핀테크 보안 위협 및 고찰

주재웅 [1], 오대명 [1], 박종혁 [1*]
[1] 서울과학기술대학교 컴퓨터공학과
[1]e-mail : {woong07, damingwu, jhpark1}@seoultech.ac.kr

Security threats and Review for FinTech

Jae Woong Joo[1],DaMing Wu, Jong Hyuk Park[1*]
Dept. of Computer Science and Engineering and Dept. of Interdisciplinary Bio IT Materials,
SeoulTech, Korea

요 약

최근 금융과 IT 가 결합한 핀테크 산업이 빠르게 성장하고 있다. 전통적 금융 서비스에서 벗어나 소비자 접근성이 높은 인터넷, 모바일 기반 디바이스의 장점을 활용하여 송금, 결제, 자산관리 등 다양한 분야의 금융서비스를 제공한다. 하지만 핀테크 기술 발전으로 네트워크, 클라이언트, 시스템 등 각각의 부문에서 새로운 보안 위협 요소가 증가 할 것이다. 본 논문에서는 핀테크 보안의 고려사항과 연구동향에 대해 살펴보고 현재 핀테크 분야에서 보안이 적용된 시스템에 대해 분석하고 취급되는 정보보호의 중요성에 대해 고찰한다.

1. 서론

최근 금융을 뜻하는 파이낸셜(Financial)과 기술(Technique)이 결합한 핀테크 산업이 빠르게 성장하고 있다. 기존 전통적 금융 서비스에서 벗어나 인터넷, 모바일 기술과 접목해 언제 어디서든 금융서비스를 사용할 수 있게 된다 [1]. 전통적인 금융서비스는 오프라인 점포를 기반으로 강력한 보안 시스템 및 데이터베이스 연계에 기반으로 금융서비스에 필수적인 보안 및 신뢰성을 확보한다. 반면에 핀테크는 스마트폰 위주의 모바일 단말기에 기반하여 간편 송금/결제, 대출, 자산관리, 크라우드 펀딩 등 각종 금융 서비스를 제공하는 기술. 전통적 금융 업무의 대체를 통한 비용 절감, 개인 맞춤형 서비스 제공할 수 있다 [2]. 또한 스마트폰의 활용한 접근성, 기술적인 이점을 활용한 편의성을 제공한다. 하지만 전통적인 금융서비스에 비해 네트워크, 클라이언트, 시스템 등의 보안문제점을 갖는다. 이러한 문제점들은 개인정보 유출과 스미싱, 해킹을 통한 정보 보안 사고가 지속적으로 발생시킨다. 또한 간편결제 시스템 뿐 아니라 크라우드 펀딩, P2P 대출 등 다양한 금융 상품 등이 등장함에 따라 보안 사고에 노출 될 분야도 더욱 다양해졌다. 이러한 다양한 신규 보안위협이 추가적으로 나오는 것에 대비해 핀테크가 해결해야 할 문제는 안전하고 즉각적인 거래를 위한 신뢰, 보안 그리고 사용자가 진정으로 원하는 가치를 쉽고 편리하게 제공할수 있는 사용자 경험이다.

본 논문에서는 핀테크 보안의 고려사항과 연구동향에 대해 살펴보고 현재 스마트폰 위주의 모바일 단말기의 위협요소 및 악성코드 유형을 분석하여 정보보호의 중요성에 대해 고찰한다.

* 교신저자: 박종혁(서울과학기술대학교)

2. 보안 고려사항

핀테크의 보안 환경에서는 무결성, 기밀성, 가용성, 접근제어, 프라이버시 등에 대해 고려해야 한다.

2.1 기밀성

와이파이를 이용하여 네트워크를 사용하는 스마트폰, 태플릿 PC 와 같은 스마트 디바이스는 공격자에 의해 데이터가 도청되거나 위/변조될 가능성이 있다. 따라서 공격자가 데이터에 대한 어떠한 정보도 얻을 수 없어야 하는 데이터 기밀성이 보증되어야 한다.

