논문 2011-48TC-2-16

효율적이고 안전한 스마트카드 기반 사용자 인증 시스템 연구

(A Study on Efficient and Secure user Authentication System based on Smart-card)

변 진 욱*

(Jin Wook Byun)

요 약

사용자 인증은 정보보안 시스템 구축 시 반드시 필수적인 핵심 기술이다. 사용자들은 인증과정을 통해 데이터베이스에 있는 자원에 접근하고 안전하게 사용할 수 있다. 사용자가 소지하는 스마트카드는 그 사용의 편리성과 대중성으로 인해 현재 중요한 인증 수단으로 각광받고 있다. 더욱이 스마트카드는 계산을 위한 저장 공간과 연산력을 확보하고 있기 때문에 효율적이고 안전한 사용자에 널리 사용될 수 있는 장점을 지니고 있다. 1981년, 램포트는 처음으로 사용자의 스마트카드를 이용해서 인증 통신 프로토콜을 설계했다. 하지만, 암호학적으로 안전한 해시함수가 체인으로 여러 번 적용됨으로 인해 높은 비용을 초래한다는 점과 이러한 해쉬 정보들이 서버에 저장되어야하므로 이와 관련한 공격 가능성들이 비판의 대상이 되었다. 이후 안전하고 효율적인 인증 통신 프로토콜 설계에 대한 연구가 활발히 진행되고 있다. 아주 최근에, Xu, Zhu, Feng 등은 증명가능하고 안전한 스마트카드 인증 프로토콜을 제안했다. 본 논문에서는 스마트카드 기반 인증 프로토콜에서 발생할 수 있는 가능한 취약점 및 공격들을 정의한다. 이를 통해, Xu, Zhu, Feng이 제안한 프로토콜이 서버의 비밀 값들을 획득한 공격자가 사용자의 비밀 값과 패스워드를 모르고도 해당 사용자를 가장 할 수 있다는 측면에서 안전하지 않다는 것을 보인다. 이에 대해 효율적이고 안전한 프로토콜을 설계하고 설계된 프로토콜의 안전성을 새롭게 분석한다.

Abstract

User authentication service is an absolutely necessary condition while securely implementing an IT service system. It allows for valid users to securely log-in the system and even to access valid resources from database. For efficiently and securely authenticating users, smart-card has been used as a popular tool because of its convenience and popularity. Furthermore the smart-card can maintain its own power for computation and storage, which makes it easier to be used in all types of authenticating environment that usually needs temporary storage and additional computation for authenticating users and server. First, in 1981, Lamport has designed an authentication service protocol based on user's smart-card. However it has been criticized in aspects of efficiency and security because it uses hash chains and the revealment of server's secret values are not considered. Over the years, many smart-card based authentication service protocol have been designed. Very recently, Xu, Zhu, Feng have suggested a provable and secure smart-card based authentication protocol. In this paper, first, we define all types of attacks in the smart-card based authentication service. According to the defined attacks, however, the protocol by Xu, Zhu, Feng is weak against an attack that an attacker with secret values of server is able to impersonate a valid user without knowing password and secret values of user. An efficient and secure countermeasure is suggested, then the security is analyzed.

Keywords : 스마트카드 인증, 사용자 인증, 패스워드 인증, 정보보안 시스템

Ⅰ. 서 론

사용자 인증 기술은 정보보안 시스템 구축 시 반드시 필수적인 핵심 요소이다. 사용자들은 인증과정을 통해 데이터베이스에 있는 자원에 접근하고 안전하게 사용할 수 있다. 일반적으로 원거리에서 사용자를 인증할 수 있는 방법에는 사용자의 암기 가능한 정보를 (예: 패스워드, PIN 번호) 이용하는 것, 사용자가 직접 소지하고 있는 스마트카드 등을 이용하는 방법, 사용자의 생체

* 정회원, 평택대학교 정보통신학과
(Department of Information and Communication, Pyeongtaek University)
접수일자: 2010년8월19일, 수정완료일: 2011년2월19일

인식 정보들을 이용하는 방법으로 분류할 수 있다. 각각의 방법에 따라 보안 프로토콜 구현 방법 및 실용화 방안, 이슈화 되는 문제들이 상이하다. 최근에는, 이러한 방법에서 더 나아가, 각기 방법들을 두 가지 이상 병합해서 사용자들에게 효율적이고 편리한 인증 서비스를 제공해주고 있다. 이러한 접근방법은 편리성과 함께 안전성을 좀 더 강화시킬 수 있다는 장점이 있기에 현재 대부분의 정보보안 서비스 시스템에 실용화되었다. 예를 들어, 사용자의 패스워드와 스마트카드를 동시에 이용해서 인증하는 방법, 사용자의 지문정보와 스마트카드를 동시에 이용하는 방법들이 그 예가 된다.

본 논문은 이러한 두 가지 요소 인증 서비스 중에서 사용자의 암기 가능한 패스워드와 스마트카드를 동시에 이용하여 인증하는 서비스에 대해서 연구한다. 패스워드는 사용자가 암기하기 편리하다는 효율성으로 인해 사용자와 서버 인증에 널리 사용되고 있다. 하지만 암기하기 편리하다는 사실은 패스워드가 선택되어지는 공간이 계산적으로 협소함을 의미하므로 공격자에게 오프라인 사전공격(dictionary attack)을 용이하게 하는 단점을 지닌다. 이러한 사전공격을 막고 사용자의 인증 정보와 관련된 비밀 정보를 저장할 수 있는 스마트카드를 이용하면 효율적이고 안전한 인증 서비스를 제공할 수 있다. 스마트카드는 대부분의 사용자들이 한 개 이상 소유하고 있으므로 대중성을 지니며, 또한 스마트카드는 자체 연산과 비밀 값들을 저장할 수 있는 메모리를 허용하기 때문에 모든 정보보안 시스템에서 사용자 인증을 위한 좋은 수단을 제공한다.

1. 관련 연구

가. 안전한 스마트카드 인증 서비스 프로토콜

1981년도에 Lamport는 처음으로 스마트카드를 이용해서 사용자를 인증할 수 있는 서비스를 제안하였다[12]. Lamport에 의한 방법은 처음이라는 점에서 중요한 의미가 있지만, 암호학적으로 안전한 해시함수가 체인으로 여러 번 적용됨으로 인해 높은 비용을 초래한다는 점과, 이 정보들이 서버에 저장되어야하므로 이와 관련한 공격 가능성이 제기되었다. 이 후 많은 개선된 프로토콜이 제안되었는데[1~5, 7, 9~14, 16~18], 그 기준은 검증자(verifier) 정보의 서버 저장 유무에 따라, 다음 두 가지로 분류될 수 있다.

