공개키 암호 기법을 이용한 패스워드 기반의 원거리 사용자 인증 프로토콜

(Password-Based Authentication Protocol for Remote Access using Public Key Cryptography)

최 은 정 † 김 찬 오 † 송 주 석 ††

(EunJeong Choi) (ChanOe Kim) (JooSeok Song)

요 약 인터넷과 같이 신뢰할 수 없는 네트워크를 통한 통신에서 비밀성과 무결성 뿐만 아니라 원거리 사용자 인증은 시스템의 보안에서 중요한 부분이다. 그러나 사용자 인증정보로서 인간이 기억할 수 있는 패스워드의 사용은 패스워드의 선택범위가 사용자의 기억에 제한 받는 낮은 비도(Entropy) 때문에 공격자의 오프라인 사전공격에 취약하다.

본 논문은 원거리 사용자 인증과 키 교환에 적합한 새로운 패스워드 인증 및 키 협상 프로토콜을 제안한다. 이 프로토콜은 오프라인 사전공격을 예방할 수 있으며 공격자에게 패스워드가 노출되더라도 이전 세션의 복호화나 이후 세션키의 손상에 영향을 미치지 않는 PFS(Perfect Forward Secrecy)를 제공한다. 또한 사용자의 패스워드가 서버의 패스워드 데이타베이스 파일에 순수하게 패스워드 자체로 저장되지 않기 때문에 공격자가 패스워드 데이타베이스를 획득하더라도 직접적으로 프로토콜의 안전성을 손상하지 않으며 직접 서버에 접근을 요청할 수 없다. 또한 PKI 및 키서버와 같은 제3의 신뢰기관을 이용하지 않기 때문에 단순인증에 적합하다. 따라서 이 프로토콜은 웹을 통한 홈뱅킹이나 사용자의 모바일 환경이 요구되는 셀룰러 폰, telnet이나 ftp와 같은 로긴 시스템, 기존 패스워드를 이용한 인증시스템 개선 등의 어플리케이션에 유용한 인증형태를 제공하며 인증정보가 장기간 저장될 필요성이 있어 위험하거나 실용적이지 못한 경우와 SSL(Secure-Sockets Layer), SET(Secure Electronic Transactions), IPSEC(Internet Protocol Security Protocol) 서비스에 추가될 수 있다.

키워드 : 공개키 암호 시스템, 패스워드, 인증, 사전공격, 이산로그, Diffie-Hellman 키교환

Abstract User authentication, including confidentiality, integrity over untrusted networks, is an important part of security for systems that allow remote access. Using human-memorable password for remote user authentication is not easy due to the low entropy of the password, which constrained by the memory of the user.

This paper presents a new password authentication and key agreement protocol suitable for authenticating users and exchanging keys over an insecure channel. The new protocol resists the dictionary attack and offers perfect forward secrecy, which means that revealing the password to an attacker does not help him obtain the session keys of past sessions against future compromises. Additionally user passwords are stored in a form that is not plaintext-equivalent to the password itself, so an attacker who captures the password database cannot use it directly to compromise security and gain immediate access to the server. It does not have to resort to a PKI or trusted third party such as a key server or arbitrator. So no keys and certificates stored on the users computer. Further desirable properties are to minimize setup time by keeping the number of flows and the computation time. This is very useful in application which secure password authentication is required such as home banking through web, SSL, SET, IPSEC, telnet, ftp, and user mobile situation.

† 비 회 원 : 연세대학교 컴퓨터공학과
eunjeong-1@hanmail.net
captin33@emerald.yonsei.ac.kr
†† 종신회원 : 연세대학교 컴퓨터공학과 교수
jssong@emerald.yonsei.ac.kr
논문접수 : 2001년 7월 16일
심사완료 : 2002년 10월 18일

Key words : Public-Key Cryptography, Password, Authentication, Dictionary Attack, Discrete Logarithm Problem, Diffie-Hellman Key Exchange

1. 서 론

공개 네트워크를 통하여 안전한 통신을 원하는 사용자는 기밀성과 무결성이 보장된 상태에서 자신이 정당한 사용자임을 증명하는 인증절차가 요구된다. 네트워크에서 개체 인증이란 어떤 사용자나 어플리케이션이 실제로 신고된 바로 그 사람(또는 것)인지를 판단하는 절차를 말하며 이러한 인증 서비스는 다음과 같은 3가지 형태의 기본정보를 기반으로 이루어진다[1].

