한국통신학회논문지 '13-06 Vol.38B No.06
http://dx.doi.org/10.7840/kics.2013.38B.6.492

PUF를 이용한 OTP 기반 거래 검증 프로토콜

이 종 훈◆, 박 민 호*, 정 수 환°

OTP-Based Transaction Verification Protocol Using PUFs

Jonghoon Lee◆, Minho Park*, Souhwan Jung°

요 약

One-Time Password(OTP) 발생기는 현재 은행이나 증권 회사에서 전자금융 거래 시에 안전한 거래를 보장하기 위해 multi-factor 인증으로 사용되고 있다. 국내 OTP 기반 전자금융 거래 검증 프로토콜은 OTP 인증 정보를 통해 사용자에 대한 신원을 확인함으로써 안전한 거래를 보장하며, 또한 Man-in-the-Browser(MITB) 공격, 메모리 해킹 공격 등에 대처하기 위해 사용된다. 하지만 지능적인 피싱, 파밍, 사회공학 공격들을 통해 OTP 생성 단말에 대한 정보를 수집하여 활용한다면 동일한 OTP 값을 생성할 수 있는 가능성이 있다. 그러므로 이와 같은 위협에 대응할 수 있는 대책이 필요하며 본고에서는 앞에서 언급한 문제점을 해결하기 위해 Physical Unclonable Functions(PUFs)을 이용한 새로운 기법을 제안한다. 먼저, 물리적으로 PUFs를 복제할 수 없는 특성은 동일한 OTP 값을 생성하는 것을 불가능하게 만든다. 또한 하드웨어적으로 OTP 발생기를 복제하는 것이 불가능하다. 결론적으로 제안된 프로토콜은 PUFs를 추가함으로써 이전 프로토콜보다 강력하고 안전한 인증 프로토콜을 제공한다.

Key Words : OTP, Authentication, PUFs, HMAC, CRPs

ABSTRACT

The One-Time Password(OTP) Generator is used as a multi-factor authentication method to ensure secure transaction during e-Financial transaction in the bank and securities company. The OTP based e-Financial Transaction Verification Protocol ensures secure e-financial transaction through confirming the user's identity using OTP authentication information and counters not only Man-in-the-Browser(MITB) attacks but also memory hacking attacks. However, it is possible to generate correct OTPs due to potential of stealing sensitive information of the OTP generator through intelligent phishing, pharming, social engineering attacks. Therefore, it needs another scheme to prevent from above threats, and this paper proposes advanced scheme using Physical Unclonable Functions(PUFs) to solve these problems. First, it is impossible to generate the same OTP values because of the hysically unclonable features of PUFs. In addition, it is impossible to clone OTP generator with hardware techniques. Consequently, the proposed protocol provides stronger and more robust authentication protocol than existing one by adding PUFs in the OTP generator.

※ 본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었습니다. (NIPA-2013-H0301-13-1003)
※ 본 연구는 산업통상자원부 및 한국산업기술평가관리원의 산업융합원천기술개발사업(정보통신)의 일환으로 수행되었습니다. (10041671, 엔터프라이즈 무선랜 통합제어 관리 시스템 기술 개발)
◆ 주저자 : 숭실대학교 전자공학과 통신망보안 연구실, ttaz@ssu.ac.kr, 학생회원
° 교신저자 : 숭실대학교 정보통신전자공학부 통신망보안 연구실, souhwanj@ssu.ac.kr, 종신회원
* 숭실대학교 정보통신전자공학부, mhp@ssu.ac.kr
논문번호 : KICS2013-04-192, 접수일자 : 2013년 4월 25일, 최종논문접수일자 : 2013년 5월 27일

Ⅰ. 서 론

OTP는 일회용 패스워드로써 안전한 인증 방법으로 활용되고 있다. 특히, 국내의 경우 전자금융 거래 시에 사용자의 신원 확인을 검증하기 위해 추가 인증 요소로 사용함으로써 안전한 전자금융 거래를 보장한다. 하지만 피싱, 파밍, 그리고 사회공학 공격들이 지능화됨에 따라 다양한 위협들이 여전히 존재하고 있다. 또한 최근 공격자들은 특정 대상을 하나의 목표로 설정하여 해당 공격 대상자의 중요 개인 정보를 수집하여 금전적인 피해 사고를 야기키시고 있다. 정교한 공격들을 통해 사용자들의 전자금융 관련 정보들을 충분히 수집한다면 금융 피해 사고로 이어질 것이다. 2011년에 SecureID라는 OTP 발생기를 제조하는 RSA의 일부 시스템이 해킹되어 OTP 발생기의 정보가 유출되었으며, 이로 인해 국내의 경우 SecureID 제품을 회수 하는 등의 조치가 있었다. 그러므로 다양한 위협에 대해 예방하기 위한 대책을 마련하는 것이 지속적으로 요구된다.

