The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 5, pp.51-60, Oct. 31, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.5.51
JIIBC 2015-5-6

전자상거래 응용에서 안전한 키 전송을 위한 PKI 좌표기법 One-Time-Pad의 설계

Design of One-Time-Pad based on PKI Coordinates Technique for a Safe Key Transmission in E-Commerce Applications

이길헌*, 전문석*, 최도현**

Kil-Hun Lee*, Moon-Seok Jun*, Do-Hyeon Choi**

요 약 전자상거래 서비스의 사용이 활발해지면서 화폐나 마찬가지인 기능을 하는 정보가 네트워크에 만연하게 되었다. 그에 따른 해킹이 증가함에 따라 이차적 보안장치가 대안으로 부상하며 OTP(One-Time Password)가 사용되기 시작했다. 하지만 완벽하다 믿었던 기존의 One-Time Password에서 취약점이 발견되면서 추가적인 보안대책이 시급하게 되었고 더 이상 보안적인 권고만이 해결책이 아니라는 판단에 이를 해결하기 위한 구체적인 방안을 필요로 하게 되었다. 본 논문은 전자상거래 응용에서 공개키를 이용하여 안전한 키 전송을 이루기 위해 PKI 좌표기법이 적용된 OTP(One-Time-Pad)를 제안한다.

Abstract As electronic commerce service became more popular, information equivalent to currency prevails in network. Accordingly, hacking into network often occurs and thus OTP (One-Time-Password) has emerged as an alternative secondary security system. However, weakness has been found in even existing One-Time Password that used to be considered 'perfect'. Therefore, it becomes very urgent to have an additional security countermeasure. As security recommendation is not considered as solution anymore, more specific plan becomes necessary. The present study proposes PKI coordinates technique-based OTP (One-Time-Pad) for a safe key transmission in E-commerce.

Key Words : OTP, Authentication, PKI, Electronic Commerce, Public Key

Ⅰ. 서 론

IT 정보통신의 발전과 함께 기존의 오프라인 거래보다 온라인상(금융, 게임, 그룹웨어 등)의 거래가 활성화되었고, 새로운 IT 기술이 도입과 함께 관련 분야에서는 전자상거래 이용이 점차 증가하는 추세이다. 이에 따라 전자상거래 분야에서는 관련 범죄수법이 고도화 되고 있는 가운데 제작회사, 배포회사, 판매회사 및 구매자 등 관련자 모두가 공통적으로 강력한 보안수단이 요구되고 있다. 일반적으로 알려진 일차 인증수단에 대한 추가 보안기술로서 보안카드, 지문인식, 음성인식 등 많은 기술들이 연구되고 있지만, 실제 활용에 있어 가장 범용성이 높은 보안기술로는 현재 One-Time Password가 있다.[9][10][14] 그림 1은 연도별 One-Time Password 거래

*정회원, 숭실대학교 컴퓨터학과
*정회원, 숭실대학교 컴퓨터학과
**정회원, 숭실대학교 컴퓨터학과(교신저자)
접수일자 2015년 8월 26일, 수정완료 2015년 9월 26일
게재확정일자 2015년 10월 9일

Received: 26 August, 2015 / Revised: 26 September, 2015 / Accepted: 9 October, 2015
**Corresponding Author: clarkent83@ssu.ac.kr
Dept of Computer Science and Engineering, Soongsil University, Korea

건수 및 이용자 수를 나타낸 그래프이다.[15]

우리나라는 2008년 4월 1일 시작한 전자금융감독규정의 보안등급 차등화 정책에 의해 텔레뱅킹 및 인터넷 뱅킹을 이용할 때 전자금융거래의 안전성 강화에 따라 보안등급을 부여하였고, One-Time Password를 사용한 거래는 현재 구분되는 3개의 보안등급에서 1등급의 위치를 차지하고 있다.[11][13][15]

그림 1. 연도 별 One-Time Password 거래 및 이용자 수
Fig. 1. Annual number of One-Time Password transactions and users

본 논문은 현재 활용되는 One-Time Password의 취약점 분석과 최근 문제가 되고 있는 최신 스마트 One-Time Password나 기존 카드형 One-Time Password 기술의 취약점을 보완하는 One-Time-Pad 생성 기법을 제안한다.

II. 관련연구

One-Time Password는 1회에 한해 사용할 수 있는 암호 시스템으로 매번 다른 암호를 이용하여 사용자를 인증하는 방식이다. 일반적으로 알려진 OTP란 One-Time Password를 말하지만, 본 논문에서 제안하는 OTP는 패드 형태의 일회용 암호인 One-Time-Pad를 의미한다.[1][2][8]

1. One-Time-Pad

OTP(One-Time-Pad)는 서버와 클라이언트 사이에 미리 약속된 규칙에 의해서 주고받는 암호를 통해 일회용 암호의 암·복호화 과정에서 변조유무에 대한 비밀성을 검사하게 된다.[1][2][3] 서버와 클라이언트 간에 주고받는 메시지는 One-Time-Pad로 암호화 되어 Cipher Text로서 상대방 사용자를 인증하게 된다. 이는 One-Time-Pad의 생성과정을 모를 경우 추측이 불가능하도록 전송용량과 동일한 크기의 암호화가 이루어진다. 암호화 크기에 있어 단점이 존재하지만, 메시지의 1 bit마다 각각 암호화가 되기 때문에 통신하는 모든 정보가 암호화된다는 장점을 보여준다. 표 1은 One-Time-Pad의 예이다.

One-Time-Pad의 각 문자는 출현 빈도가 모두 같은 것을 사용하고, 평문의 길이와 비밀키의 길이가 같은 n개의 임의 문자열로 이루어져 있다. 예를 들어, "HELLO"라는 메시지를 보낸다고 했을 때 송신과 수신 모두에서는 같은 모듈로(동일한 암·복호화 연산구조를 지님)를 사용하여 암호화와 복호화를 하게 된다.