- 개인이 소유하고 있는 것(Token based authentication: 스마트카드, 토큰)
- 개인의 신체적 특성(Biometric authentication : 지문, 홍채, 목소리)
- 개인이 알고 있는 것 (Knowledge based authentication: 패스워드, PIN)

개인이나 조직체에서 허용하는 신뢰와 안전성 수준에 따라 네트워크 보안의 강·약 레벨은 다양하게 구현될 수 있으나 일반적으로 두가지 형태의 인증정보가 결합되어 인증서비스가 제공될것을 권장하고 있다. 이렇게 두 종류 이상의 인증정보가 결합되어 인증 서비스를 제공할 때 '강한 인증 서비스'를 제공한다라고 말한다. 특히 지식기반 인증은 사용자의 기억에 의존하여 별도의 하드웨어 장치 없이도 구현가능하고, 스마트카드나 토큰 등의 분실 및 도난 문제를 예방할 수 있으므로 단순성, 편리성, 저 비용, 이동성의 장점 때문에 가장 광범위하게 사용되어지고 있다. 원거리 사용자 인증을 위한 패스워드 기반 인증 프로토콜에서 사용자는 신뢰하는 인증 서버와 기억하기 쉬운 비밀정보인 패스워드만을 공유하면 된다. 이 패스워드를 이용하여 사용자의 신원을 인증한 후 세션키를 교환하므로서 이후 세션에 대한 암호화 채널을 형성하거나 키 생성을 위한 초기값으로 사용한다. 따라서 패스워드는 사용자는 기억하기는 쉽지만 공격자가 추측하기는 어려운 정보로 선택되어져야 한다[2]. 그러나 본질적으로 패스워드가 인간의 기억력에 의존하여 선택범위와 길이가 제한되므로 공격자가 사용자의 패스워드로 유추되는 단어들을 사전화하고 이러한 사전을 이용하여 연속적으로 암호문에 복호화를 수행하는 사전 공격(Dictionary Attack)에 취약하다[1,3].

본 논문에서는 사용자 인증과 세션키 교환을 위해 서버 측에서는 공개키와 개인키를 가지며 사용자 측에서는 자신의 인증정보로서 기억하기 쉬운 패스워드만을 소유한 비대칭적 환경을 가정하며 이러한 환경에서 패스워드와 공개키 암호알고리듬을 이용하여 오프라인 패스워드 유추공격과 재사용 공격을 예방할 수 있는 프로토콜을 제안한다. 또한 상호인증과 공격자에게 패스워드의 노출이 이전 세션의 복호화나 이후 세션키의 손상에 영향을 미치지 않는 PFS(Perfect Forward Secrecy)를 지원하며 서버가 패스워드에 대한 해쉬값만을 저장하므로 공격자가 서버의 패스워드 데이타베이스를 획득하더라도 직접적으로 프로토콜의 안전성을 손상하지 않으며 직접 서버에 접근을 요청할 수 없다. 또한 PKI(Public Key Infrastructure) 및 키서버와 같은 제3의 신뢰기관을 이용하지 않기 때문에 단순(light-weight) 인증에 적합하며 프로토콜 흐름 단계와 계산시간을 최소화하였다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 패스워드 인증 프로토콜 및 취약성을 살펴보고 강한 인증을 제공하기 위해 공개키와 결합된 대표적인 프로토콜인 DH-EKE(Diffie-Hellman Encrypted Key Exchange)에 대하여 살펴본다. 3장에서는 공개키 암호 시스템을 이용한 패스워드 기반 인증프로토콜을 제안한다. 4장에서는 제안한 프로토콜의 안전성을 분석해보고 기존의 프로토콜과의 성능을 비교해 본다. 5장에서 결론 및 향후 연구 방향을 제시한다.

1.1 패스워드 기반 인증 프로토콜 설계시 요구사항

1.1.1 기본적인 안전성 요구사항

- 오프라인 사전 공격 예방(off-line password dictionary attack)

패스워드 기반 인증 프로토콜의 가장 큰 취약점은 패스워드에 대한 사전공격이다. 이러한 공격은 다시 오프라인 공격과 온라인 공격으로 구분될 수 있는데 오프라인 공격은 사용자와 서버 사이에서 정당한 인증이 수행되는 동안에 전송되는 메시지를 캡처하여 오프라인 상태에서 공격자가 추측한 패스워드 사전의 목록을 차례로 대입하는 전수조사를 통해서 유추한 패스워드와 비교하는 공격이다. 이 공격은 사용자가 다수의 컴퓨팅 장치들을 병렬로 연결하여 높은 수준의 컴퓨팅 능력이 제공되는 상태에서 수행하므로 상당히 높은 성공률을 보인다. 온라인 공격은 사용자가 각기 다른 패스워드를 사용하여 서버에 온라인 상태에서 인증을 시도하는 공격인데 오프라인 공격에 비해 로그나 시스템 스캐닝을 통해 서버 측에서 발견되어지기 쉽고 공격자가 운용할 수 있는 컴퓨팅 능력도 제한되는 단점이 있다. 이러한 온라

인 공격은 일정한 시간 동안 실패하는 인증 횟수를 제한하므로서 쉽게 예방할 수 있다[4].