본고에서는 이 문제에 대한 대책을 제시하기 전에 먼저 OTP의 기본적인 특징에 대해 살펴보고 그것의 문제점을 들여다 볼 것이다. 그런 후에 결론적으로 OTP의 문제점을 대처할 수 있는 효과적인 방법을 제시할 것이다. OTP는 기본적으로 단방향 함수인 해쉬 함수의 이점을 이용하여 랜덤한 값을 생성함으로써 Replay Attack에 대처한다. 그러나 도청, 사회공학 또는 적극적인 공격들은 여전히 존재하고 있다. 현재 국내의 경우 가장 안전하다고 판단되는 시간 동기 방식의 OTP(The Time Synchronized OTP) 발생기를 사용하고 있으며 이는 서버와 OTP 단말 간에 같은 클락 정보를 사용한다. 그러나 공격들이 점점 지능화됨에 따라 다양한 공격들이 존재하고 있으며, 특히 공격자가 특정 목표를 대상으로 하여 개인 정보를 충분히 수집한다면 같은 OTP 값을 생성할 수 있는 가능성이 있다. 그리고 또한 하드웨어적 기술을 통해 OTP 발생기를 복제할 수 있는 가능성도 간과할 수 없다. 그러므로 이와 같은 문제점들을 대처할 수 있는 안전한 방안들에 대해 반드시 고려해야 한다. 기존에는 클락 카운터를 이용한 스트림 암호 방식[1] 및 key 입력 장치를 통한 안전한 OTP에 대한 연구[2]가 있었다. 본고에서는 이와 같은 문제점들을 대처하기 위해 PUF 회로의 결과 값을 복제할 수 없는 특징을 가지고 있는 PUF의 특성을 활용하는 안전한 새 OTP 프로토콜을 제안한다.

이후 본고는 다음과 같이 구성된다. 2장에서는 실제 금융권에서 사용되고 있는 OTP 인증 시스템의 위협 요소에 대해 알아보고, 3장에서는 기존의 OTP 기반 전자금융 거래 검증 프로토콜을 살펴본 후 개선된 프로토콜에 대해 설명한다. 다음으로 4장에서는 제안한 프로토콜에 대해 분석하고, 마지막으로 5장에서는 본고의 결론을 제시한다.

Ⅱ. 보안 위협

일회용 패스워드를 생성하는 원리는 기본적으로 해쉬 함수와 같은 암호 함수의 출력 값을 사용[3,4]하며, 여기서 비밀키와 보안 토큰(Security Token)이 가지고 있는 정보를 함수의 입력 값으로 활용한다. 그림 1은 OTP 생성의 원리를 보여주며 보안 토큰 관련 정보는 단말기와 서버 사이에 공유하고 있는 정보인 Challenge, 시간, 이벤트 등을 말한다.

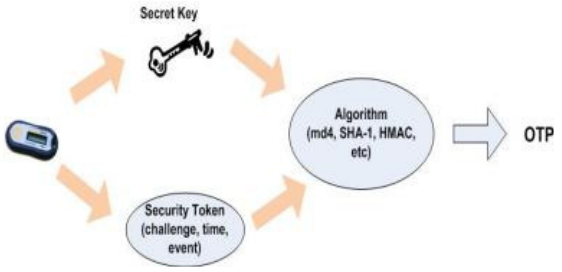

그림 1. 일회용 패스워드의 기본 원리
Fig. 1. The Principle of Generating OTP

현재 금융 시스템에서 사용하고 있는 시간 동기 방식의 OTP는 그림 2과 같이 서버와 OTP 발생기 사이에 서로 동기화된 시간 클락 정보와 비밀키로부터 생성된 OTP 인증 정보가 서로 일치하는지 확인함으로써 사용자의 신원을 확인한다.

그러나 공격자들이 다양하고 정교한 사회공학, 피싱 공격들을 이용하여 보안 토큰과 비밀키에 대한 정보를 수집한다면 충분히 같은 OTP 값을 생성할 수 있다. 다시 말해서 OTP 값을 생성하는 알고리즘을 살펴보면 단지 소프트웨어적 방법만 활용하기 때문에 같은 입력 정보만 입력한다면 같은 OTP 값을 생성하는 것은 가능하다. 게다가 공격자들이 하드웨어적 기술을 활용하여 OTP 발생기를 복제할 수 있다는 가능성도 배제할 수 없는 위협 요소이다.

그러므로 PUF와 같은 하드웨어 요소를 추가함으로써 더 안전한 방법을 제공하고자 한다. 공격자들이 OTP 발생기를 하드웨어 기술을 이용하여 복제하더라도 PUF의 특성으로 인해 PUF의 출력 값을 똑같이 만들 수 없기 때문에 같은 OTP 값을 생성하는 것 자체가 불가능하다. 또한 해당 PUF의 특성을 분석한다는 것도 실질적으로 쉽지 않다. 다음 장에서는 기존의 OTP 프로토콜을 살펴본 다음 PUF를 활용한 새로운 프로토콜을 제안함으로써 좀 더 강력한 보안을 제공하고자 한다.

