The Journal of Korean
Institute of CALS/EC
Vol. 1, No. 1, Aug. 1996

CALS의 단계별 구현을 위한 보안기술

김 중 인*, 김 석 우**

Security for CALS Implementation

Joong-in Kim, Seok-Woo Kim

Abstract

Recently the interests in NII, CALS/EC, and security are rapidly increasing. However, only one of the security issues for CALS implementation, i.e., the security for EDI implementation, has been presented in the literature. No comprehensive discussion about CALS security including other CALS applications exists. This paper intends to present such a comprehensive analysis for the security requirements and standards for the well-recognized two-phase CALS implementation. We present a framework for CALS security encompassing security protocols and systems that are arranged into the framework in terms of the CALS implementation phases, application systems, and communication modes. This framework is followed by brief descriptions of the security services and mechanisms for each CALS application.

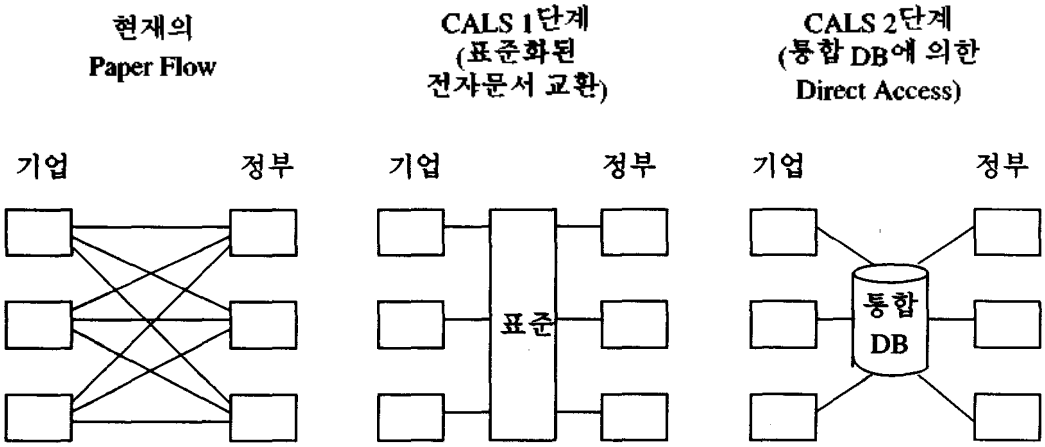
*홍익대학교 경영정보학과

**한국전자통신연구소

1. 개요

미국의 NII(National Information Infrastructure), 유럽의 Big Bang, 일본의 신사회 자본, 싱가폴의 TI2000 등과 함께 우리 한국도 정보화시대에 부응하는 정책으로 국가 초고속 정보통신망 구축계획을 핵심전략사업으로 선정하여 추진중에 있으며, 이는 CALS(Computer-aided Acquisition and Logistics Support 또는 Continuous Acquisition and Life-cycle Support, 그리고 최근에는 Commerce At the Light Speed) 개념에 기반을 두고 있다 [김철환, 김성회, 1995][최용락 등, 1995]. 국방군수산업을 중심으로 시작된 CALS 는 이제 군수분야 및 무기체계획득뿐만 아니라 각종 제조업중심의 일반 산업분야로 확대되어 통합정보시스템 및 전자상거래(Electronic Commerce: EC) 개념으로 발전하고 있다.

CALS 구현의 1 단계 목표는 표준화를 통한 디지탈정보의 교환이고, 2 단계 목표는 통합된 데이타베이스(Integrated Data Base: IDB)를 구축하여 디지탈정보를 공유하면서 제품의 전 수명주기에 활용한다는 것이다 <그림 1> [김철환, 김성회, 1995][신장균 등, 1995][van Herwijnen, 1994]. 여기서 통합 데이타베이스란 논리적으로 통합된 것으로 다양한 형태와 성질의 정보를 어디에서나 투명하게 실시간에 액세스할 수 있다는 의미이지 물리적으로는 분산된 데이타베이스를 의미한다. 이러한 IDB 개념이 민간회사에 적용되면 IPDB(Integrated Product Data Base)라 불리고, 군수 분야에 적용되면 IWSDB(Integrated Weapon System Data Base)로 불린다.



<그림 1> CALS 의 1, 2 단계 구현 목표

CALS 의 1, 2 단계구현을 위해서는 분산개방형 시스템 구조를 이루는 여러 정보 기술이 복합되어야 하는데 필요한 핵심 정보기술로는 표준화 기술, 초고속 통신망기술, 통합 데이타베이스기술, CIM/CAD/CAM 기술, 멀티미디어기술 및 정보보호 기술 등이 있다. CALS 에서는 통신망을 통해 표준화된 정보를 교환하고 (단계 1), 정보를 공유하므로 (단계 2) 전송과정에서 발생하는 정보의 노출, 파괴, 내용변경, 분실 및 전자사서함 과 통합 데이타베이스에 저장된 정보의 불법적 유출, 변조, 파괴, 위조된 정보 유통 등을 방지할 수 있는 보안체계가 필요하다 [신장균 등, 1995][이경상, 1995]. 본 논문에서는 이러한 보안위협에 대해서 정보를 안전하고 신뢰성있게 보호할 수 있는 보안기술에 대해 살펴보기로 한다.

CALS 구현의 1, 2 단계 목표인 표준화된 정보교환과 통합 데이타베이스의 공유를 구현할 수 있는 응용시스템들로는 EDI, 멀티미디어 전자우편, 디렉토리(directory) 시스템 및 분산개방형 데이타베이스 시스템이 있으며, 이들 각 시스템의 정보보호를 위한 보안기술도 함께 구현되어야 한다. 그러나 지금까지 국내에서 CALS 에 필요한 보안기술에 대해서는 EDI 보안만을 다룬 논문만이 발표되었고 [이경상, 1995], 다른 응용시스템들을 모두 포함한 종합적인 보안기술에 대한 분석이 없는 실정이다. 또한, CALS 의 1, 2 단계별 구현에 맞추어 보안기술도 단계별로 적용할 수 있도록 CALS 의 구현 단계와 정보보호기술을 mapping 시켜주는 프레임웍(framework)의 제시도 필요하다. 따라서 본 논문에서는 CALS 의 1, 2 단계 구현에 필요한 응용시스템들에 적용할 수 있는 표준화된 보안기술, 즉 보안 프로토콜 표준 및 보안 시스템 표준들을 CALS 구현 단계별, 응용 시스템별, 통신방식별로 분류하여 이를 프레임웍으로서 제시하였으며 <표 1>, 각각의 CALS 응용 시스템별로 필요한 보안서비스와 보안 메카니즘에 대해서는 본문에서 설명하였다.

