스타일러스 펜을 활용한 소유 및 속성 기반의 본인 인증 방식 제안

김현지* 장경배* 권혁동* 김현준* 서화정*†

*한성대학교 IT융합과

Proposal of possession and inherence based user athentication method using stylus pen

Hyun-Ji Kim* Kyeong-Bae Jang* Hyeok-Dong Kwon* Hyun-Jun Kim* Hwa-Jeong Seo*†

*Division of IT Convergence Engineering, Hansung University.

요 약

최근 신용카드의 사용 비중이 늘어나고 있으며 그에 따른 보안 위협이 증가함으로써 금융 거래에서의 보안이 중요해지고 있다. 신용카드 분실, 명의 도용 사고 등의 관련 범죄에 취약함에도 불구하고 카드 결제 시 사실상 보안 절차가 없는 상황이다. 이와 같은 현재 신용카드 결제의 한계점을 보완하기 위해 본 논문에서는 가속도 및 자이로스코프 센서가 내장된 스타일러스 펜을 통한 서명 과정과 기존 신용카드 결제 프로토콜을 접목시켜 보안적 기능이 없던 결제 서명 과정을 본인 인증 과정으로 바꾸어 금융 거래에서의 안전성 및 보안성을 증진시키는 방법을 제안한다.

I. 서론

최근 신용카드의 사용 비중과 결제 건수가 증가하고 있고 이에 따른 보안 위협도 커지는 추세이다. 금융감독원이 분석한 지난 5년간의 신용카드 부정사용 현황에 따르면 카드 소지자의 부주의 등에 의한 카드 분실, 도난 및 제 3자의 범죄로 인한 카드 부정사용이 연간 약 38000건 가까이 발생하고 있다. 이처럼 빈번히 발생하는 관련 범죄를 방지하기 위해 더 철저한 본인인증 과정을 위한 추가적인 보안 절차가 필요함에 따라, 새로운 인증 기법을 제안한다.

II. SET protocol (Secure Electronic Trans action) [1]

SET는 신용카드 결제 시 사용되는 프로토콜이다. 메시지 암호화, 디지털 서명 등을 통해 안전한 결제를 수행할 수 있도록 하며 메시지의 무결성이 보장되어 정당한 거래인지 판단 후 거래가 승인된다. 참여 주체는 카드 사용자, 상인, 지급정보 중계기관, 인증기관, 카드사, 매입사이며, 공개키 암호 방식(1024 비트 RSA), 비밀키 암호 방식(56 비트 DES), 서명 알고리즘(1024 비트 RSA), 해시(160 비트 SHA-1)의 알고리즘이 사용된다. SET의 가장 큰 특징은 이중 서명 알고리즘이다. 이중 서명은 고객의 지불 정보의 노출 가능성과 판매자에 의한 지불 정보의 위/변조의 가능성을 없애 정당성을 확인하기 위해 도입되었다.

SET protocol은 카드만 가지고 있다면 카드 명의자 본인이 서명하는지 확인할 방법이 없어 사실상 보안 절차가 없다는 점이 현재 신용카드 및 간편 결제 거래의 한계점이다.

III. 시스템 제안

기존의 거래 방식에서의 결제 시 서명은 형식적으로 수행되는 경우가 많아 카드를 소지하고 있다면 본인이라고 판단하여 카드 부정사용의 범죄가 발생할 우려가 크다. 이러한 한계점을 보완하기 위해 보안적 요소가 추가되어야 한다. 따라서 결제 시 사용한 카드가 실제 본인 소유임을 검증할 방법이 필요하다.

이를 위해서 가속도 센서 및 자이로스코프 센서가 내장된 스타일러스 펜을 활용하여 본인 인증 절차를 수행하는 방법을 제안하고자 한다. 카드 명의자 소유의 스타일러스 펜으로 서명되었음을 확인하여 본인임을 인증하는 방식이다. 신용카드 소유자와 스타일러스 펜의 소유자가 일치하는지 확인하고 거래의 마지막 단계인 본인 서명을 자신의 스타일러스 펜으로 하여 인증 절차를 수행한다.

본 제안기법은 보안 레벨은 높아지지만 번거로움이 있고, 평균적으로 고액결제를 하거나 보안 위협의 리스크가 큰 카드를 사용자가 사전에 등록해 두고, 해당 카드 사용 시에 적용 한다면 유의미하다고 판단되어 스마트폰에 등록된 카드에 선택적으로 제공하고자 한다.

SET 프로토콜에 본인 소유의 스타일러스 펜으로 서명함으로써 인증하는 과정이 추가되었다. 기존의 결제 과정을 거쳐 승인 가능 카드임을 확인 후 카드 사용자에게 결제 서명을 요청한다. 서명 시 스타일러스 펜의 움직임을 가속도 및 자이로센서가 측정하여 블루투스로 연결된 스마트 폰을 통해 서버로 전송하고, POS기를 통해 전송된 서명과 유사도나 시간 등의 상호 비교를 통해 거래 당사자가 자신의 카드로 거래하였고 동의했음을 인증할 수 있게 된다.