표 1. One-Time-Pad의 예
Table 1. Examples of One-Time-Pad

AKSRIG	JZTLBC	WWBZXQ	HHPASM
SJANFV	BZXQDQ	SBDZCD	MTMROP
VVSOES	DGGIAK	DCDBUS	TIYPND
VIQGBK	UCVXTW	RYJKMF	SIEKZW
BAZSTN	SBFGZC	KGBPCG	SIQSOQ
IJCWHG	DWHPER	RERYWE	SIELOA
JKFXIO	HGAAPR	SIKELA	RRAKBS
DWHPER	GRRSSE	NIKPAA	RERYWA

결론적으로 패드의 각 문자 메시지의 글자는 사전에 준비된 수치(값)으로 변하게 되어 비밀키와 메시지가 결합돼 계산되게 된다. 표 2와 표 3은 One-Time-Pad의 암호화와 복호화 과정을 나타낸다.

표 2. One-Time-Pad 암호화
Table 2. One-Time-Pad Encryption

HELLO (Plaintext)					
7(H)	4(E)	11(L)	11(L)	14(O)	message
+ 23(X)	12(M)	2(C)	10(K)	11(L)	key
= 30	16	13	21	25	message+key
= 4(E)	16(Q)	13(N)	21(V)	25(Z)	message+key (mod 26)
EQNVZ (Ciphertext)					

표 3. One-Time-Pad 복호화
Table 3. One-Time-Pad Decryption

EQNVZ (Ciphertext)					
4(E)	16(Q)	13(N)	21(V)	25(Z)	ciphertext
- 23(X)	12(M)	2(C)	10(K)	11(L)	key
= -19	4	11	11	14	ciphertext-key
= 7(H)	4(E)	11(L)	11(L)	14(O)	ciphertext-key (mod 26)
HELLO (Plaintext)					

대량의 비밀키를 안전하게 보내는 것은 상당히 어렵지만 특정 난수표를 이용해 만든 비밀키를 한 번 사용하고 다시 사용하지 않으면 완전한 암호가 된다.[4][5] 다른 이름으로 스트림 암호라고도 칭하며 비밀키를 송신자와 수신자가 모두 공유해야 할 뿐만 아니라, 짧은 키로 의

사난수를 발생하여 암호학적으로 안전한 비밀키를 매번 다르게 생성할 수 있는 효율적인 방법이다.[6][7]

2. One-Time Password

One-Time Password는 현재의 비밀번호에서 다음의 비밀번호를 유추하는 것이 굉장히 어려운 패스워드 생성 방법으로, 동일한 패스워드를 반복 사용함으로써 발생될 수 있는 패스워드 도난 문제를 예방하는데 효율적이다.[9][10]

One-Time Password는 서버와 클라이언트가 미리 약속한 방식에 의해 MAC(Message Authentication Code)을 생성하여 전달함으로써 무결성을 검증하여 인증을 받는다.[12] 그림 2는 OTP의 동작과정을 나타낸다.

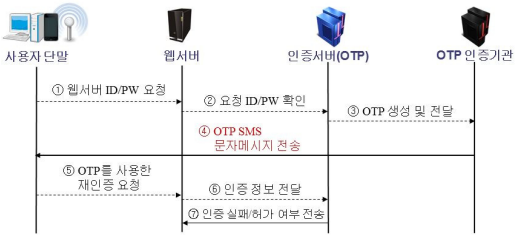

그림 2. One-Time Password 동작과정
Fig. 2. One-Time Password Operation Process

일반적으로 일정한 방식에 의해 전용 단말장치 등에 새로운 비밀번호가 생성되어 시스템에 접근할 때마다 새로운 비밀번호를 입력해야하기 때문에 해킹이나 사용자의 관리 소홀 등으로 비밀번호가 노출되는 것을 방지할 수 있다.

One-Time Password는 다양한 동기화 기술을 사용하여 생성된다. 그 동기화 기술은 생성 방법에 따라 S/Key 방식, 질의-응답(Challenge-Response)방식, 시간 동기화(Time-Synchronous) 방식, 이벤트 동기화(Event-Synchronous) 방식, (Time-Event)조합 동기화 방식 등으로 분류된다.

최근 대부분의 One-Time Password는 기존 패스워드와는 달리 단방향 해시함수를 사용하여 세션이 끝나면 폐기되기 때문에 공통적으로 재사용이 불가능한 특징을 가진다. 그 예로 뱅킹에서 사용되는 인쇄용 보안카드와 비교하면 One-Time Password는 사용자 비밀번호가 노출되더라도 새로 생성된 비밀번호를 입력해야하기 때문에 훨씬 강력한 보안성을 제공한다.

Ⅲ. 안전한 키 전송을 위한 OTP(One-Time-Pad) 설계

본 논문은 공인인증서와 사용자 USIM 정보를 이용해 전자서명을 이루는 One-Time-Pad 설계를 제안한다.

1. 기존 OTP(One-Time Password)의 취약점 분석

One-Time Password 해킹의 발생 원인은 첫째 OTP가 '절대 보안'이 가능하다는 잘못된 맹신(과신)이 문제라 할 수 있고, 두 번째 해킹 기술의 진화에 따라 OTP 사용 프로세스 상 가장 취약한 사람을 노린 해킹방법(브라우저, 키보드 해킹 등)에 의한 다양한 취약점이 존재한다는 것이다.

One-Time Password 서비스의 취약점을 살펴보면 OTP 번호를 띄우는 PC의 웹 브라우저에 악성코드가 감염되어 OTP 번호 전달과정에서 정보가 유출될 수 있다. 그리고 내부의 구조적 취약점으로 사용자와 서버 간에 30초~1분 간 유휴시간을 가짐으로써 패스워드 재사용 공격에 대한 해킹 취약점을 지닌다. 이 경우 One-Time Password 생성 시의 고정된 길이(6~15자)로 입력되는 질의/응답 값(숫자)의 단순성으로 인해 One-Time Password SEED 파일의 외부 유출시 취약점이 발생할 수 있다.

