情報保護學會論文誌
第 21 卷 第 1 號, 2011. 2

피싱 방지 및 가용성 개선을 위한 PKI기반의 모바일 OTP(One Time Password) 메커니즘에 관한 연구

김 태 형,† 이 준 호, 이 동 훈‡
고려대학교 정보보호대학원

Study on Mobile OTP(One Time Password) Mechanism based PKI for Preventing Phishing Attacks and Improving Availability

Tha-Hyung Kim,† Jun-Ho Lee, Dong-Hoon Lee‡
Financial Information Security, Graduate School for Information Security, Korea University

요 약

IT기술 및 정보통신망의 발달은 온라인 금융거래를 활성화 시켰고 사용자들은 다양한 금융서비스를 받을 수 있게 되었다. 하지만 이러한 긍정적인 효과와는 다르게 2009년 7월 7일에 발생한 DDoS(Distribute Denial of Service)공격과 같이 사용자들에게 피해를 주는 부정적인 효과도 초래하였다. 온라인 금융거래에서도 피싱(Phishing) 사이트와 같이 인증절차를 우회할 수 있는 예측 불가능한 공격이 발생하게 되었으므로 OTP(One Time Password)인증과 같이 온라인 금융거래에 이용되는 인증기술에 대해서도 다각도로 안전성을 검토해야한다. 따라서 OTP 인증의 안전성을 높이기 위해 본 논문에서는 PKI기반의 모바일 OTP 메커니즘을 제안한다. 제안하는 메커니즘은 PKI기반에서 운용되므로 사용자와 인증서버의 디지털서명과 공개키 암호화를 통하여 OTP 생성을 위한 비밀 값은 안전하게 전송되고 생성된 OTP는 사용자가 웹사이트에 입력하는 것이 아니라 모바일 단말기에서 인증서버로 직접 전송(Direct Transmission)되기 때문에 2006년에 발생한 시티은행 피싱 사이트에서 드러난 OTP 인증 방식의 문제점이 해결되고 사용자의 가용성(편의성)을 높이게 된다.

ABSTRACT

The development of IT technology and information communication networks activated to online financial transactions; the users were able to get a variety of financial services. However, unlike the positive effect that occurred on 7 July 2009 DDoS (Distribute Denial of Service) attacks, such as damaging to the user, which was caused negative effects. Authentication technology(OTP) is used to online financial transaction, which should be reviewed to safety with various points because the unpredictable attacks can bypass the authentication procedure such as phishing sites, which is occurred. Thus, this paper proposes mobile OTP(One Time Password) Mechanism, which is based on PKI to improve the safety of OTP authentication. The proposed Mechanism is operated based on PKI; the secret is transmitted safely through signatures and public key encryption of the user and the authentication server. The users do not input in the web site, but the generated OTP is directly transmitted to the authentication server. Therefore, it is improvement of the availability of the user and the resolved problem is exposed from the citibank phishing site(USA) in 2006.

Keywords: OTP, Mobile OTP, Authentication, Phishing, Availability

접수일(2010년 08월 30일), 게재확정일(2010년 10월 25일)

† 주저자, k2470585@naver.com
‡ 교신저자, donghlee@korea.ac.kr

I. 서 론

온라인상에서의 인증(Authentication)이란, 네트워크 환경에서 특정 자원에 접근하는 사용자의 신원을 파악하는 것이다. 즉, 신원이 불분명하다면 온라인 네트워크의 자원에 접근할 수 없도록 하는 것이다. 인증요소의 종류에는 지식기반(ID/Password)인증, 소유기반(보안카드, OTP 등)인증, 생체기반(홍채, 지문, 음성 등)인증이 있으며 각각의 인증요소를 사용하는 방법에 따라 단일요소인증(1-Factor), 이중요소인증(2-Factor), 삼중요소인증(3-Factor)으로 구분된다. 일반적으로 금전적인 피해가 직접적으로 없는 포털사이트나 개인 홈페이지는 ID/Password 방식으로 사용자 인증을 하고 있으나 금융거래와 같이 금전적 피해가 예상되는 서비스에 대해서는 강력한 인증이 필요하다. 하지만 초기에 사용된 온라인 금융거래를 위한 인증방법에서는 암호화 되지 않은 ID/Password 방식을 도입하였기에 쉽게 공격자에게 노출될 수 있었다. 그래서 ID/Password를 암호화하는 방식을 적용하였지만 스니핑(Sniffing), 스푸핑(Spoofing), 피싱(Phishing) 파밍(Pharming)등 공격방법이 다양해짐에 따라 안전하지 못하다는 결론에 도달하였다. 그러므로 현재에는 금융거래에서 가장 많이 사용하는 방식인 공인인증서 + 보안카드 방식(2-Factor)이 사용된다. 하지만 보안카드 역시 키보드 입력을 알 수 있는 키로그(Key Log) 공격에 취약점이 드러나 금융감독원에서는 2008년 4월 1일부터 인터넷 뱅킹 이용시 개인이체한도 1억원 이상에서는 보안카드 대신에 1등급 보안 수단인 OTP단말기를 의무적으로 사용하도록 규정하였다. 그러나 OTP단말기가 활발하게 이용되지 못하고 있는 실정이고 이는 통계자료를 통해서 알 수 있다. 2008년 말 한국은행이 발표한 통계에서 인터넷뱅킹 이용자수는 약 5260만 명으로 집계되었고 금융보안연구원이 집계한 발급된 OTP단말기 수는 377만개였다. 비율로 환산하면 7% 이다. 올해 2010년 2/4분기 자료에서는 인터넷 뱅킹 이용자수가 6334만 명이고 OTP단말기 발급 수는 약 398만개이다. 비율로 환산한다면 약 6%정도 OTP단말기를 이용하고 있는 것이다. 인터넷뱅킹 이용자수를 은행별로 중복 집계하기 때문에 현재 총인구수를 넘는 것으로 파악되지만 이러한 점을 고려하더라도 OTP이용은 아직까지는 낮은 수준이다. 이러한 상황에서 피싱 공격으로 인한 OTP의 취약점이 발견된 2006년의 시티은행 피싱 사이트 사건과 유사한 사례가 국내에도 발생한다면 사용자로 하여금 불안함이 가중되고 OTP 안전성에 대해서 의구심을 제기하게 만들어 이용률 높이지 못하게 된다.[18] 그러므로 현재 이용률을 높이기 위한 방안으로 OTP를 부가적인 장치(OTP 생성 단말기)에서 생성하는 것이 아니라 모바일 단말기에서 생성 하려는 논의가 계속 되고 있으며 모바일을 이용한 OTP인증과 관련하여 다양한 연구가 진행되고 있다.[4][5][6][7][8][9][10] 국내에서도 OTP 기술의 발전 방향으로 USIM기반 모바일 OTP 기술, 부인방지 지원 OTP 및 거래연동 OTP기술에 관하여 기술적 검토가 이루어지고 있다.[17] 본 논문에서 제안하는 모델은 모바일 단말기를 이용하여 PKI(Public Key Infrastructure)기반의 OTP생성 방식을 제안하였고 현재 OTP 동기화 방식 중 주로 사용되고 있는 시간동기(Time-Synchronous)방식이 아닌 시도 응답(Challenge- Response)방식을 사용하였다. 생성한 OTP를 사용자 PC(웹사이트)에 입력하는 것이 아니라 모바일 단말기에서 직접 인증서버로 전송하는 방식을 사용하였기 때문에 숫자나 문자를 입력해야하는 장치가 모바일 단말기 하나로 통일되어 편리함을 제공하며 예방하기 어려운 웹사이트 피싱 공격에도 안전성을 제공한다. 그리고 사용자와 서버의 디지털서명(이하 서명으로 표기)과 공개키 암호화를 통하여 OTP 생성을 위한 비밀 값은 안전하게 전송되며 OTP는 사용자가 서명을 한 후 전송되므로 부인방지 기능도 추가된다. 본 논문의 구성으로, 2장에서는 관련연구, 3장에서는 보안위협 및 요구사항을 기술한다. 4장에서는 본 논문에서 제안하는 PKI기반의 피싱 방지 및 가용성 개선을 위한 모바일 OTP 메커니즘 모델을 기술하고 5장에서는 제안모델을 각 요소에 따라 분석한다. 마지막 6장에서는 결론을 끝으로 논문을 마치고자 한다.

