서 모바일 기기의 활용 분야가 크게 확장되었고 이는 우리의 생활방식까지 변화시키고 있다.

신규 모바일 기기인 스마트폰과 스마트패드는 전반적으로 비슷한 분야에서 활용이 가능하며 세부적인 활용 분야와 적합성은 <표 3-7>과 같다[1].

〈표 3−7〉 신규 모바일 기기의 활용 적합 분야

분야	스마트폰 적합성	스마트패드 적합성	주요기능
게임	매우 높음	매우 높음	게임단말
가전	낮음	낮음	가전 허브
교육	중간	매우 높음	교육 단말
음악	높음	중간	음악 재생
방송	낮음	중간	방송단말
영화	중간	높음	다운 재생
만화	중간	매우 높음	디지털 만화 리더
출판	낮음	매우 높음	전자책 리더
의료	중간	높음	원격의료단말
자동차	높음	중간	차량 내 서비스
물류	매우 높음	높음	정보 단말
광고	높음	매우 높음	광고 게시

위와 같은 다양한 활용분야를 보다 구체적으로 살펴보면 게임 분야에서는 기존에 휴대용 게임기기로 출시되던 많은 게임들이 스마트폰이나 스마트패드 용으로 출시가 되고 있다. 특히 온라인 접속이 언제나 가능하다는 장점과 각종 내장 센서를 활용할 수 있다는 장점 때문에 신규 모바일 기기 게임 시장은 급속도로 성장하고 있다. 교육 분야의 대표적인 서비스로는 동영상강의 시청과 각종 사전 애플리케이션을 예로 들 수 있으며 음악, 영화분야에서는 애플사의 아이튠즈(iTunes)와 같은 모바일 미디어 마켓의

1) iPad 시장 전망과 모바일 산업의 변화 (ETRI 전자통신동향분석 제25권 제5호 2010년 10월)

등장으로 컨텐츠를 손쉽게 다운로드 받을 수 있는 환경이 조성되고 있다. 스마트패드의 경우 큰 화면을 강점으로 내새워 전자책 시장에서도 핵심적인 단말의 역할을 하고 있으며 자동차 분야에서는 내비게이션, 차량 내 블랙박스로 사용될 수 있다. 이밖에도 병원 내에서 의료진료 단말로의 활용 가능성을 보여주고 있으며 물류분야에서는 기존에 PDA가 담당하던 정보 단말로서의 역할을 신규 모바일 기기가 대신하고 있다. 이처럼 신규 모바일 기기의 활용 분야는 우리 삶의 전범위에 걸친다고 해도 과언이 아닐 정도로 크게 확장되고 있다.

향후 신규 모바일 기기들은 이용자 맞춤형 애플리케이션이 더욱 활성화 될 것으로 전망되며 이에 따라 애플리케이션 이용은 일상생활 전반에 보다 깊숙이 침투할 것으로 예상된다. 대표적인 모바일 애플리케이션 분야에서는 LBS, AR, SNS, 근거리 통신 기술인 RFID와 NFC 등을 활용한 M2M 서비스 등의 기술들에 대한 활용이 더욱 적극적으로 추진될 전망이며, 이들 서비스의 실제 활용 사례는 <표 3-8>과 같다.

〈표 3-8〉 신규 모바일 기기의 주요 활용 서비스 및 사례

구분	특징	사례
위치기반 서비스	통신신호를 통해 단말 위치를 인식하여 이용자의 위치에 적합한 지역 서비스 제공	- 네비게이션서비스 -주변 뉴스 및 일기예보 -위치기반 모바일 광고
증강현실	카메라를 통해 촬영된 현실 공간에 디지털 이미지를 덧씌워 현실과 가상의 경계를 허문 독특한 콘텐츠 제공	-AR코드 통한 부가정보 -LBS 연계 지역정보 -AR광고 및 프로모션
모바일 SNS	모바일 환경의 즉시성을 활용한 SNS서비스 제공. 다른 모바일 서비스와 연계하여 서비스 영역 확대	-실시간 SNS서비스 -LBS 연계로 근처 친구와 커뮤니케이션
M2M	기계간 근거리 통신 기능을 통해 모바일 결제, 데이터 송수신 등의 서비스 제공	-모바일결제 및 뱅킹 -홈 네트워크 서비스 -근거리 이동통신 -자동차 애플리케이션
일반 미디어 콘텐츠	음악, 동영상, 게임, 방송콘텐츠 등 일반 미디어 콘텐츠를모바일 환경에서 제공	- 모바일 미디어 콘텐츠재생 서비스 - DMB 등
모바일 오피스	원하는 장소에서 원격으로 이메일, SMS, 그룹웨어와 같은 업무용 애플리케이션 서비스 제공	- 스마트워크

자료: 정보통신정책연구원. 모바일 애플리케이션의 동향과 전망. 2010

이들 서비스 중 M2M을 활용한 자동차 연동 모바일 텔레매틱스 애플리케이션 시장이 개화하고 의료용 애플리케이션과 기업이 자체적으로 제작한 비즈니스용 애플리케이션도 크게 증가할 것으로 기대된다. ABI리서치는 세계 자동차용 애플리케이션 이용자가 2010년 140만 명에서 2015년 2,800만 명으로 급증할 것으로 전망하고 있으며, IDC는 2011년 미국 성인의 14%가 의료용 애플리케이션으로 건강을 관리할 것으로 예측하고 있다. 2010년 11월 출시된 아이패드iOS 4.2버전은 PC에 연결하지 않아도 기업에서 자체적으로 개발한 애플리케이션을 직원들의 아이패드에 무선으로 배포할 수 있도록 하는 기능을 갖추어 기업의 자체제작 비즈니스용 애플리케이션 증가에 기여할 전망된다.

신규 모바일기기에 이러한 대표적인 서비스들은 애플리케이션을 통해서 제공이 되며, 향후 모바일 애플리케이션은 다음과 같이 다섯 가지 형태로의 발전이 진행될 것으로 전망된다.

첫째, 자동차 애플리케이션(Automotive apps): SK Telecom은 2011년 말 자동차용 모바일 시스템을 중국에서 상용화 할 예정이다. 이 시스템은 모바일폰으로 차량관제를 할 수 있는 위젯 사용을 지원한다. 포드(Ford Motors)는 마이포드(MyFord) 터치 시스템 구축 추진하고 있다. 이 시스템은 단순히 스마트폰을 통해 클라이언트/서버 환경을 구축하여 자동차가 클라이언트가 되고 스마트폰은 서버 기능을 수행하는 구조이다.

둘째, 모바일 영상통화(Mobile VoIP+Video): 현재 진행되고 있는 모바일 VoIP의 다음 단계는 영상통화로 예상된다. 모바일폰인 Nokia N900에서는 이미 모바일 영상통화가 구현되었다. Apple도 자사가 출시한 iPhone 4에 FaceTime 을 이용하여 영상통화를 제공하였으며, 이 서비스는 Wi-Fi 네트워크에서 iPhone 4 이상 사용자만이 이용할 수 있다. 또한 야후는 Wi-Fi와 3G 네트워크를 이용한 무료 메신저 앱을 준비하고 있는데 이 앱은 모바일과 PC 간 영상통화 가능하다.

셋째, 소셜 미디어(Social Media): TNS에 따르면 모바일폰 이용자들은 평균적으로 주당 3.1시간을 소셜 네트워킹에 이용하는 반면, E-mail에는 주당 2.2시간을 이용하는 것으로 나타났다. 모바일폰 사용량이 높아지면서 소셜 미디어에서시장과 애플리케이션 시장은 상호 성장을 견인하는 구조가 확대될 전망된다.

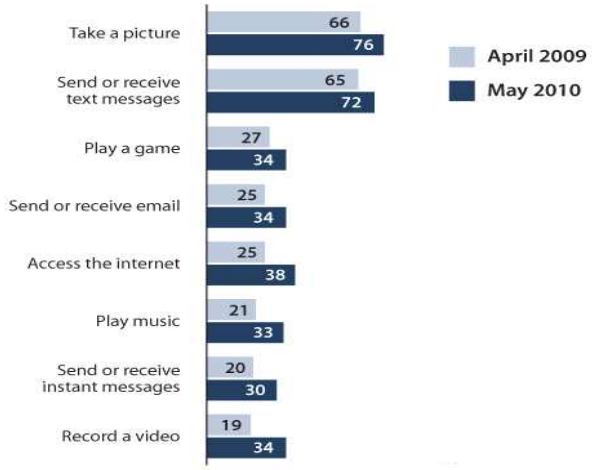
넷째, 증강현실(Augmented Reality: AR): 증강현실 앱이 지속적으로 증가할 전망이다. 증강현실형 애플리케이션은 모바일 게임은 물론 박물관 가이드까지 다양한 형태로 제공되고 있으며, 네트워킹 블로그 중 하나인 리드라이트웹(ReadWriteWeb)은 아이튠스 앱스토어에 200개 이상, 안드로이드 마켓에 50개 이상의 증강현실 앱이 있다고 분석결과를 보고하였다. 또한, Qualcomm은 자체 기술을 활용하여 새로운 애플리케이션 콘셉트와 원형(prototype)을 개발하기 위해 조지아 공대(GIT)에 증강현실게임 연구개발센터(AR gaming R&D center)를 설립하였다.

다섯째, 성인용 엔터테인먼트(Adult Entertainment): 모바일 성인 콘텐츠를 견인할 것으로 주목 받는 애플리케이션은 비디오 채팅(Video Chat). 성인용 애플리케이션 판매가

제한되고 무료 콘텐츠에 대한 접근성이 높다고 하더라도 가입자 기반 비디오 채팅 애플리케이션의 발전 가능성은 큰 것으로 예상된다.

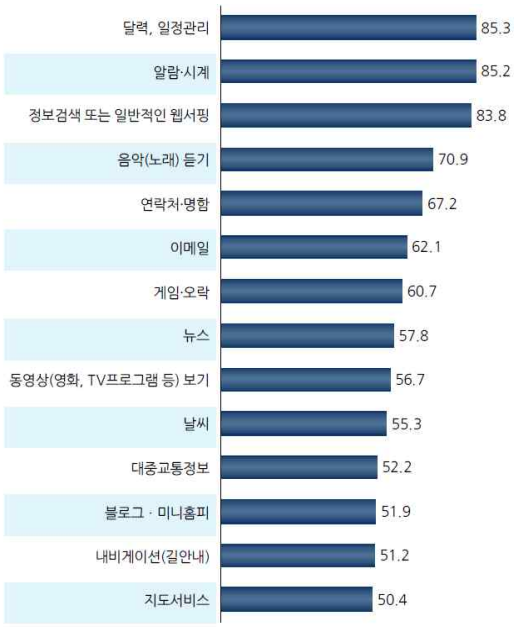
세계적으로 많은 모바일 인터넷 사용자를 확보하고 있는 미국에서는 [그림 3-18]과 같이 사진과 메시지 송수신같은 서비스의 이용률이 높고 , 국내에서는 [그림 3-19]과 같이 달력/일정관리, 알람/시계, 웹검색 부분에서 높은 이용률을 보이고 있다.

[그림 3−18] 미국 스마트폰 서비스 이용 현황



자료: Pew Research Center's internet & American Life Project, 2010

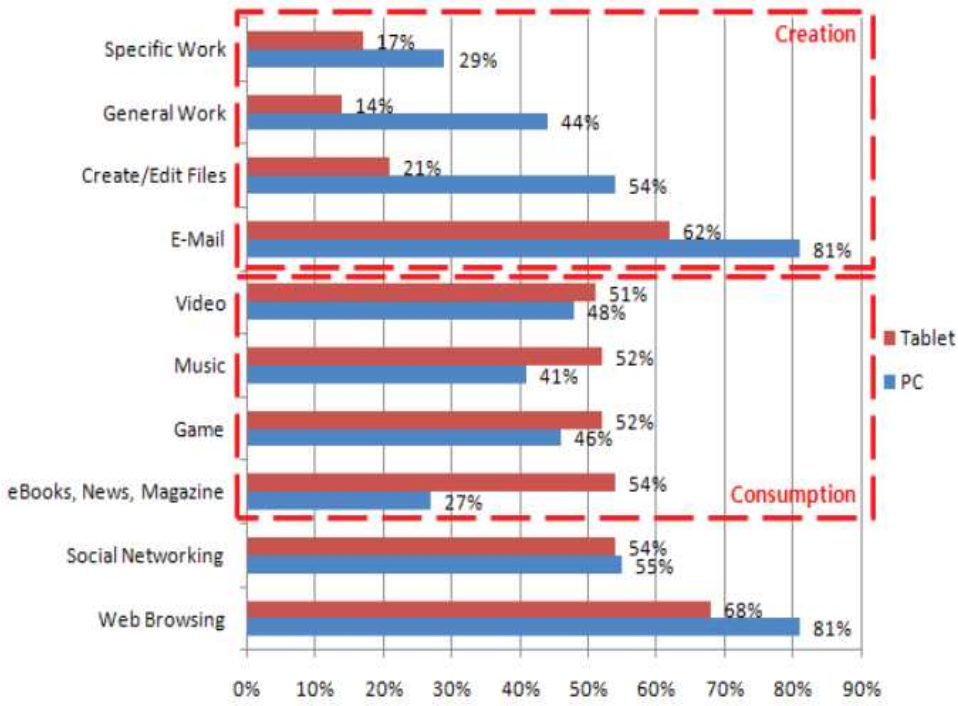
[그림 3-19] 국내 스마트폰 서비스 이용 현황



자료: 스마트폰 이용실태조사, KISA, 2010

일반 PC와 스마트패드에 대한 이용률을 비교해보면 [그림 3-20]과 같이. 스마트패드에서는 웹 검색, 이메일, 소셜 네트워킹, e북/뉴스/잡지, 게임, 음악, 비디오의 서비스를 주료 이용하며, 일반 PC에서는 웹브라우징, 이메일, 소셜네트워킹, 문서작업, 비디오, 게임등을 주로 이용한다. 이 둘을 서로 다른 양상에서 비교해보면으로 일반 PC에서는 문서작업, 이메일, 기타 작업등 주로 생산하는 일을 주로하고, 스마트패드에서는 e북/뉴스/ 잡지, 게임, 뮤직, 비디오 등 주로 생산성없는 서비스를 주로 이용하는 것으로 보인다.

[그림 3-20] 스마트패드 이용 현황



자료: Morgan Stanley Research, SAI, 2011

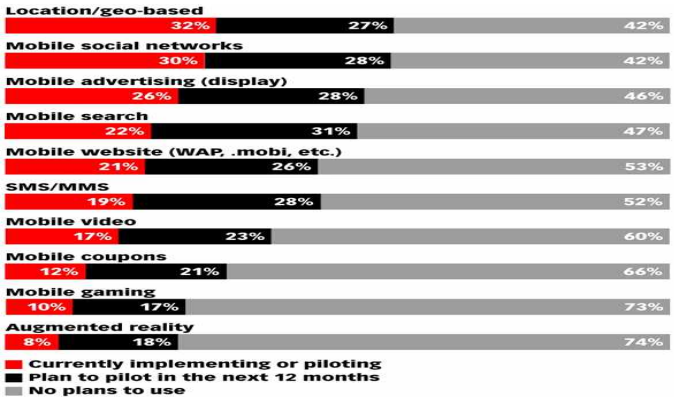
또한 사용하는 모바일 서비스별로 이용하는 시간의 비중을 살펴보면 [그림 3-21]과 같이 이메일이 38.5%로 가장 높고, 소셜네트워킹이 10.7%, 뉴스가 7.2%로 뒤를 잇는다.

[그림 3-21] 모바일 서비스별 이용시간 비중

자료: Nielsen Company, 2010.

향후에는 모바일 기기를 이용한 검색, 모바일 광고, 소셜네트워크, SMS/MMS, 위치기반 서비스의 서비스들이 이용률이 더 증가할 것으로 전망된다.

[그림 3-22] 미국 모바일 시장 전망



자료: Forrester Research, “US Interactive Marketing Online Survey", 2010

모바일인터넷 활성화, 폭발적인 스마트폰의 보급 및 확산으로 모바일인터넷과 스마트폰은 개인, 기업, 공공 부문 모두에게 생산성 및 효율성 향상의 핵심 키워드로 부각되고 있다. 앞서 살펴본 바와 같이 스마트폰을 통해 언제 어디서나 인터넷 접속이 가능한 진정한 유비쿼터스 네트워크 환경이 구축되었으며, 모바일 관련 기술의 발달로 다양한 모바일 애플리케이션을 통한 무한한서비스 창출이 가능해졌다.

이러한 기술의 진화와 인터넷 서비스 패러다임 변화에 따라 정부서비스에 있어서도 새로운 변화와 업그레이드가 필요하게 되었다. 특히 우리나라는 2010년 UN 전자정부 평가에서 1위를 차지하는 놀라운 성과를 거둔바 있다. 이러한 세계 최고 수준의 정부서비스를 지속적으로 유지하기 위해서는 모바일인터넷과 스마트폰기반의 모바일 정부서비스의 구축이 필요하다.

신규 모바일 기기의 활용 분야가 넓어짐에 따라 이전에는 없었던 여러 가지 부작용들이 발생하고 있는데 그중 하나가 모바일 환경에 대한 보안위협의 증가이다. 기존의 모바일 환경과 비교하여 보안위협이 급격히 증가한데에는 크게 두 가지 원인이 있다.

첫 번째 원인은 모바일 기기를 통한 웹서비스 접속이 가능해짐에 따라 모바일 기기로 송·수신 되는 데이터의 양이 크게 늘어나고 있다는 점이다. 특히 모바일 기기를 통한 금융결제서비스가 발달하면서 이동통신망을 통한 금융정보의 유출가능성이 높아졌

으며 스마트워크 단말기로서 사용되는 모바일 기기에서의 기업 기밀정보 유출 가능성도 높아지고 있다. 따라서 기존 PC환경에 서 발생하던 보안위협이 모바일 환경에서도 빈번히 발생되고 있다.

보안위협 증가의 두 번째 원인은 민감한 개인정보를 유출시킬 수 있는 새로운 서비스의 등장이다. 대표적인 예로 위치 기반 서비스(Location based Service, LBS)와 소셜 네트워크 서비스(Social Network Service, SNS)를 들 수 있다. 이러한 서비스들은 앞서 기술한 다양한 활용 분야에서 사용되고 있고 위치정보 등 프라이버시 관련 정보를 다루므로 개인정보 유출의 증가에 큰 영향을 미친다.

이와 같이 급격히 증가하는 모바일 환경 보안위협에 대비하기 위해서는 현재, 그리고 미래의 모바일 환경 동향에 대한 정확한 파악과 예측, 위협에 대한 정밀한 분석이 필수적이다. 또한 정부 차원에서 적극적으로 보안위협에 대응하기 위한 정보보호 대응책과 정책을 수립해야만 할 것이다.

제 2 절 신규 모바일 기기 위협 동향

1. 기술적인 측면에서의 보안위협

기술적인 측면에서의 보안위협으로는 크게 단말기기에 대한 보안위협, 네트워크 보안위협, 서비스 보안위협, 그리고 컨텐츠 보안위협으로 구분할 수 있다. 단말기기에 대한 보안위협은 다시 모바일 기기 플랫폼, 소프트웨어의 취약성 또는 악성 애플리케이션에 의해 개인정보 유출 등으로 구분이 가능하다. 또 분실로 인해 단말기의 모든 정보가 유출되는 것 또한 큰 보안 위협이다.

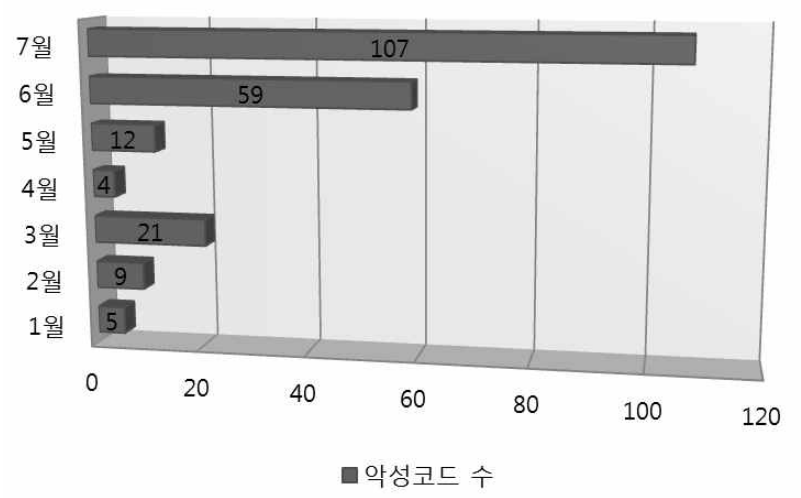
특히 최근 안드로이드를 기반으로 활동하는 악성 애플리케이션에 의한 보안위협이 많은 이슈를 야기하고 있다. 실제 중국에서 출시된 어느 애플리케이션의 경우 표면상으로는 게임 또는 성인 컨텐츠를 제공하지만, 실제로는 모바일 기기의 통화내역 및 SMS 내용을 도청하는 사례가 있었다. 2011년 3월에는 보안 애플리케이션으로 가장하여 유해 프로그램을 찾아내는 기능을 차단하여 보안을 무력화하는 애플리케이션도 등

장하였다. [그림 3-23]은 중국에서 동영상 스트리밍 플레이어로 마켓에 올라왔지만 실제로는 통화내역과 메시지 내용을 유출하는 기능을 수행하는 악성 애플리케이션이다.

[그림 3-23] 동영상 스트리밍 플레이어로 가장한 악성 애플리케이션

문제는 악성 애플리케이션에서만 발생하는 것은 아니다. 악성코드에 대한 위협 또한 존재한다. [그림 3-24]에 따르면 국내에서 2011년 상반기에만 발견된 악성코드의 수는 100여개를 넘었으며, 해외에서는 2009년 상반기 누적 건수는 524건으로 이 수는 급격하게 증가하는 추세이다.

[그림 3-24] 2011년 안드로이드 악성코드 발견 수



분실 또한 큰 보안위협이다. 모바일 기기는 휴대가 용이하다는 장점이 있지만 그만큼 분실의 위험이 존재한다. 실제로 마이크로트랜드에서 2009년 6월에 조사한 결과에 의하면 스마트폰의 분실 가능성은 노트북의 15배가 된다고 한다. 스마트폰, 스마트패드과 같은 모바일 기기가 업무용으로도 활용된다는 점을 고려할 때, 분실로 인해 기업 기밀정보의 유출 또한 가능하므로 분실로 인한 정보의 유출은 피해범위가 매우 넓을 수도 있다.

네트워크 관점에서 발생할 수 있는 위협은 무선AP로 인해 발생하는 것이 많다. 모바일 기기가 보급되면서 무선통신을 위해 무선 AP(Access Point)가 많은 장소에 설치되기 시작하였으며, 현재는 수도권 대부분 장소에서 무선인터넷을 사용할 수 있을 정도로 보급 보급되어 있다. 그러나 그만큼 무선랜(Wi-Fi)으로 초래되는 보안 위협 또한 더욱 증가하였다.

대부분의 모바일 기기에는 무선랜이 기본적으로 포함되어 있어서 3G망을 사용하지 않고도 무선 AP를 통해 인터넷을 사용할 수 있다. 하지만 검증되지 않은 무선 AP를 사용하는 사용자들은 다양한 위험에 노출될 수 있다.

가장 먼저 무선 AP를 이용하여 통신하는 구간에서 공격자는 패킷을 수집하여 멀티

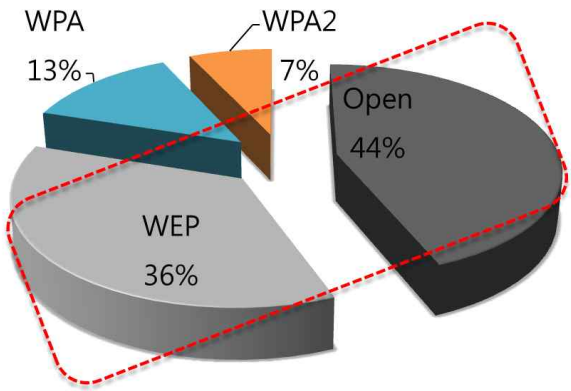
미디어 콘텐츠 유출, 패킷 위변조, 패킷의 해독을 통한 인증 및 개인 정보 유출을 시도할 수 있다. 또 다른 기기간의 통신을 중개하여 암호화된 통신내용을 복호화하고. 이 내용을 위변조하여 기기간의 통신을 방해하는 중간자공격(MITM, Man-In-The_Middle)도 가능하다. 이러한 유형 외에도 인가되지 않은 AP로 Wi-Fi 연결을 유도하여 통신내용을 수집하는 공격방법도 존재한다.

보안기능이 설정되지 않은 무선 AP를 사용하는 모바일 기기는 해킹, 개인정보 유출, 도청 등의 보안위협에 노출될 수밖에 없다. 2010년 7월 한국인터넷진흥원에서 국내 15개 시/도 29개 지역 무선 AP 42,997대를 조사한 결과, 약 44.8%가 보안설정을 하지 않은 상태로 사용되고 있는 것으로 알려졌다.

특히 조사 대상 중 가정용 사설 AP 28,312대의 경우 55.2%가 보안 설정이 미비한 것으로 나타났다. 이는 가정에서 사용되는 무선 AP에 악의적으로 접속하여 개인정보를 유출 시킬 수 있다는 것이다.

[그림 3-25]은 美 Air tight Networks사에서 전 세계 27개 공항을 대상으로 같은 조사를 한 결과를 보여주는 그래프이다. 이 결과에 따르면 공항에 설치되어있는 무선AP의 80% 이상이 보안 설정을 하지 않았거나, 보안에 취약한 WEP(Wired Equivalent Privacy) 프로토콜을 사용한 것으로 확인되었다.

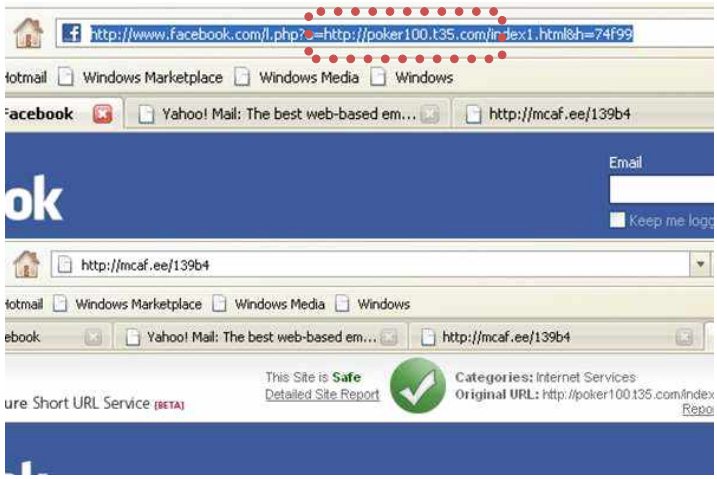
[그림 3-25] 美 Air Tight Network사,
전 세계 27개 공항 무선AP 보안 설정 조사결과



이러한 무선 네트워크에 대한 공격은 최근 확산되고 있는 모바일 뱅킹에서 심각한 피해를 초래할 수 있다. 최근 여러 금융사들이 앞다투어 모바일 뱅킹 서비스를 시작하고 있다. 이에 따라 모바일 뱅킹을 목표로 하는 악성코드 또한 속속 등장하고 있다. 악성코드는 모바일 뱅킹 서비스 동안 사용자가 입력하는 정보들을 수집하여 공격자에게 전송하는 역할을 한다. 이를 통해 공격자는 사용자의 금융정보를 획득할 수 있다.

이 외에도 상당수의 애플리케이션들이 이용자의 동의 없이 이용자의 위치정보, 단말기 정보, 연락처 정보 등을 수집하고, 또는 동의가 있더라도 불필요하게 많은 정보들을 요구하는 문제점이 존재한다. 한 예로, 최근 애플은 사용자의 동의 없이 아이폰을 사용하는 사용자의 위치 정보를 수집을 한 사례가 있다.

[그림 3-26] 단문 URL을 이용한 피싱

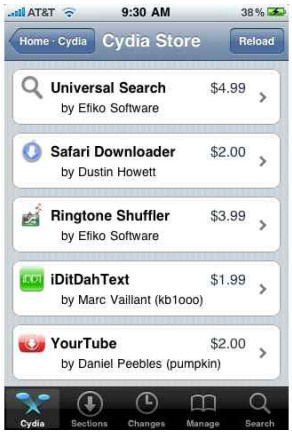


악성 애플리케이션 외에도 악의적인 사설 모바일 앱스토어, 단문 URL(인터넷 상의 URL을 모바일에서 이용하기 쉽도록 짧게 줄인 인터넷 주소)를 이용한 피싱 · 사기 위협이 발생하고 있다. [그림 3-26]는 단문 URL을 이용한 피싱의 예이다. 상단의 URL은 facebook을 통하여 도박사이트로 리다이렉트되는 주소이며, 그 주소를 단문 URL로 변환하면 아래 와 같은 URL로 변환이 된다. 공격자는 아래의 단문 URL로 접속을 하도록 유도하여 도박사이트를 접속하게 한다. 이 예제는 단순히 도박사이트지만 악성코드에 감염시키는 사이트로 접속하게 한다면 피해가 커질 수 있다.

컨텐츠에 대한 보안위협도 존재한다. 국내의 경우 Melon, Dosirak과 같은 음악 컨텐츠 서비스와 Tving과 같은 동영상 스트리밍 서비스들이 있고, 국외에서도 비슷한 여러 서비스들이 있다. 이러한 서비스 업체들은 디지털저작권관리기술(Digital Right Management)을 이용하여 컨텐츠를 암호화 하는데, 여러 요소들에 의해 파일이 해독, 해킹당하는 사례가 발생하고 있다.