검증자 정보는 사용자의 패스워드 인증을 위해 서버가 자신의 데이터베이스에 저장하는 사용자의 패스워드 관련 정보이다. 패스워드 자체가 될 수 있으며, 패스워드를 이용해서 만들 수 있는 값을 포함한다. 하지만, 검증자 정보가 공격자들에 의해 노출된다면, 인증 시스템이 부분적으로 혹은 전체적으로 안전하지 못하게 된다. 이를 방어하기 위해, 2000년에 Hwang과 Li는 Elgamal 공개키 암호화 기법을 이용해서 서버에 어떠한 사용자 관련 검증자 정보도 저장하지 않는 방법을 제안했다[7]. 하지만, 이 방법은 사용자들이 패스워드를 변경하기를 원할 때 자유롭게 변경할 수 있는 서비스를 제공하지 못했다. 더욱이 Hwang과 Li 방식은 사용자를 가장할 수 있는 공격에 취약함이 밝혀졌다[1~2, 18].

효율성을 향상시키기 위하여, Sun은 경량화된 검증자가 없는 스마트 기반 인증 서비스 프로토콜을 설계했다[14]. 하지만, 2002년도에는 Chien 등은 Sun의 방식이 단방향 인증 서비스만 제공한다고 지적하였고, 이를 개선 시켜 양방향 인증서비스가 가능한 검증자 없는 스마트 카드 인증 기법을 설계했다[3]. 하지만, Chien 등의 방법도 병행 세션 공격 (parallel session attack), 반사 공격 (reflection attack), 내부자 공격 등에 취약함이 밝혀졌다. 후에 Ku와 Chen등은 Chien등의 방법을 개선시킨 프로토콜을 제안했다[9]. 하지만, 이 프로토콜 역시, Yoon 등에 의해 병행 세션 공격과, dos(denial of service) 공격에 취약함이 밝혀졌다. Yoon 등은 이를 개선시킨 프로토콜을 제안했다[19].

위에서 살펴보았듯이, 지금까지 많은 프로토콜이 제안되었고, 제안된 프로토콜의 장점과 취약점이 각각 분석되었다. 위 프로토콜들 중 Yoon 등이 제안한 방식이 안전한 것으로 간주 되었으나, 최근에, Wang 등이 Ku와 Chen의 방식[9]과 Yoon의 방식[19]이 오프라인 패스워드 추측 공격과 위조 공격 등에 취약함을 보였다[16]. 그리고, Wang등은 이를 개선시킨 실용적이고 안전한 프로토콜을 제안하였다. 하지만, 최근에, 이 프로토콜마저

그림 1. 검증자 기반 인증 서비스 분류
Fig. 1. A classification of verifier-based authentication service.

도 가장 공격 및 오프라인 패스워드 사전 공격과 완전 순방향 비밀성(perfect forward secrecy)을 만족하지 않음이 밝혀졌다[4].

나. 증명 가능한 효율적인 스마트 카드 인증 서비스 프로토콜 연구

2009년에 Xu, Zhu, Feng들에 의해 처음으로 증명 가능한 스마트 카드 인증 서비스 연구가 수행되었다[17]. 그들은 먼저, Lee등이 제안한 인증 서비스 프로토콜이[10] 스마트카드의 정보가 공격자들에 의해 노출되었을 때 공격자가 시스템의 정당한 사용자를 가장할 수 있는 공격에 취약함을 보였다. Xu, Zhu, Feng은 스마트카드가 노출되더라도 가장 공격을 방지 할 수 있는 인증 프로토콜을 제안하였다. 무엇보다 가장 큰 공헌도는 스마트카드 인증 프로토콜 분야에서, 처음으로 공격자의 능력을 모델화 하고 공격자의 공격 이점을 계산적 가정을 이용해서 증명했다는 점이다.

2. 논문의 공헌도

Xu, Zhu, Feng의 연구결과는 스마트 카드 인증 서비스 분야에서 처음으로 공격자의 행위를 모델화했다는 점에서 의미가 있지만, 첫 시도인 만큼 안전성 모델이 완전하지 않다. 즉, 안전성 모델이 다양한 공격 시나리오를 가정하지 않고 제한된 공격 시나리오를 가정하였다. 예를 들어, 스마트카드 인증 서비스 프로토콜에는 다양한 종류의 공격이 존재하는데 모든 가능한 공격들에 대한 안전성 분석을 포함하지 않고, 오직 세션 키를 구하는 문제에 대한 안전성을 분석하였다. 이로 인해, 제안된 프로토콜은 공격자가 서버의 비밀 키를 이용한 사용자 가장 공격에 취약하다. 공격자가 서버의 비밀 정보를 획득했을 때에 서버를 가장하는 것은 현실적으로 막을 수 없다. 하지만, 공격자가 서버의 비밀 정보를 가지고 기존 사용자를 가장할 수 없도록 설계되어야 한다. 공격자가 서버의 비밀 정보를 안다고 가정한다면, 공격자가 항상 사용자들에게 새로운 스마트카드를 발급할 수 있는 가능성은 있다. 하지만, 이러한 카드 발급의 대상은 어디까지나 새로운 사용자들이며, 기존의 사용자들에게는 어떠한 안전성 문제도 야기 시키면 안 된다. 예를 들어, 서버의 비밀 키가 도난당했을 때, 도난당한 사실을 즉시 알고 이에 대해 전체 시스템을 중지하고 스마트카드를 새롭게 발급 할 수 있다면 이상적인 시스템일 것이다. 하지만, 도난 사실을 조금이라도 늦게 안다면, 그 시간 동안 공격자는 기존 사용자들을 가장해서 온라인 금전 거래 및 기타 부정행위를 할 수 있게 되며 이로 인한 경제적 손실은 크다. 그러므로 기존에 등록되어 있는 사용자들에 대해서 공격자가 서버의 비밀 정보를 획득한다 하더라도 이를 이용해 기존의 사용자를 가장 할 수 없게 설계되어야 함은 자명하다.

본 논문에서는 이러한 공격의 가능성을 제시하고 그 해결방안에 대해서 논의한다. 이와 더불어 스마트카드 인증 서비스 프로토콜에 가능한 모든 공격들을 조사하고 정의한다. 정의된 공격을 이용해서, Xu, Zhu, Feng 등이 제안한 스마트카드 인증 서비스 프로토콜의 안전성을 검증하고 분석한다. 이를 방어 할 수 있는 스마트카드 인증 서비스 프로토콜도 제안하고, 그 안전성에 대해서도 논한다.