· 전향적 보안성(Perfect Forward Secrecy) 제공

강력한 패스워드 기반 인증 시스템에서 패스워드를 이용하여 사용자의 신원을 인증한 이후에 세션 암호화 채널 형성에 사용될 세션키를 협상한다. 만약 공격자가 사용자의 키 입력을 가로채는 스니핑(sniffing) 및 백도어(backdoor)와 같은 프로그램을 이용하거나 물리적인 방법을 이용하여 현재 사용되는 패스워드를 획득한다면 이 패스워드를 이용하여 이전에 협상된 세션키를 통해 암호화 채널을 형성하여 교환된 세션의 메시지를 획득할 수 있다. 특히 대부분의 사용자들의 패스워드 변경주기가 한달 이상이므로 새로운 패스워드로 변경되기 이전에 노출될 가능성이 더욱 크다. 따라서 공격자가 패스워드를 획득하더라도 이전에 협의한 세션키들에 대한 안전성이 보장되는 것을 말한다.

· Denning-Sacco 공격 예방

프로토콜 수행중에 협상되는 세션키는 세션이 종료된 후에는 더이상 의미가 없으므로 삭제된다. 그러나 공격자가 전수조사를 비롯한 여러 다른 방법을 이용하여 세션키를 획득한 경우에 이것을 이용하여 이후 세션의 세션키를 획득하려고 시도하거나 패스워드에 대한 오프라인 사전 공격을 수행할 수 있다. 따라서 공격자가 세션키를 획득하더라도 패스워드에 대한 어떠한 정보도 노출되지 않으며 이후에 사용될 세션키에 대한 안전성이 보장되는 것을 말한다.

· 서버의 패스워드 손상에 대한 대책

서버가 저장하는 패스워드 검증자의 복사값에 따라 평문 등가 기법과 검증자 기반 기법으로 나누어지며, 평문 등가 기법은 서버가 사용자의 패스워드를 저장하는 대칭적 기법이며, 검증자 기반 기법은 서버가 사용자의 패스워드에 대한 검증자로 일 방향 함수 f를 이용하여 $f(P)$만을 저장하는 비대칭적 환경이다. 검증자 기반 기법은 평문 등가 기법에 비해 서버의 패스워드 파일이 손상되더라도 공격자가 검증자를 이용하여 순수한 패스워드를 획득할 수 없기 때문에 사용자로 위장할 수 없다. 따라서 평문 등가 기법에 비해서 더욱 안전하다.

· 명시적 키 인증성

패스워드 기반의 인증키 교환 프로토콜은 키 협상 단계와 키 확인 단계로 나누어진다. 키 협상은 세션키를 공유하기 위한 단계이며, 키 확인 단계는 두 당사자가 동일한 키를 공유하고 있음을 확인하는 단계이다. 따라서 패스워드로 상호 인증한 후에 세션키의 교환과 확인이 이루어진다.

1.1.2 프로토콜 성능 요구사항

· 메시지 교환 횟수를 최소화한다.

· 산술적 계산 및 암호화 횟수를 최소화한다.

· 전송 비트 수를 최소화한다.

· 온라인 계산량이 감소하도록 사전계산을 가능하게 한다.

2. 패스워드 기반의 인증 기법

2.1 전통적인 기법

2.1.1 단순 패스워드 전송 기법

현재 UNIX 시스템의 Telnet, FTP, Web 어플리케이션의 원거리 사용자 인증에서 사용되는 방법으로 사용자가 평문형태나 일방향 해쉬함수를 이용하여 패스워드의 이미지를 전송하고 서버 측에서는 이 전송된 메시지가 서버가 저장하고 있는 패스워드 이미지와의 동일함을 확인하므로서 검증하는 방법이다. 가장 큰 취약점은 네트워크 도청자들에 의해 수행될 수 있는 스니핑 툴에 취약하다는 점이다.

2.1.2 요구/응답(Challenge/Response) 기법

가. 사용자는 자신의 ID와 랜덤 메시지 x_1를 서버에게 전송한다.

나. 서버는 랜덤 메시지 x_2를 사용자에게 전송한다.

다. 사용자는 자신이 만든 x_1, 서버로부터 받은 랜덤 메시지 x_2, 사전 공유한 패스워드를 이용하여 응답를 생성하여 서버에게 전송한다. 서버도 사용자와 동일한 계산을 이용하여 동일한 응답 값을 생성하므로서 사용자를 검증한다.

