디지털산업정보학회 논문지 제7권 제1호-2011년 3월

안전한 스마트폰 애플리케이션 개발을 위한 보안 고려사항 및 국산암호알고리즘 적용 방안 연구

김 지 연* · 전 웅 렬** · 이 영 숙*** · 김 미 주**** · 정 현 철**** · 원 동 호*****

A Study on Security Consideration and Utilization of Domestic Encryption Algorithm for Developing Secure Smartphone Applications

Kim, Jee Yeon · Jeon, Woong Ryul · Lee, Young Sook · Kim, Mi Joo · Jung, Hyun Chul · Won, Dong Ho

〈Abstract〉

A smartphone is a mobile phone that offers more advanced computing ability and connectivity than a contemporary basic feature phone. Unlike feature phone, a smartphone allows the user to install and run more advanced applications based on a specific platform. Smartphones run complete operating system software providing a platform for application developers. A smartphone will become the default computing method for many point activities in the not-too-distant future, such as e-mail, online shopping, gaming, and even video entertainment. For smartphone that contains sensitive information and access the Internet, security is a major issue. In the 1980s, security issues were hardly noticed; however, security is a major issue for users today, which includes smart phones. Because security is much more difficult to address once deployment and implementation are underway, it should be considered from the beginning.

Recently our government recognized the importance of smartphone security and published several safety tips for using the smartphone. However, theses tips are user-oriented measures. Maintaining the security of a smartphone involves the active participation of the user. Although it is a important users understand and take full advantage of the facilities afforded by smarphone, it is more important developers distribute the secure smartphone application through the market.

In this paper we describe some scenarios in which user is invaded his/her privacy by smartphone stolen, lost, misplaced or infected with virus. Then we suggest the security considerations for securing smartphone applications in respect with developers. We also suggest the methods applying domestic encryption algorithms such as SEED, HIGHT and ARIA in developing secure applications. This suggested security considerations may be used by developers as well as users (especially organizations) interested in enhancing security to related security incidents for current and future use of smartphones.

Key Words : Smartphone Security, Security Consideration, Cryptography, Smartphone Threats, Domestic Encryption Algorithm, Secure Smartphone Applications

* KISA ISMS, PIMS 인증 심사원(제1저자)
** 성균관대 전기전자및컴퓨터공학과 박사수료
*** 호원대학교 사이버수사경찰학부 조교수
**** 한국인터넷진흥원 연구개발팀
***** 성균관대 정보통신공학부 교수(교신저자)

Ⅰ. 서론

스마트폰은 뛰어난 연산능력을 바탕으로 여러 가지 다양한 서비스를 사용자에게 제공할 수 있다. 이때 스마트폰이 제공할 수 있는 다양한 서비스의 근원은 바로 애플리케이션(이하 어플)이다. 스마트폰 어플은 PC와 달리 크기도 작고 개발시간도 짧아 저렴한 가격으로 온라인에서 판매되고 있기 때문에 전 세계 수많은 개발자들이 참여하여 다양한 기능의 응용 프로그램을 배포하고 있다. 이로 인해 기존 피처폰에서는 제공하기 힘들었던 서비스를 사용자에게 제공할 수 있게 되었다. 다양한 어플의 예로 실시간으로 버스 노선을 검색하고, 도착 시간을 확인하는 어플, 악기 연주 어플, 운동량 계산 어플 등이 있다. 최근에는 스마트폰을 이용한 뱅킹 서비스, 결제 서비스 등이 시작되면서 금융거래에도 스마트폰이 사용되고 있다.

그러나 이러한 어플을 이용하여 개인 정보와 고객 정보 등의 중요 정보가 스마트폰에 집약되면서 스마트폰 보안에 대한 우려 역시 증가하고 있다[1, 2 ,3]. 스마트폰은 모바일 기기로 PC나 노트북에 비해 크기도 작아 분실/도난의 위협이 더 높을 수 있는 반면 능력의 제한으로 PC에 비해 보안 기술 적용에 제한이 있을 수 있다. 스마트폰의 분실/도난은 스마트폰에 저장 또는 이를 이용하여 관리되는 중요정보의 노출의 위협으로 바로 연계될 수 있으며 더 나아가 이러한 정보의 악용으로 인한 피해도 발생할 수 있다.

스마트폰에 대한 보안 인식이 확산되면서 정부는 이를 예방하기 위한 각종 안전 수칙을 발표하였다[4, 5, 6]. 국내에서 공개된 안전수칙들을 사용자를 대상으로 하고 있다. 물론 스마트폰을 안전하게 사용하기 위해서는 사용자 스스로 이러한 안전 수칙을 지키고 스마트폰에서 기본으로 제공하는 여러 가지 보안 기술을 사용하는 것도 중요하지만, 스마트폰 어플 개발자들이 보안 기술을 적용한 보안 어플을 개발하여 배포하는 것이 보다 중요하다고 할 수 있다. 그러나 국내외적으로 사용자나 특정 분야나 특정 플랫폼을 고려한 가이드라인이나 수칙은 발표되고 있으나 어플 개발자를 위한 보안 가이드라인은 전무한 상황이다. 본 논문은 여러 분야에서 활용될 수 있는 어플을 개발할 때 안전한 스마트폰 사용에 기여하기 위해 고려해야 할 보안 고려 사항을 제시하도록 한다.

본 논문은 구성은 다음과 같다. 논문의 2장에서는 실생활에서 스마트폰 어플 사용 시의 보안 위협 시나리오를 살펴보고, 3장에서는 국내외 발표된 스마트폰 보안과 관련된 수칙 및 가이드라인을 살펴보도록 한다. 4장에서는 개발자가 안전한 어플을 개발할 때, 참조할 수 있는 보안 측면의 고려사항을 제시하도록 한다. 더블어 5장에서는 개발자들이 스마트폰에서의 안전한 애플리케이션 개발할 때 SEED, HIGHT, ARIA와 같은 국산 암호 알고리즘을 활용할 수 있는 방안을 제시하도록 하고 마지막 결론 부분에서는 본 논문의 활용 방안을 논의하도록 한다.

