모바일 기기에서 토큰을 이용한 간편 결제 시스템의 보안 취약점 개선을 위한 연구

오정민[1], 신용태[2]
[1]숭실대학교 컴퓨터학부
[2]숭실대학교 컴퓨터학부
jmin980317@naver.com, shin@ssu.ac.kr

Research on improving the security vulnerabilities of the easy payment system using tokens on mobile devices

Jung-Min Oh[1], Young-Tea Shin[2]
[1]Dept. of Computer Science and Engineering, Soong-Sil University
[2]Dept. of Computer Science and Engineering, Soong-Sil University

요 약

최근 결제 시스템은 인간 친화적이며 다양한 디지털 기술들의 발전으로 간편화되고 있다. 특히 핀테크의 일종인 간편 결제 시스템은 효율성과 간편성을 강조하면서 금융 시장에서 크게 화두 되는 시스템이다. 그러나 효율성과 간편성에 집중하다 보니 보안성이 낮아지는 단점을 가지고 있다. 특히, 간편 결제 시스템의 핵심인 토큰 시스템의 취약점은 가장 큰 문제를 발생할 수 있다. 이에 대응하기 위해, 이 논문에서는 기존 결제 시스템 방식에 비대칭 암호화 방식을 추가하여 간편 결제 시스템의 보안성을 높여 토큰 취약점 대응 시스템을 제안한다.

1. 서론

최근 제 4차 산업혁명의 발전과 국내의 애플페이 도입으로 인해 핀테크의 일종인 간편 결제 시스템이 더욱 인기를 얻고 있다. [1]. 한국은행 2023년 국내 지급결제동향과 전자지급서비스 이용현황에 따르면 2022년 간편 결제 서비스 일평균 이용금액은 7,326억 원으로 전년(2021년) 대비 20% 증가하였다.

이처럼 간편 결제 시스템 시장은 급격한 성장 속도를 이루면서 빠른 속도와 효율성을 추구하다 보니 보안 문제에 대해 우려의 목소리가 커지고 있다. 이를 대비해 기존 결제 방식 시스템은 [2]. 토큰(Token)이라는 무의미한 값으로 치환하여 인증하는 토큰화(Tokenization) 기술을 도입하여 보안성을 강화하고 있지만 토큰 시스템에서 발생할 수 있는 보안 취약점이 존재한다.

이에 따라, 본 논문에서는 기존 토큰시스템의 보안 취약점을 보완하기 위한 방법으로 비대칭 암호화 방식을 추가 제안하고 있다. 본 논문의 구성은 다음과 같다. 2장은 관련연구, 3장은 제안, 4장은 결론으로 구성된다.

2. 관련연구

2.1 간편 결제 시스템의 토큰 발급 절차

[3]. 간편 결제를 위해 사용자는 결제 서비스 제공 업체에 가입하고 카드 정보를 제공하며, 인증방법 (SMS, 이메일, 인증 번호)을 통해 카드 정보를 인증한다. 인증이 완료되면 결제서비스는 사용자를 위한 고유한 토큰을 발급한다. 이때 토큰 제공자는 토큰 저장소에 카드번호와 토큰 정보를 저장하고, 발급된 토큰은 카드사에 전달되어 토큰 발급이 완료된다.

2.2 토큰을 이용한 기존 간편 결제 시스템 결제 절차

[3]. 사용자가 간편 결제를 선택하면, 간편 결제 시스템은 사용자로부터 카드 정보를 요청한다. 사용자가 카드 정보를 입력하면 간편 결제 시스템은 결제를 위한 토큰을 발급하고, 사용자는 해당 토큰을 사용하여 결제를 완료한다. 이때 간편 결제 시스템은 토큰을 이용하여 실제 결제를 처리한다.

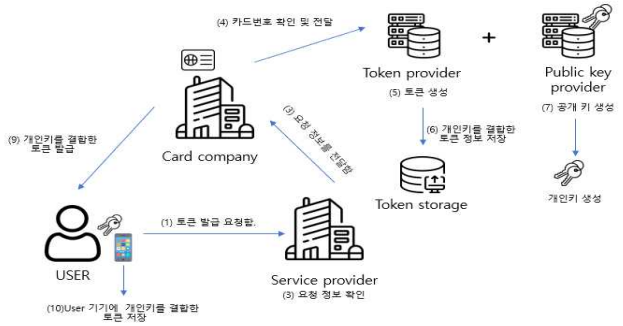
2.3 비대칭 암호화(Asymmetric Crypto)

[2]. 비대칭 암호화 방식은 누구나 볼 수 있는 공개키(Public key)와 개인키(Private key)라는 비밀키를 사용하여 암호화 및 복호화하는 방식이다. 공개키를 사용하여 암호화된 데이터는 해당 개인키만으로 해독할 수 있으며, 개인키를 소유한 수신자만이 복호화할 수 있다. 이러한 인증 기능을 제공하여 보안성을 높일 수 있는 장점을 가지고 있다.

