Journal of the Korea Academia-Industrial cooperation Society
Vol. 13, No. 12 pp. 6071-6080, 2012

http://dx.doi.org/10.5762/KAIS.2012.13.12.6071

개인정보보호를 위한 스마트카드 기반의 익명 인증 기법

이광형[1*], 박정효[2]
[1]서일대학 인터넷정보과, [2]숭실대학교 컴퓨터학과

Anonymity Certification Technique of a Smart Card base for Personal Information Protection

Kwang-Hyoung Lee[1*] and Jeong-Hyo Park[2]
[1]Dept. Internet Information, Seoil University
[2]Dept. of Computer Science, SoongSil University

요 약 금융거래를 위한 강력한 암호화 방식인 공인인증서 방식이 최근 들어 보관상의 문제점으로 인한 피해가 우려되고 있다. 본 논문에서는 이러한 문제점의 해결책으로 사용자의 실제 개인정보를 대체한 가상의 동적아이디를 활용하여 사용자를 익명 인증하는 스마트카드 기반의 익명 인증 기법을 제안한다. 본 논문에서 제안한 익명 인증 기법은 사용자의 개인정보가 내부 유출이나 중간자 공격, 제한적 재전송 공격, 서비스 거부 공격, 전방향 안전성, 은밀한 검증자 공격 등에 대해 개인정보가 유출될 우려가 없고, 사용자의 익명성을 제공함으로써 발생할 수 있는 악의적인 공용자의 불법적인 행위를 필요 시 추적할 수 있다. 비교 분석에서 기존 스마트카드를 이용한 인증과의 실험을 통한 결과 암·복호화 효율성에서 약 10%의 성능 향상을 보였고, 안전성 측면에서 가능한 위협적 요소들에 대해 증명을 통해 안전함을 확인할 수 있었다.

Abstract Regarding the official authentication method which is a strong encrypt method for financial transactions, there has recently been a concern for the problem of storage. As a solution for such problems, this study provides the anonymous authentication method based on the smart card used for such a purpose by utilizing the pseudo ID replacing the user's personal data. Such an anonymous authentication method makes it possible to prevent any inside leakage, intermediary attack, limited re-transmission attack, service-denying attack, directional safety attack and secret inspector attack in regard to the user's personal data. As a result, there would be no concern for the leakage of any personal data. In comparative analysis, after executing the comparison and analysis process through the experiment for the authentication process by using the previously-used smart card, the new one has shown about 10% a high level of efficiency for the encrypt and decrypt process together with excellent features in terms of flexibility in regard to the user's anonymity and tracking ability.

Key Words : Authentication Method, Smart Card, Pseudo ID, Anonymous Authentication Method

1. 서론

과거의 인식과는 다르게 현재는 데이터가 화폐 이상의 가치를 갖고 있는 추세에 접어들고 있기 때문에 사용자의 개인정보에 대한 문제가 더욱 높은 관심의 대상이 되고 있다. 스마트카드를 사용하는데 있어 사용자 인증을 필요로 한다는 것은 사용자가 인증을 통해 얻을 수 있는 데이터에 대한 가치가 화폐 이상의 가치로 환산될 수 있

본 논문은 2011년도 서일대학 학술연구비에 의해 연구되었음
*Corresponding Author : Kwang-Hyoung Lee (Seoil University)
Tel: +82-2-490-7226 email: dreamace@seoil.ac.kr
Received November 9, 2012 Revised November 28, 2012 Accepted December 6, 2012

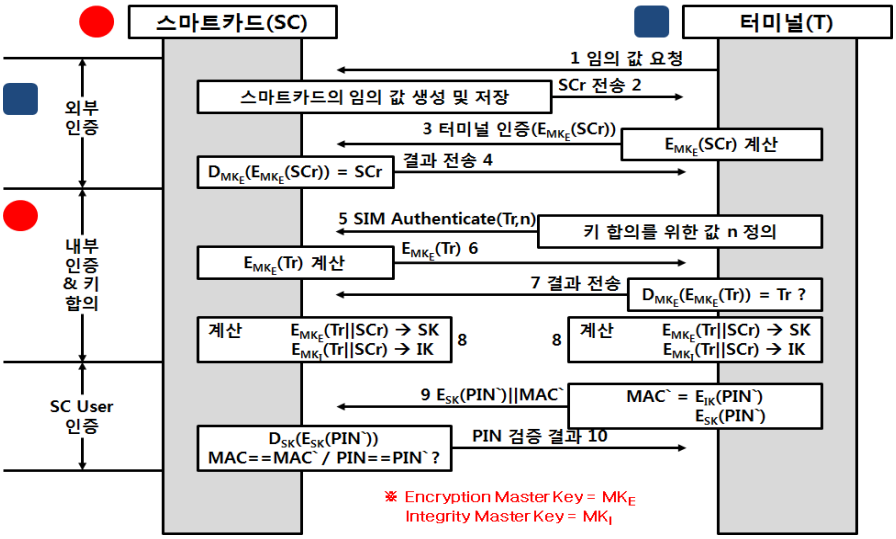
다는 것을 의미하며 최근에 이러한 부분이 집중적으로 해킹되는 이유이기도 하다[7]. 이에 따라 사용자 정보 보호는 다양한 위협에 대비할 수 있어야 하는 막중한 과제를 떠안게 되었다. 이전 해킹의 목적이 자기과시나 해커로서의 기본적인 양심을 가지는 것과는 대조적으로 최근에는 돈과 연계된 정보에 대해서 모든 수단방법을 동원하여 개인정보를 획득하고 있다. 예를 들어 2007년 1월에 개인 컴퓨터를 해킹하여 5000여 명의 공인인증서를 절취하고 국내 은행 인터넷뱅킹 사이트를 모방한 피싱 사이트를 만들어 30여 명의 주민등록번호, 계좌비밀번호, 보안카드 비밀번호 등을 절취하는 사고가 발생했다. 위의 사고사례에서 알 수 있듯이 모든 사건의 시작점에는 인증과 인가 그리고 사용자 개인에 의한 키 관리의 문제가 발생했고, 이러한 한계를 극복할 수 있는 방법론의 필요성이 대두되었다. 이에 대한 해결방법으로 공인인증서 인증 방식이 발전되었다. 하지만 금융거래를 위한 강력한 암호화 방식인 공인인증서 인증방식 조차도 최근 들어 인증서 보관의 문제점으로 인해 피해가 발생하고 있다. 또한 빈번한 사용에 따라 개인 정보의 안전한 저장 및 사용, 사용자 인증을 포함한 정보보안의 문제도 크게 부각되고 있다. 이러한 조류에 맞춰 본 논문에서는 스마트카드의 기술을 이용하여 높은 관심의 대상이 되고 있는 사용자 개인정보를 보호할 수 있는 방안을 제공한다[11.12].