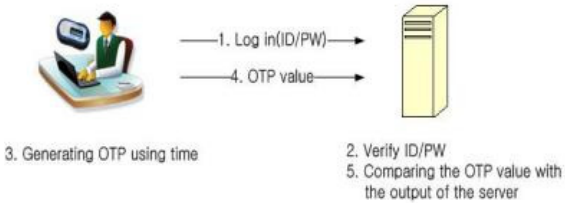

그림 2. 시간 동기 OTP의 기본 원리
Fig. 2. The Principle of Time Synchronous OTP

현재 은행 인터넷 또는 스마트 뱅킹 서비스는 그림 3에서와 같이 안전한 전자금융 거래를 위해

그림 3. 은행 시스템의 OTP 인증 정보
Fig. 3. An OTP Value of the Banking System

OTP 비밀번호를 추가 인증 정보로 사용한다. OTP 비밀번호는 매 1분마다 갱신되고 있으며, 1회만 사용이 가능하다. 실제로 OTP 비밀번호의 갱신 주기인 1분 안에 추가적으로 OTP 비밀번호를 사용했을 때에는 이미 사용하였으므로 OTP 비밀번호가 갱신된 후 사용하라는 경고 메시지를 출력한다. 다음으로 OTP 기반 전자금융 거래 검증 프로토콜은 그림 4에서와 같이 OTP 비밀번호는 비밀키, 시간 동기, 거래 정보 TI를 이용하여 HMAC-SHA1, SEED 등과 같은 암호 알고리즘을 통해 생성된다. 그림 4에서와 같이 OTP 발생기에서 실제 거래 정보 TI를 사용하고 있는지 확인하기 위해 실제 인터넷 뱅킹 시스템에서 간단한 테스트를 하였다. 우선 서로 먼저 PC에서 뱅킹 시스템에 접속하여 계좌이체를 실시하기 위해 준비하였고, OTP 비밀번호를 입력하기 전에 또 다른 PC에서 뱅킹 시스템에 접속하여 다른 계좌로 방금 전 생성한 OTP 비밀번호를 사용하여 이체를 시도한 결과 정상적으로 실행되는 것을 확인하였다. 따라서 현재 OTP 발생기에서는 거래정보 TI를 사용하지 않는 것으로 유추할 수 있으며, 또한 거래 조작 공격이 위협이 될 수 있다는 것을 예상할 수 있다.

Ⅲ. 제안 프로토콜

3.1. 기존 거래 검증 프로토콜

본고에서는 먼저 금융 시스템에서 사용되고 있는 OTP 프로토콜에 대해 살펴보고 더 강력한 OTP 프로토콜을 제시하고자 한다. 국내 금융 시스템에서 사용하고 있는 시간 동기 OTP의 보안 모델은 그림 4와 같다[5].

보안 모델에서 보듯이 거래 정보(Transaction Information)을 입력하는 방법은 3가지로 분류하고 있다.

ⓐ 사용자가 거래 정보를 직접 OTP 발생기에 부착된 키패드 등에 입력하는 방식
ⓑ 사용자터미널에 출력된 거래 정보를 OTP 발생기의 센서, 3D 바코드, QR코드 등을 통해 입력하는 방식
ⓒ 금융회사와 OTP 발생기가 직접 통신하여 거래 정보가 입력되는 방식

기존 거래 검증 프로토콜의 흐름도는 그림 5와 같으며 해당 표기는 표 1과 같다. 먼저 사용자 U_i는 계좌이체 등의 전자금융 거래를 수행하기 위해 거래 정보 TI를 사용자 터미널 A_i에 입력하여 거래 정보 TI를 금융 회사 B에 전달한다. 앞에선 언급한 3가지 방법을 통해 TI를 OTP 발생기에 입력한 후 사용자 U_i는 활성화 정보 λ를 OTP 발생기에 입력한 후 활성화 정보를 검증하여 일치할 경우 OTP 인증 정보를 생성하여 OTP 발생기 화면에 출력한다. 사용자 U_i는 OTP 인증 정보를 사용자 터미널 A_i에 입력하여 금융 회사로 B로 전달하며 금융 회사에서는 그 OTP 인증 정보에 대한 검증을 통해 사용자 신원 확인을 함으로써 전자금융 거래를 안전하게 수행한다. 하지만 앞에서 언급했듯이