<표 1> CALS 구현단계별 보안 프로토콜 및 보안 시스템 표준

CALS 구현단계	응용 시스템	통신 방식	보안 프로토콜 및 보안 시스템 표준
1 단계 (표준화를 통한 디지탈 정보 교환)	비정형화된 문서, 도면 및 멀티미디어 파일 교환을 위한 E-Mail 시스템	비연결형 통신 (connectionless, message-oriented 또는 store-and-forward)	S/MIME MOSS(PEM/MIME) MHS (X.400) MSP
	정형화된 문서 교환을 위한 EDI 시스템	비연결형 통신	UN/EDIFACT 보안 ANSI X.12 보안 Pedi (X.435) 보안

	분산개방형 디렉토리 시스템	연결형 통신 (connection-oriented, session-oriented, 또는 interactive and real-time)	X.500
2 단계 (통합데이타베이스를 통한 디지탈 정보 공유)	분산개방형 데이타베이스 시스템	연결형 통신	Kerberos DCE SESAME 데이타베이스 보안

<표 1>에서 비연결형(connectionless, store-and-forward, 또는 message-oriented) 통신방식은 사용자(cleint)가 서버(server)에 접속한 후에 계속 서버와의 연결을 유지하지 않고 메시지나 문서를 보내어서 축적시키고 나면 연결이 끊기고, 서버가 메시지 수신자에게 전달하는 store-and-forward 방식을 말한다. 연결형(connection-oriented, session-oriented, 또는 interactive and real-time) 통신 방식은 일반적으로 말하는 client/server 시스템의 통신방식으로서 사용자가 서버와의 연결을 유지하는 기간, 즉 서버에 로그인(login)해서부터 로그아웃(logout)할 때까지의 세션(session)동안 interactive 하게 메시지를 요구(request), 응답(response)형태로 주고 받는 것을 말한다 [Hale, Mannarino, 1996][Stallings, 1995a].

보안서비스란 보안위협 및 보안침해사고에 대비한 정보보호기능 들을 정의하며, 보안서비스의 지원 또는 구현을 위하여 여러가지 보안메카니즘들이 결합되어 이용된다. 즉 보안서비스는 어떤(what) 보안기능이 제공되어야만 하는지를 정의하며, 보안메카니즘은 보안서비스들을 어떻게(how) 구현할 수 있는지, 즉 보안서비스를 구현할 수 있는 방법들을 정의한다. 이러한 보안서비스와 보안메카니즘이 결합되어 실제 보안시스템으로 구현되거나 플랫폼에 무관한 시스템구현을 위한 보안프로토콜 규격(specification)으로 정의된다.

2. CALS 구현 1 단계에 필요한 보안 기술

표준화된 디지탈 자료 파일을 교환하는 기술은 정형화된 문서를 교환하는 EDI 와 비정형 문서, 멀티미디어 파일 및 도면을 교환하는 e-mail 시스템으로 나뉘어진다. EDI 는 정형화된 문서중심으로 사용되고 있고 이로 인해 CAD 와 같은 도면이나 비정형화된 멀티미디어 정보를 수용하지 못하는 제약을 가지고 있다 [이경상, 1995]. 따라서 비정형 정보를 교환하기 위해서는 e-mail 시스템을 사용하게 되며, 비정형 정보에 대한 CALS 표준을 정의하고 있는 MIL-STD-1840 의 개정판으로서 현재 작성중인 1840C 는 비정형 정보를 인터넷 e-

mail 프로토콜인 MIME(Multipurpose Internet Mail Extensions)을 사용하여 전송하도록 정의하고 있다 [신동익, 1995]. CALS 를 위해 제정된 정형화된 문서표준으로는 국제표준인 UN/EDIFACT, 미국표준인 ANSI X.12, ITU-T 표준인 Pedi (X.435)가 있고, MIL-STD-1840 에서 정의된 비정형 문서 및 도면 표준으로는 SGML, CGM, CCITT Group 4 (raster), IGES, STEP 및 PDES 등이 있다. EDI 와 e-mail 은 비연결형(connectionless-oriented, message-oriented 또는 store-and-forward) 통신방식으로서 하나 이상의 데이타 단위(data unit)로 이루어진 메시지 스트림(message stream)을 대상으로 한다. 본 절에서는 먼저 e-mail 보안 시스템들인 S/MIME(Secure MIME), PGP(Pretty Good Privacy), PGP/MIME, PEM(Privacy Enhanced Mail), MOSS(MIME Object Security Services 또는 PEM/MIME), X.400 MHS(Message Handling System) 및 MSP(Message Secure Protocol)의 보안서비스와 특징들에 대해 살펴보고, 다음으로 EDI 표준들인 UN/EDIFACT, ANSI X.12 와 Pedi (X.435)의 보안에 대해서 살펴본다.