이 프로토콜은 인증 요청마다 새로운 랜덤메시지를 사용하므로 공격자의 단순 재사용 공격(Replay attack)을 예방할 수 있으나 인증이 성공했을 경우 요구 및 응답 메시지를 공격자가 가로채서 자신이 유추한 패스워드 사전으로 전수조사(Brute-force)를 수행하여 동일한 응답이 생성되는지를 확인하므로서 패스워드가 노출될 가능성이 있다[4].

2.1.3 커버로스(Kerberos) 인증기법

커버로스 V4와 V5에서 패스워드는 초기 서비스 요청 티켓의 암호화에 사용된다. 티켓에 포함된 데이타는 사전공격을 수행하여 각기 다른 패스워드 값으로 복호화를 시도할 경우 검증 가능한 데이타들이다. V4 방법은 어떤 사용자가 언제라도 서비스 요구 티켓을 요청한 후 사전공격을 수행할 수 있으므로 요구/응답 프로토콜보다 더욱 취약하며 V5가 타임스탬프와 같은 여러 가지 형태의 사전인증(Pre-authentication)을 제공하지만 여전히 사전공격에 취약하다[2,5].

2.1.4 일회용 패스워드(One Time Passwords)

일회용 패스워드는 서버에 인증을 요청할 때마다 재사용이 불가능한 다른 패스워드를 사용하도록 하므로서 도청에 의한 사전공격과 재사용 공격을 예방할 수 있다. 만일 침입

자가 네트워 도청을 통해서 원타임 패스워드를 알아내더라도 차후 인증에서 더이상 사용되지 않기때문에 획득한 패스워드는 의미가 없다. 이러한 일회용 패스워드 시스템을 구현하기 위한 방법으로는 다음과 같은 것이 있다.

- 양측의 동기화 시간을 이용한 Time-Stamp 사용
- 양측 패스워드 리스트 내의 위치를 동기화하여 패스워드 사용

IETF OTP(One Time Password) 워킹그룹에서는 원 타임 패스워드 인증 기법들에 대해서 여러 벤더들과의 상호 운용성을 개선하기 위해서 RFC 1938(A One-Time Password System)을 작성했다. 그러나 이러한 모든 패스워드 기반의 인증방법은 오프라인 사전공격에 취약하며 공개키 지원 패스워드 인증 형태만이 공격자의 오프라인 사전 공격을 예방할 수 있다[4].

2.2 강력한 패스워드 인증기법(DH-EKE)

1992년에 Bellovin과 Merritt는 대칭키 암호와 공개키 암호를 결합하여 공격자가 유추한 패스워드의 정당성을 검증할 정보가 불충분한 EKE(Encrypted Key Exchange)라는 새로운 프로토콜을 제안하였다. EKE는 두 당사자들이 패스워드에서 비롯된 대칭키를 이용하여 그들의 임시 공개키를 암호화하는 형태이며 여러 변형된 형태로 발전되었고 가장 단순한 형태가 DH-EKE이다[3].

DH-EKE는 전통적인 Diffie-Hellman 키 협상 프로토콜이 제공할 수 없는 인증을 패스워드가 제공하는 프로토콜이다. 즉 전송되는 공개키 속성들을 인증정보인 패스워드로 암호화하여 중간자 공격을 예방하며, 오프라인 사전공격으로부터 패스워드를 보호한다. 프로토콜 수행 절차는 다음과 같이 이루어진다.

가. A는 R_A를 생성하고 패스워드 P를 대칭키 암호시스템의 암호화 키로 사용하여 $g^{R_A}(\mathrm{mod}\,p)$를 암호화한 값 $P(g^{R_A}(\mathrm{mod}\,p))$를 전송한다.

A, $P(g^{R_A}(\mathrm{mod}\,p))$ (DH-1단계)

여기서 R_A가 난수이므로 유추된 P'에 대한 어떤 정보도 노출시키지 않으며 A는 평문형태로 전송된다. 만약 A가 P로 암호화되어 전송된다면 공격자가 유추한 P'으로 암호문을 복호화하였을 경우 A를 확인하므로서 P'의 정당성이 검증 가능하므로 P에 대한 정보를 노출하게 된다.

나. B는 R_B를 생성하고 $g^{R_B}(\mathrm{mod}\,p)$를 계산한다. 또한 $P(g^{R_A}(\mathrm{mod}\,p))$를 P로 복호화하여 $R=g^{R_A R_B}(\mathrm{mod}\,p)$를 계산하고, 상호인증을 위해 $challenge_B$를 생성하여 R를 대칭키 암호시스템의 암호화 키로 사용하여 암호화한 값 $R(challenge_B)$을 전송한다.