Ⅱ. 실생활에서의 스마트폰 보안 위협 시나리오

현재 애플의 앱스토어와 안드로이드 마켓은 현재 전 세계적으로 가장 많은 어플을 보유하고 있다[7, 8]. 또한 이러한 앱스토어와 마켓 등을 통해 매일 매일 새로운 어플들이 출현하고 있다[9, 10, 11, 12, 13]. 이러한 수많은 어플들 중, 보안 기능이 필요한 어플은 크게 중요정보(개인정보, 고객정보 등)를 저장・관리하는 어플과 특정 서비스를 위해 중요정보를 전송하는 어플로 구분될 수 있다. 저장・관리하는 어플은 저장 및 관리하는 정보에 따라 다시 문서 관리, 계정 관리, 보안카드/신용카드/개인정보 관리 및 사진/동영상 관리로 구분된다. 전송에 관한 어플은 이용되는 서비스에 따라 결제 서비스, 뱅킹 서비스, 웹 검색, 이메일, 문자/메신저로 구분할 수 있다.

<표 1>은 스마트폰 어플의 구분 기준과 어플의 예를 나타낸다. <표 1>의 어플 예는 애플의 앱스토어와 안드로이드 마켓에 등록된 어플 중 보안 기능이 고려되어야

구분		응용 프로그램
저장/관리	문서 관리	Quick Office, Think Free, 한컴뷰어, Documentstogo 등
	계정 관리	Password Master, Accouts book, Moxier Wallet, Egg Wallet 등
	보안카드/신용카드/개인정보 관리	OneLock, kWallet, 보안카드 관리툴, iSCard, Seccure Card, 메모금고 등
	사진/동영상 관리	시크릿 앱, PrivateCamera, Pic Lock 등
전송	결제 서비스	INIpay Mobile 등
	뱅킹 서비스	농협NH스마트뱅킹, KB스타뱅킹, 신한 스마트폰 S뱅크, 우리은행 스마트뱅킹 등
	웹 검색	사파리, 돌핀, xScope 등
	이메일	Gmail, MailDroid, K-9 Mail 등
	문자/메신저	Secret SMS, 비밀SMS, Crypto Your Life, 카카오톡, iEncrypt 등

할 일부 어플을 선정하였다.

선정된 어플에의 보안 기능 탑재 여부를 분석한 결과, 90년대 초, 중반의 인터넷의 상황과 마찬가지로 현재 출시되는 어플 중 보안 기능이 탑재된 어플은 일부에 불과하였다.

저장·관리하는 어플에 비해 결제 서비스와 뱅킹 서비스를 포함하는 전송 어플이 보다 보안 기능이 고려되어 개발되었다고 할 수 있으며 저장·관리하는 어플에서는 문서나 사진/동영상 어플보다는 뱅킹 서비스와 연계되는 계정 관리, 보안카드/신용카드/개인정보 관리 어플이 암호 기술 등의 보안 기능 탑재율이 높았다.

만약 사용자가 보안 기능이 탑재되지 않은 어플을 사용한다면 많은 위협에 노출되게 될 것이다. 본 장에서는 스마트폰 사용자가 실제 겪을 수 있는 보안 위협을 시나리오 형식으로 살펴보도록 한다.

시나리오는 물리적으로 스마트폰을 분실/도난으로 인해 발생할 수 있는 피해와 악성코드 감염 등으로 인한 피해로 구분한다.

2.1 물리적 분실/도난으로 인한 피해

물리적 분실/도난으로 인해 1차적으로는 사용자의 개인정보가 유출될 수 있으며, 이 때 공격자가 유출된 정보를 악용하여 좀 더 심각한 범죄를 저지를 수 있다.

1. 정보 유출

스마트폰을 획득한 공격자는 우선 사용자의 위치정보를 획득할 수 있다. 예를 들어 Cardio Trainer와 같은 운동 관련 어플들은 사용자의 운동경로와 시간을 저장하고 있다. 만약 이러한 사용자 정보가 평문으로 저장되어 있다면 공격자는 손쉽게 운동할 때 사용자가 평소 어느 시점에 어떠한 경로로 움직이는 지를 가늠할 수 있다. 또한 사용자가 대중교통과 관련된 어플을 사용하는 경우 자주 이용하는 공공노선 정보도 획득할 수 있다. 또한 공격자는 스마트폰을 통해 사용자의 다양한 개인정보를 획득할 수 있다. 예를 들어 사용자가 스마트폰을 이용하여 네이버, 다음, 네이트 등의 대표적인 모바일 웹페이지를 이용할 경우 아이디와 비밀번호를 일일이 입력하는 것이 PC 환경에 비해 번거로울 수 있어 이러한 정보들을 스마트폰에 저장한다. 이러한 비밀번호가 암호화되지 않고 평문의 형태로 저장될 경우 스마트폰을 획득한 공격자는 쉽게 사용자의 비밀번호를 알 수 있으며, 이를 통해 웹페이지에 접속하여 사용자 대신, 메일 등을 확인할 수 있다. 최근 이슈가 되고 있는 트위터의 경우에도 이와 같은 위협이 발생할 수 있다. 따라서 공격자는 트위터 어플을 사용하여 사용자의 정보를 알 수 있고 이를 이용하여 사용자를 사칭할 수도 있다. 이 외에도 스마트폰에 저장되어 있는 사용자의 주소록, 이메일 주소, 문자 메시지 등이 암호화되지 않고 저장될 경우 공격자에게 유출되는 것은 순식간에 벌어질 수 있다.