2.1 E-Mail 보안

현재 사용 또는 개정중인 전자우편 보안 프로토콜로는 인터넷의 TCP/IP 프로토콜을 사용하는 S/MIME, PGP, PGP/MIME, PEM, MOSS(또는 PEM/MIME)과, ITU-T(구 CCITT)와 ISO/IEC 의 공동표준으로서 OSI(Open Systems Interconnection) 프로토콜을 사용하는 MHS (X.400), 미국 NSA(National Security Agency)의 SDNS(Secure Data Network System) 개발작업의 하나로서 MHS 에 보안서비스를 제공하기 위해 개발된 MSP 가 있다. SDNS 는 OSI 네트웍에 보안서비스를 제공하기 위한 프로토콜 개발작업으로서 MHS 의 첫 번째 버젼(1984)에서 보안서비스가 제공되지 않고 단순히 전자우편의 교환에만 사용되었기 때문에 MHS 에 보안서비스를 제공하고 국방 및 군사용으로 사용하고자 1986 년에 개발하기 시작하였다. MSP 를 이용한 미국 국방용 보안 프로젝트로 MISSI(Multilevel Information System Security Initiative)가 있다 [Hale, Mannarino, 1996]. 한편, MHS 도 새로운 권고안(1988)에서는 자체적인 보안서비스들을 포함하여 확장되었다. 따라서, 민간용 CALS 를 위해서는 인터넷 전자우편 보안 표준 프로토콜들인 S/MIME, PGP/MIME, PEM/MIME 이나 OSI 의 MHS 등을 이용하고, 국방/군사용 CALS 를 위해서는 MHS 기반하에 MSP 의 사용을 검토해 볼 수 있을 것이다. 그러나 MHS 와 MSP 의 현재 버젼들에서는 S/MIME, PGP/MIME 또는 MOSS 에서지원하는 멀티미디어 데이타를 지원하지 않는 점을 고려해야만 하며, 이에 대한 연구가 필요하다. 본 절에서는 이러한 프로토콜들에서 제공하는 보안서비스와 특징들에 대해 살펴보기로 한다.

2.1.1 S/MIME

S/MIME working group 에 의해 개발되어 IETF(Internet Engineering Task Force)주관하의 인터넷 RFC(Request For Comments)로서 발표를 계획중인 S/MIME 은 PGP 나 PEM 과 마찬가지로 데이타 비

밀성, 데이타 발신처 인증, 데이타 무결성 및 발신처 부인봉쇄 서비스를 제공한다 [RSA, 1996]. 그러나 S/MIME 은 PGP 나 PEM 과는 달리 텍스트 메일뿐만 아니라 멀티미디어 데이타 보안도 포함하고 있으며, 다음에 설명하는 PGP/MIME 의 문제점인 확장성(scalability)과 MOSS(또는 PEM/MIME)의 문제점들인 상호호환성(interoperability) 및 backward compatibility 를 극복한 프로토콜로서 S/MIME working group 에 의해 제안되고 있으나, 아직 RFC 로 채택되거나 실제로 구현되지는 않은 상태이다.

2.1.2 PGP 와 PGP/MIME

인터넷 텍스트 메일 보안의 de facto 표준으로 널리 사용되고 있는 PGP 는 다른 표준 프로토콜들과는 달리 Phil Zimmerman 개인에 의해 개발된 응용 소프트웨어로서 S/MIME 및 PEM 과 동일한 4 가지 보안서비스를 제공한다 [박현동 등, 1995][Cooper et al., 1995][Garfinkel, 1995][Hughes, 1995][Schneider, 1995][Stallings, 1994] [Stallings, 1995a][Stallings, 1995b][Zimmermann, 1994]. 한편, PGP 에 멀티미디어 MIME 메시지에 대한 보안을 첨가한 PGP/MIME 이 1996 년에 학회에서 새로 발표되었다 [Yamamoto, 1996]. 그러나 PGP 와 PGP/MIME 의 web of trust, 즉 개인의 신뢰(trust)에 근거하여 공개키를 인증 및 교환하는 방식은 소규모 workgroup 에는 적당하지만, 많은 수의 사용자나 대규모 기업환경에서는 적용 및 관리가 어렵다는 확장성 문제를 안고 있다 [RSA, 1996].

2.1.3 PEM 과 MOSS (또는 PEM/MIME)

인터넷 텍스트 메일 보안의 de jure 표준으로서 RFC 1421-1423 으로 발표된 PEM 은 S/MIME 및 PGP 와 동일한 4 가지 보안서비스를 제공한다 [Hughes, 1995][Kent, 1993][Linn, 1993][Linn, Kent, 1989][Schneider, 1995][Stallings, 1995b]. 한편, PEM 에 멀티미디어 MIME 메시지에 대한 보안을 첨가한 MOSS(또는 PEM/MIME)가 1995 년에 RFC 1848 로 발표되었다 [Crocker, 1995]. 그러나 MOSS 는 너무 많은 implementation options 를 포함하고 있어서 서로 다른 소프트웨어 개발자가 상호호환성이 없는 MOSS mailer 를 개발할 소지가 많고 [RSA, 1996], PEM 과의 backward compatibility 가 보장되지 않는 단점이 있다[Yamamoto, 1996]. 또한 PEM 에서 정의된 공개키 인증 계층구조(public-key certification hierarchy)에 대한 infrastructure 는 실질적인 구현이 어렵고 시간이 오래 걸린다는 문제점이 있다.

2.1.4 MHS (X.400) 보안

ITU-T 표준인 MHS 는 기본적으로 UA (User Agent), MS(Message Store) 및 MTA(Message Transfer Agent) 로 구성되며, 여러 MTA 의 집합을 MTS(Message Transfer System)이라 부른다. MHS 는 모두 18 개의 다양한 보안서비스를 제공하며, 18 가지 보안서비스들은 각각의 특성에 따라서 다음과 같이 다섯 개의 그룹으로 나뉘어진다 [강창구, 1996][홍주영 등, 1994][Ford, 1994].

1) 단대단(end-to-end) 서비스

이 그룹의 특징은 하부 MTS 에 영향을 받지 않고 다음과 같은 정보보호 서비스를 발신자와 수

신자(end-to-end)에게 제공한다.

- 단대단 데이타 발신처 인증(end-to-end data-origin authentication)
- 데이타 비밀성(data confidentiality)
- 데이타 무결성(data integrity)
- 메시지 순서 무결성(message sequence authentication)
- 배달 증명(proof of delivery)

2) 메시지 경로(message path) 서비스

이 그룹의 특징은 MHS 를 구성하는 구성요소(functional component, 즉 US, MS, MTA) 들을 경유하는 메시지 경로상에서의 다음과 같은 보안 서비스를 제공한다.