$P(g^{R_B}(\mathrm{mod}\,p))$, $R(challenge_B)$ (DH-2단계)

다. A는 P를 사용하여 $g^{R_B}(\mathrm{mod}\,p)$를 복호화하고 R을 생성하여 $R(challenge_B)$를 복호화할 수 있다. A는 임의의 $challenge_A$를 생성하여 $R(challenge_B, challenge_A)$를 전송한다.

라. B는 $R(challenge_B, challenge_A)$를 복호화하여 $challenge_B$가 제대로 돌아왔는지를 검증하고 $R(challenge_A)$를 전송하므로서 상호인증을 완성한다.

만약 공격자가 네트워크를 도청한다 하더라도 공격자가 유추한 패스워드 P'의 정당성을 검증할 수 있는 유용한 정보를 획득할 수 없으며 시스템 성능향상을 위해 DH-1의 메시지가 평문형태로 전송되더라도 공격자가 R_A의 값을 모르면 상호인증을 위한 DH-2의 $challenge_B$에 대한 응답을 할 수 없다. 또한 유추한 패스워드가 정확하더라도 $g^{R_A}(\mathrm{mod}\,p)$, $g^{R_B}(\mathrm{mod}\,p)$만을 알게 되므로 이들 정보만으로는 이산대수 문제의 어려움에 의하여 세션키에 대한 정보를 획득할 수 없다.

DH-EKE는 RSA나 ElGamal과 같은 다른 암호시스템을 이용하여 EKE를 구현할 경우와는 다르게 키 협상과정 자체가 무작위의 세션키를 생성하므로 세션키를 전송하는 과정이 별도로 고려되지 않아도 된다. 그러나 DH EKE는 서버측이 패스워드를 평문형태로 저장하기 때문에 만약 서버의 파일이 손상되면 패스워드를 획득한 공격자는 사용자로 위장할 수 있다. 따라서 이를 보완하기 위하여 전자서명과 패스워드의 해쉬값을 이용하여 이를 예방하는 최초의 검증자 기반 패스워드 인증 프로토콜인 A-EKE(Augmented Encrypted Key Exchange)가 제안되었다[6]. 또한 1998년에 영지식 증명(Zero Knowledge Proof)을 이용한 최초의 패스워드 인증 프로토콜인 SRP(Secure Remote Password) 프로토콜이 제안되었다[7].

3. 제안하는 패스워드 기반의 인증 모델

3.1 표기법

A, AS	정당한 실체 (사용자, 인증 서버)
ID_A , ID_{Server}	실체의 신원 (Identification)
P	사용자가 기억하는 패스워드
$H(P)$	패스워드의 해쉬값
PK_{server}	서버의 공개키
R	세션키
V	대칭키 암호시스템의 키
$[M]^{PK_{Server}}$	메시지 M을 공개키 PK_{server}를 이용하여 암호화한 값

Nonce	랜덤하게 선택한 비트 스트링
$[M]^V$, $[M]^R$	메시지 M을 각각 V, R를 키로 이용한 블록 암호문
g	유한체 $GF(P)$의 원시근
p	큰 소수(1024 비트 이상)

3.2 가정(Assumption)

- 사용자는 서버에게 인증을 시도하기 이전에 패스워드 P를 생성하여 $g^{H(P)} \bmod p$를 계산하고 서버는 패스워드 검증자로 $g^{H(P)} \bmod p$를 안전한 저장장치에 저장한다.
- 인증 서버는 공개키 암호시스템을 사용하고 인증 서버의 공개키(PK_{server})는 LDAP(Lightweight Directory Access Protocol) 디렉토리나 사용자들이 접근 가능한 공개 디렉토리에 저장하여 모든 사용자들이 쉽게 접근할 수 있도록하며 개인키는 안전하게 보관되어야 한다.
- 프로토콜에 사용되는 대칭키 암호 알고리듬, 해쉬 알고리듬, 공개키 암호 알고리듬의 충분히 큰 소수 p와 생성자 g값은 사용자와 인증 서버간에 합상되어 있으며 $\bmod p$ 표기는 생략한다.
- 사용자와 인증 서버는 *Nonce*를 생성할 수 있는 랜덤비트 생성기를 가지며 프로토콜에 선택되어지는 *Nonce*는 모두 해쉬함수 H의 특정길이를 갖는 비트 스트링이다.

3.3 프로토콜 묘사

1단계 : $A \rightarrow AS$: ID_A, $[\ Nonce_1 \oplus H(g^{H(P)})\ ]^{PK}$

2단계 : $AS \rightarrow A$: ID_{Server}, $[\ Nonce_1, Nonce_2, R\ ]^V$

$$V = g^x \bmod p$$

$$x = Nonce_1 \oplus H(g^{H(P)})$$

3단계 : $A \rightarrow AS$: $[\ Nonce_2 \oplus H(P)\ ]^R$

가. 1단계 : 사용자는 난수 $Nonce_1$를 생성하여 인증 서버와 공유하는 패스워드 검증자 $H(g^{H(P)})$와 $X\ OR$ 연산한 다음 서버의 공개키로 암호화하여 인증 서버에게 전송한다.

