논문 00-25-12T-7 한국통신학회논문지 '00-12 Vol.25 No.12T

검증 테이블이 없는 패스워드 인증 시스템

정회원 유 종 상*, 권 창 영**

A Password Authentication System without verification tables

Jong-Sang Yu*, Chang-Young Kwon** *Regular Members*

요 약

패스워드 인증 방안은 컴퓨터 시스템에서 사용자의 식별을 위해 가장 널리 사용되고 있다. 그러나 패스워드 시스템은 침입자가 쉽게 침입할 수 있다. 이러한 문제점을 해결하기 위해서는 사용자 인증 처리의 비밀성을 강화하는 3가지 범주의 기술을 채택한다. 본 논문에서는 기존의 다양한 패스워드 인증 방안을 설명하고, 패스워드를 저장하는 방법, 패스워드의 발전과정, 패스워드의 전송 등의 문제점을 지적한다. 제안하는 인증 방안은 패스워드 테이블 사용하지 않고 사용자 신원을 확인한다.

ABSTRACT

Password authentication is the most widely used mechanism for authentication legal users in computing systems. But it is easy for an intruder to enter the system. To overcome this problem, we should employ the technology of the third category to strengthen the security of the authentication process. In this paper, we will discuss various solutions to the password authentication problem. We will explain the aspects of storage, generation, and transmission on the password problem with those proposed scheme. Moreover, we will proposed user authentication system without using a password table.

Ⅰ. 서 론

해커의 공격에 대비해 이중 삼중의 안전장치를 구비하는 등 해커 방어에 세계적으로 가장 모범적인 기업으로 꼽혀왔던 Yahoo!가 2000년 2월 7일, 해커에게 공략 당했다. 이후 3일간 Buy.com(전자상거래 업체), Amazon(서적 등 쇼핑몰), E*TRADE (온라인 증권거래회사) 등 세계적인 인터넷 사이트에 대한 해커의 공격은 '사이버 아마겟돈(컴퓨터 시스템 대란)'이 닥칠 수도 있다는 가능성을 보여 주었으며 미국 하버드대의 인터넷 전자상거래 전문가인 로렌스 레시히 교수의 "많은 사람의 접속이 필요한 인터넷의 기본적인 특성을 악용한 것이어서 해킹을 막는 과정에서 인터넷 활용의 위축이 불가피하다." 라고까지 예상하고 있다. 특히, 이용자가 많은 사이트를 집중 공략하는 경우 최근 급신장 하는 인터넷 상거래는 불가피하게 큰 타격을 입게 될 것이다. 그러므로 인터넷 쇼핑몰을 운영하는 업체들은 전전긍긍하고 있다.

이런 현실 속에서 세계 최대의 소프트웨어 업체 마이크로소프트(MS)社의 중앙컴퓨터에 대한 해킹 사건에 대한 2000년 10월 로이터(샌프란시스코) 통신의 보도는 그 시사하는 바가 크다. 또한, 컴퓨터 전문가들은 포천지가 선정한 500대 기업이나 실리콘 밸리 기업들 가운데 방어체계가 취약하거나 허술한 많은 기업들이 정보 해킹을 당하고 있다고 지적한다. 일부 전문가들은 앞으로 컴퓨터 바이러스가 기업 정보를 빼내려는 의도를 가진 해킹 전문가들에게 중요한 무기가 되는 새로운 시대를 맞게 될 것으로 우려하고 있다.

* 동서울대학 전자계산과(jsyoo@haksan.dsc.ac.kr)
** 동서울대학 사무자동화과(cykwon@haksan.dsc.ac.kr)
논문번호 : T00038-0830, 접수일자 : 2000년 8월 30일

실리콘 밸리의 한 컴퓨터 보안업체 '시큐리파이(Securify)'의 보안 전문가 조엘 드 라 가자는 "해킹 사건의 80%는 십대들이 그냥 재미로 저지른 경우"이지만 "나머지 20%는 해킹을 시도하는 분명한 목표와 구체적인 계획이 있는 전문 해커들로 그 수는 점점 늘어나기 시작했다"고 지적했다. 샌프란시스코의 컴퓨터보안연구소(CSI)에 따르면 조사대상 기업 및 정부기관 10곳 중 9곳은 지난 해 해킹을 당한 적이 있었고, 이중 피해규모와 재정적 손실을 밝힌 42%의 피해총액은 2억6천500만달러에 이르고 있다. 그러나 이번 MS의 경우처럼 공개적인 망신과 주가 하락의 위험을 무릅쓰면서까지 해킹 사실을 밝히려는 기업체는 거의 없다는 점을 감안할 때 실제 피해사례는 훨씬 더 많을 것으로 전문가들은 보고 있다.

