IoT 지불 시스템 보안

이종협 (가천대학교)

목차

1. 개 요

사물인터넷(Internet of Things, IoT)의 발전과 더불어서 IoT 환경에서의 보안이 큰 이슈가 되고 있다. IoT 보안은 새로운 플랫폼에 대한 신뢰성과 안전성을 확보한다는 측면에서도 중요하지만 실제 생활에 밀접하게 연관되어 있는 IoT의 특성 때문에도 중요하게 다루어진다. IoT 환경에서의 보안 침해 사고는 실제 생활에서 밀접하게 사용되고 있는 핸드폰, 가전기기, 전구, 자물쇠 등에 대한 제어권을 외부 공격자에게 빼앗길 수 있는 위험성이 있어서 더 심각하게 여겨지고 있다.

IoT와 함께 최근 많은 관심을 받고 있는 핀테크(FinTech)분야는 전통적이고 보수적이었던 금융 서비스가 IT의 도움을 받아 급격하게 변화할 것이라는 예상에서 기대를 모으고 있다. 우선적으로 결제(payment)에 초점을 맞추어 많은 서비스들이 앞 다투어 새로운 기술을 선보이고 있다.

IoT를 통한 컴퓨팅 환경의 극적인 확장은 모바일 결제나 비트코인(Bitcoin)과 같은 새로운 금융 시스템들에 맞물려 또 다른 가능성을 열고 있다. IoT는 컴퓨팅 플랫폼에서 그치는 것이 아니라 금융 서비스의 플랫폼으로써도 역할을 할 것으로 예상되고 있다. 대표적인 예로써 IBM은 IoT 기기들이 실제 경제 주체가 되는 “Economy of Things”의 시대를 정의하며[1] 새로운 IoT 경제 환경을 선도하기 위해 준비하고 있다. 즉, IoT 경제에서는 IoT 기기가 주체적으로 경제의 참여자 역할을 하는 셈이다. 이러한 관점에서 IoT를 통한 금융 서비스의 대부분은 우선 비용을 지불하거나 지불받는 결제 서비스를 일차적인 구현 목표로 삼고 있다.

본 기고문에서는 IoT 기기를 통한 결제 서비스의 가능성과 발생할 수 있는 보안의 문제점에 대하여 알아보고자 한다. 새로운 IoT의 결제 서비스에서는 어떠한 주체(2절)가 무엇에 대하여(3절)

지불할 것이며 이를 안전하게 수행하기 위해서는 어떠한 수단을 이용해야 할 지(4절) 살펴본다.

2. 누가 무엇에 대하여 지불하는가?

전구, 냉장고, TV 등의 생활에 밀접한 물건들이 인터넷에 연결되어 구성되는 IoT 환경에서 IoT 기기들을 통하거나 기기들 간의 자동화된 결제 서비스가 생겨나는 것은 당연한 수순이라고 할 수 있다. 또한 최근 공유경제 또는 구독(subscription) 경제들의 발전은 우리가 지불하지 않았던 대상이나 서비스들이 지불의 대상이 될 수 있음을 깨닫는 인식전환을 가져왔다. 그리고 이에 맞물려 IoT 환경에서 기대할 수 있는 새로운 경제 활동들에 대하여 많은 논의가 이루어지고 있다. 대표적인 예로써 센서에 측정된 결과에 대하여 센서 기기에 직접 비용을 지불하며 데이터를 수신[2]하거나, 공공장소에서 설치된 Wi-Fi 공유기에 시간당 사용료를 지불하는 등의 새로운 비즈니스 모델의 가능성이 타진되고 있다.

IoT 기기들 간의 새로운 경제체계를 이루기 위해서는 기존의 지불 거래에 비하여 적은 금액의 많은 거래를 지속적이고 효율적으로 수행하는 Micropayment 또는 Picopayment[1]의 발달과 IoT 기기가 참여하는 자동화된 시스템의 발달이 선행되어야 한다. Micropayment와 같이 적은 금액을 결제하는 경우에는 결제 대비 소요 비용을 최소화하기 위하여 결제 과정 효율화도 중요하지만 무엇보다 매 결제 과정에서 발생하는 수수료를 최소화할 수 있어야 한다. 현재 사용되는 신용카드 기반 결제의 경우, 매 거래 시마다 결제 수수료와 함께 VAN 통신망 사용에 대한 고정적인 통신료를 지불해야 하는 상황이기 때문에 Micropayment가 바로 적용되기는 어려운 실정이다. 이러한 한계점 들을 극복하고 IoT 기기들의 경제 체계를 활성화하기 위해 기존과는 다른 결제 방법들이 개발되고 있으며 비트코인과 같은 색다른 접근 방법 또한 관심을 받고 있다.

