通信情報保護學會誌
第5卷 第1號, 1995. 3

시큐리티 제품 소개

박 태 완*

배 경

정보 보호가 최근 들어 중요한 이슈가 되고 있다. 보다 실용적인 내용을 학회지에 추가하여 소수의 전문가들만이 아닌 일반인들에게도 도움이 되고져 외국에서 실제로 설치되어 널리 쓰이고 있고 또한 국내에서도 유용하게 쓰일 수 있는 제품에 관한 정보를 제공하고자 한다.

RACAL-GUARDATA의 Gateway Security System

이 제품은 접근 제어, 데이터의 인증 및 암호화의 기능을 제공한다. 외국의 경우, 주로 IBM 대형 컴퓨터를 사용하는 대부분의 금융 기관에 설치되어 Electronic Funds Transfer(EFT), Electronic Data Interchange(EDI), Phone Banking 등에 널리 사용되고 있다.

Gateway Security System은 Access Gateway와 Secure Gateway의 두 가지 구성이 있을 수 있다. Access Gateway는 단지 접근 제어(Access Control) 기능만 제공하며 Secure Gateway는 접근 제어 뿐만 아니라 데이터의 암호화(Data Encryption) 및 인증(Data Authentication) 기능을 제공한다.

* 정회원, Information Security Korea(I.S.K.) 대표

이 제품은 Public Data Networks나 Private Data Networks을 통한 불법적인 접근 통제에 공히 사용될 수 있으며 또한 end-to-end security service를 제공하고 frame relay, cell relay, asynchronous transfer mode등의 network backbone 기술에 관계없이 사용될 수 있다. 아울러 asynchronous, X.25, SNA/SDLC, Bisync 프로토콜을 지원한다.

이 시스템은 아래에서 보듯이 여러 가지 선택 사양들로 구성되어 있어 사용자의 필요에 따라 적절히 선택, 설치할 수 있다.

1. 제공 기능

1.1 접근 제어

접근 통제를 위한 사용자 인증은 패스워드(fixed password), "WatchWord Generator", "WatchWord Soft-Token" 또는 스마트 카드(I.C. 카드)를 이용하는 네 가지 방법 중 선택하여 사용이 가능하다.

1.1.1 패스워드

일반적으로 널리 쓰이고 있는 방법으로, 6 자리부터 16 자리까지의 사용자가 정의한 패스워드를 사용하는 것이다.

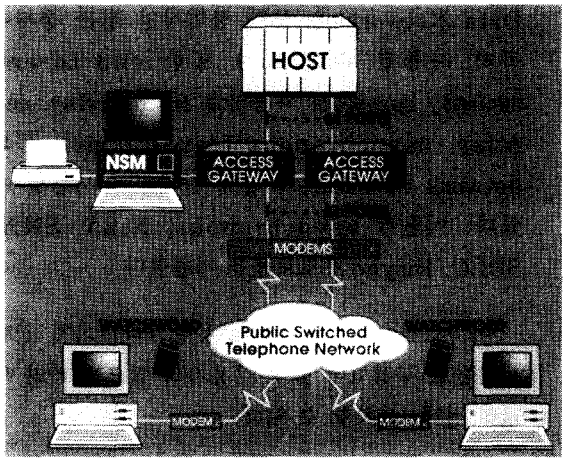
1.1.2 WatchWord Generator

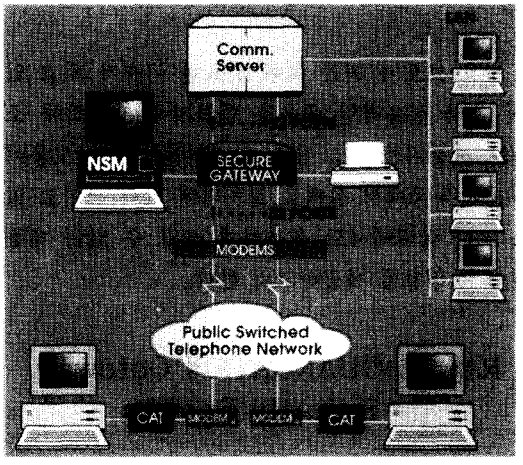
이것은 포켓 크기의 계산기 형태로 허가받은 사용자인지를 확인 한다. 특히 보안성이 없는 채널을 통한 시스템 접근시 질의와 응답(Challenge & Response)기법을 사용하여 일회용 암호로써 매번 시스템에 접근시 암호가 달라지도록 한 것이다. 또한 이것은 사람 대 컴퓨터뿐만 아니라 사람 대 사람의 인증에도 사용될 수 있다.

