通信情報保護學會誌
第8卷 第1號. 1998. 3

전산망에서의 패스워드 누출방지 기술 고찰

A Study on the Prevention of Password Exposure in a Computer Network

은 유 진*, 김 기 현*, 이 홍 섭**

요 약

본고에서는 최근 전산망에서 빈번하게 발생하고 있는 패스워드 도용에 대한 기술적 대책을 수립하기 전에 반드시 고찰해보아야 할 관련 기술들을 살펴보고자 한다. 또한, 각 관련 기술에 대한 보안 취약성을 분석하여 대응 기술을 개발하는데 있어서도, 이에 대한 기술적 이해를 돕고자 한다.

1. 서 론

오늘날 세계 각국의 통신망이 상호 연결되어 인터넷을 통한 정보의 교환이 일반화되어 가고 있는 반면 개인정보의 누출, 전산망 해킹 등 그 역기능 현상 또한 심각한 사회문제로 대두되고 있다. 그 동안 국내에서 발생한 대표적인 해킹 행위는 주로 단순 침입, ID 도용, 자료 절취, 자료 변조 및 파괴 등이며 외국의 해킹 실태는 국내에 비하여 매우 심각한 실정이다.

사용자의 ID와 패스워드를 인증 기반으로 하고 있는 현재의 유닉스(UNIX) 시스템에서 패스워드의 누출은 많은 위험성을 내포하고 있다. 최근 네트워크를 감청하거나 ID와 패스워드를 도용하기 위하여 스니퍼나 IP 스푸핑(spoofing) 등을 이용한 해킹 방법이 많이 사용되고 있다. 또한 국내에서 발생한 해킹 사례의 많은 부분들이 타인의 ID와 패스워드를 도용하거나 이를 이용하여 해킹하는 사례가 주류를 이루고 있다. '96년 9월의 경우 인터넷 서비스 망에 홈뱅킹 이용자의 패스워드와 ID를 가로챌 수 있는 변형 Telnet 프로그램을 설치하여 계좌이체를 시도하다 검거된 사례도 발생하였다.

이처럼 패스워드 도용을 이용한 불법 접속 시도 등 각종 위협에서 전산망을 안전하게 운용하기 위하여 사용자의 패스워드 누출 및 도용 방지, 사용자 신분위장 및 불법 접속 시도 방지, 그리고 PC 통신망, 금융망 등에 적용 가능한 전산망 원격 사용자 인증 기술의 확보가 필요하다.

이미 미국 및 선진 외국에서는 1980년대부

* 한국정보보호센터 기술본부 연구원
** 한국정보보호센터 기술본부장

터 이에 관한 연구를 시작, 일회용 패스워드라는 기술적인 개념을 도입하여 지속적인 연구개발을 통하여 1990년대에 이르러서는 Bellcore의 S/KEY를 비롯하여, 미해군연구소(U. S. Naval Research Laboratories)의 OPIE(One-time Password In Everything), 네덜란드의 Eindhoven 공과대학에서 Venema 프로젝트-TcpWrapper, SATAN등으로 알려져 있다-의 일환으로 개발된 LogDaemon등이 구현되어 현재, 다양한 분야의 신분확인 및 인증에 활용되어지고 있는 실정이다.

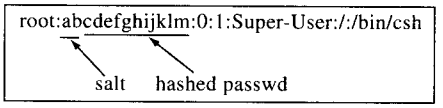
이에, 국내에서도 학계를 비롯하여 산업계 및 연구기관들이 이에 대한 기술적인 필요성 및 자주성을 확보하는 차원에서 이에 대한 연구개발이 이루어지고 있다.

2. UNIX 패스워드 시스템의 분석

기존 유닉스 시스템은 패스워드를 보관하는데 있어서, 치명적인 약점들을 많이 드러내고 있다. 이를 보강하기 위한 여러 가지 방법들이 제안되고 개선되어져 왔지만, 실제로 패스워드를 계속해서 사용하기 때문에 통신로 상에서의 도청(Eavesdropping)공격이나 재시도(Replay) 공격으로부터는 안전하지 못하다. 이에, 유닉스 패스워드 시스템의 패스워드 인증 방법을 분석하고, 공격에 취약한 면을 살펴보고자 한다.

2.1 UNIX 패스워드 시스템

일반적으로 UNIX 패스워드 시스템의 패스워드는 해쉬 형식으로 저장되어진다. 이 해쉬함수는 단 방향 함수이며 DES(Data Encryption Standard)의 변형된 버전이라 말할 수 있다. 일반적으로 패스워드는 "/etc/passwd" 파일에 저장된다. 패스워드 파일의 구조는 다음의 (그림 1)과 같다.



(그림 1) 유닉스 패스워드 파일의 구조

해쉬를 위한 라이브러리 함수로는 crypt(3) 함수가 사용되어진다. 패스워드를 해쉬하는 방법은 다음과 같다.[1]

- "salt"로 사용하기 위한 랜덤한 값 12비트를 생성한다.
- 0 비트의 메시지를 암호화하기 위한 키로써 패스워드를 사용한다.(DES를 25번 반복수행)
- 암호화의 결과에 "salt"를 앞에 붙인다.
- 프린트할 수 있는 형식으로 변환한다.

위와 같이 패스워드를 생성해서 "/etc/passwd" 파일에 저장한 후, 사용자의 로그인 요청이 있을 경우 입력으로 들어오는 사용자의 패스워드를 위와 같은 절차를 거쳐 결과 값을 얻게 된다. 이 결과 값을 가지고 "/etc/passwd" 파일에 있는 값을 비교하여 일치하면 사용자의 시스템 로그인을 허락하게 된다.

2.2 UNIX 패스워드 시스템의 취약점

위와 같이 전통적인 UNIX 시스템의 패스워드 인증 시스템은 오랜 기간이 지나면서 다음과 같은 여러 가지 취약점들이 나타나게 되었다.[2]

1) 패스워드는 평문으로 전달되어진다.

대부분의 UNIX 패스워드 인증 시스템에서

는 사용자에 의해 입력된 패스워드는 패스워드를 요구한 컴퓨터로 네트워크를 통해 평문(Cleartext)으로 전달되어진다. 이 방법은 이제 기술의 발달로 꼭 도청 장비가 아니더라도 간단한 소프트웨어를 통해서 어렵지 않게 도청할 수 있다.

2) 인증이 단 방향으로만 수행된다.

UNIX 패스워드 인증 시스템의 동작은 호스트 측에서 일방적으로 수행되어지기 때문에 호스트가 패스워드를 사용자에게 물어 볼 수 있지만, 사용자는 그들이 정말로 정당한 호스트와 통신을 하는 지의 여부는 알 수 없다. 사용자가 패스워드를 제공하기 전에 어떠한 시험도 할 수가 없는 것이다.

이것은 아주 심각한 문제인데, 예를 들어 사용자가 컴퓨터 단말에 앉아 응용 서비스 제공을 호스트 측에 요구하였다고 가정하자. 패스워드 입력 프롬프트가 화면에 나타났지만 과연 이것이 정당한 호스트로부터 생성된 것인지의 여부는 증명할 수가 없다. 이 패스워드 입력 프롬프트는 공격자에 의해 가장된 응용 프로그램일 수도 있으며, 다른 컴퓨터에 의해 보여지는 속임수 일 수도 있는 것이다.

3) 비밀정보는 호스트에 보관한다.

