韓國通信情報保護學會誌
第1卷, 第1號, 1991. 4

# 정보통신 Security 체제의 개요와 동향

김 동 규*

통신기술의 발달은 정보화 사회로 진입하는 현 시점에서 더욱 그 가치와 요구를 증가시키고 있으며 이에 따라 네트워크에 가입하는 사용자와 그 사용자들의 비밀정보(Secure information)들이 점점 늘어나고 있는 추세이다. 이러한 비밀 정보들은 통신하는 과정에서 악의있는 공격자들에 의해 쉽게 액세스(Access) 될 수 있고 심지어는 변경, 위조되어 정당한 사용자들에게 심각한 피해를 주는 위험에 노출되어 있는 상황이다. 따라서 이러한 비밀정보들의 안전성을 보장할 수 있는 다양한 메카니즘과 서비스들이 절실히 요구되고 있는 실정이다.

## 1. Security 체제의 목표

현재의 안정성(Security) 기술은 정보의 내용변경, 불법적 유출, 순서변경, 미확인 발신자 및 수신자 등과 같은 위협으로부터의 안전한 통신에 대한 요구를 완전히 충족시켜주지 못하는 상황이다.

Branstad는 안전한 통신을 이루기위한 최소한의 요구사항으로 다음과 같은 5S를 제시하였다.

- Sealed : 정당하지 않은 발견으로부터의 데이타 보호
- Sequenced : 발견되지 않은 상실이나 중복으로부터의 데이타 보호
- Secret : 정당하지 않은 내용의 노출로부터의 데이타 보호
- Signed : 데이타 송신자의 확인
- Stamped : 데이타 수신자의 확인

이러한 요구사항들을 해결하기 위한 노력의 결과로 ISO(International Organization for Standardization)/IEC(International Electrotechnical Commission) JTC1/SC21에서는 OSI(Open Systems Interconnection) 환경에서 안전성을 위한 표준 참조모형인 OSI Security Architecture(ISO DIS 7498-2)를 발표하였다. OSI Security Architecture에서는 대부분의 안전성 서비스를 OSI 응용계층, 프리젠테이션 계층 그리고 트랜스포트 계층에 위치시켰으며, 정의된 안전성 서비스들은 다음과 같다.

- 신분확인(Identification/Authentication) 서비스
- 액세스 제어(Access Control) 서비스
- 데이타 무결성(Data Integrity) 서비스
- 데이타 비밀성(Data Confidentiality) 서비스
- 부인봉쇄(Non-Repudiation) 서비스

비록 OSI Security Architecture는 매우 추상적이고 불완전한 상태이지만 안전성 서비스를 정의하고 안전성 메카니즘을 기술함으로써 안전성 문제를 OSI 환경에서 해결할 수 있다는 가능성을 제시하고 있다.

* 정회원, 아주대학교 전자계산학과

또한 미국의 NIST(National Institute of Standards and Technology)에서는 데이타의 비밀성과 무결성 서비스를 트랜스포트 계층에 위치시킨 SP4를 발표하였으며, CCITT(International Consultative Committee on Telephony and Telegraphy)에서 발표한 X.411은 X.400에 사용되는 안전한 전문을 정의하고 있다. ECMA(Europlean Computer Manufacturers Association)에서는 안전성을 논리적으로 완전하게 분해한 기능적 요소인 Facility의 개념을 도입하여 안전성 서비스를 제공하는 프레임 워크를 OSI 응용 계층에 정의하였다. LAN(Local Area Network)의 보안을 위해 IEEE(Institute of Electrical and Electronic Engineers)에서는 LLC (Logical Link Control)와 MAC(Media Access Control) 사이에 SDE(Secure Data Exchange) 프로토콜을 위치시킨 SILS(Standard for Interoperable LAN Security)를 발표하였다.