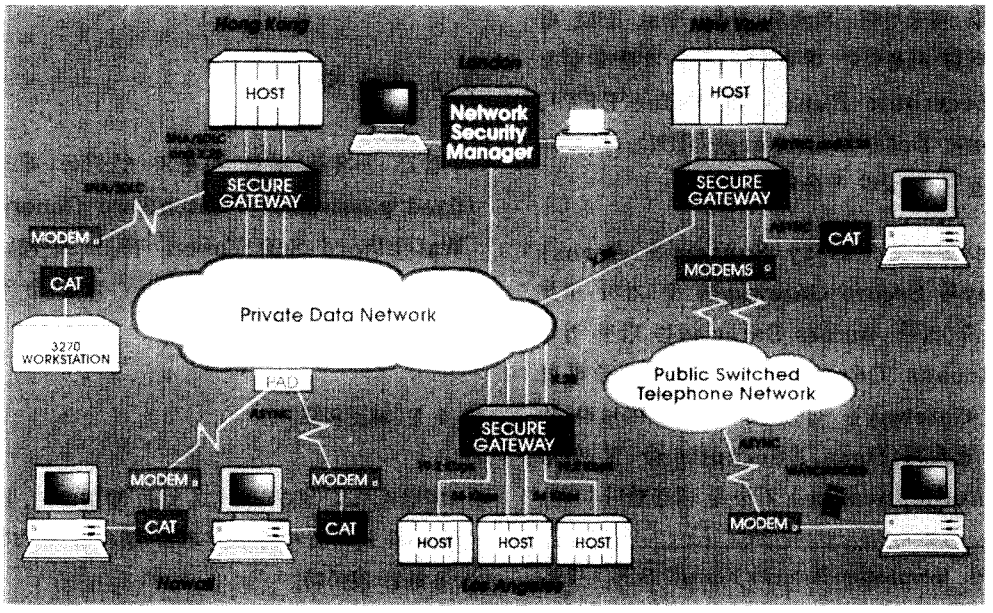
사용 방법

1. (이것은 평소에 계산기로 이용이 가능하므로) 분실로 인한 불법적 사용을 방지하기 위한 사용자 인증 확인시는 WatchWord

아 래







Generator에 Personal Identification Number(PIN)를 입력하여야 한다.

2. 터미널에 표시된 7자리 숫자(질의-challenge)를 WatchWord Generator에 입력한다.
3. 복잡한 계산 과정을 거친 후 표시되는 일회용 패스워드(7 자리, 응답-response)를 터미널에 입력한다.

1.1.3 WatchWord Soft-Token

이것의 기능은 1.1.2와 동일하며 차이점은 하드웨어가 아닌 소프트웨어 프로그램으로, 통신 프로그램인 Procomm이나 CrossTalk 등에 추가 설치하여 1.1.2와 동일한 기능을 수행케 하는 것이다.

1.1.4 스마트 카드의 사용

스마트 카드를 이용한 접근 제어 시 각 터미널에 스마트 카드 입력기(Cryptographic Authentication Terminal, CAT)를 설치하여 사용하며, 이것은 데이터의 기밀성과 무결성을 확보 하는 데에도 사용된다.