사용자의 패스워드 관련 정보를 호스트에 보관하고 있음으로 인해, 패스워드 파일이 누출되게 되면, 공격자는 이 패스워드 파일을 이용하여 사전(Dictionary) 공격을 여러 대의 컴퓨터를 이용해서 쉽게 할 수 있다.[7] 기술의 발전에 따라 컴퓨터의 연산능력이 향상되어 암호화하고 비교하는 일련의 과정이 1ms이하로 떨어지게 되었다.[4][5] 이것은 하나의 워크스테이션에서 250,000단어의 사전을 비교하는 시간이 5분이면 된다는 것을 의미한다.

이것은 다시 DES 알고리즘을 하드웨어로 구현하였을 경우 5ms로 줄어들게 되어 250,000단어의 사전을 비교하는데 1.5초면 된다.[6][8] 그래서 패스워드 파일을 누구나 읽지 못하도록 Sun Microsystem에서는 "shadow" 패스워드 파일을 제안하여 "root"만이 접근 가능하도록 하였으나, 이 또한 최근 해킹 기술의 발전에 따라 "root" 권한을 획득하여 이 파일을 크랙하는 사건들이 일어나고 있다.

3. 기존 일회용 패스워드 시스템의 비교 · 분석

앞서 살펴보았듯이 유닉스 패스워드 시스템의 단점이 계속해서 부각되어짐에 따라 사용자의 신분확인에 신뢰성을 더하기 위해, 전산망을 통해서는 사용자의 비밀정보가 오가는 것을 지양하고 사용자의 비밀정보를 이용해 단 한번의 유효성을 가지도록 하는 패스워드를 사용하게 되었다.

이처럼 여러 가지 패스워드 공격으로부터 신분확인 절차에 대한 안전성을 제공하는 일회용 패스워드 방식(One-Time Passwords Scheme)이 도입되어 현재까지 다음과 같은 다양한 방식이 제안되어 실제로 사용되기에 이르렀다.

- ○ 시간동기(Time Synchronous) 방식
- ○ DES 도전-응전(Challenge-Response) 방식
- ○ 공개키 방식
- ○ S/Key 일회용 패스워드 시스템

하지만, 이러한 방식들조차도 공격의 대상에서 벗어나지 못하고, 취약점을 드러내고 있다. 이번 장에서는 이러한 방식들을 기술적으로 살펴보고, 이 방식들이 어떤 공격 위협성으로부터 노출이 되어있는지를 알아보고자 한다.

3.1 일회용 패스워드 인증 시스템의 역사[9]

일회용 패스워드 시스템을 생성하기 위해 해쉬 함수를 사용하는 것은 Leslie Lamport에 의해 1980년에 제안되었다. 일회용 패스워드 시스템의 첫 번째 구현은 Bellcore로 알려진 Bell Communication Research Center에 의해 S/KEY 라는 이름으로 1991년에 개발되었다. Neil Haller와 John Walden이 이 개발에 참여하였고, Phil Karn에 의해 제안되어졌다.

S/KEY에 대한 상세한 설명은 RFC1760에 찾아볼 수 있다. 초기에 S/KEY는 해쉬 알고리즘으로 DES(Data Encryption Standard)를 사용하여 일회용 패스워드 인증을 구현하였다. 하지만, 그 당시 8088 시스템으로는 연산 속도를 감당할 수가 없어서 그 대신에 일회용 패스워드의 암호화된 파일을 사용하였다. 이 방법은 MD4 메시지 다이제스트 알고리즘을 기반으로 하는 시스템으로 다시 개발되어 RFC1320에 소개되었다.

이것은 다시 MD5 알고리즘으로 개선되어 RFC1321로 발표되었다. MD4가 예상외로 연산속도가 빨라서 cryptoanalytic 공격의 성공 가능성이 있음으로 인해 연산속도를 어느 정도 느리게 하고 이러한 연산 기능을 제공하기 위해 기본적인 설계를 약간 변경한 것이다.

1995년에 IETF(Internet Engineering Task Force)는 일회용 패스워드의 표준을 만드는 작업을 시작하였다. Neil Haller를 의장으로 하는 working committee에서 이것의 이름을 One Time Password System(OTP)으로 하였으며, 1996년에 RFC1938로 제정되었다.

3.2 시간동기(Time Synchronous) 방식[10]

Time-Synchronous Scheme은 매분마다(이 시간 간격은 네트워크 관리자에 의해 정해진다.) 하나씩의 난수를 생성하기 위해 난수 생성 알고리즘과 64비트 크기의 비밀키가 필요하다. 각각의 사용자에게는 특정키가 할당되어져 있는데, 이것은 지능형 토큰과 인증 서버의 데이터 베이스에 저장되어 진다.

사용자가 응용 서비스를 제공받기 위해 응용 서버에 로그인을 시도하면, 서버는 4개의 숫자로 이루어진 PIN(Personal Identification Number)과 6개의 숫자로 이루어진 난수를 요구하게 된다. 6개의 숫자로 이루어진 난수는 토큰으로부터 생성되어진다. 토큰에서 생성되어지는 난수는 토큰 안에 저장되어 있던 비밀키와 시간을 초기 값으로 하여 토큰 안의 알고리즘을 통해 만들어진다.

이렇게 만들어진 10개의 숫자가 서버로 가게 되면, 서버는 4개의 숫자(PIN)를 인덱스로 하여 서버의 데이터 베이스에서 해당 비밀키를 찾는다. 이런 다음 서버 측에서도 알고리즘에 시간과 비밀키를 넣어 생성된 6개의 랜덤 숫자들을 수신된 6개의 랜덤 숫자와 일치하는지를 검사하여, 그 두 개의 숫자들이 서로 일치하게 되면 서비스에 대한 이용 권한을 부여하게 되어 사용자 인증 절차가 끝나게 된다. Time-Synchronous Scheme에 대한 자세한 동작과정을 (그림 2)에서 볼 수 있다.

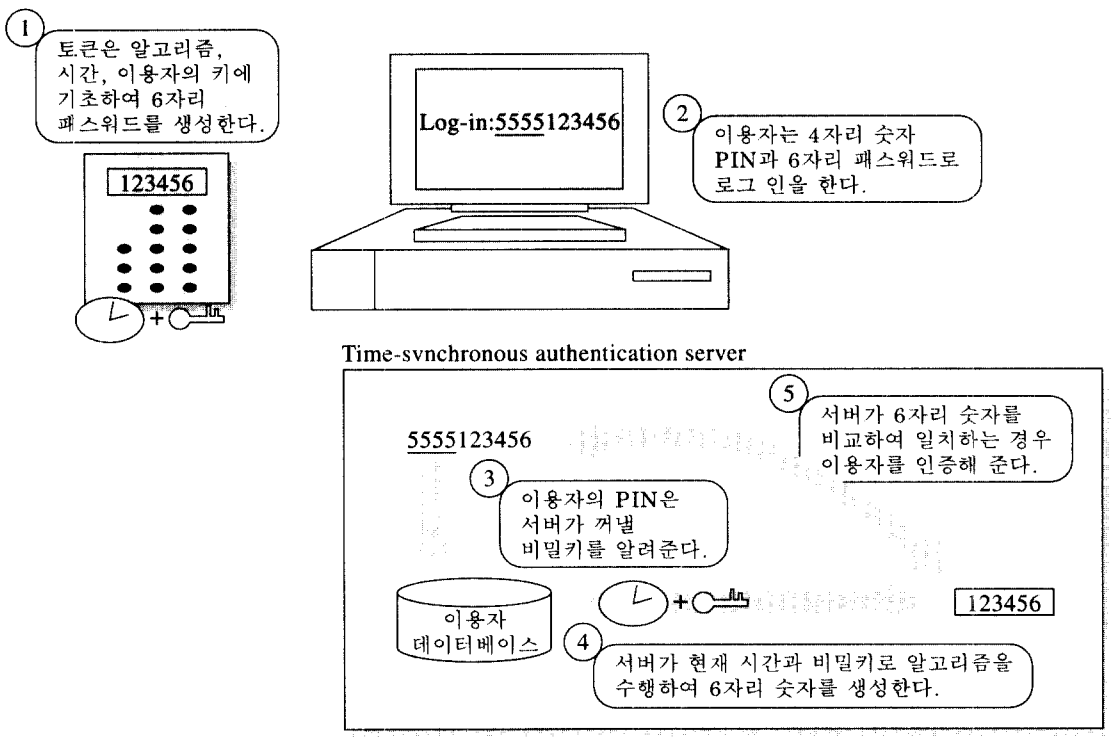
하지만 이 스킴에는 난수를 일치시키기 위해 시간에 대한 동기가 보장되어야 한다는 문제점이 존재한다. 예를 들어 서버는 캘리포니아에 있고, 토큰은 런던에 있을 경우, 시간에 대한 동기는 보장 될 수가 없을 것이다. 물론 시간 동기에 관한 문제는 약간의 부담은 있지만, Greenwich의 표준시간을 양쪽 장치에 프로그램 함으로써 해결되어 질 수는 있다.

