通信情報保護論文誌
第9券 第2號 1999. 06

S/KEY를 개선한 일회용 패스워드 메커니즘 개발

박 중길* 김 영진* 김 영길** 백 규태** 백 기영* 류 재철*

The Development of a One-time Password Mechanism Improving on S/KEY

Junggil Park Youngjin Kim Younggil Kim Gyutae Baek Kiyoung Baek Jaecheol Ryou

요약

이 논문에서는 S/KEY 메커니즘에서 사용 횟수 제한과 사전에 키를 만들어 저장해야 하는 중요한 문제점을 해결한 일회용 패스워드 메커니즘을 제안한다. 제안한 일회용 패스워드 메커니즘은 암호화 알고리즘을 이용함으로써 사용 횟수 제한 문제를 해결할 수 있으며, 패스워드로부터 인증용 키를 생성함으로써 인증용 키관리를 용이하게 하고, 인증과 더불어 클라이언트와 서버간의 통신 세션키의 분배도 가능하게 한다. 그리고 제안한 메커니즘은 스마트 카드를 이용함으로 인증 정보의 보호 및 관리가 용이하며, 서버의 challenge가 없는 클라이언트에서 서버로의 단방향 인증을 필요로 하는 시스템에 바로 적용된다.

ABSTRACT

In this paper, we propose a one-time password mechanism that solves the problems of the S/KEY: the limitation of a usage and the need of storage for keys. Because of using a cryptographic algorithm, the proposed mechanism has no the limitation of a usage. Also, because of producing the key for an authentication from a user's password, it is easy to manage the authentication key and is possible to share the session key between a client and a server after the authentication process. In addition, the proposed mechanism is easy to protect and manage the authentication information because of using a smart card, and is adopted by the system that needs a one-way authentication from a client to a server without the challenge of a server.

Keyword: one-time password, S/KEY, authentication, session key, smart card

Ⅰ. 서 론

컴퓨터의 발달은 우리 환경에 많은 변화를 가져왔다. 그 중에서도 컴퓨터가 사무환경에 끼친 영향은 실로 크다고 할 수 있다. 예전에 손으로 처리하던 모든 일들이 컴퓨터를 이용해서 처리되고 있으며, 네트워을 이용한 그룹웨어와 같은 경우 결재 서류 없이 모든 것이 컴퓨터를 이용하여

* 충남대학교 컴퓨터과학과 (jgpark@home.chungnam.ac.kr), (yjkim@home.chungnam.ac.kr), (cloud@home.chungnam.ac.kr), (jcryou@esperosun.chungnam.ac.kr)
** 한국통신 멀티미디어 연구소 (ygkim@rcunix.kotel.co.kr), (baegt@kt.co.kr)

처리되고 있다.

이와 같이 컴퓨터를 이용한 사무 환경의 발달에 따라 이에 따른 문제점이 발생하기 시작했다. 예전에는 중요한 문서를 금고에 넣어 두고 자물쇠를 잠궈 두면 되었기 때문에 회사의 내부 문서를 보호하는 일이 비교적 쉬웠다. 그러나 네트웍 및 컴퓨터로 이루어진 사무환경이 발달함에 따라 단순히 컴퓨터 자체에 대한 접근통제 방법으로는 문서를 보호하는데 큰 도움이 되지 못하는 실정이다. 이에 따라 컴퓨터에 접근하는 사람에 대해 인증을 하고 적당한 접근 권한을 설정하는 일들이 컴퓨터 운영 환경을 고려하여 제시되어야 한다.

이러한 문제들을 해결하기 위하여 컴퓨터 사용자의 정당성을 확인하는 사용자 인증 메커니즘과 같은 보호 메커니즘이 개발되고 있다. 특히, 사용자 인증 메커니즘은 컴퓨터 시스템에 대한 접근 제어를 목적으로 하는 기반 기술로서, 패스워드 메커니즘 같은 것이 이에 해당한다.

그러나, 패스워드와 같이 단순한 인증 메커니즘은 네트웍 환경에서 커다란 문제점을 가지고 있다. 사용자가 인증 검증자로 보내는 패스워드가 암호화 되지 않은 상태로 전달되기 때문에 중간에 노출될 위험이 있기 때문이다. 이에 따라 네트워크상에서 기존 방식의 패스워드 노출 취약점 등을 보완하기 위해 일회용 패스워드 방식이 제시되었다. 일회용 패스워드 방식은 기존 방식과는 달리 네트워크상에서 검증자로 전달되는 인증 요구자의 인증용 패스워드가 매번 다른 값을 갖도록 해줌으로써 패스워드가 노출 된다 하더라도 이 패스워드는 한 번 밖에 사용하지 않는 패스워드이기 때문에 다른 사용자가 이를 사용하여 인증을 받을 수 없다.

최근에는 일회용 패스워드와 같은 인증 메커니즘은 카드 내에 프로세서 칩을 장착한 스마트 카드에 구현되어 사용되고 있다. 스마트 카드에 의해 제공되는 인증 메커니즘은 사용자 인증과 개체 인증 같은 상호 인증 기능을 포함하고 있다[1][2][3][4]. 그러나, 스마트 카드는 보호 수단으로서의 기본적인 기능만을 제공함으로 스마트 카드를 이용하여 인증 시스템을 설계할 때에는 시스템의 보다 안전한 운영과 보호를 위해서 전체 시스템의 운용 환경을 고려하여 이에 적합한 보안 설계와 대책이 고려돼야 한다. 이를 위해서 스마트 카드, 카드 사용자, 컴퓨터 시스템간의 관계를 고려하여 인증 시스템을 적절히 구현해야 한다[5].