만약 업무에 활용되고 있는 스마트폰이 분실된다면, 공격자는 평문으로 저장된 다양한 이메일과 사내 기밀문서를 손쉽게 열람할 수 있다. 이러한 사내 기밀문서에는 프로젝트 기획안이 있을 수 있다. 이 경우 프로젝트 기획안이 경쟁 회사로 유출되어 비즈니스에 심각한 타격을 입을 수 있다.

2. 정보의 악용

스마트폰 분실은 단순히 개인정보의 유출로 끝나는 것이 아니라, 공격자로 인해 획득한 사용자 개인정보가 악용될 수 있다.

우선 공격자는 사용자의 위치정보를 바탕으로 강력범죄에 악용할 수 있다. 초등학생이 스마트폰을 사용하는 경우에는 초등학생의 이동 동선을 미리 파악한 후 이를 바탕으로 유괴, 납치 등을 시도할 수 있다.

또한 미리 획득한 사용자의 웹 관련 정보를 바탕으로 온라인에서 사용자를 가장할 수 있다. 이는 최근 문제가 되고 있는 메신저 피싱과 유사하다. 트위터에서 사용자를 가장한 공격자는 임의의 대상에게 300만원만 빌려달라는 식의 피싱을 시도할 수 있으며, 개인정보 및 주소록, 이메일 목록 등을 통해 도박 사이트 가입 및 활동, 스팸 전송, 피싱 등 다양한 범죄에 활용할 수 있다.

A사 직원의 스마트폰에 최근 공지된 프로젝트 입찰가격과 관련된 정보가 유출된다면 공격자는 경쟁사 B에 그 정보를 판매하고 B회사는 그 정보보다 낮은 입찰가격을 통해 불공정한 거래를 진행할 수 있다. 그 외에도 A사의 회사 기밀, 마케팅 정보, 차기 신제품 계획 등을 확인하여 자사의 비즈니스 전략에 반영하는 것도 가능하다.

3. 스마트폰의 악의적인 사용

만약 사용자가 스마트폰에 대해 기본적인 잠금 기능을 설정하지 않는다면 공격자는 분실된 또는 불법으로 획득한 사용자의 스마트폰을 임의로 사용할 수 있다. 예를 들어 공격자가 국제전화, 060 등의 상업적 전화를 무단으로 사용하여 사용자에 대한 불법 과금을 유발할 수 있다.

2.2 악성코드 감염 등으로 인한 피해

공격자는 어플, 무선 네트워크 등 다양한 경로를 통해 악성코드를 전파할 수 있고 사용자는 어플 설치, 어플 업데이트, 플랫폼 업데이트, 웹 콘텐츠 다운로드 등을 통해 악성코드에 감염될 수 있다. 안드로이드 마켓 같은 경우에는 어플의 검수 과정이 없기 때문에 개발자가 어플로 가장한 악성코드를 유포할 가능성이 높다.

1. 정보 유출

공격자는 자신이 유포한 악성코드를 이용하여 스마트폰에 평문의 형태로 사용자의 저장된 사진, 메시지 및 기타 개인정보를 자신의 기기로 빼낼 수 있다. 이 경우 사용자는 이를 인식하지 못한다. 또한 공격자는 사용자 몰래 악성코드에 감염된 스마트폰의 블루투스 등의 무선네트워크를 통해 다른 모바일 기기와의 통신을 지속적으로 시도하여 배터리가 소모되도록 할 수 있다. 이러한 배터리 소모 공격으로 인해 사용자는 스마트폰의 사용에 제약을 받는다.

공격자는 악성코드를 이용하여 사용자에게 금전적인 손실을 유발할 수도 있다. 이러한 과금 유발 공격은 2007년 러시아에서 발생한 레드브라우저(RedBrowser)가 그 예이다. 이 레드브라우저는 스마트폰이 발송하는 문자메시지를 일반 문자메시지가 아닌 프리미엄 서비스로 변경함으로써 과금을 유발하였다.

마지막으로 공격자는 악성코드를 통해 사용자의 스마트폰에 저장된 임의의 데이터를 삭제하거나 설정을 변경하여 사용자에게 피해를 줄 수 있다.

2. 정보 악용

공격자는 획득한 사용자 개인정보를 악용하거나 악의

적으로 유포할 수 있다. 스마트폰에 담겨있는 사진, 문자 등의 사생활을 악의적인 의도로 유포함으로써 사용자의 사생활에 막대한 피해를 야기할 수 있다. 또한 미리 획득한 사용자의 웹 관련 정보를 바탕으로 온라인에서 사용자를 가장할 수 있다.

Ⅲ. 스마트폰 보안을 위한 가이드라인 동향

본 장에서는 국내외 스마트폰에 관련된 각종 가이드라인을 살펴보도록 한다. 앞에서도 언급하였지만 현재 발표된 가이드라인은 스마트폰 이용자 또는 특정 서비스를 대상으로 한다.

3.1 국내 동향

1. 방송통신위원회의 스마트폰 정보보호 “이용자 10대 안전수칙”

국내에서 2009년 말부터 폭발적으로 스마트폰 사용이 증가하고 이와 관련된 보안위협의 가능성이 커짐에 따라 2010년 2월, 방송통신위원회는 스마트폰 이용자들을 위한 스마트폰 정보보호 “이용자 10대 안전수칙”을 발표하였다[4].

이 안전수칙은 방송통신위원회와 KISA를 비롯, ETRI, 이동 3사(KT, SK텔레콤, LG텔레콤), 제조3사(삼성전자, LG전자, 팬택), 백신6사(안철수연구소, 하우리, 바이러스체이서, 이스트소프트, 잉카인터넷, NHN) 등의 관련 전문가들이 참여하여 마련한 것이다.