본 논문의 구성은 다음과 같다. 제2장 관련연구에서는 스마트카드를 이용한 현행 인증 방식과 보안위협을 기술한다. 제3장에서는 2장에서 분석한 기존의 웹 서비스 이용 시 사용되는 인증 방식의 단점들을 고려해서 사용자의 편의성을 도모하고, 보안성을 강화하는 익명 인증 기법을 제안한다. 제4장에서는 구현을 보이고 기존 스마트카드를 이용한 인증 시스템의 보안 취약점과 보안 안전성에 대해 비교 분석을 통하여 안전성 및 효율성 평가를 기술한다. 마지막으로 제5장에서는 결론을 기술한다.

2. 관련연구

2.1 스마트카드 인증 메커니즘

스마트카드는 데이터의 저장성, 보안성 및 휴대성의 특성을 가지고 있으며, 이들 중 가장 중요한 기능은 데이터 보안성이다. 독립된 카드운영체제와 보안 메커니즘을 기반으로 연산기능을 가진 스마트카드 내부에 탑재된 마이크로프로세서를 이용하여 데이터 암호, 전자서명 등의 암호 및 데이터 접근 제한 기능을 제공함으로써 기밀성, 무결성, 부인봉쇄 및 인증 등의 보안 요구사항을 충족시켜준다. 스마트카드와 터미널 간에 데이터를 안전하게 송수신하기 위해서 요구되는 보안 요구사항 중 가장 중요한 것은 스마트카드가 터미널을 인증하는 외부인증(External Authentication), 터미널이 스마트카드를 인증하는 내부인증(Internal Authentication) 그리고 스마트카드와 터미널 간 안전한 세션키의 설정 및 사용자 인증 메커니즘으로 아래의 Fig. 1과 같은 절차로 수행된다[10,14,15].



[Fig. 1] AKA protocol between the smart card and the terminal

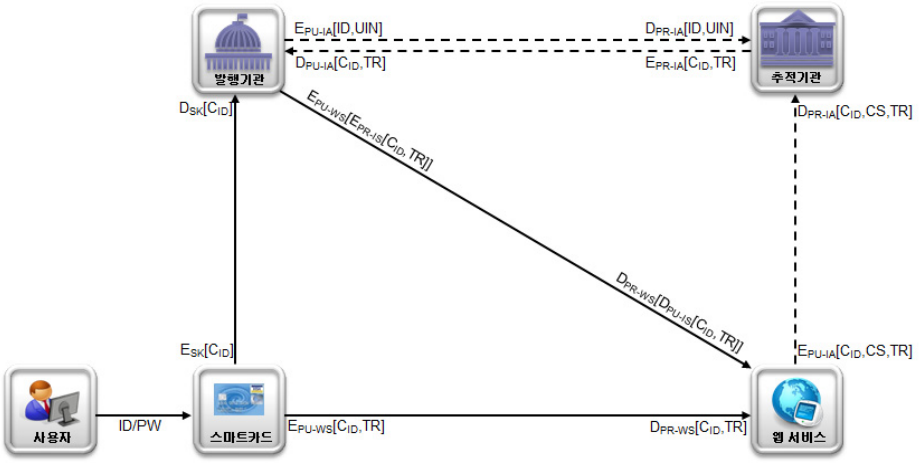
• **Step 1 (SC T)** : SC로 난수 생성을 요청한다.
• **Step 2 (SC T)** : SC 난수 SCr를 생성하여 T로 전송한다.
• **Step 3 (SC T)** : $E_{MK_E}(SCr)$을 SC로 전송한다.
① 전송 받은 SC의 난수 SCr을 T의 암호키 MK_E로 암호화한다$(E_{MK_E}(SCr))$.
• **Step 4 (SC T)** : 터미널 인증결과를 T로 전송한다.
① 전송 받은 $E_{MK_E}(SCr)$ 값을 SC의 복호키 MK_E를 사용하여 복호화한 값과 SC 자신이 소유한 SCr을 비교한다.
• **Step 5 (SC T)** : T에서 생성한 난수 Tr과 SC에서 사용될 키번호 n을 SC로 전송한다.
• **Step 6 (SC T)** : $E_{MK_E}(Tr)$을 T로 전송한다.
① 전송 받은 T의 난수 Tr을 SC의 암호키 MK_E로 암호화한다$(E_{MK_E}(Tr))$.
• **Step 7 (SC T)** : 스마트카드 인증결과를 SC로 전송한다.
① 전송받은 $E_{MK_E}(Tr)$ 값을 T의 복호키 MK_E를 사용하여 복호화한 값과 T 자신이 소유한 난수 Tr을 비교한다.
② 인증결과가 성공인 경우 전송받은 SC의 난수 SCr과 T의 난수 Tr을 연접한 후 암호 마스터키 MK_E와 인증 마스터키 MK_I로 각각 암호화하여 세션키 SK와 무결성 키 IK를 생성한다.
• **Step 8 (SC)** : 세션키 SK와 무결성 키 IK를 생성하여 키를 일치시킨다.
• **Step 9 (SC T)** : 암호화한 IIN' 정보와 IIN'에 대한 무결성 정보를 연접하여 SC로 전송한다.
① T는 IIN' 정보를 입력하여 SK 키로 암호화한다 $(E_{SK}(IIN'))$.
② T는 IIN' 정보를 IK로 암호화하여 무결성 값을 생성한다.
• **Step 10 (SC T)** : PIN 검증 결과를 T로 전송한다.
① 전송된 $E_{SK}(IIN')$ 정보를 복호화한 후, 전송된 정보에 무결성을 점검하기 위하여 IIN'에 대한 MAC 정보를 생성하여 MAC'와 비교하여 무결성을 점검한다.
② 복호화한 IIN' 정보와 SC의 EEPROM에 저장되어 있던 IIN 정보를 비교하여 사용자 인증을 수행한다.