그러나 더욱 심각한 문제는 소위 시간 편차(Time Slippage)라 불리는 것에 있다. 토큰이라는 것이 일회용이 아니고 일반적으로 수년간에 걸쳐 사용되어지는 장치이기 때문에, 하루에 단 몇 초만이라도 늦어지거나 빨라진다

면 토큰과 서버간에 동기는 또한 보장 될 수 없게 되는 것이다.

또 한가지 시간에 관련된 문제가 도사리고 있다. 토큰에서 생성된 난수가 여기서는 패스워드로 사용되어지는데, 이 패스워드에는 60초간의 유효시간이 있게 된다. 만약 해커가 네트워크 상의 패스워드를 60초안에 도청을 시도하여 PIN과 패스워드를 훔쳐 다른 서버에 접속을 시도한다면 사용자 인증에 성공하게 되는 것이다.

위와 같이 Time-Synchronous Scheme은 여러 가지의 문제점을 가지고 있어서 이를 해결하기 위한 부담이 너무 크다는 단점이 있다. (그림 2)에서 Time-Synchronous 방식에 대한 세부 작동 절차를 자세히 보여주고 있다.



(그림 2) Time-Synchronous 방식

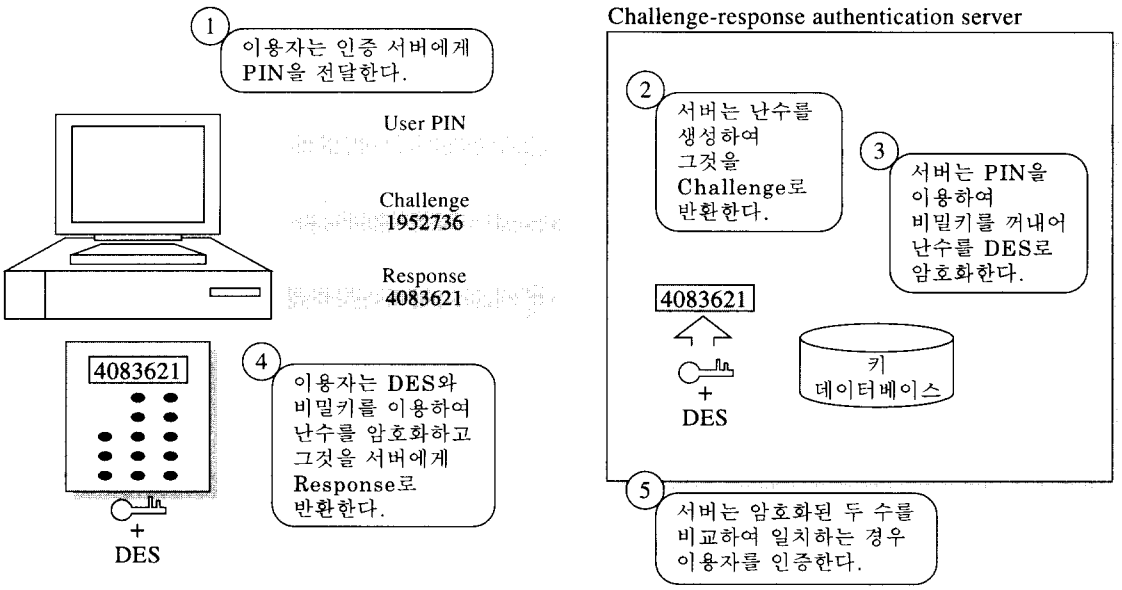
3.3 DES 도전-응전 (Challenge-Response) 방식

이 방법은 사용자가 인증 요구와 함께 사용자 식별 번호(PIN)를 인증 서버에게 전달하면, 인증 서버는 난수를 생성하여 challenge로 사용자에게 전달한다. 이와 동시에 인증 서버는 이용자의 사용자 식별 번호에 해당하는 패스워드를 키 데이터 베이스에서 꺼내 이것을 이용하여 난수의 암호화를 시작한다. Challenge를 받은 사용자는 그것을 자신의 패스워드로 암호화하여 response로 인증 서버에게 반환하다. 사용자로부터 response를 받은 인증 서버는 서버 자신이 계산한 값과 수신된 response 값을 비교하여 일치하는 경우에 사용자를 정당한 사용자로 인증하게 된다. 아래의 그림에서 그 절차들

을 잘 보여주고 있다.

Challenge-Response Scheme은 여러 번의 절차로 인해 다소 느리다는 단점이 있기는 하지만, Time-Synchronous Scheme에 비해 복잡성이 덜하고 안전성이 높기 때문에 최근 이 방법을 적용한 인증 시스템이 국외에서 많이 개발되고 있는 실정이다.

(그림 3)에서 그 동작 절차를 자세히 보여주고 있다.



(그림 3) DES Challenge-Response 방식

3.4 공개키 방식

RSA 공개키 암호화 방식은 Rivest, Shamir, 및 Adleman에 의하여 제안된 것이다. RSA 공개키 암호화 방식의 암/복호화는 소수 p와 q의 곱인 합성수 n 상에서 모듈라 연산을 함으로써 이루어진다. 각 사용자는 십진수로 100자리 이상인 소수 p와 q를 선택하여 비밀히 간직하고 두 소수의 곱인 n을 모듈라 수로 공개한다. 식 (1) 처럼 n의 Euler 함수 $\varphi(n)$과 서로소인 d를

$$\gcd(d, \varphi(n))=1 \quad (1)$$

where $\varphi(n)=\phi(p)\cdot\phi(q)=(p-1)\cdot(q-1)$

$\phi(x)$ *is Euler totient function of an integer* x.

비밀키로 선택하고 공개 쌍 (e, n) 중 e는 식 (2)과 같이 계산하며 모든 사용자에게 공개된다. 두 통신자간에 이루어지는 암/복호화 과정은 식 (3)에서 처럼 이루어진다. 즉, 사용자 A가 평문 M을 암호화하여 사용자 B에게 전송하고자 할 때

$$e\cdot d \equiv 1(\text{mod } \phi(n)), \quad (2)$$

i.e., $e\cdot d=k\cdot\phi(n)+1$, for *some integer* k.

Encipherment: $c \equiv M^e(\text{mode } n)$, for *a message* M (3)

Decipherment: $M \equiv C^d \text{ (mod } n)$, for *a ciphertext* C

사용자 A는 B의 공개키를 사용하여 평문을 암호화한 후, 통신망을 통하여 암호문 C를 B

에게 전송한다. B는 자신의 비밀키로 수신한 암호문을 복호화 한다.