3. 어떻게 지불할 것인가?

지불 서비스는 실제 돈과 관련된 금융 서비스이기 때문에 무엇보다도 보안이 중요하다. 따라서 단순히 IoT 기기들이 어떻게 지불할 것인가에 대한 논의는 어떻게 하면 안전하게 지불할 수 있는가를 의미한다. 즉 '안전한 IoT 지불 서비스는 어떻게 발전되어야 하는 가'로 이어진다. 이러한 측면에서, IoT의 결제서비스는 크게 기존의 결제 채널을 그대로 이용하면서 IoT 기기의 특성에 맞추어 발전시키는 경우와 IoT에 적합한 새로운 프로토콜이나 시스템을 이용하는 경우로 나눌 수 있다.

3.1 기존 시스템 기반의 결제 기법 적용

최근 모바일 기기를 활용하는 카카오페이, ApplePay와 같은 결제서비스의 발달이 전자의 경우에 속한다. 모바일 기기의 결제서비스는 주로 이동성이 있는 기기에서 무선을 통해 결제를 수행할 수 있게 함으로써 결제의 신속성과 편이성을 함께 제공하고 있다. 또한 경량의 서비스를 위주로 발달하였기 때문에 IoT 기기를 통하여 사용하기에 적합한 방식으로 여겨지고 있다.

하지만 내부적으로는 금액을 충전 후 사용하는 포인트 제도의 구조를 가지거나 신용카드와 가맹점 사이에서 기존 플랫폼을 재활용하여 사용하고 있다. 기존 금융 서비스에서 발생하던 보

1) 일반적으로 $10 이하의 결제를 'micropayment' $0.1 이하의 결제를 'picopayment'로 구분한다[3].

안의 문제점을 여전히 가지고 있으며 특히 자동화된 시스템으로 자율성을 가지고 동작할 것으로 예상되는 IoT 기기들에게는 이러한 보안의 취약점이 더 크게 작용할 것으로 예상된다.

ApplyPay와 같이 새로운 결제 방법 또한 token을 사용하는 등의 보안 강화를 위한 노력을 기울이고는 있지만 기본적인 바탕은 신용카드 시스템에서 사용되는 EMV 프로토콜을 벗어나지 않고 있다. 특히 EMV 프로토콜은 단말기의 구현 방법이나 프로토콜 설계 자체의 결함 등에 의해 많은 보안 취약점을 이미 드러내왔으며[4,5], 현재 많은 시스템들이 이미 설치되어 사용되어 있어 단시간 내에 기존의 모든 보안 취약점들이 사라지기는 힘든 실정이다. 또한 자동화된 IoT 기기는 사람의 개입 없이 동작한다는 점에서 자주 언급되어 오던 중간자 공격(Man-in-the-middle attack)에 더 쉽게 노출될 수 있는 가능성을 가지고 있다.

3.2 새로운 접근 방식의 결제 시스템

새로운 결제 시스템을 위해 현재의 용도에 적합한 새로운 프로토콜을 적용하는 방법이 있다. IoT와 같은 M2M(machine-to-machine) 환경에 적합한 결제시스템으로써 가장 주목을 받고 있는 것은 비트코인으로 대표되는 암호 화폐들이다.

암호 화폐는 디지털 시스템을 기반으로 자산(asset)을 만들어내고 거래를 통하여 가치를 주고받을 수 있는 방법을 제공한다. 기존 디지털 화폐도 이중지불(double spending)과 같은 고질적인 문제들을 해결하고자 많은 연구를 수행해 왔지만 2008년에 처음 제안된 비트코인이 이러한 문제들을 분산 환경에서 해결함으로써 디지털 화폐의 새로운 장을 열게 되었다. 비트코인은 은행 계좌와 비슷하지만 발급에 제한이 없는 비트코인 주소(address)와 비트코인 주소들 사이에서 비트코인 이동을 직접적으로 정의하는 거래(transaction)를 핵심 구성요소로 한다. 또한 이러한 구성요소를 분산 환경에서 안전하게 수행하기 위하여 블록체인(blockchain)이란 공개적인 장부(ledger)를 유지한다. 블록체인을 구성할 때는 Full bitcoin 노드 혹은 Miner 라고 불리는 인터넷 참여자(또는 참여 컴퓨터)들에 의한 경쟁적으로 거래참여를 유도하는 Incentive 기반의 블록 생성 기법을 적용함으로써 분산 환경에서 발생할 수 있는 공격자들의 공모와 같은 문제를 해결하고 있다. 따라서 비트코인을 위시한 최근의 암호 화폐들은 중앙 서버 없이도 P2P(Peer to Peer) 형태의 분산 환경에서 안전하게 금융 거래를 수행할 수 있는 플랫폼을 제공하는 셈이다.