3. 제안시스템

3.1 제안 기법의 모듈 구성

제안 기법의 모듈은 사용자 모듈, 스마트카드 모듈, 발행기관 모듈, 추적기관 모듈, 웹 서비스기관 모듈 그리고 이들을 연결해주는 인터페이스 모듈로 구성이 되어 있다. 인터페이스 모듈은 다른 모듈들의 오퍼레이션을 상속받아 사용하므로 오퍼레이션이나 속성을 따로 정의하지 않았다.

아래의 Fig. 2와 같이 제안시스템은 사용자가 익명으로 인증을 하기 위해 스마트카드에서 동적아이디를 생성하고 웹 서비스기관에 인증을 하는 과정과 불법사용자



[Fig. 2] Module configuration of the proposed system

발생 시 추적하는 두 단계로 구성되어 있다.

3.2 제안 기법의 상세 프로토콜

3.2.1 등록 프로토콜

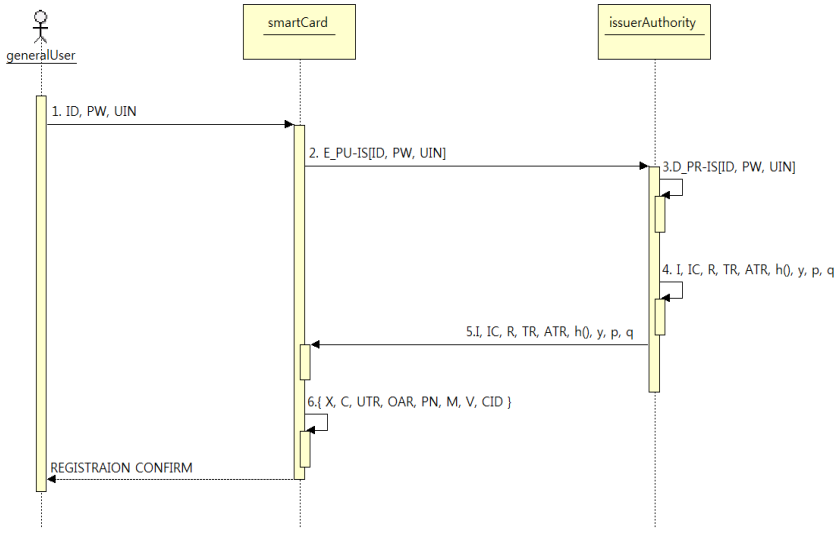
등록 프로토콜은 사용자가 스마트카드에 후발급 형태로 발행기관을 통해 어플리케이션을 다운받고 인증에 필요한 정보들을 생성 및 확인하는 단계이다. 등록 프로토콜의 시퀀스 다이어그램은 아래의 Fig. 3과 같다.

- **Step 1 (U→SC)** : 등록단계에서 사용자 인증을 위해 사용자가 스마트카드에 자신의 아이디, 패스워드, 개인정보를 입력한다.
- **Step 2 (SC→IS)** : 등록단계에서는 최초 스마트카드가 발행기관에게 사용자에게서 입력받은 아이디, 패스워드, 개인정보를 발행기관의 공개키로 암호화하여 전송한다.
- **Step 3 (IS)** : 발행기관은 스마트카드에서 받은 암호화된 정보를 자신의 개인키로 복호화한다.
- Step 4 (IS) : 발행기관은 다음과 같은 계산을 수행한다. R은 사용자의 익명성을 제공하는 동적아이디 C_{ID}값을 생성하기 위해 필요한 값이며, I와 I_C는 사용자의 아이디와 패스워드를 로그인 단계에서 빠르게 확인함으로써 효율성 증대를 위해 생성되었다. TR값은 발행기관의 공개키로 암호화된 사용자의 아이디와 사용자 정보로서 악의적인 사용자를 추적하기 위해 생성된 값이며, ATR은 정당한 사용자를 검증함과 동시에 내부 공격자의 공격을 막기 위해 사용되는 값이다. y값은 서버에 의해 선택된 비밀값으로 각 사용자의 스마트카드에 함께 저장된다.
- **Step 5 (IS)** : 발행기관은 사용자의 스마트카드에 생성된 정보를 저장하고 사용자에게 전송하여준다.
- **Step 6 (SC)** : 스마트카드는 다음과 같은 계산을 수행한다. 사용자는 스마트카드에 저장되어 있는 I와 I_C를 통해 자신의 아이디와 패스워드를 확인받은 다음, 키교환을 위해 X를 생성하고, 사용자의 익명성을 제공하기 위해 C_{ID}를 생성한다. 또한 발행기관에게 동적아이디의 무결성을 확인시켜주기 위해 C를 같이 생성한다. 또한 인증 단계에서 발행기관이 사용자 인증을 위해 필요한 값 V를 생성하고 악의적인 사용자를 추적하기 위해 필요한 TR값을 발행기관에게 안전하게 보내기 위해 UTR값을 생성한다.