- 개체 인증(entity authentication)
- 메시지 보안 레이블링(message security labeling)
- 보안 영역(security context)

3) MTS 확인(MTS corroborative) 서비스

이 그룹의 특징은 메시지 발신자와 MTS 사이에서 필요한 다음 4 가지의 메시지에 대한 인증을 제공한다.

- MTS 와 발신처 사이의 데이타 발신처 인증 (MTS-to-origin data-origin authentication)
- Probe 발신처 인증 (probe-origin authentication)
- Report 발신처 인증 (report-origin authentication)
- 제출 증명 (proof of submission)

4) 부인봉쇄 (non-repudiation) 서비스

부인봉쇄는 다음과 같은 서비스를 제공한다.

- 발신처 부인봉쇄 (non-repudiation of origin)
- 배달 부인봉쇄(non-repudiation of delivery)
- 제출 부인봉쇄(non-repudiation of submission)

5) 보안관리(security management) 서비스

MHS 프로토콜은 다음과 같은 보안관리 서비스들을 제공한다.

- 신원증명 변경(change credentials)
- 등록(register)
- MS 등록(MS-register)

2.1.5 MSP

미국 NSA 표준인 MSP 는 PGP 나 PEM 과 동일한 4 가지 보안서비스, 즉 데이타 비밀성, 데이타 발신처 인증, 데이타 무결성 및 발신처 부인봉쇄를 제공하며, 추가로 접근제어와 수신처 부인봉쇄 서비스를 포함하고 있다 [홍주영 등, 1994][MIL-STD, 1993][NIST, 1989].

2.2 EDI 보안

CALS 를 위한 상거래 문서를 교환하기 위한 EDI 표준은 UN/EDIFACT 로 정의되어 있다. 그러나 현재 미국 대부분의 EDI 구현은 ANSI X.12 를 사용하고 있어 CALS 전략에 의한 글로벌 시장의 정보화를 위해서 1998 년까지 UN/EDIFACT 로 전환하려는 업계의 합의가 미국 DISA(Data Interchange Standard Association)를 통하여 이루어 졌

으며, 현재 실행 작업이 진행되고 있다 [김규수, 1996]. 한편, X.400 MHS backbone 을 EDI 에도 이용하기 위하여 정형화된 EDI content type 을 추가하여 MHS 를 확장한 X.435(Pedi 또는 F.435)가 ITU-T 에 의해 1990 년에 발표되었다. 본절에서는 UN/EDIFACT 보안, ANSI X.12 보안 및 Pedi (X.435) 에서 제공하는 보안서비스와 특징들에 대해 살펴보기로 한다.

2.2.1 UN/EDIFACT 보안

UN/EDIFACT 를 위한 보안 표준은 현재 개발중이며, 제공되는 보안서비스는 다음과 같다: 개체 (사용자) 인증, 메시지 발신처 인증, 메시지 비밀성, 메시지 내용 (데이타) 무결성, 메시지 순서 무결성, 발신처 부인봉쇄 및 수신처 부인봉쇄 [이경상, 1995][Crocker et al., 1995].

2.2.2 ANSI X.12 보안

ANSI X.12 는 1995 년에 버젼 4 가 나와 있으며 UN/EDIFACT 표준을 수용하기 위한 버젼 5 가 제안을 준비중에 있다. 미국의 기업들은 1990 년에 공표된 버젼 3 에 따라 구현된 시스템을 사용하는 경우가 많다. ANSI X.12 에서 제공되는 보안서비스는 메시지 발신처 인증, 메시지 비밀성 및 메시지 무결성의 3 가지이다 [이경상, 1995][정동길, 1996][Ford, 1994].

2.2.3 Pedi (X.435) 보안

EDI content type 은 EDI 메시지(EDIM: EDI Message)와 EDI 통지(EDIN: EDI Notification)의 두 가지가 있다. EDI 메시지는 전송 기본 단위인 EDI interchange 를 포함한 후 현재 사용중인 EDI format(예를 들어, EDIFACT, ANSI X.12 또는 UNTDI)으로 encoding 되어 전송된다. EDI 통지는 송신된 EDI 메시지가 수신측 UA 로부터 수신자에게 전달, 비전달 또는 다른 UA 에게로 회송되었음을 알리는 것으로서, EDI 메시지의 수신측 UA 가 발신측 UA(또는 MS)에게 전송한다.

MHS 에서 제공되는 보안서비스를 가지고도 정형화된 EDI 메시지를 보호할 수는 있지만, Pedi 에서는 EDI 를 위해서 추가적으로 필요한 보안서비스를 제공하는데, 이들은 그 특징에 따라 2 개의 그룹으로 나뉘어 진다 [강창구, 1996][이정현 등, 1995][Ford, 1994].

1) 단대단 서비스
   - EDI 통지 증명(proof of EDI notification)
   - EDI 통지 부인봉쇄(non-repudiation of EDI notification)
   - 수신 내용 증명(proof of content received)
   - 수신 내용 부인봉쇄(non-repudiation of content received)
   - 발신 내용 부인봉쇄(non-repudiation of content originated)
2) MTS 와 MS 에 관련된 서비스
   - 검색 증명(proof of retrieval)
   - 검색 부인봉쇄(non-repudiation of retrieval)
   - 전달 증명(proof of transfer)
   - 전달 부인봉쇄(non-repudiation of transfer)

2.3 분산개방형 디렉토리 시스템 보안

디렉토리는 사람, 조직 등과 같은 개체(entity)에 관한 정보와 개체 사이의 인증에 필요한 정보(사용자 이름, 패스워드, 공개키 인증서 등)를 저장하고 사용자에게 이들 정보를 제공해주는 분산개방 시스템이다 [이재광, 이용준, 1994][이창진, 노봉남, 1995][최용락 등, 1995][Ford, 1994]. 즉, 디렉토리가 보안에 관련된 자료들의 저장 및 분배 메카니즘으로 사용될 수 있는데, 예를 들어 e-mail 과 EDI 관련 정보를 저장하여 메시지에 서명을 하고, 인증서비스를 제공하는데 이용될 수 있다. 그러나, e-mail 과 EDI 등의 응용분야에서 제공되는 자체 보안서비스들이 디렉토리 표준 및 서비스들과 일치하도록 디렉토리 시스템이 구축되어야 한다.