II. 관련연구

서론에서 언급하였듯이 현재 금융거래에 사용되는 OTP 동기화 방식은 주로 시간동기화 방식을 사용하고 있다.[17] 하지만 RFC 1760, RFC 1938, RFC 2289[1]와 같은 표준 및 과거의 연구들에서는[2][3] 시간동기화 방식보다는 시도 응답(Challenge- Response)방식을 기반으로 한 메커니즘을 사용하였다. 본 장에서는 현재 사용되고 있는 동기화 기술과 모바일 단말기를 이용한 OTP인증에 관련된 연구를 소개한다.

2.1 OTP 동기화 기술

OTP 동기화 기술은 시도 응답(Challenge-response)방식, 시간 동기화(Time-Synchronous)방식, 이벤트 동기화(Event-Synchronous)방식, 조합(Time+Event-Synchronous)방식과 같이 네 가지 방식으로 나눌 수 있다.

2.1.1 시도 응답(Challenge-response) 방식

서버가 제시하는 시도 값을 사용자가 알고리즘에 입력해 출력되는 값을 얻고 이를 응답 값으로 서버에 전송하여 자신을 인증하는 방식이다. 인터넷 뱅킹에서의 보안카드 숫자 입력이 바로 시도 응답 방식이다. '14번 앞의 두 자리를 입력하세요. 22번 뒤의 두 자리를 입력하세요.' 의 질문에서 '14, 22'이라는 숫자가 시도 값에 해당하며, 이에 대한 응답 값은 보안카드의 14번의 앞자리 비밀번호, 22번의 뒷자리 비밀번호가 된다. 현재 사용되는 OTP 단말기는 보통 6자리 시도 값을 입력하여 6자리의 OTP를 응답 값으로 사용한다. 서버가 임의의 난수(Random Number)를 생성하여 사용자에게 전송하면 사용자는 해당 시도 값을 OTP단말기에 입력하여 그 결과로 얻은 OTP를 다시 입력하는 방식이다. 이 방식은 사용자가 ID/Password와는 별도로, OTP단말기에 시도 값을 입력하고, 그 값을 다시 PC(웹사이트)로 입력하는 등 입력 내용이 많아서 불편하다.

2.1.2 시간 동기화(Time-Synchronous) 방식

시도 응답 방식이 가지고 있는 사용자의 입력횟수가 많은 단점을 개선하기 위해 개발된 방식으로 임의의 난수 대신에 시간 값을 OTP생성을 위한 입력 값으로 사용한다. 서버와 OTP단말기 간에 동기화된 시간을 기준으로 특정 시간 간격(보통 30초)마다 변하는 OTP를 생성하게 된다. 하지만 시간동기화 방식의 경우 특정 시간 간격마다 OTP가 변하기 때문에 OTP를 입력하는 도중에 다른 값이 생성되어 OTP가 변경되는 단점이 있다. 이러한 단점 때문에 시간 간격을 길게 설정할 경우 공격자가 중간에 OTP를 알아채 사용할 가능성이 커지게 되는 또 다른 문제점이 생길 수 있다. 그리고 시간 동기가 어긋날 경우에는 인증이 실패 할 수 있기 때문에 추가적으로 OTP단말기와 서버간의 시간 동기를 맞추는 알고리즘이 필요하다.

2.1.3 이벤트 동기화(Event-Synchronous)방식

이벤트 동기화 방식은 서버와 OTP단말기가 동기화된 시간 대신에 동일한 카운트 값을 기준으로 비밀번호를 생성하는 방식이다. 사용자가 OTP를 생성할 경우, 카운트 값을 OTP알고리즘의 입력 값으로 사용하여 OTP를 생성하고, OTP를 생성한 후에는 카운터 값을 증가시켜서 저장해두었다가 다음번에 사용한다. 이 방식의 경우 OTP단말기에서 OTP만 여러 번 생성하고 해당 OTP를 서버에 입력하지 않으면, OTP단말기와 서버 간의 카운트 값이 달라져 OTP단말기를 다시 초기화해야하는 단점을 가지고 있다.

2.1.4 조합(Time+Event-Synchronous)방식

시간동기화와 이벤트 동기화 방식의 단점을 보완하기 위해서 두 가지 방식을 조합한 OTP 생성 방식이다. 이 방식은 OTP생성 입력 값으로 시간 값과 카운터 값을 모두 사용하는 방식이다. 시간동기화와 같이 특정 시간 간격마다 비밀번호는 새로 생성되며, 같은 시간 내에 OTP 생성 요청이 여러 번 발생하면 카운트 값을 증가시켜 새로운 Password를 생성하도록 하는 방법이다. 이렇게 함으로써, 동일한 시간간격 내에서도 새로운 Password를 생성할 수 있게 되고 이를 통해 OTP Password의 1회성을 높여 안전성이 좋아진다.

2.2 모바일 단말기를 이용한 OTP인증 메커니즘

최근에 연구되고 있는 모바일 단말기를 OTP생성기기로 사용한 인증 메커니즘은 1) 안전한 모바일 기반, 2) SMS 메시지 기반, 3) 비접촉식 기반 인증과 같이 3가지로 나눌 수 있다.