나. 2단계 : 인증 서버는 자신의 개인키를 이용하여 사용자가 전송한 메시지를 복호화하여 $Nonce_1 \oplus H(g^{H(P)})$를 구한다음 이 값을 이용하여 x와 V를 생성한다. 또한 자신이 소유한 $H(g^{H(P)})$를 가지고 $X\ OR$ 연산하여 $Nonce_1$를 생성한다. V를 대칭키 암호시스템의 암호화 키로 사용하여 이 값과 자신이 생성한 난수$Nonce_2$, R를 암호화한 후 사용자에게 전송하고, x는 패스워드에 대한 정보를 노출할 위험이 있으므로 버린다.

다. 3단계 : 사용자도 x와 V를 생성하여 전송받은 메시지를 복호화한 후 $Nonce_1$을 확인하므로서 인증 서버가 정당한 패스워드 검증자를 소유하고 있음을 확인한다. 사용자는 자신이 기억하고 있는 패스워드를 이용하여 재생산한 $H(P)$와 $Nonce_2$를 $X\ OR$ 연산한 후 R를 대칭키 암호시스템의 암호화 키로 사용하여 암호화한 후 인증 서버에게 전송한다.

이 메시지를 전송받은 인증 서버는 R을 이용하여 복호화한 후 $Nonce_2$를 이용하여 $H(P)$를 구한다. 이 값을 지수로 하는 $g^{H(P)} \bmod p$를 계산한 후 자신이 저장하고 있는 패스워드 검증자와 비교하여 일치하면 인증 서버는 사용자가 정당한 패스워드를 소유하고 있음을 확인할 수 있으므로 상호 인증이 완료된다.

4. 인증 모델의 분석

4.1 안전성 분석

- 오프라인 사전 공격 예방

패스워드 기반 인증 프로토콜의 가장 큰 취약점은 공격자의 패스워드 사전 공격이며 컴퓨팅 장비의 발전으로 공격자가 오프라인에서 활용할 수 있는 계산 능력이 증가하여 더욱 위협적이다. 따라서 이를 예방하기 위해서는 정당한 인증 프로토콜 실행중에 공격자가 도청과 같은 수동적 공격으로 패스워드에 대한 어떠한 정보도 획득할 수 없어야 한다. 또한 패스워드가 검증이나 예측이 가능한 평문 메시지에 대하여 직접적인 암호화키로 사용된다면 평문과 암호문을 획득한 공격자는 자신이 추측한 패스워드 목록을 반복적으로 키로 사용하여 동일한 암호문이 생성되는지를 확인하는 검증문 공격을 수행할 수 있으므로 이러한 방법도 피해야 한다.

제안한 패스워드 기반 인증 프로토콜의 구성요소는 신분 정보(identification)외에는 랜덤한 값이거나 일방향 해쉬된 값이므로 공격자의 수동적 공격에 대해 패스워드 정보는 안전하다. 3단계에서 암호화되는 $H(P)$가 추측 가능한 평문 메시지의 해쉬값이기 때문에 랜덤한 비트 스트링 $Nonce_2$와 $X\ OR$ 연산을 수행하여 검증 불가능한 난수 메시지로 변경한 후 V를 사용하여 암호화하였다. 따라서 제안한 프로토콜에서 공격자는 자신이 추측하여 만든 패스워드 목록에 포함된 p'의 정당성을 오프라인에서 검증할 수 없다.

· 전향적 보안성 제공

제안한 프로토콜에서는 사용자와 서버사이에 공유하는 패스워드가 노출되더라도 각 세션의 암호화에 사용되는 세션키가 패스워드와 독립적으로 서버의 난수 발생시스템에 의해 생성되므로 공격자가 이전에 사용된 세션키를 획득하는 것은 불가능하다. 또한 1단계에서 $H(g^{H(P)})$값이 $Nonce_1$과 X OR 연산되어 서버의 공개키로 암호화되었기 때문에 x와 V를 획득할 수 없으며 따라서 R에 대한 정보가 노출되지 않는다.

· Denning-Sacco 공격 예방

제안한 프로토콜에서는 공격자가 세션키 R을 획득하더라도 3단계에서 $H(P)$가 $Nonce_2$와 X OR 연산되어 있으므로 패스워드에 대한 정보가 노출되지 않는다. 또한 각 세션마다 세션키는 랜덤하게 선택되어지므로 이전의 세션키로 이후의 세션키를 획득하는 것은 불가능하다.

