通信情報保護學會誌
第4卷 第2號, 1994. 6

컴퓨터 범죄 방지를 위한 정보통신망의 보호방안에 관한 연구

A Study on Prevention Scheme for Communication Network from Computer Crime

박영호*, 문상재*, 김세헌**, 강신각***, 임주환***

요 약

본 논문에서는 컴퓨터 통신망에 관련된 범죄를 유형별로 구분하고 이에 대한 기술적 방지대책을 구체적으로 제시한다. 본 논문은 컴퓨터 범죄를 경험적 기준에 의하여 구분하며 방지대책과의 관계도 분석한다. 기술적 방지대책으로 전형적인 OSI 참조모델에 기초한 보호모델 구조와 컴퓨터 범죄의 각 유형에 대해서 대처할 수 있는 보호 서비스 및 메카니즘 그리고 적용 가능한 계층을 종합적으로 분석 제시한다. 또한 보호메카니즘을 구현하는데 사용되는 대표적 보호알고리듬의 수행시간에 관해서도 기술한다.

1. 서 론

정보통신기술과 전자기술의 발전으로 우리 사회는 산업사회로부터 급속히 정보화사회로 이행되고 있으며 컴퓨터 통신망을 통한 서비스 이용이 대중화되고 있다. 그러나 컴퓨터 통신망에서 가장 큰 장애요소 중 하나로 컴퓨터 범죄를 들 수 있으며, 이러한 장애요인은 컴퓨터가 통신망을 통하여 연결되어 있는 상황에서는 더욱 심각하다. 따라서 이를 막을 수 있는 대책이 필요하다.

컴퓨터 범죄를 예방하기 위한 방지대책으로는 기술적인 통제방안을 이용하는 기술적 방지대책, 물리적 시스템 환경을 안전하게 보호하기 위한 물리적 방지대책, 컴퓨터 시스템의 관리 및 운영적인 측면에서의 관리적 방지대책, 그리고 국가적 차원에서 지원해야하는 법적/제도적 방지대책 등으로 분류되어진다. 방지대책 가운데서, 본 논문은 컴퓨터 통신망의 보호체계를 통한 기술적 방지대책을 중점적으로 다룬다.

컴퓨터 통신망의 기술적 방안으로 ISO 7498-2[1]에서는 OSI 참조모델의 각 계층에서 제공하는 보호서비스와 보호메카니즘 그리고 이들간의 관계 등을 기술하고 있으나 컴퓨터 통신망에서 발생하는 범죄에 구체적으로 대처할 수 있는 보호서비스와 보호메카니즘에 관해서는 기술하지 않았다. 또한 Sieber[2]및 Parker[3]등은 컴퓨터 범죄의 개념 및 유형에 관하여 발표한 바 있으나 이러한 컴퓨터 범죄 유형을 막을 수 있는 기술적 보호방안을

* 경북대학교 전자공학과
** 한국과학기술원 경영과학과
*** 한국전자통신연구소

구체적으로 제시한 바 없다.

본 논문에서는 컴퓨터 통신망에 관련된 범죄를 유형별로 구분하고 이에 대한 기술적 방지대책을 구체적으로 제시한다. 본 논문은 컴퓨터 범죄를 경험적 기준에 의하여 구분하며 방지대책과의 관계도 분석한다. 기술적 방지대책으로 전형적인 OSI 참조모델에 기초한 보호모델 구조와 컴퓨터 범죄의 각 유형에 대해서 대처할 수 있는 보호 서비스 및 메카니즘 그리고 적용 가능한 계층을 종합적으로 분석 제시한다. 또한 보호메카니즘을 구현하는데 사용되는 대표적 보호알고리듬의 수행시간에 관해서도 기술한다.

2. 컴퓨터 범죄의 개념과 유형

2.1 컴퓨터 범죄의 개념

컴퓨터 범죄(computer crime)의 정의에 대하여는 법률상 명확한 규정이 있는 것이 아니기 때문에, 그 개념정의는 논자에 따라서 매우 다양한다. 우선 컴퓨터 범죄를 별개의 범죄로 파악하지 않는 부정설과 이를 인정하는 긍정설로 나누어진다. 긍정설은 다시 광의로 파악하는 경우와 협의로 파악하는 경우로 견해가 나누어진다.