이에 따라 이 논문에서는 스마트 카드의 특성 및 전체 시스템의 운용 환경 등을 고려하여 인증 시스템의 구축에 쉽게 적용할 수 있는 일회용 패스워드 메커니즘을 설계하였다. 그리하여, 스마트 카드를 사용함으로써 안전성이 향상되고 관리가 용이한 인증 시스템 구축을 가능하게 하며, 암호 알고리즘에 기반을 둔 메커니즘을 사용함으로써 S/KEY와 같은 일회용 패스워드 생성 메커니즘이 갖는 문제점, 즉 사용횟수 제한, 메커니즘의 안전성이 일방향 함수의 특성에 의존하는 것 등을 해결하고자 한다.

이를 위해서, 2장에서는 기존의 패스워드 인증 메커니즘에 대해 살펴보고, 3장에서는 이 논문에서 제안하고자 하는 일회용 패스워드 인증 메커니즘의 메커니즘 내용을 기술하고, 4장에서는 3장에서 설계한 일회용 패스워드 인증 메커니즘을 이용하여 상용 스마트 카드에 적용해 실제 구현한 내용들을 기술한다. 마지막으로, 5장에서는 설계 구현한 내용을 기존 방법과 비교 분석한다.

II. 패스워드 인증 메커니즘 고찰

많은 컴퓨터 시스템에서 사용자 인증 방식으로 패스워드 메커니즘을 사용하고 있

다[6][7][8][9][10]. 패스워드 메커니즘은 (그림. 1)에서 보는 바와 같이 인증 검증자가 패스워드를 사용하여 인증 요구자를 인증하는 메커니즘이다. 인증 요구자는 식별자 id와 패스워드 p'을 이용하여 인증 메시지를 생성하고, 네트워크를 통해 인증 메시지를 인증 검증자에게 보낸다. 인증 검증자는 인증 요구자가 보내온 인증 메시지에 포함된 패스워드 p'을 자신이 저장하고 있는 패스워드 p와 비교하여 같으면 인증 요구자를 인증해준다.

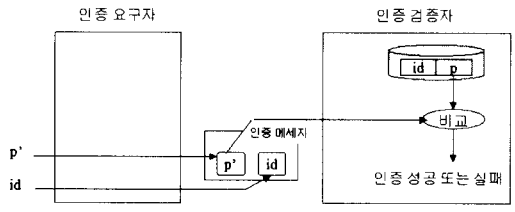


그림 1 기본적인 패스워드 인증 메커니즘
(Fig. 1) Basic password authentication mechanism

그러나, 위와 같은 패스워드 인증 메커니즘은 다음과 같은 문제점들을 갖고 있다[11].

- 패스워드 노출 : 네트워크를 통해 패스워드가 보호되지 않은 상태로 전달됨
- 패스워드 재연 : 일정한 값을 갖는 패스워드가 반복적으로 사용됨
- 검증자 침해 : 인증 검증자가 저장 관리하고 있는 인증 정보가 노출되었을 때 이것을 분석함으로써 패스워드를 추측할 수 있음

기본적인 패스워드 인증 메커니즘이 갖고 있는 이러한 문제점들을 해결하기 위하여 (그림. 2) 및 (그림. 3)과 같이 개선되거나 변형된 인증 메커니즘이 제시되었다.

(그림. 2)에 제시된 인증 메커니즘은 일방향 함수를 사용하여 구성한 패스워드 메커니즘으로서 인증 요구자로부터 인증 검증자로 전달되는 패스워드는 일방향 함수 f를 수행한 값을 사용하도록 하여 패스워드가 노출되는 것을 보호했다. 또한, 인증 검증자에 의해 저장 관리되는 사용자 인증 정보도 패스워드 값 자체를 사용하는 것이 아니라 패스워드의 일방향 함수 g를 수행한 값을 사용함으로써 검증자 침해를 방지한다. 마지막으로, 인증 요구자가 인증 메시지를 구성할 때에는 반복되지 않는 값 nrv를 사용하여 메시지를 구성하게 함으로써 패스워드 재연을 방지한다.