· 서버파일의 손상

대부분의 UNIX 시스템에서 패스워드에 대한 검증자는 패스워드에 대한 일방향 해쉬값 형태로 저장되며 허가된 일부에게만 shadow 파일형태의 읽기가 가능하도록 통제되고 있다. 그러나 트로이 목마와 같은 악성 프로그램에 감염되거나 악의적인 내부 사용자에 의해 저장 장치가 손상되는 경우에 패스워드 검증 파일이 공격자에게 노출될 수 있으며 이 패스워드를 획득한 공격자는 정당한 사용자로 위장할 수 있다.

제안한 프로토콜은 검증자 기반 인증을 제공하므로 노출시 프로토콜의 안전성 손상을 최소화할 수 있다. 공격자가 $g^{H(P)}$를 획득하더라도 이산대수 문제의 어려움에 기반하여 3단계에서 $H(P)$를 생성할 수 없으므로 사용자로 위장할 수 없다. 또한 인증 서버는 3단계에서 사용자에게 전송받은 메시지에서 유추한 $g^{H(P)}$를 저장하고 있는 패스워드 검증자와 비교하므로서 서버가 손상되었는지 확인할 수 있다.

· 명시적 키 검증 및 상호 인증

패스워드 기반 원거리 사용자 인증에서 중간자 공격은 사용자에게는 패스워드 검증자를 소유한 정당한 서버처럼 위장하고 서버에게는 정당한 패스워드를 소유한 사용자로 위장하는 공격이다[8]. 이러한 공격에 대한 대응책으로는 각 개체들이 신뢰하는 TTP의 개인키에 기반하여 발행하는 인증서를 이용하거나 TTP가 두 개체간에 세션키를 직접 생성하여 전송하는 것이 있다. 또한 Rivest와 Shamir에 의해 제안된 인터락(interlock) 프로토콜과 각자의 전자 서명된 키를 교환하거나 두 개체간에 정당한 키를 소유하였음을 상호 검증하는 방법들이 있다. 그러나 제안하는 프로토콜에서처럼 통신하는 두 개체간에 명시적으로 인증된 키를 보유하고 있음을 확신하도록 상호 인증하는 방법이 가장 손쉬운 방법이다.

제안한 프로토콜에서는 사용자가 2단계에서 $Nonce_1$을 검증하여 인증 서버가 정당한 패스워드 검증자와 세션키를 저장하고 있음을 확인하므로서 일방향 인증이 가능하다. 3단계에서 인증 서버는 사용자가 전송한 $H(P)$를 검증하여 자신의 패스워드 검증자 정보가 노출되었는지를 확인할 수 있으며 또한 사용자가 정당한 패스워드와 세션키를 보유하고 있음을 명시적으로 확인할 수 있다.

4.2 제안한 프로토콜의 성능 분석

공개 네트워크를 통하여 안전한 통신을 원하는 사용자는 암호 통신을 위하여 사전에 공개된 통신로를 통하여 키를 공유하는 과정이 필요하며 상호간에 동일한 세션키를 소유하고 있음을 확인하기 위해 여러번의 메시지 교환을 필요로한다. 표 1에서 제안한 프로토콜과 기존 프로토콜과의 메시지 교환 횟수를 비교해 본다.

표 1 각 프로토콜의 메시지 교환 횟수

프로토콜 종류	DH-EKE	SRP	A-EKE	제안 프로토콜
메시지 교환 횟수	4	6	7	3

표 1에서 제시한 바와 같이 패스워드에 기반하여 명시적으로 세션키를 교환하기 위해 A-EKE 프로토콜은 DH-EKE 프로토콜에 전자서명을 수행하는 단계가 추가되므로 가장 많은 메시지 교환을 필요로 한다. 제안된 프로토콜은 부하가 가장 많은 메시지 교환 횟수를 최소화 했으므로 성능면에서 효율적이다. 또한 성능에 영향을 미치는 중요한 또다른 요인인 사용자측에 필요한 모듈러 지수승 계산도 훨씬 효율적이라는 것을 표 2에서 알 수 있다.

제안된 프로토콜은 표 2에서 제시한 바와 같이 사용자측에 온라인 상에서 요구되어지는 모듈러 지수승의 계산은 모두 사전 계산이 가능하기 때문에 계산량의 부담이 훨씬줄어든다. 또한 인증 서버의 공개키로 메시지를 암호화하는 1단계도 사전 계산이 가능하므로 온라인 상에서는 전송받은 메시지를 서버가 개인키로 복호화하는 계산량만 증가된다고 볼 수 있다.