2009년 12월에 DRM이 적용된 아마존의 유료 컨텐츠가 비인가된 기기에서도 구동되도록 해킹된 사례가 있고, 더 과거에는 악성코드에 의해 DRM이 해지된 소프트웨어가 유포된 사례도 있다.

[그림 3-27] iPhone 사설 앱스토어 Cydia



모바일 기반의 불법 컨텐츠는 계속적으로 다양화되고 지능화되고 있다. 아이폰에서는 탈옥(Jail-breaking)을 통해 사설 앱스토어[그림 3-27]을 설치하여 불법복제 애플리케이션을 사용하거나, 안드로이드에서는 루팅(rooting)을 한 후 외장 메모리에 불법 앱을 복사하여 이용함으로써 저작권 문제가 계속적으로 야기되고 있다.

2. 기술외적 측면에서의 보안위협

기술외적 측면에서의 보안위협으로는 앱 유통환경 측면에서의 보안위협, 법제도적 보안위협, 그리고 국내외 기업 환경에서는 보안 위협으로 나눌 수 있다.

앱 유통환경에서의 보안위협으로는 마켓플레이스의 정책을 들 수 있다. 애플의 앱스토어에 애플리케이션을 등록하는 경우에는 약 2주간의 심사기간을 거쳐 승인 또는 거절이 결정된다. 이 심사기간에는 애플리케이션의 악의적인 행위, 불필요한 개인정보 수집에 대한 행위를 검사하는 과정도 포함되어있다. 기간은 다르지만 이러한 심사기간은 애플 외에 마이크로소프트의 마켓플레이스, 삼성의 앱스에도 존재한다.

하지만 현재 세계 1위의 점유율을 자랑하고 있는 구글의 안드로이드 마켓은 애플리케이션의 별다른 심사기간이 없다. 단, 구글에서 원격 삭제 기능을 갖고 있다. 원격 삭

제란 안드로이드가 정식으로 발매되었을 때부터 내장되어있던 기능으로, 마켓에서 판매되는 애플리케이션 중 문제가 되는 애플리케이션을 중앙에서 원격으로 삭제하는 기능이다.

하지만 이러한 환경은 사후약방문에 그칠 수 있다는 점에서 완전한 대책이 될 수 없다. 원격 삭제가 실행되었다는 것은 이미 그 애플리케이션에 의해 피해본 사용자가 얼마든지 충분히 있다는 의미이기 때문이다. 그리고 악성 애플리케이션이 점점 복잡하고 지능적으로 변형되어가는 추세기 때문에, 악성 애플리케이션의 조기 탐지가 어렵고, 탐지 이후 원격 삭제를 수행했다 하더라도 원격 삭제 기능을 우회하는 악성 애플리케이션의 존재를 부정할 수 없다는 문제가 있다.

[그림 3-28] 블랙마켓에서 다운로드 받은
애플리케이션을 백신으로 검사한 결과

또한 안드로이드 역시, 아이폰의 Cydia와 같은 블랙마켓이 존재한다. [그림 3-28]은 안드로이드의 블랙마켓에서 구입한 애플리케이션을 백신으로 검사한 결과를 나타낸다. 블랙마켓의 특성상 불법적인 애플리케이션을 제작하거나 악성 애플리케이션을 등록하기 용이하기 때문에, 비공식적인 마켓플레이스를 통한 애플리케이션 유통과정도 심각한 위협을 초래할 수 있다.

애플리케이션 유통과정에서의 보안위협 외에 기업 환경에서도 보안 위협은 나타날

수 있다. 현재 많은 기업들이 업무의 효율성을 높이기 위하여 모바일 기기를 이용하여 업무를 처리하고 있다. 모바일 기기에서 메일 및 문서를 비롯한 회사의 다양한 정보를 관리하기 시작하면서 모바일 기기는 단순히 개인정보가 아닌 회사 기밀정보도 새어나갈 수 있는 weak point가 되었다. 실제 2010년에 시만텍이 휴일 스마트폰 사용 실태 조사를 한 결과 응답자의 62%가 스마트폰을 이용하여 회사의 기밀 데이터를 이용하기도 한다고 대답하였다.

따라서 현재 기업들은 모바일 기기에 보안기능을 추가하고 있으며, 보안업체들은 모바일 보안 상품을 출시하고 있다.

〈표 3-9〉 주요 기업 모바일 보안 현황 및 보안업체의 모바일 보안 상품

기업	삼성전자	스마트폰 카메라 사용 불가
	포스코	스마트폰 내 앱 실행 통제 및 모니터링 가능
	현대자동차	외부 와이파이(Wi-Fi) 접속 차단
보안업체	에스원	비인가 AP 탐지, 도청기, 도촬 카메라 탐지 상품 출시
	ADT캡스	올해 안으로 네트워크 보안 상품 출시 예정

제 3 절 정보보호 대응책·정책수립 현황

1. 국내 정보보호 정책 수립 현황

최근 모바일 서비스의 신뢰성 보장 및 개인정보보호에 대한 사회적 요구가 증가함에 따라 보안의 중요성에 대한 공감대가 확산되고 있다. 모바일 악성코드 및 새로운 공격 위협의 차단 등을 통해 신규 서비스의 가용성 보장이 필요하고 위치정보·인맥정보·금융정보 등 다양한 정보의 활용이 증가함에 따라 개인정보에 대한 관리·보호의 요구가 증가하고 있다. 이를 위해 방송통신위원회는 2010년 12월 '스마트 모바일 시큐리티 종합계획'을 수립하여 2015년까지 안전한 모바일 인터넷 환경 조성을 위해 노력하고 있다. [그림 3-29]는 종합계획의 주요 내용이다.

[그림 3-29] '스마트 모바일 시큐리티 종합계획' 주요 내용

가. 무선랜 정보보호 안내서

무선 랜 정보보호 안내서는 무선 랜에 관한 설명과 무선 서비스 제공시 주요보안 취약성과 대응기술에 대해 정리하고 이에 대한 보안 방법을 제공하고 있다.

무선 랜 정보보호 안내서에서 제시하는 무선 랜 취약성은 크게 '물리적 보안 취약성', '기술적 보안 취약성', '관리적 보안 취약성' 3가지로 분류하고 있다.

1) 무선 서비스 주요 보안 취약성

❍ 물리적 보안 취약성

- 무선 랜을 구성하는데 있어 중요한 역할을 하는 무선 AP의 경우, 원활한 서비스의 제공을 위해 외부에 노출된 형태로 위치하게 되는 것이 일반적임. 이러한 무선 AP는 장비의 외부 노출로 인해 비인가자에 의한 장비의 파손 및 장비 초기화와 같은 문제가 발생할 수 있다. <표 3-9>은 무선 장비의 물리적 보안 취약점의 대표적 유형들이다.

〈표 3－10〉 무선 장비의 물리적 보안 취약점 유형

유 형	내 용
도난 및 파손	외부 노출된 무선 AP의 도난 및 파손으로 인해 장애
구성설정 초기화	무선 AP의 초기화 버튼을 통한 장비의 초기화로 인한 장애
전원 차단	무선 AP의 전원 케이블의 분리로 인한 장애
LAN 차단	무선 AP에 연결된 네트워크 케이블의 절체로 인한 장애

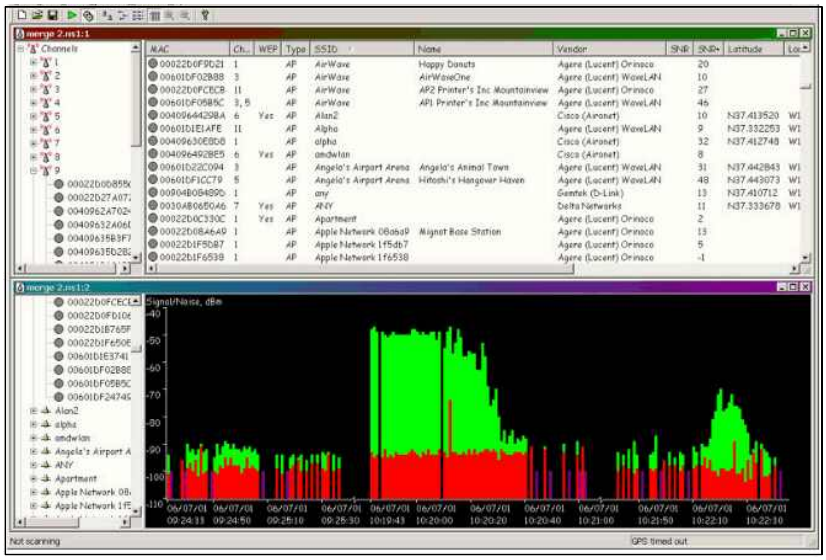
- 무선 AP로 연결되는 유선 네트워크 케이블의 경우도 무선 AP에서 발생할 수 있는 물리적 보안 취약점이 발생할 수 있으므로 기본적으로 무선 AP 및 유선 네트워크 케이블은 비인가자의 접근이 불가능한 위치에 설치가 되어야 하며, 부득이한 경우, 별도의 시설 설치를 통해 접근이 불가능하도록 철저히 보호되어야 한다.
- 무선 단말기는 무선 랜 서비스를 구성하는 주요 요소 중의 하나로서, 무선 랜 사용 업체의 필요조건에 따라 여러 형태의 무선 단말기가 존재할 수 있다. 무선 단말기의 유형 중 이동성을 가진 노트북, 스마트폰, PDA의 경우, 항상 분실의 위험성이 존재하게 되는데 이 경우, 저장 데이터의 유출은 물론 무선 랜의 내부 보안 설정이 함께 유출될 가능성이 존재한다. 따라서 무선 단말기의 경우 업무시간 외에는 반드시 정해진 장소에 보관하도록 하고, 보관 시에는 단말기의 전원을 종료하여 비인가자의 오용을 사전에 차단하도록 한다. 또한 무선 단말기의 최초 사용 시 로그인 절차 등을 적용하여 비인가자의 접근을 차단하도록 설정되어야 한다.

❍ 기술적 보안 취약성

- 무선 랜은 공기를 전송매체로 사용하는 서비스의 특성 상 불특정 다수의 신호 수신이 가능함으로 인한 도청 및 무선 장비에 대한 공격이 가능하다는 취약점이 존재한다. 또한 유선 랜에서 존재하는 공격 기법의 적용이 가능하다.
  - 도청: 무선 랜의 가장 근본적인 문제점이라 할 수 있는 도청은, 무선 AP에서

발송되는 전파의 강도와 지형에 따라 서비스가 필요한 범위 이상으로 전달될 수 있으며, 이 경우 외부의 다른 무선 클라이언트에서 무선 AP의 존재 여부 파악이 가능함과 동시에 전송되는 무선 데이터의 수신을 통한 도청이 가능하게 된다. 이 경우, 무선 데이터가 암호화 되어 있지 않은 경우 모든 전송 데이터를 도청할 수 있게 되어 문제가 발생하게 된다. 무선 전송데이터의 도청에 사용되는 별도의 S/W는 인터넷을 통해 손쉽게 구할 수 있는데, 이를 이용해 탐지되는 무선 랜의 기본적인 구성 및 설정을 파악할 수 있다. [그림 3-30]은 대표적인 무선 랜 분선 S/W인 Netstumbler의 화면으로 무선 랜의 구성 요소인 SSID, 암호화 방식, 속도 및 신호 감도 등의 정보를 파악할 수 있다.

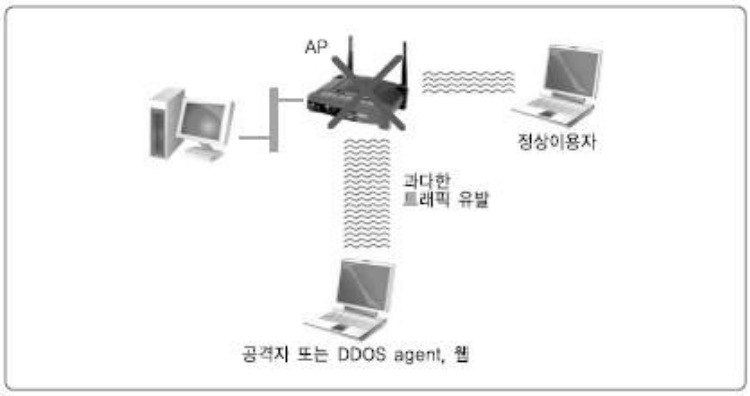
[그림 3－30] Netstumbler 실행 화면



- 서비스 거부: 서비스 거부란, 무선 서비스를 제공하는 무선 AP 장비에 대량의 무선 패킷을 전송하는 서비스 거부 공격을 통해 무선 랜을 무력화하는 것을 뜻한다. 또한, 무선 랜이 사용하는 주파수 대역에 대해 강한 방해전파를 전송하는 것도 통신에 영향을 주게 된다.

- 무선 단말기는 무선 클라이언트와의 통신을 위해 설정된 SSID를 포함한 "Probe Request" 메시지를 브로드케스트로 전송하게 된다. 이 신호를 수신한 무선 AP는 해당 클라이언트가 접속하는 것을 허용한다면 “Probe Response" 메시지를 회신하게 된다. 이러한 과정에서 다량의 request 메시지를 무선 AP로 전송하는 경우, response 메시지 회신 동작의 반복으로 인해 다른 무선 단말기의 접속이 불가능하게 된다([그림 3-31] 참조).

[그림 3-31]Probe Request 메시지 브로드케스팅을 통한 서비스 거부 공격 과정



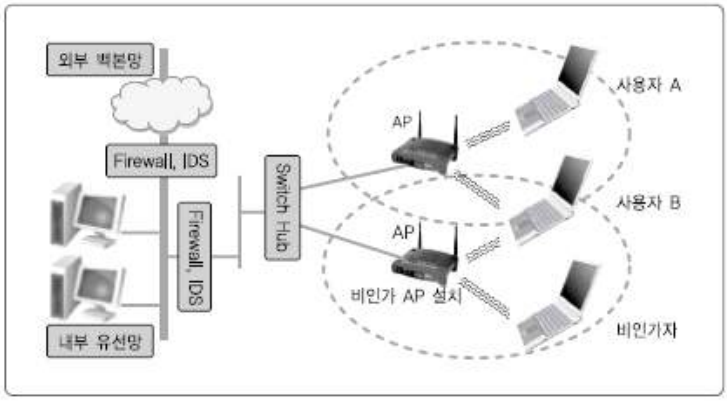
- 이러한 무선 AP에 대한 서비스 거부 공격은 실제 내부 네트워크로의 침입으로까지는 발전되지 않지만, 백화점과 같이 실시간으로 무선 랜을 이용해 주요 업무가 이루어지고 있는 경우, 공격으로 인해 발생되는 무선 랜 서비스의 중지는 치명적인 결과를 가져올 수 있게 된다.
- 이와 같이 무선 랜 자체를 이용해 회사의 중요 업무를 수행하는 경우에는, 서비스 중지 시 대체할 수 있는 별도의 유선 랜을 준비하여 만일의 경우에 대비하는 것이 반드시 필요하다.

- 불법 AP: 불법 AP는, 공격자가 불법적으로 무선 AP를 설치하여 무선 랜 사용자들의 전송 데이터를 수집하는 것으로([그림 3-32] 참조), 불법 AP의 설치

유무를 탐지하는 것은 어렵지 않으나 무선의 특성 상 정확한 불법 AP의 위치를 파악하는 것은 쉽지 않은 일이다. 일부 무선 보안 솔루션에서는 다수의 무선 AP를 이용해 불법 AP의 무선 강도 등을 참고로 대략적인 불법 AP의 위치 정보를 제공하지만, 실제 정확한 위치를 파악하고 제거하기는 어려운 상황이다.

- 불법 AP의 경우, 별도 전원 연결이 필요하므로 무선 랜이 적용된 사무 공간의 철저한 관리를 통해 불법 AP가 설치되지 않도록 관리하는 것이 가장 중요한 부분이라고 할 수 있다. 또한 불법 AP의 설치여부에 대해 보안 정책 내 별도의 항목을 추가하여 주기적으로 무선 랜 서비스 지역에 대한 점검을 진행하여 불법 AP가 설치될 수 있는 위험성을 줄여야 한다.

[그림 3-32] 불법 AP 구성도



- 무선 암호화 방식: 무선 데이터 암호화 방식으로 많이 사용되고 있는 WEP(Wired Equivalency Protocol)은 전송되는 MAC 프레임들을 40비트의 WEP 공유 비밀 키와 임의로 선택되는 24비트의 Initialization Vector(IV)로 조합된 총 64비트의 키를 이용한 RC4 스트림 암호화 방식으로 보호된다. 하지만 WEP 암호화 방식은 <표 3-11>와 같은 문제점을 갖는다.

〈표 3－11〉 WEP 암호화 방식의 문제점

번호	문제점
1	짧은 길이의 초기벡터(IV)값 사용으로 인한 재사용 가능성이 높음
2	불완전한 RC4 알고리즘 사용으로 암호 키 노출 가능
3	짧은 길이의 암호키 사용으로 인한 무작위 대입 공격 가능
4	암호 키 노출로 인한 무선 전송데이터의 노출 위험

- WPA/WPA2의 경우에도 초기 무선 랜에 접속하는 인증 단계에 사용되는 Pre-shared 키 값(PSK)을 무선 전송 패킷의 수집을 통해 유추해낼 수 있다는 취약점이 존재하는 것으로 알려져 있으나, WEP와는 달리 무선 데이터 전송 시 고정된 키 값을 이용해 무선 전송데이터를 암호화하지 않으므로 단순히 무선 전송 데이터 패킷의 수집을 통해서는 무선 전송데이터의 암호화 키 값을 유추해낼 수는 없다.

❍ 관리적 보안 취약성

- 무선랜 장비 관리 미흡: 무선 랜을 운영하는 대부분의 기관에서는 사용하는 AP의 개수 정도만 파악하고 있어, 장비의 파손 및 도난 시 무선 랜 서비스를 제공하지 못하고 있어도 이를 파악하지 못하는 경우가 발생할 수 있다. 이를 방지하기 위해 기관에서 사용하는 무선 랜 장비인 AP와 무선랜 카드 등에 대한 장비 운영 현황과 사용자 현황 등을 파악하여야 하며, 무선 랜 장비에서 제공하는 기본 값 또는 초기 값을 사용하고 있는 곳이 많아 공격자의 표적이 되고 있는 경우가 많으므로 해당 기기의 초기 비밀번호 변경이 필요하다.

- 전파관리 미흡: 무선 랜을 설치하여 운영하는 기관의 대부분은 유선 네트워크 관리자가 무선 랜도 관리하고 있는 경우가 많다. 이러한 경우에, 유선 네트워크 관리자가 무선 랜에서 사용하는 전파 특성을 파악하지 못하는 경우가 많다. 즉, 전파 자원의 관리 미흡으로 인해 무선 랜 환경에 취약성이 발생한다.

이러한 취약성에는 AP의 전파 출력 조정을 하지 않아 기관 외부로 무선 랜 전파가 유출되는 경우와 무선 랜 채널 설정 미흡으로 인해 AP간의 간섭이 발생하는 경우가 있다.

나. 클라우드 서비스 정보보호 안내서

클라우드 서비스 정보보호 안내서는 기업의 클라우드 서비스 제공 및 개인 사용자가 클라우드 서비스 이용시 준수해야할 보안 가이드라인을 정의하고 있다.

클라우드 서비스는 자원활용의 효율성 증대 및 사용자별 자원 할당 간편화를 위하여 하이퍼바이저를 사용, 모든 자원을 소프트웨어 기반으로 가상화하여 제공하는 특성을 가진다. 따라서 모든 연산 및 데이터리가 클라우드 서버에서 이루어지므로 기본적으로 사용자가 소유한 정보의 관리를 서비스 제공자에게 위탁한다. 또한 사용자별로 할당된 자원은 논리적으로는 독립적이지만 물리적으로는 동일한 자원을 공유한다.

이러한 클라우드 서비스의 특징으로 인해 발생가능한 보안취약점에 대해 클라우드 서비스 정보보호 안내서에서는 <표 3-12>와 같이 정리하였다.

〈표 3－12〉 클라우드 서비스 정보보호 위협

위협	위협내용
가상화 취약점 상속	악성코드 감염 및 확산 위협 호스트OS, 게스트OS 간 악성코드 감염 하이퍼바이저 감염시 게스트 OS로 확산
정보위탁 및 사용단말에 따른 정보유출	내부자에 의한 정보유출 관리자의 권한 남용으로 이용자 정보 열람 이용자 몰래 게스트OS의 자료 삭제/수정 인증하지 않은 이용자의 정보 접근 단말기 분실, 보안성이 취약한 단말기에 의한 정보 유출
자원 공유 및 집중화에 따른 서비스 장애	시스템 장애 시 모든 고객의 서비스 중단 서비스 장애 원인의 빠른 파악이 어려움 이용자에 의한 복구 및 패치 불가능 중앙시스템 위치 노출 시 DDoS등 공격 대상이 되기 쉬움
분산처리에 따른 보안적용의 어려움	자원공유와 가상머신 동적 재배치로 인증/접근제어 복잡도 상승 분산 컴퓨팅 시스템에 일괄적인 인증/접근제어 적용이 어려움
법규 및 규제의 문제	정보 유출 및 손실 시 책임 소재 불분명 해외 서버 사용시 국내법 적용이 불가 자원 공유에 따라 감사 증적이 어려움 클라우드 점검을 위한 보안 점검 및 규제 항목 부재

클라우드 서비스 정보보호 안내서에서는 클라우드 서비스의 이용주체를 클라우드 서비스 제공자와 클라우드 서비스 이용자, 클라우드 서비스를 활용하여 고객에게 서비스를 제공하는 사업자로 정의하였다. 서비스 이용사업자는 클라우드 서비스를 활용하여 고객에게 IT서비스를 제공하기 때문에 서비스 제공자의 정보보호 고려사항을 적용하는 것을 권장한다.

1) 관리적 측면의 정보보호

관리적 측면의 정보보호는 정보보호정책 및 약관을 수립하고 정보보호조직 구성·운영 및 인력보안을 실시한다. 또한 자산분류 및 통제와 비상대응체계를 구축하여야한다. 클라우드 서비스의 특성상 서비스의 연속성 확보 역시 관리적 측면의 정보보호에 포함된다. 마지막으로 관련 법률 및 제도를 준수해야한다.

〈표 3－13〉 관리적 측면의 정보보호

구분	보호조치 분야	주요 내용
관리적 대책	정보보호조직, 인력보안	내・외부 업무수행 관련 인력의 역할 및 권리, 보안책임 등
	정보자산 분류 및 통제	소유 및 관리 책임을 갖는 자산 목록, 정의 및 통제 방안 등
	비상대응체계 및 사고관리	비상대응체계 구성원 및 운영체계 정의, 서비스 복구 계획 등
	서비스 가용성 및 연속성	신규 보안대책 및 기술 도입에 따른 절차, 규정 등
	법제도적 준거성 확보	서비스 제공 근거법령 및 규정

2) 기술적 측면의 정보보호

클라우드 서비스 정보보호 안내서에서는 기술적 측면의 정보보호 방법은 네트워크 보안과 클라우드 시스템에 사용되는 시스템 및 가상화 보안 클라우드 시스템에 대한 물리적 보안, 데이터 저장 및 관리, 마지막으로 사용자 인증 및 접근관리에 대한 기술적 정보보호가 요구된다. 네트워크 보안은 암호화 통신, 네트워크 서비스거부공격 등에 대한 대응방안을 마련하는 것을 골자로 하며 시스템 및 가상화 보안은 악성코드에 의한 피해를 중심으로 서술하고 있다.

물리적 보안은 클라우드 서비스에 이용되는 데이터센터 구축과 데이터센터의 정보보호 대책을 정의하고 있다. 재해 대비 및 입・출입 통제 그리고 내부설비보호등을 설명한다. 클라우드 서비스에서 데이터 저장 및 관리는 저장될 데이터의 기밀수준에 따라 암호화 적용등에 관한 방법을 설명한다. 사용자 인증 및 접근제어는 서비스 이용자의 제한된 영역에 대한 접근 시도와 같은 부적잘한 행위에 대한 보안관제의 매커니즘을 설명한다.

〈표 3－14〉 기술적 측면의 정보보호

구분	보호조치 분야	주요 내용
기술적 대책	네트워크보안	접속・이용 단말의 제한등
	시스템 및 가상화 보안	사용자 세션 관리 방안등
	물리적 보안	데이터센터 및 처리서버의 지리적 위치, 입・출입 통제 방안 등
	데이터 저장・관리	개인정보취급방침, 데이터 암호화 적용절차 및 방법 등
	사용자 인증 및 접근관리	사용자 계정 및 접근 관리 정책, 특정 정보 및 상황을 위한 사용자 권한관리 등

다. 와이브로 보안기술 안내서

와이브로 보안기술 안내서는 와이브로 표준에 명시된 보안기술을 분석하고, 상용서비스에서 발생할 수 있는 보안위협에 대처하기 위한 대응방안을 기술하여 안전한 와이브로 네트워크 환경 구축 및 운영에 필요한 정보를 제공한다.

구체적으로 안내서는 와이브로의 개념 및 서비스의 특징을 다루며 망 구성 및 주요 기술을 분석하고 와이브로 표준에서 제시하고 있는 보안기술을 분석한다. 그리고 분석 내용을 바탕으로 와이브로와 유사한 환경으로 구성되는 기존 무선랜 환경과의 비교를 통하여 동일하게 발생할 수 있는 보안위협을 도출한다. 또한 와이브로 환경에서 발생할 것으로 예상되는 새로운 보안 위협을 예측하며 이동성 제공에 따른 보안위협에 대해서도 고려한다. 그리고 다양하게 도출된 보안위협에 대한 적절한 대응방안을 제시한다.

본 안내서는 다양한 보안위협을 도출했지만 최근 표준 동향을 반영하지 않고, 구체적인 와이브로 서비스 동향이 수록되지 않아 보안위협 및 대응방안의 실질적 적용 범위를 파악하기 힘들다. 그리고 실제 운용환경에서 발생했던 보안위협에 대해서 예측 가능한 보안위협만 도출 되어 있다. 이에 따른 대응방안 또한 추상적이어서 구체적인 대응방안 제시가 부분적으로 미흡한 단점을 갖고 있다.

라. 스마트폰 백신 이용 안내서

본 안내서는 스마트폰 악성코드로 인해 발생하였던 피해사례 및 악성코드 대응을 위한 주의사항을 설명하고, 국내외로 구분하여 출시된 스마트폰 전용 백신 현황 및 이용방법에 대해 설명한다.

구체적으로 스마트폰 악성코드에 의한 피해사례와 대응을 위한 주의사항을 정리하며, 국내와 국외로 구분하여 스마트폰 백신 출시현황과 통신업체별 및 백신 개발업체별 이용방법을 설명한다. 추가적으로 스마트폰 이용자의 10대 안전수칙, 스마트폰 단말별 이용 가능한 백신 현황을 정리하여 사용자도 본 안내서를 보고 쉽게 백신을 설치 및 이용할 수 있도록 설명한다.

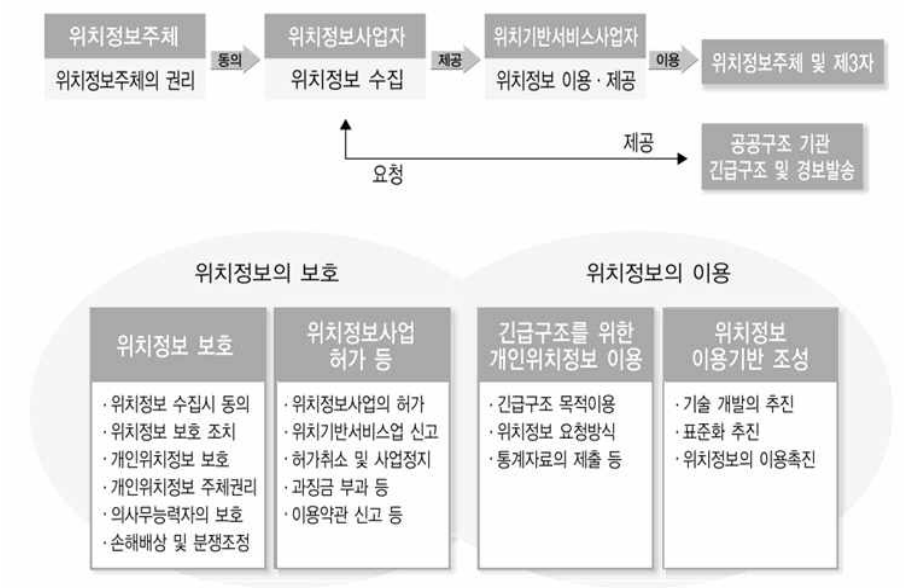
하지만 안내서에서는 기업이 만든 백신만을 소개하고 있지만 개인이 만든 백신이나 보안 프로그램과 같은 것은 소개를 하지 않는다.

덧붙여 현재 안드로이드 마켓, 통신사별 마켓(T-Store, OZ-store, Olleh) 및 애플의 앱스토어에는 보안과 관련한 카테고리가 없다. 따라서 스마트 기기 보안 프로그램의 보급을 확산하기 위해 온라인에서 보안 카테고리를 추가하는 방안을 고려해 볼 수 있다.

마. 위치정보의 보호 및 이용등에 관한 법률 해설서

위치정보는 향후 유비쿼터스 시대의 핵심 서비스 분야가 될 홈네트워크, 텔레매틱스 등 다양한 분야에서 중요한 정보 자원으로 활용될 것으로 예상된다. 그러나 위치정보의 무분별한 사용으로 인한 개인 사생활 침해의 위험이 해결되지 않는다면 위치기반서비스 산업의 활성화는 기대하기 어려울 것이다. 따라서 이러한 위치정보의 역기능을 적절히 차단하면서 위치정보 관련 서비스가 보다 광범위하게 보급되기 위해서는 프라이버시 침해가능성에 대한 우려를 완화할 수 있는 법적·제도적 장치가 필요하며 [그림 3-33]과 같은 내용으로 국내에서도 마련되었다.