1.2 데이터의 암호화

민감한 데이터의 기밀성을 확보하기 위하여 널리 쓰이는 것이 데이터의 암호화이다. 이 시스템에서는 기본적으로 Data Encryption Standard(DES) 알고리즘을 사용하나 이 알고리즘이 미 정부의 수출 규제 대상이며 우방국(frendly country)의 등록된 금융 기관(registered bank)에 한하여 수출을 허가해 주고 있는 실정이다. 그러므로 금융 기관 외의 사용자에게는 제조 회사가 자체 개발한 수출이 가능한 알고리즘만 탑재하여 판매하고 있다.

1.3 데이터의 인증

데이터의 인증이란 보통 데이터의 무결성을 의미한다. 이 기능은 WatchWord II나 CAT를 사용하여 구현하며 메시지에 전자적 코드인 Message Authentication Code(MAC)를 첨부 함으로써 보낸 사람을 확인 할 수 있을 뿐만 아니라 일단 코드의 첨부 후는 그 메시지의 변경/변조를 방지할 수 있다. MAC을 계산하기 위한 알고리즘도 기본적으로 DES를 사용한다.

2. 구성 품목

2.1 WatchWord

2.1.1 RG500, WatchWord

이것은 포켓 크기의 계산기 형태로 응답(Response)계산용 알고리즘은 DES를 포함된 암호화 알고리즘이며, 선택할 수 있는 16가지 알고리즘이 제공된다.

이 알고리즘에 사용되는 비밀 키(Secret Key)는 시스템 시큐리티 담당자가 WatchWord에 각각의 비밀 키를 입력하여 배포한다. 만약 별도의 WatchWord Controller를 설치할 경우 2개의 서로 다른 비밀 키를 제공할 수도 있다.

또한 불법적 사용을 방지하기 위한 PIN은 시스템 시큐리티 담당자가 정의해 주거나 혹은 사용자가 선택할 수도 있다.

이 장비는 Tamper-Resistant로서 비밀키나 PIN 정보에의 고의적 접근을 차단한다.

Battery backup capacitor는 바테리 교환 시 비밀키나 PIN의 소실을 방지한다. 바테리의 수명 연장을 위하여 3분간 사용이 없을 시 자동으로 꺼지며 하루에 약 1시간 이용 시 한번의 바테리 교환으로 2년 정도의 수명을 제공한다.

2.1.2 RG551/RG552, WatchWord II

이 장비는 RG500을 향상시킨 명함 크기 정도의 계산기 형태로서 사용자의 인증 뿐만 아니라 메시지나 지불(Payment)의 인증에도 사용할 수 있다.

RG500과는 다르게 숫자만이 아닌 숫자, 문자를 다 이용할 수 있으며 한 개로 8 명까지 사용할 수 있으며, 또한 16개의 다른 응용 시스템에 사용할 수도 있다.

표시 장치는 2줄로서 1줄 당 12자 까지 표시가 가능하다. 첫째 줄은 숫자와 문자의 표시가 가능하고 둘째 줄은 계산기 형태의 숫자만 가능하다. 첫째 줄에 표시되는 메시지는 응용 시스템에 따라 달라질 수 있으며 이것은 변경이 가능하다.

이것은 질의와 응답(Challenge & Response) 기법을 이용한 "Secure Sign-on Standard(ANSI X9.26)"를 기초로 하였으며 인증 기능을 이용하기 위하여는 반드시 PIN을 입력하여야 한다.

메시지 인증

WatchWord II는 메시지 인증 코드(Message Authentication Code)의 계산에도 사용이 가능하다. 이 기능의 전형적인 사용 예는 지불 명령의 인가(허가)이다.

이 기능은 지불 메시지에 전자적인 코드(MAC)를 첨부 함으로서 보낸 사람을 확인 할 수 있을 뿐만 아니라 일단 코드의 첨부 후는 그 메시지의 변경/변조가 불가능해진다.

인증 방법

1. 사용자는 관련 데이터 item들을 순차적으로 입력한다.
2. 마지막 데이터 item 입력 후 이들 데이터 item들을 사용하여 MAC을 계산하여 보여준다.

각 데이터 item들은 보통 12자까지이며 최대 36자 까지의 숫자와 문자가 가능하다.

