일회용 암호를 이용한 국산 암호 인증 시스템
Authentication System Using One Time Password

추 성 호, 제 갈 명, 박 홍 성*
Seongho Choo, Myung Jekal, Hong Seong Park*

㈜인터넷시큐리티 기술연구소, 강원대학교 제어계측공학과*
Technology Research Laboratory, Internet Security Co.,
Dept. of Control and Instrumentation Engineering, Kangwon National University*

Internet Seucurity Co.
Suite 201, 402-3 Shindorim, Guro, Seoul 152-070, Korea
Dept. of Control and Instrumentation Engineering
Kangwon Natinal University, Chunchon, Kangwon, 200-710, Korea

Phone: +82-2-633-3996, +82-361-250-6347
Fax: +82-2-633-3997, +82-361-242-2059
E-mail: somebody@security.co.kr, jkm@security.co.kr, hspark@cc.kangwon.ac.kr

Security System is based in a authentication system. This paper introduces some authentication mechanism and implements One-time password (OTP) system for user authentication with synchronizing password, managing secure values, developing password generator, and operating server software.

Keywords: One Time Password, Authentication, Security

1. 서 론

인터넷의 광범위한 응용과 더불어 인터넷 보안은 최근 중요한 관심사가 되고 있다. 보안 시스템은 그것을 구성하는 모든 요소가 완벽히 조화를 이루어야지만 그 성능을 발휘하게 된다. 어느 한 부분의 약점은 전체 시스템에 치명적인 결과를 초래하게 되므로 한 요소요소마다 치밀한 설계와 상호 협조가 필요하게 된다.

정보 보호는 크게 다음의 여섯 가지 서비스, 즉 인증 (authentication), 권한 부여 (authorization), 기밀성 (confidentiality), 무결성 (integrity), 부인방지 (nonrepudiation) 로 구성된다. 또한 이런 서비스들을 제공하기 위한 방법, 즉 보안 메커니즘 (Security Mechanism) 에는 다양한 것이 있다. 그 중 인증 서비스는 각 사용자 (사람, 응용프로그램, 장치 등) 들이 통신을 시작함에 있어 가장 처음에 요구하게 되며 그에 해당하는 접근 권한 등을 설정해 주므로 가장 핵심이 되는 서비스라고 할 수 있다. 그러나 국내에서는 그 중요성에 비해 인증 서비스에 대한 연구가 비교적 적은 실정이다.

특히, 보안 시장은 군수물자 시장과 마찬가지로 국가의 관리가 엄격하다. 현재 암호 알고리즘과 보안 사용 허가는 국가정보원에서 관리되어 지고 있다. 현재 국가망과 공공망 (금융망 등) 의 경우 외국 보안 장비의 사용과 외산 알고리즘의 사용은 금지되어 있다.

한국전자통신연구원 (ETRI) 에서 개발한 국가용 FES (대칭키 방식의 암복호화 알고리즘) 을 사용한 제품인 경우 국가 및 공공망에서 사용이 가능하며, 민수용으로는 SEED 를 한국정보보호센터 (KISA) 를 개발 보급하고 있는 중이다. 해쉬 함수의 경우도 SMD (Strengthened Message Digest) 를 개발하여 보급하였다[10].

일회용 암호 제품 (3 절에서 상세히 설명) 의 경우는 금융망에서 폰 뱅킹, PC 뱅킹에서 사용하는 것이 98 년 말에 허가가 났으며 현재 각 은행과 증권사에서 도입 중에 있다. 전화 도청 및 내부 범죄를 막기 위해 기존의 고정식 암호 시스템과 난수표 방식보다 한층 더 보안성이 강화된 시스템을 구축하고 있다. 기업이나 학교 등에서도 내부 보안을 위해 사용되고 있으며, 아직 국가적으로 사용 허가가 나지 않고, 별도의 컴퓨터가 있어야 접속 가능한 인터넷 상의 가상사설망 (VPN,

Virtual Private Network) 은 비용면에서도 많은 문제가 따르기 때문에 일회용 암호 시스템을 채용 중에 있다. 외국의 경우 포츈지 선정 500 대 기업들은 거의다 전산실 관계자 또는 영업 사원을 중심으로 이 제품을 사용 중에 있다.

본 논문은 인증 서비스를 제공하기 위한 메커니즘으로 일회용 암호 (One Time Password) 에 대해 주안점을 두었으며, 이를 이용한 인증 시스템의 구현 방법과 응용에 대해 기술한다.