Ⅱ. 스마트카드 인증 서비스 구조

스마트카드 인증 서비스는 스마트카드, 리더기, 서버, 세 개의 구성요소가 존재한다. 스마트카드는 서버에 의해 발급되고, 사용자는 스마트카드를 소지하고 있어야 하며 또한 자신의 패스워드를 반드시 기억하고 있어야 한다. 구체적인 인증 서비스는 그림 2와 같이, 스마트카드 등록단계 (registration phase), 사용자 로그 인 단계 (login phase), 사용자 인증 단계 (authentication phase)로 구성된다.

1. 인증 서비스 절차

스마트카드 등록단계는 서버가 사용자들에게 스마트카드를 발급하는 단계이며, 스마트카드에는 사용자 인증 관련 정보가 저장되어 서버에 의해 발급된다. 로그인 단계에는 사용자가 자신의 스마트카드를 리더기에 집어넣고 자신의 ID와 패스워드를 입력한다. 그 후, 인증 단계를 통해 서버가 사용자에게 발급한 스마트카드가 맞는지를 인증하게 되고, 서버와 사용자간에 공통의 세션 키를 공유하게 된다. 공유된 세션 키는 이후 서버로 부터의 다양한 서비스를 안전하게 받기 위한 암호화, 인증용 키로 사용된다.

스마트카드 인증 서비스에서 안전하다의 의미는 무엇보다 그림 2의 3번 인증과정에 있다. 즉, 3번 단계의 인증 과정에서 오직 사용자의 패스워드와 서버에 의해서 발급된 정당한 스마트카드를 둘 다 소지하고 있는 사람만이 통과할 수 있게 설계되어야 안전한 인증 프로

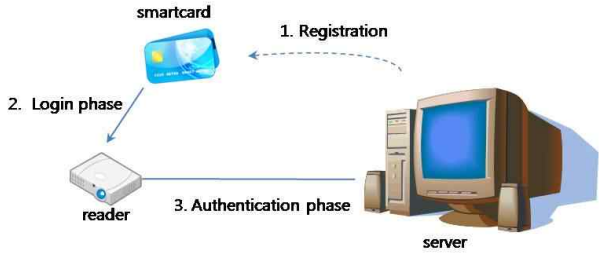

그림 2. 스마트카드 인증 서비스 절차
Fig. 2. A process of smartcard-based authentication service.

토콜이다. 예를 들어, 스마트카드와 패스워드를 모르는 사용자가 해당 사용자를 가장하거나 혹은 정당한 사용자와 서버에 의해 만들어지는 세션 키에 대한 정보를 알 수 있으면 안전하지 않다. 요약하면, 패스워드와 스마트카드를 소유한 사람만이 서버와 공통의 세션 키를 공유할 수 있게 설계되어야 한다. 스마트카드 인증 서비스에서 발생할 수 있는 공통된 취약점들을 아래에 분석하였다.

2. 스마트카드 인증 서비스의 취약점 분석

가. 발급 단계의 취약점

1번의 발급 단계는 오프라인에서 안전하게 이루어지므로 서버를 가장할 수 없다. 하지만, 서버의 인증정보가 저장된 데이터베이스가 노출된다면, 공격자는 그 정보를 이용해 누구나 서버를 가장할 수 있게 되고 사용자들에게 스마트카드를 정당하게 발급할 수 있게 된다. 이렇게 서버가 공격당해서 인증정보가 포함된 데이터베이스가 노출되었을 경우, 공격자의 서버 가장 공격 및 스마트카드의 발급을 방어할 수 있는 기술적 방법은 없다. 하지만, 그 공격자가 기존의 다른 사용자들을 가장할 수는 없어야 한다. 즉, 공격자가 취득한 데이터베이스의 인증 관련 정보들을 이용해서, 기존의 사용자를 가장할 수 없게 프로토콜이 설계되어야 한다.

나. 인증 단계의 취약점

인증 단계에는 많은 공격형태가 존재한다. 프로토콜의 결함으로 인해 사용자 및 서버를 가장 할 수 있고, 합의 되는 세션 키를 인증 정보 없이 구할 수도 있다. 또한, 프로토콜을 통해 전달되는 메시지들을 기록, 이용해서, 역으로 사용자의 패스워드를 유추해 볼 수 있다. 대부분 스마트카드 인증 프로토콜의 공격은 인증 단계의 프로토콜에서 발생한다.

다. 스마트카드 인증 서비스 프로토콜의 가정

스마트카드 인증 서비스 프로토콜을 설계할 때 가정의 범위에 따라 프로토콜 설계 어려움의 정도도 달라진다. 스마트카드 인증 프로토콜에서 보편적으로 사용되는 가정들은 다음과 같다.

[가정 1] 스마트카드 등록단계에는 서버가 안전하게 카드를 발급할 수 있다고 가정한다.

[가정 2] 서버의 데이터베이스에 저장된 서버의 개인키가 공격자에게 노출되면, 공격자가 서버를 가장하거나 혹은 공격자가 이후 사용자들에게 스마트카드를 정당하게 발급하는 것을 막을 수 없다.

본 논문에서의 발급되는 스마트카드는 변형 억제 모듈 (TRM: tamper resistant module)을 탑재했다고 가정한다. TRM 모듈은 중요 콘텐츠 암호 키나 복호화된 콘텐츠가 노출될 수 없도록 마치 블랙박스와 같이 세부 동작 과정이 드러나지 않고, 변형을 가하면 동작하지 않도록 제작된 소프트웨어 또는 하드웨어 모듈을 의미한다. 하지만, 스마트카드 위조 방지인, TRM 모듈을 사용하더라도 차분전력공격방법(DPA: differential power attack)에 의해 암호화 키 및 비밀정보를 유출할 수 있다[8].

[가정 3] 비록 스마트카드의 핵심 모듈이 TRM 방법으로 설계된다 하더라도, 핵심 모듈에 저장된 정보가 전력 분석방법으로 인해 공격자에게 노출될 수 있다. 그러므로 공격자가 스마트카드를 획득하는 것은 스마트카드 내의 인증정보를 획득하는 것을 의미한다.