[그림 3-33] 국내 위치정보 관련 법률 구성체계



〈표 3－15〉 국내 위치정보관련 법률 주요 내용

관련 규정	내용
위치정보 사업의 허가제 (법 제5조) 위치기반 서비스 사업의 신고제(법 제9조)	위치정보를 수집하여 위치기반 서비스 사업자에게 제공하는 위치정보 사업을 하고자 하는 자는 방송통신위원회의 허가를 받도록 함
위치정보 수집등의 금지 및 처벌 규정(법 제 15조 및 40조)	누구든지 개인 또는 이동성이 있는 물건의 소유자 동의 없이 개인 또는 물건의 위치정보를 수집, 이용 또는 재공학 할 수 없도록 함. 위반 시 3년 이하, 또는 3 천만원 이하의 벌금을 부과함
개인위치정보의 제 3자제공시 통보 의무 규정(법 제 19조 3항)	개인 사생활 보호를 위해 위치기반 서비스 제공자는 제 3자에게 개인위치정보를 제공할 때에는 개인위치정보주체에게 제공사실을 매회 즉시 통보하도록 함
개인정보 파기의무 규정(법 제 23조)	위치정보 사업자 및 위치기반 서비스 사업자가 개인위치정보 수집, 이용 목적을 달성할 때는 즉시 개인 위치정보를 파기하도록 하며 오, 남용을 막게 함
의사무능력자 보호 (법 제26호)	8세 이하의 아동, 금치산자, 중증 정신장애아 등에 대해서는 법정대리인, 후견인 등이 개인위치정보수집에 동의하도록 함
긴급 구조에 관한 규정(법 제 29조)	긴급 구조에 관한 요청이 있을 경우 위치정보사업자에게 개인위치정보의 제공을 요청하여 긴급구조가 원활히 이루어질 수 있게 함

2. 국외 정보보호 대응책·정책 수립 현황

가. 미국

1) 배경

2010년 5월 미국은 새로운 국가안보전략(National Security Strategy)을 발표했다. 여기서 미국은 사이버공간에 대한 위협을 국가안보의 주요 위협으로 인식하고 적대세력이 사이버공간을 활용하는 것에 대비한 전략을 제시하였다.

2) 주요 내용

가) 국가안보로서의 사이버 안전 인식

사이버 위협은 국가안보 · 공공안전 · 경제부문의 새로운 도전이다. IT는 미국의 군사 우위를 달성하는데 기여했지만 이를 통한 정부망에 대한 침입시도가 증가하고 있다. 또한, 일상생활과 공공안전이 전기와 전력에 의존하고 있는 상황에서 사이버 취약정이 대규모의 붕괴나 사회혼란을 가져올 수 있다. 그리고, 인터넷과 전자상거래로 경제적 경쟁력을 갖추었지만 사이버범죄로 인해 수백만 달러의 비용을 기업과 소비자가 부담하게 되었다. 이러한 위협을 유발하는 주체는 개인해커로부터 범죄조직, 테러조직, 국가까지 다양하다. 위협세력으로부터 안보 · 번영 · 프라이버시를 보호하기 위해 안전 · 신뢰 · 복구가 보장되는 네트워크가 필요하다. 디지털 인프라는 국가의 전략적 자신이며 안보 우선순위를 갖게 된다. 이는 미국이 국가안보의 주요부문으로 사이버 공간에서의 안전 확보를 강조한다는 점에서 의미가 있다.

나) 사이버안전 정책

첫째, 사이버안보 관련 인력과 기술 부문에 대한 투자이다. 국가 및 산업의 주요 시스템과 네트워크를 보다 확실히 방어하고 유사시 복원력을 향상하기 위해서 더 안전한 기술을 설계하도록 하고 있으며 혁신을 위한 최첨단 연구개발에 대한 투자를 지속할 것이다. 이에 따라 국가위원회로부터 학교 교실에 이르기까지 사이버안보에 대한 인식과 교양을 위한 국가차원의 복합적인 운동을 시작한다.

둘째, 공공·민간·학계 등 관련 부문 간 협력과 국제협력 강화이다. 정부·민간·개인은 독자적으로 이러한 도전에 대응할 수 없다. 따라서, 법률·데이터 보호·사고 대응 측면에서 국내 및 국제 협력을 강화하고 국가적 재난발생에 대비하여 대응계획을 마련하고 필요한 자원을 준비한다.

나. 중국

1) 개요

2010년 7월 중국 인민일보 자매지인 환구시보를 비롯한 외신들은 중국 인민해방군 기관지 해방군보를 인용하여 중국 인민해방군은 정보전쟁 시대를 맞아 디지털 안보역량을 강화하기 위해 사이버사령부를 창설하였다고 보도하였다. 사이버사령부 창설은

중앙군사위원회 주석을 겸하고 있는 후진타오 국가주석의 지시에 따른 것으로 알려지고 있다.

2) 주요 내용

가) 사이버사령부 창설 내용

중국 인민해방군 사이버사령부는 인민해방군 총참모부 직속으로 창설되었으며 전군의 사이버와 관련된 전략정보 기구를 통할하게 된다. 사이버사령부는 유사시에 대비해 사이버 공격 및 방어 체제 구축을 주요 목표로 한다. 도한, 전군에 전략정보를 지원하고 군의 정보화 및 현대화를 추진하는 것도 주 임무이다. 해방군보에 따르면 인민해방군 최고 지휘부인 중앙군사위원회는 사이버사령부가 군 전략 수립에서 핵심부대가 될 것을 지시했다고 전해진다.

중국의 사이버사령부는 미국의 사이버사령부 창설이 일정부분 영향을 끼쳤을 것으로 보인다. 2009년 6월 환구시보는 4,000여명의 네티즌을 대상으로 설문조사한 결과 전체 응답자의 94%가 '중국도 사이버사령부를 창설해야 한다' 고 응답했고 반대하는 의견은 6%에 불과했다고 보도한 바 있다. 외신 보도에 의하면 군사전문가들은 중국 사이버사령부가 창설됨에 따라 향후 중국의 사이버 분야 군사력이 대폭 강화될 것으로 전망하였다.

다. 영국

1) 개요

2010년 10월 영국 정부는 국가안보전략과 전략방어안보 보고서를 발표하면서 향후 새로운 시대는 불확실성의 시대이며 이러한 시대에는 국가안보에 대한 인식을 획기적으로 전환하고 새로운 위협에 대비하여야 한다고 지적했다. 그리고, 이러한 관점에서 영국에 대한 안보 위협과 대응방안을 제시하였다.

이에 따르면 현재부터 향후 5년간의 영구에 대한 안보위협은 위험성의 정도에 따라 크게 세가지로 나뉜다. 이 중 중대한 위협군에 해당하는 것으로 테러리즘, 사이버 공격, 자연 재해, 국제적 군사위기 등이 손꼽힌다. 이는 영국 정부가 사이버공격의 위험

성을 국가 안보 차원의 위협으로 인식한 것으로 볼 수 있다. 영국 정보가 국가안보전략과 전략방어안보 보고서에서 밝힌 위협 양상과 대응방안은 다음과 같다.

2) 주요 내용

가) 사이버공격의 위험성과 국가 안보

테러리즘과 마찬가지로 사이버공격은 미래에 간단한 위험에 그치지 않는다. 오늘날 사이버 공격은 적대국과 범죄자들 모두로부터 유발되는 위협이며 정보 · 민간부문 및 개인이 모두 피해를 입고 있다. 이에 대하여 조치를 취하지 않는다면 미래에는 이러한 위협이 더욱 확대될 것이다. 이러한 이유로 사이버안보는 영국이 가장 크게 위협받는 안보 요소 중 하나이다.

사이버공간이 긍정적인 측면에서 영국에게 많은 기회를 제공하는 반면에 사이버공간에 대한 의존도가 커짐에 따라 사이버공격으로 인한 위험도 커지고 있다. 휴대전화 · 자동차 · 냉장고 등에 이르기까지 모든 기기는 네트워크를 통하여 상호 연결될 것이다. 사이버공간에 대한 의존도 심화는 국가안보와 경제에 직접적인 위협이 될 수 있으며 테러 활동뿐만 아니라 군사적 무기로서의 역할이 계속 증가할 것이다. 그러나, 다방면에서의 사이버안보 활동은 영국이 경제적 · 안보적 측면에서 비교우위에 서도록 하는 기회를 제공할 수도 있다.

나) 사이버공격에 대한 대응

혁신적인 사이버안보 프로그램을 발전시키는 것은 국가 안보 위협에 대응하기 위한 영국의 자산과 능력의 향상에 영향을 준다. 사이버 안보 프로그램은 외국 정보, 범죄자 및 테러리스트로부터의 위협을 다루며 사이버공간이 미래 자산과 안보문제에서의 국익에 유리한 상황을 제공하는 기회를 확보하는 역할을 한다. 안보에 대한 다른 위협과 마찬가지로 모든 정부부처 및 기관은 각종 정책과 프로그램들을 통하여 국가안보 위협에 대하여 우선적으로 대응할 것을 확실히 하기 위한 유연성있는 조취를 취하는 것이 필요하다. 영국 정부는 국가사이버안보 프로그램 수행을 위하여 향후 4년간 6억 5,000만 파운드를 투입할 예정이다. 사이버안보 프로그램을 통하여 영국의 사이버범죄 대응

접근방법을 완전히 점검하고 사이버공격 탐지 및 방어 능력의 취약점을 보완하며 조직을 정비한다. 그리고, 주요 기반시설의 취약점을 보완하고 장기간의 사이버보안 연구개발 지원사업을 시행하며 사이버안보 교육 및 직무능력 향상 프로그램을 새롭게 제시한다. 또한, 사이버안보 공동체를 계속 건설하고 내각 내에 사이버안보 프로그램 관리실을 설치하는 한편, 새로운 사이버안보 전략에 따른 이행상황을 점검한다.

3. 국내외 표준화 동향

현재 스마트폰 보안 표준화는 국내·국제를 망론하고 초기 상태에 있다. 국내의 경우는 2010년 TTA 표준화 전략맵 작업을 통해 주요 표준화 아이템을 선정했고, 국외의 경우는 ITU-T 연구반 17에서 하나의 권고 가 개발되고 있다. 또한 아이폰 앱스토어에 적용되는 기존 공개키 인증서 프로파일이 사실 표준 형태로 존재한다. 향후 표준화 수요가 증가할 것으로 예상되어 본격적인 표준화가 국내외적으로 수행될 것으로 예측된다.

가. 국내 표준화 현황

국내에서는 2013년까지 스마트폰 관련 무선통신 국내외 표준화 추진을 통해 안전한 스마트폰 서비스 인프라 구축에 대한 기반을 마련하기 위한 목표를 설정하고 관련 연구와 표준화를 추진 중이다. 스마트폰 보안 국내 표준화는 이제 본격적으로 진행될 예정이다.

2010년 TTA 표준화 전략맵 작업에서 스마트폰에 대한 정의와 주요 표준화 대상 항목을 정의한 바 있다. 전략맵에서는 무선 통신망 보안 항목에 스마트폰 보안 세부항목을 설정했고, 스마트폰 세부 표준화 항목은 ‘스마트폰 플랫폼 보안기준’, ‘스마트폰 앱 보안 기준’, ‘스마트폰 인터페이스 보안기준’ 등이며, 세부 내용은 [그림 3-34]와 같다.

[그림 3-34] TTA 표준화 전략맵에 도출한 표준화 대상항목

표준화 대상항목	표준화 내용
스마트폰 플랫폼 보안기준	· 스마트폰에서 발생 가능한 침투공격, 스마트폰의 결함을 유도, 스마트폰의 정보 유출과 같은 악성 행위에 대하여 보호하고 이를 평가할 수 있는 기준 마련
스마트폰 앱 보안 기준	· 스마트폰에 제공되는 앱 서버나 앱 스토어의 앱 소프트웨어에 대한 보안 표준을 선정하여 앱에 대한 보안 평가와 검증 기준 설정
스마트폰 인터페이스 보안 기준	· 스마트폰과 PC나 다른 기기와의 연결에 사용되는 터널링(VPN) 기법
스마트폰 기반의 악성코드 수집/분석 프레임워크	· 스마트폰 등 모바일 기기를 대상으로 하는 악성코드의 수집 및 분석을 위한 프레임워크 요구사항 정의

자료: 국내외 스마트폰 보안 표준화 동향 및 추진전략, TTA Journal No 132

이외에 방송통신위원회 등 국내 주요 기관에서 스마트폰 보안 표준과 연관된 주요 활동 계획은 <표 3-16>과 같다.

<표 3－16> 국내외 스마트폰보안 표준 활동계획

국내외	기관	내용
국내	금융결제원	옴니아2, 아이폰, 안드로이드폰 등의 스마트폰에 대한 스마트폰뱅킹의 표준화 추진
	행전안전부	공공부문 모바일 응용서비스에 모바일 웹 및 모바일앱 개발을 위한 개발 가이드라인 작성
	TTA	-PG605 : 모바일 웹 서비스 보안 평가 가이드라인, 웹서비스 보안정책 모델 등 다수의 웹서비스 보안 관련 표준 제정, 모바일 종단간 통신을 위한 인증구조 외 3건 단체 표준 제정
		-PG504 : 모바일 웹 서비스에서의 메시지 보안을 위한 보안 구조 표준 제정
	방송통신위원회	'모바일시큐리티 포럼'을 통해 스마트폰 정보보호 주체별 역할을 정립하여 '스마트폰 이용자 10대 안전수칙'을 발표
국외	ITU-T SG17	모바일 상의 주요 보안 위협을 소개하여 보안 요구사항을 명시, 보안 기술 및 메커니즘을 제시하는 권고 개발 중
	MCPC	모바일 컴퓨팅 시스템 시장 확대를 목표로 하고 있으며 서비스 활성화를 위해 각 분야의 관심과 협력을 도모함
	PPCA	새로운 모바일과 무선기술에 대한 평가
	LIPS Forum	스마트폰과 일반 휴대폰(피처폰)을 포함하는 휴대폰 단말기의 다양한 사용 프로필에 대한 사양을 정의

자료: 국내외 스마트폰 보안 표준화 동향 및 추진전략, TTA Journal No 132

<표 3-16>에서와 같이 행정안전부에서는 공공부문 모바일 응용서비스에 모바일 웹 및 모바일 앱 개발을 위한 개발 가이드라인을 만들 예정이며, 금융결재원에서는 스마트폰 뱅킹의 표준화를 추진하고 있다.

특히, 스마트폰 보안과 연관되어 TTA PG 605에서는 모바일 웹 서비스 보안 평가 가이드라인[TTAS.KO-10.0245], 웹 서비스 보안 정책 모델[TTAS.KO-10.0243] 등 다수의 웹 서비스 보안 관련 표준 및 모바일 종단간 통신을 위한 인증 구조 외 3건의 단체 표준을 제정한 바 있다.

나. 국외 표준화 현황

ITU-T 연구반 17 연구과제 6은 스마트폰 보안 표준(X.msec-6)를 2009년 9월부터 개발하고 있다. 이 권고의 제목은 '모마일 폰 보안 특성'이며, 스마트폰보다 포괄적인 개념

을 갖는 모바일 폰에 대한 보안 위협과 보안 기술 및 메커니즘에 대해 표준화를 추진할 예정이다.

X.msec-6에서는 스마트폰에 대한 위협의 유형을 인터페이스, 사용자, ID 카드, 모바일 앱 서비스, 외부 인터페이스로부터 위협 등으로 구분되며, 스마트폰이 가진 취약성을 공격자가 이용한 다양한 위협 모델을 제시하고 있다.

스마트폰 보안 요구사항은 하드웨어 보안과 소프트웨어 보안으로 구성되며, 다시 소프트웨어 보안은 통신 보안, OS 보안, 애플리케이션 보안, 사용자 데이터 보안으로 구분된다. 모바일상의 취약점을 피하고, 위협 및 공격으로부터 피해를 감소시키기 위해 보안기술 및 메커니즘 기반의 하드웨어 및 소프트웨어가 만들어져야한다.

또한 아이폰 애플리케이션 게시자 신원확인 및 애플리케이션 코드의 데이터 인증 및 무결성을 확인하기 위해, 아이폰 앱 스토어에서는 ITU-T 권고 X.509에 기반한 인증서 프로파일을 사용한다. 윈도 및 안드로이드의 경우에도 인증서 기반의 코드사인을 통하여 데이터 인증 및 무결성을 확인한다. 코드사인 인증서는 국외 인증서 발급 기관 및 국내 공인인증기관에서 발급된 인증서로 사용이 가능하다. 대표적인 발급 기관에는 Verisign(국외), 금융결제원(국내) 등이 있다.

또한, 모바일 컴퓨팅 시스템의 시장 확대를 목표로 하고 있는 일본 컨소시엄인 MCPC(Mobile Computing Promotion Consortium)에서는 Smartphone 위원회를 신설하고 관련 연구와 표준화를 추진 중이다. 그리고 PPCA(Portable Computer and Communications Association)와 LIPS Forum(Linux Phone Standard) 등이 스마트폰 연구와 표준화를 진행할 예정이다.

제 4 장 신규 모바일기기의 보안 위협 및 취약점 분석

제 1 절 기술적인 측면에서의 보안위협

1. 단말기기 보안위협

단말기기 보안 위협이란 모바일 단말에서 기업•개인 정보 유출, 부정•불법 사용, 임의조작등을 유발시키는 것을 의미한다. 이러한 상황들을 발생시키는 위협으로는 악성코드 감염 위협과 단말기 분실 위협이 있다.

가. 악성코드 감염 위협

모바일 보안전문업체인 룩아웃(lookout)에서 지난 8월 3일에 발표한 2011 Mobile Threat Report'에 따르면 안드로이드 운영체제(Operation system)가 설치된 스마트폰의 경우 50만~100만대 정도가 악성코드에 감염됐을 것으로 추정되며, 이는 안드로이드폰이 악성코드에 감염될 확률은 6개월 전보다 2.5배나 높아진 것을 의미한다. 추가적으로 현재 위협상황으로 미루어보아 사용자 10명 중 3명 정도는 웹 기반 위협에 노출될 것이라 전망했다. 또한 악성코드에 감염된 안드로이드 애플리케이션이 아래 [그림 4-1]과 같이 지난 1월 80개 수준에서 6월 현재 400개 수준으로 늘어났다고 전했다.

[그림 4-1] 2011년 악성코드가 감염된 안드로이드 애플리케이션

자료 : 룩아웃, 2011

이와 같이 단말기기에 대한 악성코드 위험성은 점점 더 증가하고 있으며 감염 경로와 그로 인해 야기되는 위협 내용은 아래와 같다.

1) 감염 경로

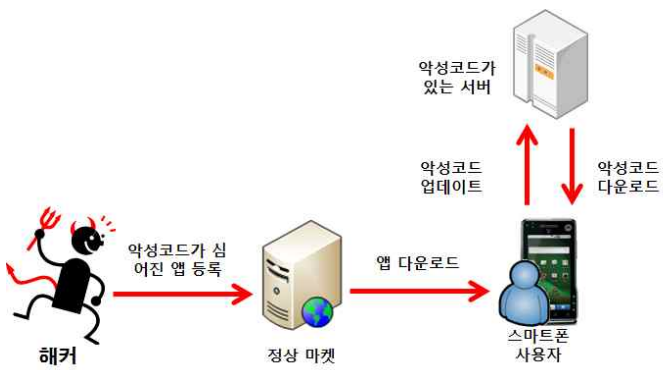
가) 악성코드가 삽입된 애플리케이션 설치

[그림 4-2]에서와 같이 해커는 악성코드가 삽입된 애플리케이션을 정상적인 애플리케이션과 결합하여 블랙마켓이라 불리는 써드 파티마켓(Third party market)이나 일반 공유 사이트에 업로드한다. 사용자는 블랙마켓 또는 인터넷을 통해 악성코드가 삽입된 애플리케이션을 본인의 스마트폰에 설치한다.

[그림 4－2] 악성코드가 심어진 애플리케이션을 통한 악성코드 감염

최근에 와서는 [그림 4-3]과 같은 형태의 악성코드 감염 경로가 증가하는 추세이다. 해커는 사용자가 많이 사용하는 정상적인 애플리케이션을 정상 마켓에 등록한다. 이 애플리케이션을 사용자가 다운받아 설치하면 업데이트를 통해 악성코드를 다운받아 기기에 설치하거나 광고메시지에 숨어 있다가 스마트폰을 감염시킨다.

[그림 4－3] 정상 마켓을 통한 악성코드 감염

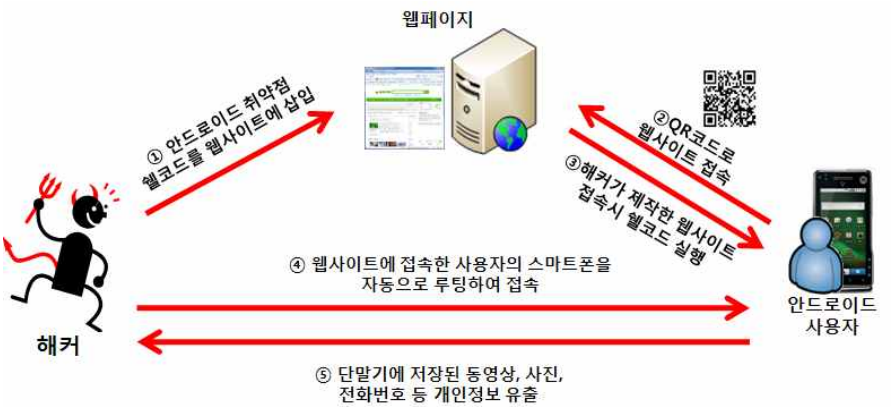


나) 웹 사이트 접속

2011년 6월에는 [그림 4-4]와 같이 스마트폰 커널에 관한 취약점을 이용하여 공격 가능한 방법이 발표되었다. 사용자가 QR-Code를 이용해 악성코드에 감염된 특정한 사이트를 접속 시 해커는 해당 스마트폰에 접속하고 커널 취약점을 이용하여 root 권한 획

득이 가능해진다. 이후 root권한을 가진 해커는 개인정보 유출을 비롯해 원하는 행동이 가능해진다.

[그림 4-4] 커널 취약점을 이용한 공격



2) 위협 내용

단말기기가 악성코드에 감염됨에 따라 다양한 피해가 나타나게 된다. 위협 내용은 크게 단말 장애, 배터리 소모, 과금 유발, 정보 유출, 좀비화 5가지로 구분할 수 있으며, 상세한 내용은 아래 표와 같다.

〈표 4－1〉 악성 코드 감염으로 인한 위협

위 협	설 명
단말 장애	스마트폰의 사용을 불가능하게 하거나 장애를 발생시킬 수 있다. 2004년에 발견된 Skulls가 한 예이다. 이 악성코드는 통화 이외의 부가 기능을 사용할 수 없게 만들었다. 2005년에 발견된 Locknut의 경우 단말기 일부 버튼을 고장 냈으며 Gavno의 경우 송수신 기능을 마비시키는 특성을 가지고 있었다.
배터리 소모	단말기기의 전력을 지속적으로 소모시켜서 방전시키는 위협이다. 2004년에 발생했던 Cabir 모바일 악성코드가 대표적이며 스스로를 전파하기 위해 블루투스 스캔을 시행하고 전파하던 악성코드이다. 이로 인해 단말기는 지속적인 배터리를 소모하게 되고 사용자는 배터리가 고갈되는 피해를 입었다.
과금 유발	메시지나 전화 시도를 지속적으로 시도하여 과금 발생을 유도하는 공격 위협이다. 대표적으로 최근 2010년에 발견된 '트레이 다이얼'이 있다. 트레이 다이얼은 윈도우 모바일 기반 악성코드로 무단으로 국제전화를 걸어 사용자에게 금전적 피해를 발생시켰다. 모바일 3D 게임과 동영상 관련 유틸리티에 포함되어 배포됐으며 50초마다 국제전화번호로 전화를 걸고 유료서비스로 접속 되어 분 단위 추가 요금을 발생해 추가적인 금전적인 피해가 있었다.
정보 유출	감염된 단말의 정보나 사용자 정보를 외부로 유출시키는 공격 위협이다. 스마트폰에 저장되는 문자메시지, 위치정보, 통화 기록 등 개인정보가 유출 대상이 되며 특히 최근 들어 인터넷 뱅킹을 비롯하여 회사의 업무까지 처리 가능하게 되면서 유출되는 정보의 위험성은 더욱 커져가고 있다.
좀비화	3.4 DDoS 대란과 같이 스마트폰도 공격에 이용될 우려가 있다. 스마트폰을 기반으로 한 모바일 인터넷전화(mVoIP) 서비스의 보안 취약점이 원인으로 지적되며 무선랜 또한 많은 위협에 노출돼 있어 스마트폰으로 착신 전화를 할 때 해커에 의해 좀비폰으로 둔갑하면서 DDoS 공격에 악용될 수 있다.

나. 단말 분실 및 정보 유출 위협

스마트폰이 활성화 되면서 이전에는 불가능하던 이메일 체크, 모바일 뱅킹을 비롯하여 증권거래 등 다양한 활동이 가능해졌다. 2011년 5월에 McAfee와 Carnegie Mellon University가 공동 조사한 보고서에 따르면 기업 내에서 모바일 기기로 업무를 처리하는 사람이 63%에 달하는 것으로 나타났으며, 스마트폰을 통하여 회사 업무처리까지 하는 경우도 있어 단말기에는 점점 더 많고 중요한 정보가 저장되며 분실 시 정보 유출

의 위험성이 더 커지고 있다.

2. 네트워크 보안 위협

스마트폰 사용자의 급격한 증가로 인해 기존 네트워크에서의 DDoS를 이용한 서비스 가용성 저해, IPS 및 방화벽 우회 등의 보안 위협이 모바일망에서도 발생하고 있다. 현재 모바일망의 트래픽이 폭발적으로 증가하고 있는 가운데 이를 악용한 mDDoS(Mobile DDoS)의 위협이 대두되고 있으며 이는 기존 장비를 이용하여 발생 가능한 위협이다. 다음은 이러한 모바일망 네트워크 취약점을 통한 피해사례에 대해 정리한 표이다.

가. 모바일 네트워크 보안 위협

모바일 망의 개방 및 3G 서비스 사용자 급증에 따라 적은 대역폭을 가진 Node B[2], RNC[3] (Radio Network Controller) 및 SGSN[4] (Serving GPRS[5] Support Node) 등에서의 망 안전성 위협이 존재한다. 또한, 모바일 사용자 및 이에 따른 3G 서비스 사용자의 급증은 데이터 트래픽의 폭발적 증가를 초래했으며 그에 따라 다수의 무선자원 할당 및 해제, 지속적인 무선자원 점유 등을 통해 3G망 가용성을 저해하는 결과가 발생하였다. 2010년 Cisco VNI (Visual Networking Index)에서는 모바일 데이터 트래픽이 2015년까지 연평균 92% 증가할 것으로 예상하였다.

3G망의 개방성, 사용자 / 데이터 트래픽 / 서비스의 폭발적 증가, 모바일 악성코드 증

---

2) Node B : UMTS (Universal Mobile Telecommunications System)에서 BTS (Base Tranceiver Station)를 표시하기 위해 사용되는 용어이다. UMTS는 이동전화나 컴퓨터 사용자들이 전 세계 어디에 있든지 간에 제3세대, 광대역 패킷 기반의 텍스트, 디지털화된 음성이나 비디오 그리고 멀티미디어 데이터를 2 Mbps 이상의 고속으로 전송할 수 있는 일관된 서비스를 말한다. BTS는 기지국을 의미하는데 주로 이동하며 업무를 운용하고 있는 무선국과 통신하기 위한 고정 무선국을 말한다.

3) RNC : UMTS radio access network의 구성요소들과 Node B를 제어한다.

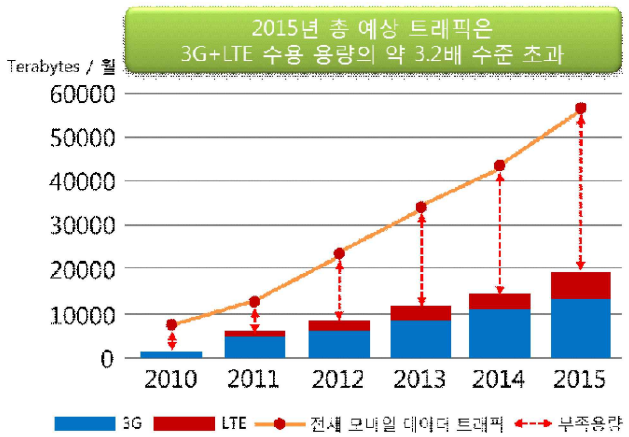
4) SGSN : 이동 단말이 보내는 또는 이동 단말로 보내지는 패킷을 전달하는 역할을 담당한다.

5) GPRS : General Packet Radio Service

가 등으로 망 안전성 보호기술 필요하다. [그림 4-5]는 향후 전 세계적인 모바일 데이터량의 증가치에 대한 예상을 그래프로 나타낸 것이다.

2015년 예상 트래픽량은 3G + LTE (Long Term Evolution) 수용 용량의 3.2배 수준으로 급격하게 증가하여, 망 안정성을 위협할 것으로 보인다. 따라서 향후, 4G(LTE, LTE Advanced)에서는 3G망에서 발생했던 보안위협을 상속하며, 보다 다양한 서비스가 제공됨에 따라 악의적인 공격 시도가 증가할 것으로 예상된다.