3.1 스타일러스 펜과 카드의 동시 소유를 통한 본인인증 방법

기존의 SET과 동일하게 진행되지만, 암호화된 지불 정보에 결제 시 사용한 카드가 등록된 스마트 폰의 소유자 이름, 해당 스마트 폰과 스타일러스 펜의 블루투스 통신 여부 등의 정보가 추가된다. 이를 통해 카드 명의자와 펜의 소유자가 같음을 증명함으로써 본인 인증이 가능해진다.

3.2 스타일러스 펜을 활용한 서명 상호 비교를 통한 본인인증 방법

스타일러스 펜은 앞서 언급한 가속도 및 자이로센서가 내장되어 있다. 두 센서를 통해 사용자의 움직임에 따른 데이터를 추출하며 측정된 데이터는 벡터 값으로 저장되고 정확한 인식이 가능하여 동작 인식 알고리즘을 거치면 사용자의 펜으로 입력한 서명을 대략적으로 알 수 있다. 스타일러스 펜은 본인 스마트 폰과 블루투스로 연결되어 있으므로 측정된 데이터를 전송하고, 스마트 폰은 전달 받은 측정값과 스타일러스 펜과의 블루투스 통신 정보를 거래 발생 시 생성되는 스마트 폰과 서버의 세션키($K_{S'}$)로 암호화 하며, 사용된 세션키($K_{S'}$)는 서버의 공개키(K_{Server})로 암호화 되어 서버로 전송된다. 동시에 POS기를 통해 입력된 서명도 전송된다. 서버는 세션키($K_{S'}$)를 통해 복호화 하여 전달된 값들의 특성벡터(모양, 압력, 속도, 시간, 획 순서 등)를 비교한 후, 두 서명의 유사도를 측정하여 일치한다고 판별되면 최종적으로 거래를 승인하게 된다.

3.3 기존방식과의 본인 인증에 대한 정확성 비교

	기존 방식	제안 기법
명의 확인 (소유기반)	낮음	높음
지문 인증 (속성기반)	없음	높음
결제 서명 (소유+행위)	사실상 낮음	매우 높음
본인인증 정확성	낮음	매우 높음

표.1. 기존 방식과의 본인인증 정확성 비교

행위적 특성을 이용한 생체인증 기반의 방식은 정확도가 매우 높고 두 서명의 발생 시점과 거래 발생 시점을 비교하여 더 정확한 본인인증이 가능해진다.

분석 요소	정확성
가속도 및 자이로센서 융합	움직임의 정확한 측정 가능
다양한 특성벡터 분석	모방 불가능
발생 시점 비교	시간 초과 시 인증 불가
	높음

표.2. 결제 서명을 통한 본인인증의 정확성

3.4 본인 인증에 대한 보안 강도 비교 분석

	기존 방식	제안 기법
복합 인증 적용	없음	있음
부인 방지 기능	사실상 없음	있음
부정사용 위협	높음	낮음
인증 정보 유출 및 해킹 위험성	높음	매우 낮음

표.3. 기존 방식과의 보안 강도 비교

본 논문에서 제안한 기법은 스타일러스 펜을 소지하고 있으며 거래 시 꺼내야 한다는 번거로움이 존재하지만 본인의 신용카드 및 스마트폰의 소지 여부와 서명 인식을 통해 복합적으로 인증함으로써, 상대적으로 인증 수단의 도난 위험이 있는 기존의 신용카드 결제 방식이나 NFC 기술을 활용한 모바일 신용카드를 통한 결제 방식보다 더 확실한 본인인증이 가능한 것이 장점이다.

IV. 결론

본 논문에서는 스타일러스 펜을 활용한 본인인증 절차를 제안하였다. 기존 본인 서명 절차는 형식상 거쳐야 하는 단순 부인 방지 서비스이지만 어차피 거쳐야 하는 서명 과정을 본인 인증 과정으로 바꾸어 금융 거래에서의 안전성 및 보안성을 증진시켰다. 또한, 도난사고 뿐만 아니라 명의 도용 사고를 방지하기 위해 카드 발급 시 본인 인증 절차에도 적용될 수 있을 것으로 보인다. 이 외에도 서명을 통한 본인인증 과정이 필요한 분야 등 다양한 분야에 적용될 수 있을 것으로 기대된다. 그러나 더 확실한 본인인증을 위해 거쳐야 할 단계와 데이터가 늘어나고 POS기 또한 해킹의 위험에 노출되어 있어 개인정보의 유출 우려가 있다.

본 제안 기법과 더불어 데이터 교환 및 키 관리에 있어 보안성이 보장된다면 더 안전한 금융 거래가 가능해질 것이다.

[참고문헌]

[1] Incheon Paik. (1998). Framework Architecture for Electronic Commerce Software System Based on SET Protocol. The Korean Institute of Information Scientists and Engineers, 25(1A), 732-734.