通信情報保護學會誌
第1卷, 第2號, 1991. 8

IEEE 컴퓨터 보안기술 연구동향

박 태 규*

1. 서 론

컴퓨터와 통신보안 연구는 1949년 이전부터 계속되어 오고 있다. 특히, "IEEE Technical Committee on Security and Privacy"는 컴퓨터 보안 분야에 있어서 가장 권위를 자랑하며 가장 전문화되어 있는 단체이다. 이 위원회는 1980년 4월부터 "Symposium on Security and Privacy"를 매년 미국 캘리포니아주의 오클랜드(Claremont 호텔)에서 개최해 오고 있으며, 1984년부터는 국제 암호연구학회(IACR : International Association for Cryptologic Research, 1983년 창립)와 공동으로 년 1회씩 같은 장소에서 같은 시기에 개최해 오고 있다. 이 심포지움은 주로 학계, 산업계, 정부 연구소 등의 연구결과들이 매년 20~30편 내외의 수준높은 논문들이 발표된다는 점에서 전세계 관련 학자들의 관심대상이 되고 있다. 또한 개최 당시의 관심사에 관한 토론을 위하여 1~2개의 주제를 선정하여 패널 토의를 하기도 한다.

본고에서는 1980년부터 1991년까지 12년동안 이 심포지움에서 발표되었던 논문을 중심으로 발표된 논문수, 논문 주제별 현황 및 특이점 등을 알아보기로 한다. 그리고 IEEE는 컴퓨터와 네트워크 보안기술 분야에서 표준화에 기여하기 위하여 각종 Project 및 Working Group을 결성하여 활동중인데 그중 LAN(Local Area Netwrok)을 보호하기 위하여 IEEE 802.10에서 수행중인 SILS(Standard for Interoperable LAN Security) Project 내용에 관해 알아보고, UNIX 운영체제의 표준화와 더불어 Security 기능을 확장하기 위한 IEEE 1003.6 Working Group의 POSIX(Portable Operating System Interface for Computer Environments) 활동내용을 알아본다.

* 정회원, 한국전자통신연구소 선임연구원

2. IEEE 심포지움 논문 동향 분석

2.1. 개 요

1980년 4월부터 시작된 "IEEE Symposium on Security and Privacy"에서 1991년 5월까지 총 12회에 걸쳐 발표된 총 논문수는 299편이며 연도별 발표 논문수는 표 1과 같다.

12년 동안 매년 큰 변화없이 거의 일정한 편수의 논문을 발표하고 있는 것이 특징이며, 처음부터 현재까지 해마다 3일 기간동안 1개의 Stream으로만 발표가 이루어지고 있는 것이 특징이라 하겠다. 그 이유는 수준높은 논문을 모든 참여자들에게 관심을 유발시킬 수 있는 것들로 선정하여 다각적 관점에

표 1. IEEE 심포지움 논문발표 현황

연도	발표논문수	패널토의 주제	개최일
'80	19	1. Verification of Secure S/W Systems.	4.14~16
'81	18	1. Cryptography, 2. Kernel Performance issue	4.27~29
'82	20	—	4.26~28
'83	21	1. Multilevel Data Management Security 2. Commercial View of Data Security 3. Bell/Lapadula + Alternative Models	4.25~27
'84	26	1. Security + Verification with Ada	4.29~5.2
'85	25	—	—
'86	23	1. Role of Encryption in LAN	4.7~9
'87	26	—	4.27~29
'88	26	—	4.18~21
'89	33	1. Computer Virus	5.1~3
'90	34	—	5.7~9
'91	28	1. Information Theory in Computer Security	5.20~11
합계	299	10	각 3일간

표 2. 주제별 논문현황

연도 / 주제	'80	'81	'82	'83	'84	'85	'86	'87	'88	'89	'90	'91	합계
운영체제 보안		6		2	3	4	5	7	8	7	9	6	57
보안모델	3	3	4	1	2	4	3	7	6	10	1	4	48
데이타베이스 보안	5	1		3	3	3	2	5	6	4	9	3	44
시스템 검증	1	3			2	5	5	4	3	1	7	6	37
네트워크 보안	1		3	6	4	3	2	2		4	4	1	30
암 호	6	1	5	6	3	5	3						29
보안요구조건	1	4		3	2		3	1	1	1		2	18
기 타	2		8		7	1			2	6	4	6	36
합 계	19	18	20	21	26	25	23	26	26	33	34	28	299

서의 비판에 도전해 보자는 의도에서라 한다.