IoT 기기를 통한 거래나 기기간의 거래 모두가 M2M에 해당하는 기기와 기기 사이의 거래이고 인터넷과의 연결성을 기반으로 하고 있는 IoT 측면에서 인터넷의 다른 노드들의 확인을 받으며 안전하게 금융 거래를 할 수 있다는 측면에서 암호 화폐의 적합성이 고려되고 있다.

4. 암호 화폐를 적용한 안전한 IoT 지불 시스템 구성 방안

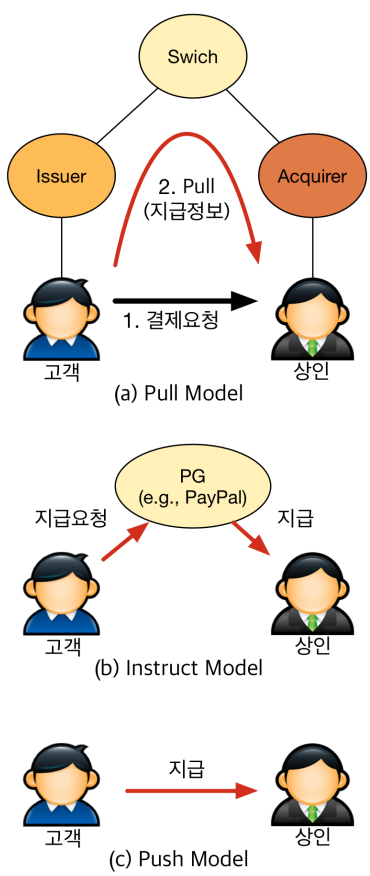
4.1 IoT 지불 시스템으로써의 암호 화폐

암호 화폐가 IoT 방식의 M2M 환경에 적용되기 적합한 이유는 다음과 같이 정리할 수 있다.

첫째, 분산 환경에서도 블록체인 기술을 바탕으로 서로 다른 영역(domain)에 속하는 기기들 간의 신뢰 구축이 가능하다. 실제 ‘economy of things’와 같은 IoT 경제가 활발해지는 상황에서는 단일 국가나 업체에 의한 IoT 장비들 간으로만 거래를 제한할 수 없기 때문에 분산 환경에서의 신뢰 구축 가능 유무가 중요하게 작용하게 된

다. 특히 금융시스템은 다양한 체제하에서 사용되는 특징을 가지고 있기 때문에 도메인 간 손쉬운 신뢰 구축은 IoT의 거래 시스템을 위한 필수 요소라 할 수 있다.

둘째, 암호 화폐를 이용한 결제과정이 기존의 시스템에 비하여 단순하며 수수료가 적다. 현재 사용되고 있는 지불 방식들은 (그림 1)과 같이 모델링 될 수 있다. 기존 신용카드를 기반으로 하는 결제 시스템은 흔히 Pull model로 불리며 고객, 상인, 신용카드 발급 기관(issuer), 상인 금융 기관(acquirer), 그리고 둘을 연결하는 중개자(switch)로 구성된다[6]. 결제에 참여하는 주체가 많아질수록 결제에 걸리는 시간과 수수료가 커지고 보안의 위험성도 함께 증가하게 된다.



(그림 1) 3가지 지불 모델

기존 신용카드를 거치지 않고 PayPal과 같은 PG(Payment Gateway)사들을 통해서 지불을 수행하는 방법도 직접 PG를 통해 지불을 지시한다는 점에서 3자가 참여하는 Instruct model로 단순화 되었지만 역시 PG사에서의 수수료를 무시할 수 없는 상황이다. 당연하게도 제일 간단한 모델은 고객이 상인에게 직접적으로 바로 지불할 수 있는 Push model이다. 현재 Push model 형태로 바로 지불 가능한 방법은 현금(cash)과 암호 화폐뿐이다. 따라서 Micropayment 형태의 작은 액수의 거래가 자주 일어날 것으로 예상되는 IoT 환경에서는 수수료와 보안에 노출되는 구간을 최소화할 수 있는 암호 화폐가 강점을 가지고 있다. (비트코인의 경우 거래 업데이트를 통하여 다수의 Micropayment 거래를 하나로 묶을 수 있어 수수료를 더 절감할 수 있다[7].)