## 2. OSI 안전성 서비스

OSI Security Architecture에 정의된 5가지 서비스를 살펴보면 첫째, 통신 관련자들의 신분을 확인하고 해당 통신에 참여할 자격 유무를 검사하는 신분확인(Authentication) 서비스가 있다. 신분확인은 연결지향(Connection oriented) 통신에서의 통신 당사자간에 신분확인과 자격유무의 점검을 위한 대등실체 신분확인(Peer entity Authentication)과 무연결지향(Connectionless oriented) 통신에서의 데이타 발신처의 신분확인과 자격유무를 점검하는 발신처 신분확인(Data origin Authentication)으로 나눌 수 있다. 둘째, 신분확인 서비스에 의해 사용자의 신분이 확인되고 나면 명시된 자원(Resource)에 대하여 액세스(Access) 할 자격이 있는가를 점검하고, 다음에는 어떤 유형의 액세스 동작(Access Operation)을 수행할 수 있는가에 대한 허락을 받도록 하여야 한다. 이러한 동작을 액세스 제어(Access Control)라 하며, 액세스 제어에는 사용자가 자원을 적법하게 사용하는가를 확인하는 사용자의 정당성(User Agent Authorization)과 대등실체간에 액세스 하고자 하는 자원이 정당한가를 확인하는 대등실체의 정당성(Peer entity Authorization)으로 구별된다. 셋째, 데이타 비밀성(Data Confidentiality) 서비스는 통신되는 데이타가 불법적으로 그 내용이 노출되는 것을 방지하는 서비스로서 전체 전문에 대해 암호화를 시키는 것과 선택적 필드(field)에 대해 암호화 시키는 것으로 구분된다. 네트워크상으로 전송되는 정보들의 비밀성을 유지하기 위하여 일반적으로 암호화를 사용하는데 암호화 시스템은 크게 두 분류로 나누어진다. 그 하나는 1977년에 IBM에 의해 제시된 DES (Data Encryption Standard) 암호화 방식이며 또 하나는 1976년 Diffie-Hellman에 의해 제시된 공중키(Public Key) 암호화 방식에 기초한 RSA(Rivest, Shamir and Adleman) 시스템이다. 넷째, 데이타 무결성(Data Integrity) 서비스는 통신되는 데이타의 정확성을 점검하는 서비스로서 둘 또는 그이상의 Communicant(전문의 수신자나 송신자로서 행동하는 자)들이 전문을 주고 받을 때 수신된 전문이 전송되는 과정에서 수정됨이 없이 도달되었는지를 확인하는 서비스를 말한다. 데이타 무결성 서비스를 위한 대표적인 메카니즘으로는 MAC(Message Authentication Code), MDC(Manipulation Detection Code), QMDC(Quadratic MDC) 등이 있다. 마지막으로, 부인봉쇄(Non-repudiation) 서비스는 이미 발생한 통신사실을 부인할 수 없도록 하는 것으로 전송된 데이타나 내용에 대한 발신 사실을 부인할 수 없도록 하는 발신부인(Non-repudiation, origin)과 수신된 데이타나 내용에 대한 발신사실을 부인할 수 없게 하는 수신부인(Non-repudiation, delivery)으로 나누어 생각할 수 있다.

## 3. LAN의 안전성 서비스

LAN은 Data Link 계층이 Broadcasting 성질을 가지므로 불법적인 사용자들로 부터의 공격이 용이하다. 그러므로 현재의 SILS(Standard for Interoperable LAN Security) 연구는 이러한 불법적인 공격을 막기위해 진행되고 있다. ISO 7498-2(ISO Security Architecture)에서는 기본적인 다섯가지 안정성 서비스중에서 Data Link 계층에 적당한 서

비스는 데이타의 비밀성으로 추천하고 있다. 그러나, ISO Security Architecture는 공중교환망(Packet Switched Networks)과 광역망(Wide Area Networks)에 이용하기 위하여 개발되었고 국지망(Local Area Networks)에서는 광역망의 Network 계층의 특징을 Data Link 계층에서 갖고 있다. 그러므로 LAN의 Data Link 계층에 ISO 7498-2의 Network 계층에 적당한 서비스, 즉, 데이타의 비밀성(Data Confidentiality)과 함께 신분확인(Authentication), 액세스 제어(Access Control), 그리고 데이타의 정확성(Data Integrity) 서비스를 구현시킬 수 있다.

이러한 필요성, 즉, LAN 사용자들 사이의 안전한 통신을 제공하기 위해 IEEE 802.10 SWG(Security Working Group)은 SILS(Standard for Interoperable LAN Security)를 발표하였다. 이것은 OSI 7계층 모델(ISO 7498)과 OSI Security Architecture (ISO 7498-2)를 따르고 있다. SILS의 목표는 안전한 IEEE 802 LAN 제품을 제공하기 위해 필요한 서비스, 프로토콜, 데이타 포맷 그리고 인터페이스의 표준안을 제공하는 것이다. 이를 위해 IEEE 802.10은 SILS를 다음 4가지 영역으로 세분화하였다.