사용자가 소지하고 있는 스마트카드와 해당 패스워드를 공격자가 둘 다 획득 했을 경우에 그 공격자가 사용자를 가장하는 것을 막을 수 있는 기술적 대안은 없다. 또한 스마트카드와 서버의 비밀 정보가 공격자에게 노출된다면, 그 공격자는 스마트카드 내에 저장된 인증정보를 전력분석방법으로 알 수 있고 이 정보들과 서버의 비밀정보를 이용해서 사용자의 패스워드를 사전공격을 통해 쉽게 알 수 있다. 이는 곧 스마트카드와 패스워드를 둘 다 알게 되는 것이므로 공격자의 사용자 가장

을 막을 수 없게 된다. 그러므로 서버의 비밀 정보와 스마트카드 둘 다 동시에 유출되지 않도록 해야 한다.

[가정 4] 사용자의 스마트카드와 해당하는 패스워드 혹은 스마트카드와 서버의 비밀 정보가 공격자에게 노출되었을 때, 공격자가 해당 사용자를 가장하는 것을 막을 수 없다.

Ⅲ. 스마트카드 인증 서비스 프로토콜의 알려진 공격 방법

본 장에서는 현재까지 알려진 스마트카드 기반 인증 프로토콜에서 발생할 수 있는 모든 공격들을 분류하면 다음과 같다.

1. 알려진 공격 방법

가. 가장 공격 (impersonation attack)

논문에서 언급되는 가장 공격은 그림 2]의 인증단계에서 발생하는 공격이며, 가장하기 위한 대상은 사용자와 서버이다. 공격자가 사용자 및 서버의 비밀 정보를 모르고도 인증단계에서 전달되는 메시지들을 이용해서 사용자 혹은 서버를 가장할 수 있으면, 가장 공격에 성공했다고 정의한다. 크게 다음의 세 가지의 경우로 분류한다.

- 사용자 가장 공격 : 공격자가 스마트카드 내의 인증정보 및 서버 데이터베이스 인증정보를 획득하는 여부에 따라 다음 세 가지의 경우로 나눈다. 첫째, 공격자가 사용자의 패스워드의 정보를 모르고도, 사용자를 인증단계 프로토콜에서 가장하는 경우이다. 이러한 경우는 공격자가 프로토콜의 결점을 파악하고, 프로토콜 메시지들을 병행적으로 이용하거나 (parallel session attack), 재 사용해서 (reflection attack) 궁극적으로 사용자들을 가장 하는 것이 목적이다. 둘째, 공격자가 사용자의 스마트카드를 획득 한 후, 차분전력공격을 통해 스마트카드 내 인증정보를 노출할 수 있고, 그 정보들만을 통해 인증단계의 프로토콜에서 사용자를 가장 하는데 성공하는 경우이다. 세 번째는 공격자가 서버의 데이터베이스 인증정보를 획득한 후 그 정보들을 통해 인증단계의 프로토콜에서 사용자를 가장 하는데 성공하는 경우이다.
- 서버 가장 공격 : 서버 가장 공격은 스마트카드 인증정보 획득 여부에 의해 다음 두 가지로 나눈다. 첫째, 공격자가 인증단계 프로토콜에서 프로토콜의 취약점을 이용해서 서버를 가장 할 수 있는 경우이고, 둘째는 사용자의 스마트카드로부터 인증정보를 획득한 후 서버를 가장하는 경우이다. 위에서 언급한 가정 2에 의해서 서버의 비밀키가 공격자에게 노출되었을 때에 서버를 가장하는 경우는 고려하지 않는다.

나. 오프라인 패스워드 사전 공격

오프라인 패스워드 사전 공격은 인증단계에서 발생하는 공격으로서, 패스워드 인증 분야에서 가장 잘 알려진 공격이다. 즉, 공격자는 인증단계에 사용되었던 메시지들을 이용해서 사용자의 패스워드를 오프라인에서 반복 추측하여 해당 패스워드를 궁극적으로 알아내는 공격이다. 패스워드 사전 공격은 다음의 두 경우로 나누어 정의된다.

- 인증 단계에 수행되는 프로토콜의 메시지들을 통해 오프라인 패스워드 추측 공격을 수행하는 경우
- 사용자의 스마트카드가 노출되었을 때, 공격자가 차분전력공격을 통해 스마트카드 내 인증정보를 노출하고 그 정보들을 통해 오프라인 패스워드 추측 공격을 수행하는 경우

다. 완전 순방향 비밀성

완전 순방향 비밀성 (perfect forward secrecy)은 사용자의 패스워드와 서버의 비밀 키 들이 공격자에게 노출되었을 때에, 공격자는 그 값들을 이용해서 이전 혹은 이후에 만들어진 세션 키를 계산할 수 없어야 하는 성질이다. 대부분의 프로토콜이 완전 순방향 비밀성을 만족시키기 위해서 계산적으로 어려운 문제(예: Diffie-Hellman 문제)를 바탕으로 세션 키를 설계한다.

Ⅳ. 기존 프로토콜 취약점 분석

본 장에서는 Xu, Zhu, Feng등이 제안한 인증 서비스 프로토콜을 살펴보고 취약점을 분석한다.

1. Xu, Zhu, Feng 프로토콜

가. 사용자 등록

서버는 $p=2q+1$를 만족하는 큰 소수 p, q를 선택한다. 또한 서버는 자신의 개인키 $x \in Z_q^*$와 일 방향 해시 함수, $h(): \{0,1\}^* \rightarrow Z_q^*$ 를 선택한 후 다음 과정을 수행한다.

(1) 사용자는 자신의 ID와 패스워드 PW를 선택한 후 서버에게 (ID, PW)를 안전한 채널을 통해 전달한다.
(2) 서버는 (ID, PW)를 받은 후에 자신의 개인키 x를 이용하여 B값을 다음과 같이 계산한다.

$$B = h(ID)^x + h(PW) \bmod p$$

(3) 서버는 스마트카드에 (ID, B, $h()$, p, q)를 저장하고 해당 사용자에게 발급한다.

나. 로그인 단계

사용자는 발급받은 스마트카드를 리더기에 집어넣고 자신의 ID와 패스워드, PW를 입력한다. 스마트카드는 다음의 과정을 수행한다.

(1) 먼저 랜덤 값 $w \in Z_q^*$를 선택하고 현재시각 T를 설정한다.
(2) B', W, 그리고 C를 다음과 같이 계산한다.

$$B' = (B - h(PW))^w \bmod p$$
$$W = h(ID)^w$$
$$C = h(T \| B' \| W \| ID)$$

(3) 메시지 (ID, C, W, T)를 서버에게 전달한다.

다. 인증 단계

스마트카드와 서버는 다음의 프로토콜을 통해 상호 인증을 수행한다.

