모바일 내 결제시스템의 안전성에 대한 연구

이정명*, 박재경O
*강서폴리텍대학 사이버보안학과,
O강서폴리텍대학 사이버보안학과
e-mail: anderson@kakao.com*, jakypark@kopo.ac.krO

A Safety Analysis of Mobile Payment Systems: Ensuring Secure and Reliable Transactions

JeongMyeong Lee*, Jae-kyung ParkO
*Dept. of Cyber Security, Korea Polytechnis,
ODept. of Cyber Security, Korea Polytechnis

● 요 약 ●

본 논문은 모바일 환경에서의 안전한 결제시스템을 위한 기술 연구에 대해 다룬다.

모바일의 급속한 발전은 보안에 악영향을 끼쳤는데, 기기 내에서 많은 개인정보가 처리되기 때문에 해커들의 놀이터가 된 만큼 보안 이슈가 증가 되었다. 이를 해결하기 위해서는 기존의 결제 시스템과 다른 방식의 보안기술이 필요하다. 그리하여 모바일 보안기술과 결제시스템 기술을 연계하여 안전한 결제시스템을 구현하는 방안에 대해 연구하였다. 안전한 결제 시스템을 구현하기 위해 필요한 기술 요소들을 제안하고 이를 바탕으로 안전한 결제시스템을 구현하기 위한 시스템 아키텍처를 제안하고, 구현된 시스템을 통해 안전성을 검증하고자 한다. 본 논문에서는 모바일 환경에서 안전한 결제시스템을 위해 모바일 보안기술과 결제시스템 기술을 연계하여 안전성을 확보할 수 있는 방법에 대해 제안하고, 이를 통해 모바일 환경에서 안전하게 결제를 이루어낼 수 있는 기술적인 기반을 마련할 수 있을 것으로 기대해본다.

키워드: 모바일(Mobile), 보안(Security), 결제시스템(Payment System), 보안기술(Security Technology), 안전성(safety)

I. Introduction

모바일 결제 시스템은 모바일 기기를 통해 상품이나 서비스를 결제하는 시스템을 의미하는데, 모바일 기기의 보급과 인터넷 이용 환경의 발전으로 인해 급속도로 성장하고 있으며, 일반적으로 모바일 앱을 통해 제공된다. 모바일 기기 사용자는 언제 어디서든 간편하게 결제를 완료 할 수 있다. 모바일 결제시스템은 신용카드결제, 휴대전화 요금청구서 결제, 전자화폐 결제 등 결제수단을 활용하기 때문에 보안적인 측면에서 많은 노력이 기울여지고 있다.

II. Preliminaries

1. 국내 동향

1) 개인정보 강화 : 데이터의 암호화, 사용자 인증 강화, 안전한 통신 프로토콜 도입 등을 통해 보안성을 강화하고 있다.

2) 모바일 플랫폼 확대: 쇼핑 앱, 은행 앱, 소셜 미디어 플랫폼 등에서 편리하고 빠른 결제를 할 수 있다.

3) NFC 기술의 활용: NFC 칩을 이용하여 결제 단말기와의 통신을 통해 결제하며, 신용카드나 체크카드 정보를 스마트폰에 등록하여 간편하게 결제할 수 있다.

4) QR 코드 결제: QR 코드를 스캔하여 결제를 진행할 수 있으며, 사용자들은 앱을 통해 결제 정보를 등록하고 간편하게 결제할 수 있다.

5) 보안 인증 기술의 도입: 지문인식, 얼굴인식 등의 생체인증 기술을 활용하여 사용자 인증을 강화한다.

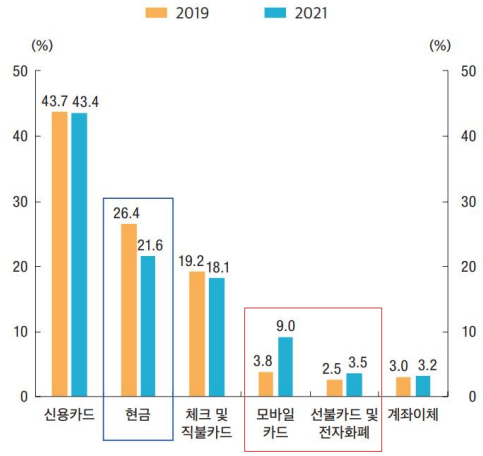

Fig. 1. The usage proportion by payment method
source. BANK OF KOREA

위 그림은 현금의 사용량은 감소, 모바일카드나 선불카드 및 전자화폐의 수는 증가했음 보여준다. 이러한 측면의 증가세는 편리성과 간편함을 추구함에서부터 나온 것이며, 사용자가 편리하고 간편하게 이용 한다는 것은 보안 측에서 문제야기 될 수 있음 짐작 할 수 있다.