국내에서 이루어진 One-Time Password 해킹은 전문적인 해킹 지식이 없는 공격자라 할지라도 진짜처럼 꾸민 피싱 사이트를 통해 해킹이 가능한 수준이다. One-Time Password 키를 유출하거나 실시간으로 접속하는 사용자의 화면을 모니터링 하고 있다가 One-Time Password 번호를 똑같이 받아치는 불법 로그인을 통해 로그인 한 유저의 접속이 끊기게 하는 등, MITM(Man-in-the-Middle Attack) 형태로 재전송 공격도 가능하다. 또한 로그인 중인 계정의 접속 중에 생기는 유휴시간 동안 재 로그인이 안 되게끔 강제로 막는 패치를 진행하는 등의 패치가 제공되었지만, 그 패치가 다시 공격받아 아예 계정과 비밀번호가 사라지는 등의 추가적인 문제가 발생하였다. 근본적으로 알고리즘이 해킹되는 것은 막지 못하고 있는 것이다.

이러한 취약점들을 해결하기 위해서는 One-Time Password를 위해 갖는 유휴시간과 더불어 동기화 인증 조건이 추가적으로 부여되어 시간에 무관한 인증이 이루어져야 한다. 또한, 생성 알고리즘에서 올바른 사용자인지 구별과 허가를 통해 승인여부에 대한 접근차단 및

통제가 이루어져야 한다.

본 논문에 사용되는 One-Time Password는 현재까지도 꾸준히 해커가 관심을 갖게 될 소지가 다분한 취약점들인 인증 유휴시간 및 MITM 등 문제점이 계속 발견되고 있기 때문이다. 2절부터 본 논문에서 사용되는 OTP는 One-Time-Pad라고 정의하며, 전체 용어는 다음의 표 4에서 설명한다.

표 4. 용어 설명
Table 4. Definition of Terms

용어	설명
OTP	One-Time-Pad
OTP-CA	OTP Certificate Authority(OTP 인증기관)
OTP-IO	OTP Issuing Organization(OTP 발급기관)
WS	(Web Server) OTP를 사용하는 웹서버
MC	Mobile Service Provider(이동통신사에서 장치정보 검증)
USER	사용자(사용자 및 장치 정보)
Digest	사용자 정보와 USIM정보를 조합한 인증정보
OTD	One-Time-Pad의 인증정보 확인을 위해 구성되는 좌표정보(OTP-IO 서버에서 검증)
PKI	(Digital) Certificate (공인인증서)
Count	Hash Chain Number(발생횟수)
Time	OTD 요청 및 생성시간 (Time_Stamp)
좌표	입력된 Hash Chain의 행렬 공간 정보
AES	Advanced Encryption Standard
USIMPIN	USIM 내부 IMEI 번호
USERPK	USER's Public Key
SYNCTC	동기화를 위한 Time과 USIM의 조합정보

2. 제안 시스템 구조도 및 전체 프로토콜

본 논문에서 제안하는 One-Time-Pad는 발급과정에서 One-Time-Pad Digest를 생성하여 기존의 One-Time Password와 다르게 메시지 내 각각의 bit에 암호화하여 통신한다.

이는 데이터를 통신함에 있어 유휴시간에 상관없는 1회용 암호가 적용된 데이터통신을 통해 기존의 One-Time Password의 취약점을 보완한다.

본 논문에서 사용되는 OTD는 One-Time-Pad를 구성하는 인증요소로서 One-Time-Pad가 갖는 암호화 용량의 한계를 극복하고자 제안하였다. OTD는 암호화 시각 bit열마다 암호화하는 것은 기존의 One-Time-Pad 방식과 동일하다. 하지만 복호화에 필요한 연산과정을 상대적으로 감소시킬 수 있고 bit열 정보를 행렬공간에 입력하여 좌표값을 갖기 때문에 빠른 연산과정과 비밀성을 함께 보장할 수 있다는 장점이 있다. 또한, 체인구조가 적용된 행렬 좌표정보로 암호화 하게 될 경우, bit열을 패딩정보로 위장하고 중간값을 탈취당하더라도 탈취된 정보를 통해 루트 정보를 알 수 없기 때문에 중간자 공격에 대응할 수 있다는 특징이 있기 때문에 체인구조를 사용하게 되었다.

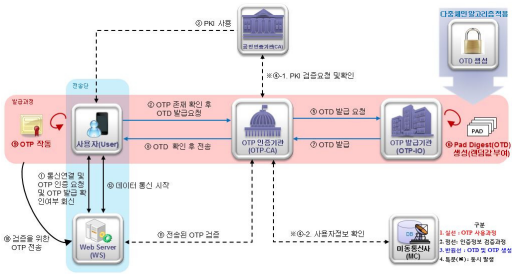

그림 3. 전체 시스템 구조도와 발급 및 인증과정
Fig. 3. Complete system schematic and issuance and authentication process

그림 3은 전체 시스템 구조도를 통해 발급 및 인증과정을 나타내었다. (USER와 OTP_CA는 Symmetric key를 공유한다고 전제한다.)