이런 상황에 초점을 맞추어 본 논문에서는 패스워드를 이용한 인증 방식에 대하여 심층적으로 분석한다. II 장에서는 패스워드 테이블을 이용한 인증 방식과 검증 테이블 방식 등 패스워드의 저장 방법에 대하여 논하고, III장에서는 앞장에서 패스워드 인증 방식에서의 문제점 즉, 패스워드 파일의 저장 및 전송에 대한 문제점을 동시에 해결하기 위한 방안으로 영지식 대화형 증명에 근거한 개인식별 프로토콜을 사용할 것을 제안한다. 이는 패스워드 테이블(파일/DB)이 필요 없는 방안이며 또한, 이 방식은 패스워드에 대한 정보가 통신채널에서 노출되지 않는 방식이다.

II. 패스워드 인증 방식

최근 인터넷이 급속도로 발전하고 컴퓨터 네트워크 시스템이 생활화되면서 컴퓨터 시스템에 내장되어 있는 데이터와 컴퓨터 자원의 공유가 가능하게 되었다. 그러나 컴퓨터 시스템 내부에 대한 침입자들에 의한 해킹으로 경제적 손실과 개인의 사생활 침해가 빈번히 발생하고 있는 실정이다. 따라서 컴퓨터 시스템 내부에 침입자들이 들어와 컴퓨터에 저장된 중요한 데이터를 파괴하고 변형하며 정보를 훔치는 피해를 막기 위한 컴퓨터 시스템 가입자 보호에 관한 연구가 활발히 진행되고 있다[1,2,3,4].

컴퓨터 시스템 가입자를 식별하기 위한 인증 방안은 3개의 영역으로 나눌 수 있다.

- 인간 고유의 특징 즉, 얼굴, 음성, 지문, 망막을 기반으로 한 시스템
- 패스워드와 같은 비밀 정보를 가지고 가입자를 식별하는 시스템
- 자기 카드, IC 카드, 키 등 특별한 물건으로 식별하는 시스템

3개의 영역 중에서 첫 번째는 가장 정확한 인증 방법이다. 그러나 인간의 신체를 식별하는 방법으로서 식별 시스템 장비와 프로그램 작성이 가장 복잡하며 비용도 많이 든다. 두 번째, 패스워드로 가입자를 식별하는 방법은 초기 컴퓨터부터 적용해온 방안으로서 가격이 저렴하고 가입자 검증 처리가 용이하다. 다른 사람에게 노출되기 문제점도 있다. 따라서 패스워드를 다른 사람에게 노출하지 말아야 한다. 이 문제를 극복하기 위해 비도가 높은 세 번째 범주의 기술을 채택하여야 한다[5,6]. 그러나 패스워드 인증 방식이 가장 일반적으로 널리 사용되고 있는 것이 현실이다. 그러므로 본고에서는 패스워드 인증 방식의 문제점에 대하여 지적하고 그 해결책을 제시하였다.

2.1. Plain Password table 이용

기존의 비밀 보호 방안 중에서 비용이 저렴하고 구현이 용이하며 사용자와 친숙한 패스워드가 가장 널리 사용되고 있다. 로그인 시 가입자의 ID와 그와 관련한 PW를 제출하면 검증하기 위해서 시스템은 패스워드 테이블에서 관련된 PW_i를 검색할 것이다. PW_i와 PW가 동일하다면 그 가입자는 정당한 권한을 가지게 되고 시스템 사용 권한을 가진다. 전적으로 이 안은 패스워드 테이블의 비밀 보호에 의존하고 있다. 이 안의 위험성은 패스워드 테이블을 컴퓨터 시스템 내부에 저장하는 것이다[7,8].

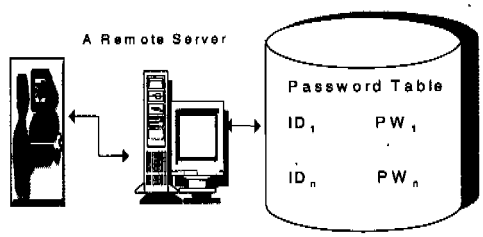


그림 1. 일반적인 패스워드 인증

예를 들어, 해킹 등의 방법으로 패스워드 테이블을 변조하거나 침입자가 시스템 패스워드를 읽고 나중에 로그인을 위하여 테이블에 위장한 패스워드를 추가하면 패스워드 시스템의 안전성은 파괴된다.

그러므로 패스워드 인증 방안이 채택되면 시스템의 비밀 보장하는 방법이 가장 중요한 문제가 된다. 패스워드 테이블이 여전히 위험하지만 패스워드 테이블이 부득이 존재하여야 되는 경우에는 다음 조건을 만족시켜야 시스템의 비밀을 보장할 수 있다.