4.2 IoT 기기의 두 가지 참여 방식

암호 화폐가 IoT에 적용되어 구현되기 위해서는 금융거래에서의 IoT 기기의 역할에 따라 구성 모델이 달라질 수 있다. 암호 화폐 시스템에서 모든 거래가 암호 화폐 시스템의 주소를 기반으로 하고 있기 때문에 주소를 소유하는 주체(또는 주소에 연관된 주체)가 누구냐에 따라 실질적으로 거래에 참여하는 주체가 결정되게 된다. 따라서 IoT 기기의 참여 방식에 맞게 암호 화폐 시스템 주소의 할당이 이루어져야 한다.

IoT 기기의 참여 정도는 기기의 자율성에 따라 결정된다. 자율성을 가지지 않는 IoT 기기의 경우에는 IoT 기기가 단순히 편리한 결제를 위한 매개체의 역할만을 하고 실제 결정은 기존과 같이 사람에 의해서 이루어지게 된다. 이러한 경우도 IoT 결제 시스템이라고 할 수는 있지만 사

실 기존의 모바일 결제 환경과 크게 달라지지 않는 셈이다. 따라서 암호 화폐의 사용 주체는 사용자이므로 암호 화폐의 주소 또한 사용자에게 할당되고 IoT 기기는 사용자의 거래 생성을 돕는 역할을 한다. 이와 반대로 자율성을 가지는 IoT 기기의 경우에는 결제 또는 거래 생성이 탑재된 프로그램의 자체 판단을 통하여 이루어지게 되는데 이때는 금융 시스템에 참여하는 주체가 IoT 기기가 되므로 주소를 IoT 기기에 직접적으로 부여하여 사용한다. 물론 IoT 기기에 할당된 주소는 해당 IoT 기기를 설치하거나 운영하는 사람 또한 이용 권한을 가지고 있겠지만, 주된 권한 행사는 사용자 보다는 IoT 기기에게 있다는 점이 다르다.

4.3 참여방식에 따른 보안 고려사항

서로 다른 두 가지 참여방법에 따라 거래와 결제 방식이 달라지므로 그에 따라 안전한 거래를 위하여 고려해야할 보안의 문제점도 달라진다.

IoT 기기의 자율성이 없는 경우는 현재의 모바일 결제 보안의 문제점과 동일한 문제를 고려해야한다. 실제 거래를 수행하는 것은 사람이므로 해당 사용자를 정확하게 확인할 수 있는 사용자-IoT 기기 사이의 안전한 인증 방법이 필요하다. 암호 화폐를 사용하는 경우에도 기본적으로는 사용자가 자신의 비밀키를 이용하여 자기 소유의 암호 화폐를 사용(정확하게는 거래)할 수 있게 되는 것이므로 기기 내부에 저장되어 있는 비밀 정보의 유지가 중요하다. 이는 다시 전통적인 시스템과 네트워크 보안의 영역이며 IoT 기기의 성능 제한을 생각할 때, 오버헤드가 적으면서도 고수준의 공격들을 방어할 수 있는 기법이 필요하다.

IoT의 자율성이 있는 경우에는 IoT 기기 내부의 프로그램 논리에 의하여 거래가 이루어지기 때문에 내부 프로그램이 정확하고 안전하게 수행되는 것이 중요하다. 보통 특정 조건을 만족시켰을 때 정해진 서비스를 제공하거나 거래를 발생하는 방식이기 때문에 프로그램 논리 자체가 복잡하지는 않으나 IoT 시스템의 안전성에 영향을 받는 다는 점은 동일하다. 하지만 암호 화폐를 사용하는 경우에는 다른 방법도 고려할 수 있다. 암호 화폐 시스템 자체 내의 기능을 이용하여 거래 수행 루틴을 IoT 기기 내부가 아닌 안전하게 검증되는 암호 화폐의 블록체인 탑재하여 보안의 위험성을 줄이는 방법이다. 암호 화폐에서 마치 프로그램과 같이 조건에 따라 거래를 수행하는 논리적 객체들을 “스마트 컨트랙트(Smart Contract)"라 부른다.