- Step ① (USER→WS) : 사용자가 특정 웹 서버로 통신연결 후 웹 서버로부터 OTP 인증 요구 수신됨
- Step ② (USER→OTP-CA) : OTP의 존재여부를 확인하며, 없을 경우 Request $USER_{PK}$를 통해 CA에 사용자의 본인인증 수행완료 후 OTP 발급신청을 위한 OTD 요청 메시지를 AES암호화 후 전송
- Step ③ (CA(PKI)→USER) : 본인인증 과정을 위한 인증서(Certificate) 검증
- Step ④-1 (OTP-CA→CA(PKI)) : $USER_{PK}$를 통해 본인확인을 위한 검증요청 및 확인응답 수신
- Step ④-2 (OTP-CA→MC) : 기기인증으로 사용자 확인을 위한 MC로 검증요청 및 확인응답 수신
- Step ⑤ (OTP-CA→OTP-IO) : 인증기관에서 발급기관으로 OTD 발급요청
- Step ⑥ (OTP-IO→OTD) : 사용자 정보와 USIM 정보를 조합하여 OTD 생성(USIM 구성 : 국가코드, 버전, 제조사코드, 일련번호, 옵션으로 구성)
- Step ⑦(OTP-IO→OTP-CA) : OTD 발급 후 OTP-CA에 송신
- Step ⑧ (OTP-CA→USER) : OTD를 사용자기기로 AES 암호화 후 전송
- Step ⑨ (USER→OTP) : OTD 수신 후 AES 복호화 후 OTD를 사용자기기에서 메시지와 OTD를 사용하여 OTP(Cipher Text)로 변환

- Step ⑩ (USER→WS) : 변환된 OTP(Cipher Text)를 웹서버에 전송
- Step ⑪ (WS↔OTP-CA) : OTP-CA에서 전송된 OTP의 $USER_{PK}$ 및 해시체인 무결성(Time&Count)을 검증 (OTP의 OTD 정보의 진위여부를 OTP-CA에서 검증함)
- Step ⑫ (WS↔USER) : 데이터 통신 시작

Step ① ~ ⑫ 과정을 통해 One-Time-Pad를 발급 및 인증하고 OTD기반의 Digest를 사용한 One-Time-Pad가 생성된다.

여기서 발생되는 Count는 해시 체인의 발생 횟수를 의미하고 OTP 발급기관에서는 사용자의 공개키를 사용하여 OTD를 생성하게 된다. 또한, 좌표라는 것은 해시 체인이 임의로 구성되어 들어가는 PAD의 행렬정보를 의미한다.

OTD을 생성하는 좌표기법 One-Time-Pad 생성 방식은 인증서와 USIM 인증 및 시간/카운트 동기화 등을 적용하여 AES 암호 알고리즘 적용 후 상호 인증방식으로 통신하므로 중간자 공격 등의 해킹에 강하게 된다.

3. One-Time-Pad 발급 프로토콜

발급 프로토콜은 사용자가 통신하고자 하는 서버(또는 사용자)와 연결을 요청하는 과정에서 요구되는 One-Time-Pad를 발급받는 과정이다.

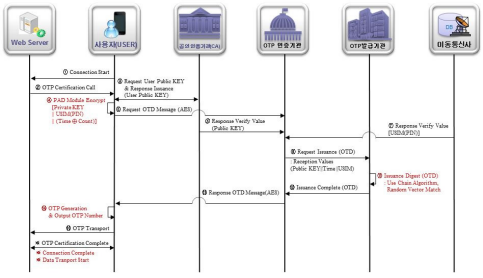

그림 4. One-Time-Pad 발급 프로토콜
Fig. 4. One-Time-Pad issuing protocol

공인인증기관에서 제공되는 공개키와 USIM 정보를 통해 통신사에서 검증할 키 값을 생성하여 One-Time-Pad 인증기관으로 전송하여 One-Time-Pad를 발급받게 된다. 그림 4는 One-Time-Pad 발급 프로토콜을 나타낸다.

- Step ① : (Connection Start) 사용자가 Web 서버로 Request_Connect 메시지 전송 → 통신 연결 시도
- Step ② : (One-Time-Pad Certification Call) Web 서버에서 사용자에게 One-Time-Pad 요구 → Response_Call 메시지로 응답
- Step ③ : (CA→ USER Verify Value) 사용자 공개키 사용→공인인증기관(CA)으로부터 공개키 Request ($USER_{PK}$) 검증 → (CA 확인) Response_Issuance ($USER_{PK}$) 수신하여 본인확인
- Step ④ : (Request OTD Message) AES로 암호화 된 OTD 발급 요청 메시지를 One-Time-Pad 인증기관에 송신(키 재료에 $USER_{PK}$, $USIM_{PIN}$, $SYNC_{TC}$ 입력)
- Step ⑤ : (CA&MC Verify Value 수신) USER 정보의 확인을 위해 CA와 MC로부터 본인확인 검증값을 수신 후 비교하여 One-Time-Pad 발급여부 결정
- Step ⑥ : (Request Issuance) OTD 발급을 위해 확인된 사용자의 CA, Time, $USIM_{PIN}$정보를 OTP-IO로 송신
- Step ⑦ : (Issuance OTD) 체인 알고리즘과 랜덤 행렬정보에 맞게 생성된 OTD를 발급
- Step ⑧ : (Issuance Complete) OTP-IO → OTP-CA로 발급된 OTD를 송신
- Step ⑨ : (Response OTD Message) 발급된 OTD를 AES로 암호화 후 USER에게 송신
- Step ⑩ : (One-Time-Pad Generation & Output) OTD를 메시지와 암호화 하여 OTP(Cipher Text) 생성 후 OTP 생성 여부를 화면에 알림
- Step ⑪ : (USER→WS) OTP 검증을 위해 웹서버로 One-Time-Pad 정보 송신
- Step ⑫ : (WS→OTP-CA) One-Time-Pad 정보 확인을 위해 웹서버에서 OTP-CA에 OTP 검증값 확인 요청
- Step ⑬ : (OTP-CA→WS) 정상발급으로 확인완료 된 One-Time-Pad 검증정보를 OTP-CA에서 WS로 회신
- Step ⑭ : (Connection Complete) One-Time-Pad 검증 완료 후 One-Time-Pad가 적용된 Data Transport Start

4. One-Time-Pad 인증 프로토콜

인증 프로토콜의 통신연결 시작(Connection Start)부터 OTD 메시지 요청(Request OTD Message) 과정까지는 발급 프로토콜과 동일하다. 인증 프로토콜에서는 그 다음 단계부터 프로토콜을 설명하였다. 그림 5는 인증 프로토콜과정을 나타낸다.