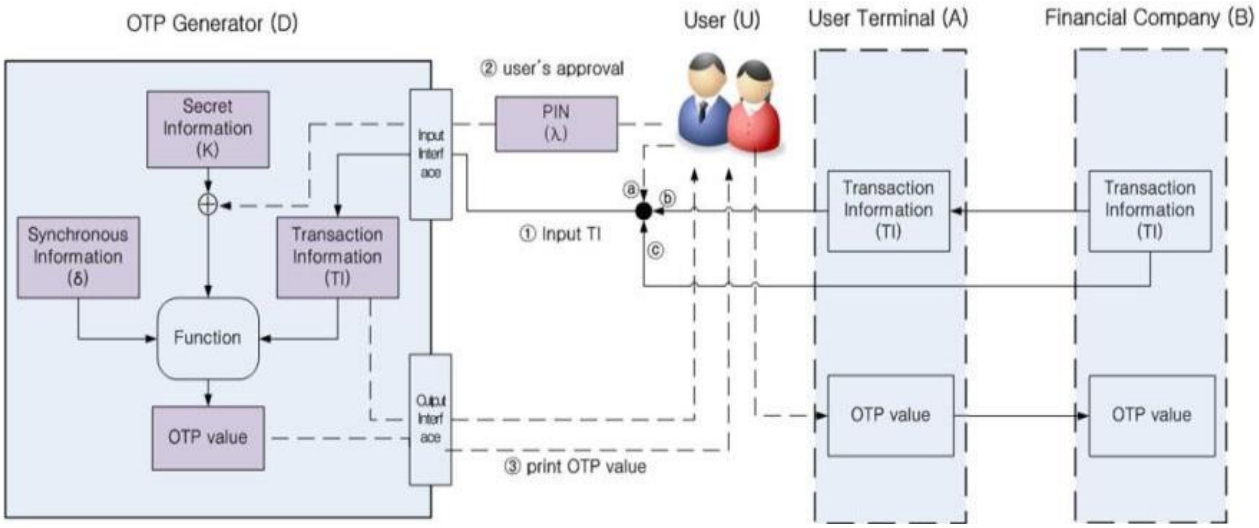

그림 4. 시간 동기 방식 OTP의 보안 모델
Fig. 4. The Security Model of Time Synchronous OTP

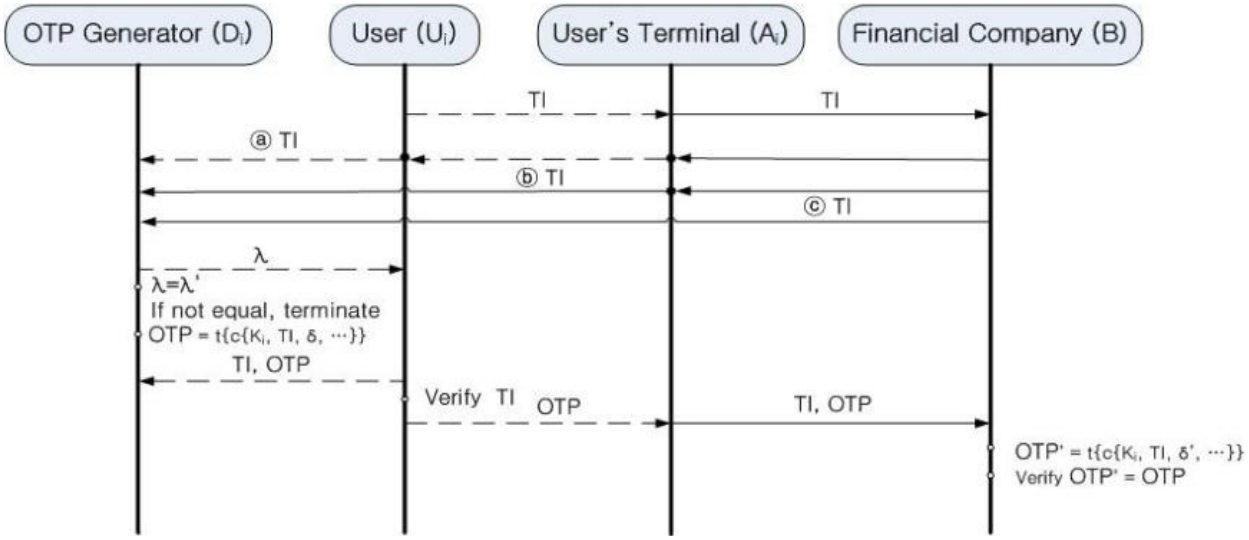

그림 5. 기존 거래 검증 프로토콜의 흐름도
Fig. 5. The Previous Protocol Flow

실질적으로 OTP 인증 정보는 거래 정보인 TI를 사용하지 않고 비밀키와 시간 동기 정보를 통해 생성된다. 거래 정보 TI를 사용하지 않기 때문에 공격자가 MITB나 도청 공격을 통해 OTP 인증 정보를 획득한 후 거래 정보 TI를 수정한다면 큰 문제를 야기 시킬 것이다. 이러한 문제에 대해 대처하기 위해 금융 시스템에서는 OTP 인증 정보를 갱신되기 전까지 한 번만 사용되도록 통제하고 있다. 하지만 공격자가 공격 대상 사용자의 OTP 인증 정보를 해당 사용자보다 먼저 입력하여 사용한다면 여전히 문제를 일으킬 수 있다.

표 1. 기존 프로토콜 표기법
Table 1. The Notation of the Previous Protocol

Notations	Descriptions
A_i	ith user's terminal
B	financial server
D_i	ith user's OTP generator
K_i	ith user's secret information
U_i	ith user
δ	sync information
λ	PIN

TI	transaction information
OTP	An OTP value
$c\{\cdot\}$	cipher algorithm
$t\{\cdot\}$	truncation algorithm
$f\{\cdot\}$	OTP generation algorithm
$A \rightarrow B$:	Send M from A to B through general communication channel
$A \dashrightarrow B$:	Send M from A to B through the channel that user recognizes

3.2. PUF의 특성

이러한 문제점들을 예방하기 위해 본고에서는 PUF와 TI를 이용하여 강력하고 안전한 인증 기법을 제안한다. 새로 제안하는 프로토콜에서는 PUF를 활용하는 기법으로 먼저 PUF가 지니고 있는 특성에 대해 살펴본 후 새로운 프로토콜에 대해 제시하겠다. Physical Unclonable Function이라는 용어의 의미에서 알 수 있듯이 물리적으로 복제할 수 없는 특징을 가지고 있는 IC 회로를 말한다. 다시 말해,