OSI 의 디렉토리 표준인 X.500 은 디렉토리가 가지고 있는 정보의 형태를 기술하고 있으며, 어떻게 이 정보들을 디렉토리로부터 얻을 수 있는가도 포함하고 있다. 또한 이러한 정보들이 어떻게 만들어지고 저장되는가에 대해서도 언급하고 있다.

X.500 디렉토리의 보안을 위해서 X.509 표준이 제정되었는데, X.509 는 다음과 같이 개체 인증(및 공개키 관리 시스템)과 접근제어의 두가지 보안서비스를 정의하고 있다 [CCITT, 1993].

X.509 는 개체 인증을 위하여 단순 인증(simple authentication)과 강한 인증(strong authentication)의 두가지 방법을 정의하고 있는데, 단순 인증은 사용자 이름과 패스워드를 사용하며, 강한 인증은 공개키 암호화 기법을 사용한 공개키 인증서(public-key certificate)를 개체의 신원확인서로 사용한다. 이때, 디렉토리 자체는 공개키의 생성이나 인증에 대한 책임이 없으며, 단지 사용자에게 공개키 인증서를 획득할 수 있는 저장소를 제공한다.

한편, 디렉토리 사용자들은 접근제어 정책에 따라 그 들에게 부여된 접근권한에 의해서 디렉토리 정보 베이스(Directory Information Base: DIB)에 저장된 정보들에 접근할 수 있다. 디렉토리 정보 베이스(DIB)는 디렉토리 정보 트리(Directory Information Tree: DIT) 구조로 구성되며, 디렉토리 정보에 대한 불법적인 탐색, 시험, 수정등의 조작을 방지하기 위해 제어할 정보대상은 디렉토리의 사용자 정보, DIT 구조와 관련된 디렉토리 정보, 그리고 접근 제어 정보(Access Control Information: ACI)를 포함하고 있는 접근제어 리스트(Access Control List: ACL) 등의 디렉토리 운용 정보로 나눌 수 있다. 여기서 DIT 구조와 관련된 디렉토리 정보는다시 DIT 의 전체, DIT 의 서브트리, DIT 내의 각각의 엔트리(entry), 각 엔트리내의 전체 속성(attribute) 및 일부 선택된 속성의 다섯 가지 범위로 나누어 보호할 수 있다.

3. CALS 구현 2 단계에 필요한 보안기술

CALS 2 단계 구현 목표인 통합 데이타베이

스외에도 다른 모든 분산 응용시스템들에 대한 보안을 제공하는 시스템으로는 MIT 에서 개발된 Kerberos(버전 4 와 5)와 ECMA(European Computer Manufacturer's Association)의 표준으로서, 프랑스의 Bull, 영국의 ICL, 독일의 Siemens 등에 의해 공동 개발된 SESAME 등이 있다. 한편, OSF(Open Systems Foundation)의 DCE(Distributed Computing Environment)는 Kerberos 버전 5 를 사용한다. 본 절에서는 먼저 일반적인 분산개방형 시스템 보안에서 고려되어야할 보안서비스와 특징들에 대해 설명하고, 다음으로 데이타베이스 보안에 대해 살펴본다.

3.1 분산개방형 시스템 보안

분산 시스템에서의 보안서비스도 앞에서 설명한 OSI 의 보안서비스들(개체 인증, 접근제어, 데이타 비밀성, 데이타 무결성 및 부인봉쇄)이 그대로 요구된다. 단지, 여기서는 비연결형(connectionless) 보안서비스를 제외한 연결형(connection-oriented) 보안서비스들이 대상이 된다. 한편, 분산 시스템에서는 사용자가 여러 컴퓨터(서버)들에 분산된 서비스들을 사용할 때 마치 하나의 컴퓨터를 사용하는 것과 똑같은 투명성(transparency)를 제공하여야 한다. 본 절에서는 투명성과 관련하여 개체 인증에서의 단일 로그인(single login 또는 single sign-on)과 접근제어에서의 delegation 에 대해 설명한 후, 데이타 비밀성, 데이타 무결성 및 부인봉쇄에 대해 간단히 살펴본다 [김석우, 1996][Hart, Rosenberg, 1995][Hughes, 1995][Kaijser et al., 1994][Kohl, Neuman, 1993][Lockhart, 1994][Neuman, Ts'o, 1994][Parker, 1991][Stallings, 1995b][White et al., 1996].

1) 개체 인증과 단일 로그인

개체 (사용자) 인증은 시스템에 접근하기 위한 선결조건으로서, 인증을 마친 후에야 사용자에게 부여된 권한에 따라 접근제어가 가능하게 된다. 마찬가지로, 분산 시스템에서의 개체 인증도 사용자(client)가 서로 다른 시스템에 분산된 여러 응용 서비스들(application servers)에 대해 서버의 수만큼 각각 인증절차를 거치지 않고, 인증 서버(authentication server)를 이용한 단 한번의 인증(single login 또는 single sign-on)만으로 필요한 모든 응용 서버에 접근할 수 있도록 하는 것이 중요하다. 인증 메카니즘으로는 암호 알고리즘을 이용한 강한 인증(strong authentication)을 사용하며, 추가로 스마트 카드나 지문등을 이용하기도 한다. 이때 인증 메카니즘으로 대칭키(symmetric key) 또는 비밀키(secret key) 알고리즘을 사용하는 시스템으로는 Kerberos 와 DCE 가 있으며, SESAME 는 대칭키 알고리즘과 X.509 를 확장한 공개키 알고리즘을 선택적으로 사용할 수 있도록 하고 있다.