2.2.1 안전한 모바일 기반 인증

모바일 단말기에 사용되는 WIM(Wireless Identity Module)을 적용한 SIM 카드를 이용하여 OTP를 생성하고 사용자는 OTP를 이용하여 인증하는 방법을 제안하였다.[5] 하지만 제안한 방법에서는 OTP를 인증한 이후에 서버가 정당한지 검증하기 때문에 악의적인 서버일 경우 매우 위험해진다. 그러므로 서버인증이 완료된 후 OTP를 인증해야 보다 안전한 인증이 된다.

2.2.2 SMS 메시지 기반 인증

사용자는 인증 서버에게 자신이 부여받거나 등록한 비밀정보(PIN 혹은 Password)를 웹사이트를 통해서 입력하거나 SMS로 전송한다. 비밀정보를 전송받은 1)서버는 모바일 단말기에 SMS를 통해 난수를 전송한 후 모바일 단말기는 난수를 이용하여 OTP를 생성하거나 2)서버에서 직접 OTP를 생성하고 SMS를 통해 모바일 단말기에 전송한다. 이 후 사용자는 모바일 단말기에서 획득한 OTP를 이용하여 서버를 통해 인증을 받는다.[4][7][8][9]

2.2.3 비접촉식 기반 인증

비접촉식 기반 인증의 특징은 모바일 단말기와 서버가 통신을 하지 않는 것이다. 비접촉으로 OTP인증이 가능한 이유는 모바일 단말기와 서버는 동일한 인자 값으로 OTP를 생성을 한다. 다시 말하여, 모바일 단말기에서 PIN이나 사용자만이 알 수 있는 비밀정보가 OTP를 생성하는 인자 값이 된다. 마찬가지로 서버 역시 모바일 단말기와 동일한 인자 값으로 OTP를 생성하기 때문에 모바일 단말기가 생성한 OTP와의 비교를 통해 인증결과를 나타낸다.[7][9]

위의 3가지 방식 모두 OTP생성에는 안전성이 보장되지만 생성한 OTP를 이용하여 인증 받을 때 문제점이 발생 된다. 즉, OTP를 웹사이트에 입력함으로서 웹사이트를 가장한 피싱 공격에 취약하게 된다.

III. 보안위협 및 요구사항

본 장에서는 모바일 단말기를 이용한 OTP 메커니즘에서 발생될 수 있는 보안위협에 대해서 알아보고 그에 따라 요구되는 사항에 대해서 알아본다.

3.1 보안 위협

개인정보 및 금융거래 정보와 같이 중요한 정보일수록 보안의 중요성은 더욱더 강조된다. 하지만 통신단말기 사이에 전송되는 정보는 제 3자를 통하여 불법적으로 유출되거나 변조되고 OTP생성을 위한 정보 역시 전송되는 과정에서 공격자에게 불법적인 공격을 받을 수 있는 위협에 노출되어 있다.

◉ 스니핑(Sniffing) : 각 객체사이에서 인증을 위해 전송되는 정보들은 공격자에게 노출 될 수 있다.

◉ 재전송 공격(Replay Attack) : 공격자는 정당한 객체들 사이에 전송되는 정보들을 획득한 후 인증을 위해 획득한 정보를 재전송함으로써 정당성을 검증받거나 중요 정보를 획득하여 정당한 객체로 위장할 수 있다.

◉ 중간자 공격(Man-In-The-Middle Attack) : 공격자는 정당한 객체들 사이에서 인증을 위해 전송되는 정보들을 가로채어 정당한 객체로 위장할 수 있고 가로챈 정보들을 분석하여 중요 정보를 획득하거나 생성하여 정당한 사용자로 위장할 수 있다.

◉ 서비스 거부 공격(Denial of Service Attack) : 공격자가 전송되는 정보를 위조 및 변조하여 정당한 객체가 인증 받지 못하도록 하거나 정당한 객체에게 지속적인 서비스를 제공하지 못하게 할 수 있다.

◉ 피싱 공격(phishing Attack) : 공격자는 정당한 객체가 가진 인증 정보(OTP정보)를 알아내기 위한 사회 공학적 사기수법을 통하여 인증정보를 획득할 수 있고 정당한 사용자로 위장할 수 있다.

3.2 요구 사항

OTP인증 메커니즘 안에서 각 객체가 주고받는 데이터는 위, 변조가 불가능해야 하고, 각 객체가 정당한 객체인지 상호간에 검증되어야 한다. 그러므로 다음과 같이 3가지 보안요소[기밀성(Confidentiality), 무결성(Integrity), 상호인증(mutual authentication)]가 요구되고, OTP생성 단말기에는 보안성(Security), 독립성(Independence), 가용성(Availability)이 추가로 요구된다.

1) OTP 보안 요구사항

◉ **기밀성(Confidentiality)** : 각 객체들 사이의 통신에서 노출되지 말아야할 비밀 정보는 허용되지 않은 객체 및 불법적인 제 3자에게 노출되지 말아야 한다. 즉, OTP값을 생성하기 전까지 통신 되는 정보들은 암호화되어 노출되지 않아야 한다.

◉ **무결성(Integrity)** : 각 객체들 사이의 통신

되는 정보들은 변경, 삭제, 재생성 되지 않아야 하며 올바른 값이 전달되어야 한다. 즉, OTP를 생성하기 위한 입력 값은 불법적인 변조가 없어야 하며 동일한 입력 값을 통하여 동일한 OTP를 생성해야 한다.

◉ **상호인증(mutual authentication)** : 각 객체들 메커니즘 내의 정보들을 이용할 수 있는 정당한 객체인지를 나타낼 수 있어야 하고 정당한 객체가 아님을 부인할 수도 없어야 한다. 즉, 모바일 OTP메커니즘 내에서 OTP를 생성하고 통신하는 객체들은 서로 간에 정당한 사용자임이 인증되어야 한다.

2) OTP생성 단말기 요구사항

◉ **보안성(Security)** : OTP단말기에는 허가된 사용자만이 접근이 가능해야 한다.

◉ **독립성(Independence)** : OTP단말기는 2-Factor인증을 위해 독립적인 인증매체의 역할을 해야 한다.

◉ **가용성(Availability)** : OTP단말기는 사용자가 이용하기에 불편함이 없어야 한다.

IV. 제안모델

본 절에서는 모바일에서 생성한 OTP를 사용자가 PC(웹사이트)에 입력하지 않고 모바일을 이용하여 서버에 직접 전송(*Direct Transmission*)토록 하는 메커니즘을 제안한다. 제안하는 메커니즘으로 인하여 첫 째, 사용자는 모바일 단말기에서 OTP를 생성하고 인증서버에게 전송하기 때문에 OTP생성 후 OTP를 다시 PC(웹사이트)에 입력해야 하는 수고가 줄어들어 가용성(편의성)이 높아지고 둘째, 모바일 단말기를 통하여 실질적으로 인증되기 때문에 PC(웹사이트)에서의 키로그 공격뿐만 아니라 피싱 공격에서도 안전성을 보장받을 수 있게 된다.