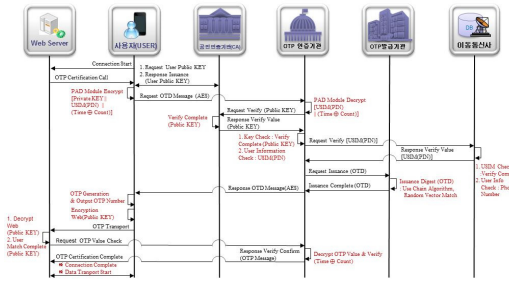

그림 5. One-Time-Pad 인증 프로토콜
Fig. 5. One-Time-Pad authentication protocol

- Step ① ~ Step ④ : 발급 프로토콜과 동일
- Step ⑤ : (OTD Decrypt) AES 복호화 후 $USER_{PK}$, $USIM_{PIN}$, $SYNC_{TC}$ 정보 추출
- Step ⑥ : (Verify Public Key) 공인인증기관(CA)으로부터 $USER_{PK}$ 검증 확인
- Step ⑦ : (Verify MC) 이동통신사(MC)에 $USIM_{PIN}$ 확인 요청 및 회신 완료
- Step ⑧ : (Request Issuance) 확인된 사용자의 OTD정보(CA, Time, $USIM_{PIN}$)를 OTP-IO로 송신하여 OTD 발급요청
- Step ⑨ : (Issuance OTD) 체인 알고리즘과 랜덤 행열정보에 맞게 생성된 OTD를 발급
- Step ⑩ : (Issuance Complete) OTP-IO → OTP-CA로 발급된 OTD를 송신
- Step ⑪ : (Response OTD Message) 발급된 OTD를 AES로 암호화 후 USER에게 송신
- Step ⑫ : (One-Time-Pad Generation & Output) OTD를 메시지와 암호화 하여 OTP(Cipher Text) 생성 후 OTP 생성 여부를 화면에 알림
- Step ⑬ : (USER→WS) One-Time-Pad 검증을 위해 웹서버로 One-Time-Pad 정보 송신
- Step ⑭ : (WS→OTP-CA) One-Time-Pad 정보 확인을 위해 웹서버에서 OTP-CA에 One-Time-Pad 검증값 확인 요청
- Step ⑮ : (OTP Value Verify) $USER_{PK}$, Time&Count 조합정보 등 해시체인 무결성 검증확인
- Step ⑮ : (OTP-CA→WS) 정상발급으로 확인완료된 OTP 검증정보를 OTP-CA에서 WS로 회신
- Step ⑯ : (Connection Complete) OTP 검증완료 후 One-Time-Pad Transaction Information Link → Data Transport Start

5. 체인 구조의 One-Time-Pad

One-Time-Pad 알고리즘에 사용되는 Digest인 OTD을 생성하기 위해 USER의 USIM, 공개키, 동기화 정보를 사용하여 체인 구조의 One-Time-Pad를 생성한다. 해시체인에서 사용하는 해시 함수는 일방향성(one-way property)를 가지는 Crypto Hash Function이다. 그림 6은 제안하는 One-Time-Pad 생성 방법을 나타낸다.

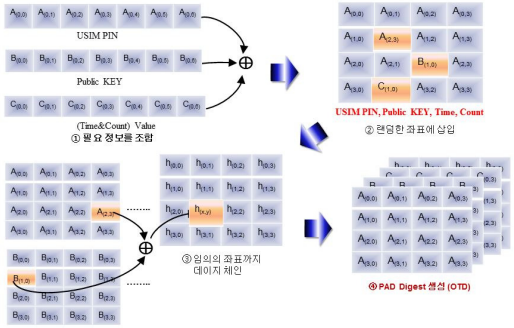

그림 6. One-Time-Pad의 OTD 생성 과정
Fig. 6. OTD Generation Process of One-Time-Pad

- Step ① : (Combinations) One-Time-Pad 생성 Module에서 사용자 정보($USIM_{PIN}$, $USER_{PK}$, $SYNC_{TC}$) 해시 알고리즘 조합함
- Step ② : (Padding) 조합된 해시 정보가 입력된 행렬(1Byte~720KByte의 크기)에 입력값을 제외한 나머지 부분에 패딩값(Random Garbage Value)을 부여 후 임의의 패드 1개의 루트값 C0을 생성함
- Step ③ : (Hash Chain) OTP-IO가 루트값 C0을 사용하여 연산과정을 통해 데이지 체인 수행(XOR)
- Step ④ : (OTD Generation) 데이지 체인 수행완료 후 One-Time-Pad Digest 생성 완료(변조유무 확인)

표 5. 해시 체인의 구성값
Table 5. Hash Chain of the Configuration Values

n : 조합된 해시 체인의 길이
h : Hash Function
Seed : x ($USIM_{PIN}$, $USER_{PK}$, $SYNC_{TC}$)
Root Value : Seed를 사용해 Seed(x)로부터 해시연산에서 얻는 마지막 값
해시 체인의 루트 값 $C_0 = h^{n+1}(x)$

표 5를 통해 관련된 구성정보를 살펴보면, 사용자 정보에 담긴 $USIM_{PIN}$, $USER_{PK}$, $SYNC_{TC}$ 정보를 통해 One-Time-Pad의 해시 체인과정을 진행한다.

$$h^n(x) = h(h^{n-1}(x)) \quad (1)$$

좌표정보를 추가적으로 패드에 삽입하며 이후 적용되는 패딩으로 인해 입력된 정보의 좌표에 대한 해시정보가 추가적으로 담기게 된다. 이후 서버에 PAD를 만들기 위해 설치된 Digest Module에서 OTD을 생성하며, 해당 좌표정보가 One-Time-Pad Digest로 사용된다.