2) 접근제어

일단 인증된 사용자에 대해서는 각 서버에의 접근권한(authority)이 정의되어 있는 접근제어정보(Access Control Information: ACI 또는 privilege attributes)가 필요하게 된다. 한대의 컴퓨터만을 고

려한 시스템에서는 사용자의 접근제어정보가 컴퓨터의 운영체제에 의해 제공된다. 즉, 사용자가 로그인 하면 인증된 식별자(authenticated identity)에 대한 접근제어정보를 같은 컴퓨터내에서 불러오게 된다. 그러나 단일 로그인을 제공하는 분산 시스템에서는 접근제어정보를 사용자가 접근하고자 하는 서버가 아닌 다른 안전한 컴퓨터(즉 privilege attribute server)에 보관하는 것이 가능하며, 그 곳에서 접근제어정보를 해당 서버로 가져오는 방법에는 push 와 pull 의 두가지가 있다. Push 방법은 사용자측 클라이언트가 안전한 컴퓨터로부터 사용자의 접근제어정보를 가져와서 서버에 제출하는 것이고, pull 방법은 클라이언트는 단지 자신의 인증된 식별자만을 서버에 제출하고 서버가 이 정보를 안전한 컴퓨터에 보내어 사용자의 접근제어정보를 받아오는 것을 말한다.

한편, 사용자가 요구하는 서비스가 하나의 서버가 아닌 여러 대의 서버에 분산되어 있을 때는 사용자에게 부여된 접근권한의 위임(delegation of authority)가 필요하다. 예를 들면, 사용자가 자신이 원하는 서비스가 어느 서버에 있는지 모르는 경우, 사용자는 단지 자신에 가장 가까이에 위치한 서버 A 에 서비스 요구(request)를 하며, 서버 A 가 사용자의 대리인(delegate)으로서 사용자가 원하는 서비스를 제공하는 서버 B 를 찾아 서비스 요구를 보내게 된다. 다시 서버 B 로부터의 응답(response)도 서버 A 를 거쳐서 사용자에게 전달된다.

3) 데이타 비밀성, 무결성 및 부인봉쇄

사용자가 인증절차중 인증서버와 주고받는 인증정보 및 인증 서버로부터 확인받은 인증정보를 응용 서버들에게 안전한 방법으로, 일반적으로 안전하지 못한 통신망을 통해서, 전달할 수 있어야 한다. 또한 인증정보뿐만 아니라 암호화 키의 분배, 사용자와 서버간의 안전한 통신, 즉 요구(request) 및 응답(response)을 위해서는 정보의 비밀성, 무결성, 그리고 부인봉쇄 서비스가 요구된다. 이를 위하여 CALS 구현 1 단계 시스템들에서 사용되는 비밀성, 무결성 및 부인봉쇄 메카니즘들이 사용될 수 있다.

3.2 데이타베이스 보안

데이타베이스 정보를 보호하기 위해서는 데이타 비밀성, 데이타 무결성 및 가용성(availability) 서비스가 고려되고 있다. 데이타 비밀성을 제공하기 위한 보안 메카니즘으로는 사용자 인증과 접근권한 부여(authorization)를 포함한 접근제어 메카니즘을 이용하는데, 대표적인 접근제어 메카니즘으로는 임의적 접근제어(Discretionary Access Control: DAC), 강제적 접근제어(Mandatory Access Control), 그리고 역할기반 접근제어(Role-based Access Conrol: RAC) 등이 있다 [김영균 등, 1994][최운식, 신동익, 1995][Castano et al., 1995]. 데이타 무결성은 데이타의 일관성(consistency)을 유지하기 위한 것으로서, 특히 데이타의 불법적인 생성, 변경 및 파괴를 방지하기 위함이다. 이를 위하여 부분적으로 백업(backup)과 복구(recovery)가 이용되면서, 동시에 부

분적으로 특정한(ad hoc) 보안모델들이 이용되기도 한다. 가용성은 인증된 사용자들이 권한이 부여된 객체에의 정당한 접근이 거부되는 것(denial of service)을 방지하기 위한 것으로서, 감사(audit) 메카니즘을 통하여 사용자의 활동 행적에 대한 감사 추적을 통해 가능토록 할 수 있다. 또한, 감사는 사후적인 분석에 의한 보안사고의 예방뿐만 아니라, 경우에 따라서는 실시간으로 작동하여 침입탐지(intrusion detection)를 하는데도 사용된다. 본 절에서는 가장 많이 연구되고, 주로 사용되는 접근제어에 대해 간단히 살펴보기로 한다.

임의적 접근제어(DAC)는 각각의 사용자(또는 주체: subject)나 사용자가 속해있는 그룹들에 대해 데이타베이스의 객체(object)에 접근할 수 있는 권한을 부여(authorization)하고 이를 접근 행렬(access matrix)을 사용하여 정의한다. 이때 사용자 식별자(identity)나 사용자 그룹 식별자에 따라 접근을 제어한다. 또한, 사용자가 데이타베이스 관리자의 승인없이도 자신이 접근권한을 갖고 있는 자원에 대해 다른 사용자가 접근하는 것을 선택적으로 허가할 수 있다.

강제적 접근제어(MAC)는 흔히 다단계 보안(Multi-Level Security: MLS)이란 말과도 의미가 일맥상통하며 객체의 비밀등급(classification 또는 sensitivity)을 여러 단계로 구분하고, 사용자에게 부여된 비밀 취급 인가등급(clearance)에 의해 접근을 제어하는 방법이다. 예를 들어, 사용자는 자신의 인가등급보다 높은 비밀등급을 갖는 객체에 대해서는 읽기는 허용되지만 쓰기는 허용되지 않도록 제어될 수 있다.

역할기반 접근제어(RAC)는 선택적 접근제어의 확장된 기법으로서, 객체에 대한 접근권한을 사용자의 역할이나 지위에 따라 부여하는 점이 각 사용자의 식별자에 대해 부여하는 선택적 접근제어와 다르다. 또한, 사용자들은 자신의 재량으로 다른 사용자에게 접근권한을 부여할 수 없다는 것도 다르다.