[그림 4－5] 3G+LTE 수용용량 vs 전체 모바일 데이터 트래픽



〈표 4－2〉 모바일망 피해 사례

사 례	비 고
연초대비 1,000% 데이터 증가에 따른 중계기 다운 및 통화품질이 저하되는 피해사례가 발생하였다.	전자신문, 2010.12
인구밀집 지역에 대한 Call Drop 현상이 증가하였다.	아주경제, 2010.1
TredDial[6] (트레드 다이얼)은 대량의 국제전화 통화를 발생시켜 과금 피해를 유도한다.	전자신문, 2010.4
2010년 12월 카카오톡 서버 비정상종료에 따른 3G망 장애가 발생하였다. 그 원인은 서버다운으로 카카오톡 가입 단말에서 지속적인 접속시도로 SGSN에 장애가 발생하였기 때문이다.	보안뉴스, 2010.12

나. 모바일 악성코드 증가에 따른 DDoS 공격 등 망 가용성 저해

악성코드에 감염된 단말은 대량의 국제전화 및 SMS 발송, 데이터 트래픽 발생시도를 통해 과금피해 유발 및 모바일망 가용성을 저해할 수 있는 과다 트래픽을 발생시킬 수 있다. 또한 3G 뿐 아니라, 인터넷망으로의 개인정보 노출, 스마트폰 데이터 노출, 스팸, 등 다수의 보안위협이 존재한다. 따라서 모바일 네트워크에서 비정상 트래픽에 대한 탐지 / 대응이 필요하다.

3. 서비스 보안위협

신규 모바일기기의 사용이 활성화됨에 따라, 이러한 신규 모바일기기를 이용한 다양한 서비스들이 제공되고 있다. 신규 모바일기기는 PC와 유사한 성능 및 기능을 제공하여 사용자들이 다양하고 편리한 서비스를 이용할 수 있게 해주고 있지만, 서비스 제공을 위해 사용자의 개인 정보, 위치 정보, 금융 정보 등을 사용하기 때문에 다양한 보안위협이 존재할 수 있다. 또한 이동성이 뛰어나고 개인정보가 저장될 수 있는 기기라는 점에서 개인정보 유출이나 금전적인 피해에 노출되기 쉽다. 신규 모바일기기를 이용한 서비스들의 보안위협으로는 위치기반서비스, 모바일 헬스케어 서비스, 모바일 RFID, 모바일 뱅킹 서비스, SNS(Social Networking Service)의 보안위협이 있다.

가. 위치기반서비스(Location Based Service, LBS)의 보안위협

위치기반서비스란, “이동통신망을 기반으로 사람이나 사물의 위치를 정확 하게 파악하고 이를 활용하는 응용시스템 및 서비스”를 통칭한다. 위치기반서비스의 보안위협은 크게 자신의 위치를 요청할 경우의 보안위협과 자신의 위치를 타인에게 제공하는 경우의 보안위협으로 나뉜다.

---

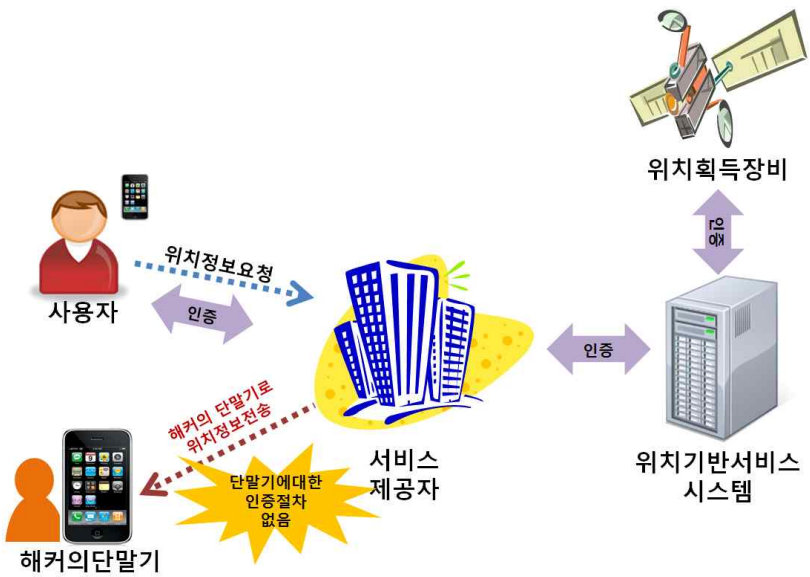
6) TredDial : 국내 첫 윈도우 모바일 기반 스마트폰 악성코드로서 2010년 4월 13일 첫 발견 이후 같은 해 4월 19일 변종이 추가 발견되었다.

1) 자신의 위치를 요청할 경우의 보안위협

가) 위치정보 해킹 위협

위치기반서비스 시스템에서는 ‘사용자와 서비스 제공자간의 인증 절차’, ‘위치기반서비스 시스템과 서비스 제공자간의 인증 절차’, ‘위치기반서비스 시스템과 위치획득 장비간의 인증 절차’ 의 세 가지 인증 절차가 요구된다. 하지만 현재의 위치기반서비스 시스템에서는 위치기반서비스 제공자와 단말기간의 인증 절차가 존재하지 않기 때문에 사용자에게 전송되는 위치정보를 해커가 자신의 단말기로 전송 받을 수 있다. 이러한 문제는 개인정보 및 프라이버시에 대한 위협으로 이어진다.

[그림 4-6] 사용자의 위치 정보 해킹 위협



나) 서버에 저장된 사용자의 위치 노출 위협

위치정보 서비스 제공자의 서버에는 서비스를 요청한 사람의 위치 정보가 저장되어 있다. 따라서 서버의 보안상 취약함으로 인해 해킹을 당하거나 내부자의 관리 소홀 및 내부자 공격으로 개인의 위치 정보가 노출 될 수 있다.

다) 가장 공격 위협

서버가 공격자가 되는 상황이나 혹은 공격자가 서버를 가장하는 공격이 존재할 수 있다. 이때 공격자는 사용자에게 잘못된 위치 정보를 전송할 수 있다.

2) 자신의 위치를 타인에게 제공하는 경우의 보안위협

가) 사생활 침해 위협

위치추적서비스가 반드시 필요한 상황도 있지만, 본인의 동의 없이 타인에 의해 사용되는 경우 사생활 침해가 될 수도 있다.

나) 재생 공격 및 가장 공격 위협

위치기반서비스는 사용자로 가장한 공격자에 의해 범죄에 악용될 수 있다. 공격자는 위치기반서비스를 악용하여 집에 누가 있는지 또는 빈집인지 아닌지를 확인하여 범죄를 저지를 수 있다. 따라서 위치기반서비스에서는 상호 인증이 매우 중요하며, 상호 인증 뿐 아니라 제 3자와 본인의 상호 동의하에 서비스가 이뤄져야 한다. 또한 위치정보 요청 프로토콜이 허술하다면 재생 공격이 가능하여 사용자를 가장하기가 보다 쉬워진다.

위치기반 서비스의 보안위협을 정리하면 아래 표와 같다.

〈표 4－3〉 위치기반 서비스의 보안위협

	보안위협	세부내용
자신의 위치를 요청할 경우	개인정보 유출	사용자에게 전송되어야 하는 위치정보의 해킹
		서버에 저장된 사용자의 위치 유출
	사회적 위협	악의적인 서비스 제공자가 사용자에게 잘못된 위치 정보 전송
자신의 위치를 타인에게 제공하는 경우	개인정보 유출	본인의 동의 없이 위치정보를 타인에게 전송하여 사생활 침해 발생
	사회적 위협	유출된 위치정보가 악용되어 범죄에 사용될 수 있음

나. 모바일 헬스케어 서비스의 보안위협

모바일 헬스케어 서비스는 신규 모바일기기를 이용하여 환자와 의사가 시간과 공간, 장소 등에 구애받지 않고 자유롭게 의료 서비스를 주고받는 모바일 기반의 서비스이다.

모바일 헬스케어 서비스 분야는 환자의 편의와 안전 측면에서 볼 때, 향후 대중화 될 서비스 분야라고 판단되지만 의료 정보는 개인의 민감한 정보임과 동시에 의학적 연구 및 공공의 의료 안전을 위해 공개되기도 해야 하는 정보이기 때문에 모바일 헬스케어에 있어서의 프라이버시 보호는 매우 중요한 문제이다. 모바일 헬스케어 서비스의 보안위협은 아래와 같다.

1) 시스템 오류에 의한 위협

잘못된 업데이트 또는 공격자에 의한 바이러스 등을 통해 시스템이 오류를 일으킬 수 있다. 이 때, 저장된 정보가 누출되는 사고가 발생한다면 프라이버시가 위협 받을 수 있다. 또한 데이터의 무결성에 문제가 생길 수 있으며, 이것은 환자의 생명에 치명적인 위협이 될 수 있다.

2) Public DB에 의한 위협

의료 연구 및 통계학적 자료를 위해 의료 DB가 공개 되어질 수 있는데, 이때 불필요한 정보까지 유출 되어 사용자의 프라이버시가 위협 받을 수 있다.

3) 전송상의 문제점으로 인한 위협

의료 자료가 신규 모바일기기에서 병원의 담당의사에게 전해질 때 공격자가 침입하여 데이터의 삽입, 변조, 삭제 등을 일으킬 수 있다. 이는 프라이버시 측면 뿐 아니라 환자의 생명과도 관련된 중요한 문제이다.

4) 저장된 사용자의 의료 정보 유출에 대한 위협

병원 측 서버에 저장된 사용자의 의료 정보가 유출 될 수 있다.

5) 서버의 스푸핑 공격에 대한 위협

병원이 아닌 곳 예를 들어 의약 제품을 파는 회사가 서버인척 하여 접근한 뒤, 이메일이나 각종 수단으로 자 회사의 제품을 광고할 수 있게 되어 프라이버시침해를 받을 수 있다. 모바일 헬스케어 서비스의 보안위협을 정리하면 아래 표와 같다.

〈표 4－4〉 모바일 헬스케어 서비스의 보안위협

보안위협	세부내용
개인정보 유출	시스템 오류에 의한 개인정보의 유출
	병원 측 서버에 저장된 사용자의 의료 정보가 유출
	데이터베이스 공개에 의한 개인정보 유출
	전송되는 의료 데이터의 해킹
데이터 변조	시스템 오류에 의한 데이터 변경
	해커에 의한 전송되는 데이터의 변조
스팸	서버의 스푸핑 공격을 통한 스팸메일 발송

다. 모바일 RFID의 보안위협

최근 신규 모바일기기에 장착할 수 있을 만큼 작은 크기의 RFID 리더기가 개발되었고 이에 따라 다양한 모바일 RFID 서비스가 제공되고 있다. 모바일 RFID 서비스의 예로는 식품에 RFID 태그를 부착하여 제조/유통 이력을 확인하는 서비스, 관광지의 주요 시설물에 RFID를 부착하여 해당 정보를 제공하는 서비스, 택시의 안심 귀가 서비스 등이 있다.

모바일 RFID는 크게 RFID 태그가 신규 모바일기기에 부착되어 신분증, 현관 열쇠, 지불 및 결제 등의 용도로 이용되는 방식과 신규 모바일기기에 RFID 리더기 기능이 탑재된 방식 두 가지로 구분할 수 있다. 각 방식에 대한 보안위협은 아래와 같다.

1) 신규 모바일기기 + RFID 태그

신규 모바일기기에 RFID 태그가 내장된 형태로, 이 경우 내장된 RFID 태그는 일반적인 RFID와 같은 기능을 한다. 따라서 이에 대한 개인 정보의 위협도 일반 RFID와 유사하다.

가) 위치기반 위협

특정 장소에 숨겨진 리더에 대해 두 가지 유형의 프라이버시 위협이 발생한다. 첫 번째 위협은 RFID 태그를 부착한 물건을 들고 가는 개인에 대해 추적이 가능하다는 것이고, 두 번째 위협은 태그가 부착된 물건의 위치정보가 알려질 수 있다는 것이다.

나) 고유정보에 관한 위협

태그에는 개인 정보나 고유의 ID와 같은 정보가 기록되어 있으며 이러한 고유정보가 유출 될 수 있다.

다) 거래에 관한 위협

모바일 RFID 서비스를 이용하는 사용자가 어떤 물건을 구매 할 때, 계좌번호나 신용카드정보 같은 추가적인 정보가 전달된다. 이러한 정보가 누출되면 개인정보 및 금전

적인 문제가 발생할 수 있다.

2) 신규 모바일기기 + RFID 리더기

신규 모바일기기에 RFID 리더가 내장된 형태로, 이 경우 리더기 기능을 가진 사용자가 공격자가 되어 RFID 태그를 가진 사람의 프라이버시를 침해하는 경우와 반대로 리더기 기능을 가진 사용자가 자신의 프라이버시를 침해당하는 경우로 나누어 생각할 수 있다.

가) 타인의 프라이버시를 침해하는 경우

RFID 리더 기능이 탑재된 신규 모바일기기를 가지고 있는 사람은 원하는 장소에서 언제든지 태그를 읽어 들여 태그의 정보를 수집할 수 있기 때문에 정보의 무한적인 수집이 가능하며, 이는 타인의 프라이버시를 침해할 수 있다.

나) 자신의 프라이버시가 침해당하는 경우

RFID 리더 기능이 탑재된 신규 모바일기기를 가지고 있는 사용자가 무선통신을 이용하여 모바일 RFID 서비스를 사용하게 되면 모바일 RFID 서비스 제공자가 모바일 RFID 리더기의 위치를 알 수 있게 된다. 이는 리더기 기능을 가진 사용자의 위치를 노출시켜 프라이버시를 침해할 수 있다.

모바일 RFID의 보안위협을 정리하면 아래 표와 같다.

〈표 4－5〉 모바일 RFID의 보안위협

	보안위협	세부내용
신규 모바일기기 + RFID 태그	개인정보 유출	RFID 태그를 부착한 물건 및 개인의 위치 정보 유출
		태그에 저장된 개인정보 유출
		RFID를 이용한 금융거래 시 계좌번호나 신용카드와 같은 금융정보 해킹
신규 모바일기기 + RFID 리더기	타인의 프라이버시 침해	RFID 리더기를 사용한 타인의 태그 정보 수집
	자신의 프라이버시 침해	무선통신에서 RFID 서비스 이용 시 RFID 리더기의 위치 노출

라. 모바일 뱅킹 서비스의 보안위협

스마트폰의 보급과 더불어 스마트폰을 사용한 모바일 뱅킹 서비스의 이용자 수가 늘고 있다. 모바일 뱅킹은 폰뱅킹의 편의성과 인터넷뱅킹의 기능성이 결합되어 언제 어디서나 금융거래를 할 수 있다는 강점을 가지고 있지만 모바일 뱅킹 서비스의 보안체계가 허술해 해킹에 무방비 상태라는 지적이 제기되고 있다.

모바일 뱅킹 서비스에서의 보안위협은 상상이상으로, 이미 외국에서는 SAS(Strategic Application System)[7]나 피싱이 결합된 공격이나 금전적인 목적의 공격이 나타나고 있어 PC수준의 보안대책이 필요하다. 금융감독원은 스마트폰 금융 보안에 대한 우려로 2010년 1월 7일 스마트폰 안전대책 발표했으며, 금융보안연구원도 스마트폰 애플리케이션 취약성 분석을 위한 신기술 기반 분석센터를 구축하고 전자금융 서비스 적용이 문제가 없는지 보안 적합성 테스트를 지원하고 모니터링을 강화할 방침이라고 발표했다. 그러나 스마트폰을 이용한 금융서비스에 대해 거창한 규제보다는 융통성 있는 정

7) 미국 North Carolina에 있는 SAS연구소에 의해 개발된 통계분석 패키지로 처음에는 통계적 전산 처리를 위한 것이었으나 지금은 시계열 분석(SAS/ETS), 파일 관리, 데이터베이스(SAS/SQL), 그래프(SAS/GRAPH), OR(SAS/OR)등 거의 모든 자료 처리에 막강한 힘을 발휘하고 있다.

책과 가이드라인이 필요하다는 주장도 있었다.

신규 모바일기기를 이용한 모바일 뱅킹 서비스의 위협은 크게 악성코드, 무선인터넷 중계기, 신규 모바일기기의 분실로 분류할 수 있다.

1) 악성코드의 모바일 뱅킹 서비스 보안위협

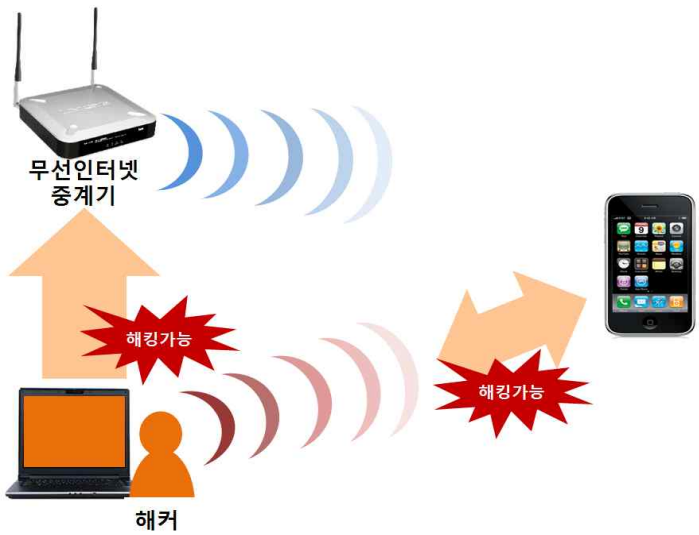
모바일 악성코드는 초기에 단순히 전파를 목적으로 하거나 단말의 기능적 동작을 마비시키는 형태에서 개인정보의 유출 및 금전적 이득을 목적으로 하는 형태로 변화하고 있다. 국내의 경우, 2009년 4월에 최초로 스마트폰 악성코드로 인한 피해사례가 발생하였고 악성코드로 스마트폰 내부에 저장된 공인인증서를 해킹한 사례도 발견되었다.

악성코드로 인한 개인정보와 공인인증서의 유출은 모바일 뱅킹 서비스의 큰 위협 요소가 될 수 있으며, 특히 스마트폰 내부에 저장된 공인인증서를 해킹하는 악성코드, 금융거래와 관련된 개인정보를 유출시키는 악성코드, 온라인 뱅킹 중 전송되는 금융 정보를 탈취하는 악성코드 등은 모바일 뱅킹 서비스에 있어 커다란 위협이 될 수 있다.

2) 무선인터넷 중계기의 모바일 뱅킹 서비스 보안위협

스마트폰은 무선인터넷 중계기를 통해 정보를 주고받는다. 2009년 방송통신위원회가 조사한 자료에 따르면 현재 국내에는 약 500만대의 무선인터넷 중계기가 보급되어 있지만 이 중에서 74%인 370여 만 대가 보안이 적용되지 않은 무선인터넷 중계기로 파악되고 있다. 해커가 스마트폰이 아닌 무선인터넷 중계기를 해킹하면 아이디, 비밀 번호 뿐만 아니라 스마트폰에 파일형태로 저장된 공인인증서도 순식간에 복사 할 수 있다. 또한 보안카드 번호를 재구성하면 금융거래까지 가능하다. 실제로 2010년 국정감사에서 보안이 적용되지 않은 무선인터넷 중계기를 해킹하여 사용자 정보를 비롯한 공인인증서 해킹을 시연하였다. 무선인터넷 중계기 해킹은 크게 자체 공격과 가짜 무선인터넷 중계기 공격으로 분류된다.

[그림 4-7] 무선인터넷 중계기의 보안위협



가) 자체 공격

스마트폰을 이용하여 인터넷에 접속하기 위해서는 무선인터넷 중계기를 통해 접속해야, 하는데 대부분의 무선인터넷 중계기가 매우 취약하기 때문에 스마트폰과 무선인터넷 중계기가 서로 주고받는 정보를 해커가 마음대로 볼 수 있다. 결국 해커는 손쉽게 각종 아이디나 비밀번호, 공인인증서까지 해킹 할 수 있게 되는 셈이다. 국내에서 발생된 사례로 2008년 노트북, 무선랜카드 등 장비를 이용하여 무선인터넷 중계기를 해킹한 사건이 발생했다. 무선인터넷 중계기의 보안이 취약하다는 점을 이용해 네트워크에 직접 접속하지 않고 무선인터넷 중계기를 해킹해 관리자 아이디와 비밀번호를 유출했다.

나) 가짜 무선인터넷 중계기 공격

가짜 무선인터넷 중계기는 무선 네트워크 연결과정 중 결합 및 인증절차의 취약점을 이용한 방법으로 해커가 무선인터넷 중계기인 척 사용자들을 유인해 접속하게 만든 뒤

정보를 빼내어가는 방법이다.

해커는 자신의 노트북을 무선인터넷 중계기로 전환하여 DNS(Domain Name Service), DHCP(Dynamic Host Configuration Protocol), HTTP(Hyper Text Transfer Protocol) 등의 서비스를 활성화 시켜 사용자들이 자주 사용하는 SSID(Service Set IDentifier), 예를 들어'NESXXX, IPTIXX, MYLGXXX'를 도용해 사용자들을 유인하는 방법이다. 만약 해커가 커피숍이나 카페에서 위와 같이 가짜 무선인터넷 중계기 공격 기법을 사용하고, 이름을 커피숍 명으로 도용한다면 수많은 사용자들은 이 사실을 모른 채 해커의 무선인터넷 중계기를 커피숍의 무선인터넷 중계기로 착각하고 접속하게 되어 개인정보의 유출이 가능하다.

3) 신규 모바일기기 분실의 모바일 뱅킹 서비스 보안위협

스마트폰은 일반 휴대폰과 달리 PIMS(Personal Information Management System, 개인정보 관리 시스템)나 이메일 등을 많이 사용하여 분실 시 여러 가지 보안의 문제가 나타날 수 있다. 스마트폰 분실로 인한 피해유형으로 스마트폰 내부에 저장된 개인정보 및 공인인증서의 유출, 단말 복제, 악성코드 삽입 등의 보안위협이 있다.

모바일 뱅킹 서비스의 보안위협을 정리하면 아래 표와 같다.

〈표 4－6〉 모바일 뱅킹 서비스의 보안위협

보안위협	세부내용
악성코드	악성코드를 이용한 공인인증서, 계좌번호, 계좌 비밀번호 등의 금융정보 탈취
무선인터넷 중계기 해킹	무선인터넷 중계기를 해킹하여 사용자 금융정보 탈취
	가짜 무선인터넷 중계기를 이용하여 사용자 금융정보 탈취
신규 모바일기기 분실	신규 모바일기기가 분실된 경우 내부에 저장된 금융정보 유출

마. SNS (Social Networking Service)의 보안위협

SNS는 온라인상 동일한 관심사를 가진 사람들 간의 인적 네트워크 형성을 지원하는 서비스로 ‘트위터’와 ‘페이스북’ 등이 대표적이다. 최근 신규 모바일기기의 확산으로 이용자 수 및 사용량이 급증하였으며, 이에 따라 SNS과 관련된 보안위협들도 함께 증가하고 있다.

1) 프라이버시 위협

최근 정보검색 기술의 발전으로 개인 프로파일을 수집할 수 있다. SNS의 특성상 익명으로 온라인상에서 활동하는 것이 아닌 자신의 소속, 연락처, 취미, 활동내역, 개인 사진 등의 모든 정보를 오픈한 상태에서 상호 신뢰성을 가지고 소통하기를 원하기 때문에 이러한 개인 프로파일이 수집되어 개인 프라이버시 침해가 발생할 수 있다. 이러한 정보추적은 쉽게 이루어질 수 있으며 개인 프로파일 정보가 위·변조되어 오남용될 수 있는 소지가 있다. 또한 이러한 프로파일 수집으로 2차 데이터 수집을 할 수 있는데, 예를 들면 SNS 접속시간, 장소, 이동경로, 개인 송수신 메시지, 개인 사진 등이 악용될 수 있다.

2) 바이러스 위협과 스팸

SNS는 신뢰를 바탕으로 서로 관심사가 동일한 온라인 네트워킹이다 보니 서로의 신뢰감이 상당히 중요한 역할을 한다. 하지만 누가 보냈는지 모를 파일에서 바이러스나 스팸에 노출되어 나 자신은 물론 다른 사람에게 피해를 입힐 수 있다.

3) 사회적 위협

SNS를 이용하면서 가장 위험한 것은 SNS를 이용한 사이버 스토킹, 사회공학적 기법을 이용한 정보 유출, 타인의 계정 도용 또는 명예회손 등과 같은 사회적 위협이 될 수 있다. 이미 국내에서도 유사한 사례가 있는데, ‘허경영 트위터’나 ‘손담비 트위터’ 등이 타인의 명의를 도용한 가짜로 밝혀진 경우가 있다. 또한, 최근에는 기업이나 조직에서 트위터를 이용하는 경우가 많아, 사회 공학적 기법을 통해 기업 기밀이 유출

될 수도 있다.

SNS의 보안위협을 정리하면 아래 표와 같다.

〈표 4－7〉 SNS의 보안위협

보안위협	세부내용
프라이버시 침해	SNS에 공개된 정보추적을 통한 프라이버시 침해
바이러스 위협과 스팸	SNS를 통한 바이러스 배포 및 스팸 전송
사회적 위협	SNS를 통한 사이버 스토킹, 사회공학적 기법을 이용한 정보 유출, 타인의 계정 도용 또는 명예회손 등

바. 자동차 보안위협

MtoM 통신(Machine to Machine)은 언제 어디서나 안전하고 편리하게 실시간 이용할 수 있는 미래 방송통신 융합 ICT(정보통신기술) 인프라로의 진화를 의미한다. MtoM은 사람이 직접 하기에 위험하거나 힘든 일, 시간이 많이 소요되는 일 등을 기계가 대신한다는 장점이 있으며, 자동차의 텔레매틱스나 내비게이션, 스마트 계량기, 자동판매기 등 다양한 분야에 적용되고 있다. 이 중 자동차에서 쓰이는 텔레매틱스나 GPS 기반의 네비게이션 등을 이용한 서비스는 운전자의 개인정보와 위치정보가 사용되면서 이에 따른 보안 위협들도 함께 증가하고 있다.

〈표 4－8〉 자동차 보안위협

보안위협	세부내용
타인의 프라이버시 침해	블랙박스 등의 영상장비를 이용한 주변 상시 촬영
무선 인터넷 해킹	차량과 차량간 통신, 차량과 서비스 제공자간의 무선통신 과정에서 차량 운행 정보 및 운전자의 개인정보 유출
위치정보의 불법적인 유출	본인의 동의 없이 위치정보를 타인에게 전송하는 경우 사생활 침해 발생
	유출된 위치정보는 범죄에 악용될 수 있음

1) 타인의 프라이버시 위협

최근 자동차 사고의 시비를 가리기 위해 차량용 블랙박스(EDR, Event Data Recorder)가 점차적으로 보급되고 있다. 차량용 블랙박스는 충돌 전후의 사고를 기록해서 사고 정황 파악에 필요한 정보를 제공한다. 따라서 우리나라는 2013년까지 버스와 택시 등 사업용 차량에 블랙박스를 의무적으로 장착하도록 교통안전법을 개정, 공포해 현재 추진 중이다. 하지만 택시 내 승객들의 민감한 대화내용이나 모습들이 승객의 의도와 무관하게 기록되고 있으며, 개인 차량의 경우도 주행 중 의도와 무관하게 타인의 프라이버시를 침해할 수 있는 내용들이 같이 저장되어 인터넷에 유출되는 등 타인의 프라이버시를 침해하는 사례가 증가하고 있다.

2) 무선 인터넷 해킹

텔레매틱스란 텔레커뮤니케이션과 인포매틱스의 합성어로, 무선 네트워크를 통해 차량을 원격 진단하고, 무선모뎀을 장착한 오토 PC로 교통 및 생활 정보, 긴급구난 등의 각종 정보를 이용할 수 있는 기술을 뜻한다. 최근 텔레매틱스 서비스 개발이 활발하여 현대자동차와 LG텔레콤은 무선차량 정보서비스 개발을 위한 전략적 제휴를 체결하였으며, 대우자동차는 한국통신프리텔과 손잡고 이동통신과 위치추적 기술을 접목한 드림넷 서비스 제휴를 체결하였다.

미국 라스베이거스 컨벤션 센터에서 열린 2012년 국제전자제품 박람회(CES)에서는

기아자동차가 북미 텔레매틱스 회사인 유보(UVO)와 함께 차세대 텔레매틱스 서비스를 선보였다. 이를 이용하면 고객 휴대폰과 연동, 사고신호를 자동 통보해 긴급출동을 유도하고, 차량 상태를 진단하는 것도 가능하다. 또한 스마트폰과 연동하여 주차위치를 확인하거나 문자 메시지를 음성으로 읽어주는 서비스도 제공한다. 이처럼 무선 네트워크를 이용한 각종 서비스가 시행됨에 따라 운전자의 개인정보나 차량 운행정보 등의 유출 가능성이 우려되고 있다.

[그림 4-8] 텔레매틱스 서비스 자동차

3) 위치정보의 불법적인 유출

최근 도로 상의 교통사고 다발지역, 휴게소 정보, 통과지점의 제한속도 안내 등 다양한 정보에 대한 데이터베이스가 구축되어 GPS(Global Positioning System)와 함께 다양한 서비스로 발전되었다. 하지만 운전자의 위치정보가 서버에 저장되는 경우에는 타인에게 운전자의 위치정보가 유출되어 사생활 침해의 문제가 발생할 우려가 있다.