4.1 메커니즘 가정

인증 메커니즘의 환경은 한국인터넷진흥원에서 제정한 무선단말기에서의 공인인증서 저장 및 이용 기술규격과 무선단말기와 PC간 공인인증서 전송을 위한 기술규격의 바탕이 되는 PKI 기반에서 운영된다. 클라이언트(Client)측인 모바일 단말기 및 사용자 PC와 서버(Server)측인 인증서버는 CA(Certificate Authority)로부터 인증서를 발급받을 수 있고 서로의 공개키를 알 수 있어 서명과 공개키 암호화를 통하여 통신(클라이언트(모바일 단말기)와 서버와의 통신, 예: 소켓통신)이 가능하다.

4.2 인증 단계별 시나리오

제안 메커니즘의 구조는 (1) 사용자 인증 단계 (2) 인증서버 OTP생성 단계 (3) 난수 확인 단계 (4) 모바일 OTP생성 및 전송 단계 (5) 모바일 OTP인증 단계와 같이 5단계로 구성되어 있다 [그림 1].

4.2.1 메커니즘 계수

메커니즘 구조를 설명하는데 다음과 같은 계수를 사용한다.

◉ U_P (User PC) : 사용자 PC.

◉ U_M (User Mobile) : 사용자 모바일.

◉ *AS* (Authentication Server) : 인증서버.

◉ *OPW* (OTP Generation Password) : OTP생성을 위한 비밀번호.

◉ *SRN* (Server Random Number) : 인증서버용 난수. (※*MRN*과 동일)

◉ *MRN* (Mobile Random Number) : 모바일 단말기용 난수. (※*SRN*과 동일)

◉ $Sign_S$ (A)(Server Sign Algorithm) : 인자 값 A를 인증서버의 개인키로 서명.

◉ $Sign_U$ (A)(User Sign Algorithm) : 인자 값 A를 사용자의 개인키로 서명.

◉ $Veri_S$ (A)(Server Verification Algorithm) : 인자 값 A를 인증서버의 공개키로 검증.

◉ $Veri_U$ (A)(User Verification Algorithm) : 인자 값 A를 사용자의 공개키로 검증.

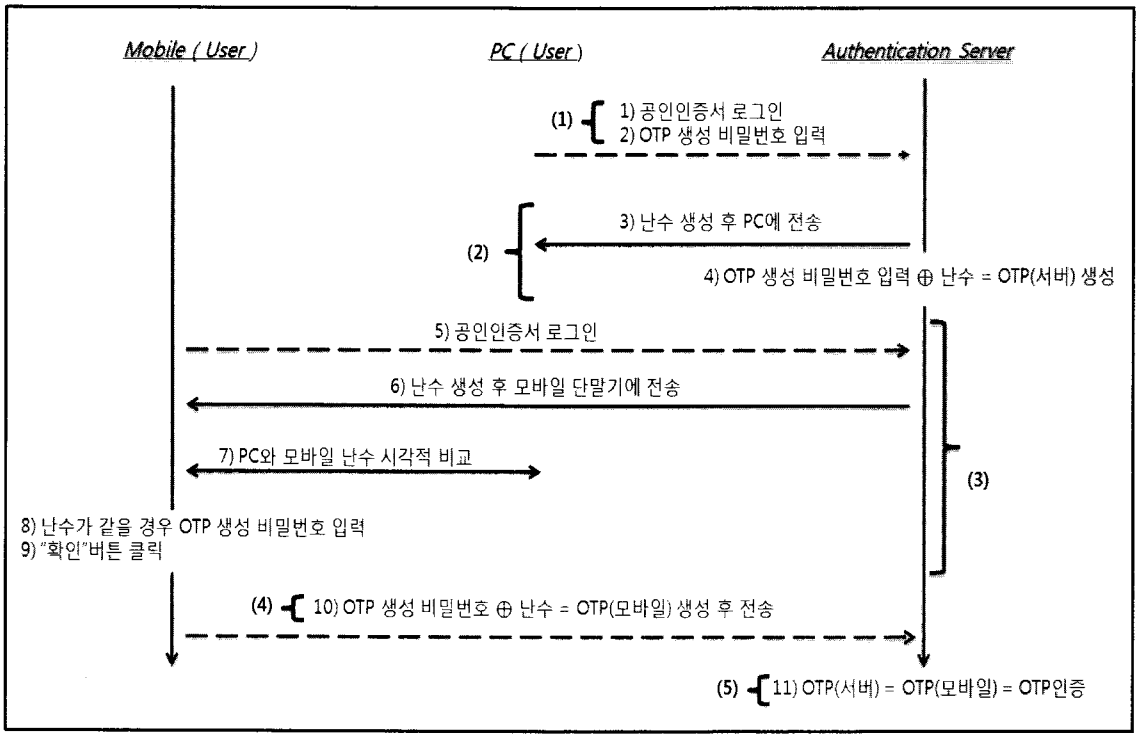
◉ Enc_S (A)(Server Encryption Algorithm) : 인자 값 A를 인증서버의 공개키로 암호화.

◉ Enc_U (A)(User Encryption Algorithm) : 인자 값 A를 사용자의 공개키로 암호화.

◉ Dec_S (A)(Server Encryption Algorithm) : 인자 값 A를 인증서버의 개인키로 복호화.

◉ Dec_U (A)(User Encryption Algorithm) : 인자 값 A를 사용자의 개인키로 복호화.

◉ *MOTP* : 모바일 단말기에서 생성된 OTP.



〔그림 1〕 제안모델의 메커니즘 구조

◉ *SOTP* : 인증서버에서 생성된 OTP.
◉ *OTP(A)* : 인자 값 A를 OTP 생성 알고리즘에 적.용
◉ *OA* (OTP Authentication) : OTP 인증완료.
◉ *Direct Transmission* : 모바일 단말기에서 인증서버에 직접 전송.(웹사이트에 OTP를 입력하지 않음)

4.2.2 각 단계별 인증 메커니즘

제안모델의 인증 메커니즘을 단계별로 구체화하여 프로토콜로 나타내었다〔그림 2〕.