Euler의 정리로부터 n과 서로소인 임의의 정수 M(메시지)은 식 (4)와 같고

$$(M^{\phi(n)})^k \equiv 1(\text{mod } n), \text{ for } \textit{some integer } k \quad (4)$$

식(2)에 의하여 식 (3)의 복호화 과정은 식 (5)로 유도된다. 이것을 다시 식 (5)에 식 (4)를 대입하면 식(6)이 되어 결과적으로 복호화 과정이 증명된다.

$$M \equiv C^d \equiv M^{e \cdot d} \equiv M^{k \cdot \phi(n)+1}(\text{mod } n) \quad (5)$$

$$C^d \equiv M^{e \cdot \phi(n)+1} \equiv (M^{\phi(n)})^k \cdot M \equiv M(\text{mod } n) \quad (6)$$

RSA 공개키 암호법의 안전도는 합성수인 모듈라 수 n을 소인수 분해하는 난이도 비례한다. n을 소인수 분해하면 $\varphi(n)$을 알 수 있고 따라서 공개키로부터 비밀키가 분석될 수 있기 때문이다. 식 (7)은 합성수 n을 소인수 분해할 때 요구되는 연산 횟수를 나타낸다.

$$O(\exp(\sqrt{\ln n \ln \ln n})) \quad (7)$$

3.5 S/Key 일회용 패스워드 시스템

S/Key 일회용 패스워드 시스템은 미국의 Bellcore사에 의하여 개발된 일회용 패스워드 방식이며 IETF의 일회용 패스워드 인증 워킹 그룹에서 작성한 표준 RFC에 기술되어 있다. 또한 BorderWare 등 많은 방화벽 시스템에서 S/Key를 사용하고 있다.

1) S/Key 일회용 패스워드 시스템의 특징

S/Key 일회용 패스워드 시스템은 네트워크상의 도청(Eaveasdropping)이나 재시도(replay) 공격으로부터 안전한 인증 기능을 제공한다. 이 시스템은 기존의 one-time 혹은 multi-use 인증 시스템들에 비해 여러 가지 장점을 가지고 있다. S/Key 인증 시스템은 passive attack에 대해 사용자의 패스워드를 보호하기 위한 간단한 스킴이다.

이 제품은 거의 모든 UNIX 시스템에 추가적인 하드웨어 없이, 패스워드 정보를 저장하지 않고 쉽고 빠르게 설치할 수 있다. S/Key 시스템은 통신 기능을 가진 PC에도 사용이 가능하다. S/Key 일회용 패스워드 시스템의 특징을 요약해보면 다음과 같다.

- 도청공격에 안전하다.
- 사용하기에 개념적으로 간단하고 쉽다.
- 비밀 패스워드를 기억하도록 한다.
- 자동화되어질 수 있다.
- 알고리즘이 비밀이 아니다.
- 어떤 비밀 정보도 호스트에 보관되지 않는다.

2) S/Key 일회용 패스워드 시스템의 동작절차

S/Key 일회용 패스워드 시스템에는 두 가지 측면이 존재한다. 하나는 사용자 혹은 클라이언트 측면인데, 적절한 일회용 패스워드가 생성되어져야 한다. 다른 하나는 시스템 혹은 서버 측면으로, 일회용 패스워드가 검사되어져야 한다. 일회용 패스워드는 MD4 단방향 해쉬 함수를 이용해서 생성되고 검사되어진다. 이 시스템은 8바이트의 입력을 받아 8바이트의 출력을 얻도록 제작되었다.

일회용 패스워드는 단 방향 함수를 여러 번 적용함으로 계속해서 생성되어진다. 즉, 첫 번째 일회용 패스워드는 사용자의 비밀 패스워드(s)를 정해진 특정 수(n) 만큼의 단 방향 함수를 수행함으로 생성되어진다. n=4 라고 가정하면,

$$p(1)=f(f(f(f(s))))$$

다음 일회용 패스워드는 사용자의 패스워드를 단 방향 함수에 n-1번 수행함으로 생성되

어진다.

p(2) = f(f(f(s)))

일회용 패스워드 $p(i)$의 사용을 모니터하고 있는 도청 자는 다음 패스워드 $p(i+1)$를 생성해낼 수 없을 것이다. 처음 시점에서 사용자의 비밀키를 알지 못하면 도청이 불가능하게 된다.

처음에 호스트 컴퓨터는 수신한 일회용 패스워드의 복사 본을 저장하고, 그것을 단 방향 함수에 적용한다. 만약 그 결과가 시스템의 패스워드 파일 안에 저장된 복사본과 일치하지 않으면, 그 인증 요구는 실패하게 된다. 만약 그들이 일치하면, 시스템 패스워드 파일 안에 있는 사용자의 엔트리는 단 방향 함수의 마지막 실행 전에 저장되어 있던 일회용 패스워드의 복사 본으로 갱신되어진다.

사용자에 의해 수행된 단 방향 함수의 수가 하나씩 줄어들기 때문에, 어는 시점에 다다르면 사용자는 시스템을 재초기화 해야만 한다. 이것은 일련의 새로운 일회용 패스워드를 시작하기 위해 특별한 버전의 passwd 명령어 실행으로 이루어진다.

S/Key 일회용 패스워드 인증 시스템은 하나의 pass-phrase로부터 일련의 일회용 패스워드들을 생성하는데 계산 능력을 이용한다. 이 인증 시스템의 보안은 사용자에게만 알려져 있는 비밀 pass-phrase에 전적으로 의존하고 있다. 전체 비밀 정보는 어떤 계산 장치로도 찾아낼 수 없는 형태로 저장되어진다.

위에서 언급된 바와 같이, 일련의 일회용 패스워드는 컴퓨터를 사용하여 비밀 패스워드로부터 생성되어진다. 요구되어진 계산은 노트북이나 palm-top등을 포함하는 다양한 기종의 PC나 UNIX에서 수행되어진다. 한 벤더는 수요가 많을 경우 30$이하에서 신용카드 크기의 장치로 만들어질 수 있다고 말한다.

또한 이 프로그램은 플로피 디스크에 저장되어지고 수행되어질 수 있다. 이것은 비밀 패스워드를 잡아낼 수 있는 트로이 목마가 없는 신뢰하지 못하는 원격 컴퓨터에서도 작동이 가능하다. 이것은 미리 계산하여 몇 개의 일회용 패스워드를 프린트해서 사용할 수도 있다.

내부적으로 일회용 패스워드는 64비트 숫자이다. 64비트 숫자를 입력하는 것은 그리 좋지 못하다. 그래서 일회용 패스워드는 6개의 짧은 단어(1-4 letters)로 바뀌어진다. 각각의 단어는 2048개의 단어 사전으로부터 선택되어진다. 이 사전의 내용은 비밀이 아니다.

S/Key 일회용 패스워드 시스템의 전체적인 동작 절차는 다음의 (그림 4)에서 자세히 알 수 있다.