다음 절에서는 인증 매커니즘과 그의 문제점들을 개략적으로 나열해 봄으로써 일회용 암호 시스템이 필요한 이유를 살펴보고 3 절에서는 일회용 암호를 이용한 인증 시스템의 구현에 대하여 논의하고, 마지막으로 결론을 맺겠다.

2. 인증 메커니즘

인증 메커니즘은 주로 다음의 세 가지 개념에 기초를 두고 있다. 첫번째로 '아는 것'이다. 인증을 받기를 원하는 사람 (인증 요구자) 은 암호, 또는 PIN (Personal Identity Number) 등 자신이 알고 있는 무언가를 제시하고자 한다. 두번째로 '가긴 것'은 인증 요구자는 열쇠, 뱃지, 자기 카드 (magnetic card), 또는 파일 (인증서) 이나 스마트 카드 (smart card, IC card) 등에 저장된 개인키 (private key) 를 보여줄 수도 있다. 마지막으로 '자신의 몸, 생체', 즉 변하지 않으면서 확인이 가능한 생체의 무언가, 예를 들어 음성, 지문, 홍체 등을 이용하여 정당한 사용자인지를 구별할 수 있다. 그 외에 영지식 (zero knowledge) 인증 개념도 연구 중에 있다.

일반적으로 이 중 두 가지 이상의 방법을 이용하여 인증을 함으로써 보안성을 한층 강화시키며 다중요소 인증 시스템 (multifactor authentication system) 이라고 한다.[3]

이 세가지를 구체적으로 살펴보면,

2.1. Something You Know – 아는 것

가장 널리 쓰이는 방법으로 쓰기 편하다는 장점이 있는 반면에, 암호를 요구하는 기관들이 많아짐에 따라 인간 기억력의 한계가 있고, 하나의 암호를 공통적으로 사용했을 경우의 위험성과 누출 시의 불편함 등의 단점이 있다. 또한 인터넷과 같이 공개된 네트웍을 통해 암호화되지 않은 상태로 전송이 될 경우 쉽게 도청이 되며, 시스템 침입자에 의해 암호 파일이 읽혀질 수 있다. 또한 기억하기 쉽게 하기 위해 만든 암호는 쉽게 유추될 수도 있고, 사전 공격 (dictionary attack) 에도 취약하며, 옆에서 키입력을 지켜보는 사람에 의해, 또는 암호를 물어보는 속임수 프로그램에 의해 유출될 수도 있다. 그런 단점을 해결하는 유일한 방법은 암호를 어렵게 만들고 자주 변경할 수 있지만 관리의 어려움이 있으며 그마저도 도청의 위험은 항상 있게 된다.

결과적으로 보안 시스템 공격자들이 많이 쓰는 방법인 스니핑 (sniffing), 스푸핑 (spoofing), 암호 유추 프로그램 등에 모두 취약하다.

이에 대해 일회용 암호 메커니즘은 사용자의 인증 요구 때마다 새로운 암호를 생성하여 사용함으로써 시스템 내에 암호 파일을 보관해 둘 필요가 없으며, 암호가 항상 바뀌므로 설사 한번 도청, 또는 누출된다고 하더라도 문제가 되지 않으며 사전 공격 등에도 안전한 대처 방안이 된다.[2]

2.2. Something You Have – 가진 것

일반적으로 인증을 받기 위해 쓰이는 물건을 '토큰 (token)'이라고 부른다. 토큰은 그 내부 메커니즘이 쉽게 읽혀져서는 안 되며, 복조 불가능해야 한다. 또한 사용이 편리해야 하며 휴대가 간편할수록 좋다. 컴퓨터 또는 인터넷 환경에서 응용되기 위해서 보통 스마트 카드 (smart card), PCMCIA 카드, 일회용 암호 생성기, USB 키, 보안 카드 등의 형태로 만들어지게 된다. 일반적으로 PIN 을 입력함으로써 잠김 상태가 풀리게 되어 사용이 가능해지는 절차를 갖는다.

또한 PCMCIA 카드 등은 내부에 고성능의 데이터 처리 능력을 가지게 하여 특수한 경우 인증뿐만 아니라 암복호화 기능을 담당하기도 한다. 스마트 카드 등을 이용할 경우 요즘 널리 쓰이고 있는 인증서 (certificate) 를 내장할 수도 있으며 따로 키입력 절차 없이 바로 인증이 될 수 있기도 하다.[5]

단점은 항상 휴대해야 한다는 것으로 분실의 위험성이 있으며, 사용을 위해서는 리더기 등의 특별한 장치가 필요하며, 해체에 대비해야 한다는 것 등이 있다. 장점은 외울 것이 거의 없다는 것이다. 이를 이용한 OTP 의 운용에 대해서는 다음 장에서 구체적으로 서술한다.