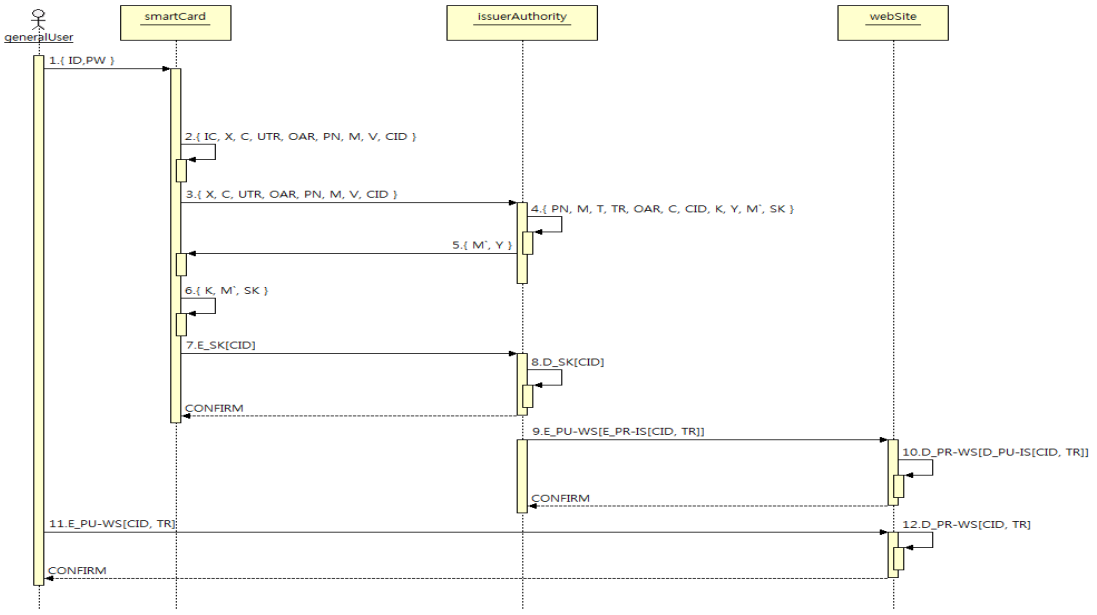
3.2.2 인증 프로토콜

인증 프로토콜은 사용자가 웹 서비스 기관을 이용하기 위해 스마트카드에서 생성한 동적아이디를 기반으로 부분익명성을 보장하는 익명 인증을 한다. 또한 부분익명성의 문제점인 불법사용자 발생 시 문제를 처리하기 위하여 추적정보를 생성하여 공유하는 작업을 한다. 인증 프로토콜의 시퀀스 다이어그램은 다음의 Fig. 4와 같다.

- **Step 1 (U→SC)** : 사용자가 웹 서비스 기관을 이용하고 스마트카드에서 사용자 인증을 하기 위해 ID, PW를 사용자가 입력한다.



[Fig. 3] Registration Protocol



[Fig. 4] Authentication Protocol

- **Step 2 (SC)** : 스마트카드는 다음과 같은 계산을 수행한다. 사용자는 스마트카드를 통해 자신의 아이디와 패스워드를 확인 받은 다음, 키 교환을 위한 값 X와 사용자 익명성을 위한 값 C_{ID}를 생성한다. V는 인증 단계에서 원격 서버의 사용자 인증을 위해 필요한 값이며 이때 사용된 값 $\{a,r,e,n\}$는 스마트카드에 의해 생성된 랜덤 값이다. UTR은 악의적인 사용자를 추적하기 위해 필요한 값 TR을 원격 서버에 안전하게 보내기 위해 생성한 값이다.
- **Step 3 (SC→IS)** : 스마트카드는 사용자의 PIN 인증 후 발행기관에 자신이 생성해낸 정보를 전송하게 된다.
- **Step 4 (IS)** : 발행기관은 스마트카드로부터 전송받은 정보의 확인 작업과 세션키 생성작업을 하게 된다. $PN ? = (n \oplus X)$, $M ? = h(e \oplus PN)$이 성립하는지 확인한다.

발행기관은 다음 계산을 통해 C_{ID}를 검증하는데 필요한 값을 얻어 낸다. 발행기관의 비밀키를 이용해 C를 생성하고 C_{ID}를 확인한다. 그 값이 서로 일치한다면 다음 계산을 통해 TR을 얻는다. 만약 C_{ID}와 식이 일치 하면 발행기관은 다음 단계를 수행한다.