3) S/Key 일회용 패스워드 시스템의 취약점

가. 사전(Dictionary) 공격

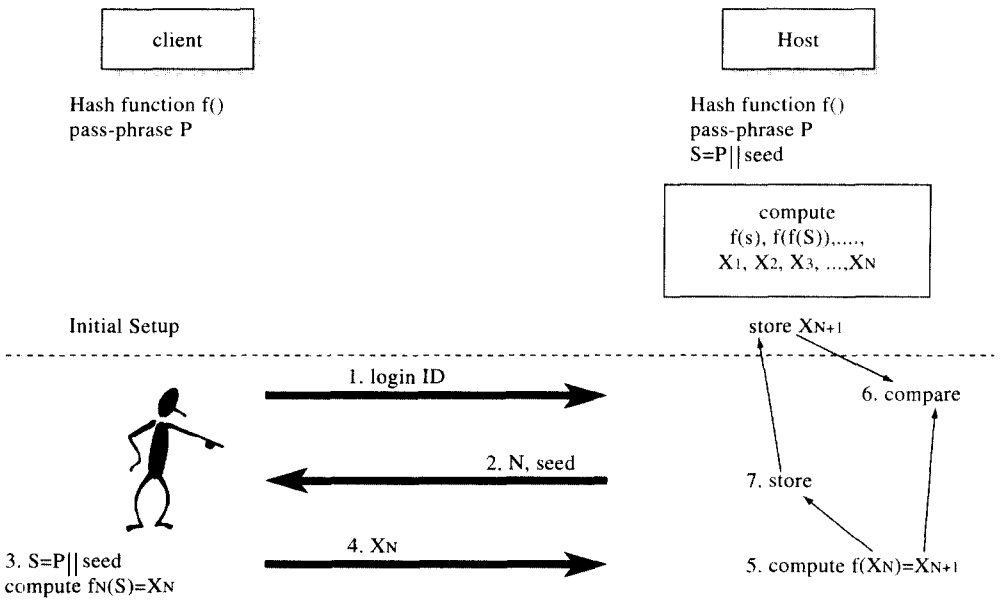
제일 처음 이야기할 S/Key의 취약점은 모든 정보가 평문(Plaintext)으로 전파되어진다는 것에 있다. 이것은 challenge와 response를 알 수 있다는 것을 의미하며, 이 정보들을 가지고 사전의 단어들에 적용한 challenge의 결과와 비교하는 것이다.

username : jdoe
challenge : 99 k113355
response : WELD GUY CHIMP SWING GONE

위와 같은 정보로부터 사용자 jdoe의 실제 패스워드를 다음과 같이 유추해낼 수 있게 된다.

시도 1)
dictionary word 1 : love
challenge : 99 k113355
response : BAD LOST CRUMB HIDE KNOT

시도 2)
dictionary word 2 : hack
challenge : 99 k113355



(그림 4) S/Key의 동작 절차

response : FORT HARD BIKE HIT SWING

시도 3)
dictionary word 3 : secret
challenge : 99 k113355
reponse : WELD GUY CHIMP SWING GONE

여기서 우리는 사용자 jdoe의 실제 패스워드 "secret"을 알게 되고, 이 정보를 가지고 challenge에 상관없이 정당한 일회용 패스워드를 생성해 낼 수 있게 된다. 이것은 현재 S/Key 패키지가 클라이언트나 서버 어디서도 사용자 패스워드 선택시에 보안성 검사를 하지 않는다는 중요한 결점을 가지고 있다는 것이다.

Dictionary 공격에 대한 다른 문제점은 /etc/skeykeys 파일에 있다. 아주 놀랍게도 skey를 사용하고 있는 호스트들이 이 파일에 부적절한 permission을 가지고 있다는 것이다. 이 파일은 누구나 읽기 가능하도록 하지 말아야 한다. skeykeys 파일의 구조는 아래와 같다.

root 0072 k113357 12afaa8be65f0502
Jun 29,1995 12:40:48
jdoe 0099 k113355 c7f42dfd84914af3
May 30,1995 16:20:19
[etc...]

여기서 우리는 사용자 이름, iteration counter, seed, 그리고 다섯 단어 response의 16진수 표현을 볼 수 있다. 나머지 세필드는 단순히 날짜 시간 정보들이다. 이 파일의 정보들을 가지고 앞서 언급한 dictionary 공격 방식 그대로 해킹이 가능하다.

나. 스푸핑(Spoofing) 공격

Iteration counter가 seed와 함께 클라이언트 측으로 전송이 되어지기 때문에, 서버로 위장하는 공격 가능성을 가지게 된다. 이 방법은 가짜 게이트웨이를 설정함으로 수행되어진다. 다음의 시나리오를

살펴보자.

login : jdoe /* jdoe가 telnet으로 호스트에 접속 시도한 후 */
s/key 55 k113355 /* jdoe는 98번째의 challenge 대신에 55번째의 challenge 를 받았다.*/
password :

password : MY SPIT LOFT HEAD REAR
/* jdoe의 계산기는 그의 패스워드를 이용하여 55 k113355에 대한 response를 생성한다. */

Login incorrect
login : /* 가짜 호스트는 login이 틀렸다고 말하고, jdoe가 실제로 원하는 호스트로 다음 연결을 하게 한다. */

여기서 55 k113355 challenge로부터 얻어진 response를 가지고 스니퍼는 해쉬 함수를 이용하여 나머지 response들을 알아낼 수 있게 된다. 예를 들면, 지금 가지고 있는 정보를 이용해서 60 k113355에 대한 response를 알고 싶다면, 해쉬 함수를 다섯 번만 수행하면 원하는 response를 얻을 수 있게 되는 것이다.

다. Race 공격

이것은 같은 키를 가지고 동시에 login을 시도하는 두 프로세스를 허용하는 skey의 문제점에 관한 내용이다. 만약 공격자가 지나가는 jdoe의 response들을 잡을 수 있다면, 같은 호스트에 다른 telnet 세션을 열 수 있고, iteration counter가 줄어들기 이전의 같은 challenge를 얻을 수 있다. 그후 jdoe의 response를 가지고 login을 시도하여 운 좋게 locking problem이 발생하게 된다면, 둘다 같은 challenge와 response를 가지고 login에 성공하게 된다. 이것은 S/Key의 소스 코드를 수정하여 쉽게 고쳐질 수 있는 문제이다.

라. MONKEY(S/Key attack)

MONKEY는 S/Key 일회용패스워드 크래킹 프로그램으로 다음과 같이 구성되어 있다.

dictionary md4.c md4.h mod_passwd.c monkey.c monkey.h monkey_crack.h put.c readme.now.really skeykeys sniffed white_paper

MONKEY는 모든 정보가 평문(Plaintext)로 전송되는 S/Key의 취약성을 이용한다. 먼저 스니퍼 프로그램인 snifferd를 이용하여 challenge와 response를 알아내고 스니퍼한 정보들을 가지고 사전의 단어들에 적용하여 challenge의 결과와 비교하는 것이다. 스니퍼한 username, challenge, response와 같은 정보로부터 dictionary attack을 통하여 사용자의 실제 패스워드를 유추해본다. 또한 누구나 읽기 가능하도록 되어있는 /etc/skeykeys 파일을 가지고 MONKEY를 수행하므로써 dictionary attack이 가능하다.

4. 결 론

본고에서는 사용자의 신분확인을 위해 사용되는 패스워드의 누출을 막기위해 지금까지 알려진 기술들을 소개하였고 이에 대한 보안 취약점들을 다각도로 분석해보았다.

국내에서도 일회용패스워드 방식의 도입에 대한 필요성이 제기되어, 이에 대한 적용 기술로서 어떠한 것들이 있는지 다방면으로 분석중이다. 현재 국내에서는 미래산업의 소프트포럼이 OnceID를 개발하였고, 삼성전자, 퓨쳐시스템, 씨엔아이 등이 일회용 패스워드 방식과 관련 제품들을 개발, 혹은 개발중에 있으며, IC카드 소프트웨어 개발 전문업체인 동성정보통신도 최근 PC 뱅킹의 보안 강화를 위해 매직링크

시크릿 키(MSK)를 개발하여 데이콤이 제공하는 PC뱅킹 보안솔루션으로 적용키로 했다.