(1) 서버는 메시지 (ID, C, W, T)를 받은 후, 먼저 ID가 자신이 발급한 ID인지 검증한다. 자신이 발급한 ID가 아니면, 사용자의 로그인 요구를 거절하고, 인증단계는 실패한다. 서버는 메시지를 받은 시간 T'에 대해서 T와 T'의 시간차가 미리 정해진 유효 시간 범위 안에 있는지도 검증한다. 또한, 서버는 $B'' = W^x$를 계산하고 받은 메시지 C 값이 $h(T \| B'' \| W \| ID)$인지 검증한다. 그렇지 않으면, 사용자의 로그인 요구를 거절하고, 인증단계도 실패한다. 서버는 랜덤 값 $m \in Z_q^*$을 선택하고, T''를 현재시간으로 설정한다. $M = h(ID)^m$를 계산하고, 이를 이용하여 $C' = h(M \| B'' \| T'' \| ID)$도 계산하고, ($ID$, C', M, T'')를 사용자에게 전달한다.
(2) 사용자는 메시지를 받은 후 ID와 T''를 검증하고, C'이 $h(M \| B'' \| T'' \| ID)$와 동일한지 검사한다. 모두 맞으면, 사용자는 서버를 인증하게 된다. 사용자와 서버는 공통의 세션 키를 다음과 같이 계산한다.

$$sk = h(ID \| M \| W \| M^w) = h(ID \| M \| W \| W^m)$$

2. Xu, Zhu, Feng 프로토콜 안전성 분석

가. 세션 키 생성 원리

먼저, 사용자가 먼저 정확한 패스워드 PW를 입력해야 B'을 계산할 수 있다. B'은 추후 사용자가 서버를 인증할 때 인증자 역할을 수행하는 메시지 C의 핵심 요소가 된다. 그러므로 정확한 PW를 알고 있는 사용자만이 B'을 유도할 수 있고 이를 이용해서 C값을 만들어 인증을 통과하게 된다. 이와 반대로 서버는 사용자로부터 (ID, C, W, T)를 받으면, $B'' = W^x$을 계산한 후 C'을 만들어 메시지 (ID, C', M, T'')를 사용자에게 전달한다. C'은 사용자가 서버를 인증하는 핵심 요소가 되고, $h(M \| B'' \| T'' \| ID)$로 이루어진다. 그 중 중요한 값은 $B'' = W^x = h(ID)^{wx}$로서, w는 사용자의 일회성 랜덤 값이고, x는 사용자의 비밀 값이다. 그러므로 서버는 x를 알고 있어야지만 B'', C'을 만들어 사용자로부터 인증을 통과 할 수 있다.

나. 가장 공격에 대한 취약성 분석

제안된 프로토콜은 공격자의 사용자 가장 공격에 취약하다. 우선 서버의 비밀 키가 노출되었을 때 가정 2에 의해서 서버를 가장하는 것을 막을 수는 없지만, 사용자를 가장하는 것은 막을 수 있도록 프로토콜이 설계되어야 한다. 하지만, 프로토콜은 서버의 비밀 키 x가 노출되었을 때, 사용자의 패스워드 PW를 모르고도 사용자가 서버에게 보내는 첫 번째 메시지를 위조할 수 있고 궁극적으로 정당한 세션 키를 만들 수 있게 된다. 그 과정을 상세히 설명하면 다음과 같다.

● **로그인 단계**

(1) 공격자가 서버의 개인 키 x를 알고 있다면, 메시지 (ID, C, W, T)를 쉽게 위조할 수 있다. 우선 공격자는 자신의 랜덤 값 s를 선택하고 현재시각 T를 설정한다.

(2) ID는 공개 된 값이고, B', W를 계산할 수 있다면 쉽게 C도 계산 할 수 있다. 정당한 B는 사용자가 선택한 랜덤 값 w에 대해 $h(ID)^{wx}$ 형태이다. 즉, 공격자의 랜덤 값 s에 대해서 B'값, $h(ID)^{ws}$을 계산할 수 있다. 마찬가지로 공격자는 $W=h(ID)^s$를 계산한다.

(3) 랜덤한 값 s와 현재시각 T에 대해서 (ID, C, W, T)를 위조하여, 사용자에게 보낸다.

● **인증 단계**

(1) 서버가 (ID, C, W, T)를 받은 후 ID가 자신이 발급한 ID인지 검증하고, T와 T'의 시간차가 미리 정해진 유효 시간 범위 안에 있는지도 검증한다. 또한, 서버는 자신의 개인키를 이용하여 $B'' = W^x$를 계산하고 받은 메시지 C 값이 $h(T\|B''\|W\|ID)$인지 검증한다. 위조된 메시지 (ID, C, W, T)는 사용자 측에서 랜덤하게 만든 값 w를 공격자가 s로 변경 한 것을 제외하고는 모두 동일한 형태이기 때문에 모든 검증 과정을 성공적으로 통과한다. 모든 검증이 성공적으로 끝나면, 서버는 랜덤 값 $m \in Z_p^*$을 선택하고, T''를 현재시간으로 설정한다. $M = h(ID)^m$를 계산하고, 이를 이용하여 $C' = h(M\|B''\|T''\|ID)$도 계산하고, (ID, C', M, T'')를 공격자에게 전달한다.

(2) 공격자는 메시지를 받은 후 서버와의 공통의 세션 키를 다음과 같이 계산한다.

$$sk' = h(ID\|M\|W\|M^s) = h(ID\|M\|W\|W^m)$$

V. 강화된 스마트카드 기반 인증 서비스 프로토콜

기존 프로토콜의 취약점을 강화하기 위한 핵심 아이디어는 스마트카드에 PKI 사용을 위한 공개키와 개인키를 저장하는 것이다. 즉, 스마트카드에 다음 두 가지 항목에 대한 저장을 의무화 한다.

- 카드 소지자의 서명 용 개인 키
- 카드 소지자의 개인 키에 대응되는 인증서

스마트카드에 개인 키와 인증서를 저장할 수 있는 공간은 현실적으로 충분하다. 또한 주어진 메시지를 전자서명 할 수 있는 연산력도 스마트카드 운영체제를 통해 충분히 수행 가능하다. 이러한 스마트카드의 실용적인 사용 예를 NIST에서 표준으로 정의한 개인식별 카드를 통해 이후 자세히 살펴본다. 우선, 스마트카드에 전자서명을 할 수 있는 능력을 이용하여 Xu, Zhu, Feng등이 제안한 프로토콜의 취약점을 보완하였다. 개선된 프로토콜은 다음과 같다.

