글 정대근(에이쓰리시큐리티 보안기술팀장)
사진 SHUTTERSTOCK

스마트 금융 확대와 모바일 보안 플랫폼 강화 흐름 분석

스마트 기기 기반 금융서비스가 증가하고 SNS의 금융 인프라 구축이 늘면서 모바일 보안에 대한 관심이 커지고 있다. 모바일 기기는 그 특성상 소유자의 의지에 따라 안전 여부가 결정되는데, 이제는 개발 프로세스에서도 보안성 검토가 필요하다.

최근 IT업계의 가장 큰 이슈는 빅데이터와 IoT(사물인터넷)라는 두 줄기로 나뉜다. 그중 IoT는 IPv6를 기반으로 어디서든지 네트워크를 활용할 수 있도록 개념을 정립한 유비쿼터스와 그 맥락을 같이하고 있다. 사물인터넷은 현재 실생활과 밀접하게 연관되어 아주 활발한 연구가 이뤄지는 분야며 많은 단체들이 협업을 통해 실용화 및 편의성 증진을 위해 노력하고 있다. 사물인터넷을 추진하는 데 있어 가장 필요한 것은 모바일 환경이다.

국내 이동통신 가입자 중 스마트폰 가입자가 2012년 3분기에 이미 70%에 육박했다. 지금은 분명 더 늘어났을 것이다. 모바일 기기는 사용자에게 편의성과 휴대성, 기동성을 제공하는데 최근 금융서비스와 결합하면서 활용도가 더욱 높아졌다. 앞으로 사용자들은 모바일 기기를 통해 이동 중에도 SNS 금융서비스를 이용할 수 있게 됐다. 그저 사진을 올리고 친구들과 댓글을 주고받는 형태에서 한층 더 진화한 것이다. 기업 입장에서 모바일 기기는 인적, 물적 네트워크의 사용을 극대화할 수 있는 최적의 단말기다.

하지만 모바일 환경의 실용화가 빠르게 진행되고 사용자 접근성이 지속적으로 발전한 반면, 모바일 환경의 보안성에 대해서는 준비가 다소 부족했던 것이 현실이다. 모바일 기기를 통해 화폐가 오갈 수 있는 요즘 상황에서 보안 위협에 노출된다는 것은 작은 불편을 감수하는 것을 넘어 재산상의 피해로 연결될 수 있기 때문에 과거와는 달리 각별한 주의가 필요하다.

최근 공공기관에서 모바일 사용이 확대되면서 보안 · 통제를 위한 솔루션 도입도 증가하고 있다. 산업인력공단, 중앙선관위, 기술보증기금 등의 정부 산하기관 및 공공기관에서 모바일 보안 솔루션에 대한 관심과 수요가 늘어나고 있는 상황이다.

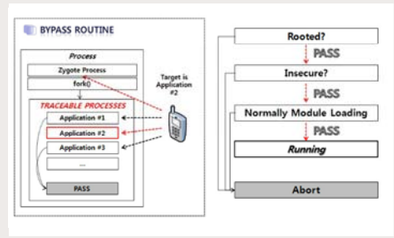
모바일 보안에 관한 새로운 시도들

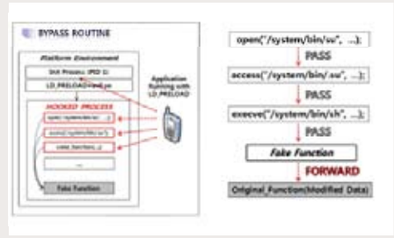
최근 모바일 플랫폼 업체들이 기업 고객 관련 서비스를 강화하면서 보안 업체들도 바빠졌다. 과거 모바일 보안은 기기관리 측면에서만 논의되었다. 카메라에 보안 스티커를 붙이는 등 기본적인 기능을 막는 용도였다. 하지만 최근에는 모바일 애플리케이션 관리, 모바일 가상화, 암호화 통신 기술 등이 적극적으로 활용된다. 일례로 구글은 지난 6월 열린 구글 I/O컨퍼런스에서 모바일 보안 요소들을 지원하는 '안드로이드 포 워크' 플랫폼을 공개했다. 기업용과 개인용 앱을 구분해 보안성을 높이고 사용자 편의성을 보장한다는 취지다.