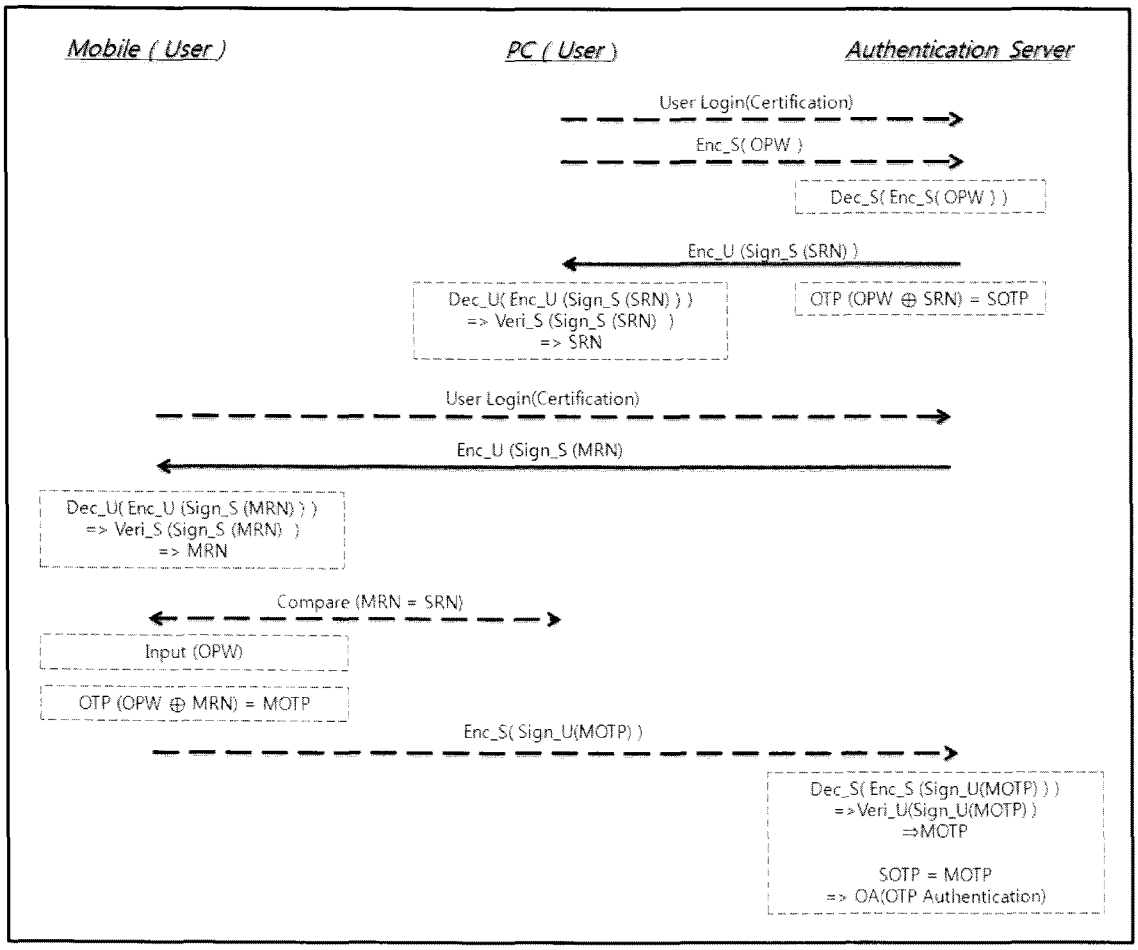
◉ **사용자 인증 단계** : 사용자는 PC(웹사이트)에서 공인인증서 로그인을 한다. 로그인 후 OTP 생성을 위한 비밀번호를 입력한다.

1) $U_P \rightarrow AS$: 사용자 인증서 로그인.
2) U_P : OPW 입력.
3) $U_P \rightarrow AS$: $Enc_S(OPW)$ 생성 후 인증서버에 전송.
4) AS : $Dec_S(Enc_S(OPW)) = OPW$ 획득.

◉ **인증서버 OTP 생성 단계** : 사용자가 인증된 후 인증서버가 OTP생성을 위한 비밀번호를 획득하면 인증서버는 2개의 같은 난수를 생성하여 하나는 사용자의 PC(웹사이트)에 전송하고 다른 하나는 사용자의 모바일 단말기에 전송한다. 그리고 OTP생성을 위한 비밀번호와 인증서버 자신이 생성한 난수를 XOR하여 OTP생성 알고리즘의 입력 값으로 사용한다.

5) AS : SRN, MRN 생성. ($SRN = MRN$)
6) AS : $Sign_S(SRN), Sign_S(MRN)$ 생성.
7) AS : $Enc_U(Sign_S(SRN)), Enc_U(Sign_S(MRN))$ 생성.
8) $AS \rightarrow U_P$: $Enc_U(Sign_S(SRN))$를 사용자 PC에 전송.
9) U_P : $Dec_U(Enc_U(Sign_S(SRN)))$
$\Rightarrow Veri_S(Sign_S(SRN)) \Rightarrow SRN$ 획득.
10) AS : $OTP(OPW \oplus SRN) = SOTP$ 생성.

◉ **난수 확인 단계** : 사용자는 모바일 단말기에 설치된 공인인증서에 로그인을 하면 인증서버로부터 받은 난수를 볼 수 있다. 그리고 PC(웹사이트)와 모바일 단말기에서 받은 난수가 동일한지 비교하고 OTP생성을 위한 비밀번호를 입력한 후 "확인"버튼을 누른다〔그림 3〕.



〔그림 2〕 제안모델의 단계별 인증 프로토콜 흐름도

11) $U_M \rightarrow AS$: 사용자 인증서 로그인.

12) $AS \rightarrow U_M$: $Enc_U(Sign_S(MRN))$를 사용자 모바일 단말기에 전송.

13) U_M : $Dec_U(Enc_U(Sign_S(MRN)))$ $\Rightarrow$ $Veri_S(Sign_S(MRN))$ $\Rightarrow$ MRN 획득. (9번 참조)

14) $U_M \leftrightarrow U_P$: $MRN = SRN$ 비교확인.(화면을 통한 시각적 비교)

15) U_M : OPW 입력.

◉ **모바일 OTP 생성 및 전송 단계** : 모바일 단말기는 OTP생성을 위한 비밀번호와 인증서버로부터 받은 난수를 XOR하여 OTP를 생성하고 인증서버에 OTP를 전송한다.

16) U_M : $OTP(OPW \oplus MRN) = MOTP$ 생성.

17) $U_M \rightarrow AS$: $Enc_S(Sign_U(MOTP))$ 생성 후 인증서버에 전송.(*Direct Transmission*)

◉ **모바일 OTP 인증 단계** : 인증서버는 자신이 생성한 OTP와 모바일 단말기로부터 받은 OTP를 비교하고 동일하다면 인증을 완료한다.

18) AS : $Dec_S(Enc_S(Sign_U(MOTP)))$ $\Rightarrow$ $Veri_U(Sign_U(MOTP))$ $\Rightarrow$ $MOTP$ 획득.