(1) 패스워드는 패스워드 테이블에 평문 형태가 아닌 변형된 형태로 저장되어야 한다
(2) 해킹 등의 방법으로 패스워드 테이블에서 어떠한 정보를 획득하여도 침입자는 가입자의 패스워드를 추측할 수 없어야 된다.
(3) 패스워드 테이블을 교체하거나 변형하여도 시스템에 침입하려는 침입자에게 아무런 도움이 되지 않아야 한다.

2.2. Public Verification Table 이용

패스워드 테이블을 획득할 수 있는 방법은 많이 있다. 예를 들어, 메모리 덤프와 시스템 백업 테이블을 검색하여 패스워드 테이블을 획득할 수 있다. 침입자가 테이블 접근을 한 적이 있다면 그 시스템은 안전하지 않다. 가입자 ID와 패스워드, 가입자로 위장, 그리고 패스워드 추측 등 소모적인 공격이 있을 가능성이 있다.

그리고 침입자가 검증 테이블에 있는 정보를 변조하는 것을 막을 수가 없다. 메모리 보호 관점에서 보면, 시스템 내에 평문의 패스워드 파일을 저장하는 방법은 비밀 보호에 상당한 취약점을 가지고 있다. 패스워드 파일 관리는 시스템에 부하를 부가하게 된다. 가입자의 패스워드를 일방향 함수(One Way Function)나 암호 알고리즘으로 변환한다.

패스워드 테이블의 안전을 위해 일방향 함수를 제안한 것은 Evan이었다[9]. 직관적으로 일방향 함수는 적용하기가 쉬우나 복원이 어렵다.

함수 F : A → B 가 일방향 함수이면,
(1) A에 있는 모든 x에 대하여 F(x)는 쉽게 계산된다.
(2) B에 있는 모든 y = F(x)에 대하여 x의 계산은 어렵다.

가입자의 패스워드 x를 저장하는 대신에 시스템은 y = F(x) 값을 저장한다. 패스워드 테이블을 검증 테이블로 대신할 수 있다.

패스워드를 일방향 함수로 부호화하여도 검증 테이블은 공격당하기 쉬운 약점이 있다. 검증 테이블은 시스템에 예약된 특별한 공간에 저장할 필요가 있다. 원격 접속 시스템에서도 위장 침입 가능성이 존재한다. 침입자는 정당한 로그인 요청을 가로챌 수 있으며 합법적인 가입자처럼 후에 로그인 요청을 한다. 특히, 이 문제는 불안한 채널을 통하여 원격 접속하는 시스템에서 발생한다. 침입자는 임의의 x에 대한 F(x) 값을 생성하여 접속을 시도하거나 다른 일방향 함수 F'를 만들어 검증 테이블을 F'(x)로 변경하려는 시도를 할 수 있다.

2.3. Test Pattern Table 이용

패스워드는 컴퓨터에서 만들거나 가입자에 의해 자유롭게 선택한다. 컴퓨터에서 패스워드의 작성은 쉽고도 어려운 문제이다. 그러나 그 패스워드는 가입자가 기억하기 어렵다. 가입자가 패스워드를 쉽게 선택할 수 있다. 추측이 가능한 패스워드 선택은 피해야 한다. 그러므로 가입자는 쉽게 추측할 수 있다.

패스워드나 검증 테이블 저장의 필요성을 없애기 위해서 계정과 패스워드의 관계 함수를 만든다. 하나는 모든 패스워드와 계정간의 관계를 표현하는 함수를 고안하는 것이다. 다른 하나는 패스워드로부터 계정을 만드는 특정한 함수를 만드는 것이다. 패스워드와 계정간의 관계는 Chang과 Liaw의 해서 제안되었다. 가입자는 계정을 정규화하고 패스워드를 선택할 수 있었다. (ID와 PW)를 다항식으로 표현하였다. 그 후, 패스워드 테이블 대신에 함수를 저장하게 되었다[3, 10].

$$P(X) = a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots\cdots + a_1X + a_0$$

컴퓨터 내부에 다항식 함수를 이용하여 n개의 계수($a_{n-1}, a_{n-2}, \cdots\cdots a_0$)를 저장한다. 그러므로 패스워드 테이블을 저장할 필요는 없지만, 시스템 내에 동등한 데이터를 유지해야 함으로 컴퓨터 내부에 패스워드 테이블을 저장하지 않을 목적은 성취되지 않았다. 또한 이 방식은 새로운 가입자 등록이나 기존 가입자의 패스워드 변경시 계산량이 많은 것이 단점이다.

