



## 스마트폰 정보보호

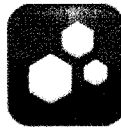
지난 10년 동안 인터넷은 우리 생활에 가히 혁명적인 영향을 끼쳐 왔습니다. 그러나 지난 10년이 인터넷 혁명의 시대였다고 한다면 향후 10년간은 모바일 혁명의 시대가 될 것이라고들 이야기합니다. 모바일 혁명 시대의 핵심에는 스마트폰이 자리하고 있습니다. 작년 이맘때쯤 국내에 아이폰이 도입되면서 국내에도 불붙기 시작한 스마트폰 광풍은 모든 비즈니스와 우리 생활에서 혁명을 예고하고 있습니다. 스마트폰 플랫폼 개발업체, 이동통신업체, 단말 기업체, 콘텐츠 개발자 등 다양한 플레이어들이 모바일 생태계 속에서 새로운 비즈니스 모델들을 탄생시키고 있고, 개인들의 생활 속에서도 스마트폰은 깊숙이 자리매김하고 있습니다. 이처럼 우리 산업 전반과 삶에 새로운 변화를 일으키고 있는 스마트폰은 과연 안전한 것일까요? 스마트폰은 다양한 앱이 구동될 수 있는 개방형 플랫폼을 가지고 있고, 앱스토어를 통해 누구

나 앱 사용자이자 제공자도 될 수 있습니다. 또한, 3G뿐만 아니라 Wi-Fi, Bluetooth, PC Sync 등 다양한 네트워킹 기능을 제공해 줍니다. 이러한 개방성을 바탕으로 스마트폰은 급격하게 성장하고 있지만 개방성은 악성코드 감염, 해킹, 프라이버시 침해 등 역기능이 발생할 수 있는 여건도 마련해 주고 있습니다.

실제로 스마트폰 해킹 사고는 국내외에서 빈번하게 발생되고 있고 그 피해가 증가하고 있는 추세입니다. 올 4월에 국내에서도 첫 스마트폰용 악성코드가 발견되었고, 전 세계적으로 524건의 모바일 악성코드가 발견되었습니다. 이처럼 스마트폰 해킹은 현실화되어 우리를 위협하고 있습니다. 본 특집에서는 스마트폰 보안과 관련한 정부의 정책방향, 보안위협과 사례, 프라이버시 이슈, 보안시장 전망, 국내외 표준화 동향, 전문인력 양성계획 등을 살펴보도록 하겠습니다.



# IT Expert Interview



정현철 | TTA 사이버보안 PG503 의장, KISA 융합보호R&D팀 팀장



## Q1 스마트폰의 개념은 무엇이며 일반 피쳐폰과 차별화되는 특징들은 무엇이 있습니까?

피쳐폰(기능폰, Feature Phone)은 휴대폰에 카메라와 MP3 플레이어 등의 부가 기능이 내장되면서 일반 휴대폰에 비해 특색있는 휴대폰을 말합니다. 이에 반해 똑똑한(Smart) 휴대폰인 스마트폰은 개방성을 가장 큰 특징으로 하고 있고 세부적으로 아래와 같은 차별화된 특징을 가집니다.

먼저, OS측면에서 범용 OS(General Purpose Operating System)를 사용하여 피쳐폰의 실시간 운영체제(RealTime Operating System)와 차별화됩니다. 스마트폰의 범용 OS는 다양한 응용프로그램들이 구동될 수 있는 환경을 제공해 주는 개방형 OS인 반면에 피쳐폰의 실시간 운영체제는 제조사에서 제공되는 기능에 특화되어 있어 추가적인 응용 프로그램이 구동될 수 없는 폐쇄형 OS입니다.

둘째, 응용프로그램과 콘텐츠를 자유롭게 설치하고 삭제할 수 있습니다. 애플 앱스토어에는 30만 개, 구글 안드로이드 마켓에는 10만 개 가량의 앱이 존재합니다. 피쳐폰에서는 통신사에서 제공한 앱만을 사용할 수 있었지만, 스마트폰은 사용자가 자유롭게 선택하여 설치할 수 있습니다.