회사 내에 모바일 보안 구역을 설정하자는 움직임도 있다. 단말기가 보안 구역 안에 들어오면 카메라나 녹음기, 블루투스, 테더링 등을 자동으로 차단하는 것이다. 이를 위해 무선신호에 의한 위치기반 방식과 물리보안 시스템 연동 방식 등이 연구되고 있다. 이렇듯 모바일 보안에 관해 다양한 새로운 시도들이 진행되고 있다.

소유자의 성향에 따라 보안 환경 변한다

최근 한 보안 솔루션 업체에서 주최한 보안 관리전략 세미나 'SMS Security Management Strategy 2014'에서 '모바일 금융거래 애플리케이션의 보안대책 우회기법'이라는 세션이 열렸다. 모바일 애플리케이션의 실행 흐름 조작을 통해 보안대책을 우회하는 기법이다.





위 그림은 임의의 시스템 콜을 사용한 모바일 앱 실행 플로 변조를 설명한 것이다. ptrace()

시스템 콜을 사용하여 특정 시스템 콜의 실행 전 인자 정보 조작이나 실행 후 반환값 조작을 통해 모바일 앱 실행에 조작을 가하는 방법이다. 위의 그림은 임의의 함수 후킹을 통한 방법으로 LD_PRELOAD 환경 변수를 init프로세스에 적용하여 특정 라이브러리의 함수 로직에 대해 조작을 가하는 방법이다. 일반적으로 시스템 콜이라는 단어와 함수라는 단어를 혼재해 사용하기도 하지만, 시스템콜이란 kernel에 직접 interrupt를 일으키는 구조이고 함수는 그보다 상위에 포진되어 라이브러리 형태로 존재하는 형태이기에 구분지어서 설명하기도 한다.

LD_PRELOAD에 대해 별도의 Shared Object를 제작하고 SSL-Strip를 구현하는 방법을 시연했다. 관련 내용이 아래 블로그에 정리되어 있으니 관심이 있는 사람은 참고하면 좋겠다.

*모바일 애플리케이션 분석 방법에 관한 고찰 : http://teamcrak.tistory.com/377

*zygote 프로세스에 LD_PRELOAD 환경 변수 삽입하기 : http://teamcrak.tistory.com/378

시연에서 표현하고자 했던 문제의 본질은 루팅Rooting이나 탈옥JailBreak된 모바일 기기를 사용하는 것은 사용자 자신이 보안을 스스로 포기하는 것과 같다는 메시지를 전하기 위해서였다. 모바일 기기는 소유자의 오너십에 따라 보안 환경이 결정된다. 제조사에서 만든 보안 환경을 사용자가 자의적으로 수정해 사용하는 경우가 있기 때문에 개개인의 인식 전환이 우선 필요하다.

위 그림은 안드로이드 애플리케이션 실행 변조 툴(A.K.A ardb)을 표현한 것이다. 프로그램 및 디바이스 변조 탐지를 우회하기 위한 목적으로 시작되었기 때문에 툴 이름이 Android Rooting Detection By Pass Tool로 설정되어 있다. 이 툴은 -p 옵션과 -f 옵션을 사용하도록 되어 있다. -p옵션은 package 이름을 인자로 받게 되며 -f 옵션은 일반 console상에서 실행할 프로그램 경로 정보를 인자로 받는다. 위의 경우 com.testbank 프로그램이 실행되면 이를 추적하고, fork() 시스템 콜 실행을 탐지해 그 결과값을 -1로 조작하도록 한 화면이다. 루팅 탐지 케이스의 경우 특정 경로의 파일이 존재하거나 실행되는 경우를 루팅되었다고 판별하기도 하고, 탐지 루틴을 Shered object 안에 구현 후 해당 object의 내부 함수를 실행해 판별하기도 한다.

모바일 설계자에게 필요한 것은?