스마트폰 정보보호 “이용자 10대 안전수칙”은 스마트폰 관련 악성코드 감염, 침해사고 발생 등의 보안위협을 사전에 예방하고, 이상증상 발생 시 피해를 최소화 할 수 있도록 다음의 대응내용을 포함하고 있다.

① 의심스러운 애플리케이션 다운로드하지 않기
② 신뢰할 수 없는 사이트 방문하지 않기
③ 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제하기
④ 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호 변경하기
⑤ 블루투스 기능 등 무선 인터페이스는 사용 시에만 켜놓기
⑥ 이상증상이 지속될 경우 악성코드 감염여부 확인하기
⑦ 다운로드한 파일은 바이러스 유무를 검사한 후 사용하기
⑧ PC에도 백신프로그램을 설치하고 정기적으로 바이러스 검사하기
⑨ 스마트폰 플랫폼의 구조를 임의로 변경하지 않기
⑩ 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트 하기

2. 금융감독원의 “스마트폰 전자금융서비스 안전대책” 및 “스마트폰 금융거래 10계명 및 안내서”

2011년 1월 금융감독원은 금융회사 및 금융정보보호전문기관의 전문가로 구성된 “스마트폰 전자금융서비스 안전대책 마련 T/F”를 함께 마련한 “스마트폰 전자금융서비스 안전대책”을 발표하였다[5].

이 안전대책을 스마트폰을 이용한 전자금융서비스의 혁신을 지원하면서 예상되는 잠재적인 보안위협으로부터 고객정보를 보호하고 안전하게 스마트폰 기반 전자금융거래를 하도록 적정한 보안 기준을 마련하는 데 중점을 두었다. 안전대책은 전자금융거래 부분, 기술적 침해대응 부분, 취약점 모니터링 부분 등 3개 분야로 나누어 수립되었다.

또한 금융감독원은 “스마트폰 전자금융서비스 안전대책”에 이어, 2011년 2월에는 금융소비자들이 스마트폰 전자금융거래를 보다 안전하게 이용하기 위해 지켜야할 “스마트폰 금융거래 10계명 및 안내서”를 마련하였다[6]. 이는 과거 다수의 전자금융사고가 이용자의 금융정보 관

리 소홀로 인해 발생한 점을 감안한 것이다.

금융감독원의 금융거래 10계명은 스마트폰의 도난·분실·해킹 등으로 인해 발생할 수 있는 전자금융사고 예방을 위해 사용자들의 유의사항을 포함하고 있다.

3.2 국외 동향

1. NIST의 "휴대폰 및 PDA 보안에 관한 가이드라인"

2008년 10월 NIST가 발간한 권고안(SP800-128)으로 휴대폰과 PDA 장치에 대한 전반적인 사항과 이러한 장치의 취급에 관해 보안과 관련된 조직의 결정에 대한 정보를 제공한다[14]. 즉, 이 권고안은 휴대폰과 PDA 장치의 사용과 관련된 위협과 기술적 위험 그리고 이러한 위협과 위험에 대한 대응 방안을 상세히 설명하고 있다. 이 권고안은 조직은 휴대폰과 PDA 장치와 관련된 보안을 개선하고 사고를 감소할 수 있도록 하는 것에 목적을 둔다.

본 권고안이 다루고 있는 위협 및 위험은 분실, 도난, 비인가된 접근, 악성코드, 스팸, 도청, 복제 등을 포함하고 있다. 이에 대한 대응책에 대해서는 사용자 측면의 대책과 조직 측면의 대책으로 구분하고 있다.

사용자 측면의 대책은 사용하고 있는 휴대폰과 PDA 장치에 대한 물리적인 통제를 유지하고 장치에서 제공하는 사용자 인증 기능을 이용하며 데이터를 백업하고 장치에 민감한 데이터 저장을 자제, 무선 인터페이스 사용 자제, 백신의 사용 등을 포함하고 있다.

조직 측면의 대책은 이동 장치 사용에 대한 보안 정책의 설정, 배치 및 운영 계획의 마련, 위험 평가 및 관리 수행, 훈련을 통한 보안 인식 확산, 설정 통제 및 관리 수행을 포함하고 있다.

NIST의 권고안은 개발자의 애플리케이션 개발에 대한 사항은 포함하고 있지 않다.

2. MS의 "개발자를 스마트폰 애플리케이션 보안 및 코드 서명 모델에 대한 실용적인 가이드"

2003년 2월에 공개된 본 가이드는 윈도우즈 모바일기반의 스마트폰 애플리케이션을 안전하게 배포하기 위한 코드 서명 기법 기반의 보안 모델을 소개하고 있다[15].

코드 서명 기법은 데이터 콘텐츠의 출처를 인증하기 위한 보안 기법으로 특정 보안 수준 이하의 애플리케이션이 무분별하게 배포되는 것을 방지하기 위함이다. MS의 가이드는 윈도우즈 모바일 기반의 스마트폰 애플리케이션 개발자가 코드 서명을 위한 인증서를 획득하는 방법, 획득한 인증서를 이용하여 코드 서명을 생성하는 방법 등을 포함하고 있다.

Ⅳ. 안전한 스마트폰 어플 개발시 보안 권고사항

본 절에서는 안전한 스마트폰 어플 개발시의 보안 고려사항을 저장·관리 어플과 전송 어플로 구분하여 제시하도록 한다.