□ part A－Model(P802.10A)

part B, part C, 그리고 part D 표준안의 관련성을 설명한다.

| | ISO 7498-2 Services | + *LAN Services* |
|---|---|---|
| Layer 7 Application | Authentication, Access Control, Data Confidentiality, Data Integrity, Non-repudiation | Authentication, Access Control, Data Confidentiality, Data Intergrity, Non-repudiation |
| Layer 6 Presentation | Data Confidentiality | Data Confidentiality |
| Layer 5 Session | | |
| Layer 4 Transport | Authentication, Access Control, Data Confidentiality Data Integrity | Authentication, Access Control, Data Confidentiality Data Integrity |
| Layer 3 Network | Authentication, Access Control, Data Confidentiality Data Integrity | Authentication, Access Control, Data Confidentiality Data Intergrity |
| Layer 2 Link | Data Confidentiality | *Authentication、Access Control,* Data Confidentiality *Data Intergrity* |
| Layer 1 Physical | Data Confidentiality | Data Confidentiality |

그림 1. 제안된 서비스의 비교

□ part B－Secure Data Exchange(P802.10B)
MAC(Media Access Control)Sublayer 상위에서 안전한 무연결 서비스를 제공한다.

□ part C－Key Management(P802.10C)
안전성 서비스를 제공하는 SDE(Secure Data Exchange) sublayer에서 사용하는 키(Key)를 제공한다.

□ part D－Security／System Management
각각의 안전성 프로토콜을 객체(Object)로 간주하고 총괄적으로 관리한다. 현재 part A와 part B는 초안(Draft)이 발표되었고 part C와 part D는 연구가 진행되고 있다. 그림 1에 ISO 7498-2 서비스와 LAN 서비스를 보여주고 있다.

## 4. 안전성 메카니즘

OSI 구조에 특별히 유관한 메카니즘은 크게 예방 메카니즘, 검출 메카니즘, 복구 메카니즘의 세가지 유형으로 나눌 수 있다(이들은 서로 중복되는 경우도 있다). 이러한 메카니즘은 암호화, 디지탈 서명, 액세스 제어, 데이타의 정확성, 실체의 신분확인, 교통의 Padding, 경로제어, 공증, 세방향 교환이다.

각각의 메카니즘에 대하여 알아보면 암호화(encipherment／encryption)는 데이타나 교통 흐름 정보의 기밀성을 제공하며 다수의 다른 메카니즘을 보완할 수 있다. Link encryption, end-to-end encryption, 대칭형／비대칭형 encryption, 그리고 키 배분 프로토콜과 키 배분 센타 형태의 키 관리가 암호화와 관련되는 인자들이다. 디지탈 서명 메카니즘의 요체는 비밀 키를 사용하지 않고서는 데이타 전문을 생성 할 수 없다는 사실을 이용하는 것이다. 다음 3가지 조건으로 대별할 수 있다. 비밀키의 소지자 아닌 어느 누구도 서명된 데이타 단위를 생성할 수 없다는 제삼자 조건, 수신자는 서명 데이타 단위를 생성할 수 없다는 송신자 조건이다. 액세스 제어는 사용자의 신분이 확인된 후에 그 사용자가 명시된 자원을 액세스할 자격이 있는가를 점검하고 다음에는 어떤 유형의 동작을 수행할 수 있는가에 대한 허락을 받도록 한다. 데이타의 정확성은 Checksum과 Sequencing(Timestamping)을 사용하여 전송된 데이타가 사고 혹은 고의로 수정되지 않았음을 확인할 수 있다. 실체의 신분확인은 패스워드와 암호화 메카니즘을 이용하여 신분확인을 수행한다. 교통의 padding은 실제의 데이타가 아닌 정보를 안전성 제공의 목적으로 고의로 삽입할 수 있다. 경로제어는 어떤 수준의 안전성을 달성하는데에 필요하거나 유용한 전송경로를 선택할 수 있도록 한다. 공증(notarization)은 안전성 서비스를 제공하는데 있어 송신자와 수신자가 아닌 제삼자의 위치에 있는 중재자의 개입을 통하도록 한다. 이는 보통 디지탈 서명 메카니즘과 함께 사용되며 송신사실의 부인과 수신사실의 부인을 봉쇄하는데 필요하다. 세방향 교환(3-way handshake)은 정보가 전달되는 과정에 상실되거나 중복되는 것을 정확히 검출하여 필요한 동기를 행할 수 있게 한다. 데이타의 정확성 서비스를 실현하는데 유용한 메카니즘이다.

## 5. 기술 동향

현재까지의 안전성 서비스를 위한 관련 기술동향을 살펴보면 다음과 같다.