One-Time-Pad 구현에 사용되는 알고리즘의 생성과정을 살펴보면, 송신된 시간과 Count 정보의 조합 값을 비교 연산 파라미터로 사용한다. 일단 시간을 각 시, 분, 초에 따라 나누고 Count를 송신된 PAD의 bits/수만큼 부여하여 24로 나눈다. 조건이 부여된 수를 해당 자리마다 2진수로 변환하고 임의의 자리에 테이블의 변환 값을 넣어 PAD의 일정한 위치에 변환 좌표의 위치가 담긴 값을 담는다. 이로 인해 hn(x)를 알고 있어도 $h^{n-1}(x)$는 계산할 수 없기 때문에 공격자의 패스워드 예측 공격이 불가능하게 된다.

Ⅳ. 실험 및 결과

제안한 알고리즘의 성능(효율성)과 보안성을 비교하기 위해 많이 알려진 암호화방법을 사용하여 만들어진 One-Time Password와의 차이점을 분석한다. 구현을 위해 구성한 시스템 개발은 표 6의 환경에서 진행되었다.

표 6. 시스템 개발 환경
Table 6. System Development Environment

하드웨어	OS	Windows7 Ultimate K(x86)
	CPU	Intel Core2 Duo E7200 @2.53GHz
	RAM	2.00 GB
개발도구	Client	MS-Visual Studio 2010
	Server	MS-SQL Server 2008

1. 성능 분석

구현에 사용되는 알고리즘의 생성 과정을 살펴보면, 표 7은 각각 다른 암호화 기법이 적용된 One-Time Password를 구성하고, 제안하는 One-Time-Pad를 비교 분석 한 것이다. 각각 인증방법에 따라 다른 메시지 전송방법과 암호 알고리즘 간 성능 차이를 비교한 것으로서 조합정보의 종류에 따라 결과 값을 측정하였다.

표 7. One-Time-Pad 비교분석
Table 7. One-Time-Pad Comparative analysis

	방법1	방법2	방법3	제안
인증방법	Password	USIM	인증서	OTD
기기인증	Y	Y	Y	Y
상호인증	N	N	N	Y
메시지 전송방법	대칭키& Password 암호화	대칭키& USIM PIN 암호화	인증서 공개키 암호화	인증서&USIM 조합
암호 알고리즘	SEED	3-DES	AES	AES
사용자등급	2	1	1	1

생성기법에 따른 비교분석을 위해 각각의 인증방법 및 암호 알고리즘에 따라 암호화 코딩을 수행하였다. 그 결과로 그림 7의 처리시간 분석결과가 도출되었고 제안하는 방식을 제외한 다른 3가지를 살펴보았다.

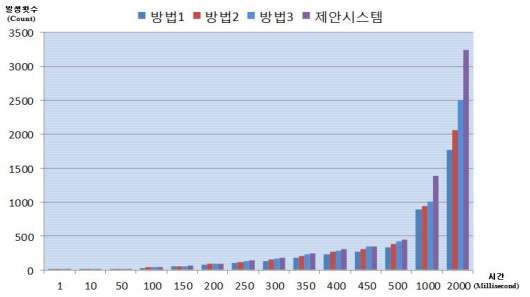

그림 7. 처리시간 비교분석 (그래프)
Fig. 7. Comparative analysis Processing Time (Graph)

1회부터 2000회까지 연속적으로 One-Time Password 및 One-Time-Pad를 생성하였을 경우, 효율성 면에서 제안시스템의 암호화 방법은 다른 방법에 비해 현저히 낮은 수치를 기록했다. 하지만 본인확인의 측면을 살펴봤을 경우 높은 보안성을 가질 수 있도록 하는 특징을 부여했다는 강점이 있다. 또한 인증서와 USIM을 함께 인증하므로 메시지 구성 시 인증요소의 다양화와 해시 체인의 사용으로 인해 중간자 공격으로 인한 사용자 인증 정보의 취득이 어렵게 하는 특징을 지닌다.

그림 7과 표 8은 웹에서 인증기관과 발행기관 서버 사이의 업무 처리량 대비 처리시간 수치와 그래프를 나타낸다. 그림 7의 처리시간은 Millisecond(밀리초) 단위이며 Count는 발생횟수를 의미한다. 각 수치는 서버에서 측정한 각 암호화방법별 One-Time Password와

One-Time-Pad의 인증 횟수이며, 1번부터 2000번까지 생성시(임의로 지정한 횟수: 1000번에 1초)로 시험하였을 때의 측정된 소요시간 결과 값이다.

현재 금융보안연구원에서 기본적으로 요구하는 성능은 초당 500건의 인증처리이고, 실제 One-Time Password를 보유한 업체의 처리시간은 평균 1,500~2,000 건이다.

이런 점을 감안했을 때, 현재 비교분석을 위해 사용된 정보가 1Byte의 텍스트 메시지이고, 1,000 밀리초에 약 1,383 건의 발생률을 보이는 결과로 인해 PKI를 활용한 방법보다 제안된 One-Time-Pad의 효율성은 좋지 않지만, 보다 안전한 구조를 지니며 기본적으로 요구하는 성능 수치를 충족함을 구현과정을 통해 증명하였다.

표 8. 처리시간 비교 분석 (시간단위 : 밀리초)
Table 8. Comparative analysis Processing Time (Millisecond)

처리 시간	발생횟수			
	방법1	방법2	방법3	제안시스템
1	0.523	0.679	0.703	0.811
10	3.288	3.602	3.974	4.191
50	14.596	15.724	15.686	17.073
100	31.968	33.357	35.202	36.423
150	54.007	55.462	58.034	60.542
200	82.384	84.201	89.993	93.164
250	102.953	114.624	128.803	144.045
300	130.059	150.521	169.909	184.278
350	174.698	201.673	227.004	241.901
400	229.153	265.185	284.567	301.087
450	272.806	309.012	339.766	350.138
500	334.521	384.958	423.812	447.295
1000	890.468	940.025	1005.513	1383.703
2000	1762.095	2063.007	2504.919	3240.557

2. 안전성 분석

측정된 처리시간을 비교하여 보면 제안하는 시스템이 다른 제품에 비해 연산시간에 추가적인 지연이 발생했지만 사용되는 키 재료와 그 보안성 측면에서 볼 때 표 9과 같은 강력한 보안성을 보장한다.