특히 일회용패스워드는 가격이 제품의 성패를 좌우할 것으로 보고 기존 국내외 개발 제품들의 장단점을 비교 검토해 기능은 떨어지지 않으면서도 생산단가를 최소화할 수 있는 제품을 개발하는 것이 중요하다.

한국정보보호센터의 침입차단시스템 평가기준에서도 K4등급을 취득하기 위해서는 재사용(replay) 공격으로부터 안전해야 한다고 규정하고 있는데, 이는 일회용 패스워드 방식의 사용을 말하고 있는 것이다. 이처럼, 이제는 단순한 패스워드 시스템에서 탈피하여 다양한 패스워드 공격으로부터 안전성을 보장할 수 있는 사용자 신분확인 시스템을 도입하여, 정보시스템의 안전성 향상을 지향해야 할 것이다.

참 고 문 헌

[1] 홍기용외, 전산망정보보호(접근통제기술), 한국정보보호센터, 1996.12

[2] 은유진, 지능형 토큰을 이용한 사용자 인증시스템의 설계 및 구현, 석사학위논문, 1997.

[3] '96네트웍제품연감, (주)데이터월드, p.593~p.596, 1996.3.

[4] Matt Bishop, "An Application of a Fast Data Encryption Standard Implement-at:on", Computing Systems, vol. 1, no. 3, pp.221-254, Summer1988.

[5] David C. Feldmeier and Philip R. Karn, "UNIX Password Security-Ten Years Later", CRYPTO Proceedings, Summer 1989.

[6] Philip Leong and Chris Tham, "UNIX Password Encryption Considered Insecure", USENIX Winter Conference Proceedings, January 1991.

[7] Danial V.Klein, "Foiling the Cracker: A Survey of and Improvements to Password Security"

[8] Robert T. Morris and Ken Thompson, "Password Security: A Case History", Communications of the ACM, vol. 22, no. 11, pp.594-597, November 1979.

[9] Chris Hare, Karanjit Siyan, Internet Firewalls and Network Security 2nd edition, New Riders, 1996.

[10] Johna Till Johnson, "Enterprise Better Safe Than Sorry Security", Data Communication, March 1995.

[11] R. Rivest, The MD5 Message-Digest Algorithm, RFC 1321, April 1992.

[12] R. Rivest, The MD4 Message-Digest Algorithm, RFC 1320, April 1992.

[13] N. Haller, The S/KEY One-Time Password System, RFC 1760, February 1995.

[14] N. Haller & C. Metz, A One-Time Password System, RFC 1938, May 1996.

부록. 국외 패스워드 관련 제품현황 요약표[3]

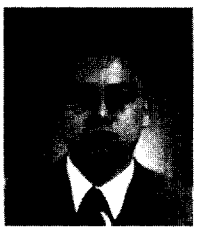
공급회사	제 품 명	주 요 특 징	가 격
Activcard	Activcard Multi-User Passport	포터블 휴대형 인증 디바이스. 네트웍 정보에 액세스를 요청하거나 EDI 및 EFT 통신 거래를 실시하는 사용자들을 인증 해 준다. 랜, 왠, PSTN, 인터넷 및 인트라넷용 도전-응전 비동기/이벤트 모드 및 time-sync 모드에서 실행된다.	50 유닛용 $66 이상
Ascend	Authenticati-on Server Software	이 소프트웨어 패키지는 1회 암호 능력, 이동중인 사용자 및 원격 사용자를 위해 토큰을 기반으로 한 도전, 모듈식/확장성 있는 설계, 각 사용자용으로 구성 할 수 있는 방법론 및 서비스, 그리고 서버 한 대로 여러 개의 방화벽을 제어하는 능력 등을 통해 더 풍부한 보안 조치를 제공 해 준다.	$1,500 이상
Communicati on Devices	Authenticato-r Tokens	이 회사는 mobile 및 기타 다이얼인 애플리케이션용으로 인증 토큰 전 계열을 제공하고 있다. 각종 모델들은 인가받지 않은 액세스를 막아주는 한편 이러한 액세스가 사용자에게 미치는 영향을 최소화 해 준다. 도스, 윈도우, IBM OS/2 및 매킨토시 클라이언트들을 지원한다. 이용가능한 포맷은 소프트웨어, 하드웨어, 계산기 및 무선호출기.	$35 이상
Cybersafe	Cybersafe Application Security Toolkit	GSS-API에 기반을 두고 있다. 이 툴킷은 프로그래머들이 자신들의 네트웍 애플리케이션들을 안전하게 보호할 수 있게 해 준다. 대부분의 유닉스 플랫폼, 윈도우 16비트 및 32비트 플랫폼들, 그리고 OS/2용으로 이용할 수 있다.	3,000이상 추가 툴킷은 각각 $295
	Cybersafe SNAP	프로그래머들이 저대역폭 프로토콜을 사용하여 애플리케이션들을 안전하게 보호할 수 있게 해 준다. 대부분의 유닉스 플랫폼들과 윈도우 16비트 및 32비트 플랫폼에서 이용할 수 있다.	인증 서버 $4,000 이상, 툴킷 $5,000 이상
Cylink	Secure Domain	시큐어 도메인의 액세스 제어 및 보안 기능은 여러 노드, 도메인, 서브네트웍 및 네크웍들이 하나의 완벽한 환경에서 함께 통신할 수 있게 해 준다.	미국에서 $9,500
	Securenode Card	동사의 시큐어스택 및 NIC 와 함께 보안 솔루션으로 사용된다.	미국에서 $3,995
	Securenode Unit	네트웍 디바이스와 네트웍 사이에 시리얼로 연결되어 비 PC 디바이스들이 안전 한 네트웍 환경에서 통신하는데 필요한 보안을 제공한다.	$7,000
	Netgate Remote Access Management Server	수천대의 휴대용 및 홈 컴퓨터, 원격 사무실 연결, 다이얼인 라우터 및 브릿지, 그리고 기타 EIA-232 디바이스들을 관리한다. 트랜스패런트한 암호 인증 및 주문형 암호화를 제공한다.	$57,500 이상
	Securefram-e	프레임 릴레이 네트웍 전반에서 민감한 정보를 부주의한 노출 또는 공격으로부터 보호 해 준다. 인증을 받고 비밀리에 안전한 네트웍 접속이 가능하게 해 준다.	$5,900 이상
	Securetravel er for Windows	윈도우에 기반을 둔 모든 통신 시스템들 뒤에서 트랜스패런트하게 실행되는 한편 다이얼인 세션들을 안전하게 비밀리에 유지 해 준다.	$295 이상
	Securepocket Traveler	인증에 기반을 둔 보안 클라이언트. 랩탑 및 데스크탑 PC, 그리고 비동기 시리얼 인터페이스를 갖춘 그밖의 디바이스들로부터 다이얼업 액세스를 위한 자동 인증 및 암호화를 제공한다.	$525 이상
	Securegate Server	엔터프라이즈 네트웍에 다이얼업 액세스 하기 위한 동사의 정보 보안 솔루션의 핵심. 동사의 시큐어액세스 시스템 사용 권한을 증명해주기도 한다.	$8,000-$100,000