2.3. Something You Are – 자신의 몸, 생체

일반적으로 가장 고수준의 사용자 인증이 필요할 때 쓰이는 방법으로 미리 입력해 놓은 사람의 생체 (biometrics) 패턴을 검사하여 비교한다. 보안적 성능이 약한 것에서 강한 것 순으로, 싸인 (signature), 자판 입력 패턴 (사람마다 일정한 리듬이 있음), 음성, 손도장, 지문 (fingerprint), 홍채 (retina pattern) 등으로 나열할 수 있다. 보통 고가의 장비와 기술이 필요하다는 단점이 있다.

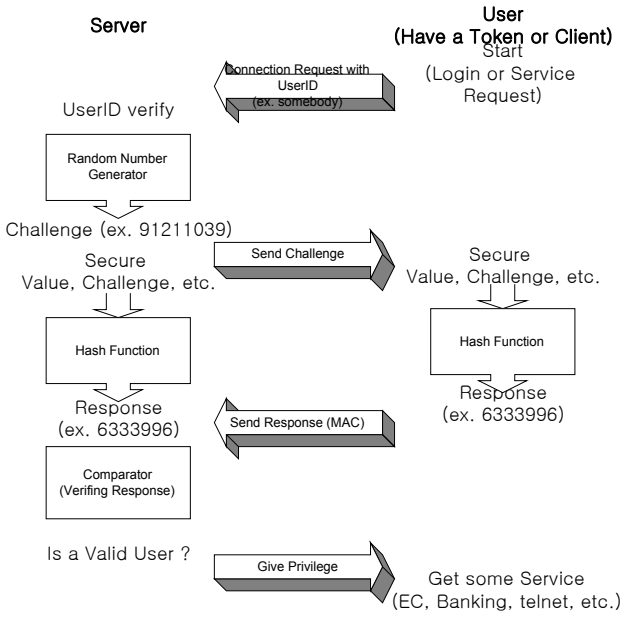

Fig. 1. Challenge/Response Method

3. 일회용 암호 인증 시스템의 구현

사용자의 인증 요구 시, 즉 접속 초기나 접속 후에도 중요도를 지니는 특정 서비스의 제공을 위해 암호를 확인하는 것이 일반적인 방법이다. 하지만 앞에서 서술한 바와 같이 기존의 암호 시스템은 많은 취약점을 가지고 있었고, 이에 대한 해결책으로 제시된 것이 일회용 암호 메커니즘이다. 일회용 암호 매커니즘을 구성하는 요소들은 보안/암호 알고리즘이 내장된 토큰 혹은 일회용 암호 생성기와 인증 서버와 인증 클라이언트로 구성되어 있다.

3.1. 보안/암호 알고리즘

일회용 암호 메커니즘은 서버측과 클라이언트 측이 미리 약속한 방식에 의해 MAC (Message Authentication Code) 을 생성하여 전달함으로써 무결성을 검증하여 인증을 받게 되는 방식이다. 일반적으로 무결성 검증에는 해쉬 함수들이 사용되며, MD4, MD5, RC4, IDEA, HS5DM, SMD 등이 사용된다. 알고리즘은 토큰의 메모리 용량과 컴퓨팅 능력에 의해 선택되어지게 된다.[1][7]

3.2 암호 동기화 방식

일회용 암호 메커니즘은 서버와 클라이언트(또는 토큰) 사이에 미리 약속된 규칙에 의해서 클라이언트 쪽에서 생성한 일회용 암호를 서버 측에 보내면 서버 측도 같은 규칙에 의해 사용자 데이터가 들어있는 데이터베이스에서 비밀값을 가져온 후, 일회용 암호를 생성하여 서로 비교하는 형식이다. 인증이 필요할 때 일회용 암호만 주고 받기 때문에 토큰은 서버와 물리적으로 연결될 필요는 없다. 토큰에서 생성된 암호를 사람이 키보드를 통해 입력하는 형태로 동작하게 된다. 이 때 양쪽의 암호를 동기화 시키는 것이 이 메커니즘의 가장 핵심이며 그 방법에는 다음과 같은 것들이 있다.