초기에는 이 심포지움의 영역을 넓히기 위한 노력이 계속되어 그 분야가 Crypto, Computer Security, Database, Systems, Network 분야로 영역이 확장되었다. 그러나 1981년에 CRYPTO Conference가 처음으로 탄생하면서 암호학 분야의 논문들이 CRYPTO Conference쪽으로 유도되고 있다. 12년동안 발표된 논문들을 주제별로 분류한 현황은

표 2에서 보는 바와 같으며, 80년대 초기부터 중반('86년)까지는 암호에 관한 논문도 운영체제 보안이나 보안시스템에 대한 검증, 네트워크 보안분야 등과 거의 같은 수준으로 발표되다가 그 이후에는 CRYPTO Conference 등으로 유도되어 거의 없는 상태이다.

2.2. 암호 및 네트워크 분야

암호분야의 논문들은 주로 메세지 인증, Database 암호화, 암호시스템 설계 및 강도평가, Match Making, Key 관리, Password 생성기 등이며, 이론적인 것들이 대부분이다. 미국의 Security 기술의 최상의 목표는 National Security 확보로 상업용보다 강도나 정책에 있어 우선한다. '83년의 "Verfication of Treaty Compilance Revised"(G.J. Simmons)에서는 미·소간의 핵 실험조약을 지킬 것을 확인하는데 메세지 인증 기술을 사용한 예를 소개하고 있다. 데이타 베이스 암호화에 관한 것은 관계형 데이타 베이스의 효율성과 보안성의 양측면을 주로 다루고 있다.

네트워크 보안분야에서는 호스트와 호스트, 호스트와 터미날 사이의 통신에 있어서 사용자, 터미날, 호스트, 프로세스 등과 같은 통신주체와 통신객체(매체)상의 안전성 확보를 위한 것들이 주류를 이루고 있으며, 기밀등급(Top Secret, Secret, Confidential, Sensitive, Unclassified)별 처리에 따른 통신시의 처리방법에 관한 것들과 SDNS(Secure Data Network System)에서 갖는 Security Protocol에 관한 것들이 주로 발표되고 있다. 이러한 네트워크 보안의 실현 및 구현은 UNIX 네트워크 환경하에서 이루어지고 있는 논문들이 많다.

2.3. 보안모델·운영체제 보안 및 시스템 검증분야

이 분야는 논문이 가장 많이 발표되는 분야로 주로 보안모델에 대한 고찰 및 형식화, 군용·상업용 컴퓨터 보안기준에 따른 운영체제의 엑세스 제어, 사용자의 식별, 인증, 감사기법 등에 대해 요구조건을 분석·정의하고 그 실현방법에 역점을 두고 있다. 엑세스 제어는 군용에 있어서는 정보의 누설을 방지하기 위한 READ 엑세스 제어를 중요시 하는 반면, 상업용에서는 Data의 변경, 무결성(Integrity)을 위한 WRITE 제어를 중요시 하고 있다는 점이 특징이라 하겠다.