공급회사	제 품 명	주 요 특 징	가 격
Digital Pathways	Securenet Keys	PIN 보호를 받는 시큐어넷 키는 액세스 제어 디바이스인 Defend- er 및 Defender Security Server 들과 함께 사용되어 원격 사용자를 인증 해 준다. 키는 ANSI X9.9를 지원하는 일회 암호를 만들어주는 도전-응전 인증 프로세스에서 비전용 DES 알고리즘을 사용한다. 시큐어넷 키는 다양한 써드파티 보안 제품들과 사용될 수 있다.	키당 $40
	Software Securenet Keys	중심 비즈니스 사이트에서 멀리 떨어져 있는 랩탑 또는 웍스테이션들에 통합되어있다. PIN 및 복사 보호를 받는 이 키들은 동사의 액세스 제어 디바이스인 Defender 및 Defender Server. 그리고 써드파티 보안 시스템들(방화벽 및 메인프레임 액세스 제어 시스템 포함)과 함께 사용된다. 도스, 윈도우 3.x, 윈도우95 및 애플톡 리모트액세스용으로 이용할 수 있다.	키당 $25
	Windows Defender Management Software	원격 액세스 애플리케이션의 모든 보안 측면을 관리하기 위해 윈도우에 기반을 둔 애플리케이션을 제공한다. 시스템 관리자가 중앙의 콘솔 한곳에서 방어 시스템을 구성하고, 오디트 데이터를 수집하며, 보안 서브시스템들에 대한 진단을 수행할 수 있게 해 준다.	$1,595
	Defender Mgmt. Software Reports	가공을 거치지 않은 오디트 데이터를 관리 정보로 전환해주는, 윈도우에 기반을 둔 애플리이션을 제공한다.	$495
Eliashim Microcomput -ers	Easysafe	노트북, 랩탑 및 스탠드얼론 PC용 액세스 제어 제품. 인가를 받지 않은 액세스를 막기 위해 하드 디스크 및 스크린 블랭킹의 데이터 암호화와 결합된 부트 암호 메카니즘을 제공한다. LPT, COM 및 플로피포트들의 이용을 막을 수 있게 구성될 수 있다.	스테이션당 $7,900 이상
	Mastersafe	이 컴퓨터 제어 시스템은 스탠드얼론, 멀티유저 및 네트웍으로 연결된 PC들에 대한 액세스를 제한한다. 제어 능력에는 암호 액세스, 데이터 암호화, 그리고 하드 드라이브/프로그램/주변기기 포션에 액세스 제한 등이 포함된다.	10인 사용자 네트웍 버전은 $950
Information Resource Engineering	Safenet/Dial	세이프넷/다이얼 사용자들은 독특한 PIN을 입력하고 모뎀이 자동으로 모든 다이얼인 세션용으로 새롭고 복잡한 암호를 만들어 준다. 한 해커가 암호한개를 캡처하면 그 암호는 그순간 무용지물화된다.	DES 버전은 $695
	Safenet/LAN	암호화된 통신만을 허용하거나, 또는 네트웍주소 및 소켓 서비스에 기반을 두고 확실한 액세스를 유연하고 안전하게 필터할 수 있게 해 준다. 세이프넷/랜은 해커들이 방화벽 침투에 사용하는 spoofing 공격으로부터 막아주는 암호능력을 사용하여 보안 헤더를 자동으로 만들어 준다.	$4,995 이상
	Safenet/Certi fica-te Center	세이프넷/랜을 통합한 시스템을 자동으로 중앙에서 관리 해 준다. TCP/IP와 함께 사용되며 CA(Certificate Authority)로, 그리고 ANSI X9.17키 분배 센터로 사용된다. 인증 관리, 오디팅, 경보 보고, 그리고 네트웍 관리를 수행한다. 또한 광범위한 보안 제품들을 지원한다.	$15,995
	A1000 Single-Line Host/DES	최고 32명의 원격 다이얼인 사용자들에게 랜, PABX, 또는 호스트 컴퓨터 액세스를 보호해주는 데스크탑 제품. 또한 ANSI X9.17에 따라 PIN 및 키들의 자동 관리를 제공한다.	$795
	A1000 Single-Line Host/Export able	전용 암호화 기능을 사용한다.	$1,100
	AX200 Encrypting Token/Expor tabl-e	포켓 크기의 임의 암호 생성기 겸 데이터 암호기인 이 제품은 각 세션용으로 새로운 임의의 암호를 생성해주며, 엑스포트할 수 있는 IRE 전용 알고리즘인 Atlas를 사용하여 데이터를 암호화 해 준다.	$425

공급회사	제 품 명	주 요 특 징	가 격
Information Resource Engineering	AX200*Encry pting Token/DES	포켓 크기의 암호화 토큰, 임의 암호 생성기 겸 데이터 암호기. 미국내외 보안 표준들을 준수하며, 모든 통신 세션용으로 새로운 임의 암호를 자동으로 생성해 준다. DES 암호화를 사용하여 전송된 데이터의 프라이버시가 보호된다.	$295
	AX400 Encrypting Token with Modem	포켓 크기의 암호화 토큰, 14.4kbps 모뎀 한 개와 함께 제공된다. 미국내외 보안 표준들은 준수하며, DES를 사용하여 모든 통신 세션용으로 새로운 임의 암호를 생성해 준다.	$495 엑스포트 가능한 버전은 $715
	IRE Network Security Systems	산업표준 DES 또는 엑스포트 가능한 알고리즘인 Atlas를 사용하여 다이얼업, 전용 회선, 사설 및 공중 X.25를 안전하게 보호하고 랜 및 왠들을 저장후 전송한다.	$295 이상
	C3000 Security/Key Management System	IRE 네트웍 보안 시스템들을 관리하며, 수천개의 원격 암호화 토큰을 갖춘 대형 상업용 애플리케이션들을 지원한다. ANSI X9.17을 준수하는 중앙집중식, 자동 키 관리 및 네트웍 관리 기능을 제공한다.	$19,800
Leemah Datacom	Fastraq V.34 Security Modem	V.34 팩스/데이타/음성 모뎀 한 개와 내장형 보안 기능을 제공한다. 동사의 DES 인증 토큰들과 함께 사용되어 안전한 콜인을 제공하며, 비동기 또는 동기, 전이중 또는 반이중 모드 2인 사용자 데이터베이스(64인으로 확장 가능) 플래시 롬 그리고 자동 속도 선택을 제공한다.	$300 이상
	Infocard II	신용카드 크기의 이 디바이스는 데이터 또는 음성망 액세스를 위해 사용자 인증을 제공한다. 보안 기능을 강화하기 위해 PIN을 enter하는 사용자가 토큰을 활성화하도록 요구하는 옵션을 갖출 수도 있다. 그 빡의 구성 옵션으로 도전-응전 및/또는 응전 모드들이 포함된다.	$50
	Infokey User Authentication Token	네트웍 및 프로토콜에 독립적인 인포키 토큰은 사용자의 모뎀과 송신용 전화 회선 사이에 플러그인 된다. 안전한 시스템이 액세스될 때에만 인포키를 활성화시키는 톤체크, 그리고 인증이 끝날 때까지 원격 사용자의 모뎀을 전화선에서 막아주는 모뎀락을 제공한다. 표준 모뎀들, 통신 소프트웨어, 그리고 PC 또는 단 말기들과 함께 사용된다.	$150 이상
	Safeconnect User Authentication Token Plus Modem	타입 II PCMCIA 카드에서 14.4kbps 데이터/팩스/음성 모뎀 한 개에 DES 도전-응전 사용자 인증을 추가 해 준다. 표준 통신 및 옴성 메시징 소프트웨어와 함께 사용된다.	$400 이상
	Traqnet 2000 Series Access Control System	수신 전화선과 모뎀 사이에 설치되어 네트웍 액세스 포인트를 보호해 준다. 동사의 개인용 인증 디바이스 및 보안 관리 소프트웨어와 함께 사용된다.	$950 이상
Optimum Electronics	DL 1000	서버들 또는 여러 가지 인증 모드를 갖춘 다른 종류의 프론트 엔드 장비들에 1-13,000 다이얼업 회선을 보호 해 준다. 규모에 제한없이 사용자들이 동시에 지원될 수 있으며, 각각은 하나의 독특한 사용자 프로파일을 가질 수 있다. 이 프로파일들은 언제 어떤포트 액세스가 허용되는지, 또 어떤 종류의 인증이 요구되는지 결정 해 준다.	$3,885 이상
	PC Passkey	PC, 노트북, 랩탑, 또는 도스에 기반을 둔 모든 운영체제를 보호 해 준다. 옵션으로 다양한 종류의 암호화, 부트 부호, 플로피 디스크 암호화, 타임아웃, 그리고 스크린 블랭킹이 있다. 이 제품은 사용자가 결정한 패러미터들을 사용하여 자동으로 설치될 수 있다.	$100
	SCS-2	이 싱글 다이얼업 회선 보호 디바이스는 한 다이얼업 사용자가 액세스를 얻기 위해 충족시켜야 하는 기준을 결정해주는 개인 프로파일들을 최고 100개까지 지원한다. 이 기준에는 시간 및 암호 콜백, 임의 암호 생성기, 또는 소프트웨어에 기반을 둔 인증이 포함될 수 있다. 모뎀 및 컴퓨터에 독립적이며 최고 57.6kbps 데이터 속도를 지원한다.	약 $795
PC Guardian	Workstation Manager Plus	한 곳에서 각 윅스테이션에 설치된다. 네트웨어와 통합되어 있으며 읽기 전용 디렉토리 제어 및 싱글 사이온을 제공한다. 도스 및 윈도우와 호환된다.	$150-$300

