금융거래와 LFSR를 활용한 보안 방식 제안

김기환 · 박성환 · 유서영 · 이훈재

동서대학교

Proposal of security method using financial transactions and OTP

Ki-hwan Kim · Seong-hwan Parkn · Seo-yeong Yu · Hoon-jae Lee

Dongseo University

E-mail : ghksdl90@naver.com / hjlee@gdsu.dongseo.ac.kr

요 약

현대사회의 금전적인 거래는 대부분 온라인상에서 거래되고 있으며, 오프라인상에서도 현금거래 이외에도 카드 및 스마트폰 등으로 거래가 가능하다. 온라인상에서 이루어지는 금전적인 거래의 장점은 구매과정이 간략하고 현찰로 인한 부피증가와 무게 등의 이동성 저하 요인이 사라진다는 점이다. 그러나 온라인 환경은 물리적인 거리에 제약사항이 없으며, 타인에게 개인정보가 노출될 경우 금전적 손실과 직결될 수 있다는 문제가 있다. 물론 대부분의 금융권에서는 금융 사고에 대비한 보안 정책이 운영되고 있기에 별다른 문제는 없다. 본 논문에서는 OTP를 활용하여 고정적인 카드번호, 유효기간, CVC 등을 매회 임의로 변경하는 것으로 암호화된 정보의 탈취 방지 및 간단한 구조로 동작이 가능함을 보이고자 한다.

ABSTRACT

Most of the financial transactions in modern society are traded online, and offline transactions can be made with cards and smart phones in addition to cash transactions. The advantage of monetary transactions on-line is that the purchasing process is simple, volume increases due to cash, and mobility degradation factors such as weight disappear. However, the online environment has no limitation on the physical distance, and there is a problem that if personal information is exposed to another person, it can be directly connected with financial loss. Of course, in most financial sectors, there is no problem because security policies are prepared for financial accidents. In this paper, we show that it is possible to prevent stealing of encrypted information and to operate with a simple structure by arbitrarily changing the fixed card number, expiration date, and CVC every time using OTP.

키워드

OTP, LFSR, Security, Card, Personal informations

Ⅰ. 서 론

최근에는 편의점에서 1000원을 결제할 때도 신용카드를 사용하는 경우가 많으며 현금보다는 체크카드 및 신용카드를 주로 사용한다. 이와 같은 거래방식의 변화는 생활방식과 소비패턴의 변화를 일으키고 있다. 하지만, 이러한 급격하게 카드 사용비율이 높아지면서 보안상의 문제점도 나타나고 있다. 몇 가지 사례로 한국 온라인 쇼핑몰에서 600여 건의 신용카드 도용사고가 발생하였다. 이에 업계 관계자는 마그네틱 카드에 담긴 고객 정보가 일부 유출돼 신용카드 도용사고가 벌어진 것으로 추정하였다. 해외구매 역시 국내 신용카드가 무더기 해킹된 정황이 포착되었다. 그 정보가 유출될 경우 무단 복제, 부정사용, 카드 번호 유출 등의 위험이 심각하다. 실제로 미국과 중국 등에서 몇 분 간격으로 수백 달러가 결제되거나 해외 사설 주차장 등 온라인뿐만 아니라 오프라인 가맹점에

서도 부정사용 사고가 발생했다. 신용카드의 카드 번호, CVC, 비밀번호를 알면 해커의 불법적인 사용을 막지 못하는 실정이다. 본 논문에서는 OTP와 LFSR을 활용하여 인증 방식을 제안한다.

II. 관련 연구

1. OTP 생성 및 인증 방식

OTP가 등장하게 된 이유는 인터넷의 폭발적인 보급 때문이다. 경제적 행위의 안전을 보장하기에 적합하다고 볼 수 있다. OTP는 일회용 인증번호 생성기라는 의미로써 수학적 유추가 불가능하다. 고정된 번호 대신 무작위로 생성되는 일회용 번호를 이용하는 사용자 인증 방식의 단말기로 OTP의 핵심 원리는 인증번호가 일회용이라는 것이다.

1.1. 시간 동기화 방식

OTP를 생성하기 위해 사용하는 입력 값으로 시간을 사용하는 방식이다. 사용자는 현재 시간을 입력으로 OTP를 생성해 서버로 전송하고, 서버 역시 같은 방식으로 OTP를 생성하여 사용자가 전송한 값의 유효성을 검사한다[4].

임의의 입력이 필요하지 않다는 점에서 사용하기 간편하고, 사용자가 서버와 통신해야 하는 횟수가 비교적 적다. 또 서버에서 사용자에 입력을 보내는 방식이 아니므로, 여타 OTP 생성 방식에 비해 피싱에 안전하다. 한편 사용자에서 시간 정보를 이용해 OTP를 생성하므로, 스마트폰 등의 모바일 기기도 사용자로 사용되기 적합하다는 점 역시 비용 절감 측면에서 장점이다.

하지만 사용자와 서버의 시간 동기화가 정확하지 않으면 인증에 실패하게 된다는 단점이 있으며, 이를 보완하기 위해 일반적으로 1~2 분 정도를 OTP 생성 간격으로 둔다.