4.4 스마트 컨트랙트(Smart Contract)

스마트 컨트랙트는 ‘프로그램 가능한 돈(programmable money)’이란 암호 화폐 시스템의 특징이 가장 잘 드러나는 기능으로써 암호 화폐에 따라 구현 방식은 다르다. 비트코인의 경우 일반적인 디지털 서명이 아닌 특정한 조건을 가지는 거래를 만들고, 조건이 만족되는 경우에 해당 거래에 묶여 있는 비트코인이 사용되는 방식이고, 최근 높은 범용성으로 관심을 받고 있는 이더리움(Ethereum)의 경우에는 Contract에 해당하는 주소 자체를 생성하여 주소에 일정 금액과 금액을 사용하기 위한 조건이 담긴 프로그램을 함께 담을 수 있게 하는 높은 수준의 스마트 컨트랙트 기능을 선보이고 있다. 특히 스마트 컨트랙트는 암호 화폐 시스템의 일부이기 때문에 비트코인과 같은 제한적인 형태이던 이더리움의 독립된 형태이던 블록체인 내부에서 존재하면서 시스템에 참여하고 있는 모든 Full 노드들에 의해서 검증의 대상이 된다. 그래서 IoT 외부에 존

재하면서도 IoT 거래와 관련된 작업을 안전하게 수행할 수 있는 플랫폼으로 사용할 수 있다. 즉 IoT 기기는 가장 기본적인 서비스만을 제공하고 지불관련 프로그램은 스마트 컨트랙트 형태로 블록체인에서 확인 받는 이원화된 구조로 안전성을 높일 수 있다.

5. 결 론

IoT 환경에서의 결제는 모바일 결제를 제외하고는 아직 연구 및 개발 단계에 머물러 있다. 자율성을 가지는 IoT 기기의 결제의 경우에는 모델이 가지고 있는 가능성 때문에 많은 논의가 이루어지고 있지만 역시 구체적인 정립이 아직 필요한 실정이다. 비록 구체적인 서비스 모델이 없는 상황에서 보안을 적용하기에는 어려운 점이 있지만 장기적인 관점에서 신뢰성 있는 IoT환경의 거래 시스템을 구성하기 위해서는 모델 정립 과정에서 보안의 문제들이 함께 고려되어야 한다.

IoT 환경은 기존의 컴퓨팅 환경의 연장선에 있다. 따라서 기존 컴퓨팅 환경에서 사용되던 기법들을 그대로 적용하여 IoT 환경에서의 결제 또는 지불 시스템을 만드는 방향으로 현재 서비스들이 개발되고 발표되고 있으나 이는 IoT가 단순히 무선통신이 가능한 작은 기기들의 모임이 아님을 간과하는 것이다. 따라서 새로운 플랫폼에서 금융 서비스가 발생하는 이유 및 의미를 고려하고 플랫폼에 맞는 안전한 거래 시스템을 구성하는 방안에 대한 고민이 지속적으로 필요한 시점이다.

참 고 문 헌

[1] Brody, P., and Pureswaran, V. Device Democracy. IBM Global Business Services, 2014.

[2] Wörner, D., and Bomhard, von, T. “When your sensor earns money: exchanging data for cash with Bitcoin”, Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, 2014

[3] Isaac, J. T., and Zeadally, S. “Secure Mobile Payment Systems”, IT Professional, 16(3), pp.36-43.

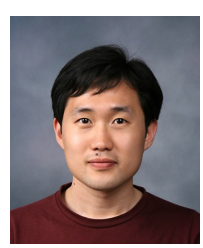
[4] Murdoch, S. J., Drimer, S., Anderson, R., and Bond, M. (2010). “Chip and PIN is Broken”, Proceedings of the 2010 IEEE Symposium on Security and Privacy, 2010, pp.433-446.

[5] Bond, M., Choudary, O., Murdoch, S. J., Skorobogatov, S., & Anderson, R. “Chip and Skim: Cloning EMV Cards with the Pre-play Attack”, Proceedings of the 2014 IEEE Symposium on Security and Privacy, 2014.

[6] Richard Gendal, “Who will decide the future of retail payments?”, Insights on business, IBM Banking.

[7] Bitcoin Contracts, https://en.bitcoin.it/wiki/Contracts

저 자 약 력



이 종 협

이메일 : jonghyup@gachon.ac.kr

- 2009년 8월 연세대학교 컴퓨터과학과 졸업(공학박사)
- 2009년 9월~2012년 2월 Carnegie Mellon, CyLab 연구소(박사후연구원)
- 2012년 3월~2015년 2월 한국교통대학교 소프트웨어학과 조교수
- 2015년 3월~현재 가천대학교 금융수학과 조교수
- 관심분야 : 금융 보안, 소프트웨어 보안