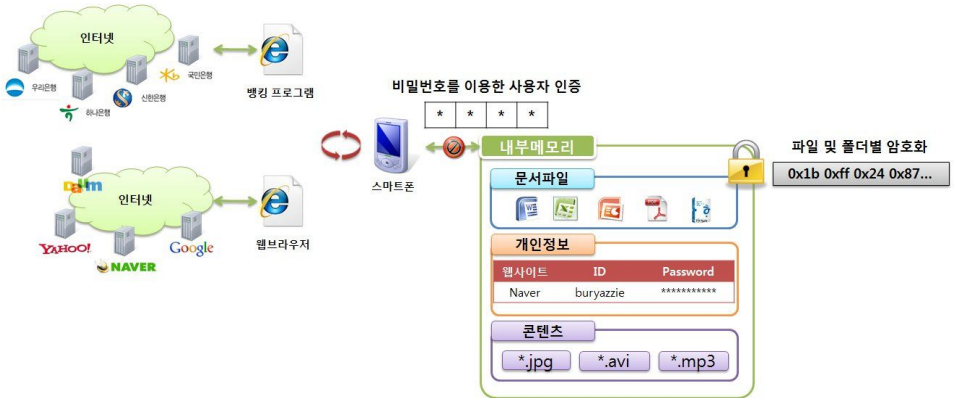
4.1 안전한 저장·관리 어플 개발시 운영 및 기술 권고사항

■ 암호화

- o 스마트폰의 분실 및 도난 시 저장된 데이터의 기밀성을 유지하기 위해서는 암호화 적용을 권고한다.
- o 이 경우 암호화가 적용되는 정보의 크기, 스마트폰의 연산 능력 등을 참고하여 암호 적용 대상과 범위를 고려해야 한다.

중요 정보를 저장/관리하는 어플에서는 저장되는 정보의 기밀성을 보장하기 위해 암호알고리즘 사용을 기본적으로 고려하여 적용하여야 한다. 일반적으로 암호알고리즘을 적용할 때에는 스마트폰의 연산능력을 고려하여 암호화 적용 대상과 적용 범위를 신중하게 선택해야 한다.

예를 들어 사진 및 동영상과 같은 경우에는 일반 문서보다 용량이 크므로 암호화를 강제적으로 적용하는 것



<그림 1> 보안기술이 적용된 저장·관리 어플

보다는 사용자가 원하는 경우 선택적으로 적용할 수 있게 하거나 폴더보다는 파일 단위의 암호화를 유도함으로써 스마트폰의 연산 부담을 덜 수 있다. 반면 계정관리, 보안카드/신용카드/개인정보 관리 어플의 경우에는 개인의 민감한 정보들을 다루기 때문에 암호화를 필수적으로 적용할 것을 권고한다. 활용하고자 하는 알고리즘의 종류와 키 길이 및 유효기간에 대한 사항은 KISA의 "암호이용안내서[16]"를 참조한다. 안내서는 SEED, HAS-160, KCDSA 등의 국산 암호 알고리즘을 포함해 보안강도에 따라 선택 가능한 암호 알고리즘의 종류와 키 길이, 유효기간을 소개한다. 예를 들어 대칭키 암호 알고리즘을 적용하여 2015년까지 사용한다면 안내서에 따라 보안강도는 112비트 이상이며, SEED, ARIA-128/192/256을 선택하면 된다.

만약 중요 정보 저장/관리 어플이 암호화를 지원하지 않는다면 사용자는 분실 및 도난 시의 저장된 정보의 유출에 대비하여 스마트폰의 잠김 기능을 이용하는 것도 하나의 방법이다. 또한 스마트폰 자체 내에서 제공하는 삭제 프로그램 또는 원격 삭제 프로그램 등을 사용하여 공격자에게 정보 유출을 방지할 수 있다. 일부 스마트폰은 사용자가 패스워드를 특정 횟수 이상 잘못 입력할 경우 저장된 데이터를 삭제하도록 설정하는 기능을 제공한다.

■ 완전 삭제

0 어플을 통해 저장/관리되었던 중요 정보를 삭제하거나 또는 해당 어플을 제거할 때 중요 정보가 스마트폰에 남지 않도록 하기 위해 완전삭제 기술 적용을 권고한다.

어플을 통해 저장/관리되는 정보는 스마트폰의 플래시 메모리에 저장된다. 플래시 메모리는 특성상 사용자가 어플을 통해 정보를 삭제하거나 또는 어플을 제거하더라도 실제로는 물리적 메모리에서 해당 정보가 삭제되는 것은 아니다. 플래시 메모리를 오래 사용하기 위해 여러 번 데이터를 삭제해야 하는 물리적인 삭제보다는 논리적인 삭제 방식을 일반적으로 선택하기 때문이다. 논리적인 삭제의 경우 메모리를 복구할 경우 주요 정보를 공격자가 획득할 수 있는 위험이 존재한다.

그러므로 개발자는 어플을 통해 저장/관리되었던 중요 정보가 삭제되거나 또는 해당 어플이 제거될 때 중요 정보가 스마트폰에 남지 않도록 하기 위해 완전삭제 기술 적용을 고려해야 한다.

따라서 계정관리 어플, 개인정보 관리 어플 등 사용자의 인증정보, 사용자의 금융정보를 담고 있는 어플은 해당 어플의 제거시 물리적으로도 완전히 삭제되는 와이핑 기술을 적용하는 방안을 반드시 고려할 것을 권고한다.

메모리에 잔존해있는 정보들은 잦은 덮어쓰기가 아니면 완전히 삭제되지 않고 남아있기 때문에 복구가 가능하다는 점을 주의해야 한다.

■ 접근제어

- 스마트폰의 분실 및 도난 시 어플 자체에 대한 접근을 통제할 수 있는 기술 적용을 권고한다.
- 비밀번호를 이용하여 접근 제어할 경우 안전성을 높이기 위해 비밀번호의 길이, 구성방법(숫자, 영소문자, 특수문자 등의 다양한 조합), 변경 주기, 입력 횟수의 제한 등을 고려한다.