a) 질의/응답(Challenge/Response) 방식

서버측에서 난수 발생기를 사용해 일정한 자릿수의 질의값를 클라이언트 측으로 보내면 그 질의값을 토큰, 즉 암호 발생기에 입력하여 응답값을 생성해 내게 된다. 일반적으로 telnet, ftp, www 등의 프로토콜을 이용하여 시스템 로긴 시 UserID를 서버에 입력하면 서버 측에서 질의값을 보내오며 응답값을 물어보게 된다. 그 질의값을 토큰에 입력하여 응답값을 생성하게 된다. 질의값의 입력은 사람이 직접 토큰의 버튼을 누르거나, 화면에 바코드 형태로 점멸하면 포토 센서가 장착된 토큰을 근접시키는 방식 등으로 구현된다.[6]

토큰은 서버에서 보내온 질의값과 토큰 자체에 가지고 있는 비밀값 (secure value, 또는 private key) 등을 가지고 해쉬 함수를 이용하여 적당한 처리를 함으로써 응답값을 생성하며, 생성된 응답값을 서버 측으로 보냄으로써 인증을 받게 된다.

서버와 클라이언트 사이에서 서로 질의값과 응답값을 주고 받으므로 상호 인증이 가능하다

하지만, 질의값이 똑같은 것이 또 나오거나 자주나온다면 보안성에 문제가 있다.

b) 사건 동기 (Event Sync.) 방식

응답값을 생성할 때 해쉬 함수의 입력으로 비밀값과 어느 특정한 사건이 일어난 횟수 등을 함께 사용하는 방법이다. 즉, 질의/응답 방식과 비교하면 질의값으로 특정 사건을 수치화한 것을 사용한다고 볼 수 있다. 이렇게 함으로써 서버 측에서 질의값을 받을 필요가 없어지고, 이것은 질의/응답 방식의 단점을 보완할 수 있게 되는 것이다. 하지만 미리 예측 가능한 사건을 이용할 때는 앞으로 생성될 응답값이 예측 가능하다는 단점이 있다.

c) 시간 동기 (Time Sync.) 방식

해쉬 함수의 입력으로 비밀값과 현재의 시간(실시간) 을 입력하는 방식으로, 서버 측과 클라이언트는 시간이라는 공통된 값을 가짐으로써 동기화 시킬 수 있다는 것에 착안하였다.

토큰의 분실을 대비하여, 일회용 암호는 [사용자의 PIN, 토큰에서 생성된 응답값]로 구성하며, 이 경우, 네트웍 상에 PIN 이 흐르게 된다는 것과 PIN 이 항상 서버에 등록되어 있어야하므로 변경에 불편함이 따른다는 단점이 있다. 하지만 토큰에 PIN 을 입력하는 절차를 없앰으로써 사용의 간편성을 도모할 수 있다.

이 경우 토큰의 시간을 함부로 고칠 수 없게 만드는 것이 중요하다. 보통 이 방식의 토큰은 1 분에 한번씩 암호가 바뀌게 된다. 서버 측과 클라이언트 측 사이에 시계가 오차가 날 수 있으며 그 오차를 보정하는 방법이 이 방식의 핵심이 된다.

d) Event based Challenge/Response (Multi Mode) 방식

질의/응답 방식의 단점과 이벤트 동기 방식의 단점을 없애기 위해 두 방식을 함께 사용한 방법으로, 토큰은 같은 질의값에도 매번 다른 응답값을 생성해 내게 된다.[8]

3.3 일회용 암호 생성기 (Token)

일회용 암호 생성기로 휴대가 간편해야 하기 때문에 명함 크기의 계산기 모양, 열쇠고리 모양, 스마트 카드, USB 키 등의 형태로 만들어진다. 질의값 또는 응답값의 입력 및 작동 방법 등 사용이 간편해야 한다.

일반적으로 일회용 암호 시스템에 쓰이는 토큰의 경우 데이터 암복호화 기능이 필요 없기 때문에 소형으로 컴퓨터와 접속 장치 없이 단순 연산 기능, 디스플레이 기능, 버튼 인터페이스 만으로 구현된다.