2.4. 패스워드 전송

일반적인 패스워드 인증 방식에서 패스워드를 전송할 때에 고려할 사항은 안전성 및 통신량이다. 터미널(클라이언트)과 센터(서버) 사이의 패스워드 전송은 통신채널에서의 도청 때문에 매우 위험하다. 이미 제안된 많은 방식에서는 도청 문제에 대하여는 고려하지 않았다. 그러나, 이 문제는 대부분 간

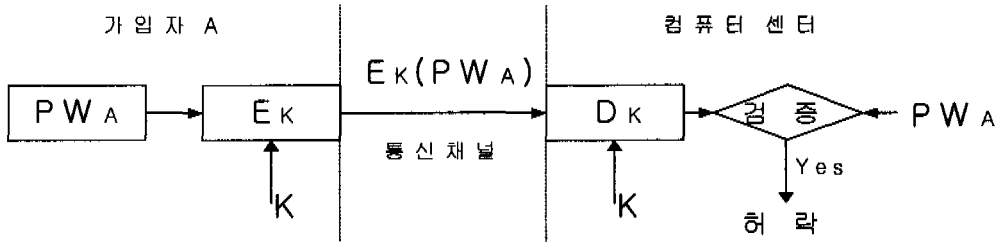


그림 2. 일반적인 패스워드 인증

과하고 넘어갈 수 있으나, 컴퓨터 통신망상에서 원격로그인하는 경우 도청 문제를 해결하여야 한다.

일반적인 패스워드 인증 방식에서는 도청문제를 해결하기 위해서는 그림과 같이 인증하면 된다. 가입자 A의 패스워드를 암호화하여 비보호 통신채널로 전송하면, 센터에서 복호화하여 저장되어 있는 패스워드와 검증하여 통신 세션을 허락하면 된다.

이와 같은 방법으로 도청의 문제는 해결 가능하나, 비보호 통신로에 패스워드와 관련된 정보가 전송된다는 것은 능동적인 공격자(해커 등)로부터 안전하다고 할 수 없으며, 더욱이 센터에 저장되어 있는 패스워드 파일의 저장 문제는 여전히 존재한다. 그러므로 본 논문에서는 센터에 패스워드 파일이 존재하지 않으면서 통신채널에 패스워드와 관련된 그 어떤 정보도 노출되지 않는 방안에 대한 강구가 필요하다.

Ⅲ. 패스워드 인증 방식의 문제점 해결 방안

앞에서 패스워드 인증 방식에서의 문제점 즉, 패스워드 파일의 저장 및 전송에 대한 문제점을 지적하였다. 이러한 문제점을 동시에 해결하기 위한 방안으로 암호학 영역에서 활발히 연구되고 있는 영지식 대화형 증명에 근거한 개인식별 프로토콜을 사용할 것을 제안하는 바이다. 계산이론 관점에서 패스워드 인증 방식이 속하는 NP 증명 방식에 대하여 논하고, NP 증명 방식을 일반화한 영지식 대화형 증명 방식에 대하여 기술한다. 끝으로 기존의 패스워드 인증 방식을 대체할 수 있는 영지식에 근거한 개인식별 프로토콜에 대하여 논하고자 한다.

3.1. *NP* 증명 방식

*NP*증명 방식은 대화형 통신이 가능하면서 증명자 P가 무한 계산 능력을 갖는 결정 튜링 기계와 검증자 V가 다항식 계산 능력을 갖는 결정 튜링 기계로 구성되며 증명자 P와 검증자 V는 *NP* 문제 X를 공통 입력으로 받아들인다. 무한한 계산 능력을 갖는 증명자 P가 문제 X의 해 α를 구하여 검증자 V에게 전송하면 다항식 계산 능력을 갖는 검증자 V가 X의 해인지 판단하는 방식을 *NP* 증명 방식이라고 한다[11].

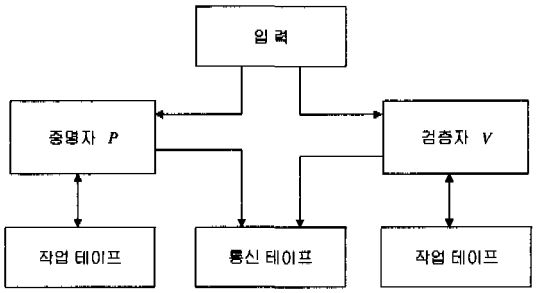


그림 3. *NP* 증명 방식

증명자 P는 입력 X를 받아 작업 테이프를 이용하여 문제 X의 해 α를 계산한다. 증명자 P는 계산된 해 α를 통신 테이프를 통하여 검증자 V에게 전송한다. 검증자 V는 증명자 P로부터 받은 문제 X의 해 α를 확인하여 증명자 P를 확인한다.