1. 프로토콜 제안

가. 사용자 등록

사용자 등록과정은 기존 과정과 동일하다. 서버는 처음 $p=2q+1$를 만족하는 큰 소수 p, q를 선택한다. 또한 서버는 자신의 개인키 $x \in Z_q^*$와 일 방향 해시 함수, $h() : \{0,1\}^* \rightarrow Z_q^*$ 를 선택한다.

(1) 사용자는 자신의 ID와 패스워드 PW를 선택한 후 서버에게 (ID, PW)를 안전한 채널을 통해 전달한다.

(2) 서버는 (ID, PW)를 받은 후에 자신의 개인키 x를 이용하여 B값을 다음과 같이 계산한다.

$$B = h(ID)^x + h(PW) \bmod p$$

(3) 서버는 스마트카드에 개인키와 공개키를 생성하여 개인키 sk 와 공개키 pk에 대한 인증서 $cert(pk)$를 서버의 개인키를 이용해서 발급한다.

(4) 서버는 스마트카드에 $(ID, B, h(), p, q, sk, cert(pk))$를 저장하고 해당 사용자에게 발급한다.

나. 로그인 단계

사용자는 발급받은 스마트카드를 리더기에 집어넣고 자신의 ID와 패스워드, PW를 입력한다.

(1) 먼저 랜덤 값 $w \in Z_q^*$를 선택하고 현재시각 T를 설정한다.

(2) B', W, 그리고 C를 다음과 같이 계산한다.

$$B' = (B - h(pw^*))^w \bmod p$$
$$W = h(ID)^w$$
$$C = h(T \| B' \| W \| ID)$$

(3) 메시지 α=(ID, C, W, T)를 생성하고 자신의 개인키 sk로 서명한 값(= $Sig_{sk}(\alpha)$)과 스마트카드에 저장된 공개키에 대한 인증서 $cert(pk)$를 읽어서 서버에게 함께 전달한다.

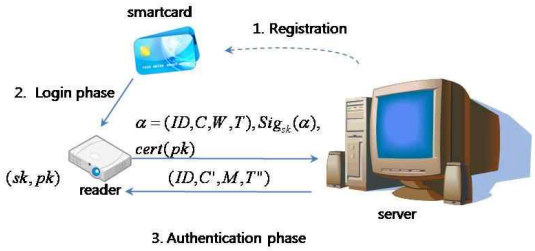

그림 3. 강화된 스마트카드 기반 인증 프로토콜
Fig. 3. A strong smartcard-based authentication protocol.

다. 인증 단계

(1) 서버는 메시지 α=(ID, C, W, T), $Sig_{sk}(\alpha)$, $cert(pk)$를 받은 후, 먼저 메시지 α에 대한 서명 값을 해당 인증서로 검증한다. 검증이 올바르지 않으면, 사용자의 로그인 요구를 거절하고 인증단계는 실패한다. 그 후 ID가 자신이 발급한 ID인지 검증한다. 서버는 메시지를 받은 시간 T'에 대해서 T와 T'의 시간차가 미리 정해진 유효 시간 범위 안에 있는지도 검증한다. 또한, 서버는 $B'' = W^x$를 계산하고 받은 메시지 C 값이 $h(T \| B'' \| W \| ID)$인지 검증한다. 모든 검증과정에서 하나라도 올바르게 수행되지 않으면, 사용자의 로그인 요구를 거절하고, 인증단계가 실패한다. 서버는 랜덤 값 $m \in Z_p^*$을 선택하고, T''를 현재시간으로 설정한다.

$M = h(ID)^m$를 계산하고 이를 이용하여 $C' = h(M \| B'' \| T'' \| ID)$도 계산한다. 최종적으로 (ID, C′, M, T′′)를 사용자에게 전달한다.

(2) 사용자는 메시지를 받은 후 ID와 T'를 검증하고, C'이 $h(M \| B'' \| T'' \| ID)$와 동일한지 검사한다. 모두 맞으면, 사용자는 서버를 인증하게 된다. 사용자와 서버는 공통의 세션 키 sk를 다음과 같이 계산한다.

$$sk' = h(ID \| M \| W \| M^w) = h(ID \| M \| W \| W^m)$$

2. 안전성 분석

제안한 인증 서비스 프로토콜이 3장에서 정의한 잘 알려진 공격들에 대해 안전함을 분석한다.

가. 사용자 가장 공격

- **(경우 1)** 공격자가 사용자의 패스워드 및 개인 키의 정보를 모르고도, 인증단계의 리더기를 대신해서 사용자를 인증단계 프로토콜에서 가장하는 경우 : 제안된 프로토콜은 올바른 패스워드와 사용자 개인키를 알지 못하면, 정당한 α=(ID, C, W, T) 값을 생성할 수 없고 이와 더불어 정당한 서명 값 $Sig_{sk}(\alpha)$을 만들 수 없다. 서버가 사용자를 검증하는 방법은 $B' = h(ID)^{xw}$값이 받은 $W = h(ID)^w$ 값에 x를 승한 값과 동일한지 비교함으로써 이루어진다. 공격자가 임의의 W값을 생성할 수는 있지만 x 값을 모르기 때문에 정당한 $B' = h(ID)^{xw}$값을 생성할 수 없고 이에 대한 서명도 위조할 수 없다.
- **(경우 2)** 공격자가 사용자의 스마트카드를 획득 한 후, 차분전력공격을 통해 스마트카드 내 인증정보를 노출할 수 있고 그 정보들을 통해 인증단계의 프로토콜에서 사용자를 가장 하는데 성공하는 경우 : 제안된 프로토콜의 스마트카드내의 인증정보는 (ID, B, $h()$, p, q, sk, $cert(pk)$) 이다. sk가 노출되므로 사용자의 서명을 위조 할 수 있지만 궁극적으로 사용자를 가장하기 위해서는 정당한 α=(ID, C, W, T)를 생성해야 한다. 이를 위해서, $B' = h(ID)^{xw}$값을 이용해서 C를 만들어야 하지만, 사용자의 정당한 패스워드를 모르고는 B'값을 만들 수 없기에 C도 만들 수 없다.
- **(경우 3)** 공격자가 서버의 데이터베이스 인증정보를 획득한 후 그 정보들을 통해 인증단계의 프로토콜에서 사용자를 가장 하는데 성공하는 경우 : Xu, Zhu, Feng등이 제안한 프로토콜은 이 공격에 안전하지 않음을 보였다. 제안한 프로토콜은 스마트카드 내에 개인 키를 저장하고 이를 통해 인증 단계에서 전자서명 값을 전달한다. 그러므로 비록 공격자가 서버의 개인 키 x를 소유해서 임의의 α=(ID, C, W, T) 값을 생성한다하더라도 전자서명 값

$Sig_{sk}(\alpha)$를 만들 수 없으므로 이 경우에 대한 안전성이 보장된다.