2. 모바일 결제 시스템으로 인해 일어날 수 있는 보안문제

1) 악성 앱 : 기기 내 설치된 악성 앱으로 인해 정보 탈취할 수 있다.

2) 네트워크 스니핑 : 공용 네트워크를 통해 데이터가 전송될 때, 해커는 스니핑 기술을 이용하여 데이터 탈취가능하다.

3) 피싱 : 악성 메일이나 메시지를 통해 결제 정보를 입력하도록 유도하는 피싱 사기가 일어날 수 있다.

라. 탈옥된 기기 : 탈옥된 IOS나 루팅 된 안드로이드 기기를 사용시 보안에 취약하다.

마. 결제 서비스의 취약점 : 결제 서비스 업체의 보안 취약점으로 인해 사용자 정보가 유출 가능성이 있다.

III. The Proposed Scheme

1. 결제 시스템의 보안 검증 및 강화

1) 취약점 분석 : 모의해킹을 시도하거나, 보안 취약점 스캐너를 이용하여 취약점을 분석한다.

2) 보안 인증 : 정부나 제3기관에서 인증을 받아 결제 시스템의 보안성을 인증 받는다.

3) 암호화 : SSL(Secure Sockets Layer) 또는 TLS(Transport Layer Security) 등의 암호화 기술을 이용한다.

4) 이중 인증 : 결제 외 추가적인 인증을 요구한다.

5) 보안 솔루션 : 방화벽, 침입 탐지 시스템, 보안 감사 시스템 등을 이용한다.

2. 결제시스템 보안 연구

1) 보안 강화를 위한 인증 방법 연구: 생체인식, 지문인식, 얼굴인식 등 다양한 인증 방법 개발한다.

2) 모바일 결제 시스템과 블록체인 기술의 결합 연구: 블록체인 기술을 활용하여 모바일 결제 시스템의 보안과 투명성을 강화할 수 있는 방법을 연구한다.

3) 모바일 결제 시스템과 인공지능 기술의 결합 연구: 인공지능 기술을 활용하여 모바일 결제 시스템의 사용자 경험을 개선하고, 보안 위협을 탐지하고 대응하는 방법을 연구한다.

4) 사용성 개선 연구: 사용자가 모바일 결제 시스템을 보다 편리하게 이용할 수 있는 UI/UX 개선과 사용자 중심의 결제 시스템 개발

IV. Conclusions

본 연구는 결제시스템 보안의 다양한 측면을 조사하고, 현재의 보안 조치, 취약점, 그리고 신흥 기술들을 분석함으로써, 민감한 결제 정보를 보호하고 사용자들을 잠재적인 위협으로부터 보호하는 데 강력한 보안 조치가 필수적임을 확인했다.

암호화 기술, 안전한 인증 방법, 지속적인 모니터링 및 탐지 시스템 등 보안의 중요성을 강조하고, 블록체인과 인공지능 같은 기술들을 결제시스템 보안과 연계함으로써 투명성, 불변성, 사기 탐지 능력을 확보하여 보안성을 더욱 강화할 수 있다.

그러나 새로운 결제 방식과 채널과 관련된 잠재적 위험 등 새로운 보안에 대한 더 많은 연구가 필요하다.

REFERENCES

[1] E. Smirni, and G. Ciardo, "Workload-Aware Load Balancing for Cluster Web Servers," IEEE Trans. on Parallel and Distributed Systems, Vol. 16, No. 3, pp. 219-232, March 2005.

[2] Kdhong, "An Efficient Dynamic Workload Balancing Strategy," Journal of The Korea Society of Computer and Information, Vol. 15, No. 1, pp. 1-10, Nov. 2010.