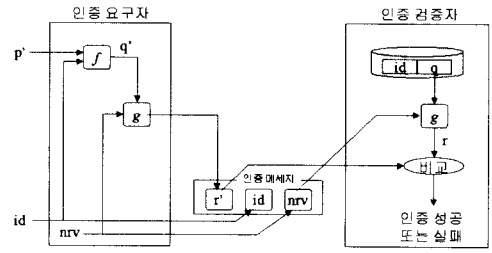


그림 2 검증자 침해 및 패스워드 노출/재연 방지를 고려한 패스워드 인증 메커니즘
(Fig. 2) The password authentication mechanism considered for a verifier attack and a password exposure/replay

(그림. 3)에 제시된 인증 메커니즘은, 패스워드 인증 메커니즘은 아니지만, 패스워드와 같은 역할을 하는 변형된 개념의 키와 암호 알고리즘을 사용하여 구성한 메커니즘으로서, 인증 요구자로부터 인증 검증자로 전달되는 인증 메시지를 암호 또는 서명하여 인증을 수행하게 된다. 여기에서는 암호 또는 서명에 사용되는 키가 노출되지 않기 때문에 키 또는 패스워드 노출과 같은 문제점은 없다. 반면에 인증 검증자 측에서 복호 또는 검증에 사용되는 키 값을 저장해 두기 때문에, 검증자 침해에 대비하여 키 값 자체를 다른 암호 알고리즘 또는 다른 키 값을 이용하여 보호함으로써 침해를 방지해야 한다. 여기에서도, 앞서의 패스워드 인증 메커니즘에서와 마찬가지로, 인증 요구자가 인증 메시지를 구성할 때에는 반복되지 않는 값 nrv를 사용하여 메시지를 구성하게 함으로써 인증

메시지 재연을 방지한다.

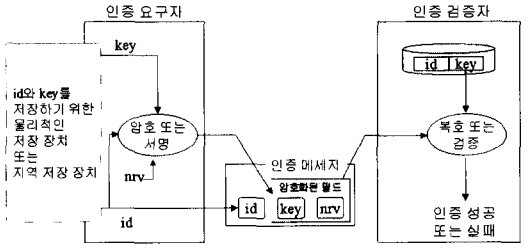


그림 3 간단한 암호화 기반의 인증 메커니즘
(Fig. 3) The authentication mechanism based on a simple encryption

일반적으로, 인증 메커니즘의 동작 또는 성립 원칙을 살펴 보면, 대부분의 인증 메커니즘에 적용되는 두 가지 원칙이 다음과 같다는 것을 알 수 있다[11][12][13][14].

- 알고 있는 것(패스워드, ...)
- 소유하고 있는 것(신용카드, 신분증, ...)

앞에서 기술한 (그림. 2)와 같은 패스워드 인증 메커니즘은 "알고 있는 것"을 이용하여 사용자를 인증하는 방식으로 "소유하고 있는 것"을 인증에 포함하지 않았다. 인증 메커니즘이 "소유하고 있는 것"을 통해서 사용자를 인증하도록 지원하기 위해서는 물리적인 저장 장치(이하 토큰)를 사용해야만 한다. 반면에, (그림. 3)과 같은 암호화 기반의 인증 메커니즘에서는 물리적인 토큰에 해당하는 "소유하고 있는 것"을 인증에 포함하고는 있으나, 패스워드와 같이 "알고 있는 것"을 포함하고 있지 않다. 그러므로, 암호 알고리즘에 사용되는 키와 더불어 추가적으로 사용자 패스워드를 기억하고 비교하는 능력이 있는 스마트 카드와 같은 저장 장치를 물리적인 토큰으로 사용해야만 한다.

그러므로, 인증 메커니즘의 두가지 원칙을 적용한 일반적인 방식은 사용자가 패스워드를 사용하여 먼저 자신을 인증하고, 사용자를 대신하는 장비는 암호 알고리즘을 사용하여 궁극적인 인증 검증자에게 사용자를 인증하게 한다. 실제로 이와 같은 방식은 여러 가지 조합으로 구현되지만, 중요한 것은 사용자가 "알고 있는" 패스워드와 사용자가 "소유하고 있는" 스마트 카드를 사용한다는 것이다.

이 논문에서도 이런 방식을 적용하여, 앞서 살펴 본 패스워드 메커니즘과 스마트 카드와 같은 물리적인 토큰을 사용하는 암호 기반의 인증 메커니즘을 사용함으로써 "알고 있는 것"과 "소유하고 있는 것"을 통한 사용자 인증이 이루어지도록 인증 메커니즘을 구성한다.

III. 일회용 패스워드 인증 메커니즘 설계

기존에 제안된 S/KEY 일회용 패스워드 생성 메커니즘은 (그림. 4)에서 나타난 바와 같이 일방향 함수를 사용하여 패스워드를 생성하게 되어 있다. 여기에서는 맨 처음 난수 R 값을 생성하고 이 값에 대해 $X_{n+1}=f(f(f(f(R))))$ 이 되도록 일방향 함수 f 를 n+1 번 수행하여 X_{n+1} 을 구한다. 그리고, R과 X_{n+1} 을 각각 인증 요구자와 검증자에게 시스템 최초 설정 시 전달하여 저장해 둔다[10].

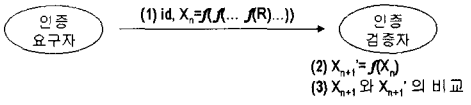


그림 4 일방향 함수를 사용한 기존 일회용 패스워드 메커니즘
(Fig. 4) The one-time password mechanism using one-way hash function

이렇게 설정된 상태에서 인증 요구자가 검증자에게 인증을 받을 필요가 생기면, (그림. 4)의 (1)에서처럼 자신의 사용자 번호인 id와 일방향 함수 f 를 n 번 수행한 X_n을 인증 정보로 인증 검증자에게 전달하게 된다. (2)에서 인증 검증자는 전달 받은 인증 정보의 X_n을 이용하여 일방향 함수 f 를 1회 더 계산함으로써 $X_{n+1}'=f(X_n)$ 을 구

한다. (3)에서 인증 검증자는 앞서 계산된 X_{n+1}'값을 시스템 설정 시 저장한 X_{n+1} 값과 비교하여 같으면 인증 요구자를 인증하게 된다. 인증이 성공적으로 이뤄지게 되면 인증 검증자는 X_n 을 다시 저장한다.