스마트폰이 분실될 경우 공격자는 어플을 통해 저장/관리되는 정보에 접근할 수 있기 때문에 어플 자체에 대한 접근을 제어하는 것이 중요하다. 그러므로 개발자는 어플 자체에 대한 접근을 통제할 수 있는 기술 적용을 고려하여야 한다. 범용적으로 사용되는 비밀번호 방식을 적용할 경우 안전성을 높이기 위해 비밀번호의 길이, 구성방법(숫자, 영소문자, 특수문자 등의 다양한 조합), 변경 주기, 입력 횟수의 제한 등을 고려한다. 보다 자세한 사항은 "암호이용안내서" 제3장 패스워드 및 키 관리 방안의 내용을 참조할 수 있다.

사용자는 어플에 초기 설정된 비밀번호를 반드시 변경하도록 하여야 한다.

<그림 1>은 이러한 권고사항이 적용된 저장·관리 어플의 개념도를 보여준다.

4.2 안전한 전송 어플 개발시 운영 및 기술 권고사항

다음은 개발자가 안전한 전송 어플을 사용자에게 제공하기 위해 고려해야 할 운영 및 기술 권고사항이다. 전송 어플의 종류에 따라 다음의 권고사항을 선택적으로 고려할 수 있다. 전송 어플 중에서 수신된 정보를 저장 관리하는 기능을 제공한다면 앞에서 언급한 저장/관리 어플의 운영 및 기술 권고 사항을 따르도록 한다.

■ 암호화

- 전송되는 데이터의 기밀성을 유지하기 위해서는 암호화 적용을 권고한다.
- 이 경우 암호화가 적용되는 정보의 크기, 스마트폰의 연산 능력 등을 참고하여 암호 적용 대상과 범위를 고려해야 한다.

전송 어플에서는 전송되는 정보의 기밀성을 보장하기 위해 암호알고리즘 사용을 기본적으로 고려하여 적용하여야 한다. 일반적으로 암호알고리즘을 적용할 때에는 스마트폰의 연산능력을 고려하여 암호화 적용 대상과 적용 범위를 신중하게 선택해야 한다.

활용하고자 하는 알고리즘의 종류와 키 길이 및 유효기간에 대한 사항은 KISA의 "암호이용안내서[3]"를 참조한다.

전송 어플에서 전송되는 정보는 어플에 따라 다를 수 있다. 이 정보는 개인의 사적인 정보일 수도 있고 공인인증서 및 공인인증서 비밀번호, 신용카드 번호 및 신용카드 비밀번호, 결제 내역 등으로 노출될 경우 개인에게 직접적으로 금전적 피해를 주는 정보일 수도 있다. 따라서 전송되는 정보에는 반드시 암호화가 적용되어야 한다. 아울러 전송되는 정보는 이후에 스마트폰 내부에도 저장되므로 앞에서 제시한 저장·관리 어플에서의 운영 및 기술 권고사항을 참조하도록 한다.

■ 입력장치 보안

- 스마트폰을 통해 입력되는 ID와 비밀번호 등의 주요 정보의 기밀성을 유지하기 위해 입력 정보에의 암호화 적용 또는 입력 정보를 숨길 수 있는 기술을 사용할 것을 권고한다.

키보드 해킹은 사용자 몰래 사용자 PC에 설치된 악성코드를 이용하여 사용자가 키보드를 통해 입력하는 정보를 공격자에게 유출시키는 공격 기법이다. 이러한 키보드 해킹을 통해 사용자가 입력하는 개인정보, 비밀번호 등의 다양한 정보가 유출되고 이는 피싱, 명의도용 등의 2차 피해로 이어질 수 있다. PC 환경에서는 이러한 위협

에 대응하기 위해 키보드 보안 프로그램 또는 가상 키보드를 사용한다.

스마트폰 역시 이러한 위협이 존재할 수 있으므로 키패드를 통해 입력되는 내용을 암호화하거나 가상의 키보드를 사용하여 입력하는 내용을 숨기는 기술 등이 적용이 필요하다.

■ SSL 통신

- 브라우저와 웹서버간의 안전한 통신을 위해 SSL 통신 프로토콜의 사용을 권고한다.

결제 서비스, 뱅킹 서비스, 웹 검색 관련 어플들은 외부 서버와 통신할 때 안전한 통신환경을 구축하기 위해 SSL 프로토콜 사용을 권장한다.

■ 기타

- 웹 검색 어플에서는 프라이버시 보호를 위해 캐시파일 형태로 스마트폰에 남는 사용자의 방문 기록을 완전 삭제할 수 있는 기술 적용을 권장한다.
- 전송 어플에는 일정 기간이 지나도록 사용자의 사용이 없거나 사용이 완료되면 프로그램이 종료되도록 할 것을 권장한다.
- 사용자는 이메일 또는 문자/메신저를 통해 전송되는 파일 내에 악성코드가 포함되어 있을 수 있다는 것을 주지하고 있어야 한다.

V. 국산 암호 알고리즘 적용 방안

본 절에서는 개발자들이 스마트폰에서의 안전한 애플리케이션 개발할 때 SEED, HIGHT, ARIA와 같은 국산 암호 알고리즘을 활용할 수 있는 방안을 제시하도록 한다. 적용하는 방법은 크게 두 가지로 구분할 수 있다. 첫 번째는 암호 알고리즘을 라이브러리 형태로 구현하여 모바일 기기에 삽입하는 방법이고, 두 번째 방법은 실행 프로그램 형태로 구현하여 모바일 기기에 설치하는 방법이다.

5.1 라이브러리 형태로 구현하여 삽입

라이브러리는 소프트웨어를 만들 때 사용되는 클래스나 서브루틴의 모임을 말한다. 여기에서 클래스란 동일한 목적을 지니는 함수들이 모임이며, 일반적으로 객체지향 프로그래밍에서 기능은 함수로 구현된다. 즉, 암호 라이브러리란, 암호 기능을 구현한 함수들의 집합으로 볼 수 있다.