공급회사	제 품 명	주 요 특 징	가 격
Platinum	Platinum Autosecure	유닉스 서버에 적극적인 액세스 제어를 제공하며, 중/대규모 컴퓨터 센터용으로 완벽한 솔루션을 제공한다.	클라이언트 $50이상. 서버 $1,000 이상
QPSXCcmm unications	Viewfinder	X.509 보안 추가 기능을 갖춘 X.500 디렉토리 소프트웨어. 중/대규모 대기업에 맞게 확장되며, 퍼블리싱 키, 인증 및 키 취소를 위한 추가 기능들도 포함하고 있다.	기본 디렉토리 $75,000
Radlinx	Passaport Access Server	인증 기능을 갖춘 이 원격 액세스 서버는 모든 TCP/IP 랜에 설치될 수 있다. 최고 64포트를 통해 모뎀들을 연결할 수 있다. 이 회사는 CHAP를 사용하여 원격 시스템들로부터 ID 및 암호를 안전하게 옮겨주는 소프트웨어를 제공하고 있다. 이 제품을 위한 모든 인증 및 암호화 소프트웨어는 동사의 FTP 사이트에서 다운로드 받을 수 있다.	$500-$6,500
Security Dynamics	SecurID Modem Techniques	SecurID 모뎀은 동사의 자동 two-factor 사용자 인증 기술은 통신 소프트웨어 및 모토로라 V.34 PC 카드 모뎀 한 개와 통합하였다. 이 모뎀은 이동중인 사용자들이 데이터 및 팩스를 송수신하는 것은 물론 랩탑 컴퓨터에서 본사 네트웍에 액세스할 수 있게 해 준다. 또 휴대전화에 연결 해 준다. 이 모뎀은 동사의 Ace/Server 소프트웨어 및 액세스 제어 모듈들과 함께 사용되어 사용자 신원을 인증 해 준다.	$450
Telequip	Crypta Plus	보안 기능을 내장한 PCMCLA 플래시 메모리 카드. 액세스 제어, 안전한 원격 로그온, 퍼블릭 키 암호화, 그리고 디지털 서명 기능들을 포함하고 있다. 윈도우 프로그램은 사용자가 플래시 메모리에 액세스를 얻기 전에 또는 암호 지원 프로세서에 저장된 암호화 키들을 사용하기 전에 이 카드의 잠금장치를 풀도록 요구하고 있다.	$70 이상
Digital Pathways	Defender Security Server	윈도우 NT 또는 인텔 PowerPC 프로세서에서 실행된다. 다이얼인, ISDN, 프레임 릴레이 및 ATM 애플리케이션들과의 광역 또는 원격 액세스 접속을 위해 하나의 보안 애플리케이션을 통해 인증을 제공한다.	$1,995 이상
	Defender Series	호스트, 프로토콜 및 애플리케이션들에 독립적인 멀티포트, 고속 안전 원격 액세스를 제공한다. 하나의 섀시에서 최고 48개의 EIA-232 통신포트와 최고 8,000 사용자를 동시에 지원한다. 각 포트는 몇가지 작동 모드를 지원하도록 구성될 수 있다.	$9,995-$13,995
FSA	Powerlogin	시스템 관리자들에게 유닉스 로그인 및 암호 환경에 대한 제어권을 제공한다. 썬, HP, IBM, DEC, SGI, 시퀀트 및 모토로라 유닉스 플랫폼용으로 이용할 수 있다.	유닛당 $99 이상
	Powertelne	퍼블릭 키 암호체계를 사용하여 시뢰할 수 없는 네트웍에서 안전한 원격 로그인을 제공한다. 우수성을 입증받은 퍼블릭 키 암호화 기술을 사용하여 불안전한 네트웍에서 2대의 컴퓨터간에 원격 로그인을 위한 안전한 전용 채널을 제공한다. 채널의 각 끝에서 만들어진 데이터 및 키스트로크는 네트웍 전반에 전송되기 전에 안전하게 암호화되어 이동중에 민감한 정보의 인티그리티 및 프라이버시를 보호받는다. 썬, HP, IBM, DEC, SGI 시퀀트 및 모토로라 유닉스 플랫폼용으로 이용할 수 있다.	유닛당 $39 이상
Onetics (Ssia)	Donax MA Series	이 메시지 인증 디바이스는 공중망의 호스트 자원들에 대한 비인가 액세스로부터 보호 해 준다.	$770 이상
Openvision	Axxion-Authenticate 1.3	DES 암호화를 사용하여 글로벌 네트웍 전반에 걸쳐 전송된 데이터를 암호화해 주는 네트웍 보안 애플리이션. 대부분의 유닉스 플랫폼과 윈도우 NT시스템에서 실행된다.	$4,700 이상

□ 著者紹介



은 유 진

1995년 아주대학(학사, 컴퓨터공학)
1997년 아주대학교(석사, 컴퓨터공학)
1996년 12월 ~ 현재 한국정보보호센터 기술본부 주임연구원
1997년 10월 ~ 현재 한국정보통신기술협회 정보보호기술 연구위원

※ 주관심분야 : 컴퓨터/네트워크 정보보호

김 기 현

1993년 경북대학교(공학사, 전자공학과)
1995년 경북대학교(공학석사, 전자공학과)
1995년 7월 ~ 1996년 7월 데이콤 시외전화구축팀
1996년 7월 ~ 현재 한국정보보호센터 기술본부 주임연구원
1997년 10월 ~ 현재 TTA 정보보호기술연구위원회 간사

※ 주관심분야 : 시스템 및 네트워크 정보보호

이 홍 섭

1979년 한양대학교(학사, 전자공학)
1985년 한양대학교(석사, 전자공학)
1980년 ~ 1996년 한국전자통신연구소, 연구원 ~ 책임연구원, 실장
1996년 ~ 현재 한국정보보호센터, 연구개발부장, 기술본부장
정보통신기술협회 정보보호분과위원회 의장
한국통신정보보호학회 상임이사

※ 주관심분야 : 시스템 및 네트워크 정보보호