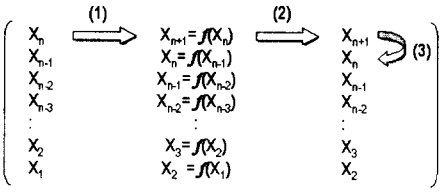


그림 5 기존 일회용 패스워드 메커니즘에서의 일방향 함수 운용 개념
(Fig. 5) The operation concept of one-way hash function in one-time password mechanism

(그림. 5)는 이러한 S/KEY 일회용 패스워드 생성 메커니즘에서 인증 정보를 생성하기 위해 인증 요구자와 검증자가 각각 일방향 함수를 어떻게 사용하는지 구체적으로 보여준다. 최초 시스템 설정 시에 인증 요구자와 검증자는 R 값에 대해서 $f(f(f(f(R))))$ 이 되도록 일방향 함수 f 를 n 번, n+1 번 수행하여 각각 X_n, X_{n+1} 을 갖고 있게 된다. 이때 R 값은 인증 요구자가 알고 있는 값으로 인증 요구자는 이 값으로부터 일방향 함수 f 를 수행하여 임의의 n에 대하여 X_n을 계산하는 것이 가능하지만, 인증 검증자는 요구자가 전달해준 X_n 에 대해 일방향 함수 f 를 수행하여 $X_{n+1}=f(X_n)$ 을 계산하는 것만 가능하다.

(그림. 5)의 (1)에서 인증 요구자가 R 값에 대해 일방향 함수 f 를 n 번 수행하여 X_n 을 인증 검증자에게 전달한다. (2)에서 인증 검증자는 전달 받은 X_n에 대해 일방향 함수 f 를 수행하여 $X_{n+1}=f(X_n)$ 을 계산한다. 그 다음, (3)에서 시스템 설정 시에 저장되어 있던 X_{n+1} 과 (2)의 계산 결과를 비교하여 같으면 인증 요구자를 인증하게 되고 요구자로부터 전달 받은 X_n 을 저장하여 다음 인증 과정에서 사용한다.

다음 인증 과정이 수행되면, (1)에서 인증 요구자는 다시 R 값에 대해 일방향 함수 f 를 n-1 번 수행하여 X_{n-1} 을 인증 검증자에게 전달한다. (2)에서 인증 검증자는 전달 받은 X_{n-1}에 대해 일방향 함수 f 를 수행하여 $X_n=f(X_{n-1})$을 계산한다. 그 다음, (3)에서 저장되어 있던 X_n 과 (2)의 계산 결과를 비교하여 같으면 인증 요구자를 인증하게 되고 요구자로부터 전달 받은 X_{n-1} 을 저장하여 다음 인증 과정에서 사용한다. 이와 같은 과정이 X_1 일 때까지 반복된다.

그렇지만, 위와 같은 일회용 패스워드 생성 메커니즘에는 다음과 같은 문제점이 존재하게 된다.

① 사용 횟수에 대한 제한이 있다.
② 인증 요구자는 인증에 사용되는 일회용 패스워드를 미리 생성하거나 매번 필요한 횟수만큼 함수를 수행하여 계산해야 한다.
③ 메커니즘의 안전성이 일방향 함수의 특성에 의존한다.

그리고 별도의 기밀성 서비스를 하기 위해서는 인증 요구자에 대한 인증만을 수행함으로 인증 검증자와 요구자간에 다시 키 분배 과정을 수행해야 하는 불편함이 있다.

이 논문에서는 이러한 문제점을 갖는 S/KEY 방식을 개선하여 일방향 함수(one-way function) 및 암호 알고리즘(encryption algorithm)을 이용한 일회용 패스워드(one-time password) 메커니즘을 제안하였다. (그림. 6)은 이 논문에서 제안한 일회용 패스워드 생성 메커니즘에 대해 나타내고 있다.

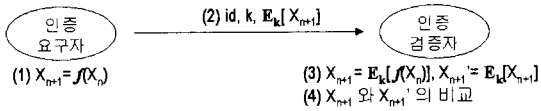


그림 6 일방향 함수 및 암호 알고리즘을 사용하여 제안한 일회용 패스워드 메커니즘
(Fig. 6) The proposed one-time password mechanism using one-way hash function and encryption algorithm

제안한 메커니즘에서는 맨 처음 시스템 설정 시에 난수인 초기값 X_0를 생성하여 이 값을 각각 인증 요구자와 검증자에 저장해 둔다. 이 상태에서 인증 요구자가 검증자로부터 인증을 받기 위해 (그림. 6)의 (1)에서 $X_{n+1}=f(X_n)$를 계산한다. 그리고, (2)에서 자신의 사용자 번호인 id와 키 k, $E_k[X_{n+1}]$를 인증 정보로 인증 검증자에게 전달하게 된다. (여기에 사용된 암호 알고리즘 E는 임의의 키를 사용하여 데이터 암호화 기능을 수행한다.) (3)에서 인증 검증자도 (1)에서와 마찬가지로 $X_{n+1}=f(X_n)$를 계산하고 이를 암호화하여 $E_k[X_{n+1}]$을 구한다. (4)에서 인증 검증자는 (2)에서 보내온 x 값과 (3)에서 구한 x'값을 비교하여 같으면 인증 요구자를 인증하게 된다. 인증이 성공적으로 이뤄지게 되면 인증 검증자는 X_{n+1}값을 저장해 둔다.