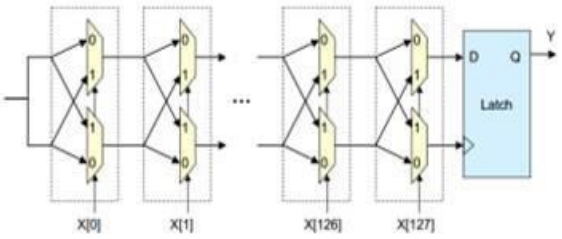

그림 6. Arbiter PUF 회로의 지연 경로
Fig. 6. An arbiter PUF delay circuit

공격자가 PUF의 IC 회로를 복제하더라도 원래 PUF IC 회로가 지니고 있는 특성까지 복제할 수 없다는 것이다. 따라서 공격자가 PUF 회로를 복제하더라도 같은 PUF의 출력 값을 생성하는 것이 불가능하다. 그림 6에서와 같이 다양한 PUF 회로 중 Arbiter PUF는 회로의 입력 값에 의해 delay 경로가 결정되며 어떤 path의 값이 먼저 도착하느냐에 따라 출력 값이 결정된다[6]. 또한 같은 delay 경로로 설정되었다하더라도 각 회로 소자가 가지고 있는 하드웨어 특성으로 인해 각 PUF 회로마다 출력 값이 다르게 나타난다. [7]에서는 기존의 연구된 PUF의 특징 및 장·단점에 대해 설명하고 있다. PUF는 회로가 가지고 있는 랜덤한 특징을 통해 입력에 대한 출력 값을 생성하며 이 출력 값은 PUF 회로마다 서로 다르다. 이러한 PUF의 특징을 활용하여 Challenge-Response 인증이나 키 생성 알고리즘으로 사용한다[6]. 그림 7에서와 같이 Challenge-Response Pairs(CRPs)를 이용하여 서버의 CRP 테이블 정보와 비교함으로써 인증을 수행할 수 있고 또한 PUF의 출력 값을 해쉬 함수를 통해 비밀키를 생성하는데 사용할 수 있다. PUF를 통해 인증 기법으로 활용하는데 있어 가장 큰 문제는 인증 서버에서 상당히 많은 양의 CRPs 테이블을 저장 관리해야 하므로 서버에 상당량의 부하가 예상된다. [8][9][10][11]에서는 RFID에서 PUF를 이용하여 HMAC 기반의 상호 인증 프로토콜에 대해 많은 연구들이 진행되었으며, PUF가 가지고 있는 문제점을 해결하기 위한 새로운 인증 프로토콜들을 제시하고 있다. 본고에서는 효율적인 PUF 인증 기법을 제안하고, 이를 OTP 프로토콜에 적용하여 강력하고 효과적인 인증 기법을 제시한다.

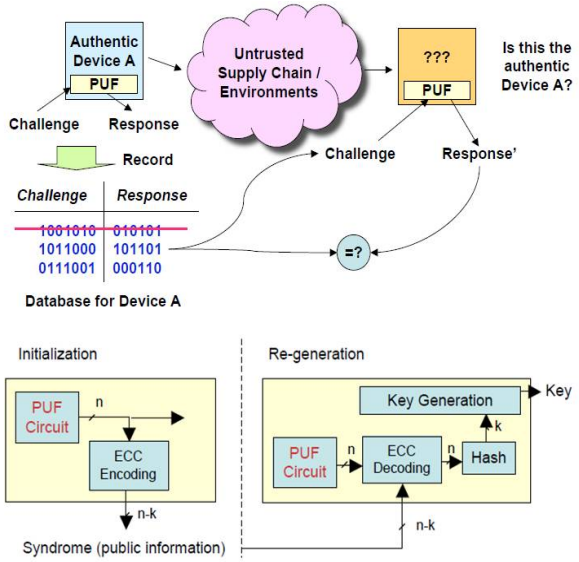

그림 7. PUF 기반 인증 및 키 생성 원리
Fig. 7. Overview of PUF-based Authentication and Cryptographic Key Generation

3.3. 제안 프로토콜

본고에서는 먼저 거래 정보 TI를 입력하는 방식 중 3번째 방법인 금융 시스템과 OTP 발생기 간에 PUF의 CRPs와 거래 정보 TI를 주고받을 수 있는 통신 채널이 설정되어 있다는 것을 가정한다. OTP 발생기의 모델은 그림 8과 같이 기존 OTP 발생기 모델에 PUF를 추가한 형태의 모델로 개선하여 제안한다.

본고에서 제안하는 OTP 발생기를 고려했을 때 거래 검증 프로토콜은 그림 9와 같으며, 각 단계별

절차는 다음과 같다. 이 프로토콜은 PUF의 CRP를

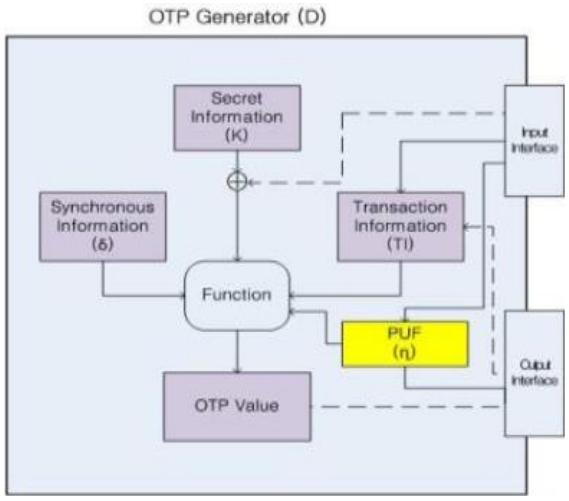

그림 8. 제안하는 OTP 발생기 모델
Fig. 8. The Proposed OTP Generator Model

안전하게 보호하기 위해 표준 암호 함수를 사용하며, 메시지의 에러를 체크하기 위해 HMAC 기반의 해쉬 함수를 사용한다.

