모바일 애플리케이션의 SSL Pinning 우회에 대한 대응방안 연구

신상길*
김문현 교수**
*성균관대학교 정보보호학과 석사과정
**성균관대학교 정보보호학과 교수 (교신저자)
e-mail : thanksto@skku.edu

A Study on countermeasures against Mobile Application's SSL Pinning bypass

Sang-Gil Shin*
*Dept. of Information Security, Sungkyunkwan University
**Professor, Dept. of Information Security, Sungkyunkwan University

요 약

스마트폰 애플리케이션의 종류가 다양해지고 사용 빈도수가 높아지는 만큼 정보보안에 대한 중요성도 나날이 증가하고 있다. 최근 기업, 금융기관들은 스마트폰 애플리케이션 서비스에서 사용자와 서버 간 통신 시 MITM 공격에 대비하기 위해 SSL Pinning 기술을 사용하고 있는데 본 연구에서는 이를 우회할 수 있는 방법을 소개하고 시연하며, 이에 대한 대응방안을 소개한다.

1. 서론

시간과 장소에 구애받지 않고 활발히 사용되고 있는 스마트폰은 만 6 세 이상 국민의 85%가 보유하고 있다.[1] 이러한 현상은 누구에게나 공개되어 있는 SDK(Software Development Kit)를 이용하여 자유롭게 애플리케이션을 개발/배포할 수 있기 때문이다. 이렇게 스마트폰이 보급되면서 은행이나 증권사 등의 금융사도 스마트폰 금융 애플리케이션을 제작· 배포하고 있는데, 2009 년 말 13,000 명에 불과하던 스마트폰 기반의 모바일뱅킹 가입자는 2016 년 기준으로 7 천만명을 돌파했다.[2]

이처럼 스마트폰 사용 빈도수가 높아지는 만큼 정보보안에 대한 중요성도 나날이 증가하고 있다. 통신 시 전송되는 개인정보, 금융정보, 기밀정보와 같은 민감 정보들이 송수신, 사용, 변환, 저장, 보관의 과정에서 어느 것 하나 소홀히 할 수가 없기 때문이다.

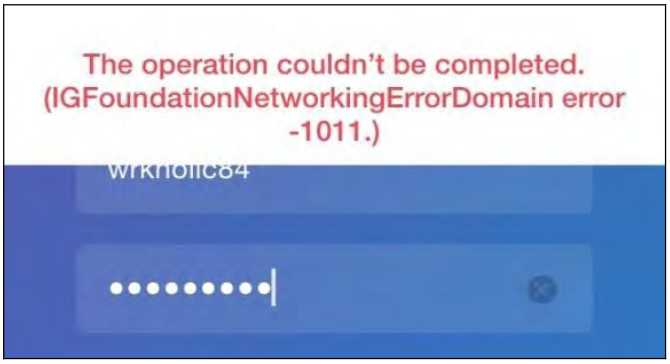
본 논문에서는 모바일 애플리케이션에서 사용하고 있는 SSL Pinning 기술이 우회 가능함을 보이고, 이에 대한 대응방안을 분석하였다.

2. 본론

기업, 금융기관들은 그 중의 사용자와 서버 간 통신 시 송수신되는 정보들이 MITM(Man In The Middle) 공격으로 인한 탈취, 변조를 막고자 여러 기술을 사용하고 있는데 SSL Pinning 이 그 중 하나이다. 스마트폰의 '신뢰할 수 있는 저장소'와 서버의 인증서 일치 여부에 의존하는 것은 보안상 구멍이 생기게 된다. 스마트폰의 '신뢰할 수 있는 저장소'는 쉽게 공격당할 수 있고 안전하지 않은 인증서를 설치할 수 있다. 이는 잠재적으로 MITM 공격을 허용한다. 공격자가 모바일 애플리케이션과 서버 간에 송수신하는 패킷을 캡쳐해서 패킷을 분석하거나, 인자 값 변조 등의 공격으로 웹 서비스를 불법으로 이용하게 한다. SSL Pinning 은 모바일 애플리케이션이을 이용하는 사용자와 서버 간 통신 시, 규약한 인증서가 아닌 타 인증서 사용을 막는 것이다.[3]

PC 에서 프록시 툴을 이용하여 모바일 단말기와 프록시 연결을 위해 세팅을 한다. 다음 모바일 단말기를 Wi-Fi 로 PC 와 동일 네트워크에 연결한 다음, 프록시를 설정한다. [4] 이후 PC 에서 프록시 모바일 단말기에서 전송되는 웹 서비스 패킷이 PC 프록시 툴에서 캡쳐된다면 준비가 끝난 것이다. SSL Pinning 이 적용되어 있는 Instagram 을 실행한다.