해체 방지 기능 (tamperproof) 을 위해 토큰 속의 모든 중요한 데이터는 RAM, Secure EEPROM 등에 위치하여야 하며, 해체 시도 시 전원이 오프되며 그간 사용된 모든 데이터가 자동 소거되는 기능이 필수적이다. 또한 토큰 자체 운영 프로그램도 RAM 등 휘발성 메모리에서 동작하게 하는 것이 바람직하며 최소한 외부에서 읽혀질 수 없도록 마스킹 (masking) 되어 사용되거나 OTP (One Time Programmable) 타입일 경우 외부에서 읽기 방지가 되는 프로세서가 사용되어져야 한다.

스마트 카드를 이용하는 경우 해체 방지 기능에서 탁월한 효과를 보게 된다. 하지만 COS (Card Operating System) 에 일회용 암호 알고리즘이 들어가야 하며, 별도의 접속 장치가 필요하기 때문에 많은 비용이 소모되는 단점이 있다. [9]

3.4 인증 서버 (Authentication Server)

인증에 필요한 데이터를 저장하고 있는 보안이 강화된 데이터베이스와 인증 데몬 (daemon), 인증 프로세스 메니져, 실시간 인증 모니터, 강한 상호 인증 (strongened mutual authenticaton) 기반 위의 관리용 프로그램, 로그 작성기 등으로 구성되며 시스템 자체의 보안과 더불어 네트웍 상의 침입을 막을 수 있는 구조로 보호되어야 한다. 또한 신뢰성을 강화하기 위해 이중 서버 (dual server) 형태로 운영되기도 한다.

3.5 인증 클라이언트 (Authentication Client)

서버와 토큰 사이에서 에이전트 (agent) 기능을 담당하는 프로그램을 말하며, 이 때 사용자 고유의 비밀값은 하드웨어 형태로 보관되어야 한다. 암호화하여 파일 형태로 저장되어 질 수도 있지만 결국은 프로그램 수행 중에 복호화된 값이 계산되어 나오기 때문이다. 일반적으로 스마트 카드를 이용할 때 stand-alone 형태의 프로그램이나 웹 브라우저의 Plug-In 또는 ActiveX 등의 형태로 구현되며, 이 경우 사용자는 별도의 질의값이나 암호 입력 절차 없이 자동으로 로긴할 수 있는 편리성을 강구한 것이다.