1.2. 챌린지 • 응답 방식

서버에서 난수 생성 등을 통해 임의의 수를 생성하고 사용자에 그 값을 전송하면, 사용자가 그 값으로 OTP를 생성해 응답한 값으로 인증하는 방식이다[3].

입력이 매번 임의의 값이 된다는 측면에서는 안전성을 갖추고 있으나, 네트워크 모니터링에 의해 전송되는 값들이 노출될 경우 매우 취약해진다는 단점이 있다. 또 서버와 사용자 사이의 통신 횟수도 비교적 많이 요구된다.

1.3. 이벤트 동기화 방식

서버와 사용자가 카운트 값을 동일하게 증가시켜 가며, 해당 카운트 값을 입력으로 OTP를 생성해 인증하는 방식이다.

다만 사용자에서 OTP를 생성하기만 하고 인증에 사용하지 않으면, 서버와 사용자의 카운트 값이 불일치하게 된다는 문제점이 있다. 이러한 문제를 보완하기 위해 어느 정도 오차 범위 내에서는 인증을 허용하는 방법이나, 카운트가 어긋났다고 판단될 경우 연속된 OTP를 받아 유효성을 판별하는 방법 등이 사용된다.

2. OTP 전달 방식

2.1 OTP 토큰

OTP 토큰이라 불리는 별도의 하드웨어를 사용자로 사용하는 방식이다. 기기 자체에서 해킹이 이루어지기는 힘들지만, 토큰을 구입해야 하므로 추가 비용이 필요하며 휴대하기에 불편하다는 단점이 있다[3].

2.2. 스마트폰 앱

별도의 하드웨어 장비를 필요로 하지 않아서 추가 비용 없이도 OTP 서비스를 이용할 수 있는 방식이다[3]. 해당 스마트폰에 맞게 제공되는 앱을 설치함으로써 이용할 수 있다. 물론 서버 측에서 이 방식을 지원하지 않으면 이용할 수 없으며, 스마트폰 OS에 따라 이용이 제한될 수 있다으며 해킹 위험성이 높다는 단점이 있다.

2.3. SMS

SMS로 OTP를 전달하는 방식이다. 스마트폰이 아닌 어떤 종류의 휴대전화만 있어도 이용 가능하다는 장점이 있지만, SMS 자체의 해킹 위험성에 의해 현재는 거의 사용되지 않고 있다[5].

3. LFSR

선형 되먹임 스프트 레지스터(Linear Feedback Shift-Register:LFSR)는 0 또는 1을 레지스터에 이전 상태 값들의 선형 함수로 계산되는 구조를 가지고 있다[2]. 선형 함수는 주로 배타적 논리합(XOR)로 연결하고 초기값을 시드(Seed)라고 부른다[1].

LFSR로 생성된 수열은 그림1, 그림 2와 같이 피보나치 방식 혹은 갈루아 방식의 이진수로 생각할 수 있다. 두 가지 방식에서 영향을 미치는 출력을 “탭(Tap)”이라고 하며, N 비트의 길이를 가지는 LFSR은 $2^N - 1$ 주기를 가지는 결정론적인 시스템이다.

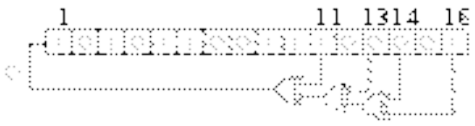

그림 1. 피보나치 LFSR 동작구조

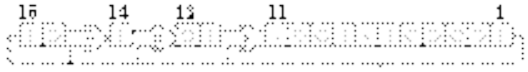

그림 2. 갈루아 LFSR 동작구조

III. 제안방식

본 논문에서는 전체적인 구성은 OTP의 챌린지 응답 방식과 시간 동기화 방식을 활용하고 상호간 인증에는 LFSR을 활용해보았다.

1. 초기화

초기화를 위하여 카드정보(Card number : N)와 고유번호(Seed : S) 그리고 시간(Time : T)을 입력해야만 한다. 위의 3가지 항목은 식 (1)처럼 모두 자연수를 원자로 가지는 집합이다.

$$N, S, T \in R \quad (1)$$

또한 카드정보는 16자리 숫자로 구성되어 있으며, 시간은 4자리 년도와 2자리 월 2자리 일로 총 8자리의 숫자로 구성된다. 마지막으로 고유번호는 임의의 길이로 생성이 가능하며, LFSR의 길이보다는 크거나 같은 구성을 취하는 것으로 만족할 수 있다.

초기값은 식(2)와 같이 카드번호와 시간을 곱하고 고유값을 더하여 128비트 크기로 나눈 나머지이다.

$$(N^{*}\ T+S)\bmod 128 = LFSR_{Init} \quad (2)$$

초기화 단계의 마지막으로 그림 1과 같이 3가지 고유정보를 입력하여 128비트 LFSR에 대입한다.