19) AS : $MOTP = SOTP$ 비교확인 후 인증

V. 제안모델의 분석

금융거래에는 특히 사용자의 정당성이 검증되어야 하고 특히, 안전한 금융거래를 위해 모바일 단말기를 사용할 때에는 전송되는 정보가 기밀하고 위, 변조가 없어야 하며 사용자가 정당하게 인증 받는 다는 것을 알 수 있어야 한다.

5.1 보안위협에 대한 분석

3장에서 소개한 위협인 스니핑, 재전송 공격, 중간자 공격, 서비스 거부 공격, 피싱 공격에 대하여 제안 모델의 안정성을 분석한다.

◉ **스니핑(Sniffing)** : 인증서버 및 모바일 단말기로 전송되는 정보들은 공개키[Enc_S, Enc_U]로 암호화되기 때문에 개인키를 알고 있지 않는 이상 공격자는 원하는 정보를 알 수 없다.

◉ **재전송 공격(Replay Attack)** : OTP를 생성하는 입력 값이 인증서버와 모바일에 전송되는 난수(*SRN*, *MRN*)에 의존하고 있으므로 난수(*SRN*, *MRN*)를 가로채어 다음세션에 재전송하는 것 자체가 무의미한 것이다. 즉, 공격자가 난수(*SRN*, *MRN*)를 가로채고 OTP를 만들어 인증서버에 보내어도 인증서버는 이전 세션과 다른 난수(*SRN*)값으로 OTP를 생성하기 때문에 인증받을 수 없다.

◉ **중간자 공격(Man-In-The-Middle Attack)** : 인증서버와 모바일에 전송되는 난수(*SRN*, *MRN*)와 OTP를 변조하기 위해서는 사용자의 개인키[$Sign_U$]를 알아야하기 때문에 공격자는 변조가 불가능하다. 그리고 PC에 전송되는 난수와 모바일 단말기에 전송되는 난수를 동시에 변조하기란 더 불가능 하다.

◉ **서비스 거부 공격(Denial of Service Attack)** : 난수(*SRN*, *MRN*)를 다르게 변조하여 OTP를 생성하지 못하게 하기 위해서는 중간자 공격과 마찬가지로 사용자의 개인키[$Sign_U$]를 알아야하기 때문에 불가능하다.

◉ **피싱 공격(phishing Attack)** : 모바일 단말기는 OTP만 생성하는 것이 아니라 OTP를 인증서버에 직접 전송(*Direct Transmission*)하고 OTP가 평문이 아닌 사용자의 서과 인증서버의 공개키로 암호화$Enc_S(Sign_U(MOTP))$ 되어 전송되므로 웹사이트를 통해 OTP를 획득하려 것과 같은 사회 공학적 피싱 공격은 무의미하게 된다.

5.2 요구사항에 대한 분석

제안모델의 메커니즘이 3장에서 기술한 OTP보안 요구사항과 OTP생성 단말기의 요구사항에 만족되는지 분석한다.

5.2.1 OTP 보안 요구사항 분석

다음에서는 OTP 보안 요구사항의 분석을 통하여 제안모델이 안전성을 살펴보고 보안위협과 요구사항과의 관계 분석을 한다 〔표 1〕.

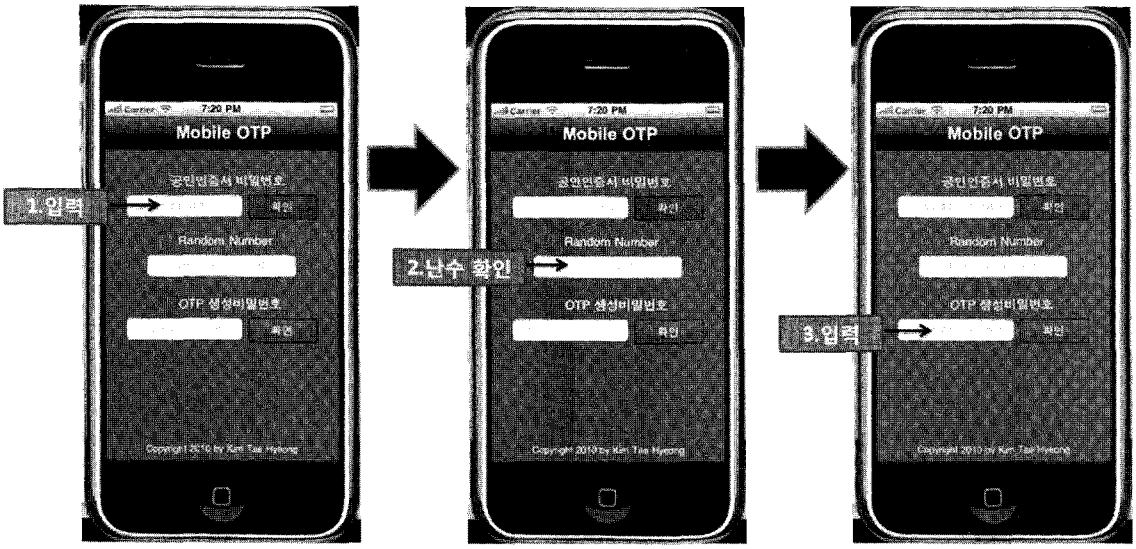
◉ **기밀성(Confidentiality)** : 난수(*SRN*, *MRN*)와 OTP를 모두 공개키로 암호화[Enc_S, Enc_U]하여 전송함으로서 기밀성이 보장된다.

◉ **무결성(Integrity)** : 1) 난수(*SRN*, *MRN*)가 사용자의 PC와 모바일 단말기에 전송될 때 위, 변조가 없어야 하기 때문에 PC와 모바일 단말기를 통하여 시각적으로 난수비교(*SRN* = *MRN*)를 하도록 하였고, 2) 난수(*SRN*, *MRN*)와 OTP는 서명과 공개키 암호화[$Enc_U(Sign_S(SRN))$, $Enc_U(Sign_S(MRN))$, $Enc_S(Sign_U(MOTP))$]를 통하여 전송하기 때문에 무결성이 보장된다.

◉ **상호인증(mutual authentication)** : 난수(*SRN*, *MRN*)를 전송할 때 인증서버는 자신의

〔표 1〕 제안모델 제공요소 대비 보안위협 및 요구사항 관계도

제안모델 제공요소	보안 위협	효과	요구 사항	효과
Enc_S, Enc_U	스니핑 방지	방지	기밀성 무결성	제공
$Sign_S$, $Sign_U$	중간자 공격 서비스거부 공격 피싱 공격 방지	방지	무결성 상호인증	제공
MRN = *SRN*	재전송 공격방지	방지	무결성	제공
MOTP = *SOTP*			상호인증	제공
Direct Transmission	피싱 공격방지	방지		



〔그림 3〕 모바일 단말기에서의 입력방식

개인키로 서명[$Sign_S(SRN)$, $Sign_S(MRN)$] 하여 전송하고 사용자에게 검증된다. 마찬가지로 OTP를 전송할 때 사용자는 자신의 개인키로 서명[$Sign_U(MOTP)$]하여 전송하고 인증서버에게 검증된다. 마지막으로 인증서버와 사용자가 생성한 OTP[$MOTP = SOTP$]를 비교함으로서 서로간의 인증은 보장된다.