- **Step 5 (IS→SC)** : 발행기관은 사용자에게 메시지 M'을 계산하여 Y와 함께 보낸다.
- **Step 6 (SC)** : 스마트카드는 메시지 M'과 Y를 받고 다음과 같은 수행을 하고 식을 확인해서 일치 하는지 확인한다. M'값이 일치 한다면 사용자와 발행기관은 SK를 이용해 다음과 같이 세션키를 생성한다.
- **Step 7 (SC→IS)** : 스마트카드는 자신이 생성해낸 세션키 SK를 이용해 C_{ID}를 AES/CBC 대칭키 암호 알고리즘을 이용해 암호화한 후 발행기관에 전송한다.
- **Step 8 (IS)** : 발행기관은 스마트카드에게서 받은 정보를 자신이 생성해낸 SK를 가지고 복호화해서 이전에 만든 C_{ID}값과 비교하여 확인한다.
- **Step 9 (IS→WS)** : 발행기관은 사용자의 스마트카드에서 생성해낸 C_{ID}를 보장하기 위해 자신의 개인키로 서명하고 웹 서비스 기관의 공개키로 암호화하여 전송한다.
- **Step 10 (WS)** : 웹 서비스 기관은 발행기관에서 보낸 암호화된 정보를 자신의 개인키로 복호화하여 서명된 정보를 확인한다.
- **Step 11 (U→WS)** : 사용자는 자신의 동적아이디가 검증된 것을 확인 후 웹 서비스를 사용하기 위해 웹 서비스 기관의 공개키로 자신의 동적아이디와 추적 정보를 암호화하여 전송한다.
- **Step 12 (WS)** : 웹 서비스 기관은 사용자로부터 받은 암호화된 정보를 자신의 개인키로 복호화한다. 발행기관은 스마트카드로부터 받은 $\{X, C, UTR,$

$OAR, PN, M, V, CID\}$ 메시지를 이용하여 C_{ID} 검증에 필요한 값을 얻어낸다. 이때 OAR값은 서버의 개인키 x를 이용하여 생성되기 때문에 오직 발행기관만이 할 수 있으며 이를 통해 내부 공격자에 대한 가장 공격에 안전하다. 또한 M'은 상호인증을 위해 발행기관에 의해 생성된 값으로 사용자의 스마트카드에 전송되어지며 SK는 사용자와 발행기관 간의 SK로서 동적아이디 C_{ID}를 스마트카드의 SK로 AES/CBC 대칭키 암호 알고리즘으로 암호화하여 발행기관에 전송하면 발행기관은 사용자로부터 받은 암호화된 정보를 자신이 생성해낸 SK로 복호화하여 검증작업을 한다.

3.2.3 추적 프로토콜

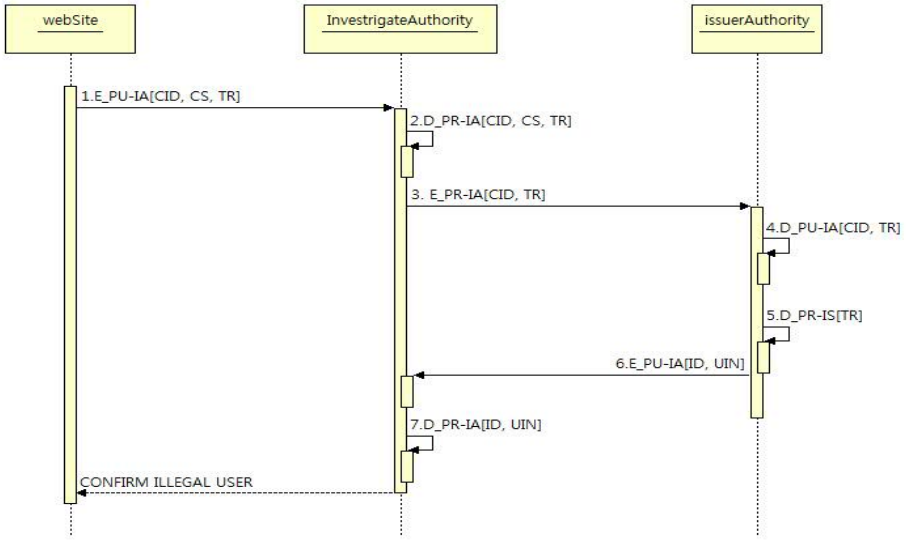
발행기관은 사용자로부터 받은 메시지 $\{X, C, UTR, OAR, PN, M, V, CID\}$ 중에서 V값을 이용하여 사용자 추적을 위해 필요한 값 $T = h(PW \oplus r)$을 얻어 낸다. 이 값은 UTR값과 XOR 연산을 통해 TR값을 얻게 되며 추적기관에 제출되는 불법 사용자에 대한 불법행위 보고서 CS와 함께 추적기관에 제출된다.

추적 프로토콜의 시퀀스 다이어그램은 Fig. 5와 같다.

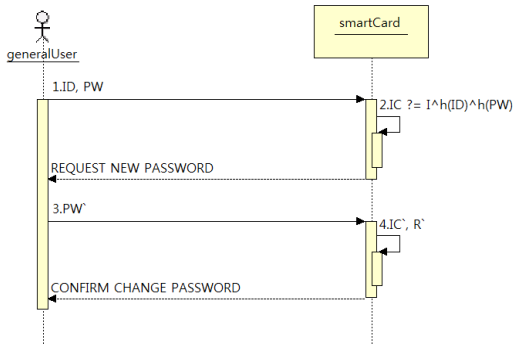
- **Step 1 (WS→IA)** : 웹 서비스 기관은 악의적인 사용자의 C_{ID}, TR과 불법행위 보고서 CS를 추적기관의 공개키로 암호화하여 제출한다.
- **Step 2 (IA)** : 추적기관은 웹 서비스 기관으로부터 전송받은 암호화된 정보를 자신의 개인키로 복호화하여 불법행위 보고서를 확인한다.
- **Step 3 (IA→IS)** : 추적기관은 C_{ID}, TR을 자신의 개인키로 서명하여 발행기관에게 전송하여 사용자 추적정보를 요청한다.
- **Step 4 (IS)** : 발행기관은 추적기관으로부터 받은 서명된 정보를 추적기관의 공개키로 서명을 검증하여 정보를 확인한다.
- **Step 5 (IS)** : 발행기관은 TR을 추적가능한 정보로 복호화하기 위해 자신의 개인키로 복호화한다.
- **Step 6 (IS→IA)** : 발행기관은 추적가능한 정보로 사용자의 원래 아이디와 개인정보를 추적기관의 공개키로 암호화하여 전송한다.
- **Step 7 (IA)** : 추적기관은 발행기관으로부터 받은 암호화된 정보를 자신의 개인키로 복호화하여 불법사용자를 추적한다.