모바일 애플리케이션이나 플랫폼을 설계하는 측에서는 최근 루팅이나 탈옥에 대해 많은 고민을 하고 있다. 이에 대해 개발자들은 다음과 같은 사항을 고려해야 한다. 우선 구축하기 전 설계 단계에서 보안성 검토 프로세스를 추가하여 가능한 모든 기능에 대해 보안성을 검증해야 한다. 사용자 관점에서 보안 취약점으로 인해 사용자 개인 정보 유출과 같은 상황으로 발전할 경우 금전적인 손실이 있을 수 있고, 2차 범죄로 이어질 가능성도 존재한다. 아울러 서비스 관점에서는 신뢰도 하락으로 이어진다. 현재 많은 개발 프로세스에서 보안성 검토 프로세스는 거의 수행되고 있지 않으며 보안을 위해 첨가된 기능이 오히려 악용되는 사례도 있을 수 있으므로 이에 대한 대책이 절실하다.

또한 암호화와 보안을 오해하는 사례가 적지 않다. 가장 많은 경우가 종단 간 통신 암호화에 대해 오해하고 있는 부분이다. 암호화 통신은 중간자 공격Man In The Middle Attack과 같은 공격으로부터 보안성을 강화하기 위한 대책일 뿐인데 암호화를 했으니 안전하다고 인식하는 경우가 있다. 하지만 이것은 환경을 고려하지 않은 것이다. 암호화 통신 환경은 통신 관점에서 보면 안전하지만 클라이언트 관점에서 보면 루팅이나 탈옥과 같은 환경에서는 안전하지 않다고 해석할 수 있다.

최근 모바일 보안 솔루션 관련 핫 이슈는?

최근 개발된 모바일 보안 플랫폼 중 가장 이슈가 된 것은 삼성의 녹스Knox다. 안드로이드 4.3 이상 운영체제에 최적화되어 있다고 알려져 있다. 녹스를 다른 플랫폼과 같은 방법을 사용하여 루팅할 경우 하드웨어에 적재된 값인 워런티Warrenty 비트가 변경되고 사후 제조사가 A/S를 보증하지 않도록 되어 있다. 이에 대해 외국의 지오핫이라는 해커가 플랫폼 자체의 취약점만으로 루팅을 할 수 있다고 주장하기도 했다.

공인인증서 유심 내장 스마트 인증 서비스도 주목받고 있다. 파일 형태의 공인인증서 유출 가능성을 효과적으로 차단하지만 한편으로는 메모리 접근 형태로 공인인증서를 유출할 수 있다는 가능성이 제기된 바 있다. KAIST 정보보호대학원은 유심에 들어간 공인인증서를 탈취하는 것은 어렵지만 스마트 인증 서비스를 이용하는 과정 전반에 보안이 고려되지 않았다고 지적했다. 이에 대해 통신3사는 "스마트 인증은 유심에서 공인인증서를 빼가는 것을 방지하는 서비스이며 PC에서 스마트폰으로 옮기는 과정에서 나타는 취약점은 특수한 상황에서 일어나는 공격으로 일어나기 희박하다"고 밝혔다.

모바일 보안은 지속적으로 최신 공격 형태를 분석하여 이에 대해 대처하는 것이 중요하다. 공격 기법은 날이 갈수록 지능화되어가고 있는데 이에 대응하는 방법이 발전하지 않는다면 기존의 방어체계를 우회하는 방법이 계속 발견될 것이다. 또한 패킹Packing, 난독화Obfuscation 등을 통한 방법도 있다. 패킹이나 난독화를 통해 모든 보안 문제가 완전히 해결되지는 않지만, 악의적인 목적을 가진 해커들의 분석을 어렵게 만드는 것도 모바일 보안 수준을 높이는 방법이 된다.

모바일 보안은 앞으로 어떤 방향성을 가질까. 우선 기술적 측면에서는 PC 보안 솔루션과 맥락을 같이할 것으로 보인다. 아울러 서비스 측면에서는 보안과 편의성은 반비례한다는 것이 지금까지의 속설이었다. 보안성을 높이면 사용자의 편의성이 줄어들고 반대로 편의성을 높이면 보안성이 저하된다는 지적이다. 앞으로 벤더사 입장에서 사용자의 편의성을 크게 저하시키지 않는 범위 내에서 자체적으로 보안성의 수준이 조정되거나, 법률적 최소 보안 요건(기존 소프트웨어의 기술적 보호 조치와 같은 법적 강제 항목)이 존재한다면 이에 따라 강제적으로 사용자의 편의성보다 보안성을 우선시하는 서비스가 등장할 것으로 보인다.