나. 서버 가장 공격

- **(경우 1)** 공격자가 인증단계 프로토콜에서 서버를 가장 할 수 있는 경우 : 서버를 가장하기 위해서는 정당한 (*ID, C′, M, T″*) 값을 사용자에게 전달해야 한다. *M, T″* 및 *ID*는 *x*값을 모르고도 쉽게 위조할 수 있지만, *C′* 값은 $B'' = W^x$ 값을 이용해서 계산되어지므로 *x*값을 소유한 서버만이 계산할 수 있는 값이다. 그러므로 이 경우에 대해서도 안전하다.
- **(경우 2)** 사용자의 스마트카드로부터 인증정보를 획득한 후 서버를 가장하는 경우 : 사용자의 스마트카드로부터 인증정보 (*ID, B, h(), p, q, sk, cert(pk)*)를 얻는다하더라도 서버를 대신할 수 없다. 서버를 가장하기 위해서는 위의 경우 2처럼 *x*값의 소유가 반드시 필요하다.

다. 오프라인 패스워드 사전 공격

- **(경우 1)** 인증 단계에 수행되는 프로토콜의 메시지들을 통해 오프라인 패스워드 추측 공격을 수행하는 경우 : 공격자가 획득할 수 있는 메시지는 (*ID, C′, M, T″*)와 (*ID, C, W, T*)이다. 이 모든 메시지에는 패스워드 정보가 포함되어 있지 않으므로 두 메시지 집합들을 통해 패스워드에 대한 사전공격은 불가능하다.
- **(경우 2)** 서버의 데이터베이스에서 서버의 비밀 정보가 공격자에게 노출되었을 때 그 정보들을 이용해서 사용자들의 패스워드를 오프라인으로 공격하는 경우 : 서버의 비밀 정보는 *x*이다. 이 값은 인증단계에서 $B'' = W^x$의 형태로 전달된다. 즉, 인증단계에서 전달되는 메시지 (*ID, C′, M, T″*)와 (*ID, C, W, T*)는 *x*값과 패스워드와 독립적인 랜덤한 값으로 구성되므로 패스워드 정보를 알아낼 수 없다. *x*값을 이용해서 인증단계의 메시지들 (*ID, C′, M, T″*)와 (*ID, C, W, T*)로 부터 패스워드를 알아 낼 수 없으므로 이 경우에 대한 안전성이 보장된다.
- **(경우 3)** 사용자의 스마트카드 및 서버의 비밀 키가 노출되었을 때, 공격자가 차분전력공격을 통해 스마트카드 내 인증정보를 노출하고 서버의 비밀 키를 통해 오프라인 패스워드 추측 공격을 수행하는 경우 : 만약 공격자가 스마트카드를 통해 (*ID, B, h(), p, q, sk, cert(pk)*) 값을 알 수 있고 서버의 비밀 키 값을 안다면 쉽게 패스워드를 사전 공격 할 수 있다. $B = h(ID)^x + h(PW)$ 값 및 *x* 값을 통해서 공격자가 임의로 선택한 패스워드에 대해 $h(ID)^x$를 뺀 값이 *B*와 동일한지 검증할 수 있기 때문이다. 하지만, 앞서 언급한 가정 4에 의해서 현실적으로 막을 수 없는 공격이다.

다. 완전 순방향 비밀성

사용자와 서버가 형성하는 세션 키는 다음과 같다.

$$sk' = h(ID \| M \| W \| M^w) = h(ID \| M \| W \| W^m)$$

비록 사용자의 개인 키 *sk, PW* 와 서버의 개인 키 *x*가 노출된다 하더라도 $h(ID)^w$, $h(ID)^m$ 값을 통해 $h(ID)^{wm}$ 값을 구할 수 없기 때문에 *sk*값을 계산할 수 없으므로 완전 순방향 비밀성이 만족된다.

3. 스마트 카드에 PKI 적용의 실례 연구

스마트카드에 PKI 기술을 적용한 개인 인증 기술은 이론 연구 및 상용화 단계를 넘어 국가 보안을 위한 기술 정책으로도 널리 활용되고 있다. 대표적인 것이 미국의 개인 식별 및 인증을 위한 PIV 카드 (Personal Identity Verification card)이다. PIV 카드는 미 연방정부의 보안을 강화하기 위해 국토안보 대통령 명령 12호 (HSPD-12)에 의해 도입된 것으로써, 카드 소지자의 다양한 개인 식별 및 인증정보(예: 카드 소지의 사진, 지문, 인증서, 암호화 키)를 담고 있는 카드이다. 2008년에는 NIST에서 PIV 카드를 각 시민단체의 접근통제 시스템에도 적용하기 위한 가이드라인을 작성하였으며, 이로 인해, 기존 미 연방 정부 내에서만 사용하던 PIV 카드는 각 시민단체에도 사용할 수 있게 되었다.

가. PIV 카드에 사용되는 키의 종류

미국립표준국(NIST)에서 발행한 FIPS 201 문서는 PIV(personal identification verification)와 관련한 기술, 기능, 절차적 표준을 정의하고 그 구체적 과정을 명시화하였다[6, 15]. FIPS 201문서에 PIV 카드 인증을 위해 전자서명 알고리즘, 키 관리, 암호화 알고리즘의 종류와 키 크기에 대해 명시하였다. 사용되는 암호화 키의 종류는 다음과 같다.

- 비대칭적 PIV 인증 키

- 카드 인증 키
- 문서 및 메시지를 전자서명하기 위한 비대칭 전자서명 키
- 키 설정과 키 전달을 지원하기 위한 비대칭 키 관리 키

비대칭적 PIV 인증 키는 카드 소지자의 인증 절차를 수행할 때 반드시 필요한 키로써 개인 키와 해당 공개키로 구성되고, 공개키는 인증서 형태로 PIV 카드에 반드시 저장되어야 한다. 그러므로 본 논문에 제안한 스마트카드 인증 시스템에서 개인 키와 공개키 인증서를 저장하는 핵심 아이디어는 매우 현실적이라 할 수 있다. 카드 인증 키는 물리적인 접근을 위해 사용되는 키로서 선택적인 키이며, 비 대칭 키 혹은 대칭 키로 사용될 수 있다. 나머지 두 키는 문서 및 메시지 서명과 키 전달을 위해 필요한 키이다.