5.2.2 OTP단말기 요구사항 분석

- **보안성(Security)** : 사용자에게 개별적으로 부여한 *OPW*을 인증서버의 공개키로 암호화[$Enc_S(OPW)$]하여 전송함으로서 모바일 단말기 사용의 보안성이 보장된다.
- **독립성(Independence)** : 모바일 단말기에서 OTP를 생성하고 생성된 OTP를 PC(웹사이트)에 입력하지 않고 모바일 단말기에서 직접 인증서버로 전송하기 때문에 별도의 물리적인 인증장치로서의 독립성이 보장된다.
- **가용성(Availability)** : 사용자가 OTP를 생성하기 위해 모바일 단말기에 문자를 입력하는 횟수는 2번(①공인인증서 로그인, ②*OPW*입력)이므로 기존의 모바일 단말기를 이용한 OTP생성 방식과 입력횟수(①모바일 OTP 소프트웨어 접속을 위한 로그인, ②PC(웹사이트)에 생성된 OTP번호 입력)와 같다. 그러나 현재 사용되는 방식에는 OTP를 생성한 후 PC(웹사이트)에 입력해야 하는 번거로움이 있었지만 제안모델에서의 모든 입력은 모바일 단말기에서 이루어지므로 가용성(편의성)면에서 우수하다고 볼 수 있다〔그림 3〕.

5.2.3 관련연구와 제안모델 비교분석

2장의 관련연구에서 살펴본 안전한 모바일 기반인증, SMS 메시지 기반 인증, 비접촉식 기반인증 모두 안전하게 OTP를 생성하는 방법이고 제안모델 역시 안전하게 OTP를 생성한다. 하지만 OTP를 이용하여 인증하는 방법에 있어서 제안모델을 제외한 인증 메커니즘은 웹사이트에 사용자가 OTP를 직접 입력해야 하는 방식이기 때문에 사회공학적인 방법을 이용한 피싱 사이트를 통하여 실질적으로 가장 중요한 OTP가 노출될 수 있다. 이미 공인인증서가 노출되어 OTP 인증 이전까지의 공격하는데 어려움이 없고 OTP 인증여부에 따라 공격이 성공된다면 OTP 획득은 굉장히 의미 있는 공격이 된다. 제로데이(Zero-Day) 공격처럼 예측 불허의 공격은 언제나 발생할 수 있기 때문에 대비가 필요하다. 그리고 모바일에서 생성한 OTP를 웹사이트에 직접 입력하는 행위자체는 실제 사용자가 입력했는지 증명할 수 없고 사용자로 하여금 굉장히 번거롭게 만들어 가용성(편의성)을 저하시키게 된다. 이러한 점을 비추어 볼 때 제안모델은 3가지의 장점이 있다〔표 2〕.

1) 인증서버와 단말기의 비밀을 통한 인증보다는

〔표 2〕 관련연구 VS 제안모델 분석도

분석요소 \ 모델	안전한 모바일 기반인증[5]	SMS 메시지 기반인증[4][7][8][9]	비접촉식 기반인증[7][9]	제안모델
인증기관(CA)을 통한 서버인증	미 제공(X)	미 제공(X)	미 제공(X)	제공(O) (피싱방지)
Direct Transmission (OTP직접전송)	미 제공(X)	미 제공(X)	미 제공(X)	제공(O) (피싱방지)
OTP소유자 검증	미 제공(X)	미 제공(X)	미 제공(X)	제공(O) (부인방지)
공개키/개인키 연산	해당 없음(X)	해당 없음(X)	해당 없음(X)	해당 있음(O)

PKI의 인증기관(Certificate Authority)을 통하여 서버인증이 되므로 안전성이 보장된다.

2) OTP를 웹사이트에 전송하기까지 모바일 단말기에 사용자만이 알고 있는 비밀 값(P/W, PIN등)을 입력하는 횟수는 2번이지만 모바일 단말기에서 OTP를 생성하고 인증서버에 직접 전송(*Direct Transmission*)하므로 PC(웹사이트)에 OTP를 입력하지 않아도 된다. (피싱 방지 및 가용성 개선)
3) OTP에 사용자의 서명을 한 후에 전송하므로 온라인 금융거래를 하려는 실제 소유자가 OTP를 생성했다는 것을 입증 할 수 있다.(부인방지)

그러나 제안모델은 안전한 모바일 기반인증, SMS 메시지 기반 인증, 비접촉식 기반인증과 달리 PKI기반에서 운용되므로 공개키 및 개인키 연산을 해야 한다 〔표 2〕. 하지만 국내에서는 이미 PKI기반의 공인인증서를 사용하는 모바일 뱅킹(USIM 방식, VM 방식, 스마트폰 뱅킹)이 이용되고 있기 때문에 제안 모델을 모바일 단말기에서 실질적으로 구현하는데 추가적인 인프라가 필요하지 않고 더구나 연산에 따르는 문제는 고려사항이 되지 않는다고 볼 수 있다. 특히 하드웨어나 소프트웨어의 성능이 뛰어난 스마트폰이 대중화 되고 있기 때문에 앞으로는 더욱더 제안 모델의 구현 및 실사용에는 문제될 것이 없을 것으로 판단된다.