보안 요구사항이 안전하다고 보는 이유는 제안시스템이 1차로 해시 체인이 수식된 결과값을 소유한 상태로 AES 암호화 통신을 하게 되므로, AES가 불안전하더라도 생성된 수식값을 풀지 못한다는 특징을 지니기 때문이다. 이 생성정보는 시간정보 뿐만 아니라 기기정보 및 Hash chain 구조를 포함하고 있기 때문에, 동기화에 있어 보안요소가 추가된 형태를 지닌다. 결과적으로 One-Time Password 생성시점만으로 동기화가 이루어지는 기존방식에 비해 중간자 공격 및 세션 가로채기가 되더라도 OTD를 복호화 할 수 없으면 OTP 결과를 알 수 없다는 장점을 지닌다.

결과적으로 안전성 비교분석 내용을 살펴보면, 최근에 지속적으로 발생되고 있는 MITM 공격을 포함하여 유휴시간을 통한 재사용 공격 등의 문제점을 해결하였다. 표 9는 보안성 비교 분석을 위해 제작된 3가지 방법과 제안된 One-Time-Pad의 요구사항 점검표이다.

표 9. 보안성 비교분석
Table 9. Comparative analysis Security

보안 요구사항		방법1	방법2	방법3	제안 시스템
1	비밀정보 추측 방지	안전	안전	안전	안전
	피싱 및 파밍 방지	취약	안전	안전	안전
	유출 및 노출 방지	안전	안전	안전	안전
	위조 및 변조 방지	안전	안전	안전	안전
2	인증정보 재사용 방지	취약	안전	안전	안전
	인증정보 생성값 유출 방지	취약	안전	안전	안전
	중간자 공격 대응	취약	취약	취약	안전
	세션 가로채기 방지	취약	취약	취약	안전
	거래사실 부인 방지	취약	안전	안전	안전
3	물리적 공격 대응	취약	안전	안전	안전

- 비밀정보 추측 방지 : 비인가자가 인증정보 등을 추측하여 인증을 시도하는 공격이며 제안한 인증은 추측만으로 암호화 연산과정 및 인증정보를 알 수 없다.
- 피싱 및 파밍 방지 : 전자금융거래 이용자의 인증정보를 One-Time-Pad 인증기관과 사용자 정보의 확인을 거쳐 인증하게 되기 때문에, 접속한 정보처리시스템이 정당한지 여부를 식별 및 인증할 수 있다.
- 유출 및 노출 방지 : 전자금융거래 이용자와 정보처리시스템 사이에 전송되는 전자금융거래내역 등 중요정보를 암호화 하였고, 해시 체인의 연산과정 시 지니는 보안성으로 인해 비밀성 및 무결성이 보장된다.
- 위조 및 변조 방지 : 이용 중 위조나 변조 시도가 있을 시 패드의 동기화 정보가 바뀌게 되므로, 금융기관이 전자금융 거래내역의 위변조 발생여부를 확인할 수 있다.
- 인증정보 재사용 방지 : 비인가자에 의해 인증정보가 재사용되는 것을 확인할 수 있도록 동기화 정보

가 일회성으로 포함된다.

- 인증정보 생성값 유출 방지 : 모듈을 통한 알고리즘 구현을 통해 중간 전달체계인 사람이 끼어들지 않게 되므로, 사용자와 서버로부터 화면 모니터링 및 키보드 해킹을 통해 인증정보 생성 값이 유출되지 않는다.
- 중간자 공격 대응 : 이용자와 정보처리시스템 사이에 인증세션이 생성된 이후 비인가자가 해당 세션정보를 가로채더라도, 서버와 사용자간 동기화 정보가 증감함으로써 일치하지 않게 되어 인증정보 획득이 불가능하게 된다.
- 세션 가로채기 방지 : 이용자와 정보처리시스템 사이에 인증세션이 생성된 후 비인가자가 해당 세션정보를 이용해 인증을 시도하더라도, 사용자 등록이 되어있지 않은 이용자일 경우 인증이 불가능하게 된다.
- 거래사실 부인 방지 : 금융기관에서 이용자 및 금융기관의 전자금융거래 사실 및 내역은 해당 기관 외에는 수정이 불가능하므로 부인할 수 없다.
- 물리적 공격 대응 : 인증수단에 저장된 인증정보 생성값 등 비밀정보는 일회성을 띄게 되므로 물리적으로 유출될 수 없다. 또한 모듈에 입력되는 생성 정보는 물리적으로 추측할 수 없으며 해당 사용자에 의해 등록된 정보로서 생성 및 갱신되므로 유출될 수 없는 구조를 지닌다.
- 보안등급의 요구사항 : 각 보안등급은 이전 보안등급을 만족한다.

V. 결 론

최근 One-Time Password 보안 기술은 전자상거래 응용방법의 빠른 변화에 따라 새로운 분야에 적용 가능한 알고리즘의 범용성이 필수적이다. 본 논문이 제안하는 One-Time-Pad 알고리즘은 여러 환경에서 적용 가능한 특징을 고려하였다.

성능 분석 결과 알고리즘 연산 회수에 따른 지연이 다소 발생했고 제안하는 One-Time-Pad 외에 임의로 구성된 3가지의 One-Time Password 생성방법과 비교 분석해본 결과, 2차 보안수단으로서 지녀야할 효율성 면에서는 다른 방법에 비해 낮은 수치를 나타냈지만 보안성면에 있어 가지는 복잡도로 인해 보안성은 강화될 수 있다는 것을 확인하였다.