(그림. 7)은 제안한 일회용 패스워드 생성 메커니즘에서 인증 정보를 생성하기 위해 인증 요구자와 검증자가 각각 일방향 함수와 암호 알고리즘을 어떻게 사용하는지 구체적으로 보여준다. 여기에서는 최초 시스템 설정 시에 난수 R 값을 각각 인증 요구자와 검증자에 저장한다. 그러므로, 인증 요구자와 검증자는 $X_0=R$ 로부터 $X_{n+1}=f(X_n)$ 을 구하는 것이 가능하며, 여기에서 생성되는 일련의 값들은 외부로 노출되지 않도록 안전하게 각자가 잘 보관하여 관리해야 한다.

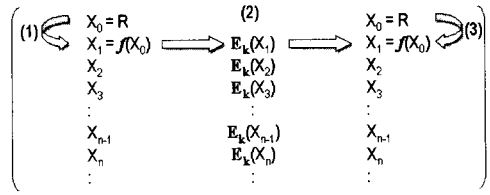


그림 7 제안한 일회용 패스워드 메커니즘에서의 일방향 함수 및 암호 알고리즘의 운용 개념
(Fig. 7) The operation concept of one-way hash function and encryption algorithm using proposed one-time password mechanism

(그림. 7)의 (1)에서 인증 요구자는 $X_0=R$ 값에 대해 일방향 함수 f 를 수행하여 $X_1=f(X_0)$ 을 생성한다. (2)에서 인증 요구자는 X_1 값을 E로 암호화 하여 $E_k[X_1]$ 값을 인증 검증자로 전달한다. (3)에서 인증 검증자는 자신이 저장하고 있는 $X_0=R$로부터 $X_1=f(X_0)$을 구하여 이를 E로 암호화 하여 $E_k[X_1]$ 값을 구한 뒤에 (2)에서 전달 받은 값과 비교하게 되고, 값이 같으면 인증 요구자를 인증하게 된다. 새로 계산된 $X_1=f(X_0)$ 값은 인증 요구자와 검증자가 각각 저장하여 다음 인증 과정에서 사용된다.

다시, 다음 인증 과정이 수행되면, (1)에서 인증 요구자는 저장된 X_1 값에 대해 일방향 함수 f 를 수행하여 $X_2=f(X_1)$ 을 생성한다. (2)에서 인증 요구자는 X_2 값을 E로 암호화 하여 $E_k[X_2]$ 값을 인증 검증자로 전달한다. (3)에서 인증 검증자도 자신이 저장하고 있는 X_1 값으로부터 $X_2=f(X_1)$을 구하고 이를 E로 암호화 하여 $E_k[X_2]$ 값을 구한 뒤에 (2)에서 전달 받은 값과 비교하게 되고, 값이 같으면 인증 요구자를 인증하게 된다. 인증 요구자와 검증자는 새로 계산된 $X_2=f(X_1)$ 값을 저장하여 다음 인증 과정에서 사용한다. 이와 같은 과정이 계속 반복된다.

일방향 함수와 암호 알고리즘을 적용하여 제안한 일회용 패스워드 메커니즘을 이용하여 인증 프로토콜을 수행할 때에 인증

요구자 및 검증자가 수행해야 하는 연산 절차와 인증 정보 전달 과정이 (그림. 8)에 나타나 있다.

인증 요구자는 자신의 사용자 번호인 id, 저장되어 있는 X_n, 그리고 기타 사용자관련 정보인 text를 이용하여 $X_{n+1}= f(id \| X_n \| text)$를 계산한다. 다음으로 인증 정보를 암호화하기 위한 키 생성을 위해 난수 r을 생성하여 암호 알고리즘 E를 통해 키 $k = E_{Xn}(r)$을 계산한다. 그리고, 앞에서 계산된 X_{n+1}, k로부터 $x = E_k(X_{n+1})$을 계산한다. 마지막 단계로 인증 요구자는 검증자에게 id, r, x를 전달하게 된다.

인증 검증자는 id, r, x를 전달 받은 뒤에 먼저 $X_{n+1}= f(id \| X_n \| text)$를 계산한다. 그리고, $k = E_{Xn}(r)$을 계산하여 인증 정보 암호화에 사용된 키 값을 계산한다. 그 다음에 앞서 계산된 k, X_{n+1}을 이용하여 $x'= E_k(X_{n+1})$을 계산한다. 여기에서 계산된 x'을 인증 요구자가 보내온 x와 비교하여 같으면 요구자를 인증하게 된다. 인증이 성공적으로 이뤄지면 인증 요구자와 검증자는 각각 X_{n+1}를 저장하여 다음 인증 프로토콜이 수행될 때 사용하게 된다.