대부분의 학자들은 광의로 해석하여 "컴퓨터가 행위의 수단 또는 목적인 모든 범죄적 현상"을 컴퓨터 범죄라고 한다[1]. 미국과 일본의 공식적인 견해도 모두 컴퓨터 범죄의 개념을 광의로 해석하고 있다. 미국 정부에서는 "컴퓨터와 관련된 범죄(computer related crime)"라는 용어를 쓰고 이것은 "컴퓨터 프로그램을 조작하는 것과 같은 극히 기술적으로 세련된 범죄는 물론이고, 컴퓨터 시스템에 대한 허위입력과 출력의 오용에서 유래되는 것"이라고 정의를 내리고 있다. 한편 미국의 변호사협회에서는 컴퓨터 범죄를 컴퓨터를 다른 범죄(절도, 사기, 횡령 등)를 용이하게 하는 수단으로서 이용하는 범죄와 컴퓨터를 범죄의 희생물(방해나 파괴의 대상)로 되게 하는 범죄 등의 두 부분으로 나누고 있다. 일본 경시청에서는 컴퓨터 범죄를 "컴퓨터 시스템에 가하여지는 범죄 또는 이것을 악용하는 범죄"라고 매우 포괄적으로 정의하고 있다. 반면 Sieber는 컴퓨터 범죄의 개념을 협의로 해석하여 "컴퓨터가 행위의 수단 또는 목적인 고의의 재산적 침해만을 컴퓨터 범죄"라고 한다[2].

두 견해의 차이는 컴퓨터 범죄의 개념에 재산적 침해와는 별도로 개인의 사생활에 대한 비밀의 침해나 국가적, 정치적 기밀에 대한 침해를 포함시키느냐에 있다고 할 수 있다. 컴퓨터 시스템과 관련하여 발생하는 범죄행위가 재산침해 행위가 중심이 되는 것은 사실이나 개인의 비밀이나 국가의 기밀을 침해하는 행위도 무시할 수 없다. 행정전산망 등 기간전산망의 확충으로 개인의 각종 데이타가 컴퓨터에 수록되어 이용되고 있고 국가의 기밀도 컴퓨터에 저장되어 활용되고 있는 현실을 고려할 때, 이들 비밀을 침해하는 행위는 개인 사생활의 평온과 국가의 안전에 크나큰 위험이 아닐 수 없다. 따라서 컴퓨터 시스템과 관련하여 발생되는 처벌가능하고 또한 처벌할 가치가 있는 모든 행위를 컴퓨터 범죄로 파악하는 것이 바람직하다.

2.2 컴퓨터 범죄의 유형

컴퓨터 범죄를 좀 더 정확하게 파악하기 위해서는 구체적으로 그 형태가 어떻게 나타나는지를 알아보는 것이 필요하다. 그런데 컴퓨터 산업의 발달과 과학기술의 향상으로 새로운 범죄수단이 계속해서 등장하기 때문에 그 유형을 일정한 기준에 의하여 분류하는 방법이 아직 확립되어 있지 않고 학자에 따라서 각각 그 유형을 다르게 분류하고 있다.

Parker[3]는 손해의 유형에 따라서 ① 파괴에 의한 손해(loss from vandalism) ② 정보나 재산의 사기 혹은 절도에 의한 손해(loss from information or property fraud and theft) ③ 재정적 사기 혹은 절도에 의한 손해(loss from