특히 국내 2차 보안기술들의 경우 대부분이 특정 플랫폼에 한정되어 실행되기 때문에 간단한 DLL 후킹을 사용한 공격만으로도 암호를 알아낼 수 있다. 이러한 One-Time Password의 취약성에 대한 관리자는 2채널 인증에 대한 보안 강화를 위해 노력을 기울여야 하며, 원초적으로는 위와 같은 기술적인 결함이 해결되어야 할 것이다.

향후 본 논문에서 제안하는 알고리즘과 더불어 해당 기관과의 금융거래 관련된 거래 설정에 대한 조건을 부여한다면, 지금까지 거론된 해킹사례의 문제점을 해결하는데 큰 도움이 될 것으로 예상된다. 하지만, 텍스트 정보를 위한 처리가 아닌 대용량의 정보 처리를 위한 One-Time-Pad의 발생이 이루어지는 경우는 효율성면에 있어 확실한 개선사항이 필요할 것으로 판단된다. 결과적으로 본 논문의 One-Time-Pad를 금융 서비스뿐만 아니라 게임, 모바일 등 각 응용서비스 별로 상호 인증 등에 활용한다면 그 범위는 크게 확장될 수 있을 것이다.

References

[1] Dirk Rijmenants, “IS One-time Pad History?”, Cipher Machines & Cryptology, Mar, 2015.

[2] Jeong-In Kim, Nam-Hi Kang, “Secure Configuration Scheme of Pre-shared Key for Lightweight Devices in internet of Things”, International Journal of Internet, Broadcasting and Communication (IJIBC), vol. 15, no. 3, pp.1-6, June, 2015.

[3] Dirk Rijmenants, “THE COMPLETE GUIDE TO SECURE COMMUNICATIONS WITH THE ONE TIME PAD CIPHER”, Cipher Machines & Cryptology, Dec, 2014.

[4] Sang-Ho Lee, Sung-Bea Kang, Dae-Hun Nyang, Kung-Hee Lee, “Effective Palm Print Authentication Guideline Image with Smart Phone”, Journal of the Korea Institute of Communication Sciences (J-KICS), vol. 39C, issue. 11, pp.994-999, Nov, 2014.

[5] Young-chul Choung, Kwang-Cheol Rim, “Research of Secret Communication Using Quantum key

Distribution and AES", Journal of the Korea Institute of Information and Communication Engineering (JKIICE), vol. 18, no. 1, pp. 84-90, Jan, 2014.

[6] Young-Do Joo, "Analysis on Security Vulnerabilities of a Biometric-based User Authentication Scheme for Wireless Sensor Networks", International Journal of Internet, Broadcasting and Communication (IJIBC), vol. 14, no. 1, pp.147-153, Feb, 2014.

[7] Won-Keun Choi, "Resource Manager of QoS Supporting of Q-MOTP for Multimedia Object Data Transfer in MPLS Network Using Q-CBQ", Journal of the Korea Institute of Communication Sciences(J-KICS), vol. 38B, issue. 12, pp.962-966, Dec, 2013.

[8] Nithin Nagaraj, "One-Time Pad as a nonlinear dynamical system", Commun ications in Nonlinear Science and Numerical Simulation(CNSNS) vol. 17, issue. 11, pp. 4029-4036, Nov. 2012.

[9] Telecommunications Technology Association, "Algorithm Profile for One-Time Password", TTAK.KO-12.0193, Dec, 2012.

[10] Rosslin John Robles, Tai-Hoon Kim, "Securing Internet-based SCADA Wireless Component Communication", International Journal of Internet, Broadcasting and Communication (IJIBC), vol. 4, no. 1, pp. 3-7, Feb, 2012.

[11] Jung-Woo An, "A study on interactive authentication method using mobile one time password interlocked transaction for secure electronic financial transactions", Kookmin Univ, Master's thesis, Feb, 2010.

[12] Hae-soon Ahn, Eun-jun Yoon, Ki-dong Bu, In-gil Nam, "Secure and Efficient DB Security and Authentication Scheme for RFID System", The Journal of Korea Information and Communications Society (J-KICS), vol. 36, issue. 4C, pp. 197-206, Apr, 2011.

[13] Telecommunications Technology Association, "Guideline for Implementing Secure Mobile Systems Based on PKI", TTAE.IT-X1122, Dec, 2009.

[14] Young-Tae KIM, Su-Mi Lee, Bong-Nam Noh, "The Considerable Security Issues on the Security Enforcement of Cryptographic Technology in Finance Fields", Journal of the Korea Institute of Information Security and Cryptology (KIISC), vol. 19, no. 4, pp.137-142, Aug, 2009.

[15] Jong-In Lim, Dong-Hoon Lee, "Study on using secure passwords in the financial sector", Financial Informatization Promotion Committee Secretariat Bank of Korea pay stations, Research Service report, 2008.

저자 소개

이 길 헌(정회원)

- 2009년 2월 : 서일대학교 정보통신공학과 졸업
- 2012년 8월 : 숭실대학교 컴퓨터학과 석사
- 2013년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 박사과정

<주관심분야 : 컴퓨터통신, 정보보안, 암호학, 빅데이터, IoT>

전 문 석(정회원)

- 1981년 2월 : 숭실대학교 전산학과 졸업
- 1986년 2월 : University of Maryland Computer Science 석사
- 1989년 2월 : University of Maryland Computer Science 박사
- 1991년 ~ 현재 : 숭실대학교 컴퓨터학과 정교수

<주관심분야 : 정보보호, 네트워크 보안, 암호학>

최 도 현(정회원)

- 2008년 2월 : 동서울대학교 컴퓨터소프트웨어학과 공학사
- 2010년 8월 : 숭실대학교 컴퓨터학과 석사
- 2010년 9월 ~ 현재 : 숭실대학교 컴퓨터학과 박사과정

<주관심분야 : 모바일 보안, PKI, Secure Coding>