Instagram 실행 후 로그인을 위해 'Facebook 으로 로그인'을 클릭한다. SSL Pinning 이 적용되어 있는 앱에서는 프록시 설정이 되어있는 단말기가, 규약한 인증서가 아닌 프록시 툴의 인증서로 MITM 을 시도하기 때문에, 해당 앱의 실행이 불가하고 에러 메시지가 출력된다.

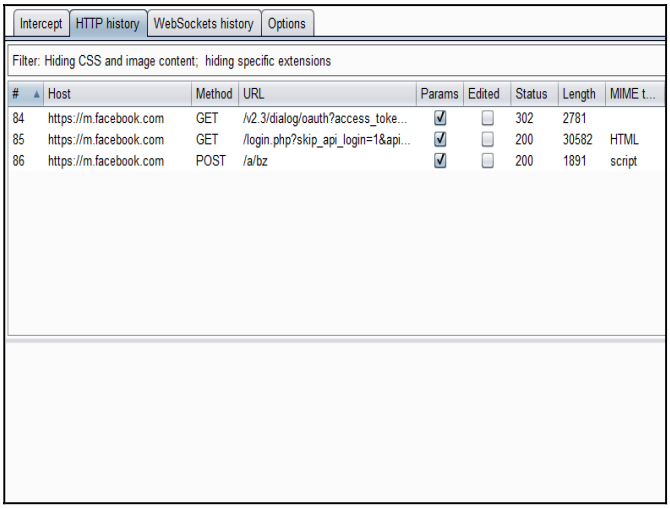


(그림 1) 네트워크 오류 메시지

그러나 루팅, 탈옥된 단말기에서 SSL Pinning 을 POC 툴이 Blackhat 에서 발표되었다.[6] 루팅, 탈옥된 단말기에 해당 앱을 설치 후 재부팅하면 SSL Pinning 을 우회할 수 있는 앱이 활성화되고 이를 실행한다. 앱은 디바이스의 신뢰할 수 있는 저장소를 무시하고 자체적으로 앱 내부에 하드 코딩되어 저장된 인증서로 서명된 호스트에만 SSL 연결을 맺는 것이 SSL Pinning 인데, 이를 무효화하는 것이다.

(그림 2) SSL Unpinning 시도

설치한 프로그램을 이용하여 Instagram 앱 실행 시 Instagram 패킷은 PC 에 세팅되어 있는 프록시 툴에 패킷이 캡쳐되어 있다.



(그림 3) 프록시 툴로 Instagram 앱 패킷 캡쳐 가능

앱은 디바이스의 신뢰할 수 있는 저장소를 무시하고 자체적으로 앱 내부에 하드 코딩되어 저장된 인증서로 서명된 호스트에만 SSL 연결을 맺는 것이 SSL Pinning 은 이렇게 루팅, 탈옥된 단말기에서는 프로그램에서 무용지물이 된다. 이에 대비하는 방법은 루팅, 탈옥된 단말기에서 SSL Pinning 이 적용된 앱을 실행할 수 없도록 해야한다. 모바일 앱 상에서 모바일 앱이 설치된 단말기가 순정여부를 검증하는 로직이 존재하면 이는 해결된다.

(그림 4) 모바일 앱에서 단말기의 순정여부를 검증하는 화면 예시

3. 결론

본 논문은 모바일 애플리케이션에서 발생할 수 있는 보안 위협과 그 대응책에 대한 연구이다. 루팅, 탈옥 단말기에서 앱이 실행될 경우 SSL Pinning 이 우회되는 위협을 보이기 위하여 모바일 애플리케이션 중 하나인 Instagram 애플리케이션을 대상으로 사례 연구를 진행하였다. 해당 연구에서 Instagram 은 SSL Unpinning 에 취약하였고, 공격자는 이를 이용하여 https 구간 내 패킷 캡쳐 및 변조가 가능함을 보였다. 마지막으로 이에 대한 대응 방법을 소개하였다.

향후 연구로는 현재 본 연구를 기반으로 본 연구에서 사례 조사한 취약점 외에 다른 취약점들을 다른 여러 모바일 애플리케이션을 대상으로 시연할 예정이며, 대응 방법 또한 실제 구현을 통해 연구할 예정이다.

참고문헌

[1] 미래창조과학부, "2016 년 인터넷이용실태조사 결과", 2016
[2] 뉴스다임, "모바일뱅킹 등록고객 7 천만명 돌파", 2016
[3] OWASP, "Certificate and Public Key Pinning", https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning
[4] Google Nexus 고객센터 "Wi-Fi 네트워크에 연결 - 고급 Wi-Fi 설정 - 프록시 설정 구성", https://support.google.com/nexus/answer/2819519?hl=ko
[5] GitHub "ios-ssl-kill-switch", https://github.com/iSECPartners/ios-ssl-kill-switch
[6] Blackhat, "When Security Gets in the Way", https://media.blackhat.com/bh-us-12/Turbo/Diquet/BH_US_12_Diqut_Osborne_Mobile_Certificate_Pinning_Slides.pdf