VI. 결론

인터넷 뱅킹 사용자수는 3월에 6163만 명에서 6월말까지 171만 명(2.8%) 증가하여 6334만 명이고 만약 같은 비율로 증가한다면 3/4분기에는 약 6500만 명이 될 것이다. 지속적으로 사용자가 증가할수록 온라인 금융거래는 활발해 질 것이고 이를 노리는 해킹 및 사기 수법도 지능화되고 그 숫자도 증가할 것이다. 정보통신 인프라가 잘 갖추어진 국내의 환경은 앞으로도 예측 불허한 공격을 맞이해야 하며 안전성이 보장되는 인증기술도 무용지물이 될 수도 있다. 즉, 2009년 7월 7일에 발생한 DDoS공격에 대비하지 못하여 혼란을 빚었듯이 현재의 인증기술을 무력화 시키는 공격이 발생하여 온라인 금융대란을 맞이할 수도 있다. 국내의 온라인 금융거래를 위한 사용자 인증 기반은 PKI기반으로서 안전성이 아주 우수하다. 이러한 기반을 활용하여 보다 강력한 인증 기술을 구축해야만 앞으로의 공격에 대비가 가능하다. 따라서 본 논문에서는 PKI 기반에서 모바일 단말기와 서버의 동기화를 위해 시도 응답(Challenge- Response)방식을 사용하여 OTP를 생성하는 메커니즘을 제안하였고 제안하는 메커니즘은 PKI기반에서 운용되므로 사용자와 서버의 서명과 공개키 암호화를 통하여 OTP 생성을 위한 비밀 값은 안전하게 전송된다. 생성된 OTP는 사용자가 웹사이트에 입력하는 것이 아니라 모바일 단말기에서 인증서버로 직접 전송(*Direct Transmission*)되기 때문에 2006년에 발생한 시티은행 피싱 사이트에서 드러난 OTP 인증방식의 문제점이 해결되고 사용자의 가용성(편의성)을 높인다. 본 논문에서 제안한 것과 같이 앞으로도 안전성이 높은 OTP의 장점을 이용하여 강력한 인증 메커니즘에 대한 연구가 활발해야 할 것이고 스마트폰의 대중화로 인하여 연산 및 구현에 대한 부담이 줄어드는 만큼 안전성이 높은 PKI기반과의 연동을 하여 사용자에게 보다 안전하고 편리한 온라인 금융거래 서비스를 제공해야 할 것이다.

참고문헌

〔1〕 Haller, N.M, C. Metz, P. Nesser, M. Straw, "A One-Time Password System", RFC 2289. Fab. 1998.
〔2〕 Mitchell, C.J, Chen, L., "Comments on the S/KEY User Authentication Scheme",

ACM Operating Systems Review. Vol. 30. No. 4. pp. 12- 16, Oct. 1996.

[3] Yeh, T.C., Shen, H.Y., Hwang, J.J. "A Secure One-time Password Authentication Scheme Using Smart Cards", IEICE Trans. Commun. Vol. E85-B. No. 11. Nov. 2002.

[4] Abdulaziz S., Almazyad and Yasir Ahmad, "A New Approach in T-FA Authentication with OTP Using Mobile Phone", SecTech 2009, CCIS, Vol 58, pp.9-17, Dec. 2009

[5] Helena Rif'a-Pous, "A Secure Mobile-Based Authentication System for e-Banking", OTM 2009, Part II, LNCS 5871, pp. 848 - 860, Nov. 2009.

[6] Jacek Lach, "Using Mobile Devices for User Authentication", CN 2010, CCIS 79, pp. 263 - 268, June. 2010.

[7] Fadi Aloul1, Syed Zahidi1, Wasim El-Hajj, "Multi Factor Authentication Using Mobile Phones", International Journal of Mathematics and Computer Science, Vol4, no. 2, pp. 65 - 80, 2009(Special Issue-Analytic Number Theory)

[8] Steffen Hallsteinsen, Ivar Jorstad, Do Van Thanh, "Using the mobile phone as a security token for unified authentication," Second International Conference on Systems and Networks Communications (ICSNC 2007), icsnc, pp.68, August. 2007

[9] Fadi Aloul, Syed Zahidi, Wassim El-Hajj, "Two Factor Authentication Using Mobile Phones", Computer Systems and Applications, AICCSA 2009. IEEE/ACS International Conference. May. 2009.

[10] Jongpil Jeong, Min Young Chung, and Hyunseung Choo, "Integrated OTP-Based User Authentication and Access Control Scheme in Home Networks" APNOMS 2007. LNCS 4773, pp. 123 - 133, 2007.

[11] Hyeran Mun, Kyusuk Han and Kwangjo Kim, "3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement based on EAP-AKA", Proceedings of Wireless Telecommunication Symposium, Prague, pp 1-8, Apr. 2009.

[12] Christoforos Ntantogian, Christos Xenakis, "One-Pass EAP-AKA Authentication in 3G-WLAN Integrated Networks", Wireless Pers Commun Vol48, pp 569-584, March. 2009

[13] 강수영, 이임영, "OTP를 활용한 UICC (Universal IC Card) 기반의 인증 메커니즘에 관한 연구", 한국정보보호학회논문지. Vol.18, No 2, pp.21-31, 2008년 4월

[14] 최재덕, 정수환, "이질적인 무선 네트워크 환경에서 인증 연동을 위한 비UICC 방식의 EAP-AKA 인증", 대한전자공학회논문지, Vol46, No.5, pp. 168-177, 2009년 5월.

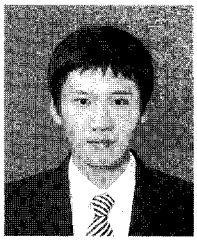
[15] "무선단말기에서의 공인인증서 저장 및 이용 기술 규격", v1.12, 한국인터넷진흥원(KISA), 2010년 3월.

[16] "무선단말기와 PC간 공인인증서 전송을 위한 기술 규격", v2.00, 한국인터넷진흥원(KISA), 2010년 3월.

[17] 강우진, "OTP 기술동향 및 센터소개", OTP 보안과 최신 인증기술 세미나, 금융보안연구원(FSA). 2010년 6월.

[18] Brian Krebs. "Citibank Phish Spoofs 2-Factor Authentication", The washington post, Security Fix, Jul. 2006 (http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_sp

〈著者紹介〉



김 태 형 (Tha-Hyung Kim) 학생회원
2004년 1월~2006년 12월 Korea Hosiden 개발품질프로젝트팀 사원(연구원)
2008년 2월: 명지대학교 전자공학과 졸업(학사)
2011년 2월: 고려대학교 정보보호대학원 금융보안전공 (공학석사)
〈관심분야〉 암호프로토콜, 모바일 OTP, 전자금융보안, 사용자 인증기술

이 준 호 (Jun-Ho Lee) 학생회원
2004년 2월: 고려대학교 전산학과 졸업(학사)
2006년 2월: 고려대학교 정보경영공학전문대학원 (공학석사)
2006년 3월~현재 고려대학교 정보경영공학전문대학원 (박사수료)
〈관심분야〉 암호프로토콜, VANET, USIM 보안, 애드 혹 네트워크, 응용암호

이 동 훈 (Dong-Hoon Lee) 종신회원
1983년 8월: 고려대학교 경제학과 졸업(학사)
1987년 12월: Oklahoma University 전산학 대학원(공학 석사)
1992년 5월: Oklahoma University 전산학 대학원(공학 박사)
1993년 3월~1997년 2월 고려대학교 전산학과 조교수
1997년 3월~2001년 2월 고려대학교 전산학과 부교수
2001년 2월~현재 고려대학교 정보보호대학원 교수
〈관심분야〉 암호프로토콜, 암호이론, USN이론, 키 교환, 익명성연구, PET 기술