길이, 형태(숫자, 문자 등), 형식 등이 모두 응용 시스템에 따라 변형이 가능하다.

16개 까지의 비밀키가 비휘발성 메모리에 저장되어 있으며 이중 어느 것을 사용할지는 초기화 시에 정해 줄 수 있다.

이 MAC는 기본적으로 국제적인 표준 알고리즘인 ANSI X9.9/ISO 8731-1를 이용하여 8자리 Hexadecimal 값을 계산하고 응용 시스템의 특성에 따라 12자리 까지의 decimal digit을 계산해 낼 수도 있다.

또 하나의 사용 가능한 선택 기능으로는 메시지에 일련 번호를 부여하여 메시지의 중복을 방지할 수 있다.

MAC 확인/Non-repudiation 기능

다른 사용자에 의하여 계산된 MAC의 확인 기능이 있으며 또한 MAC은 단지 최초 발생자만이 발생시킬 수 있으므로 전자 서명과 같이 부인 봉쇄(Non-repudiation)의 목적으로도 사용될 수 있다. Network 응용 시스템에서는 다수의 사람으로 부터 받은 메시지를 확인할 수 있게 구성하여 사용할 수도 있다.

PIN 관리

WatchWord II에의 접근은 PIN에 의하여 통제된다. 그러나 PIN기능을 사용하지 않을수도 있으므로 다양한 적용이 가능하다.

위협시에 대비하여 제2의 PIN을 설정할 수 있으며 제2의 PIN 사용 시 호스트쪽에서 이를 감지하여 적절한 조처를 취할 수 있다.

PIN은 최대 8자리까지이며 최소 자리 수도 정할 수 있다. 사용자는 언제든지 PIN을 변경할 수

있으며 맨 처음 사용 시 강제로 PIN을 교체토록 할 수 있다. 한번 사용한 PIN의 재사용 및 단순한 PIN의 사용을 금지할 수도 있으며 PIN의 입력시 표시 장치에 나타나게 할 수도 있다.

잘못된 PIN의 입력 시 2 가지 처리 방법이 있다. 첫째는 PIN이 틀리다는 메시지를 보여주는 것이며 둘째는 틀린 결과값을 보여 주는 것이다. 첫번째 경우 정해진 회수 만큼 잘못된 PIN을 연속 입력 하게되면 더 이상 사용이 불가능(Lock) 해져 해지용(Unlock) PIN의 입력이나 시큐리티 담당자 만이 이를 풀어 줄 수 있다.

하나의 WatchWord II는 8명의 사용자에게 각 2개의 PIN을 할당할 수 있다. 즉16개의 키를 제공하며 이것은 WatchWord Verify, MAC Generate, MAC Verify Unlock등과 같이 별개의 용도에 사용될 수도 있다. 또한 이것은 서로 다른 16개의 응용 시스템의 접근 제어에 사용될 수도 있다는 것을 의미한다.

이것은 계산기로도 사용할 수 있으나 이 계산기 기능을 취소할 수도 있다.

2.2 Cryptographic Authentication Terminal(CAT)

CAT는 스마트 카드 입력기로서 터미널과 PC로부터의 접근 제어, 데이터의 암호화/복호화 그리고 인증에 사용할 수 있고 EFT와 EDI 등에도 널리 쓰이고 있다.

터미널이나 PC와는 RS-232C asynchronous로 연결되며 속도는 300-19,300 baud로 모뎀과 PC와의 사이에 설치된다.

스마트 카드는 기본적으로 암호 키를 저장하는데 사용되나 사용자의 응용 시스템에 따라 지불 허락, 로그-온 절차 등의 여러 가지 데이터의 읽기나 쓰기에 사용될 수 있다.

근본적으로 이것은 여러 가지 시큐리티 기능을 수행하는데 사용되고 설치된 한대의 CAT가 호스트에서 돌아가는 여러 가지 응용 시스템에 따라 서로 다른 시큐리티 기능을 수행하는데 사용될 수 있다.

응용 시스템 개발을 용이하게 하기 위하여 Application Programming Interface (API)를 제공한다.