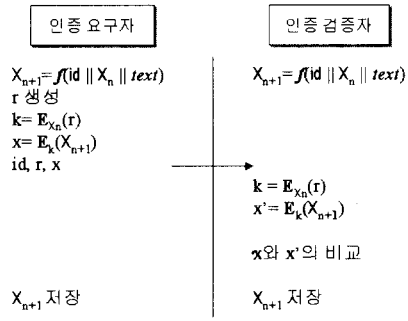


그림 8 제안한 일회용 패스워드 메커니즘을 이용한 인증 프로토콜
(Fig. 8) The authentication protocol using posposed one-time password mechanism

위에서 제안한 일회용 패스워드 메커니즘에서는 일회용 패스워드가 $X_0=R$, $X_1=f(X_0)$, $X_2=f(X_1)$, 형태로 생성되기 때문에 사용 횟수에 대한 제한이 없을 뿐 아니라 이를 미리 생성하거나 매번 필요한 횟수만큼 반복하여 함수를 계산하지 않아도 된다. 또한, 위 메커니즘은 메커니즘의 안전성이 암호 알고리즘의 특성에 의존한다. 그리고 인증 과정 수행이 완료된 후에는 인증 검증자와 요구자간에 비밀 통신을 위한 통신 세션 키 분배가 이루어 진다.

Ⅳ. 일회용 패스워드 인증 메커니즘 구현

클라이언트/서버 환경에 스마트 카드 기반의 일회용 패스워드 인증 메커니즘을 적용했을 때 사용자는 서버로 접속하기 위해서 자신의 패스워드와 스마트 카드를 사용하게 된다(여기에서 사용자가 입력하는 패스워드는 일회용 패스워드가 아닌 스마트 카드가 사용자 인증을 위해 사용하는 패스워드임). 이렇게 사용자가 서버로 접속 하기 위해서 스마트 카드를 이용하는 인증 메커니즘을 구현한다면 사용자, 스마트 카드, 클라이언트 각각에 대한 인증이 요구된다. 사용자가 스마트 카드의 정당한 소유자인지 인증이 이뤄져야 하고, 스마트 카드는 정당하게 발급된 것인지 인증이 이뤄져야 하고, 클라이언트는 서버로의 접속을 위해서 인증이 이뤄져야 한다[4].

표 2 인증 프로토콜에 사용되는 인증 데이터
<Table. 1> The authentication data used in authentication protocol

	서버	클라이언트	스마트 카드	사용자	비고
id(8), sn(8)	○	×	○	×	
pw(8)	×	×	×	○	
seed1(16)	×	×	○	×	seed1=MD5(id‖sn‖pw)
seed2(16)	○	×	○	×	$seed2_0$=난수 $seed2_n$=MD5(id‖우‖$seed2_{n-1}$)

그러므로, 여기에서 구현되는 인증 메커니즘은 이렇게 각 인증 대상에 대해 인증이 이뤄지도록 하기 위해서, 사용자로부터 패스워드를 입력 받아 인증 관련 정보를 클라이언트 상에 생성시킨 뒤에 클라이언트와 스마트 카드 간에 인증을 수행하고,

그 다음 스마트 카드로부터 읽어 들인 일회용 패스워드 생성 정보를 사용하여 서버와 인증을 수행하도록 한다. 이러한 인증 메커니즘에 사용되는 인증 수행에 관련된 인증 데이터는 <표. 1>과 같다.

인증 데이터에는 사용자 구분자 id, 카드 발급 번호 sn, 그리고 사용자 패스워드 pw가 있고, 암호화 기반의 인증 메커니즘을 사용했기 때문에 여기에 사용되는 사용자 인증용 키 seed1과 클라이언트 인증용 키 seed2가 있다. <표. 1>에 나타난 바와 같이, 서버측에는 id, sn을 사용자 등록 시에 생성하게 되고, 스마트 카드에는 id, sn, seed1, seed2를 카드 발급 시에 생성하게 되고, 클라이언트는 어떤 값도 저장하지 않게 된다. 그리고 사용자는 자신의 패스워드 pw를 인증 시에 사용한다.

이 논문에서 제안한 인증 메커니즘의 구현에는 8 비트 CPU, 8K 바이트 데이터 메모리를 갖는 스마트 카드를 사용하였으며, 이 스마트 카드는 DES 및 T-DES암호 알고리즘을 수행한다. 구현된 인증 메커니즘은, 우선적으로 사용자 인증 프로토콜을 수행하며, 서버로 접속하기 위해서 클라이언트 인증 프로토콜을 수행한다. 사용자 인증 과정에서는 회답요구-응답(challenge-response) 방식의 인증 방법을 사용하며, 제안한 알고리즘은 클라이언트와 서버 사이의 인증에 사용된다.

사용자 인증 프로토콜은 사용자, 스마트 카드 및 클라이언트 간에 수행되는 프로토콜로서 사용자를 인증하는 과정이다. 이를 위해 인증 세션 생성 단계와 사용자 인증 단계를 거치게 된다.