나. PIV 카드에 저장되는 인증 정보 종류

또한 PIV 카드 내에 안전하게 보관해야 할 대상들을 다음과 같이 규정하였다.

- PIV 카드에 저장된 각 비 대칭키를 위한 X.509 인증서
- 카드 소지자의 고유 식별번호를 CHUID(Card Holder Unique Identifier) 전자서명 한 값
- 생체 인식 정보를 전자서명 한 값
- SP 800-73에서 정의한 기타 보안 대상(security object)

PIV 카드에 저장된 X.509 인증서는 카드 인증키에 대응되는 공개키에 대한 인증서이다. 인증서는 사전에 신뢰기관에 의해서 발행된다. 본 논문에 제안된 프로토콜은 키 종류와 저장 정보의 형태 관점에서 본다면 PIV 카드의 보안 규격사항을 준수하였다. 즉, 스마트카드를 발행할 때 개인 키와 공개 키에 해당하는 인증서를 미리 생성 한 후에 스마트카드에 의무적으로 저장하고 발급하도록 하였다. 그러므로 본 프로토콜에서 제안한 프로토콜은 이러한 PIV 카드의 규격사항과 동일한 스마트카드 시스템을 사용하여 기존 프로토콜의 취약점을 실용적으로 개선하였다.

Ⅵ. 결 론

본 논문에서는 효율적이고 안전한 스마트카드 인증 서비스 프로토콜에 대해서 연구하였다. 이를 위해 먼저 스마트카드 인증 서비스 절차, 안전성 정의, 그리고 잘 알려진 공격 등에 대해서 정의하였다. 정의된 안전성 기준을 바탕으로 최근에 설계된 Xu, Zhu, Feng등의 프로토콜이 서버의 비밀 값을 가진 공격자가 임의의 모든 사용자를 가장할 수 있는 공격에 취약함을 보였다. 이러한 취약점을 보완하기 위해 NIST 표준 PIV 카드의 규격처럼 스마트카드에 사용자의 비밀 키를 저장하게 함으로써 해당 취약점을 보완하였다.

서버 관리자는 제공 서비스의 연속성 및 안전성을 동시에 유지하기 위해서 많은 노력을 경주한다. 이러한 사실은 서버와 서버 관리자가 항상 위험에 노출되어 있음을 내포하며, 자신의 비밀 키가 노출되었는지도 모르는 상황에서 업무를 수행할 가능성이 높다. 비록 비밀 키가 노출되었음에도 불구하고 업무를 수행한 시간이 길지 않다하더라도 그 짧은 기간에 공격자가 노출된 비밀 키를 이용해서 사용자를 가장할 수 있다면 보안서비스 상 매우 심각한 문제를 야기한다. 아직까지 많은 스마트카드 인증 서비스 프로토콜들이 제안되었지만 이러한 공격에 대해서 언급하고 개선안을 제안한 논문은 없었다. 본 논문에서는 이러한 공격의 위험성 및 현실적인 개선방안을 제안했다는 측면에서 매우 큰 의미가 있다.

참 고 문 헌

[1] C.K. Chan, L.M. Cheng, Cryptanalysis of a remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 46 (4) (2000) 992 - 993.

[2] C.C. Chang, K.F. Hwang, Some forgery attacks on a remote user authentication scheme using smart cards, Informatica 14 (3) (2003) 289 - .294.

[3] H.Y. Chien, J.K. Jan, Y.M. Tseng, An efficient and practical solution to remote authentication: smart card, Computer and Security 21 (4) (2002) 372 - .375.

[4] H. Chung, W. Ku, M. Tsaur, Weakness and improvement of Wang et al.'s remote user password authentication scheme for resource limited environments, Computer Standards & Interfaces, 31 (2009) 863-868

[5] W. Diffie, P.C. van Oorschot, M.J. Wiener, Authentication and authenticated key exchanges, Designs Codes and Cryptography 2 (2) (1992)

107 - .125.
[6] [FIPS201] Federal Information Processing Standard 201-1, Change Notice 1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006. (See http://csrc.nist.gov)
[7] M.S. Hwang, L.H. Li, A new remote user authentication scheme using smart card, IEEE Transactions on Consumer Electronics 46 (1) (2000) 28 - .30.
[8] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, Proc. Advances in Cryptology (CRYPTO'99), 1999, pp. 388 - 397.
[9] W.C. Ku, S.M. Chen, Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 50 (1) (2004) 204 - 207.
[10] S.W. Lee, H.S. Kim, K.Y. Yoo, Improvement of Chien et al.'s remote user authentication scheme using smart cards, Computer Standards and Interfaces 27 (2005) 181 - .183.
[11] N.Y. Lee, Y.C. Chiu, Improved remote authentication scheme with smart card, Computer Standards and Interfaces 27 (2005) 177 - .180.
[12] L. Lamport, Password authentication within secure communication, Communications of the ACM 24 (1981) 770 - .772.
[13] T.S. Messerges, E.A. Dabbish, R.H. Sloan, Examining smart-card security under the threat of power analysis attacks, IEEE Transactions on Computers 51 (5) (2002) 541 - 552
[14] H.M. Sun, An efficient remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 46 (4) (2000) 958 - 961.
[15] [SP800-78-2] NIST Special Publication 800-78-2, Cryptographic Algorithms and Key sizes for Personal Identity verification, February 2010. (See http://csrc.nist.gov)
[16] X.M. Wang, W.F. Zhang, J.S. Zhang, M.K. Khan, Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards, Computer Standards and Interfaces 29 (5) (2007) 507 - 512.
[17] J. Xu, W. Zhu, D. Feng, An improved smart card based password authentication scheme with provable security Computer Standards & Interfaces 31 (2009) 723-728
[18] H.T. Yeh, H.M. Sun, B.T. Hsieh, Security of a remote user authentication scheme using smart cards, IEICE Transactions on Communications E87-B (1) (2004) 192 - 194
[19] E.J. Yoon, E.K. Ryu, K.Y. Yoo, Further improvement of an efficient password based remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 50 (2) (2004) 612 - 614.

저 자 소 개

변 진 욱(정회원)
2001년 고려대학교 전산학과 이학사 졸업.
2003년 고려대학교 정보보호 대학원 공학석사 취득.
2006년 고려대학교 정보보호 대학원 공학박사 취득
2007년 런던대학, ISG, 박사 후 연구원
2008년 평택대학교 정보통신학과 전임강사
2010년 평택대학교 정보통신학과 조교수
<주관심분야 : 정보보호 프로토콜, 프라이버시 보호 기술, 패스워드 인증, 정보통신 프로토콜>