4. 콘텐츠 보안위협

콘텐츠 위협중 대표적인 위협 유형으로는 콘텐츠 상의 DRM(Digital Right Management) 공격 위협이 있다. DRM이란, 디지털 콘텐츠의 불법유통과 복제를 방지하

고, 적법한 사용자만이 콘텐츠를 사용케 하며, 과금 서비스 등을 통하여 디지털 콘텐츠 저작권을 관리하는 기술이다. 그러나 낮은 데이터 전송 속도와 높은 패킷 전송 실패율을 갖는 무선 인터넷 망을 기반으로 하는 무선 디바이스에 기존 유선 DRM을 적용할 경우, 적은 메모리 자원, 제한된 처리 능력 등의 제약 사항으로 인하여 복잡한 암호화 알고리즘을 사용할 수 없다. 이러한 제약사항을 해결하고 모바일 환경에서의 효율적인 DRM 시스템 도입 요구로 인하여 모바일 DRM 시스템이 개발된다. 다음 <표 4-9>는 기존의 유선 인터넷 기반의 인터넷 DRM과 무선 영역까지의 확장을 고려한 모바일 DRM의 비교를 나타낸다.

〈표 4－9〉 인터넷 DRM과 모바일 DRM의 비교

유형	인터넷 DRM	모바일 DRM
콘텐츠 타입	영화, 음악, 기밀문서, 기업 문서와 같은 가치가 높은 콘텐츠가 주류	소규모 콘텐츠가 주류였으나 영화, 음악, 방송, 게임과 같은 가치가 높은 콘텐츠가 점차 대두
서비스 제공업체	가치 순환에서 상대적으로 적은 역할 담당	인터넷 서비스 제공자보다 다양하고 안정적인 서비스 제공 ※ 가치 순환에서 보다 큰 역할 담당
제 품 운 영 환경	- 파일 포맷 및 렌더링 애플리케이션에 종속적인 DRM 시스템이 주류 - 충분한 컴퓨팅 자원(ex. 대역폭, 메모리) - 필요한 S/W의 자유로운 업그레이드 및 패치 가능 - 주류 OS 존재	- 파일 포맷 및 렌더링 애플리케이션에 독립적인 DRM 시스템 - 부족한 컴퓨팅 자원 - OS의 영향으로 S/W의 업그레이드 및 패치 제약 - OS 및 플랫폼 종속적
표준화	- MS WMRM과 같은 Proprietary DRM을 기반으로 De facto Standard가 주류	- OMA DRM과 같은 De jure Standard가 주류이나 Proprietary DRM의 영향력이 점차 높아짐(MS WMRM, Apple Fairplay 등)

가. 모바일 DRM 위협

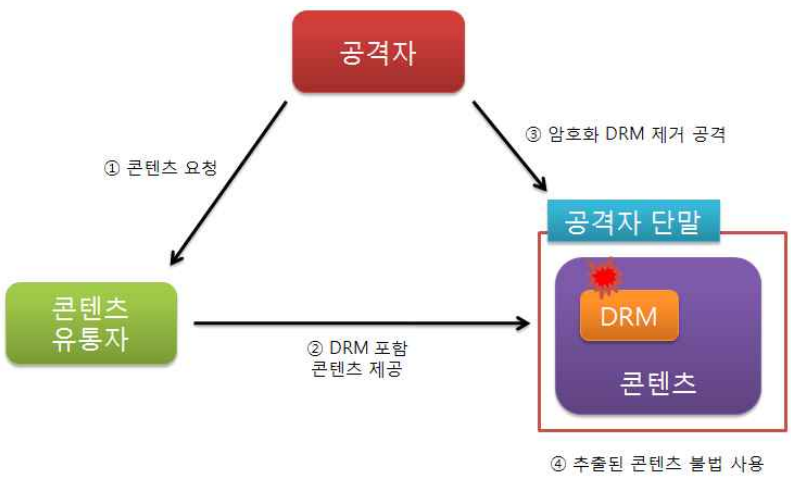
1) 모바일 DRM 기술적 위협 유형 및 사례

DRM 시스템 상에서 가능한 기능상의 공격 형태는 다음과 같이 콘텐츠 추출, 콘텐츠 주입, 그리고 단말기상의 저작권 조작 등으로 구분할 수 있다.

가) 콘텐츠 추출

콘텐츠 추출은 암호화되어진 콘텐츠로부터 DRM 기술을 제거 또는 조작하여 이용 가능하도록 만드는 것이다. 공격 대상이 되는 콘텐츠는 DRM 기술이 적용된 콘텐츠 체인을 이루고 있으며, 콘텐츠의 사용은 원저작권자의 요구에 따라 사용되고 지불 절차가 이루어진다. 콘텐츠 추출은 단말기 내부에서 이루어지며 다른 단말기로 재전송되는 것은 포함하지 않는다. 따라서 콘텐츠 추출은 콘텐츠 유통자와 이용 단말기, 또는 단말기 내의 특정 위치에서 콘텐츠 이동 시 일어날 수 있다. 콘텐츠 추출 공격 유형을 도식화하면 다음 [그림 4-9]와 같다.

[그림 4-9] 콘텐츠 추출 공격

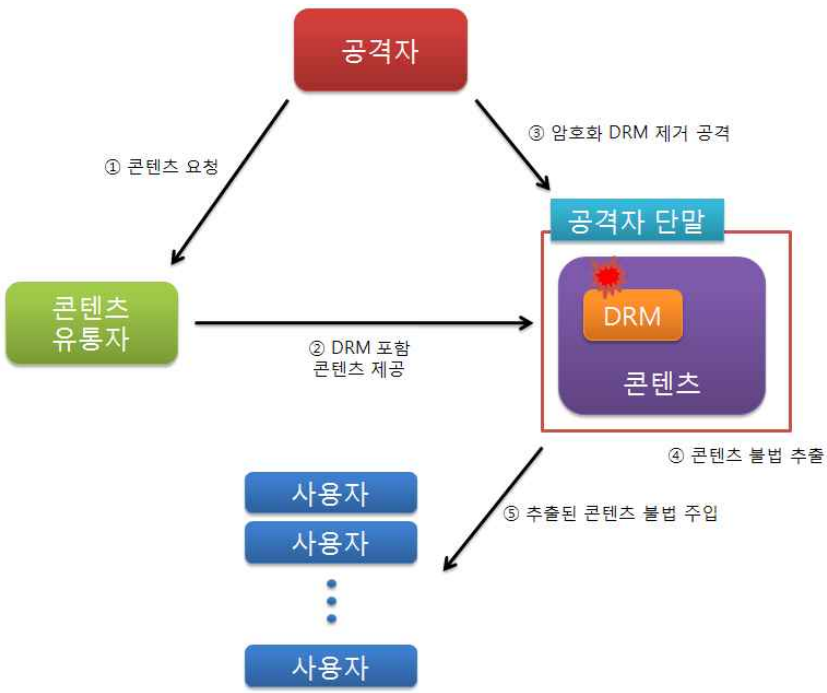


나) 콘텐츠 주입

콘텐츠 주입은 단말기 내에서 이용 가능한 형태의 콘텐츠를 다른 단말기로 재전송하여 비 인가된 사용을 허락하는 공격을 말한다. 콘텐츠 주입은 먼저 콘텐츠 추출 공격을 시도하여 성공하게 되면 불법적인 재사용을 위하여 행해지는 악의적인 공격 방법이

다. 콘텐츠 주입 공격 유형을 도식화하면 다음 [그림 4-10]과 같다.

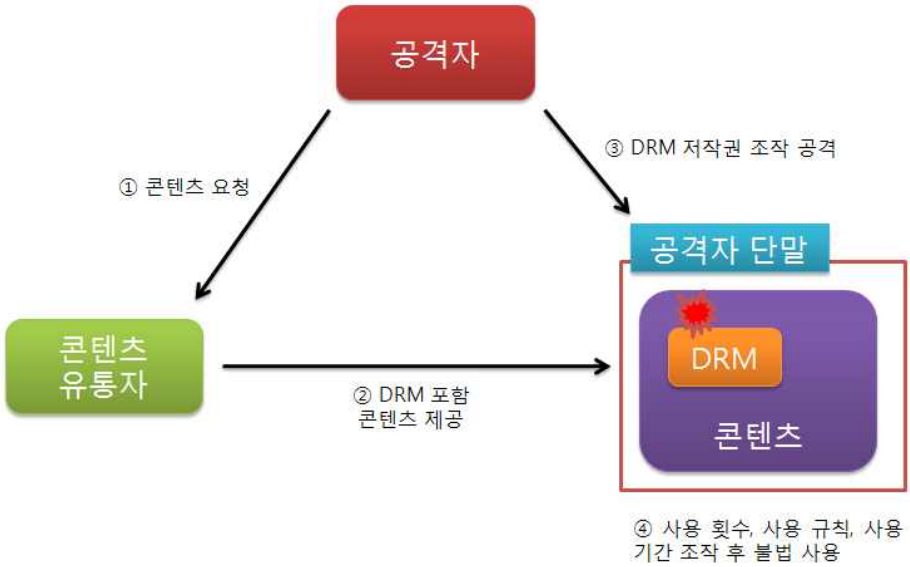
[그림 4-10] 콘텐츠 주입 공격



다) 단말기 상의 저작권 조작

단말기 상의 저작권 조작은 DRM 기술이 적용된 콘텐츠와 해당 콘텐츠의 저작권 내의 사용 규칙을 변경하는 공격이다. 이 공격을 통해 콘텐츠는 저작권자의 의도와는 다른 사용 규칙을 적용받아 불법 사용을 가능하게 한다. 예를 들어, 저작권 내의 사용 규칙상의 실행 횟수를 무제한으로 변경 하에 무제한 사용 가능하도록 하는 등의 공격을 말한다. 단말기 상의 저작권 조작 공격 유형을 도식화하면 다음 [그림 4-11]과 같다.

[그림 4-11] 단말기 상의 저작권 공격



이러한 악의적인 공격자의 모바일 DRM 공격 유형을 통하여 지난 수년간 DRM 해킹·위협에 노출되었다. 다음 <표 4-10>는 대표적인 DRM 위협 사례를 보여준다.

〈표 4－10〉 DRM 위협 사례

발생년도	내 용
2006	MS의 ‘윈도 미디어 DRM’이 공격을 받았다. ‘FairUse4WM’이라는 프로그램은 지난 8월 한 포럼에서 갑자기 등장한다. 이 프로그램은 MS의 멀티미디어 재생 SW인 ‘윈도 미디어 플레이어 10’과 ‘윈도 미디어 플레이어 11’의 인코딩을 이용하는 음악 다운로드 사이트에서 DRM 기술을 제거하는 공격을 수행한다. 애플도 ‘QTFairUse6’라는 프로그램을 이용한 아이튠스의 음악 파일 디코딩 작업에 방해 공격을 받았다.
2009	아마존 킨들 e북 콘텐츠를 인증 받지 않은 다른 기기에서 사용하지 못하도록 보호해주는 DRM이 해커에 의해 공격받았다. 아마존은 킨들용 콘텐츠를 ‘.azw’ 형식으로 판매하는데 이는 일종의 DRM기술로 킨들 e북 단말기나 PC용 킨들을 설치했을 때만 사용할 수 있다. 파일을 불법으로 인증 받지 않은 기기에 담을 수 없도록 보호하는 역할을 한다. 하지만 해커들은 DRM을 해지하는 프로그램을 개발하여 해당 파일을 다른 파일 형식으로 변환하여 기기에 저장할 수 있게 해주는 방법으로 DRM을 우회하였다.
2010	아이폰, 아이팟, 아이패드 등의 콘텐츠 창고인 아이튠스(iTunes)가 공격을 받았다. 아이튠스를 통해 구매한 음악, 영화, 동영상 등의 다양한 파일들이 아무 제약없이 무료로 배포되는 ‘에이전트 프로그램’이라는 해킹 프로그램을 통해 안드로이드 폰으로 옮겨 쓸 수 있게 되었다.
2011	아이폰 4S의 핵심 서비스인 Siri(음성인식 서비스)가 해킹당했다. Siri는 아이폰 4S에서만 사용할 수 있도록 되어 있지만 소프트웨어의 락을 해제하여 기존의 아이폰이나 아이팟 터치에서도 일부 기능을 사용할 수 있도록 하였다.

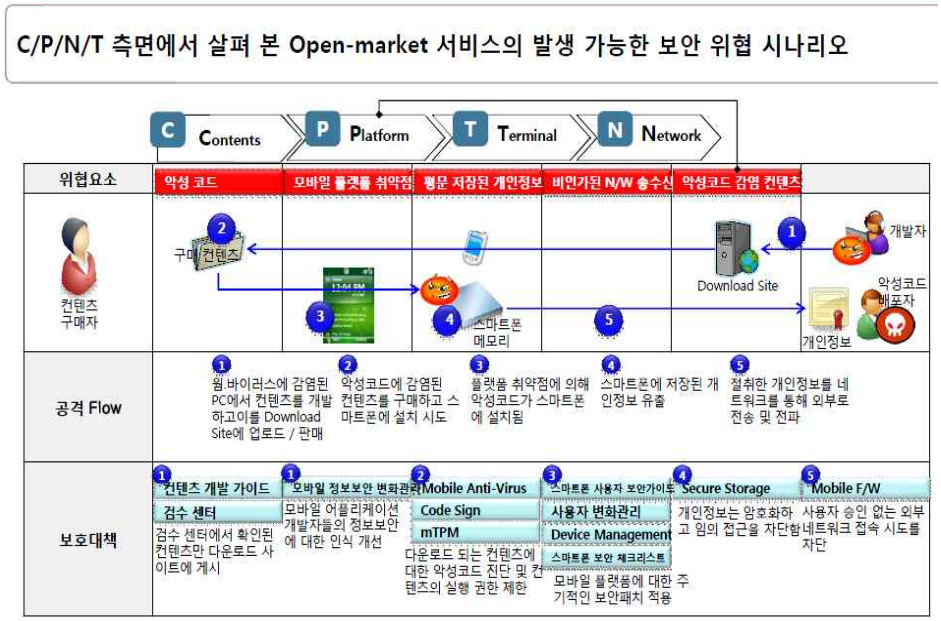
제 2 절 기술외적 측면에서의 보안 위협

1. 앱 유통환경 보안 위협

스마트폰 시장이 확대되면서 전문가들이 지적한 가장 큰 스마트폰 보안 문제는 스마트폰 애플리케이션과 그 유통 구조의 취약성이다. 현재 블랙베리, 심비안, 아이폰, 안드로이드 등 스마트폰용 모바일 OS를 제공하는 기업들이 애플리케이션 보안성 검증절차

를 진행하고 있지만 악성 애플리케이션을 앱스토어를 통해 사용자가 설치하기 전 단계에서 완벽하게 걸러내기 어렵다는 허점이 있기 때문이다.

[그림 4－12] Open-Market 보안위협 시나리오



또한 애플리케이션을 사고 파는 시장인 애플리케이션 스토어(일명 앱스토어)가 대중화됨에 따라서, 기존의 모바일 애플리케이션과는 달리 스마트폰에서는 애플리케이션 스토어가 개방적이기에 개발자들은 애플리케이션을 개발해 자유롭게 배포할 수 있다. 따라서, 일반적으로 개인 개발자 혹은 프로그램 제작사나 통신회사에서 만든 애플리케이션들이 오픈마켓이라고 하는 애플리케이션 스토어에 등록되고, 사용자는 무료 혹은 비용을 지불한 뒤 다운로드 받아 설치하는 방식으로 작동한다.

이러한 과정에서, 콘텐츠가 만일 악성코드에 감염된 상태로 배포되어 사용자에게 전파 되거나 구매한 콘텐츠 설치 과정에서 웜, 바이러스 등에 감염된다면 심각한 보안위협이 발생할 수 있다. 대표적인 애플리케이션 스토어에 대한 보안 위협으로 애플리케이션 스토어 상에 저장된 데이터를 기한 없이 사용하기 위한 크랙 시도, 제작 툴을 이용

한 커스텀 펌웨어 생성, 탈옥(Jailbreak)한 아이폰과 안드로이드의 루팅폰에 의해 불법 애플리케이션 다운로드 등을 들 수 있다.

다음은 앱 유통환경에서의 보안 위협에 대한 대표적인 사례를 보여준다.

가. 불법 개인정보 수집

최근 스마트폰 기기의 불법적인 정보 수집기능을 가지는 애플리케이션이 지속적으로 발견되고 있으며, 이렇게 유출된 정보들은 복제 휴대폰, 스팸 광고에 사용되는 DB 거래 등의 목적으로 악용될 위험이 매우 크다.

1) 앱을 통한 불법적인 개인정보 수집 사례

다수의 안드로이드앱이 사용자들의 단말기 고유번호를 수집하고 있는 것으로 드러났다. 한 보안업체가 집계한 결과 3G 단말기의 식별번호인 IMEI를 수집하는 안드로이드 앱이 국내외 100개가 넘는 것으로 밝혀졌다. 일부 앱은 IMSI나 USIM 시리얼번호 등 USIM에 저장된 각종 정보까지 수집하고 있는 상황에서 국내서도 이런 정보를 수집하는 앱들이 나오고 있어 법적으로 논란의 소지를 띄고 있다.

- 안드로이드용 스카이프 앱은 사용자의 통화 내역이나 메시지 전송 내역 등 개인 정보를 캐시 형태로 저장하는데, 사용자 정보를 빼돌리는 악성 앱이 스카이프의 사용자 정보에 접근할 수 있는 것으로 드러났다. 개인정보를 빼돌리는 악성 앱이 안드로이드 마켓에 배포되고 있어 심각한 보안 위협이 발생할 여지가 있다. 악성 앱이 접근할 수 있는 스카이프 사용자 정보는 e메일 주소, 사용자 ID, 생년월일, 휴대폰 번호, 대화기록 등이다.

- 애플의 아이폰이 개인의 위치정보를 축적하는 것과 같이 스마트폰 애플리케이션을 통해 개인 위치정보를 무단으로 수집. 활용한 사례가 빈번히 보고되고 있다. 애플의 iOS나 구글의 안드로이드 등 스마트폰 운영체제(OS)가 누구에게나 개방돼 있다는 것을 악용해 OS 단위에서 수집된 개인의 위치정보를 통해 불법으로 지역 맞춤형 광고를 내

보내는 등 위치정보 무단 수집에 악용된 앱 대부분은 음원, 게임, 뉴스, 생활정보, 쇼핑, 교육 등 위치정보와 전혀 관계없는 서비스를 제공하고 있다.

나. 모바일 악성코드 불법유포

모바일 악성코드는 스마트폰을 포함한 모바일 단말을 대상으로 정보유출, 단말 파괴, 불법 과금 등의 악의적인 행위를 수행하기 위한 악성 프로그램으로 정의할 수 있다. 모바일 악성코드는 모바일 단말의 성장과 더불어 규모면에서 빠르게 증가하고 있고, 위협 요인도 다양화되고 있다.

[그림 4－13] 증가하고 있는 스마트폰 악성코드 발견추이

모바일 악성코드가 증가하는 원인은 악의적인 목적을 가진 악성코드의 제작 및 유통이 가능한 개방형 단말기의 증가와 함께 블루투스, Wi-Fi와 USB 등 외부 접속의 다양화가 원인이라고 할 수 있다. 모바일 악성코드는 초기에 단순히 전파를 목적으로 하거나 단말의 기능적 동작을 마비시키는 형태에서 개인정보의 유출 및 금전적 이득을 목적으로 하는 형태로 변화되고 있다. 지금까지 존재한 모바일 악성코드를 주요 활동별 특성을 반영하여 분류하면 5가지 형태로 구분할 수 있다.

1) 단말 장애 유발형 악성코드

단말의 사용을 불가능하게 만들거나 장애를 유발하는 공격 유형이다. 2004년에 발견된 Skulls가 단말의 기능을 마비시키는 단말 장애 유발형 악성코드의 한 예이다. 이 악

성코드는 모든 메뉴 아이콘을 해골로 변경시키고 통화 이외의 부가기능을 사용할 수 없게 만든다. 2005년에 발견된 Locknut 악성코드는 단말의 일부 키 버튼을 고장내는 특성을 가지고 있다. 이외에도 전화의 송수신 기능을 마비시키는 Gavno가 등장하였다.

- 콘텐츠 삭제, 아이콘 변경 등을 통해 기기의 사용을 불가능하게 만들거나 일부 기능을 마비시키는 공격 수행
- 단말기 UI 변경, 단말기 파손(오류 발생), 정보(파일, 일정, 전화번호 등) 및 프로그램 삭제 등
- 장치이용을 제한하는 공격으로 공격자의 의도에 따라 특정 전화번호에 대해서 발신과 착신을 차단할 수 있으며, 긴급 상황 발생 시 단말 기능을 방해함으로써 혼란과 장애를 초래

▷ 장치이용 제한 악성코드
o Skull(2004) : 단말기의 시스템 애플리케이션을 다른 파일로 교체하여 단말기 사용을 불가능하게 하는 악성코드
o Bootton(2005) : 단말기에 설치된 응용 프로그램 아이콘 변경, 전화통화 외에 다른 기능을 사용하지 못하게 하는 악성코드
o BlankFont(2005) : 단말기 폰트파일 사용을 불가능하게 하는 악성코드
o Ikee(2009) : 유럽등지에서 유포되기 시작했으며, 아이폰의 바탕화면을 80년대 팝가수 릭 애슬리 사진으로 변경하는 악성코드
o Liberty(2000) : 단말의 모든 애플리케이션 삭제 및 재부팅

2) 배터리 소모형 악성코드

단말의 전력을 지속적으로 소모시켜 배터리를 고갈시키는 공격 유형이다. 2004년에 블루투스를 통해 전파되는 최초의 모바일 악성코드인 Cabir가 대표적이다. Cabir는 단말의 침해를 유발하지 않는 대신 지속적으로 인근 단말의 블루투스를 스캐닝하고, 블루투스를 통해 악성코드를 전파하는 특징을 가지고 있다. 감염된 단말은 지속적인 스캐닝을 통해 배터리의 고갈 피해를 입게 된다.

- 과도한 CPU 연산이나 네트워크 통신을 유발함으로써, 스마트폰의 배터리를 고갈시켜 스마트폰을 이용한 실시간 업무 수행을 방해하고, 업무 장애를 초래

3) 과금 유발형 악성코드

단말의 메시징 서비스나 전화 시도를 지속적으로 시도하여 과금을 발생시키는 공격 유형이다. 즉, SMS/MMS(멀티미디어 메시지)를 통한 바이러스 감염 등으로 강제통화, 대량 SMS(스팸문자)를 발송하여 비정상인 요금 유발, 휴대전화 소액결제, 무선 인터넷 이용, 유료전화서비스 악용 등의 문제를 발생시킨다.

- 스마트폰 사용자 20%가 SMS, MMS 및 메일을 통해 피싱 메시지를 수신 (시만텍, 2010.4, KISA 내부자료)
- 러시아에서 발생한 RedBrowser는 감염된 스마트폰에서 일반 메시지보다 비싼 프리미엄 요금으로 문자메시지를 발생시켜 사용자에게 과금(2007)
- 부정 과금 발생 시 사용자와 사업자 간의 분쟁시비 발생도 우려

▷ 부정과금 유발 악성코드
o Mosquit(2004) : 고액의 비용을 청구하는 서비스 전화번호 리스트를 포함하여, 단말기 사용자 몰래 SMS 메시지를 해당 전화번호로 보냄으로써 고액의 서비스 이용료 부과
o CommWarrior(2005) : MMS에 자신의 복사본을 첨부하고 단말기 주소록에 있는 모든 연락처에 발송함으로써 단말기 소유자에게 고액의 서비스 이용료 부과
o Timofonica(2000) : 임의로 생성된 번호로 문자 메시지 전송
o CommWarrior(2005) : MMS에 자신의 메시지 복사본을 첨부하고 단말기 주소록에 있는 모든 연락처에 발송하는 악성코드
o RedBrowser(2006) : 모바일 인터넷 사이트 방문 애플리케이션으로 위장하여 프리미엄 문자메시지를 전송하는 악성코드

4) 정보 유출형 악성코드

감염된 단말의 정보나 사용자 정보를 외부로 유출시키는 공격 유형이다. 2008년 발견된 Infojack이 대표적인 예이다. 이 악성코드는 합법적인 애플리케이션이 단말에 다운로드 될 때 .cab 설치파일과 함께 포함되어 설치되고, 설치된 후 특정 웹 서버에 접속하여 Infojack의 나머지 부분을 다운로드하여 재설치한다. 설치가 완료되면 단말의 보안 설정을 변경하고 단말의 시리얼 번호, OS, 설치된 애플리케이션 등 단말의 정보를 외부로 전송하여 2차 공격을 용이하게 한다. 사용자의 정보를 외부로 유출시키는 또 다른

악성코드로는 Flexispy, PBStealer가 있다. Flexispy는 스파이웨어 형태의 상용 악성코드로써 스마트폰의 전화기록, 문자메시지 내용을 특정 웹 서버로 전송하는 기능을 가지고 있다.

- 스마트폰의 블루투스 및 애플리케이션을 통해 이용자가 인지하지 못한 채 SMS, 통화기록, 위치정보 등의 개인정보 유출 가능
- 자녀 및 직원 관리 목적으로 정상적으로 판매되고 있는 프로그램(예: Mobile-Spy)을 이용하여 SMS, 통화기록, 위치정보 등을 포함한 이용자의 개인정보 유출 및 모니터링 등 악의적으로 사용
- 블루투스나 무선랜 기능 등이 인지하지 못하는 상태에서 사용가능하게 되었을 경우 타인의 무단접속 등으로 정보유출 가능

▷ 개인정보 유출 악성코드
o PBStealer(2005) : 전화번호부 압축 프로그램으로 가장한 악성코드로 단말기에 저장된 전화번호를 외부 단말기로 유출
o Infojack(2008) : 단말의 보안설정 변경 및 단말정보(OS, 설치 애플리케이션) 등을 2차 공격하기 위해 외부로 전송하는 악성코드
o iPhone/Privacy.A(2009) : 감염된 아이폰에서 무선랜을 접속하는 경우 개인정보(문자메시지, 이메일 등)를 원격지로 전달
o Duh Worm(2009) : 아이폰을 이용한 금융관련 거래에서 SMS 기반 인증코드(6자리)를 훔쳐 원격지로 전송하는 등의 금전적인 피해 유발 가능

5) 크로스 플랫폼형 악성코드

모바일 단말을 통해 PC를 감염시키는 공격 유형이다. 2005년에 발생된 Cardtrap.A가 최초의 크로스 플랫폼형 악성코드로써 폰의 메모리 카드에 윈도 웜을 복사하여, 감염된 폰 메모리 카드를 PC에 장착했을 때 autorun를 통해 PC를 자동으로 감염시켜 데이터를 삭제하거나 성능을 저하시킨다. 모바일 기기간의 확산이 아닌 모바일 기기에서 PC를 감염시킨다는 점에서 새로운 형태의 공격 유형이라 할 수 있다.

다. 기업별 앱 유통환경에서의 보안위협

1) 애플 - 앱 스토어

<표 4－11> 애플-앱스토어의 앱 유통 환경에서의 보안위협

구분	내용
유통환경	- 애플 앱스토어는 애플의 관리 하에 운영되는 스토어로 애플리케이션은 애플이 제공하는 심사 기준에 따라야 하며, 이 기준에 어긋날 경우 앱을 등록할 수 없도록 하는 '폐쇄형' 운영 구조를 갖고 있다. - 21만여 개의 앱이 등록(2010년 7월 기준)되어 있다. - 애플 앱스토어의 애플리케이션이 자체적인 결제 시스템이나 애플 사업과의 잠재적인 경쟁 등이 있을 경우 등록이 거절되는 경우가 있어 이슈화되기도 한다.
보안위협	- 아이폰의 경우 애플이 앱스토어를 통해 사전 검증이라는 제도를 두고 있지만, Cydia 등 블랙 마켓 존재를 통해 앱의 유통도 이루어지고 있고, 탈옥(JailBreak)이 된 경우 검증되지 않은 앱을 설치할 수 있으므로 동일한 이슈가 발생할 수 있다. - 애플이 앱에 대한 검증을 수행하는 애플의 앱스토어가 안드로이드 마켓에 대해 보안성은 우수하지만, 이 부분도 앱의 전체적인 기능이나 사용성 검증 보다는 자신들이 제공한 가이드에 따라 사용 API를 준수하였는지, 앱이 유통되는 국가의 법적인 저해 요소가 없는지 수준에 머물기 때문에 실제 사용자의 개인 정보 보호에 대한 부분에 대한 이슈가 있다. - 애플의 검증을 통해 앱스토어를 통해 배포된 국내 앱 하나가 지난 3월말 2~30분 사이에 3G망을 통해 2~300M를 사용하는 현상과 같이 사용성을 검증하지 못한 경우가 있었고, 이는 웹이 악성보다는 앱의 버그로 인해 과다 트래픽을 사용하게 된 경우로 애플의 검증이 완벽하지 않다는 반증으로 볼 수 있다.

2) 구글 - 안드로이드 마켓

<표 4－12> 구글-안드로이드 마켓의 앱 유통 환경에서의 보안위협

구분	내용
유통환경	- 구글의 안드로이드 마켓은 애플 앱스토어와 달리 마켓을 열어 놓고 개입하지 않는 '개방형' 정책을 펴고 있다. - 안드로이드 마켓에는 애플리케이션 개발자 누구나 등록 가능하지만 최소한의 검증도 이루어지지 않아 마켓 자체가 악의적인 앱을 유포할 수 있는 곳으로 활용될 수 있다. - 5만여 개의 앱이 등록되어 있다(2010년 7월 기준) - 최근에 국내에서도 유로 결제가 가능해져 안드로이드 마켓이 활성화 될 것으로 예상된다.
보안위협	- 구글은 개발 가이드만을 제공하고 있고 안드로이드의 앱을 설치할 때 안드로이드 마켓, 웹을 통한 다운로드 설치, ADB(Anroid Debug Bridge)를 통한 설치 등 다양한 방법을 제공하고 있어 앱에 대한 검증이 거의 되고 있지 않다. - 구글에서 플랫폼의 분산화(Fragmentation)로 인한 위험을 제어하기 위해 CTS(Compliance Test Suite)를 제공할 예정이지만 플랫폼에 대한 검증 또는 인증만 가능하고 애플리케이션에 대한 대안은 준비되지 않은 상태이다. - 구글은 최근 안드로이드마켓에서 악성프로그램58개를 발견, 이를 통해 악성앱을 설치한 스마트폰은 총26만대에 이른다. - 안드로이드는 무단 SMS 발송이나 개인 정보를 빼가는 스파이웨어 형태의 앱이 10여 종 발견되었고 현재 증가 추세에 있다. - 구글의 '안드로이드 마켓'에 은행 결제 애플리케이션을 가장해 사용자의 카드 정보를 빼가는 피싱 애플리케이션이 등장했다. 이는 대부분의 스마트폰용 애플리케이션 스토어들이 등록 전 확인 및 제제수단을 갖추지 않아 악의적 목적을 갖는 애플리케이션의 등록을 완전히 차단할 수 없기 때문에 발생된다.