3.2.4 패스워드 변경 프로토콜

사용자가 현재 자신의 패스워드 PW를 새로운 패스워드 PW^*로 바꾸고자 할 때, 사용자는 발행기관과는 상관없이 스마트카드만을 이용하여 새로운 패스워드 PW^*로 교체 할 수 있다. 패스워드 변경 프로토콜의 시퀀스 다이어그램은 다음의 Fig. 6과 같다.



[Fig. 5] Tracking Protocol



[Fig. 6] Password change protocol

- **Step 1 (U→SC)** : 사용자는 자신의 스마트카드를 리더기에 삽입 후, 자신의 현재 아이디와 패스워드를 입력한다.
- **Step 2 (SC)** : 스마트카드는 IC값을 확인한다.
- **Step 3 (U→SC)** : 스마트카드는 IC와 R값을 비교해보고 확인이 끝난 후 자신의 새로운 패스워드를 입력한다.
- **Step 4 (SC)** : 만약 값이 일치하면 스마트카드는 다음과 같은 수행을 하여 패스워드를 교체한다.
- **Step 5 (SC)** : 스마트카드는 새롭게 생성된 IC^*와 R^*값을 저장한다.

사용자의 패스워드 변경은 IC와 R값을 단지 IC^*와 R^*값으로 변경하는 것뿐 아니라 이후에 동적아이디 C_{ID}값을 생성하는데 영향을 주며 사용자의 패스워드 변경이 어플리케이션을 발급할 때 생성해준 값들과는 별도로 사용자와 스마트카드 안에서만 처리되기 때문에 선발급형 형태의 스마트카드 어플리케이션보다 보안성이 뛰어나다고 할 수 있다. 또한 사용자는 자신의 아이디와 패스워드를 마음대로 변경할 수 있으므로 사용자의 편의성 또한 뛰어나다.

4. 성능분석

4.1 비교분석

현재 타 사에서 사용되고 있는 스마트카드 인증 기법은 공인인증서를 기반으로 한 인증 기법으로서 인증서의 보관문제와 사용자의 익명성이 보장되지 않는 문제점을 갖고 있었다. 아래의 Table 1은 기존 시스템과의 하드웨어 비교분석을 보인다.

4.1.1 효율성 비교분석

기존 시스템들과 제안 시스템의 효율성을 비교 분석하기 위해 클라이언트의 어플리케이션, 발행기관의 서버, 웹 서비스 기관 서버 사이의 총 처리량을 트랜잭션 당 처리시간으로 비교 분석하였다. 비교 분석 결과는 각각의 모듈에서 연산된 결과를 메쉬 구조로 중간에 위치한 테스트 서버의 화면에 결과물만 모아서 확인하는 작업으로 진행되었다. 클라이언트, 발행기관 서버, 웹 서비스기관 서버, 테스트 서버 모두 동일한 하드웨어 조건에서 실행하였고

[Table 1] Comparative analysis of the existing system

	A社	B社	C社	제안시스템
MCU	8bits CPU	8bits CPU	8bits CPU	8bits CPU
ROM size	390 Kbytes	240 Kbytes	300 Kbytes	160 Kbytes
RAM size	6 Kbytes	7 Kbytes	6 Kbytes	4 Kbytes
EEPROM size	80 Kbytes	72 Kbytes	34 Kbytes	72 Kbytes
Crypto	SEED, RSA	DES, RSA	3-DES, RSA	AES, RSA
Inter face	ISO 7816 ISO 14443 TypeB	ISO 7816 ISO 14443 TypeA / Mifare 1K	ISO 7816	ISO 7816 ISO 14443 TypeB
Application	VSDC 현금IC 금융IC T-Money Hi-Pass 공인인증서	VSDC 현금IC 금융IC T-Money 공인인증서	VSDC 현금IC 공인인증서	VSDC 현금IC 금융IC T-Money Hi-Pass 공인인증서

[Table 2] per processing time of the transaction

	A社	B社	C社	제안기법
1T	0.621	0.569	0.655	0.537
10T	3.515	3.505	3.571	3.474
100T	34.883	33.161	35.741	32.719
200T	84.804	84.428	88.659	84.112
300T	170.703	156.218	178.407	155.423
400T	249.073	223.625	253.033	216.134
500T	360.425	359.531	369.173	331.389
600T	493.728	468.716	502.839	451.768
700T	645.356	619.574	674.513	597.524
800T	818.541	785.461	852.847	731.938
900T	1012.428	1006.841	1095.095	972.014
1000T	1278.194	1174.806	1283.895	1120.394

각각의 측정시간 또한 분석하여 결과를 만들었다. 테스트 서버에서의 처리시간을 위의 Table 2에 작성하였다.

Table 2와 같이 트랜잭션을 1회 시행하였을 때부터 1000번 시행하였을 때까지의 시간을 측정하였다.