라이브러리는 크게 정적 라이브러리와 동적 라이브러리로 구분할 수 있는데, 정적 라이브러리는 컴파일러가 소스 파일을 컴파일 할 때 참조하는 프로그램 모듈인 반면 동적 라이브러리는 프로그램이 수행 도중 해당 모듈이 필요할 때 호출하여 사용하는 라이브러리를 의미한다. 정적 라이브러리는 컴파일러가 소스 파일을 컴파일 할 때 라이브러리를 포함시키기 때문에 실행속도는 동적 라이브러리에 비해 빠르나 프로그램의 크기가 커진다는 단점이 있다. 최근 프로그램들은 이미 용량이 거대하고, 다양한 기능을 포함해야 하기 때문에 정적 라이브러리보다는 동적 라이브러리를 많이 사용한다.

국산 암호 알고리즘을 활용할 수 있는 방안 중의 하나는 바로 동적 라이브러리 형태로 알고리즘을 구현하여 스마트폰에 삽입하는 것이다. 이렇게 암호 라이브러리가 스마트폰에 삽입되어 있으면 추후 개발자가 암호기능을 갖는 어플을 개발하고자 할 때 다른 추가적인 프로그램 설치 없이 암호 알고리즘을 자유롭게 사용할 수 있다는 장점이 있다.

스마트폰에 암호 라이브러리를 구현하여 삽입하는 방법은 플랫폼 제조사와 협의하여 생산 단계에서부터 국산 암호 라이브러리를 포함하여 스마트폰을 출시하는 것과 사용자가 출시된 스마트폰에 직접 암호 라이브러리를 추가하는 것이 있다.

보다 이상적인 방법은 전자이나 이는 플랫폼 제조사와의 긴밀한 협의가 필요하며 플랫폼 제조사의 정책에 따라 암호 알고리즘의 수용 여부가 결정된다.

반면 후자의 방법은 사용자 입장에서는 좀 더 자유로

울 수 있다. 현재 안드로이드 플랫폼에는 공개 라이브러리인 OpenSSL의 설치가 가능하고 OpenSSL에는 국산 암호 알고리즘인 SEED가 포함되어 있기 때문에, 암호 기능을 갖는 어플을 개발하고자 하는 개발자에게 OpenSSL의 설치 후 사용을 권장하면 된다. 그러나 라이브러리의 추가가 모든 플랫폼에서 가능한 것은 아니다. 아이폰의 경우 애플사가 제공하는 함수 사용만이 가능하기 때문에 사용자가 직접 라이브러리를 추가하는 것은 불가능하다.

5.2 실행 프로그램 형태로 구현하여 삽입

국산 암호 알고리즘을 추가하는 또 다른 방법은 프로그램 형태로 구현하는 것이다. 예를 들어, PC로 인터넷 뱅킹을 사용하는 경우를 살펴보자. 사용자는 인터넷 뱅킹을 사용하기 위해 몇몇 Active X를 다운받아 설치해야 한다. 이렇게 설치된 Active X는 유기적으로 동작하면서 서로에게 필요한 기능을 제공한다. 예를 들어 사용자가 로그인을 하는 경우 우선 키보드 보안 프로그램이 활성화되면서 사용자가 입력하는 공인인증서 비밀번호가 암호화된다. 암호화된 비밀번호는 공인인증서를 관리하는 모듈로 전달되고, 공인인증서를 관리하는 모듈은 사용자가 입력한 비밀번호로부터 사용자의 개인키를 추출하여 인터넷 뱅킹 서비스를 제공하게 된다.

라이브러리 형태로 암호 알고리즘을 추가하는 것이 불가능하다면, 이처럼 Active X의 프로그램 형태로 개발하여 배포하는 방법도 고려할 수 있다. 하지만 이러한 방법은 크게 세 가지 단점을 지닌다.

첫째, 스마트폰은 PC에 비해 계산능력이 많이 부족하기 때문에, 성능의 저하를 야기할 수 있다.

둘째, 라이브러리 형태로 배포하는 것에 비해 확장성이 떨어진다. 라이브러리 형태로 배포하는 경우 개발자는 암호 알고리즘을 사용하는 어플 개발 시, 플랫폼 개발환경을 준수하면서 함수만 호출하면 기능을 사용할 수 있으나 프로그램 형태로 개발하는 경우 개발자는 플랫폼 개발환경 뿐만 아니라, 암호 알고리즘 사용을 위한 프로그램 간의 통신까지 신경을 써야 한다. 따라서 개발자는 다양한 입출력 인자와 형태, 조건 등을 고려해서 프로그래밍을 해야 한다.

셋째, 사용자가 보안을 선택적으로 적용하게 된다. 사용자가 암호 알고리즘을 포함하고 있는 프로그램을 설치하지 않으면 암호 알고리즘이 보급되지 않는다. 라이브러리는 협의를 통해 생산과정에서 포함시키거나, 또는 플랫폼 업데이트 형식으로 암호 알고리즘의 설치를 강제할 수 있다. 그러나 프로그램 형태로 배포하는 것은 사용자에게 선택과 관련한 전권을 부여하는 것으로 사용자가 선택하지 않으면 암호 알고리즘은 보급이 되지 않는다.

따라서 국산 암호 알고리즘의 보급을 위한 이상적인 방법은 라이브러리 형태로 구현하여 보급하는 것이다.

VI. 결론

본 논문에서는 스마트폰 어플 구현 동향 및 이러한 어플이 보안 기능 없이 실생활에 사용될 수 있는 위협 시나리오를 분석하였다. 그리고 이러한 위협에 대응하기 위해 기존 가이드가 스마트폰 이용자 측면에서의 보안 고려 사항들을 제시하고 있는 반면 본 논문에서는 스마트폰 어플 개발자 측면에서 안전한 어플을 개발할 때의 보안 고려 사항을 제시하였다. 더불어 SEED 등의 국산 암호 알고리즘을 보안 기능이 탑재된 어플 개발시 적용할 수 있는 방안을 설명하였다. 본 논문에서 제시한 사항은 스마트폰 개발자뿐만 아니라 사용자 및 스마트폰 기반 서비스를 제공하는 관리자에게 유용한 지침서가 될 것으로 기대한다.