셋째, 응용프로그램의 양방향성도 스마트폰의 중요한 특징 중의 하나일 것입니다. 피쳐폰의 응용프로그램들은 이동통신사 또는 이동통신사와 계약관계를 맺은 CP(Content Provider)들에 의해서만 제공되는 폐쇄형이었습니다. 하지만, 스마트폰은 프로그램 개발자나 개인 누구나 앱을 만들어서 앱스토어를 통해 배포할 수 있습니다. 즉, 개인도 앱의 소비자인 동시에 공급자가 될 수 있는 환경입니다.



**Q2 스마트폰에서 다양한 기능 및 응용서비스들이 활용되고 있는데, 보안 관련 문제점들은 어떤 것들이 있는지 설명 부탁드립니다.**

스마트폰은 Wi-Fi, 3G/4G, Bluetooth, PC Sync 등 다양한 채널을 통해 다른 네트워크 또는 장비와 연결되어 응용프로그램 및 정보가 공유되는 환경을 제공하고 있습니다. 또한, 스마트폰의 가장 큰 특징인 개방성은 공급자와 소비자 간의 유기적인 생태계를 조성하여 스마트폰 이용의 폭발적인 증가를 이끌었지만, 보안 관점에서는 상당히 큰 취약점이 될 수도 있습니다. 다양한 네트워크 접점을 가지고 있고, 개방형 OS 구조이며, 누구나 앱을 만들어 올릴 수 있고, 사용자들이 앱을 자유롭게 설치할 수 있는 환경은 해킹이나 악성 코드 감염에 더할 나위 없이 좋은 환경을 제공해 줍니다. 공격자는 악성 코드를 삽입한 앱을 앱스토어에 업로드 함으로써 악성 코드를 유포할 수도 있으며, 사용자는 Bluetooth를 통해 자신도 모르게 악성 코드에 감염될 수도 있습니

다. 그리고 스마트폰은 소형기기이며 이동성이 있어 분실의 위험도 큼니다.

또한 스마트폰 안에는 전화번호부, 통화내역, 사적인 사진이나 동영상, 사내 메일서버와 연동된 이메일, 비즈니스 일정관리, 모바일 banking 정보, 증권거래 정보 등 다양한 개인정보와 금융정보, 그리고 고객정보들이 집약되어 있습니다.

해킹, 악성 코드 감염 또는 분실 등을 통해 스마트폰 안에 저장되어 있거나 전송되는 정보들이 유출되거나 위·변조될 수 있습니다. 특히, PC에 비해 스마트폰에 저장된 정보들이 사적인 내용이 많아 프라이버시 침해가 심각할 수 있고, 스마트폰에 악성 코드 감염후 스팸 전화 등을 통해 전화요금 폭탄을 당할 수도 있어 PC에 비해 훨씬 큰 피해를 당할 수 있습니다.



### Q3 스마트폰 보안 사고에 대한 구체적인 사례와 이용자 및 정부 차원에서의 대응방안을 말씀해 주신다면...

대기업에 다니는 A씨는 얼마전 회식자리에서 스마트폰을 잃어버렸는데, 최근에 진행하고 프로젝트 관련 이메일과 기밀문서들이 스마트폰에 저장되어 있어 이 정보가 경쟁회사로 유출되지 않을까 노심초사하고 있습니다.

몇 달 전 스마트폰을 구입한 대학생 B양은 월말 휴대전화요금 통지서를 보고 놀라움을 금치 못했습니다. 국제통화료와 데이터 이용료가 무려 수백만 원이 청구되었기 때문입니다. 대학생 B양은 몇 주 전에 모바일 게임을 설치한 이후, 배터리가 빨리 방전되고 가끔 통화가 끊기는 현상이 있었지만 대수롭지 않게 생각했었습니다.

위의 2가지 시나리오는 가상으로 만들어 본 것이지만 우리 주변에 충분히 일어날 수 있는 시나리오이며 이미 유사한 사고가 발생되고 있습니다.