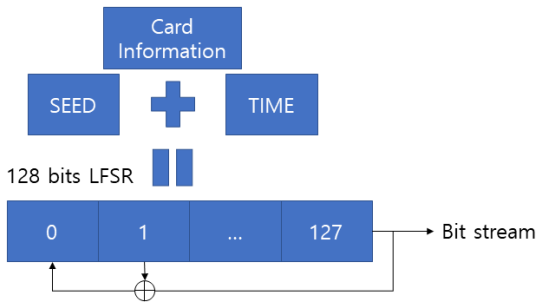

그림 3. 초기화 과정

2. 사용자 동작

사용자측에서는 초기화 과정 후 서버에 신분을 인증하기 위하여 LFSR을 통해 식 (2)처럼 사용자와 서버간의 약속된 위치(K_S)를 사용하여 생성된 64비트 가운데 16비트를 선택하여 전송한다.

$$LFSR_{128}(M)|K_S|error = LFSR_u \quad (3)$$

이때, 16비트 가운데 임의의 4비트 이상이 잘못된 값으로 치환한다. 최종적으로 식(3)과 같이 16비트와 M회 LFSR을 동작시킨 결과를 사용해야 하기에 16비트와 M을 서버에 전송한다.

$$LFSR_{user}, M(running) \quad (4)$$

3. 서버 동작

먼저 서버는 LFSR 초기화를 진행하고 식(4)처럼 사용자에게 수신 받은 내용에서 M을 확인하고 인의의 동작하여 사용자로부터 전달받은 16비트 가운데 틀린 위치를 찾아낸다.

$$LFSR_u|LFSR_s = find_{error} \quad (5)$$

이후 임의로 K번 LFSR을 동작시킨 64비트 결과를 가공하여 16비트로 생성한다. 이때, 사용자로부터 전달받은 16비트의 틀린 정보 위치를 반전시켜 선택하여 연산 후 사용자에게 전송한다.

$$LFSR_{128}(M+K)|K_S|!error = LFSR_s \quad (6)$$

4. 상호간 인증

사용자측은 임의의 문제로 요청하고 서버는 요청에 대한 응답을 해결하는 것으로 서버는 사용자에 대한 인증을 수행할 수 있다. 반대로 서버가 사용자에게 다른 문제로 요청하여 사용자가 올바른 사용자측과 서버측간의 전송에러가 존재하지 않는다면 상호간의 인증이 완료된다.

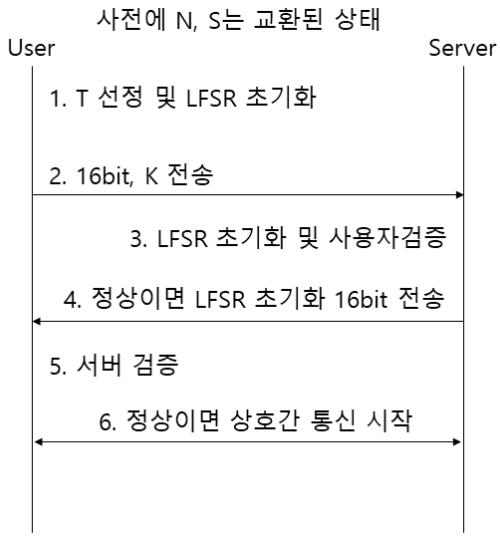

그림 4. 상호인증 과정 정리

IV. 결론

OTP와 LFSR을 혼용하여 사용하는 것으로 신용카드와 결합을 통해 사용자의 개인정보가 해킹되지 않게 막고, 사용자가 실시간으로 16자리 카드번호가 변경되는 것을 제안하였다. 특히 카드번호는 대부분 공개되어 있는 부분이 많은데 해커가 카드

번호, 고객정보를 가지고 침입했을 경우를 대비하여 제안하였다. 본 논문에서는 제안만 이루어진 상태이므로 추후에 구현을 해볼 예정이다. 본 논문을 집필하면서 현재 카드 보안 체계와 각종 보안 구조에 대하여 공부할 수 있었으며, 앞으로의 미래 보안 기술 발전 동향에 대하여 많은 것을 알 수 있었다고 생각한다.

Acknowledgement

이 논문은 2018년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원(No.2018-0-00285,무인이동체를 위한 HD급 영상 데이터 및 제어 신호 암복호 처리용 고신뢰 듀얼코어 SoC 및 운용시스템 개발)과 2016년도 정부정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(과제번호: NRF-2016R1D1A1B01011908).

References

[1] Linear-feedback shift registerp[Internet]. Available : https://en.wikipedia.org/wiki/Linear-feedback_shift_register.

[2] 선형되먹임 시프트 레지스터[Internet]. Available : https://ko.wikipedia.org/wiki/%EC%84%A0%ED%98%95_%EB%90%98%EB%A8%B9%EC%9E%84_%EC%8B%9C%ED%94%84%ED%8A%B8_%EB%A0%88%EC%A7%80%EC%8A%A4%ED%84%B0.

[3] OTP[Internet]. Available : https://namu.wiki/w/OTP

[4] 2차인증 소개[Internet]. Available : https://d2.naver.com/helloworld/279640

[5] OTP[Internet]. Available : http://wiki.wikisecurity.net/wiki:otp