2.2 무결성

수신자는 전송된 메시지가 공격자에 의해 위/변조되지 않았음을 확인 할 수 있어야 한다. 따라서 해쉬함수를 이용하여 생성된 값은 메시지의 무결성을 보장한다. 또한 해쉬 함수 자체에 대한 안전성이 요구된다.

2.3 가용성

스마트 폰, 태플릿 PC 와 같은 스마트 디바이스는 언제 어디서나 이용이 가능한 대신 한정된 배터리를 사용하기 때문에 전력이 제한적이다. 또한 스마트 디바이스의 연산량이 늘어나면 소모하는 자원의 양이 증가한다. 따라서 적은 연산량으로 효과적인 데이터 전송을 행하는 가용성 보장 방안이 요구된다.

2.4 접근제어

사용자의 정보에 접근제어를 통해 데이터 및 시스템에 접근제어를 해야 한다. 인가 되지 않은 관리자 및 기타사용자에게 권한 및 역할을 부여하여 정보접근에 제한을 둔다.

2.5 프라이버시 보호

핀테크에서 취급되는 개인정보가 외부로 유출되거나 공개되었을 경우 프라이버시 침해가 된다 [3]. 또한 경제적인 피해를 대비하여 프라이버시 보호가 제공되어야 한다.

3. 모바일 위협요소 및 악성코드 유형

3.1 모바일 위협요소

모바일 보안에는 다양한 요소가 영향을 미치는데, 이는 크게 세가지로 분류할 수 있다. 애플리케이션 기반의 위협, 웹 기반의 위협, 그리고 네트워크 기반의 위협으로 나눌 수 있다.

애플리케이션 기반의 위협은 주로 다운 가능한 애플리케이션과 관련하여 발생한다 [3]. 악의적인 의도로 개발된 소프트웨어 애플리케이션과 같은 악성 소프트웨어를 통해 개인정보 유출이 가능하다. 이러한 개인정보 유출은 스파이웨어에 의해서 발생하며, 스파이웨어는 사용자 동의 없이 위치, 연락처, 통화내역, 이메일, 사진, 문자 메시지 등의 데이터를 수집 가능하게 한다. 이렇듯 악성 애플리케이션은 자동적으로 다운이 되거나 기계적으로 중단되거나 개인정보를 무단으로 해킹하는 등의 오작동을 유발한다.

웹 기반의 위협은 PC 뿐만 아니라 모바일 보안과 관련하여 지속적으로 이슈가 되고 있다 [4]. 단말기의 OS 취약점으로 인한 관리자 권한 획득, 악성코드를 통한 개인 정보 유출, 모바일 웹 브라우저의 취약점의 경우에는 웹 브라우저의 구성 요소에 내재되어 있는 소프트웨어 보안 결함으로 인해 공격자의 악의적인 악성코드가 다운로드되어 설치되는 보안 사고가 발생할 수 있다.

네트워크 기반 위협은 로컬 무선 네트워크와 모바일 네트워크로 인해 발생한다 [5]. 특히 와이파이 스니핑은 데이터가 많은 애플리케이션과 웹페이지를 통하여 전송되도록 한다. 사용자는 데이터의 전달 유무에 대한 인지가 이루어지지 않기 때문에 보안의 문제가 더욱 심각하다.

3.2 모바일 악성코드 유형

모바일 악성코드 유형은 금전적인 목적, 개인정보 유출, 시스템 파괴 등이 있다.

모바일 단말 악성코드 : 모바일 단말에서 동작하면서 시스템을 파괴하거나 저장된 개인정보 등을 유출하는 악의적 활동을 수행하는 코드이다 [6]. 모바일 단말을 공격하는 악성코드는 모바일 단말의 기능을 마비시키거나 모바일 단말 내에 저장된 정보의 유출 및 금전적 이익을 취하는 것을 목적으로 하고 있다.