- ISO 7498／2 OSI framework 정의
- SC21의 각 WG, SC20의 각 WG에서 Working Draft를 수시로 생성
- SC27 조직 진행중(Security에 관한 사항을 통합하여 표준화 연구추진)
- ISO TC68 Banking Security
- ECMA TC32의 각 TG에서 Security 표준화 연구 진행중
- NIST의 SIG-SEC에서 OSI Security System 구현 표준화 진행중
- NSA에서 SDNS SP3와 SP4 표준 Protocol 제정
- IEEE 802. 10 SILS(LAN Security)가 1988년에 조직된 이래로 급속하게 LAN Security 표준 제정 활동을 진척 시키고 있음
- ISSA에서 Security 관련 국제 표준화 활동과는 별개로 Vendor Association 위치에서의

각종 Security 제품 개발 촉진활동을 활발히 전개하고 있음

현재 PC 레벨의 다수의 제품들이 시장에 나오고 있고 최근부터 Network 환경관련 Security 제품 개발에 역점을 두기 시작하였음.

- 단독 System, Network, Internet, Distributed System의 순으로 Security System은 점점 복잡도를 더해가며 기술적으로 해결되어야 할 과제들이 난이도를 더하여 간다.

현재 단독 System 환경에서는 Confidentiality의 전부, Integrity의 일부가 이해되고 있고 Network 환경에서는 Confidentiality의 전부가 이해되고 있는 수준인 것으로 평가되나 그 이상은 이해도가 극히 미약하거나 전무한 실정이므로 앞으로 먼길을 걸어가야 할 노상에 있다고 말할 수 있다.

## 6. 결 론

현재까지의 국제 기술동향을 볼 때 다양한 환경에서 양단간에 다양한 유형의 데이타를 효율적으로 전송하는 반송기술은 괄목할 수준까지 진척되었고 이제는 다양한 제품들이 산업체에서 생산 공급되고 있다.

그러나, 새로운 문제는 양단간에 데이타가 반송되는 과정에서 정보통신의 안전성에 관한 다양한 장애가 발생된다는 사실이다. 이 장애는 비 고의적인 에러조건에 해당되는 것도 있고 고의적인 공격의 결과로 야기되는 것도 있다. 어느 쪽이건 통신되는 정보에 대한 사용자의 안전성 요구사항을 충족시킬 수 있어야만 정보통신이 사용될 수 있다.

사용자의 요구사항을 충족시키기 위해서는 안전성에 관한 기술적인 문제가 해결되어야 한다. 기술적인 해결책은 보편적인 적용을 위하여 표준화되어야 한다. 국제 연구계의 연구결과를 바탕으로 다양한 표준화 기관이나 기구에서 국제표준 제정을 활발히 추진하고 있다.

한국에서도 이러한 기술과 표준화 양면에서의 연구와 실용화 작업이 조직적으로 진척되어야 할 필요에 직면해 있다. 행정 전산망, 금융 전산망, 연구교육망, 국방망, 공안망, 국민생활 정보망, 의료 보건망 등의 국가 기간 전산망, 급격한 수요확대가 일어나고 있는 각종 국지망(LAN), 정보화 사회를 지향하는 국가 정책으로서의 통신산업 개방확대정책에 보조를 맞춘 산업체 중심의 다양한 부가가치 통신망(VAN) 등에서 정보통신 안전문제가 긴급한 과제로 부상되고 있음은 주지의 사실이다. 정보통신 안전체제는 다양한 구성요소를 지니는 복잡한 시스템이다. 그러므로 실용화 제품 레벨에서의 광범위한 수요 발생에 직면하여 기술적인 해결책의 정립과 호환성 있는 제품 개발을 가능케 하기 위한 표준 모형의 개발요구에 직면하여 있다.

우선적으로 이 분야의 국제기술동향에 편승하여 내용을 소화하고 이와 병행하여 우리 나름대로의 독자적인 연구개발을 추진하여 그 결과로써 국제 기술동향에 기여하고 또 표준화를 통한 실제적용을 확대하여 나감으로써 정보화 사회의 정착에 필수적인 하나의 관건을 달성할 수 있다.

## □ 著者紹介


**김 동 규(正會員)**

1944年生

서울大學校 工科大學 卒業(學士)

서울大學校 自然科學大學院 卒業(碩士)

美國 KANSAS 州立大 大學院 卒業(Ph.D. 電算學, 情報通信 專攻)

美國 KANSAS 州立大 電算學科 講師

現在 아주大學校 電算學科 教授

研究 關心 分野 : 컴퓨터 네트워크, 情報通信 프로토콜 엔지니어링, 情報通信 Security, 分散 處理 시스템