인증 세션 생성 단계는 인증 메커니즘이 수행되는 한 세션 동안에 사용할 세션키를 생성하는 단계로서 (그림. 9)와 같다. 클라이언트에는 아무런 인증 데이터도 저장되어 있지 않기 때문에 스마트 카드에 저장되어 있는 id, sn과 사용자가 입력해주는 pw를 사용하여 세션키 생성에 필요한 seed1을 이 단계에서 생성하게 된다. 그 다음에 클라이언트와 스마트 카드 간에 난수를 교환한 뒤에 앞서 계산된 seed1을 사용하여 세션키를 계산하게 된다.

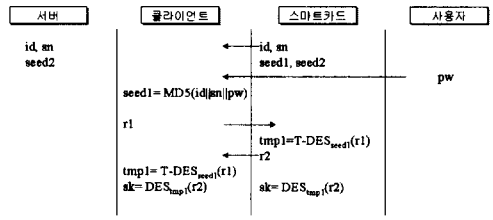


그림 9 인증 세션 생성 단계
(Fig. 9) The authentication session generation process

사용자 인증 단계는 앞서 생성된 세션키를 사용하여 회답요구-응답 방식으로 사용자 인증을 실시하는 단계로서 (그림. 10)과 같다.

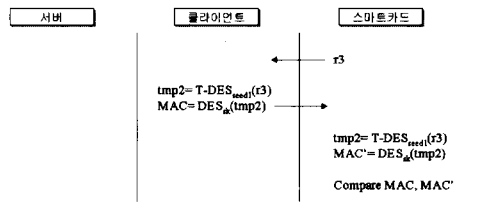


그림 10 사용자 인증 수행 단계
(Fig. 10) The user authentication process

클라이언트 인증 프로토콜은 네트워크 상의 서버와 클라이언트 간에 수행되는 프로토콜로서 서버에 접속하기 위해서 클라이언트가 서버로부터 인증을 받기 위한 과정이다. 이를 위해 클라이언트 인증 수행 단계와 클라이언트 인증 정보 변경 단계를 거치게 된다.

클라이언트 인증 수행 단계는 앞서 설계한 일회용 패스워드 메커니즘에 따라 생성한 일회용 패스워드를 서버측으로 전송하는 단계로서 (그림. 11)과 같다. 구현에 사용된 스마트 카드가 DES 기반의 암호 알고리즘을 사용하기 때문에 이에 맞춰서 인증 메시지 암호 알고리즘으로 DES를, 암호화 키 생성에 관련돼서 난수 r_1, r_2를 사용

하게 되었다. 그렇기 때문에 인증 메시지는 사용자 구분자 id, 난수 r_1, rs, 그리고 암호화된 값 x로 구성되어 전송된다.

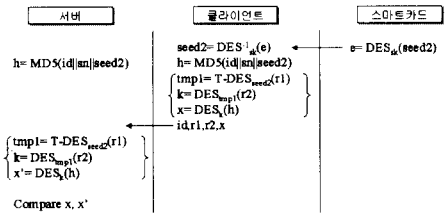


그림 11 클라이언트 인증 수행 단계
(Fig. 11) The client authentication process

클라이언트 인증 정보 변경 단계는 인증 수행 단계를 성공적으로 수행한 뒤에 다음 인증 수행 단계에서 사용하게 될 인증 정보를 서버와 스마트 카드에 각각 저장하는 단계로서 (그림. 12)와 같다.

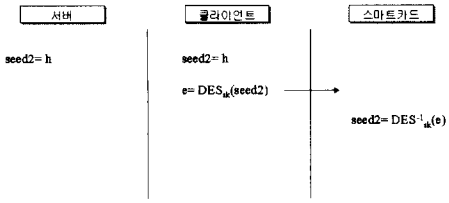


그림 12 클라이언트 인증 정보 변경 단계
(Fig. 12) The client authentication information change process

V. 결론

이 논문에서 제안하는 스마트 카드를 이용한 클라이언트/서버 환경에 적합한 일회용 패스워드 메커니즘은 암호화 알고리즘을 이용하여 사용 횟수에 제한이 없으며, 패스워드로부터 인증용 키를 생성하기 때문에 암호 알고리즘을 사용하더라도 클라이언트상의 사용자 인증용 키 관리가 용이하고, 인증과 더불어 클라이언트와 서버간에 통신 세션 키 분배를 실시할 수 있게 한다. 그 외 다른 항목에 대한 기존의 S/KEY 인증 메커니즘과 스마트 카드에 적합한 일회용 패스워드 메커니즘간의 비교 결과는 <표. 2>와 같다.

표 3 알고리즘 비교 분석
<Table. 2> The comparison/analysis of algorithm

	S/KEY 알고리즘	개발 알고리즘
사용횟수	n	∞
키 저장	n	1
안전성	One-way Function에 의존	암호알고리즘에 의존
키 분배	×	○

제안한 인증 시스템에서는 S/KEY 메커니즘에 사용 횟수의 제한이 있는 문제점과 미리 키를 만들어 저장해야 하는 문제점을 해결하였으며, 암호 알고리즘을 사용함으로써 안전성을 향상시켰고, 인증과 더불어 서버와 클라이언트간에 세션키의 분배도 가능하게 했다. 또한, 스마트 카드를 적용하여 인증 메커니즘을 구성함으로써 사용자 인증 과정이 보다 더 안전하게 이뤄지고 인증 정보의 보호 및 관리가 용이하게 이뤄질 수 있게 하였다. 그리고, 클라이언트에서 서버로의 인증 과정이 일방향성을 갖게 함으로써 네트워크 상에서 트래픽 부담을 줄일 수 있는 형태로 개발했다.