하지만 현재 완벽한 익명인증을 제공하는 시스템이 없으므로 약간의 비교 오류가 있을 수 있다

4.1.2 안전성 비교분석

(1) 패스워드 추측 공격

사용자 익명성이 보장되는 프로토콜에서는 ID와 PW가 추측공격의 대상이 된다. 제안한 익명 인증 프로토콜에서 ID와 PW는 발행기관의 공개키로 암호화되어서 전송되므로 PW에 관한 정보는 오직 V, UTR, OAR 값을 통해서만 추측할 수 있다. 그러나 V, UTR, OAR 값은 다음과 같은 연산을 포함하고 있다. $V= h(M \oplus y) \oplus h(PW \oplus r)$, $UTR= h(PW \oplus r) \oplus TR$, $OAR= h(PW \oplus r) \oplus ATR$로 암호학적 해시함수의 일방향성과 난수의 예측불가능성에 의존하고 있으므로 PW를 추측하기 어렵다.

(2) 사용자 가장 공격

제안된 인증 프로토콜은 외부·내부 공격자에 의한 가장 공격에 안전하다. 외부 공격자가 정당한 사용자의 아이디와 패스워드를 얻었다고 가정하였을 때, 정당한 로그인 정보를 위조하기 위해서는 V값 안에 포함된 비밀값 y를 알아야 $h(M \oplus y)$를 만들 수 있다. 하지만 공격자는 서버의 비밀값 y를 알지 못하기 때문에 정당한 사용자인척 가장할 수 없다. 내부 공격자일 경우 $h(x)$를 얻어도 TR값과 서버의 비밀키 x로 이루어진 OAR값을 생성할 수 없기 때문에 C_{ID}를 구성할 수 없다. 또한 상호 인증을 위해 생성된 M값에 OAR값이 포함되어 있어서 내부 공격자에 의한 가장 공격은 불가능하다.

(3) 제한된 재전송 공격

제안된 인증 프로토콜에서 발행기관은 임의값 PN의 재료로 X을 이용하여 특정 시간 안에서의 새로운 메시지임을 확인할 수 있다. 따라서 제안된 프로토콜은 재생공격에 안전하다. 또한 M과 V값을 생성할 때 스마트카드에 의해 생성된 임의값이 사용된다. 이 값들은 매번 사용자가 인증을 요청할 때마다 바뀌므로 제안된 기법은 제한된 재전송 공격에 안전하다.

(4) 전방향 안전성

공격자가 사용자의 K나 PW를 알아냈다 하더라도 이전에 사용자가 사용했던 어떠한 SK도 알 수 없을 경우, 프로토콜이 전방향 안전성을 만족한다고 한다. 공격자가 사용자의 PW를 제안한 익명 인증 프로토콜에서는 등록단계와 인증단계에서는 사용자의 PW에 관한 정보를 독단적으로 다루지 않고 $h(PW \oplus r)$로 사용하기 때문에 등록단계와 인증단계에는 영향을 주지 않는다. 따라서 이전에 사용됐던 어떠한 SK도 얻어낼 수 없으며 공격자가 사용자의 ID를 안다고 해도 공격자는 발행기관의 임의값 y와 발행기관의 비밀키 x를 모르기 때문에 어떤 SK도 알 수 없다. 그러므로 제안시스템은 전방향 안전성을 만족한다고 할 수 있다.

(5) 서비스 거부 공격

제안한 익명 인증 기법에서는 타임스탬프 대신 임의값을 사용하여 메시지의 정당성을 확인하는 방식을 사용하므로 타임스탬프를 이용한 서비스 거부 공격에 안전하다. 즉, 연속적인 메시지 재전송 공격이 오더라도 시간에 대한 검사를 하지 않으므로 한번 접속을 시도한 합법적인 사용자가 서비스를 받지 못하는 경우는 발생하지 않는다. 그러므로 서비스 거부 공격에 안전하다.

5. 결론

본 논문에서는 패스워드 파일이나 확인 테이블 사용을 완전히 버린 새로운 스마트카드를 이용한 익명 인증 프로토콜로서 공인인증서는 필요시에만 사용하여 스마트카드 세션키의 안전한 생성과 분배 그리고 사용자의 익명성에 대한 연구를 하였다.

세션키의 안전한 분배를 위한 방법으로 스마트카드와 발행기관 각각의 비밀키를 이용한 키시드를 만들어 교환함으로서 직접적인 비밀키의 유추를 막고 키시드의 연산만으로 비밀키에 대한 검증 및 확인이 가능하고 세션키의 생성은 키시드를 바탕으로 각각 연산하여 생성하므로 중간에서 키시드를 획득한 공격자는 세션키를 생성할 수 없고 오직 스마트카드와 발행기관만이 세션키를 생성해 낼 수 있다. 사용자의 부분적인 익명성을 보장하기 위한 방법으로 스마트카드에서 일회성으로 생성해낸 동적아이디를 발행기관의 검증을 거치고 자신이 발행한 스마트카드 확인절차를 거쳐 웹 서비스 기관에 인증을 해주기 때문에 사용자는 스마트카드의 동적아이디를 가지고 웹 서비스를 받게 된다. 이는 인터넷이 우리 생활에 가져다주는 편리함과 즐거움 이면에 인터넷을 사용함으로서 우리가 원하지 않은 방법으로 많은 개인정보들이 노출되는 것을 막아주고, 정당한 범위 내에서, 즉 다른 사람에게 피해를 주지 않는 범위 내에서 개인의 신분을 드러내지 않은 채 인터넷을 이용할 수 있게 해준다. 하지만 이러한 사용자 익명성의 문제는 불법적인 사용자들의 위법적인 행위를 야기할 수도 있다. 이러한 문제점을 해결하기 위해 추적 가능한 동적아이디로 원래 사용자의 정보를 추적할 수 있는 기능도 있다. 현재 이러한 시도의 일환으로 사용자에 대한 익명 인증 기법에 관한 연구가 활발히 진행되고 있고, 실생활에 적용할 수 있을 만큼 충분히 실용적인 디지털 서명 방법들이 제안되고 있다. 하지만 디지털 인증서를 사용함은 완벽한 익명 인증뿐만 아니라 개인정보의 유출문제도 아직 해결하지 못한 실정이다. 본 논문에서는 이러한 취약점들을 파악하여 근본적으로 해결하였다.