2. 법 제도적 보안 위협

가. 국내외 스마트 모바일 정보보안 관련법

현행법상으로는 스마트 기기가 통신기기와 개인용 컴퓨터가 합쳐진 것이기 때문에 어떠한 법적 규율을 받아야 하는지 모호한 측면이 있으므로 스마트 기기 및 서비스 이용자에 대한 이용자 보호의 관점에서의 법적 보호 장치가 미흡하다.

1) 국내

정보보안과 관련된 주요 법률로 「정보통신기반보호법」이 있는데, 동 법은 정보통신망 중에서 '지정'을 통하여 주요 정보통신기반시설로 지정한 후 보안을 강화하는 내용을 담고 있다. 그리고 「전자정부법」에서 공공부문의 정보보안에 관하여 규율하고 있는데, 동 법은 정보통신망 등 보안대책 수립 및 시행(제56조), 행정기관 등의 정보 시스템 감리(제57조) 그리고 행정전자서명의 인증(제29조) 등에 관한 내용들을 담고 있다. 그리고 민간부문에 대한 정보보안 규정으로 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 있는데, 동 법은 정보통신망의 안정성 확보 등(제45조), 집적된 정보통신시설의 보호(제46조), 집적 정보 통신시설 사업자의 긴급대응(제46조의2), 정보보호 안전진단(제46조의3), 정보보호 관리체계의 인증(제47조), 이용자의 정보보호(제47조의3), 정보통신망 침해행위 등의 금지(제48조), 침해사고의 대응 및 신고 등(제48조의2 내지 제48조의3), 비밀 등의 보호(제49조), 속이는 행위에 의한 개인정보의 수집금지 등(제49조의2) 등을 규정하고 있다.

또한, 국내 정보보안 관련 법제는 공공부문과 민간부문을 나눠 규정하고 있는 것으로 보인다. 그런데 전자적 침해행위는 공공부문과 민간부문을 구분하지 않는다. 다양한 개별법에 관련 규정이 산재됨에 따라 조문 간 중복문제를 포함한 규범갈등의 소지가 내재되어 있다. 뿐만 아니라 첨단과학기술의 급속한 발전에 따라가는 것에 급급해 수차례의 개정을 거치면서 법규내용의 일관성마저 흔들리고 있다.[8] 그러므로 스마트 모바

8) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 「전산망 보급 확장과 이용촉진에 관한 법률」로 법명이 변경되었다가 2001년 1월 전부개정에서 현재의 법명으로 재 변경 되었다. 동 법은 1986년 이래 30여회에 걸쳐 개정되면서, 정보통신망의 이용촉진에 관한 내용에서부터 전자문서 활용, 정보보안 및 개인정보 보호, 통신 과금

일이 급속히 발전하고 있는 현 시점에서 정보보안에 관한 전반적인 법제 정비가 필요하다.

다음은 국내의 무선랜 보안에 관한 내용이다. 그러나 무선 AP의 취약한 보안 실태 문제를 완화하기 위해 사업자나 이용자에게 보안설정 등 정보보호조치 의무를 부과하거나 행정청에게 보안 현황을 점검할 권한을 구체적으로 규정한 현행법은 없다. 다만 안전 진단 기준, 개인정보 보호 조치 기준, 가이드라인 등의 개정을 통해서 용이하게 적용할 수 있는 조항은 일부 존재하고 있다. 무선 AP의 보안 강화를 위하여 주체별 적용을 고려해 볼 만한 현행법은 다음과 같다.

<표 4－13> AP 보안 강화를 위한 주체별 고려 현행법

의무 주체	현행법
- 무선 AP를 제공하는 사업자(ISP)	정보통신망법
- 사설 무선 AP 사용자(개인, 기업 등)	법적 근거 없음
- 공공 무선랜(Municipal Wireless network)을 운영하는 지방자치단체 등 공공기관	전자정부법
- 무선 AP를 수입·제조하여 판매하는 자	전파법
- 호텔, 공항 등 무선AP를 설치하여 고객에 대한 무선랜 서비스 제공자	정보통신망법

가) 정보통신망 이용촉진 및 정보보호 등에 관한 법률

방송통신위원회는 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법) 제46조의3 제1항[9]을 정보보호 안전진단의 일부로서 안전진단 수행기관을 통하

서비스 등에 관한 서로 각기 다른 내용을 단일법에 규정함으로써 법규내용의 일관성이 모호하다는 비판을 받고 있다.

9) 제46조의3 (정보보호 안전진단) ① 다음 각 호의 어느 하나에 해당하는 자는 방송통신위원회가 안전진단을 수행할 수 있다고 인정한 자(이하 “안전진단 수행기관”이라 한다)로부터 자신의 정보통신망 또는 집적정보통신시설에 대하여 매년 정보보호지침에

여 해당 ISP를 대상으로 무선랜 보안 현황을 점검할 수 있는 법적 근거로 삼을 수도 있을 것이다. 그러나 이 규정의 적용을 받을 주체는 극히 제한적이므로, 정보통신서비스 제공자에 해당되지 않는 사설 AP의 경우에는 이러한 안전진단을 받아야 할 법적 의무가 없다. 따라서 무선랜 공급의 상당한 비율을 차지하는 동시에 보안에 가장 취약한 사설 AP의 경우에는 행정기관의 무선랜 보안 점검을 실시할 법적 근거가 현행법상으로는 전혀 존재하지 않는다.

나) 전파법

전파법 제53조 제1항[10]은 방송통신위원회에게 무선설비규칙을 위반한 자에 대하여 소속 공무원에게 조사 또는 시험할 수 있는 권한을 부여하고 있다. 무선설비규칙(제98조)에 무선랜 보안 관련 규정을 신설하게 되는 경우에는, 방송통신위원회는 동법 제 53조 제1항을 해당 ISP나 사설AP 소유자등을 대상으로 무선랜 보안 현황을 점검할 수 있는 법적 근거로 삼을 수 있는 여지가 있다. 그러나 현행 무선설비규칙을 그대로 적용하는 한 전파법에 따라 AP가 무선설비규칙을 위반하였는가를 점검할 법적 근거는 미비하다고 할 것이다.

다) 전기통신사업법

따른 정보보호 안전진단을 받아야 한다. 이 경우 안전진단 수행기관은 15명 이상의 정보보호 기술인력을 보유하고 최근 3년 이내에 정보보호컨설팅을 수행한 실적이 있는 법인이어야 한다.

1. 「전기통신사업법」 제2조제1항제1호에 따른 전기통신사업자로서 전국적으로 정보통신망서비스를 제공하는 자(이하 “주요정보통신서비스 제공자”라 한다)
2. 집적정보통신시설 사업자
3. 정보통신서비스 제공자로서 매출액, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자

10) 제 45조 (기술기준) 무선설비는 주파수 허용편차와 공중선전력 등 방송통신위원회 고시로 정하는 기술기준에 적합하여야 한다.

제 53조 (조사 및 조치) ① 방송통신위원회는 제19조, 제25조, 제26조, 제29조, 제45조, 제46조, 제52조, 제57조 또는 제58조를 위반한 자가 있다고 인정되면 방송통신위원회 고시로 정하는 바에 따라 소속 공무원에게 조사 또는 시험하도록 할 수 있다.

전기통신사업법 제38조의2제2항[11]의 “전기통신역무의 품질”의 개념을 “무선랜 보안 수준”을 포함하도록 포괄적으로 해석할 수 있다면, 방송통신 위원회는 전기통신역무 품질평가의 일부로서 무선랜 역무를 제공하는 ISP를 대상으로 무선랜 보안 현황을 점검할 수 있는 법적 근거로 삼을 수 있다. 그러나 이는 Hot-spot이나 FMC에나 적용할 수 있을 것이다.

라) 통신비밀보호법

통신비밀보호법은 범죄수사 또는 국가안보를 위한 통신제한조치와 긴급통신제한조치를 규정하고 있다. ISP나 사설AP 소유자 등을 대상으로 무선랜 보안 현황을 점검할 수 있는 법적 근거로 삼기에는 적절치 않다.

정부가 무선랜 보안 대책의 일환으로 무선접속장치(AP)에 암호와 패스워드를 의무화하는 법안을 검토 중인 것으로 밝혀졌다. 무선 AP의 보안기능 설정을 위한 초기 패스워드가 동일하게 설정된 데다 인터넷에 공개돼 보안이 취약하다는 것과 대부분의 사설 AP는 이용자가 보안 설정을 하지 않아 누구나 쉽게 무단 접속을 할 수 있다는 문제점이 있다. 또한 무선랜 보안 해킹의 가장 큰 문제점은 공유된 AP로 접속한 해커가 네트워크에 침투해 데이터를 유출한 후 빠져나가면, 기술적으로 추적이 불가능하다는 점이다. 이 경우 모든 책임을 AP를 제공하는 가입자가 지게되는 불합리한 측면이 있다.

2) 국외

OECD의 「시스템 및 네트워크의 정보보안에 관한 가이드라인」(OCECDGuidlines for the Security of Information System and Networks: Towards a Culture of Security)」에

11) 제38조의2(전기통신역무의 품질개선 등) ①전기통신사업자는 그가 제공하는 전기통신역무의 품질을 개선하기 위하여 노력하여야 한다.
② 방송통신위원회는 전기통신역무의 품질을 개선하고 이용자의 편익을 증진하기 위하여 전기통신역무의 품질 평가등 필요한 시책을 강구하여야 한다.
③ 방송통신위원회는 전기통신사업자에게 제2항의 규정에 의한 전기통신역무의 품질평가 등에 필요한 자료의 제출을 명할 수 있다.

서 국제적 보안관리 기준을 마련하고 있다.

아래의 <표 4-14>는 해외 무선랜 보안 법규에 관한 내용을 정리한 것이다.

<표 4－14> 해외 무선랜 보안 관련 법규

국가	관련 법규		
	통신 사업자에 대하여 의무를 부과하는 법규	사용자의 권한없는 접근을 금지, 처벌하는 법규	통신요금의 회피를 목적으로 타인의 서비스를 이용하는 것을 금지하는 법규
미국	-캘리포니아 주:사업 및 직업법 22948.6조 -뉴욕 주:공공인터넷보호법	-2009 House Bill 1011 -CFAA(The Computer Fraud and Abuse Act) -ECPA(the Electronic Communications Privacy Act) MICH. COMP. LAWS ANN. §752.795	AS 11.46.200. Theft of Services
영국	디지털 경제법	경찰 및 사법절차에 관한 법률(Police and justice Act 2006)	통신법 (Communications Act 2003)
싱가포르		컴퓨터 오용에 관한 법률(Computer Misuse Act)	전기통신법 (Telecommunications Act)
캐나다		제342.1조	제326조
기타	-나이지리아:Nigerian Communications Act 2003	호주:Cybercrime Act 2001 일본: 부정액세스행위 금지 등에 관한 법률	

법제도 정비과정에서는 OECD 가이드라인에서와 같이 정보보안 원칙을 선언 하여 명확한 법해석의 기준을 제시하고, 이동성 및 개인화 등의 스마트 모바일의 특성을 적극 반영하며, 현재 다수 법령에 산재되어 있는 정보보안 관련 규정들을 취합·정리하여 일관된 법규적용이 가능한 체계로 정비하여야 할 것이다. 그리고 이 외에도 민관 공조

체계 구축 및 침해사고 대응능력 강화 훈련 등에 대한 법제도적 뒷받침이 필요하다.

나. 스마트폰 보안 국내외 표준화 동향

스마트폰의 보급과 활성화에 따라 기존 PC에서 발생하던 보안 위협이 스마트폰에서 발생하는 등 사회적으로 큰 파장을 일으키고 있다. 따라서 최근에는 스마트폰을 보호하고 안전하게 연동 사용이 가능케 하는 스마트폰 보안 표준에 대한 요구가 스마트폰 서비스 사업자와 보안 제품 사업자 등에서 나타나고 있다. 그러나 현재 스마트폰 보안 표준화는 국내,국제를 망론하고 아직 초기 상태에 있다. 국내의 경우는 2010년 TTA 표준화 전략 맵 작업을 통해 주요 표준화 아이템을 선정 하였고, 국외의 경우 ITU-T 연구반 17에서 하나의 권고가 개발되고 있다.

1) 표준화 추진 전략

스마트폰은 국내뿐만 아니라 국제적으로도 큰 관심을 불러일으키고 있지만 현재 국내외 스마트폰 보안 관련 표준화 작업은 이제 막 시작하는 수준이다. 따라서 TTA를 통한 국내 표준의 추진과 ITU-T를 통한 국제 표준의 추진 등 국내외 표준화 추진을 동시에 진행하여 국내 기술의 국제 표준을 선정할 필요성이 있다.

가) 국내

국내에서는 2013년까지 스마트폰 관련 무선통신 국 내외 표준화 추진을 통해 안전한 스마트폰 서비스 인 프라 구축에 대한 기반을 마련하기 위한 관련 연구와 표준화를 추진 중이다. TTA 표준화 전략맵에 도출한 스마트폰 세부 표준화 항목 및 내용은 <표 4-15>와 같다. 특히, 스마트폰 보안과 연관되어 TTA PG 605에서는 다수의 웹 서비스 보안 관련 표준 및 모바일 종단간 통신을 위한 인증 구조 외 3건의 단체 표준을 제정한 바 있다.

<표 4－15> TTA 표준화 전략맵에 도출한 표준화 대상항목

표준화 대상 항목	표준화 내용

스마트폰 플랫폼 보안기준	-스마트폰에서 발생 가능한 침투공격, 스마트폰의 결함을 유도, 스마트폰의 정보 유출과 같은 악성 행위에 대하여 보호하고 이를 평가할 수 있는 기준 마련
스마트폰 앱 보안 기준	-스마트폰에 제공되는 앱 서버나 앱 스토어의 앱 소프트웨어에 대한 보안 표준을 선정하여 앱에 대한 보안 평가와 검증 기준 설정
스마트폰 인터페이스 보안 기준	-스마트폰과 PC나 다른 기기와의 연결에 사용되는 터널링(VPN) 기법
스마트폰 기반의 악성코드 수집/분석 프레임워크	-스마트폰 등 모바일 기기를 대상으로 하는 악성코드의 수집 및 분석을 위한 프레임워크 요구사항 정의

나) 국외

ITU-T 연구반 17 연구과제 6은 스마트폰 보안 표준(X.msec-6)를 2009년 9월부터 개발하고 있으며, 모바일 폰에 대한 보안위협과 보안기술 및 메커니즘에 대해 표준화를 추진할 예정이다. 또한, 모바일 컴퓨팅 시스템의 시장 확대를 목표로 하고 있는 일본 컨소시엄인 MCPC(Mobile Computing Promotion Consortium)에서는 Smartphone 위원회를 신설하고 관련 연구와 표준화를 추진 중이다. 이 밖에도 PPCA(Portable Computer and Communications Association)와 LIPS Forum(Linux Phone Standard) 등이 스마트폰 연구와 표준화를 진행할 예정이다.

<표 4－16>국내외 스마트폰 표준화 동향 및 관련 추진사항

국내외	기관	내용
국내	금융결제원	옴니아2, 아이폰, 안드로이드폰 등의 스마트폰에 대한 스마트폰 뱅킹의 표준화 추진
	행정안전부	공공부문 모바일 응용서비스에 모바일 웹 및 모바일 앱 개발을 위한 개발 가이드라인 작성
	TTA	PG605 : 모바일 웹 서비스 보안 평가 가이드라인, 웹서비스 보안정책 모델 등 다수의 웹서비스 보안 관련 표준 제정, 모바일 종단간 통신을 위한 인증구조 외 3건 단체 표준 제정
		PG504 : 모바일 웹 서비스에서의 메시지 보안을 위한 보안 구조 표준 제정
	방송통신위원회	‘모바일 시큐리티 포럼’을 통해 스마트폰 정보보호 주체별 역할을 정립하여 ‘스마트폰 이용자 10대 안전수칙’을 발표
국외	ITU-T SG17	모바일 상의 주요 보안 위협을 소개하여 보안 요구사항을

		명시, 보안 기술 및 메커니즘을 제시하는 권고 개발 중
	MCPC	모바일 컴퓨팅 시스템 시장 확대를 목표로 하고 있으며 서비스 활성화를 위해 각 분야의 관심과 협력을 도모함
	PPCA	새로운 모바일과 무선기술에 대한 평가
	LIPS Forum	스마트폰과 일반 휴대폰(피처폰)을 포함하는 휴대폰 단말기의 다양한 사용 프로필에 대한 사양을 정의

다. 국내외 기업환경에서의 보안위협

최근 기업에서는 효율적인 기업 네트워크 형성을 위해 모바일과 클라우드 컴퓨팅을 사용하는 추세에 있다. 이러한 모바일 기기와 클라우드 컴퓨팅의 활용이 기업 업무환경 및 생산성 향상에 기여하는 바가 크지만 역으로 보안 위협 및 데이터 손실 위험이 증가하고 있는 상황에 직면하고 있다.

다음은 기업 네트워크의 대표적 사례인 모바일 오피스와 클라우드 컴퓨팅 환경에서의 보안위협 사례들을 보여준다.

1) 모바일 오피스

[그림 4－14] 모바일 오피스 환경

모바일 오피스란 언제 어디서나 모바일 단말기를 이용해 외부에서 회사 업무를 처리할 수 있는 시스템으로 기업의 생산성 향상 및 업무능률 향상을 위해 점차 확대되고 있는 상황이다.

가) 모바일 오피스의 보안위협

① 내부 망 노출의 위험성

-메일, 결제시스템 등 기업 내부 망과의 정보연동에 따른 내부 망 노출가능

② 트래픽 도청의 위험성

-Email, 문서의 전송 등 기업 활동 관련 정보 전송 시 트래픽 도청의 위험성

③ 권한 없는 접근의 위험성

- 권한 없는 외부자의 모바일 오피스 시스템 접근의 위험성
- 내부 직원의 권한을 넘는 정보 접근의 위험성

나) 모바일 오피스에서의 법적리스크

① IT Compliance Risk

IT Compliance란 특정 규제를 만족시킬 수 있도록 기업의 IT 인프라와 업무 프로세스 구축 및 재정을 도와주는 지침이다. 기업 비지니스에서는 IT의존도가 심화되면서 기업 활동을 효과적으로 규제하기 위한 비지니스 활동을 지원하는 정보처리 시스템과 디지털 데이터에 대한 규제가 필수적이게 됨에따라 IT Compliance 미준수 시 경제적 손실, 인지도 하락등 각종 위험이 크다.

[그림 4－15] IT Compliance의 요소 및 Risk

[그림 4－16] 모바일 오피스 IT Compliance Risk 및 고려사항

② Privacy Risk

- Customer Information Privacy Risk

: 영업활동을 위해 기업의 고객 개인정보수집이 늘어나고 있으며, 개인정보가 유/노출 될 경우 소송 등 리스크 발생

- Workplace Privacy Risk

: 업무용 Mobile에서 E-mail, PIN 메시지 등이 수집되는 사례가 늘고있어 이에 따른 직원들의 사생활 침해 논란 발생

<표 4－17> 국내외 기업의 개인정보 유출/소송 사례

위협구분	기업	내용
Customer Information Privacy Risk	옥션	° 1,863만 명의 개인정보 DB전체가 해커에 의해 유출 ° 14만명이 1일당 100~200만원의 배상금 요구하는 소송발생
	GS칼텍스	° 1,125만명의 개인정보 DB가 내부직원에 의해 유출 ° 4만여 명이 1일단 100만원의 배상금 요구하는 소송발생
Workplace Privacy Risk	Research In Motion	° 통신 양방의 동의 없이 통신기록을 수집함에 따라 Big Brother화 되는 문제발생
	블랙베리	° PIN 메세지의 서버축적에 의한 개인정보침해

③ Copyright / Infringement Risk

저작물 및 소프트웨어 구입 시 모바일 오피스 환경을 고려한 계약이 필요하고, 내부 통제 및 직원의 보안의식 필요하다.

。 저작 문서의 저작권 침해 위험성

- 저작권법: 저작물에 대한 전송 및 배포제한, 사적이용 등의 경우에 한해 전송 및 복제 허용

- 저작문서의 저작권 침해 위험: 모바일 오피스를 통한 저작물 전송 및 공유 시 저작권법상 접촉 될 수 있는 문제

。 소프트웨어 저작권 침해 위험성

- 가상화 소프트웨어 저작권 문제: 모바일 오피스에서 소프트웨어 가상화 기술을 이용할 경우 소프트웨어의 라이센스 저작권 침해기능

- 우회 등을 통한 소프트웨어 설치문제: 업무용 모바일에서 JailBreaking등을 통해 저작권이 있는 소프트웨어 우회설치 및 DRM Attack의 문제

다) 국내외 모바일 오피스 보안위협

<표 4－18> 국내외 모바일 오피스 보안위협 사례

국내 사례	국외 사례
- 우리나라의 국가정보원은 스마트폰으로 내부 전산망에 들어가 전자 결재를 하거나 내부 이메일을 열람하는 행위를 제한할 것을 지시한 공문을 모든 공공기관에 송부(2010.1)11)	－ 독일정부는 연방정보보안청(BSI) 권고에 따라 공무원들에게 보안 문제를 이유로 블랙베리와 아이폰 사용 금지 권고(2010.8.11) － 프랑스 컴퓨터긴급대응센터(CERTA)는 해커들이 아이폰 등 애플 제품에서 사용자 정보의 유출 및 통화 도청이 가능함을 경고(2010.8.6) － 사우디아라비아 통신당국은 국가보안을 이유로 블랙베리 서비스 중단을 명령하였으나, RIM사와 합의 후 서비스 재개 예정(2010.8.9.)

4) 클라우드 컴퓨팅 환경

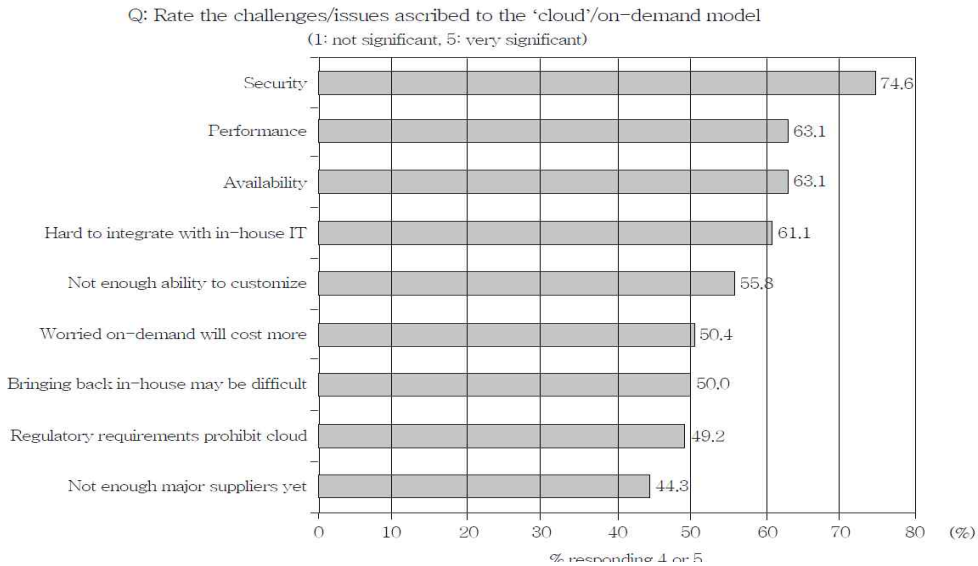
전 세계적으로 주목받고 있는 클라우드 컴퓨팅이 이제 국내에서도 본격적으로 추진되고 있으며, 이는 개인 뿐만 아니라 기업들에게도 더 이상 선택의 한 방식이 아닌 필수적인 고려 요소로 인식되고 있다. 그러나 책임문제 명확화 없이 제 3업체에 의존하고 개인데이터를 상업적으로 활용할 가능성이 있으며, 이에 따른 기업정보/고객정보가 유출되는 개인정보보호문제를 야기할 수 있다. 아직 국내에서는 클라우드 컴퓨팅에 관한 보안 법률이 미흡하여 대책마련이 시급한 상태이다.

클라우드 컴퓨팅은 IT 자원을 소유하지 않고 일부 또는 모두를 아웃소싱 하는 형태이다. 이런 경우는 필연적으로 보안 문제가 제기될 수 밖에 없다. 아래 [그림4-9]는 시장 조사 기관인 IDC에서 244명의 IT 관련 임원들에게 IT cloud 서비스에 관하여 그들의 견해와 활용에 대하여 조사한 것 중의 하나로, 보안을 해결해야 할 첫번째 과제로 꼽고

있다.

클라우드 컴퓨팅의 보안 이슈는 두 가지 소비자 영역으로 나누어서 생각해 볼 수 있다.

[그림 4－17] 클라우드 컴퓨팅의 문제



가) 개인 사용자 관점의 보안

개인 사용자는 이메일, 블로그, 동호회, 사진 및 파일 저장과 공유 서비스를 주로 이용하며, 무료로 제공하는 서비스를 선호하는 특성을 갖는다. 개인 사용자 관점에서 우려하는 보안 문제를 열거하면 다음과 같다.

① 개인정보 노출

② 개인에 대한 감시

③개인 데이터에 대한 상업적 목적의 가공

나) 기업 사용자 관점의 보안

기업 사용자는 자신이 소유하던 IT 자산을 클라우드 형태로 제공받기를 원하지만,

자신의 데이터가 타인과 공유되기를 원하지 않는다. 기업 사용자는 안정성과 안전성을 제공하면 비용을 지불할 의사가 있으며, 때에 따라서는 local cloud와 같이 자신이 직접 운영하기도 한다. 기업 사용자 입장에서 우려하는 보안 문제를 열거하면 다음과 같다.

① 서비스 중단
② 기업 정보 훼손
③ 기업 정보 유출
④ 고객 정보 유출
⑤ 법/규제 준수
⑥ e-discovery 대응

이와 같이 개인 사용자와 기업 사용자는 클라우드 컴퓨팅에 대한 보안 요구사항이 다르다. 개인 사용자는 익명성 보장에 중점을 두는 반면, 기업 사용자는 컴플라이언스에 중점을 두는 경향이 있다.

특히, 클라우드 컴퓨팅 환경적 특성상의 보안위협은 다음과 같다.

- 데이터와 정보가 집중되어 있다보니 클라우드 서비스 공급업체의 직원 혹은 서비스 관계자에 의해 중요 정보가 유출될 수 있음
- 외부에서 해커나 크래커의 공격대상이 되기 쉬움
- 클라우드 인프라는 동적으로 운영되므로 정해진 정책 적용의 실패/오류(예. 접근권한 정책이나 기술의 적용 실패 등)로 인한 데이터 유출 혹은 인프라 내 장애로 인한 데이터 손실 등이 주요한 보안 위협이 될 수 있음

이러한 클라우드 컴퓨팅 환경 하에서의 보안 위협이나 취약점에 대한 영향은 동일한 환경의 다른 사용자나 기업에 대해 파급이 가능하다는 점에서 위험이 더 크다.

각 클라우드 컴퓨팅의 서비스 모델에 따라 나타날 수 있는 보안 취약점은 아래와 같다.

<표 4－19> 서비스모델별 클라우드 컴퓨팅의 보안 취약점

서비스 모델	클라우드 서비스 공급자 측면	클라우드 서비스 이용자 측면

SaaS	-서비스 모델 중 공급자의 보안 책임이 가장 큼. -SaaS 형태로 제공하는 소프트웨어의 안전하지 않은 개발로 인한 보안 결함. -(가상화된 혹은 공급 받은) 미들웨어, 네트워크, 운영 체제상의 보안 취약점과 패치 적용이 용이하지 않고, 접근 통제가 실패할 수 있음. - 네트워크 간 암호화되지 않은 중요 정보 전달 등.	-이용자가 필요한 보안 통제 및 관리 적용 어려움. -내부 애플리케이션 연계를 위한 SaaS 상의 소프트웨어와의 인터페이스를 통한 악의적인 공격 - 중요 데이터와 개인정보에 대한 실제 암호화 및 접근 통제 여부에 대한 확인이 어려우며, 기업 및 이용자 표준 암호화 알고리즘 적용 및 변경 어려움. -감사 및 모니터링 등 보증 활동을 위한 데이터를 제공받기 어려움. - 가용성 확보가 용이하지 않은 높은 서비스 의존성
PaaS	-(가상화된 혹은 공급 받은) 미들웨어, 네트워크, 운영 체제상의 보안 취약점과 접근 통제가 실패할 수 있음. - 네트워크 간 암호화되지 않은 중요 정보 전달 등.	-PaaS상에서 개발하는 소프트웨어와 인터페이스의 안전하지 않은 개발로 인한 보안 결함 -개방 소스에 대한 보호가 용이하지 않거나, 원하는 보안 기능 구현이 어려울 수 있음. -개발 플랫폼과 서비스 플랫폼 사이의 차이로 인한 보안 결함.
IaaS	-(가상화된) 네트워크 및 운영체제 상의 보안 취약점. -(가상화된)네트워크 간 암호화되지 않은 중요 정보 전달 등.	-서비스 모델 중 이용자의 보안 책임이 가장 큼. -이용자의 활용 방식에 따라 다양한 보안 취약점 존재.