표 2. 제안하는 프로토콜의 표기법
Table 2. The Notation of the Proposed Protocol

Notations	Descriptions
C_D	The challenge of PUF from the Financial Company
R_D	The response of PUF from C_D
$E_K(\cdot)$	Encryption Function with K(Secret Key)
$H_K(\cdot)$	HMAC hash function with K(Secret Key)

단계 1 : 사용자가 거래 정보 TI를 사용자 터미널에 입력한다.

단계 2 : 사용자가 거래 정보 TI를 Hello 메시지로써 사용자의 OTP 발생기와 금융회사 서버에 전달한다.

단계 3 : 금융회사 서버는 수식 (1)과 같이 현재 Challenge C_0와 다음 인증에서 사용할 C_1을 해당 사용자의 OTP 발생기로 전달한다. 즉, 다음 인증 절차에서는 C_0가 아닌 C_1을 보낼 것이다.

$$C_0 \| E_{R_0}(C_1) \| H_{R_0}(C_0 \| E_{R_0}(C_1)) \quad (1)$$

단계 4 : OTP 발생기는 수식 (2)와 같이 현재 Response R_0와 다음에 사용할 R_1을 금융회사 서버로 전달한다. PUF의 Response는 PUF를 통해서만 알 수 있기 때문에 다음에 사용할 R_1을 서버로 전송해야 한다.

$$E_{R_0}(R_0 \| R_1) \| H_{R_0}(E_{R_0}(R_0 \| R_1)) \quad (2)$$

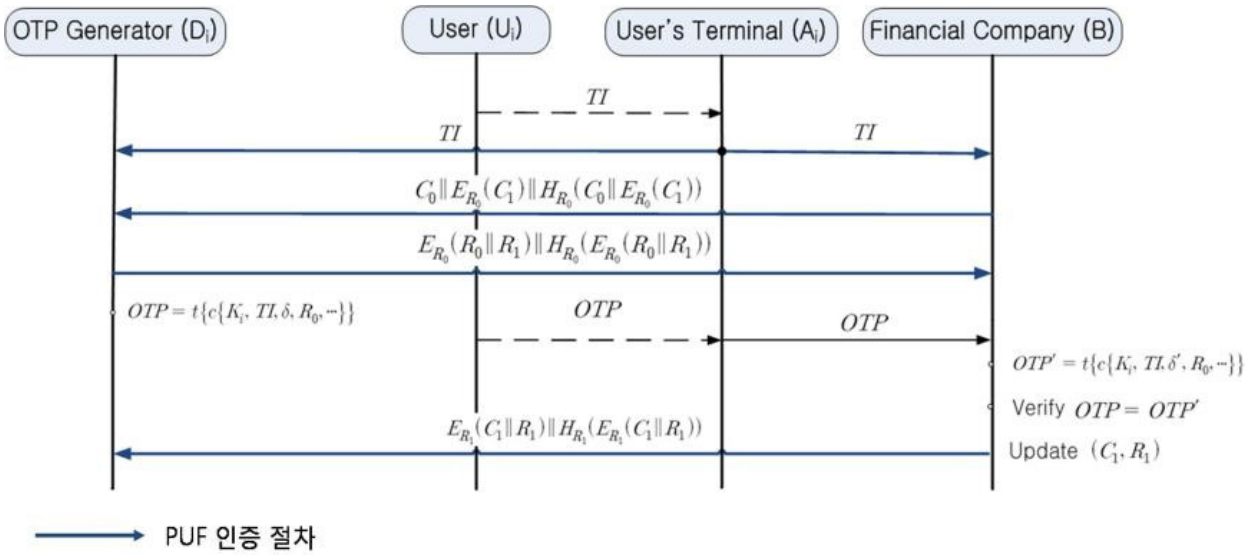

그림 9. 제안하는 거래 검증 프로토콜 흐름도
Fig. 9. The Proposed Protocol Flow

단계 5 : OTP 발생기는 수식 (3)과 같이 OTP 인증 정보를 생성하며 사용자는 OTP 인증 정보를 사용자 터미널을 통해 금융회사 서버로 전달한다. OTP 인증 정보 생성 시 타임 스탬프 등 다른 정보를 추가적으로 사용가능하다.

$$OTP = t\{c\{K_i, TI, \delta, R_0, \cdots\}\} \quad (3)$$

단계 6 : 금융회사 서버는 전달받은 OTP 인증 정보가 일치하는지 검증한 후에 다음 사용할 CRP를 업데이트하며, 수식 (4)와 같이 최종 ACK 메시지로 다음 번 CRP를 OTP 발생기로 전송한다. 여기서 ACK 메시지는 R_1으로 암호화하여 전송한다.

$$E_{R_1}(C_1 \| R_1) \| H_{R_1}(E_{R_1}(C_1 \| R_1)) \quad (4)$$

제안 프로토콜은 인증 과정 중에 다음에 사용할 CRP를 갱신함으로써 CRPs를 관리하는데 효율적인 방법을 제공한다. 또한 OTP 인증 정보는 표준 암호함수에 의해 생성되는데 입력 정보에 PUF의 Response 값을 추가함으로써 비밀번호를 예측하는 것은 더 어렵다.