세가지 접근제어가 사용되는 경우를 보면, 강제적 접근제어는 주로 비밀등급이 명확히 구분되는 군사 정보에 적용되며, 임의적 접근제어는 행정이나 상업 정보에 적용된다. 역할기반 접근제어는 임의적 접근제어보다도 더 행정이나 상업정보에 적합한 것으로 평가받고 있다. 특히 보안을 유지해야 하는 객체의 수가 많고, 이러한 객체들에 대한 사용자들의 요구사항들이 많이 중복되는 경우에는 역할기반 접근제어가 유리하다. 또한, 강제적 접근제어에서는 모든 객체들을 유사한 비밀등급으로 분류하여 보호하는 반면에 역할기반 접근제어는 현실적인 응용에서 서로 다른 방법들을 통하여 사용자의 접근권한이 다양하게 부여될 수 있다는 장점이 있다.

4. 결론

본 논문에서는 CALS의 1, 2단계 구현에 필요한 응용시스템들에 적용할 수 있는 표준화된 보안기술들을 CALS 구현 단계별, 응용 시스템별,

통신방식별로 분류하였으며, 각각의 CALS 응용 시스템별로 필요한 보안서비스와 보안메카니즘에 대해서 살펴보았다. 특히, 메시지중심의 1 단계 구현 목표와 분산, 공유된 데이타 처리의 2 단계 목표의 구현은 실질적인 초고속 정보통신 환경을 구축하게 될 것이며, 다양한 응용 프로그램 및 정보통신 기반에서 필요로 하는 보안기술들을 요구하게 될 것이다. CALS/EC 의 산업정보화 및 전자상거래는 초고속 정보 서비스를 가능케 하는 기반구축으로 역할하게 되며, 이 기반구축은 본 논문에서 살펴본 멀티미디어 e-mail, EDI, 디렉토리 및 분산 데이타베이스 등의 통합을 전제로 구성된다. 정보화 사회의 역기능 대책으로 발전되어온 보안기술 역시 CALS 의 단계별 구현에 따라 기존의 e-mail, EDI 등 각 요소별 보안기술이 통합되어야 할 것이다. Kerberos, DCE, SESAME 등의 분산개방형 환경에서의 보안구조는 요소별 보안기술의 통합과 표준화를 겨냥한 하나의 해결책으로서 제시되었지만, CALS 의 1 단계 구현에서부터 출발한 모든 요소별 보안기술을 한번에 수용하기는 아직 구체화되지 못하고 있다. 본 논문은 가장 최근에 연구 개발중인 SESAME 를 실제 CALS/EC 시스템에 접목시키기 위한 설계 작업의 일환으로 제반 보안기술을 분석, 정합한 작업의 일부로서, 메시지 시스템과 분산개방형 시스템의 보안구조의 구현이 CALS 의 1, 2 단계 구현단계에 사상(mapping)됨을 보이고 있다. 결국, 정보화 역기능 방지를 위한 보안기술이 미래의 산업정보화 및 전자상거래에 필요하다면, CALS/EC 의 구현은 보안기술의 단계별 구현을 포함하여야 하며, 본 논문에서 제시한 보안기술 및 우리 실정에 맞는 보안 프로토콜 및 보안 시스템 표준의 개발이 CALS 의 응용 시스템 개발과 함께 단계별로 추진되어야 할 것이다.

참고문헌

[강창구, 1996] 강창구, EDI 정보보호 서비스 분석, 제 2 차 안전한 EDI 관련기술 심포지움, 한국전자통신연구소 주관, 한국통신 주최, pp. 3-17, 1996.

[김규수, 1996] 김규수, CALS 표준체제와 구현방법론, 월간 컴퓨터, pp. 145-149, 1996.

[김석우, 1996] 김석우, 분산망 정보보호 시스템 기술 및 응용, 제 2 회 한국 전산망 보안기술 워크숍(NETSEC-KR'96), 통신정보보호학회, pp. 327-337, 1996.

[김영균 등, 1994] 김영균, 서재현, 노봉남, 객체지향 데이타베이스 보안, 통신정보보호학회지, 제 4 권 제 4 호, pp. 71-87, 1994.

[김청환, 김성회, 1995] 김철환, 김성회, CALS 구현사례 현황 조사 연구, 한국정보통신진흥협회, 1995.

[박현동 등, 1995] 박현동, 류재철, 임채호, 변옥환, 전자우편 보안 -PGP-, 통신정보보호학회지, 제 5 권 제 4 호, pp. 58-90, 1995.

[신동익, 1995] 신동익, CALS 와 표준화, 정보과학회지, 제 13 권 제 11 호, pp. 17-25, 1995.

[신장균 등, 1995] 신장균, 나민영, 이승희, CALS 구현을 위한 정보기술, 정보과학회지, 제 13 권 제 11 호, pp. 5-16, 1995.

[이경상, 1995] 이경상, CALS 표준에 따른 EDI 보안, 정보과학회지, 제 13 권 제 11 호, pp. 68-76, 1995.

[이재광, 이용준 1994] 이재광, 이용준, X.500 디렉토리 정보보호, 통신정보보호학회지, 제 4 권 제 3 호, pp. 22-33, 1994.

[이정현 등, 1995] 이정현, 윤이중, 김대호, 이대기, X.435 EDI 정보보호 서비스 데이타 구조 분석, 통신정보보호학회지, 제 5 권 제 3 호, pp. 69-85, 1995.

[이창진, 노봉남 1995] 이창진, 노봉남, OSI 통신망에서의 응용 계층 보안, 통신정보보호학회지, 제 5 권 제 3 호, pp. 87-95, 1995.

[정동길, 1996] 정동길, EDI 표준화 추진체계에 대하여, 월간 정보화사회, pp. 12-21, 1996.

[최용락 등, 1995] 최용락, 강창구, 김대호, X.500 디렉토리 모델과 정보보호 서비스, 통신정보보

호학회지, 제 5 권 제 3 호, pp. 49-68, 1995.

[최운식, 신동익, 1995] 최운식, 신동익, 논리적 보안 통제, 통신정보보호학회지, 제 5 권 제 4 호, pp. 102-111, 1995.

[홍주영 등, 1994] 홍주영, 윤이중, 김대호, 전자우편 시스템의 보호 방식 분석, 통신정보보호학회지, 제 4 권 제 2 호, pp. 7-17, 1994.