과금 유발형 악성코드 : 모바일 단말의 SMS 서비스나 송신 서비스를 지속적으로 시도하여 과금을 발생시키는 악성코드 유형이다 [7]. 감염된 기기는 사용자도 모르게 불특정 다수에게 SMS 및 송신을 함으로써 이용자에게 금전적 피해를 입히는 악성코드이다.

정보 유출형 악성코드 : 감염된 모바일 단말기의 정보나 사용자의 개인정보를 외부로 유출시키는 악성코드 유형이다 [8]. 악성코드가 설치되고 나면 기기의 보안설정을 변경하고 기기의 정보를 외부로 전송하여 추가적인 공격을 용이하게 한다. 또한 사용자의 위치 정보를 빼가는 악성 스파이웨어도 있다.

크로스 플랫폼형 악성코드 : 모바일 단말을 통해 PC 를 감염시키는 악성코드 유형으로 메모리카드에 웜을 복사하여, 감염된 메모리카드를 PC 에 장착했을 때 autorun 기능을 통해 PC 를 자동으로 악성코드에 감염시킨다 [9].

4. 결론 및 고찰

본 논문에서는 핀테크 보안 고려사항과 모바일 위협 요소 및 악성코드 유형에 대해 논의하였다.

핀테크는 모바일결제, 송금, 개인자산관리, 크라우드펀딩 등 금융 서비스와 관련된 기술임에도 불구하고 스마트폰의 보안 취약점을 노려 많은 범죄가 이뤄지고 있으며 범죄 규모와 피해는 증가하고 있다. 또한 악성코드는 더욱 지능화되고 정보 유출, 불법 과금, 부정 사용 등과 같은 다양한 형태로 변형되어 모바일 공격의 규모와 피해가 증가하고 있다. 따라서 안전성, 무결성, 가용성, 신뢰성이 제공된 핀테크 서비스 환경을 제공하기 위해 사용자 행동기반의 능동적이고 총체적인 새로운 스마트폰 보안 기술 개발이 요구된다.

Acknowledgment

"본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 ICT 연구센터육성 지원사업의 연구결과로 수행되었음" (IITP-2015-H8501-15-1014)

참고문헌

[1] 이주연, 최운호. "차세대 성장동력 핀테크(Fin Tech)의 융합과 진화", 대한산업공학회,ie 매거진 21(4), pp.47-52, 2014.

[2] Dapp T F, Slomka L, AG D B, et al. “Fintech–The digital (r) evolution in the financial sector”. 2014.

[3] Lin, Ying Dar, et al. "Mobile Application Security." Computer 47.6, pp.21-23, 2014.

[3] Enck W, Ongtang M, McDaniel P. “Understanding an droid security”, IEEE security & privacy, Volume:7, pp.50-57, 2009.

[4] M. Keith, "Android 2.0-2.1 Reverse Shell Exploit", http://www.exploit-db.com/exploits/15423/

[5] Wright J, Dawson Jr M E, Omar M. “Cyber Security and Mobile Threats: The Need For Antivirus Applications For Smart Phones”. Journal of Information Systems Technology and Planning, 5(14), pp.40-60, 2012.

[6] Peng S, Yu S, Yang A. “Smartphone malware and its propagation modeling: A survey”, IEEE Communications Surveys & Tutorials 16(2), pp. 925-941, 2014.

[7] Seo S H, Gupta A, Sallam A M, et al. “Detecting mobile malware threats to homeland security through static analysis”, Journal of Network and Computer Applications 38, pp.43-53, 2014.

[8] Felt, Adrienne Porter, et al. "A survey of mobile malware in the wild.", Proceedings of the 1st ACM wor

kshop on Security and privacy in smartphones and mobile devices. ACM,pp.3-14, 2011.

[9] Lindorfer M, Neumayr M, Caballero J, et al. “POST ER: Cross-platform malware: write once, infect every where”, Proceedings of the 2013 ACM SIGSAC conf erence on Computer & communications security, pp.1 425-1428, 2013