NP 증명 방식의 예로는 패스워드(password)를 이용한 사용자 인증을 들 수 있다. 컴퓨터 시스템 사용자 P가 컴퓨터 시스템 V에게 패스워드를 전송하면 컴퓨터 시스템은 이 패스워드가 컴퓨터 시스템 사용자의 정당한 패스워드인지 검증하여 인증하는 방식이다. 이와 같은 *NP*증명 방식은 증명자가 검증자에게 전송하는 정보 α가 너무나 중요하여 암호학의 입장에서 보면 그 적용 분야가 극히 제한될 수밖에 없다. 그러므로 *NP*증명 방식의 약점을 보완하기 위한 새로운 증명 방식이 필요하게 되었다.

3.2. 영지식 대화형 증명 방식

영지식 대화형 증명 방식은 *NP* 증명 방식을 두 가지 면에서 일반화시킨 증명 방식이며 암호화 프로토콜의 안전성 문제를 해결하기 위하여 제시된

모델이다[12]. 영지식 대화형 증명 방식이다. 즉, *NP* 증명 방식은 결정 튜링 기계상에서 정의되었으나 대화형 증명 방식은 확률 튜링 기계상에서 정의된다. 또한 *NP* 증명 방식은 증명자 *P*가 검증자 *V*에게 자신의 정보를 전송하는 일방향 방식이나 대화형 증명 방식은 검증자 *V*도 자신의 정보를 증명자 *P*에게 전송하는 양방향 방식이다.

먼저 대화형 튜링 기계는 한 개씩의 읽기 전용 테이프, 작업 테이프, 랜덤 테이프, 읽기 전용 테이프, 쓰기 전용 통신 테이프를 갖는다.

랜덤 테이프는 무한한 랜덤 비트들로 구성되어 있으며 왼쪽에서 오른쪽으로만 탐색이 가능하다. 대화형 튜링 기계가 동전을 던진다고 하는 것은 대화형 튜링 기계 자신의 랜덤 테이프에서 다음 비트를 읽는다는 것이다. 입력 테이프를 공유하는 대화형 튜링기계 *P*와 *V*의 순서쌍을 대화형 프로토콜이라 하고 (*P*, *V*)로 표시하며 구성은 그림 4.과 같다.

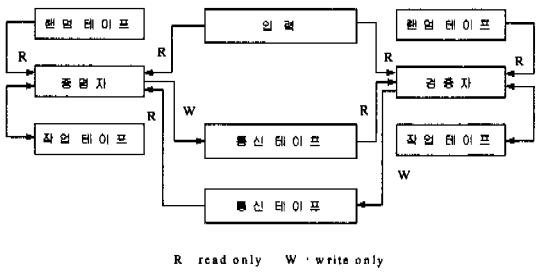


그림 4. 대화형 프로토콜

직관적으로 영지식 대화형 증명 방식을 설명하면, 증명자 P와 검증자 V가 대화(interactive)를 통하여 어떤 사실을 증명하는 방식으로 어떤 사실의 정당성에 관한 정보만을 교환하고 그 이외의 어떤 정보도 노출시키지 않는다는 의미를 내포하고 있다. 즉, 증명자(prover)가 자신만이 아는 비밀정보를 검증자(verifier)에게 직접 전송하지 않고, 자신의 비밀정보가 아닌 어떤 다른 정보를 전송하여 검증자에게 자신만이 비밀정보를 알고 있다는 것을 증명할 수 있는 방식으로 상대방 인증 방식에 있어서 가히 혁신적인 것이다. 이후 많은 영지식 대화형 증명 방식들이 발표되었으며 이러한 증명 방식들은 $P \neq NP$라는 가정 아래 *NP*에 속하는 언어들을 이용하여 상대방을 인증하는데 *NP*에 속하는 모든 언어는 영지식 대화형 증명 방식에 이용될 수 있음을 Goldreich, Micali와 Wigderson이 확인하였다[13].

영지식 대화형 증명 방식을 이용한 암호화 프로토콜은 그 안전성을 학문적으로 엄격하게 증명할 수 있는 방법이므로 최근 각종 암호화 프로토콜 구성시 영지식 대화형 증명 방식을 기본적인 도구로 사용하고 있다.

3.3. ZKIP에 근거한 개인식별 프로토콜

개인식별 문제는 암호학의 여러 분야에서 발생하는 매우 중요한 문제 중의 하나이다. 개인식별은 가입자 A가 가입자 B와 협조하여 A는 B에게 자신이 A임을 증명할 수 있으나, 제 3자인 C는 A로 위장하여 B에게 자신이 A라고 속일 수 없는 사용자 인증(entity authentication) 기능에 가입자 B도 제 3자 D에게 자신이 A라고 증명할 수 없는 조건이 추가된 기능이다[14].