다중 사용자 환경에서 자원을 공유함으로써 발생되는 엑세스 제어 문제를 해결하기 위하여 운용체제에 Kernel Base로 보안기능을 넣은 Security Kernel 개념을 심은 시스템으로는 IBM KVM/370. Honeywell의 SCOMP, IBM의 Secure XENIX, AT & T의 UNIX System V/MLS, DEC의 VMM(Virtual Machine Monitor) 등에 관한 논문들이 많이 발표되고 있다. 현재 운영체제의 보안연구는 DoD가 1985년에 발표한 신뢰성 컴퓨터 시스템 평가기준인 TCSEC(Trusted Computer System Evaluation Criteria)에 따르기 위한 모델, 설계, 구현방법 등이 대부분을 이루고 있다. 이러한 시스템의 환경은 UNIX 계열이 주류를 이루고 있으며, 이런 환경하에서 연구·개발된 시스템들에 대한 평가 및 검증은 TCSEC의 등급 기준 요소에 부합하는가 하는 평가와 Kernel S/W, Data Flow, Covert Channel 등의 검증, 분석 등을 Euclid, INA, JO, GYPSY와 같은 검증 시스템 개발 언어를 이용하여 수행하는 내용의 논문들이 많다. 또한 보안모델중 기밀의 다중 등급을 처리할 수 있는 BLP(Bell/Lapadula) 모델의 장단점 분석, 적용에 대한 것들도 많이 발표되고 있다.

2.4. 데이타 베이스 보안 및 보안 요구조건

컴퓨터의 이용방법이 데이타 베이스를 구성하여 여러 사용자가 사용하게 됨으로써 자원의 공유성과 보안성을 절충하게 되는데, 데이타 베이스 관리 시스템에서도 운영체제의 보안과 비슷하게 기밀등급에 따른 Multilevel DataBase Access Control, Integrity Control, Statistical DataBase에서의 Inference Control 등이 많이 이루어지고 있다. 또한 보안요구조건으로는 안전한 컴퓨터 시스템 개발을 위한 요구조건(TCSEC 등) 등이 미국방성이 중심이 되어

연구되고, 발표되고 있다. 이는 군용, 상업용 기준을 별도로 설정하지 않고 TCSEC의 7개 등급(A1, B3, B2, B1, C2, C1, D)을 두어 주로 군용은 B급 이상, 상업용은 C급 이상 등으로 등급을 따르도록 하고 있는 상황이다. 이 분야의 발표논문들은 보안성에 관한 신뢰성 평가방법을 적용하여 논하는 것들이 대부분이다.

2.5. 기타 분야

Fault-tolerance, Computer 바이러스 감지, 퇴치 방법, 침입감지 시스템, S/W Engineering 기법을 이용한 Secure 시스템 설계, Information Flow, Information Privacy Issue 등에 대한 논문 등이 발표되고 있다.

3. IEEE UNIX 보안 표준화 활동

UNIX 운영체제의 기본 Interface 표준화를 위하여 IEEE POSIX.1 Working Group(P1003.1)이 구성되었으며 '88년에 IEEE Std.1003.1-1988(또는 POSIX.1)을 발간하였다. 이 표준은 보안에 관한 필요성을 느껴 1988년에 보안기능을 확장하기 위하여 P1003.1 Working Group에서 또다른 Working Group인 P1003.6(Security Extensions to POSIX)을 만들었다. 이 그룹은 '88년 3월 미국 워싱턴에서 처음으로 회동을 갖고 현재까지 약 2~3개월에 한 번씩 모여 보안에 관한 작업을 해오고 있기 때문에 비교적 많은 진전을 이루고 있다. 현재('91.6.)까지 발간된 Draft인 P1003.6 Draft 11을 중심으로 내용을 살펴보면 다음과 같다.

P1003.6의 관점은 기본 POSIX 인터페이스 규격(IEEE POSIX P1003.1, ISO/IEC IS 9945-1)에 확장된 보안기능을 위해 인터페이스를 정의하고 있고, 그 범위는 부가적 보안 매카니즘에 대한 새로운 시스템 기능(System Function)과 명령어들의 정의를 포함하고 있다. 그리고 보안 주체와 객체간의 구분 및 보안정책은 명확하게 정의하고 있으나 뚜렷한 보안 모델은 정의하지 않고 있다. 또한 신뢰성 있는 시스템에 대한 요구사항은 DoD의 TCSEC으로부터 도입하고 있으며, 타당성이 있는 새로운 요구사항도 또한 포함을 시키고 있다.

이 그룹은 다음의 4개의 서브그룹으로 구성해 작업을 진행하고 있다.