표 2 프로토콜 계산시 사용자측에 필요한 모듈러 지수승의 횟수

모듈러 지수승	DH-EKE	제안 프로토콜
요구되어지는 모듈러 지수승 총 횟수	2	1
사전에 계산 가능한 모듈러 지수승 횟수	1	1

5. 결론 및 향후 연구 방향

본 논문은 원거리 사용자 인증을 위한 직접 인증의 형태로서 서버가 공개키 암호시스템의 공개키와 개인키를 소유하고 사용자는 자신의 인증정보로서 단순히 기억하기 쉬운 패스워드만을 소유한 비대칭적 상황에서 오프라인 패스워드 유추공격을 예방하고 중간자 공격 예방을 위한 상호인증과 세션키의 교환, 공격자가 패스워드를 획득하더라도 이전 세션을 복호화할 수 없는 전향적 보안성 제공 및 세션키의 노출을 통한 패스워드의 유추방지를 제공하며 서버의 패스워드 파일이 손상되더라도 공격자가 직접 패스워드를 획득할 수 없는 검증자 기반 인증을 제공하는 프로토콜을 제안하고 그 안전성에 대하여 고려해 보았다. 이러한 인증 프로토콜은 보안성이 요구되는 웹을 통한 홈뱅킹 어플리케이션이나 기존의 telnet, ftp와 같은 네트워크 로긴 시스템, 이동성이 요구되는 휴대폰과 같은 소형장치에서의 인증에 사용될 수 있으며 SSL, IPSEC, SET과 같은 어플리케이션에서도 유용하게 사용될 수 있다[9].

본 논문의 추가적인 연구 방향을 살펴보면 대칭키 암호 시스템을 사용하는 프로토콜에 비하여 수행 속도가 저하되는데 이에 대한 공식화된 수행속도 비교가 이루어져야 하며 안전성이 특정한 암호알고리듬이나 함수에 의존하지 않아야 한다. 또한 사용자들이 서버의 공개키를 획득하기 위한 PKI 환경에서의 적용방안등에 대한 연구가 고려되어야 한다.

참 고 문 헌

[1] Thomas Wu. "The Secure Remote Password Protocol," 1998 Internet Society Network and Distributed System Security Symposium, San Diego, March 1998, pp97-98.

[2] Barry Jaspan, "Dual workfactor Encrypted Key Exchange: Efficiently Preventing Password Chaining and Dictionary Attacks," Sixth USENIX UNIX Security Symposium, July 1996.

[3] S.M.Bellovin and M.Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attack," Proceedings of the I.E.E.E. Symposium on Research in Security and Privacy, Oakland, May 1992.

[4] Shai Halevi, Hugo Krawczyk, "public-key cryptography and password protocols," ACM Transactions on Information and System Security, Vol.2, No.3, August 1999, pp 230-268.

[5] B. Schneier, "Applied Cryptography, 2nd Edition," John Wiley & Sons, 1995, pp52-55.

[6] Steven M. Bellovin, Michael Merritt, "Augmented Encrypted Key and Exchange : a Password-Based Protocol Secure Against Dictionary Attacks Password File Compromise," ACM Conference on Computer and Communications Security, 1993.

[7] Thomas Wu. "The Secure Remote Password Protocol," in Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium, San Diego, CA, March 1998, pp.97-111.

[8] W. Stalling, "Cryptography and Network Security," Prentice-Hall, 1999, pp303-311.

[9] Peter Buhler and Thomas Eirich, "Secure Password Based Cipher Suite for TLS," Proc. of the Symposium on Network and Distributed Systems Security Symposium, February 2000.

[10] David Jablon, "Public Key Methods for Shared Secret Authentication," RSA '98 Crypto Track Talk, January 14, 1998, http://www.integritysciences.com/rsa98/sld034.html

최 은 정

2000년 2월 연세대학교 수학과 이학박사 2001년 1월 ~ 2002년 11월 연세대학교 컴퓨터공학과 Post. doc

김 찬 오

1995년 2월 금오공과대학교 전자공학과 학사. 2002년 2월 연세대학교 공과대학 컴퓨터과학과 석사. 2002년 9월~현재 육군 부사관학교 전산장교 재직. 관심분야는 암호학, 네트워크 프로토콜, 시스템 보안

송 주 석

1976년 서울대학교 전기공학과 학사 1979년 한국과학원 전기 및 전자공학과 석사. 1988년 Univ. of California Berkley 전산과학 박사. 1979년~1982년 한국 전기통신 연구소 전임 연구원. 1982년 중앙 전기 주식회사 개발 자문. 1988년~1989년 Naval Postgraduate School 조교수. 1989년~현재 연세대학교 컴퓨터공학과 교수. 관심분야는 컴퓨터 네트워크, 프로토콜 공학, 정보통신, 분산운영체제