Ⅳ. 제안 프로토콜의 분석

앞서 2장에서 언급했듯이 피싱, 파밍, 그리고 사회공학 공격들은 심각한 문제를 야기 시키고 있다. 이러한 문제들을 포함하여 도청, 메시지 블락, Replay 공격과 같은 다른 위협들에 대해 분석한다.

4.1. 도청 공격

제안하는 프로토콜은 $C_0 \| E_{R_0}(C_1) \| H_{R_0}(C_0 \| E_{R_0}(C_1))$, $E_{R_0}(R_0 \| R_1) \| H_{R_0}(E_{R_0}(R_0 \| R_1))$, $E_{R_1}(C_1 \| R_1) \| H_{R_1}(E_{R_1}(C_1 \| R_1))$와 같이 업데이트 정보를 PUF의 Reponse 값을 비밀키로 이용하여 암호화하여 보호하므로 공격자들은 어떤 정보도 복원할 수 없다. 따라서 제안 프로토콜은 도청 공격으로부터 안전하다.

4.2. 메시지 블락 공격

제안 프로토콜은 CRP 정보를 갱신하기 전에 OTP 비밀번호 일치여부를 검증하고 있으며, 검증이 완료되면 해당 CRP 튜플 (C_D, R_D)를 갱신하며, 그렇지 않은 경우에는 OTP 인증이 실패하였으므로 갱신하지 않는다. 따라서 제안 프로토콜은 메시지 블락 공격으로부터 안전하다.

4.3. Replay 공격

기본적으로 OTP 비밀번호는 일회용 비밀번호이므로 Replay 공격은 무의미하다. 또한 OTP 발생기와 금융회사 서버 간에 주고받는 인증 메시지는 매번 CRP 정보가 업데이트되기 때문에 Replay 공격은 무의미하다. 즉, CRP 정보는 한 번만 사용하고 다음에는 사용하지 않는다. 그러므로 제안 프로토콜은 Replay 공격으로부터 안전하다.

4.4. Spoofing 공격

제안 프로토콜에서 인증을 위해 주고받는 CRP는 OTP 발생기와 금융회사 서버만 공유하고 있는 정보로써 암호화되어 보호되고 있다. 또한 CRP, OTP 비밀번호는 기본적으로 일치하지 않을 경우 인증 실패로 이어진다. 다음으로 제안 프로토콜은 체크섬으로 HMAC 기반의 해쉬 값을 추가하여 인증 메시지들의 무결성을 검증하기 때문에 Spoofing 공격으로부터 안전하다.

4.5. Physical 공격

제안 프로토콜은 PUF의 특징으로 인해 Response, R_D 정보를 저장할 필요가 없기 때문에 메모리에 저장되지 않는다. OTP 발생기는 Challenge를 서버로부터 받을 때 마다 PUF의 입력으로 Challenge 값을 입력하여 출력된 Response 값을 사용하면 되기 때문에 공격자는 비밀키인 R_D를 획득할 수 없다.

4.6. 복제 공격

제안하는 OTP 발생기는 기존의 OTP 발생기에 PUF를 추가하고 있으며, PUF의 특성상 물리적으로 OTP 발생기를 복제하는 것은 불가능하다. 그러므로 복제 공격은 불가능하다.

제안 프로토콜은 위에서 분석한대로 도청, 메시지 블락, Replay, Spoofing, Physical, 복제 공격으로부터 안전하게 보호되고 있다. 하지만 지능적인 피싱과 파밍 공격들은 여전히 문제로 남아 있다. 기존 프로토콜뿐만 아니라 제안 프로토콜의 경우에도 시간 동기 정보를 매분마다 갱신하고 있으며 실시간으로 이 정보들을 획득한다는 것은 불가능하다.

Ⅴ. 결 론

현재 사용하는 OTP 기반 전자금융 거래 검증 프로토콜은 OTP 발생기와 금융 시스템 서버 간에 비밀키와 시간 동기 정보를 사용하고 있다. OTP 비밀번호는 또한 다른 시스템에서도 multi-factor 인증 기법으로 사용자의 신원을 확인하기 위해 사용되고 있다. 하지만 사용자의 개인 정보를 수집하기 위한 다양하고 지능적인 사회 공학, 피싱 공격들이 증가하고 있다. 공격자들이 특정 대상의 개인 정보를 수집하고 그 정보들을 복합적으로 사용한다면 또 다른 금융 피해 사고를 야기 시킬 수 있다. 하지만 실제 금융 시스템에서 거래 정보 *TI*를 사용하지 않기 때문에 거재 조작 공격에 대한 위협이 있으며, OTP 비밀번호가 소프트웨어적으로 생성되기 때문에 입력 정보만 획득한다면 충분히 같은 OTP 비밀번호를 만들어 낼 수 있다. 따라서 안전하고 강력한 인증을 위해서는 하드웨어적인 요소가 필요하다.