다) 국내외 클라우드 컴퓨팅 보안위협 사례 - 모바일 DDoS

감염된 좀비 단말기는 특정 사이트에 트래픽을 유발하거나 특정 단말기에 SMS를 전송함으로써 부정 과금 유발 및 웹사이트 마비, 단말이용 불능을 야기한다.

° 스마트폰 자체를 DDoS 유발용 단말기로 사용 가능

– 악성코드・웜 등에 의해 감염된 스마트폰을 좀비 클라이언트로 악용하여 DDoS 공격에 사용 가능함을 경고(안철수연구소, 2010.1, KISA 내부자료)

– 2009년에는 감염된 아이폰을 봇넷의 좀비로 만들어 스팸 및 DDoS 공격에 활용 가능한 ‘iPhone/iBotNet.A’ 사례 발생

▷ 스마트폰을 이용한 분산서비스거부(DDoS) 공격 발생 경고(KISA 인터넷침해대응센터 「2009년 12월 인터넷 침해사고 동향 및 분석 월보」, 2010.1.24)
o 스마트폰에서 DDoS 공격이 발생할 경우 사용한 트래픽량 만큼 과금되는 스마트폰 특성상 직접적인 금전피해도 예상
o 스마트폰을 통해 인터넷 접속이 손쉬운 특성으로 이 같은 위협이 높아지고 있으며, 이에 대한 대비의 필요성 강조

제 5 장 안전한 신규 모바일 기기 이용 환경 구축을 위한 보안 대책

본 장은 전자 정부 서비스의 기술적 보안대상을 단말기기, 네트워크, 응용 서비스, 콘텐츠 영역으로 구분하여 각 영역별 보안 대책을 분석을 목적으로 한다.

각 영역별 보안 대책은 [그림 5-1]와 같이 표현 할 수 있다. 단말기기 영역은 스마트폰, 태블릿 PC 등 모바일 기기 상에서 일어날 수 있는 침해사고에 대한 기술적 보안 대책에 해당하며, 네트워크 영역은 네트워크상에서 발생할 수 있는 침해사고 보안대책이다. 응용 서비스 보안 대책은 SNS, LBS, 뱅킹 등 모바일 단말 기반의 신규서비스의 침해사고 보안대책(모바일 PKI 인증, 모바일 방화벽)을 일컫는다. 모바일 콘텐츠 영역은 뉴스, 방송, 음악, 라디오, 영화 등 의 콘텐츠를 사용함에 있어 발생할 수 있는 침해사고 보안대책이다.

[그림 5－1] 영역에 따른 신규 모바일 기기 보안 대책

제 1 절 기술적인 측면에서의 보안대책

1. 단말기기 보안 대책

가. 보안 요구사항 분석

단말기기 보안 영역은 스마트폰, 태블릿과 같은 모바일 단말기 상에서 일어날 수 있는 침해사고 대응 및 대비를 위한 영역이다. 단말 보안 영역은 악성코드 감염, 단말 동작 마비, 단말 분실 및 정보 유출 등의 침해사고가 발생할 수 있으며, [그림 5-2]와 같이 모바일 OS 보호, 사용자 인증, 악성코드 대응의 범주에서 보안 요구 사항 및 대책이 필요하다.

[그림 5－2] 단말 보안 요구사항 분석

각각의 범주별 보안요구사항을 분석하여 <표 5-1>과 같이 구성하였다.

<표 5－1> 단말 보안 요구사항 분석

분 류		세부 요구 사항
사용자 인증	수행 시점	- 구동시 사용자 인증 수행 - 일정시간 미사용시, 자동 잠금 - 잠김 해제시 사용자 인증 수행
	인증 방법	- 추측하기 어려운 8자리 이상의 비밀번호 사용 - 비밀번호 평문 저장 금지
	인증실패 조치	- 일정횟수 이상 인증 실패시 보안 담당자만 해제 가능
악성코드 대응	안티 바이러스	- 안티바이러스 SW 설치 - 최신 엔진 상태 유지 - 실시간 감시 수행
		- 기술적 통제된 정기적인 검사 수행
	안전한 인터넷 이용	- 의심스러운 파일 다운로드 금지 - 다운로드 파일 검사 후 실행
모바일 OS 보호	모바일 OS 보안패치	- 모바일 OS 보안패치 최신상태 유지
	모바일 OS 변조방지	- 기술적 통제된 주기적 모바일 OS의 무결성을 검사하여 변조 방지

나. 보안 대책

단말 보안 요구사항을 만족시키기 위한 기술적인 안전 대책은 <표 5-2>와 같다. 표에서 기술 확보 가능 시기에 따라, 단기, 중기, 장기로 구분하였는데, 단기는 1년 내에 현재 확보 가능한 기술을, 중기는 2년 내에 확보 가능한 기술을, 장기는 2년 이후에 확보 가능한 기술을 일컫는다.

<표 5－2> 단말 보안 기술적 대책

분류	세부 보안 대책	시기별		
		단기	중기	장기
사용자 인증 대책	- 패스워드 미설정/일정회수 이상 입력 오류시 사용 차단	√		
	- 패스워드 자동 잠금 설정 탐지	√		
	- 전자서명(PKI) 인증서	√		
	- 인증서와 동등한 보안성을 가지는 인증 솔루션 적용 (OTP 등)		√	
단말 인증 대책	- 전자서명(PKI) 기반 단말 인증 및 키분배	√		
	- 기기인증서 기반 단말 인증 및 키분배		√	
악성코드 대책	- 전용 백신 S/W 제공	√		
	- 이동 저장매체 접속시 악성코드 자동탐지 및 삭제	√		
	- 악성행위 탐지 시 세션 강제 종료 및 로그 기록	√		
플랫폼 보안대책	- 플랫폼 구조변경(탈옥, 루팅 등) 자동 탐지		√	
	- 코드서명 기반 플랫폼 무결성 검증		√	
	- 실행영역의 논리적 권한 분리 (Sandboxing)		√	
	- 실행영역 메모리 무결성 검증			√
	- 멀티 태스킹 기능 차단		√	
	- 멀티 태스킹 기능 선택적 제어 기능			√
	- 사용자 프로세스의 파일시스템 접근 권한 제한		√	
TPM 보안 대책	- 부트타임 커널 데이터 무결성 검증 (루팅 및 플랫폼 변조 대응)		√	
	- 실행시간 플랫폼 무결성 원격 검증			√
	- 실행 전 앱 무결성 검증 (앱 위변조 검사)		√	
	- 실행시간 앱 무결성 원격 검증 (외부 공격 대응)			√
	- 하드웨어적 위조방지기능 탑재		√	
	- 안전한 저장 공간(RTS)에 개인키, 인증서 저장 관리	√		

1) 사용자 인증 대책

사용자 인증은 ID/패스워드(8자리 이상) 방식 또는 전자서명(PKI)기반 인증서 방식을 우선 적용하도록 한다. 이때 PKI 인증서는 단말이 제공하는 안전한 공간에 저장하여야 한다. 패스워드 방식의 경우, 패스워드가 설정 되어 있지 않거나 일정회수 이상의 입력 오류시에는 사용이 차단되어야 하고, 패스워드 자동 잠금 기능의 설정 여부를 판단할 수 있어야 한다. 중요 결재사항의 인증시에는 PKI 인증서와 더불어, 추가적인 인증 솔루션(OTP등)을 적용하여야 한다.

2) 단말 인증 대책

단말 식별 및 인증을 위해서는 PKI 인증서 또는 기기인증서 방식을 적용하도록 한다. 또한, 암호키 분배를 위해서도 인증서 기반 방식을 적용하도록 한다. 단말 인증을 위한 전자서명 생성 및 검증 알고리즘으로는 RSA(2,048비트), 해쉬 함수는 SHA-2(256비트) 보안 수준 이상의 알고리즘을 사용할 것을 권장한다.

3) 악성코드 대책

Virus, Trojan, Worm 등 유해 프로그램을 통한 해킹 및 네트워크 공격 방지를 위해 전용 Anti-Virus 단말 솔루션을 제공하여야 한다. 스마트폰 단말에 대한 백신프로그램 설치를 의무화하고 자동 업데이트 기능을 지원하여야 한다. 스마트폰에 저장매체(SD 카드 등) 접속 시, 저장매체에 악성코드 설치 여부를 자동점검 및 삭제하는 기능을 제공하여야 한다. Jailbreaking, Rooting 등으로 인해 모바일 OS의 무결성이 보장되지 않을 경우 스마트 전자정부 서비스 접속을 차단하여야 한다. 또한 비정상적인 접속 및 비정상적인 자료 송신 시에는 강제로 세션을 종료시키고, 세션에 대한 정보를 로그로 남겨야 한다.

4) 플랫폼 보안 대책

스마트폰 OS의 무결성을 검사하기 위해 탈옥(Jailbreaking), 루팅(Rooting) 등 플랫폼 구조변경 유무를 자동으로 탐지할 수 있어야 한다. 운영체제 커널 모듈, 보안 라이브러리 모듈 등에 대한 시스템 소프트웨어 실행 단계에서 코드서명에 기반한 무결성 검사

를 실시하여야 한다. 샌드박스(Sandbox)[12] 등에 기반한 업무용・개인용 앱 실행영역이 논리적으로 분리되어야 한다. 프로세스 메모리 후킹 등 실행시 시스템 메모리 영역에서 코드의 변경 또는 조작을 시도하는 악성코드의 경우 정적 코드 무결성 검사에서 탐지되지 않기 때문에, 메모리에 로딩된 코드의 동적 무결성을 점검하는 기능을 제공하여야 한다. 또한, 코드 서명이 없는 앱이 설치되었더라도 커널에서 실행되지 못하도록 프로세스별 실행 권한(Privilege) 제어 기능을 제공하여야 한다.

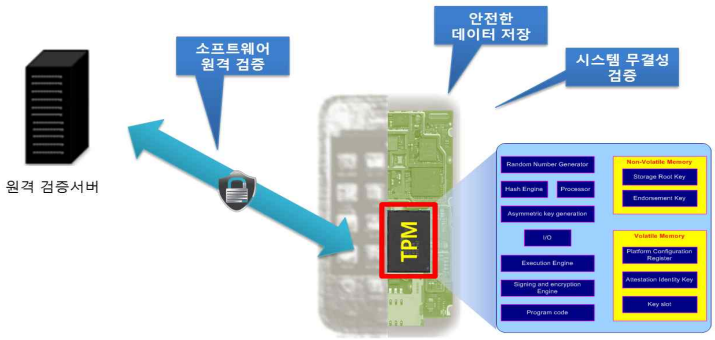
앱의 동작시 플랫폼의 멀티태스킹 기능을 차단하거나, 앱의 특성에 따라 선택적으로 백그라운드 프로세스의 동작을 제어할 수 있어야 한다. 아울러, 파일 시스템에 대한 접근 권한을 제한하고 사용자 프로세스의 시스템 자원에 대한 접근을 방지하여야 한다.

5) TPM 보안 대책

단말 불법 복제, 도청 및 악용, 개인정보 보호 위협, 악성 코드 삽입 등 외부 공격으로부터 데이터, 키, 인증서 등을 하드웨어 적으로 안전하게 보호 하고, 비밀키를 하드웨어 외부로 유출하지 않으면서 암복호 및 서명 검증 기능 수행이 가능하도록 하는 하드웨어 칩형태의 보안 솔루션을 TPM(Trusted Platform Module)이라 부른다. TPM이 단말에 장착되면 [그림 5-3]과 같이 사용자 인증, 플랫폼 무결성 인증, 앱 무결성 인증, 원격 검증 등 다양한 범주에서 보다 안전하고 신뢰성 있는 보안 솔루션을 제공할 수 있다.

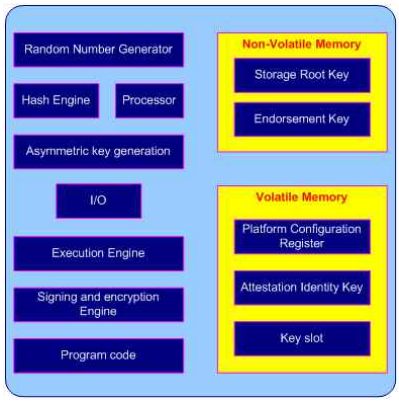
12) 보호된 영역 안에서만 3rd party application이 동작될 수 있도록 하는 시스템 소프트웨어 기능으로, 네트워크를 통해 전송받은 applications의 시스템 자원에 대한 접근을 제한하는 기능을 제공한다.

[그림 5－3] TPM기반 단말 보안 기능



TPM은 [그림 5-4]과 같이 크게 BIOS, 메모리, 암호 프로세서로 구성되어, 안전한 데이터 저장공간을 제공하며, 신뢰할 수 있는 플랫폼 동작을 위한 보안 모듈로 칩형태로 단말기에 내장된다.

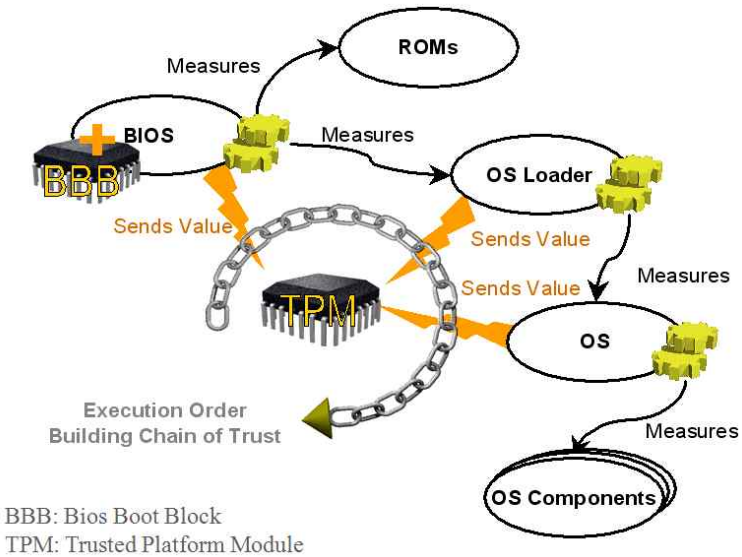
[그림 5－4] TPM 구성 요소



TPM의 비휘발성 메모리에는 2종류의 키 정보를 안전하게 저장할 수 있다. TPM 제조 단계에서 주입되는 Endorsement Key와 TPM 외부에 저장되는 키들을 암호화하기 위한 Storage Root Key가 있다. 휘발성 메모리에는 확장 연산(extend operation)을 통해 플랫폼 무결성 측정값(measurement)을 저장하기 위한 160비트 크기의 메모리 공간인 플랫

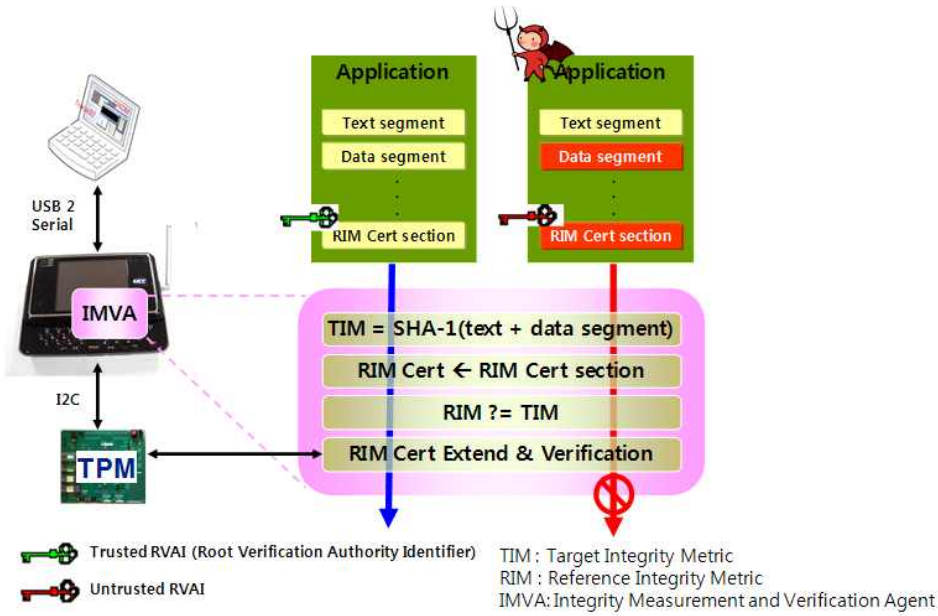
폼 구성 레지스터 (Platform Configuration Register: PCR)과 TPM에서 사용하기 위한 키를 로딩해 두는 공간이 키 슬롯 (Key Slot)이 있다. 키 슬롯의 수에는 제한이 있기 때문에 슬롯 수 이상으로 키를 사용하게 되면 로드된 키를 TPM 외부의 캐쉬에 임시로 저장한다. 또한, 플랫폼이 신뢰할 수 있는 상태임을 원격으로 다른 플랫폼에게 증명하는 과정인 원격 검증(Remote Attestation)시 플랫폼 사용자의 익명성이 보장되어야 한다. 이를 위해 Attestation Identity Key (AIK)가 별도로 안전하게 저장된다.

[그림 5－5] TPM 기반 플랫폼 무결성 검증 과정



TPM의 주된 기능은 커널 이미지, 라이브러리, 커널 모듈 등의 비트 이미지에 대한 위변조여부를 [그림 5-5]에서와 같이 BIOS, 부트로더(Boot Loader), OS, OS 컴포넌트 단계별로 칩 내에서 검사하여 결과를 알려준다.

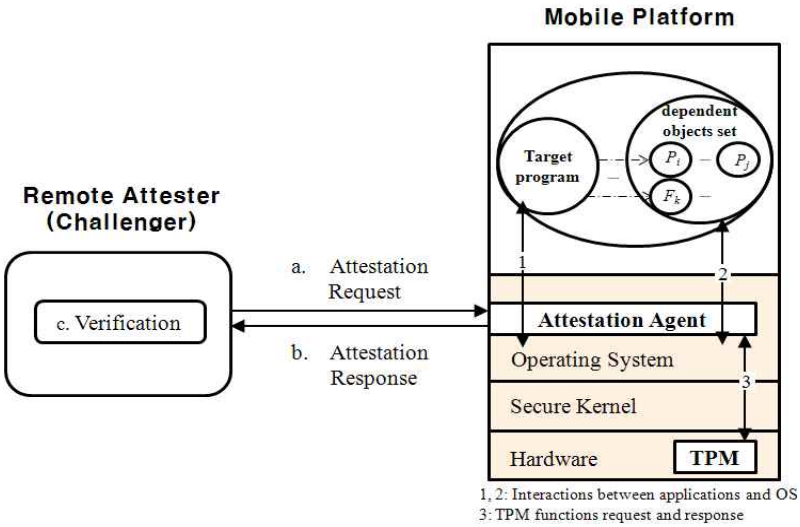
[그림 5－6] TPM 기반 앱 무결성 검증 과정



또한, 플랫폼 뿐만 아니라 TPM 기반으로 보다 안전하게 사용자 앱의 무결성을 [그림 5-6]와 같이 검증할 수 있다.

TPM 기반의 플랫폼 및 앱 무결성을 [그림 5-7]과 같이 원격으로 검증할 수 있다. 이를 위해, 단말에는 원격검증 에이전트(Remote Attestation Agent)가 탑재되어야 하고, 모바일 센터에는 원격 검증 서버(Remote Attester)가 구축되어야 한다.

[그림 5－7] TPM 기반 플랫폼 및 앱 무결성 원격 검증 과정



TPM은 단말 보안을 보다 근본적으로 제공할 수 있다는 기대감이 높으나, 몇가지 선결해야할 장애물이 많아 단기간에 적용하기 어려울 것으로 판단된다.

앞서 설명하였듯이, TPM에는 단말 제조사 또는 통신사가 발급하게 될 Endorment Key에 대응하는 공개키 인증서 체계(PKI)와, Storage Root Key에 대응하는 단말별 인증서 체계, 그리고, 원격 검증을 위한 익명 인증서 체계(Privacy PKI)가 별도로 사전 구축되어야 TPM 본래의 제 기능이 발휘될 수 있기 때문이다.

따라서, 단말 플랫폼 무결성 검증 용도, 즉, 소프트웨어 기반 코드 검증 루틴의 하드웨어화와 비밀키의 저장장치로만 TPM 기능을 국한할 경우에는 현재의 기술로 활용 가능할 것이나, 앱 무결성 검증, 원격 검증 등 체계적인 보안 검증 기능의 핵심 역할을 담당하려면, 단순히 하드웨어 칩 구현만 되어서는 안되고, 서로 다른 주체에 의한 PKI 구축 및 이로 인한 운용, 연동 문제 해결이 수반된 후에 도입하는 것이 바람직해 보인다. 또한, PKI 기반이 아닌 다른 접근 방법에 대한 해결책도 고려해 볼 필요가 있을 것으로 사료된다.

2. 네트워크 보안 대책

가. 보안 요구사항 분석

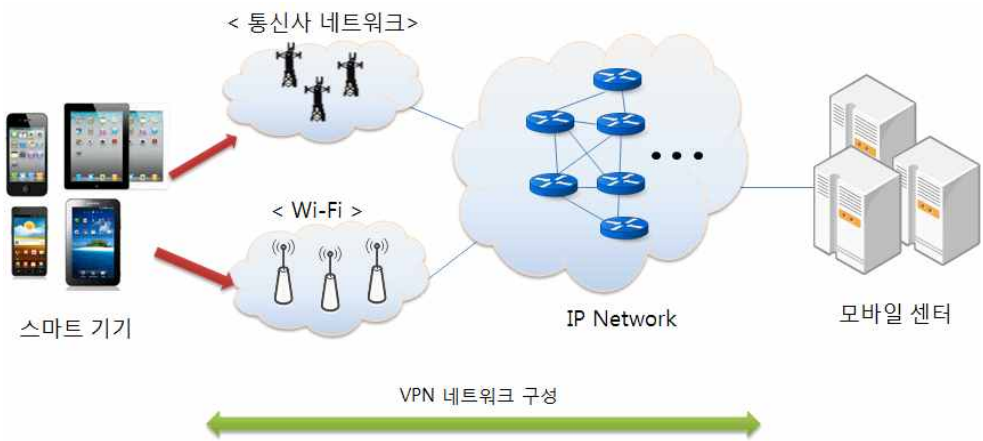
스마트기기가 주로 사용하는 무선 네트워크는 공개된 망을 통해 데이터 송수신이 이루어지는 특징을 가진다. 이 때문에 근본적으로 많은 보안 취약점을 가지고 있다.

네트워크 영역은 물리적 계층과 네트워크 계층으로 구분하며 각각의 보안 요구사항을 [그림 5-8]과 같이 분석한다.

물리적 계층에서는 악의적인 공격자가 내부망 근처에서 무선랜이나 기타연결 방식을 통하여 사내망에 접근할 위협이 있어, 무선랜 운용 및 기타 연결방식에 대하여 보안 요구사항을 분석이 필요하다.

네트워크 계층은 모바일 기기와 모바일 센터간 데이터 송수신에 참여하는 모든 네트워크 영역의 취약점을 분석하고 대처 할 수 있도록 침입차단, VPN, 보안관제 등을 고려한다.

[그림 5－8] 네트워크 영역 보안 대책



네트워크 영역의 세부적인 보안 요구 사항은 다음 <표 5-3>과 같다.

<표 5－3> 네트워크 보안 요구사항 분석

분 류		세부 요구 사항
물리적 계층	무선랜	- 인가된 내부 무선 AP만 운용 및 접속 허용 - 접속시 스마트폰 사용자 인증 및 암호화 통신 사용 - AP의 SSID Broadcast 통제
	기타	- 허가 받지 않은 장치를 통한 인터넷 연결 금지(예: 테더링 기능 사용금지)
네트워크 계층	무선 침입방지 시스템	- 기관내 무선랜 운용시 비인가 무선 단말・AP 탐지 등을 위한 무선 침입방지시스템 운영
	VPN	- 스마트폰에서 모바일 센터영역까지 VPN 적용 - VPN 클라이언트는 보안담당자의 통제를 받아 배포 - VPN이 동작하는 동안 他프로세스들의 통신은 모두 차단
	보안관제	- 해킹, 웜・바이러스 감염 대응을 위한 보안관제

나. 보안 대책

네트워크 보안 요구사항을 만족시키기 위한 기술적인 보안 대책은 <표 5-4>와 같다.

<표 5－4> 네트워크 보안 기술적 대책

분류	세부 보안 대책	시기별		
		단기	중기	장기
무선망 연결 대책	- 비인가 장비로부터의 무선랜 접속 차단	√		
	- 불법 AP, 애드혹 연결차단 및 탐지	√		
	- Wi-Fi, 3G 이외의 서비스 (예: 블루투스) 접속 방식 차단	√		
	- 이동통신망(3W)만을 통한 서비스 연결	√		
업무망 연동 대책	- 열람용 및 메모 보고용 서버 별도 구성		√	
	- 단말-업무망의 직접 접속 차단	√		
통신망 암호화 대책	- 안전한 암호화 통신채널(WPA2 등) 사용	√		
	- PKI 기반 VPN 인증 및 보안 채널 생성	√		

1) 무선망 연결 대책

높은 보안 수준을 요구하는 서비스의 접속은 이동통신망(CDMA, WCDMA, WiBro, LTE)과 WPA2와 같은 암호화 통신을 사용하는 무선랜(Wi-Fi)를 사용하여야 한다. 암호화 통신을 제공하지 않는 무선랜에서 모바일 뱅킹과 같은 높은 보안 수준이 요구되는 서비스의 접속은 차단되어야 한다.

2) 업무망 연동 대책

사용자 단말이 업무 서버로의 직접 연결을 차단하여야 하고, 단순 열람 및 메모 보고 서비스의 경우에도 게시판, 메모보고 서버와 업무망 간의 연동을 금지하고, 게시판, 메모 보고 서비스를 통해 민감, 중요사항 및 공문, 보고서 원문 소통이 통제되어야 한다.

업무망 직접 연결 차단을 위한 대책으로는 중계서버를 활용 하는 등 보안적합성 검증에 부합하는 다양한 방식으로 제공될 수 있다.

3) 통신망 암호화 대책

구내전화망 접속용 무선랜에 MAC주소 기반 비인가장비 접속을 차단하여야 하고, 안

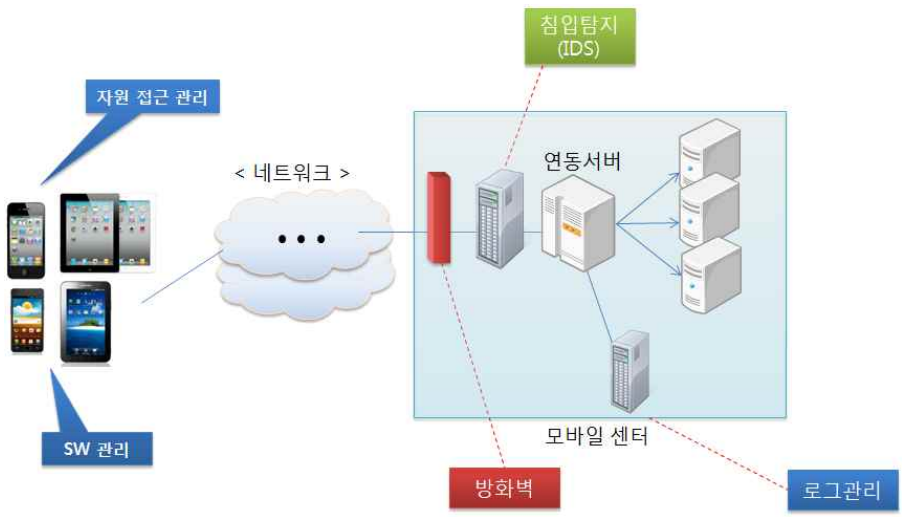
전한 인증 및 암호화 통신(WPA2 등)을 사용하영야 한다. 종단간 데이터 및 음성의 도·감청 방지를 위해 암호화(AES 128bit, ARIA 128bit)된 통신채널을 생성하여야 한다. VPN 인증 및 보안 채널 생성에 사용되는 인증서는 PKI기반 인증서를 적용하는 것을 원칙으로 한다.

3. 응용 서비스 보안 대책

가. 보안 요구사항 분석

응용 서비스 보안 영역은 SNS, LBS 등 모바일 단말 기반의 신규 서비스 상에서 일어날 수 있는 침해사고 대응 및 대비를 위한 영역이다. 응용 서비스 보안 영역에서는 위치/개인정보 유출, 모바일 뱅킹 해킹, 서비스 불법 사용 등의 침해사고가 발생할 수 있다. 때문에 [그림 5-9]와 같이 단말 기기에서 자원 접근 관리, SW관리에 관한 대책이 필요하며, 모바일 센터에서 침입탐지시스템(IDS), 방화벽 운용 및 서비스 로그 관리에 대한 대책이 필요하다.

[그림 5－9] 응용 서비스 보안 대책



응용 서비스 보안을 위한 세부적인 요구 사항은 다음 <표 5-5>과 같다.