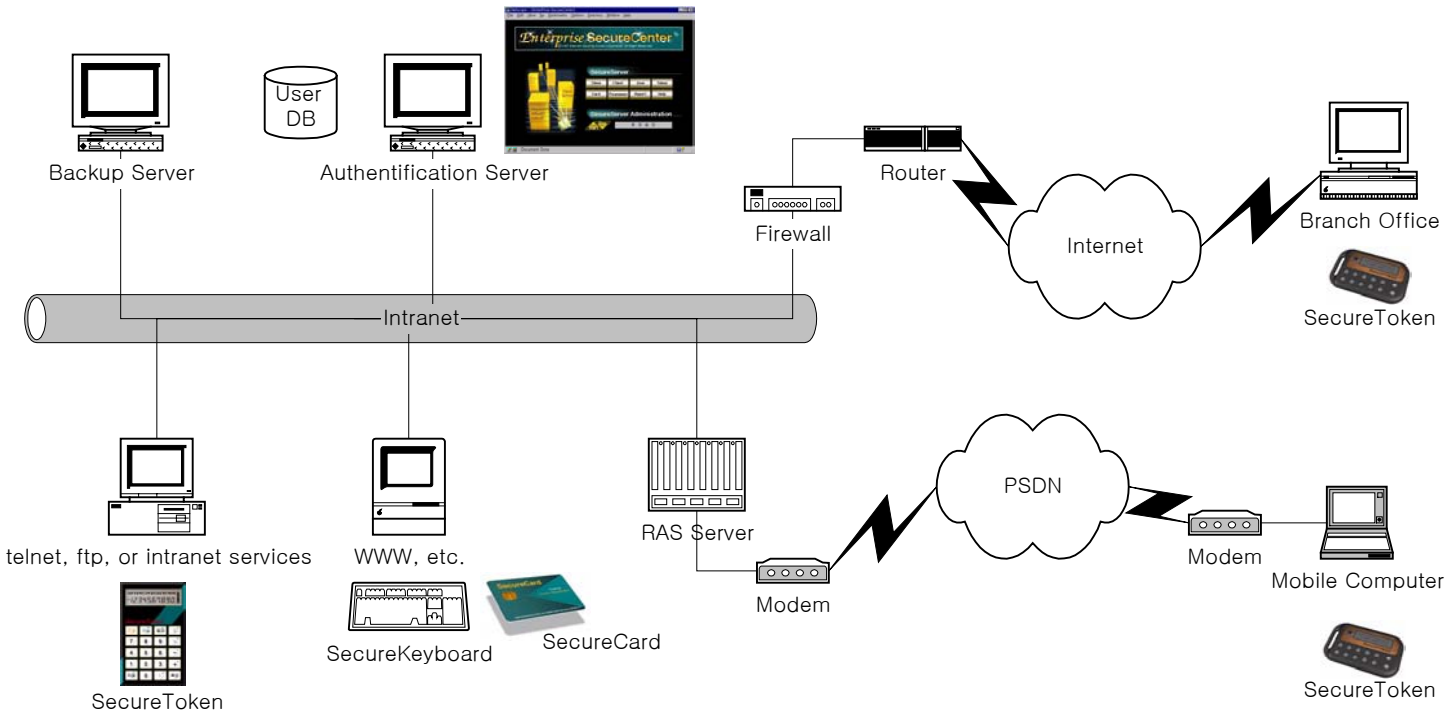

Fig. 2. Authentication System Diagram

3.6 인증 시스템의 구조

일반적인 인증 시스템은 Fig. 2. 와 같이 구성된다. 인트라넷 (intranet, local network) 은 방화벽 (firewall) 로 보호가 되어 있으며, 네트웍 내에는 인증 서버와 백업 서버, RAS 서버, 기타 클라이언트 컴퓨터들이 위치하게 된다. 이 때 인증 서버 자체의 보안도 무척 중요하다. 사용자들의 정보가 들어가 있는 User DB 도 보안이 되는 데이터베이스 시스템 위에 위치해야 한다. 인증 서버는 사용자의 인증 요구에 응답하여 주고, 각 어플리케이션 서버 (application server) 에 현재 사용자들의 인증 정보를 알려주는 역할을 하면서, 실시간으로 인증 시스템의 상태를 파일의 형태로 남기게 된다. 또한 사용자들의 정보들을 관리해 줄 수 있는 관리자 프로그램에 의해 전체 시스템의 동작을 관리하게 된다.

만약의 사태를 대비하기 위해 백업 서버는 인증 서버의 최신 데이터들을 항상 백업해 놓게 되며 필요 시 인증 서버 역할을 대신하게 된다.

사용자들은 토큰이나 스마트 카드를 이용하여 인증 서버로부터 인증을 받아 다른 어플리케이션 서버를 사용할 수 있는 권한을 획득하게 된다. 각 어플리케이션 서버들은 또한 인증 서버와 연결되어 사용자의 현재 인증 상태를 항상 감시하고 적당한 서비스 요구 권한을 주게 된다.

일회용 암호 시스템의 특성 즉, 암호가 누출되어도 문제가 없는 성질에 의해 인터넷이나 공중전화망 (PSDN) 등의 공중망을 통해 인트라넷에 접근이 가능하다.

각 클라이언트들을 사용하는 사용자들은 여러가지 다양한 형태의 토큰, 스마트 카드 등을 이용하게 된다.

4. 결 론

본 논문은 인증 메커니즘에 대해 살펴보았고, 그 중 일회용 암호를 이용한 방법의 구현에 대해 논의하였고, 그와 관련된 응용 시스템의 구조를 제시하였다.

보안 시스템의 근간이 되는 인증 시스템은 그 방법론과 정밀성 향상에서 많은 연구가 필요하다.

REFERENCES

[1] A. J. Menezes, P. C. Oorschot & S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press LLC, 1997.

[2] Haller & Atkinson, *RFC1704 On Internet Authentication*, Oct. 1994.

[3] Jalal Feghhi, Jalil Feghhi & P. Williams, *Digital Certificates: Applied Internet Security*, Addison-Wesley, 1999.

[4] N. Haller, *RFC1760 The S/KEY One-Time Password System*, Feb. 1995.

[5] RSA Data Security, http://www.rsa.com

[6] Vasco Data Security, http://www.vasco.com

[7] W. Stallings, *Network and Internetwork Security: Principles and Practice*, IEEE Press, 1995.

[8] ㈜인터넷시큐리티, *Enterprise SecureCenter User's Manual 2nd Ed.*, 1999.

[9] 삼성전자㈜, *SCOS 1.5 Reference Manual*, 1998.

[10] 한국전자통신연구원, *데이터 파일보호기술 전수자료*, 1998. 12.