Fiat-Shamir 개인식별 프로토콜(이하 FS 프로토콜)은 ZKIP의 개념에 Shamir 자신이 최초로 제안한 ID 개념을 첨가한 프로토콜이다. 이 프로토콜의 안전성은 충분히 큰 두 소수 p, q의 곱인 n의 소인수분해를 모를 때, 제곱근을 구하는 문제는 어려운 문제(NP 문제)라는 것에 근거한다.

사전 준비 과정에서 신뢰할 수 있는 센터는 소수 p, q 비밀리에 선택하고, 512 비트 이상의 $n = p \cdot q$을 공개한다. 카드발급 과정에서 센터는 합법적인 사용자에게 카드를 발급할 때 그 사용자에 관한 정보(이름, 주민등록번호, 주소 등)와 카드에 관한 정보(유효기간 등)를 결합한 ID_i를 준비하고, mod n 상에서 ID_i의 평방근을 계산하여 그 역수 S_i를 각 가입자의 비밀키로 한다. 사실, 모든 ID_i가 mod n 상에서 평방근을 갖지는 않으므로, 이 문제의 해결책으로 임의의 스트링이 입력되면 [0, n)이 출력되는 의사 랜덤 함수(pseudo random function) h를 선택하여 모든 가입자에게 공개하고 다음과 같이 비밀키를 생성한다.

① $P_j = h(ID_i, k_j)$ (j = 1, ..., m) 을 구한다.

② 이 중에서 k개의 평방잉여 선택, 각 P_j^{-1}의 가장 작은 제곱근 S_j를 k개 계산한다.

③ ID_i와 k개의 S_j, 각각의 j값을 스마트 카드에 담아 사용자에게 발급한다.

가입자 A와 가입자 B가 개인식별을 행하는 프로토콜은 다음과 같다.

프로토콜 3.1. FS 개인식별 프로토콜

순서 1-1. 가입자 A는 ID_A를 가입자 B에게 전송한다.

순서 2-1. 가입자 B는 $P_j = h(ID_A, k_j)$ (j = 1, ..., k)를 계산한다.

아래의 순서 3-1에서 순서 6-1을 t회 반복한다.

순서 3-1. 가입자 A는 $r \in_R Z_n^*$ 를 선택한다.

3-2. 가입자 A는 $x = r^2 \pmod n$를 계산한다.

3-3. 가입자 A는 x를 가입자 B에게 전송한다.

순서 4-1. 가입자 B는 $(d_1, ..., d_k) \in_R \{0, 1\}$ 를 선택한다.

4-2. 가입자 B는 가입자 A에게 $(d_1, ..., d_k)$를 전송한다.

순서 5-1. 가입자 A는 $y = r \cdot \prod_{d_j=1} S_j \pmod n$을 계산한다.

5-2. 가입자 A는 y를 가입자 B에게 전송한다.

순서 6-1. 가입자 B는 $x = y^2 \cdot \prod_{d_j=1} P_j \pmod n$이 성립하는지 검증한다.

가입자 A, B가 위의 프로토콜을 수행하면, 검증과정 $y^2 \cdot \prod_{d_j=1} P_j = r^2 \cdot \prod_{d_j=1} (S_j^2 \cdot P_j) = r^2 = x \pmod n$이 항상 성립한다. FS 프로토콜은 임의의 k, t에 대하여 영지식이며 안전성은 안전 파라메터 k, t에 의존한다(security level = 2^{-kt}). FS 프로토콜에서 t회 동안 보낼 모든 x 및 d를 1회에 전송하는 병렬 프로토콜은 영지식이 아니다. FS 프로토콜을 이용하면 비밀 정보(S_j : 패스워드)를 센터에 저장할 필요가 없으며 비보호 통신로 상에서 패스워드에 관련된 그 어떤 정보도 노출되지 않는다.

FS 프로토콜의 문제점은 현재 스마트 카드 프로세서의 제약 조건들은 사용 알고리즘의 선택시 엄격한 제한을 수반하게 되는데 비해 반복 횟수와 증명자가 많은 메모리를 필요로 한다는 것이다.

Ohta-Okamoto 개인식별 프로토콜(이하 OO 프로토콜)은 FS 프로토콜의 효율성을 개선한 프로토콜로 FS 프로토콜의 멱승 지수부를 기소수 L로 확장한 프로토콜이다. OO 프로토콜은 FS 프로토콜의 문제점인 증명자와 검증자 사이의 반복 횟수를 1회로 개선하였으며, 적은 메모리로 개인식별이 가능한 프로토콜이다. 그러나, 계산량에 있어서는 FS 프로토콜에 비하여 약 2 ~ 3배 정도 증가한다.