<표 5－5> 응용 서비스 보안 요구사항 분석

분 류		세부 요구 사항
자원관리	H/W지원 접근통제	- 마이크, GPS, 카메라 등 HW에 대한 인가된 프로그램만 접근허용
SW 관리	S/W배포 및 설치	- 신뢰할 수 있는 인증기관에서 서명 또는 허가한 SW만 설치하도록 기술적 통제 수행
관리자 인증	계정관리	- 개발시 사용된 계정 및 비밀번호 폐기 - 8자리 이상의 비밀번호 사용 - 비밀번호 암호화 저장
	수행시점	- 업무 서버 접근시, 인증 수행 - 일정기간 입력이 없을시, 자동으로 업무 서버와 접속 해제
	인증방법	- 비밀번호 혹은 전자서명 인증서를 이용한 인증 수행 - OTP, 보안카드, 바이오인식 등의 방법으로 추가 인증을 수행
로그관리	사용자 행위 기록	- 스마트폰 사용자가 업무서비스에서 수행한 작업내역 기록 - 로그를 관리하기 위한 별도의 서버 운영
악성코드 대응	불필요한 서비스 제거	- 불필요한 서비스와 포트를 차단
	호스트 방화벽	- 별도의 호스트 기반 방화벽 운영

나. 보안 대책

응용 서비스 보안 요구사항을 만족시키기 위한 기술적인 안전 대책은 <표 5-7>와 같다.

<표 5－6> 응용 서비스 보안 기술적 대책

분류	세부 보안 대책	시기별		
		단기	중기	장기
앱 보안 대책	- 신뢰된 인증기관에 의한 코드서명 적용		√	
	- 이동통신망만을 통한 업데이트	√		
	- 패치관리시스템(PMS) 통한 버전 관리	√		
	- 소프트웨어(코드서명) 기반 앱무결성 검증		√	
	- 주요 H/W(카메라, GPS, 마이크)에 인가된 SW만 접근 허용	√		
원격제어 대책	- 디바이스 설정값(configuration)의 변경 탐지 및 복구		√	
	- 플랫폼 무결성 원격 검증 (Remote Attestation)			√
	- 앱 무결성 원격 검증 (Remote Attestation)			√
접속 관리 대책	- P2P, 웹하드 접속 금지	√		
	- 스마트폰-PC간 유무선 직접연결 차단	√		
	- 스마트폰-PC간 테더링 연결 차단	√		
	- 업무용 PC에 스마트폰용 매체(USB, microSD등) 제어 시스템 설치	√		
침입차단 및 방지 대책	- 방화벽, IDS 등 보안장비 구축 및 운영	√		
	- 주기적인 로그 분석을 통한 비정상 접속 여부 점검	√		
	- 앱 업데이트 서버 URL 검증 및 모니터링		√	
보안관제	- 24시간 보안관제	√		
전용 플랫폼 대책	- 민간과 분리하여 행정기관 전용으로 구축		√	
서버보안	- 비밀번호 또는 PKI 인증서 적용	√		
	- 이용자 로그 암호화 저장	√		

1) 앱 보안 대책

위치정보 및 개인정보를 사용하는 모바일뱅킹, SNS와 같은 응용 서비스 앱에 대해서는 공인된 앱 검증기관으로부터 CC 수준의 보안성 검증을 받아야 하고, 검증된 앱은 앱 검증기관이 발급한 코드 서명용 인증서에 기반한 코드서명 기술을 적용하여야 한다. 스마트폰 제조사 또는 통신사의 사전 검증을 받지 않았거나, 개인 등 신뢰할 수 없는

자가 자체 서명한 앱은 설치할 수 없도록 기술적 통제 장치가 마련되어야 한다.

응용 서비스 앱의 패치 및 정기 업데이트는 무선랜(WiFi)을 통해서는 할 수 없고, 이동통신망(CDMA, WCDMA, WiBro)을 통해서만 하여야 한다. 애플리케이션 공급 사이트(앱스토어, T스토어, 쇼스토어 등)를 통한 원격 패치 및 정기 업데이트는 허용하되, PC와의 연동 방식(PC Sync)은 PC 측면에서 사용자 인증 등 추가적인 보안 대책을 적용한 경우에만 허용하여야 한다. 또한, 설치된 소프트웨어 버전 등의 관리를 위하여 PMS(Patch Management System) 환경을 구축・운영하여야 한다.

소프트웨어 구동 시 단말 프로세스 환경에서 해킹 여부를 필수로 검증하여 변조되지 않은 단말기 환경에서만 접속이 가능하도록 하여야 한다. 스마트 전자정부 서비스 앱에 대한 안전성을 공인된 앱검증 기관의 인증서를 이용하여 앱의 코드서명 확인을 통해 무결성 여부를 판단한다. 또한, 스마트폰 H/W(카메라, GPS, 마이크 등)에 대한 임의 접근을 허용하지 않아야 한다.

2) 원격제어 대책

주요 디바이스의 설정값(configuration)을 임의로 변경할 수 없도록 하고, 이의 변경시 자동 탐지 및 복구 기능을 제공하여야 한다. 앱 및 플랫폼 구성정보와 실행코드의 무결성을 원격에서 주기적으로 검증(Remote Attestation)할 수 있어야 한다. 이를 위해 모바일 센터에서는 원격 검증 서버(Remote Attester)를 운영하여야 한다.

3) 접속관리 대책

스마트폰을 이용한 P2P, 웹하드 접속을 단말에서 차단하는 기능을 제공하여야 한다. 스마트폰과 일반 PC간의 유무선 직접 연결을 통한 데이터 전송을 통제할 수 있어야 하고, 스마트폰과 PC간의 테더링(Tethering)[13] 연결을 차단하여야 한다. 또한, 업무용 PC에는 스마트폰용 저장매체(USB, microSD 등)에 대한 접근을 통제할 수 있는 기능이 제공되어야 한다.

13) 스마트폰이 무선모뎀이나 AP로 활용되어 인터넷을 이용할 수 있도록 하는 기능

4) 침입 차단 및 방지 대책

해킹 및 비인가자의 접근 차단을 위해 이동통신망과 연동되는 구간에 침입차단시스템 구축·운영하고, 비정상 트래픽의 상시 모니터링을 위해 이동통신망과 연동되는 구간에 유해트래픽탐지시스템 구축·운영하여야 한다.

5) 보안 관제

위협관리대응 및 침해사고 대응시스템을 구축·운영하여, 24시간 보안관제를 실시한다. 침해사고 및 보안정보를 안내 및 공지를 통해서 각각의 서비스에 제공하고, 웹을 통한 침해사고 접수, 처리 및 결과통보하도록 한다.

6) 전용 플랫폼 대책

스마트 전자정부 서비스용 모바일 플랫폼은 정부통합전산센터 등에 민간과 분리하여 행정기관 전용으로 구축하여야 한다. 모바일 플랫폼은 일반적으로 보안·통신환경, 모바일서버(웹서버 등), View서버 등으로 구성 된다.

7) 서버 보안

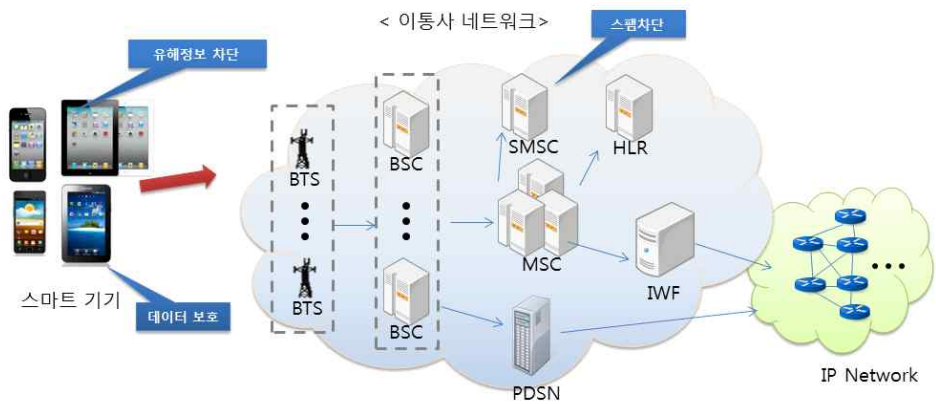
모든 서버는 호스트 기반의 방화벽 운용, 비밀번호 또는 인증서 적용, 로그관리, 불필요한 포트 차단 및 접근·권한 통제 등의 기능을 제공하여야 한다. 또한, 모바일 플랫폼에서 행정서비스 관련 자료는 저장하지 않으며, 이용자 로그 등에 대하여만 암호화하여 저장할 수 있다.

4. 콘텐츠 보안 대책

가. 보안 요구사항 분석

콘텐츠 보안 영역은 웹, 미디어, 문서, 앱 등의 스마트 기기 상의 콘텐츠를 사용함에 있어 발생할 수 있는 침해사고 보안대책이다. 콘텐츠 보안 영역은 [그림 5-10]과 같이 데이터 보호, 모바일 스팸 방지, 유해정보 차단 범주로 나누어진다.

[그림 5－10] 콘텐츠 보안 요구사항 분석



각각의 범주별 보안요구사항을 분석하여 <표 5-7>과 같이 구성하였다.

<표 5－7> 콘텐츠 보안 요구사항 분석

분 류		세부 요구 사항
데이터 보호	저장매체 접속통제	- 스마트폰↔업무PC 접속 및 데이터 전송 통제 - 담당자에게 허가받은 저장매체만 스마트폰에 사용
	데이터 저장여부	- 기업 기밀 및 기술 콘텐츠는 자료저장을 통제 ※ 휘발성 메모리 저장만 가능. 불가피한 경우 파일은 암호화하여 임시 저장 후 삭제
	화면 캡처 방지	- 기업 기밀 및 기술 콘텐츠는 화면 캡처 방지
	분실 및 도난 대책	- 분실 및 도난 스마트폰에 대한 원격 삭제 기능 제공
모바일 스팸 방지		- 모바일 스팸(SMS, MMS) 필터링 기능 제공 - 스팸머 블랙 리스트 관리 · 스팸신고 기능 제공
유해정보 차단		- 미성년자 유해정보 접근 차단

나. 보안 대책

콘텐츠 보안 요구사항을 만족시키기 위한 기술적인 안전 대책은 <표 5-9>와 같다.

<표 5－8> 콘텐츠 보안 기술적 대책

분류		세부 보안 대책	시기별		
			단기	중기	장기
접속 관리 대책		- P2P, 웹하드 접속 금지	√		
		- 스마트폰-PC간 유무선 직접연결 차단	√		
		- 스마트폰-PC간 테더링 연결 차단	√		
		- 업무용 PC에 스마트폰용 매체(USB, microSD등) 제어 시스템 설치	√		
문서 보안 대책		- 첨부파일을 이미지화하여 보기만 가능	√		
		- 업무화면에 대한 화면캡처 방지	√		
		- 문서 DRM 적용	√		
		- 전송 문서 및 임시저장 문서 암호화	√		
		- 인가된 N-스크린을 통한 문서 유통을 위한 접근제어		√	
모바일 스팸 방지 대책	사용자	- 키워드 기반 모바일 스팸(SMS, MMS) 필터링	√		
		- 스팸 신고 기능 제공	√		
	통신사업자	- 스팸차단 및 스팸머 판별 / 관리 시스템 구축			√
		- 키워드 및 행위 기반 모바일 스팸 필터링		√	
		- 단위 시간당 최대 송신 가능 메시지 제한		√	
유해정보 차단 대책		- 유해정보 차단 앱 기본 설치 (단말기 실 사용자 별 유해정보 접근제어)	√		

1) 접속관리 대책

스마트폰을 이용한 P2P, 웹하드 접속을 단말에서 차단하는 기능을 제공하여야 한다. 스마트폰과 일반 PC간의 유무선 직접 연결을 통한 데이터 전송을 통제할 수 있어야 하고, 스마트폰과 PC간의 테더링(Tethering)[14] 연결을 차단하여야 한다. 또한, 업무용 PC에는 스마트폰용 저장매체(USB, microSD 등)에 대한 접근을 통제할 수 있는 기능이 제공되어야 한다.

2) 문서 보안 대책

14) 스마트폰이 무선모뎀이나 AP로 활용되어 인터넷을 이용할 수 있도록 하는 기능

중요문서 보호, 열람 이력 등을 관리하기 위해 DRM 기술을 기본적으로 적용하여야 한다. 기업용 및 행망용 모바일 오피스 서비스에서는 업무 관련 첨부된 파일은 단말에 저장되지 않도록 하며, 이미지 등 편집이 불가능한 형태로 변환하여 스트리밍 방식으로 이용자 단말로 전송되어야 한다. 스트리밍 방식으로 첨부파일을 확인하는 뷰어 프로그램을 지원하되, 세션 타이머 기능을 적용하여 자동으로 종료되도록 조치하여야 한다. 뷰어 프로그램은 동시에 복수의 자료를 열람할 수 없도록 기능을 제한하고, 프로그램 종료 시 임시 저장된 파일은 삭제하여야 한다.

업무 자료는 프린터 등을 통한 외부 출력이 불가능하여야 하고, 업무 화면에 대한 화면 캡처 기능이 방지되어야 한다. 모든 업무용 문서는 전송시 뿐만 아니라 스마트폰에 임시 저장 시에도 암호화 하고 메모리에 로딩 시에만 복호화 할 수 있어야 한다. 암호 알고리즘으로는 AES(128비트), ARIA(128비트) 또는 이상 수준의 알고리즘을 사용할 것을 권장한다.

3) 모바일 스팸 방지 대책

모바일 스팸 방지 하기 위해서는 사용자 단말에서 키워드 기반 모바일 스팸(SMS, MMS) 필터링과 스팸 신고 기능을 제공해야한다. 단말에 모바일 스팸 필터 앱을 기본 제공하여, 정의된 키워드 기반으로 모바일 스팸을 차단하고, 미처 처리 되지 못한 스팸은 사용자가 원터치로 이통사에 신고할 수 있는 기능을 메시지 수신 앱에 제공하도록 한다.

이통사는 키워드 및 행위 기반 모바일 스팸 관리 시스템을 구축하여, 모바일 스팸을 필터링하고 스패머 리스트를 작성하여 차단한다. 또한 단위 시간당 최대 송신 가능 메시지를 제한한다.

4) 유해정보 차단 대책

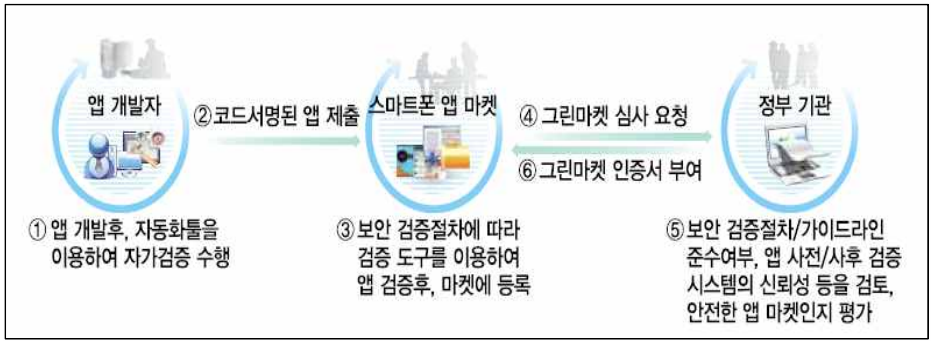
스마트폰 및 태블릿PC 등 스마트 기기 출하시 기본 설정으로 유해정보를 차단하는 애플리케이션을 설치하여, 단말기 실사용자가 미성년자일 경우 미성년자 유해정보(웹사이트, 동영상, 사진, 앱 등) 접근을 차단하도록 한다.

제 2 절 기술외적 측면에서의 보안대책

1. 안전한 애플리케이션 유통환경 보안 대책

안전한 애플리케이션 유통 환경 조성을 위해 스마트폰 애플리케이션에 대한 표준화된 검증 기준 및 절차를 마련해 이를 준수하도록 한다. 애플리케이션에 대한 보안 검증 절차 및 가이드라인을 준수하고 지속적인 사후 관리를 수행하는 마켓을 선정하여 신뢰할 수 있는 애플리케이션을 제공하는 마켓임을 정부가 인증하는 '그린 마켓 인증서'를 부여할 수 있다.

[그림 5－11] 안전한 스마트폰 애플리케이션 유통을 위한 그린 마켓 인증서



모바일 환경에서는 개인화된 기기의 사용으로 청소년 등에게 무분별한 유해정보의 확산이 우려된다. 따라서 청소년들에게 모바일 기기를 통해 전파되는 유해정보를 차단할 수 있는 애플리케이션을 개발 및 보급해야 하며 단말기 판매 시 기본적으로 유해정보를 차단할 수 있는 애플리케이션을 설치하도록 하여 이용자의 연령에 따라 작동할 수 있도록 하고, 유통 중인 스마트폰용 애플리케이션의 유해성, 선정성 및 프라이버시 침해 여부 등을 조사하는 모니터링 기능도 포함되어야 한다.

2. 법제도적 보안 대책

스마트폰 이용자의 증가로 인한 무선 네트워크 사용량 증가로 인해 무선 네트워크의 안전성을 확보해야 한다. 무선랜 보안 관리를 강화하기 위해 무선랜 보안 표준모델 개발, 보안인식 제고 및 무선랜 보안 법제의 개선이 필요하다. 무선랜 보안 운영 표준 모델에 기반한 공중 Wi-Fi존을 구축하는 한편 무선 AP의 초기 패스워드 변경 여부, 보안 설정 여부, 인증・암호화 지침 준수 여부를 현장 점검하는 등 사설 무선랜의 보안운영 상황을 주기적으로 점검・개선해야 한다.

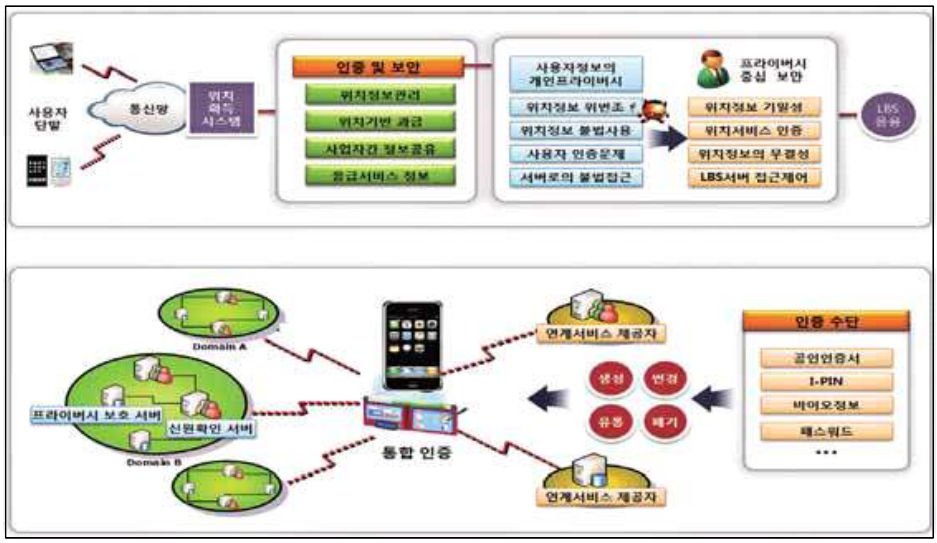
그리고 유・무선 연동구간에 대한 보안 연동체계를 구축하여 DDoS 대응시스템 등 기존 유선망 중심의 보안체계를 무선망・IP 백본망 연동구간까지 확대해야 한다.

모바일 인터넷이 활성화되면서 각종 신규 모바일 서비스가 등장하고 있다. 이러한 모바일 서비스에 대해 아래와 같은 보안 대책을 통해 이용자가 안심하고 이용할 수 있는 환경을 조성해야 한다.

첫째, 안전한 모바일 오피스 및 스마트워크 시스템 이용을 위한 단말, 시스템, 법적 문제 등 스마트 워크의 보안요소에 따른 정보보호 가이드라인을 개발하여 보급해야 한다. 이를 위해 모바일 오피스 사업자의 법적책임을 명확히 하고 이용자의 권익보호를 위한 관련 법제도를 개선해야 한다. 또한, 개인정보 제공 또는 위탁에 대한 통일된 법적 근거, 개인정보 유출 ・ 유실 시 배상 방안등에 대한 법적 기준을 마련하고 모바일 오피스를 구성하는 기술 및 제품의 보안성 평가 기준을 마련하는 인증제도를 개성해야 한다. 아울러, 보안성을 고려한 모바일 오피스 도입의 모범사례를 발굴・홍보하여 모바일 오피스 확산을 위한 기반 환경을 조성해야 한다.

둘째, 최근 이용율이 급증하고 있는 모바일 SNS의 보안을 강화해야 한다. 위치정보 등 개인정보 유출사고 사전방지를 위해 개인정보 수집 시 개인정보 침해 위험성 사전 고지 및 수집 동의 방안 등의 법제도를 마련해야 한다. 또한, 위치정보보호를 위해 개인 위치정보 자기제어시스템을 구축해야 한다. 이를 통해 위치정보 사업자나 위치기반 서비스 사업자로 하여금 이용자가 위치정보 사용내역을 확인할 수 있도록 하여 이용자의 자기 위치정보 통제권을 강화할 수 있도록 해야 한다.

[그림 5－12] 위치기반 프라이버시 보호



그리고 단축 URL을 악용한 악성코드 유포 및 피싱 사이트 유포를 예방하기 위해 국내외 단축 URL관련 정보 공유 체계를 구축해야 한다.

셋째, 모바일 클라우드 보안체계를 강화해야 한다. 이기종 플랫폼간 상호운용성 확보를 위한 통합인증체계를 구축하고 사고 원인 분석을 위한 '모바일 클라우드 포렌식' 기술을 개발하는 한편, 모바일 클라우드 서비스 유형 및 정보의 민감도에 따라 차등화된 보안 서비스를 제공하기 위한 표준 가이드라인을 마련해야 하며 도한, 모바일 클라우드 서비스 제공자간 신종 위협정보 공유와 신속 대응을 위한 침해대응체계가 마련되어야 한다.

3. 국내외 기업을 고려한 보안 대책 및 규제 방안

스마트 폰과 모바일 네트워크의 진화에 따라 기업의 스마트 워크 환경은 진화하고 있다. 기업의 스마트폰 사용자들이 메일 확인, 통화, 문서 리뷰 등 업무 용도로 스마트 폰을 활용하고 있으며, 업무 시스템의 생산성 및 효율성 증대를 위해, 스마트 워크 솔루션을 도입하는 기업도 늘고 있다.

그러나 스마트 워크 환경 구축을 추진하려는 많은 기업들이 가장 우려하는 것이 바로 보안 문제이다. 최근 해킹을 통한 고객 정보 유출 등 다양한 보안 사고가 발생함에 따라 새로운 디바이스의 보안 위협 요소에 대한 우려도 커지고 있다. 특히, 스마트 기기의 이동성과 개방성으로 인해 유선 및 PC 환경에 비해 다양한 위험 요소를 대비해야 함에 따라, 많은 기업이 모바일 오피스 환경 도입에 앞서 위험 요소 분석 및 대응책 마련에 집중해야 한다.

기업의 모바일 보안 사고 방지를 위해서는 디바이스, 네트워크, 콘텐츠, 사용자 인증의 4가지 영역에서의 보안을 강화해야 한다.

첫째, Device대한 보안에 있어 가장 큰 위협이 될 수 있는 모바일 기기의 분실 및 도난에 대해 [신고]->[잠금]->[백업]->[삭제]->[회수]->[해제]->[복원] 의 Process 구축이 필요하다. 특히 USB, SD카드, Bluetooth, 카메라 등 매체에 대한 제어 기능과 보안 프로그램 보호 기능을 통해 사용자 임의로 보안 기능을 무력화하는 행위를 방지할 수 있으며 안드로이드의 루팅(Rooting) 및 iOS의 탈옥(Jailbreak) 여부의 탐지를 통해 보안 사고를 예방할 수 있다.

둘째, Network에 대한 보안으로써 Wi-Fi 사용 시, 사내에 설치된 AP에 대한 불법 사용자의 접근 및 Rouge AP를 통한 정보 가로채기 등의 위협도 Wireless IPS를 모듈화하여 운용해야 한다.

셋째, Contents에 대한 보안으로 기업 구성원이 스마트 기기의 설치 및 실행 중인 애플리케이션 및 컨텐츠를 정기적으로 확인하는 것이 필요하다. 또한, 기업에서는 기업용 안티 말웨어(Anti Malware) 제품을 모듈화 하여, 악의적인 애플리케이션 발생 시 해당 애플리케이션을 블랙 리스트화 하고 악의적인 애플리케이션이 설치된 모바일 기기에 대해 원격에서 관리해 주는 다각적인 대응을 할 수 있다.

마지막으로 모바일 기기 인증 시 일정 횟수 이상 실패 후 화면 잠금, 강력한 비밀번호 설정 통제, 화면 잠금 정책 제어 등 기기를 분실하거나 도난당해도 무차별적인 비밀번호 입력을 통한 정보 유출을 막을 수 있다.

기업에서는 스마트 워크 도입 시, 보안 위협 요소를 지속적으로 분석하고, 기존 IT시스템과의 연관성 및 정책 등을 함께 고려해야 한다. 이렇게 구축된 모바일 보안 시스템은 기업 전체의 IT보안의 관점에서 통합적으로 관리되고, 함께 진화/발전시켜야 한다.

이와 더불어, 기업 구성원 개개인의 모바일 보안에 대한 관심 증대 및 보안의식 고취 역시 매우 중요하다. 최근에는 기업뿐만 아니라 개인 고객을 위한 보안 솔루션도 많이 출시되고 있으며, 가장 보편적인 모바일 백신 다운로드 등 개인 및 기업 정보를 보호하려는 개인의 노력이 더욱 중요하다.

4. 예방 중심 보안 대책 및 규제

스마트 사회로 발전하며 지금까지 경험하지 못했던 스마트 기기가 개발 활용되고 있으며, 개인, 기업, 정부 등 다양한 조직에서 이러한 스마트 기기를 활용하게 될 것이라는 것에 의심의 여지가 없다. 특히 정보의 이동이 국가 안에서 제한되는 것이 아닌 국경이 없이 매우 자유스럽게 넘나들게 되고 있다. 예를들면 스마트 기기를 이용하는 개인 또는 자동차의 위치정보가 세계 어디에서도 쉽게 알 수 있다. 이러한 새로운 스마트 기기는 기존에는 없었던 보안 및 안전 문제가 필연적으로 해결되어야 한다.

스마트 사회의 특징은 속도에 있다. 기존 산업 사회에서의 사고는 그 전파력이 그리 빠르지 않았으나, 스마트 사회의 사이버 사회는 그 전파력이 빛의 속도이다. 예를 들면 자동차의 취약점은 발견이 되어도 시간을 두고 리콜을 하여 수선을 하여도 된다. 그렇지만, 스마트 기기에 포함된 취약점은 발견이 되면 그 즉시 전세계 사용자에 영향을 받게 되고 피해가 생길 수 있게 된다. 또한 스마트 사회에서의 사이버 사고는 그 크기가 대형이다. 안드로이드 앱 몇 개가 500만 스마트 폰을 감염시켰다고 발표가 되었듯이 그 개수 및 피해액이 매우 천문학적 숫자가 되어 가고 있다.

이러한 스마트 기기의 특징으로 사이버 사고가 발생한 후에 백신을 만들거나 패치를 만들어 대처하는 사후 대처 방법 보다는 사이버 사고 예방 정책으로 가는 것이 옳다고 본다. 예를 들면 소프트웨어 개발 시 시큐어 코딩 표준 및 시큐어 소프트웨어 개발 방법론을 사용하도록 규제하여 소프트웨어 취약점을 개발 당시부터 방지할 수 있도록 하여야 하며, 또한 본 보고서에서 제안한 다양한 예방 정책을 활용하도록 하여야 한다. 규제는 없는 것이 좋으나, 스마트 사회, 스마트 환경으로 성공적으로 정착을 하기 전까지는 새로운 기술 개발과 적절한 규제가 매우 중요하다고 판단이 된다.

참 고 문 헌

국내 문헌

방송통신위원회 (2010), 『스마트 모바일 시큐리티 종합계획』.

정보통신정책연구원 (2010), 『모바일 애플리케이션의 동향과 전망』.

ZDNet Korea (2011), 『韓 스마트폰 가입자 2천만 돌파, 급성장 깜짝』.

디지털타임스 (2011).

한국정보화진흥원 (2010), 『국가정보화백서』.

일본 MIC 경제연구소 (2010), 『2010년 2월 조사자료』.

염흥렬, 장기헌 (2010), 『국내외 스마트폰 보안 표준화 동향 및 추진전략』, TTA Journal No 132, pp 54~60.

신호철 (2010), 『모바일 애플리케이션의 동향과 전망』, 제 22권 22호 통권 498호, 정보통신정책연구원.

한국인터넷진흥원 (2011),『스마트 모바일 강국 실현 2011년 상반기 스마트폰 이용실태조사』, 한국방송통신위원회.

해외 문헌

Forrester Research. (2010). “US Interactive Marketing Online Survey.”

IHS iSuppli Research. (2011). “By 2015 smarphones will rule the mobile planet.”

IHS iSuppli Research. (2011). “Media Tablet Forecast Increased as Apple’s Dominance Grow.”

Morgan Stanley Research. (2011). SAI.

Zokem LTD. (2010)

MCPC/Impress. (2010). “R&D joint survey conducted in September.”

Neilsen Company. (2010).

Pew Research. (2010). “Center’s internet & American Life Project.”
OVUM. (2010). “Mobile voice and data forecast pack: 2010-15.“.
Lookout. 2011

● 저 자 소 개 ●

최 진 영

· 서울대 컴퓨터공학과 졸업
· Drexel대 컴퓨터공학과 석사
· Pennsylvania대 컴퓨터정보과학과 박사
· 현 고려대학교 교수

방송통신정책연구 11-진흥-라-07

신규 모바일 기기 정보보호 연구

(Study on Security for New Mobile Devices)

2011년 12월 31일 인쇄
2011년 12월 31일 발행

발행인 방송통신위원회 위원장
발행처 방송통신위원회
서울특별시 종로구 세종로 20
TEL: 02-750-1114
E-mail: webmaster@kcc.go.kr
Homepage: www.kcc.go.kr
인 쇄 고려문화사