참고문헌

[1] 이영숙, 김지연, "스마트폰 보안 기술 분석," 디지털산업정보학회 논문지, 제6권, 제2호, 2010, pp. 91-105.

[2] 강동호, 김기영, "개방형 모바일 환경에서 스마트폰 보안기술," 한국정보보호학회지, 제19권, 5호, 2009, pp. 21-28.

[3] 이정우, 박대우, "휴대폰과 스마트폰의 모바일 포렌식 추출방법 연구," 디지털산업정보학회 논문지, 제6권, 제3호, 2010, pp. 79-89.

[4] 방송통신위원회, "스마트폰 정보보호 이용자 10대 안전 수칙," http://www.kisa.or.kr, 2010. 2.

[5] 금융감독원, "스마트폰 전자금융서비스 안전대책," http://www.fss.or.kr/, 2010. 1.

[6] 금융감독원, "스마트폰 금융거래 10계명," http://www.fss.or.kr/, 2011. 2.

[7] 아이폰 앱스토어, www.apple.com/iphone/apps-for-iphone/

[8] 안드로이드 마켓, www.android.com/market/

[9] 허재두, 성정식, 손종무, 이현정, 정영식, 백의현, "모바일 앱스토어 기술동향," 전자통신동향분석, 제25권, 제3호, 2010.

[10] 한컴뷰어, www.haansoft.com

[11] Quickoffice, www.quickoffice.com/quickoffice_connect_suite_iphone/

[12] INIpay Mobile, www.inicis.com/

[13] Secret SMS, handheld.softpedia.com/

[14] NIST, "Guidelines on Cell Phone and PDA Security(SP 800-124)," http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf, 2008. 10.

[15] MS, "A Practical Guide to the Smartphone Application Security and Code Signing Model for Developers," http://msdn.microsoft.com/en-us/library/ms839377.aspx, 2003. 2.

[16] 한국인터넷진흥원, "암호이용안내서," http://www.kisa.or.kr, 2008. 7.

■ 저자소개 ■

김 지 연
Kim, Jee Yeon

2007년 9월~현재
KISA ISMS, PIMS 인증 심사원
1996년 12월~2007년 1월
한국정보보호진흥원 선임연구원
2006년 2월 성균관대학교
전기전자및컴퓨터공학과(공학박사)
2007년 2월 성균관대학교 정보공학과(공학석사)
1995년 2월 성균관대학교 정보공학과(공학사)

관심분야 : 암호프로토콜 암호이론,
정보보호관리체계 인증
E-mail : jeeyeonkim@paran.com

전 웅 렬
Jeon, Woong Ryul

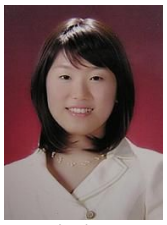
2008년~현재
성균관대학교
전기전자컴퓨터공학과 박사수료
2008년 2월 성균관대학교
전기전자컴퓨터공학과 (공학석사)
2006년 2월 성균관대학교 컴퓨터공학과(공학사)

관심분야 : 보안성평가, 스마트폰 보안
E-mail : wrjeon@security.re.kr

이 영 숙
Lee, Young Sook

2009년 3월~현재
호원대학교 사이버수사경찰학부
조교수
2010년 3월~현재
호원대학교 기획조정처 경영평가
실장
2008년 8월 성균관대학교 컴퓨터공학과
(공학박사)
2005년 2월 성균관대학교 정보보호학과
(공학석사)
1987년 2월 성균관대학교 정보공학과(공학사)

관심분야 : 암호프로토콜, 네트워크 보안,
스마트폰 보안, 디지털포렌식
E-mail : ysooklee@howon.ac.kr



김 미 주
Kim, Mi Joo

2008년 4월~현재 한국인터넷진흥원 연구개발팀 주임연구원
2008년 9월~현재 순천향대학교 정보보호학과 박사과정
2008년 2월 순천향대학교 정보보호학과 (공학석사)
2006년 2월 순천향대학교 정보보호학과 (공학사)

관심분야 : 정보보호, 표준화
E-mail : mijoo.kim@kisa.or.kr

정 현 철
Jung, Hyun Chul

1996년 7월~현재 한국인터넷진흥원 연구개발팀 팀장
2006년 9월~현재 고려대학교 정보보호대학원 박사과정
1999년 8월 광운대학교 전자계산학과(석사)
1996년 2월 서울시립대학교 전산통계학과(학사)

관심분야 : 침해사고대응, 융합서비스보안, 네트워크보안, 컴퓨터포렌식
E-mail : hcjung@kisa.or.kr

원 동 호
Won, Dong Ho

1976년~1988년 성균관대학교 전자공학과 (학사, 석사, 박사)
1978년~1980년 한국전자통신연구원 전임연구원
1995년~1997년 성균관대학교 교학처장
1997년~1998년 정보화추진위원회 자문위원 (발령 정보화추진위원회 위원장 국무총리)
1999년~2001년 성균관대학교 정보통신대학원 원장
2002년~2003년 한국정보보호학회 회장
2002년~2004년 성균관대학교 연구처장
2005년~현 재 정보보호인증기술연구소 소장
2009년~현 재 성균관대학교 BK21 사업단장

관심분야 : 암호이론, 정보이론, 정보보호
E-mail : dhwon@security.re.kr

논문접수일 : 2011년 1월 31일
수 정 일 : 2011년 2월 11일(1차), 2월 27일(2차)
게재확정일 : 2011년 3월 5일