OO 개인식별 프로토콜은 사전 준비 과정에서 신뢰할 수 있는 센터가 소수 p, q를 비밀리에 선택하고, 그 곱인 n을 공개한다. 또한, $\phi(n)$과 서로소인 L를 선택하여 공개한다.

카드발급 과정에서 센터는 가입자의 ID_i를 준비하고, mod n 상에서 ID_i의 L승근을 계산하여 각 가입자의 비밀키 S_i로 한다.

프로토콜 3.2. OO 개인식별 프로토콜

순서 1-1. 가입자 A는 $r \in_R Z_n^*$ 를 선택한다.

1-2. 가입자 A는 $x = r^L \pmod n$를 계산한다.

1-3. 가입자 A는 ID_A와 x를 가입자 B에게 전송한다.

순서 2-1. 가입자 B는 $d \in_R Z_n$를 선택한다.

2-2. 가입자 B는 가입자 A에게 d를 전송한다.

순서 3-1. 가입자 A는 $y = r \cdot S_A^d \pmod n$을 계산한다.

3-2. 가입자 A는 y를 가입자 B에게 전송한다.

순서 4-1. 가입자 B는 $y^L = x \cdot ID_A^d \pmod n$이 성립하는지 검증한다.

가입자 A와 가입자 B가 위 프로토콜을 수행하면, 검증과정 $y^L = (r \cdot S_A^d)^L = (r \cdot (ID_A^{1/L})^d)^L = r^L \cdot ID_A^d = x \cdot ID_A^d \pmod n$이 항상 성립한다. FS 개인식별 프로토콜에 비하여 비밀키가 k개에서 1개로 줄어들어 비밀키 저장에 필요한 메모리를 감소시켰으며, FS 프로토콜에서는 순서 3-1에서 순서 6-1을 t회 반복하는 데 반하여 OO 프로토콜에서는 순서 1-1에서 순서 4-1을 1회 행하므로 통신 효율을 개선하였다. 이 프로토콜의 안전성은 안전 파라메터 L에 의존(security level = 1/L)하며 n의 소인수를 모르고 L 제곱근을 구하기 어렵다는 문제에 근거한다. OO 프로토콜을 이용하면 비밀 정보(S_j : 패스워드)를 센터에 저장할 필요가 없으며 비보호 통신로 상에서 패스워드에 관련된 그 어떤 정보도 노출되지 않는다. 이와 비슷한 형태인 Guillou-Quisquater 개인식별 프로토콜이 있으며 OO 프로토콜과 비교 분석하면 연구에 도움이 될 것이다.

Ⅳ. 결 론

해커의 공격에 대비해 이중 삼중의 안전장치를 구비하는 등 해커 방어에 세계적으로 가장 모범적인 기업으로 꼽혀왔던 Yahoo!나 MS가 해커에게 공략 당하는 현실이다. 1999년 정보통신부는 우수 쇼핑몰 지정제도를 도입키로 하고 업체의 신청을 받았다. 설명회에는 수백개 업체가 참석하여 성황을 이루었으나 보안 문제를 중점 점검한다는 평가기준이 알려지자 28개 업체만이 심사를 받겠다고 신청하였으며, 그중 심사를 통과한 업체는 10개에 불과했다. 업계에서는 보안시스템을 제대로 갖춘 업체는

5-10% 정도인 것으로 파악되고 있다.

또한, 국내 쇼핑몰의 경우 실제 거래가 일어나는 인터넷 쇼핑몰은 700-800개 정도이며 몇몇 업체를 제외하면 대부분 적자를 면하지 못하고 있는 실정이다. 또한, 월 500만원 이하의 매출을 올리는 업체가 80% 이상으로 보안 시스템에 투자하거나 안전장치를 마련하는 것은 꿈도 꾸지 못하는 것이 현실이다.

이런 상황에서 본고에서는 패스워드 인증 방식에서 패스워드 파일의 저장 및 전송에 대한 문제점에 대하여 지적하였으며, 이 문제점을 동시에 해결하기 위한 방안으로 암호학 영역에서 활발히 연구되고 있는 영지식 대화형 증명에 근거한 개인식별 프로토콜을 사용할 것을 제안하였다. OO 프로토콜을 패스워드 인증 방식에 활용할 때 FS 프로토콜를 활용하는 경우 보다 비밀키가 k개에서 1개로 줄어들어 비밀키 저장에 필요한 메모리를 감소시켰으며, 이 프로토콜의 안전성은 안전 파라메터 L에 의존(security level = 1/L)하며 n의 소인수를 모르고 L 제곱근을 구하기 어렵다는 문제에 근거한다.