지난 2009년 11월에는 아이폰(iPhone)에서 동작하는 웜(Worm)이 최초로 발견되어 주요 보안 사이트들이 일제히 보도했습니다. 국내에서도 지난 4월, '트래드다이얼'이라는 스마트폰용 악성코드가 국내 최초로 발견되었습니다. 이 악성코드는 윈도우즈 모바일 운영체제를 사용하는 155명의 스마트폰 사용자들을 감염시켜 사용자 몰래 국제전화를 걸었습니다.

또한, 얼마전 11월에는 빠른 전파력을 가진 스마트

폰 악성코드가 중국에서 100만여 대의 스마트폰을 감염시켜 국내 상륙을 걱정하는 등 스마트폰 보안사고가 현실화되어 가고 있습니다. 전 세계 모바일 악성코드 발견 누적 건수는 2009년 상반기에 이미 524건이 발견되어 전년 대비 크게 증가하고 있습니다(출처: Smobilesystems, 2009.6).

스마트폰 보안사고를 예방하기 위해서 스마트폰 이용자들은 신뢰할 수 없는 사이트에서 의심스러운 애플리케이션을 다운로드 받지 말아야 합니다. 검증된 애플리케이션을 결정할 때 다른 사용자들의 사용후기도 참고할 수 있습니다. 또한, 분실에 대비하여 반드시 패스워드를 설정하고, 소위 탈옥이라고 하는 스마트폰 플랫폼의 구조를 임의로 변경하지 않아야 합니다.

정부에서는 기존의 유선 위주의 인터넷 정보보호 대책을 보완해 모바일 환경으로의 네트워크 진화와 개방형 구조를 가진 스마트폰의 특성을 반영한 보안정책을 마련할 필요가 있습니다. 뿐만 아니라 스마트폰을 정보시스템으로 보지 않고 단순 전화기로 여길 수 있는 일반인들을 대상으로 스마트폰의 보안에 대한 인식을 제고하는 노력도 필요하겠습니다. 마지막으로 점차 지능화·고도화될 것으로 예상되는 스마트폰 보안사고에 대비하여 스마트폰 보안 핵심원천기술을 확보해야 할 것입니다.



**Q4 스마트폰에서의 정보보호 관련 국내외 표준 활동 현황과 향후 국제표준화 대응 방향에 대한 설명을 부탁드립니다.**

국내 표준화 활동을 살펴보면, 스마트폰 응용에 대한 보안 표준으로 TTA 정보보호기술위원회 산하의 ‘응용보안 및 평가인증 프로젝트그룹’에서 스마트폰 등 모바일 개인 단말을 업무에 활용하는 조직을 위한 보안 지침을 정의하는 ‘조직에서의 모바일 개인 단말의 보안 지침’과 모바일 단말의 통신 상황에 대한 인지를 통해 보안 설정을 재구성하는 ‘모바일 통신 단말용 상황인지형 보안재구성 프레임워크’에 대한 표준화가 진행되고 있습니다.

국제 표준화 활동으로는 ITU-T SG17(보안 연구 그룹) Q.6(유비쿼터스 보안 분과)에서 중국측의 제안으로 스마트폰에서의 보안 이슈에 대한 전반적인 사항을 다루는 X.msec-6(Security aspects of mobile phones)에 대

한 표준화가 진행 중에 있습니다. X.msec-6에 대한 문서 개발은 우리나라 및 일본에서도 적극적인 의견 개진 및 논의를 통해서 진행되고 있습니다. 또한 동일 분과에서 모바일 단말의 통신 상황에 대한 인지를 통해 보안 설정을 재구성하는 X.msec-5(Security requirements and mechanism for reconfiguration of mobile device with multiple communication interfaces)에 대한 표준화도 진행 중에 있으며, 이 아이템은 국내 표준화와 동시 추진 중에 있습니다.

이렇듯 스마트폰 보안에 대한 표준화가 국내외에서 진행되고 있지만, 스마트폰의 성장세와 고려할 때 아직까지 부족한 실정입니다.