3. 제안

3.1 비대칭 암호화를 결합한 간편 결제시스템의 토큰 발급 절차

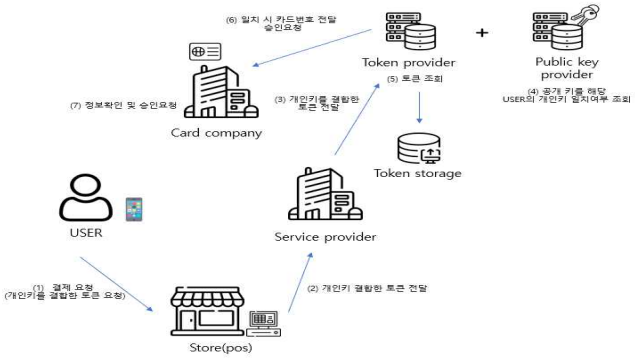
제안하는 간편 결제 시스템의 토큰 발급 모델은 기본 동작은 (그림 1)과 같다. 기존 간편 결제 시스템과 유사하게 토큰 생성 절차를 따르지만, 토큰 생성 시 추가로 공개키와 사용자를 위한 개인키를 생성한다. 그리고 해당 토큰을 사용자의 개인키와 결합하여 캡슐화하여 저장소에 저장한다. 이후 기존 간편 결제 시스템과 동일하며, 사용자에게 개인키를 결합한 토큰을 제공하면서 해당 토큰을 사용자의 모바일 기기에 저장하며, 이를 통해 개인키만으로 해당 토큰을 복호화하여 사용할 수 있다. 이러한 방식은 보안성을 강화하는 역할을 하게 된다.



(그림 1) Token issuance system using asymmetric encryption

3.2 비대칭 암호화 이용한 간편 결제 시스템의 결제 절차

제안하는 간편 결제 시스템 결제 절차 모델의 기본 동작은 (그림 2)와 같다. 이 모델은 기존 간편 결제 시스템의 결제 절차를 따르면서, 토큰 저장소에서 공개키와 사용자의 개인키의 일치 여부를 확인한다. 이 과정에서 공개키가 사용자의 개인키와 일치하지 않으면 해당 토큰 조회를 할 수 없다. 하지만 공개키와 개인키가 일치하면, 사용자 토큰을 조회하고 해당 토큰값이 유효한지 확인 후, 결제를 완료한다. 이러한 과정을 거쳐 보안성을 높일 수 있으며, 결제 시스템의 안정성과 신뢰성을 확보할 수 있다.



(그림 2)An Asymmetric Crypto-based easy payment system.

4. 결론

본 논문에서는 모바일 기기에서 토큰을 이용한 간편 결제 시스템의 보안 취약점을 개선하기 위해 비대칭 암호화를 결합한 토큰 발급 및 결제 시스템 설계를 제안한다. 비대칭 암호화의 장점으로 인해 해당 개인키를 사용해야만 복호화가 가능하기 때문에 기존 간편 결제 시스템 중 토큰 취약점에 대한 보안성을 강화할 수 있다. 향후 연구 방향으로는 대칭 암호화에 비해 암호화된 키의 크기가 크고 복호화에 걸리는 연산시간이 더 길기 때문에 해당 문제를 해결할 수 있는 방안에 대해 연구를 진행할 예정이다.

Acknowledgement

"본 연구는 과학기술정보통신부및정보통신기획평가원의 SW중심대학사업의 연구결과로 수행되었음"(2018-0-00209)

참고문헌

[1] 경제정보센터(2023), 2022년 중 전자지급서비스 이용 현황 2023.03.30. https://eiec.kdi.re.kr/policy/materialView.do?num=236736&topic=

[2] 김보승(2011). 디지털 동영상 보호를 위한 대칭키 알고리즘 기반의 부분 암호화 기법, 숭실대학교 대학원 컴퓨터학과 학위논문

[3] 손위동(2016). 간편 결제 시스템의 토큰 발급 과정 보안 취약점 개선에 관한 연구. 동국대학교 국제정보대학원 학위논문