지금까지 일회용 패스워드 메커니즘을 적용하여 개발된 제품들은 대부분 일회용 패스워드 생성에 특정 하드웨어 장치를 사용해야 하는 방식으로 개발됨으로써 개발품의 단가를 높이고 이를 적용한 시스템의 유지 보수를 까다롭게 해왔다. 이 논문에서는 이러한 점들을 고려하여 기존 일회용 패스워드 생성 메커니즘을 개선한 스마트 카드와 같은 범용 저장 장치에 적합하도록 인증 메커니즘을 설계하였고, 기존에 패스워드 메커니즘을 사용하거나 단방향 인증을 사용하는 응용에 쉽게 적용 가능하도록 구현하였다.

참고 문헌

[1] Gemplus, *GPS120 Application*

Programmer's Guide, 12. 1993.
[2] Gemplus, GPS120 Reference Guide, 06. 1993.
[3] Gemplus, GPS120 User's Guide, 09. 1993.
[4] 현대전자(주), HYUNDAI COS(HYC 201/802) User's Guide, 1997.
[5] 신진원, 권태경, 송주석, "스마트 카드 시스템의 보안 기능 분석 및 설계에 관한 고찰", 한국통신정보보호학회 종합학술발표회 논문집, Vol 5, No. 1, pp. 265-74, 11. 1995.
[6] "OnceID and Oasis," http://www.softforum.co.kr:4040/product/OnceID_Oasis.html.
[7] "One-Time Passcode Software for User Authentication," http://www.securitydynamics.com/solutions /pro ducts /sofidata.html.
[8] "SecurID Tokens Datasheet," http://www.securitydynamics.com/solutions/products/tokens.html.
[9] Neil M. Haller and Philip R. Karn, "Description of The S/KEY One-Time Password System," http://www-staff.lboro.ac.uk/~ccgpg/skey.html.
[10] "패스워드 누출방지 기술," http://www.kisa.or.kr/K_tech/exp/netsec/password.html.
[11] Warwick Ford, Computer Communication Security, Prentice Hall, pp.109-148, 1994.
[12] 최용락, 소우영, 이재광, 이임영, 통신망 정보 보호(Network and Internetwork Security Principles and Practice), 도서출판 그린, 02. 1996.
[13] Bruce Schneier, Applied Cryptography, Second Edition, John Wiley & Sons, 1996.
[14] William Stallings, Network and Internetwork Security, Prentice-Hall, 1995.

□ 著者紹介

박 중 길 **정회원**

1986년 2월 : 동국대학교 전자계산학과(학사)
1988년 2월 : 서강대학교 전자계산학과(석사)
1988년~현재 : 국방과학연구소 선임연구원
1998년~현재 : 충남대학교 컴퓨터과학과 박사과정

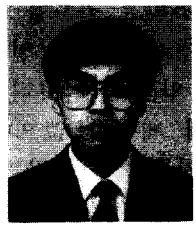
〈관심분야〉 컴퓨터통신보안, 접근통제, 암호이론

김 영 진 **정회원**

1989년 2월 : 중앙대학교 전자계산학과(학사)
1998년~현재 : 충남대학교 컴퓨터과학과 석사과정

〈관심분야〉 컴퓨터통신보안, 스마트카드 응용, 정보보호 이론

김 영 길 **정회원**



1990년 : 한양대학교 전자계산학과 (학사)
1992년 : 숭실대학교 전자계산학과 (석사)
1992년~현재 : 한국통신 멀티미디어연구소 전임연구원

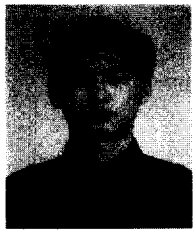
〈관심분야〉 인터넷보안, PKI

백 규 태 **정회원**

1985년 : 연세대학교 전기공학과 (학사)
1989년 : Lehigh Univ. Computer Science (석사)
1995년 : Lehigh Univ. Computer Science (박사)
1995년 : ATLSS Research Center, Lehigh Univ. Research Engineer
1996년~현재 한국통신 멀티미디어연구소 선임연구원

〈관심분야〉 컴퓨터/네트워크 보안, PKI, AI, CSCW

백 기 영 **정회원**



1996년 : 충남대학교 컴퓨터과학과 졸업 (학사)
1998년 : 충남대학교 대학원 컴퓨터과학과 (석사)
1998년~현재 : 충남대학교 대학원 컴퓨터과학과 박사과정

〈관심분야〉 보안 프로토콜, PKI, 디렉토리 서버

류 재 철 **정회원**

1985년 : 한양대학교 산업공학과(학사)
1988년 : Iowa State University 전산학과(석사)
1990년 : Northwestern University 전산학과(박사)
1991년~현재 : 충남대학교 컴퓨터과학과 부교수

〈관심분야〉 컴퓨터 및 통신망 보안, 전자상거래, 분산