향후에는 본 논문에서 제안한 스마트카드 기반의 익명 인증 프로토콜과 현행 사용 중인 스마트카드를 이용한 공인인증서를 적절히 사용하여 완전한 익명성과 사용자 인증 그리고 불법적인 사용자 추적을 가능하게 하는 기법을 각 응용분야별로 즉, 스마트카드를 활용한 전자지불 시스템, 전자화폐, 모바일 결제 카드 등을 위한 연구가 지속적으로 요구된다. 또한 응용분야 뿐만 아니라 익명 인증 기법을 필요로 하는 다른 분야에도 적용이 되어야 할 것이다.

References

[1] Ki-young Kim, “A one-time password-based authentication system for Consideration”, proceeding of KIISC, Vol.17 No.3, pp.26-31, 2007.

[2] Yi-Roo Baek, Doo-Hwan Oh, Kwang-Eun Gil and Jae-Cheol Ha1, “Implementation of a Remote Authentication System Using Smartcards to Guarantee User Anonymity to Third Party”, Journal of KAIS, v.12, no.5, pp.2322-2326, 2011.

[3] Wang-Seong Park, Jong-Pil Jung, Chang-Sub Park, Dong-Hoon Lee, “Password authentication protocol for Consideration”, proceeding of KIISC, Vol.9 No.4, pp.51-63, 1999.

[4] Cheol-Oh Kang, Joong0Gil Park, Soon-Jwa Hong, Byung-Cheol Bae, “A Study on the Algorithm of Improved One-Time Password using Time and Time Correction”, The KIPS Transactions : Part 8-C No.4, pp.373-378, 2001.

[5] Je-Ho Song, “Design of Inner Key scheduler block for Smart Card”, Journal of KAIS, v.11, no.12, pp.4962-4967, 2011.

[6] Je-Ho Song, Woochoun Lee, “The Design of Hybr id Cryptosystem for Smart Card”, Journal of KAIS, v.12, no.5, pp. 232-2326, 2011.

[7] Sung-Woon Lee, Hyun-Sung Kim, Kee-Young Yoo, “A Password - based Efficient Key Exchange Protocol”, Journal of KIISE : Information Networking Vol.31 No.4, pp.347-352, 2004.

[8] Dong-Hyun Choi, Seung-Joo Kim, Dong-Ho Won, “One-time password Technical Analysis and Standardization”, proceeding of KIISC, Vol.17 No.3, pp.12-17, 2007.

[9] Eun-Jeong Choi, Chan-Oe Kim, Joo-Seok Song, “Password-Based Authentication Protocol for Remote

Access using Public Key Cryptography", Journal of KIISE : Information Networking, Vol.30 No.1, pp.75-83, 2003.

[10] Jong-Seok Choi, Seung-Soo Shin, Kun-Hee Han, "Three-Party Key Exchange Protocol Providing Usser Anonymity based on Smartcards", Journal of KAIS, v.10, no.2, pp.388-395, 2009.

[11] J.Lv and Y.Han, "Enhanced DES Implementation Secure Against High-Order Differential Power Analysis in Smartcards", ACISP 2005, LNCS 3502, pp.195-206, 2005, Article(CrossRefLink)

[12] J.R.Rao, P.Rohatgi and H. Scherzer, "Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards". IBM Watson Research Center, in 2002 IEEE Symposium on Security and Privacy, Oakland, CA, May 2002, Article(CrossRefLink)

[13] L.Goublin and J.Patarin, "DES and differential power analysis", in proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Springer-Verlag, 1999.

[14] T.S.Messerges, E.A.Dabish and R.H.Sloan, "Investigation of Power Analysis Attacks on Smartcards", in Proceedings of USENIX workshop on Smartcard Technology, pp.151-161, May 1999.

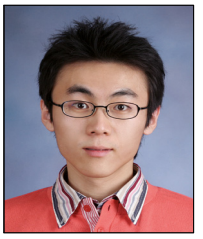
[15] Y.S.Son and D.H.Lee, "The Key Management System using the Secret Sharing Scheme Applicable to Smart Card", KIPS Transaction, VOL.11-C, NO 5, pp.373-378, 2004.

이 광 형(Kwang-Hyoung Lee) **[종신회원]**

- 1998년 2월 : 광주대학교 컴퓨터공학과 졸업(공학사)
- 2002년 2월 : 숭실대학교 컴퓨터공학과 (공학석사)
- 2005년 2원 : 숭실대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학 인터넷정보과 부교수

<관심분야>
멀티미디어 데이터 검색, 영상처리, 멀티미디어 보안, DRM, USN, 학습콘텐츠

박 정 효(Jeong-Hyo Park) **[정회원]**



- 2009년 2월 : 숭실대학교 컴퓨터학과 졸업(공학사)
- 2011년 2월 : 숭실대학교 일반대학원 정보보안(정보보안석사)
- 2011년 3월 ~ 현재 : 숭실대학교 일반대학원 컴퓨터공학과 (박사과정)

<관심분야>
정보통신, 통신보안, 암호이론