[Castano et al., 1995] Castano, S., Fugini, M.G., Martella, G., and Samarati, P., Database Security, ACM Press, Addison-Wesley Publishing Company, 1995.

[CCITT, 1993] CCITT Recommendation X.509, Information Technology-Open Systems Interconnections-The Directory: Authentication Framework, 1993.

[Cooper et al., 1995] Cooper, F.J., Chris, G., Halvey, J.K., Hughes, L., Morgan, L., Siyan, K., Stallings, W., and Stephenson, P., Implementing Internet Security, New Riders Publishing, Indianapolis, Indiana, 1995.

[Crocker et al., 1995] Crocker, S., Freed, N., Galvin, J., and Murphy, S., MIME Object Security Service, RFC 1848, 1995.

[Dosdale, 1994] Dosdale, T., Security in EDIFACT Systems, Computer Communications, Vol. 17, No. 7, pp. 532-537, 1994.

[Ford, 1994] Ford, W., Computer Communications Security, Prentice Hall PTR, Englewood Cliffs, New Jersey, 1994.

[Garfinkel, 1995] Garfinkel, S., PGP: Pretty Good Privacy, O'Reilly & Associates, Inc., Sebastopol, California, 1995.

[Hale, Mannarino, 1996] Hale, M. and Mannarino, T., MISSI Compliance for Commercial-Off-The-Shelf Firewalls, Proceedings of the 1996 Canadian Computer Security Symposium, pp. 17-27, 1996.

[Hart, Rosenberg, 1995] Hart, J.M. and Rosenberg, B., Client/Server Computing for Technical Professionals, Addison Wesley Publishing Co., 1995.

[Hughes, 1995] Hughes, L.J., Actually Useful Internet Security Techniques, New Riders Publishing, Indianapolis, Indiana, 1995.

[Kaijser et al., 1994] Kaijser, P., Parker, T., and Pinkas, D., SESAME: The Solution to Security for Open Distributed Systems, Computer Communications, Vol. 17, No. 7, pp. 501-518, 1994.

[Kaufman et al., 1995] Kaufman, C.K., Perlman R., and Speciner, M., Network Security: Private Communication in a Public World, Prentice Hall PTR, Englewood Cliffs, New Jersey, 1995.

[Kent, 1993] Kent, S.T., Internet Privacy Enhanced Mail, Communications of the ACM, Vol. 36, No. 8, pp.

48-60, 1993.

[Kohl, Neuman, 1993] Kohl, J. and Neuman, B., The Kerberos Network Authentication Service (V5), RFC 1510, 1993.

[Linn, 1993] Linn, J., Privacy Enhancement for Internet Electronic Mail: Part I, Part II, Part III, Part IV, RFC 1421-1423, 1993.

[Linn, Kent, 1989] Linn, J. and Kent, S.T., Privacy for DARPA-Internet Mail, Proceedings of the 12th National Computer Security Conference, Baltimore, MD, October 10-13, pp. 215-229, 1989.

[Lockhart, 1994] Lockhart, H.W., OSF DCE: Guide to Developing Distributed Applications, McGraw-Hill, Inc., 1994.

[MIL-STD, 1993] MIL-STD-2045-18500-1, Information Technology DoD Standardized Profiles AMHXn(D) Message Handling Systems Message Security Protocol (MSP), 1993.

[Neuman, Ts'o, 1994] Neuman, B.C. and Ts'o, T., Kerberos: An Authentication Service for Computer Networks, IEEE Communications, Vol. 32, No. 9, pp. 33-38, 1994.

[NIST, 1989] NIST, SDNS Message Security Protocol, SDN.701, Rev. 1.5, 1989.

[Parker, 1991] Parker, T.A., A Secure European System for Applications in a Multivendor Environment (The SESAME Project), Proceedings of the 14th National Computer Security Conference, Baltimore, MD, 1991.

[RSA, 1996] RSA Data Security Inc., S/MIME Frequently Asked Questions, http://www.rsa.com/rsa/S-MIME/smimeqa.htm, 1996.

[Schneider, 1995] Schneider, B., E-Mail Security, John Wiley & Sons, Inc., New York, New York, 1995.

[Stallings, 1994] Stallings, W., Pretty Good Privacy, BYTE, pp. 193-196, July 1994.

[Stallings, 1995a] Stallings, W., Protect Your Privacy: The PGP User's Guide, Prentice Hall PTR, Englewood Cliffs, New Jersey, 1995.

[Stallings, 1995b] Stallings, W., Network and Internetwork Security Principles and Practice, Prentice Hall PTR, Englewood Cliffs, New Jersey, 1995.

[Stallings, 1996] Stallings, W., Internet Security Handbook, IDG Books, Foster City, California, 1996.

[van Herwijnen, 1994] van Herwijnen, E., Practical SGML, Kluwer Academic Publishers, Norwell, Massachusetts, 1994

[White et al., 1996] White, G.B., Fisch, E.A., and Pooch, U.W., Computer System and Network Security, CRC Presss, Inc., 1996.

[Yamamoto, 1996] Yamamoto, K., An Integration of PGP and MIME, IEEE Proceedings of the Simposium on Network and Distributed Systems Security (SNDSS)'96, pp. 17-24, 1996.

[Zimmermann, 1994] Zimmermann, P.R., PGP™ User's Guide: Vol. I, Vol. II, Phil's Pretty Good Software, 1994.

저자 소개

김 중 인

1987 한양대 산업공학과 (학사)

1989 한양대 산업공학과 (석사)

1995 Arizona State University 산업공학과 (박사)

1996 ~ 현재 홍익대학교 경영정보학과 전임강사

관심분야: CALS/EC, Information Systems Analysis & Design, Network Security, Object-Orientation

김 석 우

1979 항공대 통신정보공학과 (학사)

1989 New Jersey Institute of Technology 전산학과 (석사)

1995 아주대학교 컴퓨터공학과 (박사)

1986 - 1988 AT&T BELL Lab. 방문연구원

1980 ~ 현재 한국전자통신연구소 책임연구원

관심분야: Computer Security, Network Security, MHS Security