향후 연구로는 보다 안전한 인증을 위하여 스마트 카드를 이용한 인증 방식에 관한 연구 및 국내 소규모 쇼핑몰에 적용하면 효율적인 개인식별 프로토콜에 대한 연구가 필요하다고 판단된다. 특히, 계산 능력이 적은 컴퓨터에서도 효율적인 개인식별을 할 수 있는 효율적인 개인식별 프로토콜 개발이 시급하다고 판단된다.

참 고 문 헌

[1] C.C. Chang and L.H. Wu, "A new password authentication scheme," Journal of Information Science and Engineering, pp.139-147, 1990.

[2] Tzong-Chen Wu,"Remote login authentication scheme based on a geometric approach," Computer Communications, Vol.18, No.12, pp.959-963, 1995.

[3] Jinn-Ke Jan, Yu-Yii Chen, "Paramita Wisdom" password authentication scheme without verification tables, "The Journal of System and Software 42, 45-57, 1998.

[4] 신 종태, 강 창구, 김 대호, "사용자 신분 확인을 위한 자동 패스워드 시스템 설계," 한국정보처리응용학회, 추계 학술발표논문집, 제 1권 제 2호, pp. 127-130, 1994.

[5] M. S. Hwang, "A remote password authentication scheme based on the digital signature method," International Journal Of Computer Mathematics, pp.657-666, 1999.

[6] L. Lamport, "Password authentication with insecure communication," Communications of ACM, Vol.24, pp.770-772, 1981.

[7] C.C. Chang and L.H. Wu, "A password authentication scheme based upon Rabin's public-key cryptosystem," Proceedings of the International Conference on Systems Management '90, Hong Kong, pp.425-429, 1990.

[8] C.H. Lin, C.C. Chang, T.C. Wu and R.C.T. Lee, "Password authentication using Newton's in interpolating polynomials," Information Systems, Vol.16, No.1, pp.97-102, 1991.

[9] A. Evans, W. Kantrowitz and E. Weiss, "A user authentication system not requiring secrecy in the computer," Communications of the ACM, Vol.17, pp.437-442, 1974.

[10] C.S. Laih, L. Harn and D. Huang, "Password authentication using quadratic residues," Proceedings of the International computer Symposium 1988, Taipei, Taiwan, R.O.C., pp.1484-1489, 1988.

[11] S.Goldwasser, S.Micali, C.Rackoff, "The Knowledge Complexity of Interactive Proof Systems," The 17th ACM STOC, pp.291-304, 1985.

[12] 권 창영, 이 인숙, 원 동호, "영지식 대화형 증명 방식 및 응용 프로토콜," 대한전자공학회 학회지, 제 20권, 제 2호, pp.101-114, 1993.

[13] O.Goldreich, S.Micali, A.Wigderson, "Proofs that Yield Nothing But their Validity," Proceedings of Crypto '86, pp.171-185, 1986. "Proofs that Yield Nothing But Their Validity or All Languages in NP Have Zero Knowledge Proofs," Tech. Rep.#544, Israel Institute of Technology, Department of Computer Science, 1989.

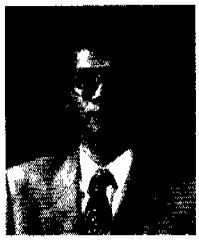
[14] 권 창영, 원 동호, "Self-Certified 공개키 방식에 관한 고찰," 한국통신정보보호학회 학회지, pp.80-86, 1993.

유 종 상(Jong-Sang Yu)

1982년 : 중앙대학교 전자계산
학과 졸업(이학사)
1987년 : 중앙대학교 대학원
전자계산과 졸업(이학석사)
2000년 : 단국대학교 대학원
박사과정 수료

1982년~1986년 : 범양상선(주) 전산실
1987년~1992년 : 경주전문대학 전산과 조교수
1992년~현재 : 동서울대학 전자계산과 부교수
<주관심 분야> Fault Tolerance, 암호학

권 창 영(Chang-Young Kwon)



1983년 : 성균관대학교
수학교육과 졸업
1991년 : 성균관대학교 대학원
정보공학과 졸업(공학석사)
1994년 : 성균관대학교 대학원
정보공학과 졸업(공학박사)

1982년~1988년 : (주)KOLON 정보 SYSTEM실 팀장
1993년~현재 : 동서울대학 사무자동화과 조교수
<주관심 분야> 암호이론, 암호기술, 정보관리