본고에서는 PUF를 이용한 새로운 OTP 프로토콜을 제시함으로써 더 안전한 인증을 보장한다. 우선 새로 제안하는 OTP 발생기는 PUF라는 하드웨어 요소를 추가함으로써 견고성을 향상시킴으로써 OTP 발생기가 복제되는 것을 막을 수 있다. 다음으로 OTP 비밀번호를 생성하는 입력에 PUF의 Response 값을 추가하여 더 안전하고 견고하게 한다. 하지만 앞에서 언급했듯이 제안한 프로토콜은 OTP 발생기와 금융 시스템 서버 간에 서로 PUF 메시지와 거래 정보를 주고받기 위한 통신 채널이 필요하다. 만약 통신 채널이 제한된다면 키패드가 부착된 OTP 발생기를 이용해 사용자가 직접 PUF 관련 정보를 입력하는 방법을 고려할 수 있다. 결론적으로 새로 제안한 프로토콜은 기존의 OTP 기반 전자금융 거래 검증 프로토콜보다 보안을 더 향상시키며, 또한 더 강력한 인증 방법을 제공한다.

References

[1] S. Cho, H.-J. Lee, H.-T. Lim, and S.-G. Lee, “OTP authentication protocol for stream cipher using clock-counter,” in *Proc. KICS Int. Conf. Commun. 2008 (KICS ICC 2012)*, pp. 245-248, Jeju Island, Korea, July 2008.

[2] S. Kim, J. Seo, H. Song, S. Lee, S. Kim, and D. Won, “A secure OTP system using key input devices for financial service,” in *Proc. KICS Int. Conf. Commun. 2008 (KICS ICC 2012)*, pp. 353-357, Seoul, Korea, Nov. 2008.

[3] N. Haller, C. Metz, P. Nesser, and M. Straw, “*A one-time password system*,” IETF RFC 2289, Feb. 1998.

[4] D. M’Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen, “*HOTP: An HMAC-based one-time password algorithm*,” IETF RFC 4226, Dec. 2005.

[5] H. W. Sim, W. J. Kang, and H. Y. Park, “*An one time password based e-financial transaction verification protocol*,” *TTAK.KO-12.0167*, Dec. 2011.

[6] G. Edward Suh and Srinivas Devadas, “Physical unclonable functions for device authentication and secret key generation,” in *Proc. 44th ACM Annu. Design Automation Conf. 2007*, pp. 9-14, San Diego, U.S.A., June 2007.

[7] J. Lee, P. Choi, and D. Kim, “The password-based authentication paradigm on M2M(번역),” *Review of KIISC*, vol. 22, no. 1, pp. 39-46, Feb. 2012.

[8] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, “Lightweight mutual authentication and ownership transfer for RFID systems,” in *Proc. IEEE INFOCOM 2010*, pp. 1-5, San Diego, U.S.A., Mar. 2010.

[9] M. Akgün, M. S. Kiraz, and H. Demirci, “Cryptanalysis of lightweight mutual authentication and ownership Transfer for RFID System,” in *Proc. IEEE Lightweight Security & Privacy: Devices, Protocols and Applicat. (LightSec)*, pp. 20-25, Istanbul, Turkey, Mar. 2011.

[10] S. W. Jung and S. Jung, “HRP: a HMAC-based RFID mutual authentication protocol using PUF,” in *Proc. IEEE Int. Conf. Inform Networking 2013*, Bangkok, Thailand, Jan. 2013.

[11] J. Shin, J. Lee, C. Jeong, and K. Ahn, “Symmetric key-based RFID mutual authentication protocol utilizing PUF,” in *Proc. KICS Int. Conf. Commun. 2012 (KICS ICC 2012)*, pp. 790-791, Jeju Island, Korea, June 2012.

이 종 훈 (Jonghoon Lee)

2005년 2월 숭실대학교 정보통신전자공학부 졸업
2012년 3월~현재 숭실대학교 전자공학과 석사과정
<관심분야> 클라우드 보안, 무선 네트워크 보안

박 민 호 (Minho Park)

2000년 2월 고려대학교 전자공학과 졸업
2002년 2월 고려대학교 전자공학과 석사
2010년 2월 서울대학교 전기 컴퓨터공학부 박사
2010년 3월~2011년 4월 삼성전자 네트워크 사업부 책임연구원
2011년 5월~2013년 2월 Carnegie Mellon University, CyLab 박사후 연구원
2013년 3월~현재 숭실대학교 정보통신전자공학부 조교수
<관심분야> SNS 보안, 클라우드 보안, 유무선 네트워크 보안

정 수 환 (Souhwan Jung)

1985년 2월 서울대학교 전자공학과 졸업
1987년 2월 서울대학교 전자공학과 석사
1988년~1991년 한국통신 전임연구원
1996년 6월 University of Washington 박사
1997년 Stellar One Corp. Senior Engineer
1997년~현재 숭실대학교 정보통신전자공학부 교수
<관심분야> 이동 및 무선 네트워크 보안, VoIP 보안, SNS 보안, 클라우드 보안