따라서, 스마트폰에서 악성행위를 방지하고 보안수단에 대한 평가 기준을 제시하는 스마트폰 플랫폼 보안 기준을 표준화하는 등 보다 적극적으로 스마트폰 보안 이슈에 대해 국제 표준화 선점 노력이 필요합니다.

### Q5 스마트폰을 포함한 모바일 보안 분야에서 보안기 술력을 확보하기 위한 전략 및 전문 인력양성 계획에 대해 말씀해 주신다면...

모바일 보안 분야의 국내 기술력 확보를 위해서는 기존 인력의 심화 교육 및 재교육 등을 통한 전문인력 양성이 시급합니다. 일반 애플리케이션 개발자를 대상으로 모바일 보안 분야 심화 단기과정 개설을 통한 융·복합형 개발자 양성 및 대학생을 대상으로 기초 실무과정 개설을 통한 미래 전문가 양성이 필요합니다.

정부와 KISA에서는 중소 무선인터넷업체 직원을 대상으로 모바일 웹, 애플리케이션, 네트워크, 정보보호 등을 포괄하는 '무선인터넷 활성화 및 보안 교육 과정'을 개설하여 교육하고 있습니다. 또한 전국의 대학정보보호 동아리 학생들을 대상으로 무선인터넷 보안 관련 교육을 실시하고 있으며, 이외에도 일반인들의 모바일 보안에 관한 인식 제고를 위한 온라인 교육 과정을 서비스할 계획입니다.

2011년에는 정부의 예산 지원 하에 모바일 보안 분야의 고용계약형 석사과정이 KAIST, 동국대, 아주대 등 3개 대학에 처음으로 개설될 예정입니다. 이 석사과정은 모바일 보안 관련 기업과 대학이 컨소시엄을 구성해 공동으로 교과과정을 기획하고 교육을 진행하며, 이 석사과정의 학생은 교육 수수료 후 석사학위를 취득하고, 컨소시엄에 참여한 모바일 보안 관련 기업에 취업하게 됩니다.

### Q6 스마트폰 전반적인 국내외 시장현황 및 향후 전망에 대해 간략히 말씀해 주신다면...

전 세계 무선인터넷 이용량은 2009년 대비 148% 증가하였고(출처: Quantcast), 국내 스마트폰 사용자도 2009년 말 75만에서 2010년 5월 197만으로 5개월여 만에 2.6배 증가하는 등 무선 인터넷과 스마트폰 사용은 급격히 증가하고 있습니다. 스마트폰의 보급 확산과 함께 모바일 SNS, 모바일 상거래, 모바일 뱅킹, 모바일 오피스, 모바일 검색, 위치기반 서비스, 모바일 게임 등 다양한 모바일 비즈니스가 새롭게 부각되고 있습니다. 많은 시장 전문가들은 모바일 콘텐츠, 단말기 부가서비스 등 분야별로 발전속도나 성장률은 다를 수 있지만 전체 시장규모는 5년 후 약 5배 이상 성장할 것으로 예측하고 있습니다.

모바일 혁명의 시대에 떠오르고 있는 많은 비즈니스 영역 중 보안도 주목을 받고 있습니다. 계정정보, 금융정보, 전화번호부, 사진/동영상, 이메일 등 스마트폰을 통해 수많은 민감한 정보들이 저장·전송되고 있으며, 스마트폰용 악성코드가 이미 524건 발견되기도 했습니다. 이처럼 모바일 보안의 중요성이 인식되고 있는 환경에서 모바일 보안 시장은 모바일 바이러스 백신, 모바일 결제 보안 솔루션, 모바일 콘텐츠 보호 솔루션, 암호화 제품, 모바일 사용자 인증 제품 등 다양한 보안 솔루션들이 출시되고, 시장규모도 확대될 것으로 예측하고 있습니다. 연간 7,800억 원에 불과한 국내 정보보호 시장을 모바일 혁명의 시대를 기회로 시장을 확대하고 해외에까지 진출할 수 있는 기회로 삼을 필요가 있습니다. **TTA**