PIN pad와 LCD 표시 장치가 있는 것과 없는 것이 있으며 PIN pad가 있는 것은 직접 PIN을 입력하거나 PIN을 변경할 수 있고, PIN pad나 LCD 표시 장치가 없는 것은 PC나 터미널의 키보드를 통하여 입력한다.

아래와 같은 시큐리티 관련 ANSI와 ISO의 표준을 지원한다.

ANSI X9.9/ ISO 8730/ISO 8731-1	Authentication of stored or transmitted data
ANSI X9.17/ISO 8732	Key management & exchange of authentication and encryption keys
ANSI X9.26	Sign-on authentication for local and remote applications
ANSI X9.23/ ISO 10261-1	Encryption and decryption of local files and transmitted data
ANSI X12.42/X12.58	Electronic Data Interchange(EDI)
ANSI X3.92/X3.106/	Data Encryption Algorithm and ISO 8732 modes of operation

2.3 Network Security Manager(NSM)

2.3.1 Gateway Security Module(GSM)

이것은 호스트의 front-end Security Processor로서 호스트에의 접근 통제 뿐만 아니라 온-라인 키 분배 및 네트워크의 시큐리티 관리 등을 제공한다. 이것은 tamper-resistant 모듈로써, 원격지에 설치된 CAT와 호스트 사이에 주고 받는 데이터의 인증 및 암호화/복호화에 사용되는 암호 키를 저장하고 있다.

작은 시스템 환경하에서는 모니터와 키보드를 추가하여 Network Security Manager로 사용할 수 있다.

2.3.2 Network Security Manager(NSM)

NSM은 GSM에 모니터와 키보드를 추가한 것으로 모든 시큐리티와 네트워크의 중앙 관리를 수행한다. 여러 대의 GSM으로 구성된 큰 시스템 환경하에서는 만약 NSM에 문제가 발생하면 여러 GSM 중 적절한 것을 NSM으로 대체, 사용할 수 있다.

NSM은 사용자들의 데이터를 보호(암호화, 인증, 암호화+인증)하는데 사용되는 암호 키를 스마트 카드나 WatchWord에 할당하며 스마트 카드 사용자에게는 PIN도 할당한다.

데이터 베이스(스마트 카드의 추가, 소거 등)는 NSM에 의하여 자동으로 GSM에 업데이트된다.

미리 정의해 놓은 시큐리티 관련 문제들은 각 GSM으로 부터 NSM에 보고하도록 되어 있으며 NSM 콘솔에서 통신 회선을 재 조정하거나 분실된 스마트 카드 관련 데이터의 소거 및 헥커의 불법적 접근의 감시 등을 할 수 있다.

소프트웨어/펌웨어의 업그레이드는 NSM에 설치된 카세트 테이프 장치에 의하여 이루어지며 NSM에 설치한 후 연결된 GSM에는 NSM에 의하여 자동으로 이루어진다.

시스템 사용에 대한 39일간의 감사 기록(Audit Trail)도 유지한다.

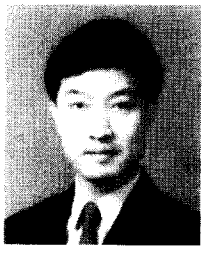
3. 지원하는 시큐리티 관련 표준들

ANSI X3.92, X3.106, X9.9, X9.17, X9.23, X9.26

FIPS 46, 113,140

ISO 8730, 8731-1, 8732, 10126

□ 著者紹介



박 태 완(정회원)

1981년 울산공과대학 전자계산학과(학사)
1982년 ~ 1987년 홍콩 상하이 은행 부산/서울 지점, 전산 책임자
1987년 ~ 1989년 하이야트 리젠시 부산, 전산 실장
1989년 ~ 1991년 내쇼날 호주 은행 서울 지점, 전산 실장
1991년 ~ 1993년 University of London, Royal Holloway College
Master of Science in Information Security
1994년 ~ 현재 Information Security Korea(I.S.K.) 대표
CISA, Certified Information System Auditor