- DAC 서브 그룹 : DAC(Discretionary Access Control) 기법 관련작업
- MAC 서브 그룹 : MAC(Mandatory Access Control) 기법, Information Labeling(IL) 관련작업
- Privileges 서브 그룹 : 운영체제의 Privilege 통제 관련작업
- Audit Trails 서브 그룹 : 감사, 추적기법 관련 작업

이중 MAC 서브 그룹에서는 MAC와 IL의 인터페이스는 기밀 등급별 처리를 하지 않는 시스템과의 호환성을 위해 Option으로 정하고 있다. 이 P1003.6 그룹의 핵심기고자는 미국의 AT&T이며, UNIX 사용자 그룹인 /user/ group도 활발히 POSIX 표준화에 기여하고 있다.

4. IEEE LAN 보안 표준화 활동

LAN(Local Area Network) 관련 표준화 작업은 아직도 초기 단계라 할수 있다. 미국의 IEEE가 LAN에 대한 표준을 제정함에 선두적인 리더라는 데는 아무 이의가 없다. IEEE 802.10 Working Group은 '88. 7월부터 LAN을 보호하기 위한 표준을 만들기 위해 SILS 프로젝트를 수행하고 있다. 이런 목적에 대한 기반조건으로서 OSI 환경의 Product와의 상호 연동 등을 최대한 보장하며, 암호화에 의해 제공되는 최소 허용 가능한 보안 서비

그림 1. IEEE 802.10 작업분야

작업분야	Layer 구분	진행상태
SDE(Secure Data Exchange)	Layer 2	완 료
Key Management	Layer 7	'89.7 시작
System/Security Management	Lyer 7	〃

그림 2. 보안서비스와 ISO Layer 관계

위협요인	보안 서비스	IS 7498-2	SILS
데이타 변조	Peer Entity Authentication	3,4,7	7(?)
	Data Origin Authentication	3,4,7	2,7
불법자원 이용	Access Control Service	3,4,7	2,7
불법노출	Connection Confidentiality	1,2,3,4,6,7	2
	Connectionless Confidentiality	2,3,4,5,7	2
	Selective Field Confidentiality	6,7	7
	Traffic Flow Confidentiality	1,3,7	NO
위 장	Connection Integrity	3,4,7	NO
	Selective Field Integrity	3,4,7	7
	Connectionless Integrity	3,4,7	2
부 인	Origin Non-Repudiation	7	7(?)
	Delivery Non-Repudiation	7	7(?)

스를 명시하는 것 등이다. 이 Group은 Transparent SDE Sublayer(Data Link Layer의 MAC와 LLC Sublayer 사이에 위치함)를 제안하고 있다. 이 표준의 목적은 LAN의 위장위협과 Captured Packet의 변조를 막기 위한 것이다.

IEEE 802.10에서의 표준화 작업은 그림 1과 같이 3개의 분야로 나누어 작업을 하고 있으며, '89년 7월에 SILS 모델과 Secure Data Exchange Protocol을 제시할 정도로 1년만에 큰 진전을 보이고 있다.

SDE는 현재 Working Draft 형태의 문서가 나와 있으며 키이 관리와 보안관리 분야는 아직 Working Draft가 발표되지 않았다. 그리고 LAN 환경에서의 위협요인과 보안서비스의 관계 및 ISO 7498-2 Network Security 구조에서의 Layer 위치, SILS의 Layer 위치와의 관계는 그림 2와 같다.

참 고 문 헌

1. Proceedings of the 1980－1991. Symposium on Security and Privacy, IEEE Computer Society Press, California, 1980－1991.

2. Standard for Interoperable Local Area Network (LAN) Security(SILS) Part B(Secure Data Exchange), IEEE, 1990. 1.

3. Draft Security Interface for the Portable Operating System Interface for Computer Environments, IEEE, 1991.

□ 筈者紹介

朴 泰 奎(正會員)

1956年 8月 10日生
慶北大學校 電子計算機工學科 學士
忠南大學校 電算統計學科(電算學 專攻) 碩士
韓國國防研究院 研究員 勤務 現在 韓國電子通信研究所 室長