financial fraud or theft) ④ 권한없는 사용이나 서비스의 판매에 의한 손해(loss from unauthorized use or sale of service)로, Rohner[4]는 ① 조작(manipulation) ② 파괴(sabotage) ③ 스파이 ④ 서비스 시간의 부정사용으로, Tiedemann[5]은 손해의 범위와 행위방법을 기준으로 하여 ① 조작 ② 전자자료처리 영역에서의 경제스파이 ③ 전자자료처리 영역에서의 파괴 ④ 서비스시간의 부정사용으로, Sieber[6]는 ① 자료변경 ② 자료의 무효화 ③ 불법적인 자료획득과 자료이동 ④ 컴퓨터 하드웨어에 대한 공격으로, Schweitzer[7]는 ① 사기 및 횡령(fraud and embezzlement) ② 컴퓨터 서비스의 절취(theft of computing services) ③ 해커(hackers) ④ 정보의 절취(theft of information) ⑤ 컴퓨터 자원에 대한 공격(attacks on computers resources)으로, 門田 涉[8]은 ① CD(cash dispenser) 범죄 ② 부정데이타 입력 ③ 데이타, 프로그램 등의 부정입수 ④ 컴퓨터 파괴 ⑤ 컴퓨터의 부정사용 ⑥ 프로그램의 변경 또는 소거 ⑦ 자기 데이타 등 전자기록물의 훼손으로 나누고 있다. 이와 같이 컴퓨터 범죄의 유형에 대해서는 보는 관점과 기준에 따라서 다소의 차이가 있는데 이것은 분류방법이 법학적 기준이 아닌 경험적 기준에 의거하고 있기 때문이다.

본 논문에서는 경험적인 기준에 의하여 행위자의 컴퓨터에 대한 범죄행위방법에 따라서 다음의 여섯 가지로 분류한다.

1. 컴퓨터 횡령

컴퓨터 횡령은 일반적으로 컴퓨터의 권한없는 부정조작으로 발생한다. 컴퓨터 부정조작에 대해서는 학자에 따라서 서로 다르게 정의하고 있다. Rohner[4]는 불법적인 목적을 추구하는, 컴퓨터에 있어서의 인력매체 내용의 변경, 프로그램의 변경 혹은 자료처리과정에 대한 간섭을 컴퓨터 부정조작이라고 정의하고 있으며, Sieber[6]는 컴퓨터 부정조작을 행위자가 컴퓨터의 처리결과(output) 혹은 인쇄출력(print-out)을 변경시켜 이로 인하여 자신의 재산적 이익을 얻기 위한 의도를 가지고 전자자료처리의 영역에 있어서 부분적인 자료변경을 시도하는 것으로 정의하고 있다. 따라서 컴퓨터 횡령이란 컴퓨터 정보의 입력, 처리, 출력 과정에서 컴퓨터를 불법적으로 조작하여 금품을 횡령하는 것이라고 할 수 있다. 컴퓨터 횡령은 데이타의 입력과정에서 발생하는 입력 트랜잭션 조작, 컴퓨터에 의한 처리과정에서 발생하는 프로그램 변조, 출력조작, 그리고 콘솔조작 등으로 나누어진다.

2. 컴퓨터 자원의 절취

컴퓨터 자원이란 컴퓨터 하드웨어, 소프트웨어, 데이타뿐만 아니라 컴퓨터가 제공하는 서비스 등 컴퓨터와 관련된 모든 자원을 말한다. 여기서 중요시되는 것은 컴퓨터 프로그램이나 데이타를 절취하는 컴퓨터 스파이 행위와 타인의 컴퓨터를 권한없이 사용하는 서비스의 부정사용이다. 컴퓨터 하드웨어를 절취하는 행위는 일반적인 절취행위와 유사하게 다루어질 수 있을 것이다. 컴퓨터 자원의 절취는 프로그램 및 데이타의 절취, 종사직원의 이직에 따른 유출, 그리고 서비스의 부정사용 등으로 나누어진다.

3. 해커

컴퓨터 시스템의 가장 큰 위협중의 하나로 대두되고 있는 문제가 시스템에 불법적으로 접근하는 행위이다. 소위 해킹(hacking)이라고 불리는 이러한 행동은 사용이 허락되지 않은 컴퓨터 시스템에 불법적으로 접근하여 그 시스템 내부를 들여다보기도 하고, 파일을 꺼내보기도 하며, 시스템을 불법적으로 이용하거나 심지어는 시스템의 일부를 실수 또는 고의로 손상시키기도 한다. 이러한 행동을 즐기는 사람들을 가리켜 해커라고 부른다. 해커들이 암약하는 것은 꼭 컴퓨터의 내부에 한하

지 않는다. 앞으로 급증할 것이 예상되고 또 보안 대책상 골치거리가 될 것은 '와이어 트랩(wire trap)'의 문제이다. 와이어 트랩이란 통신회선상에 전기신호 형태로 흐르고 있는 정보를 전자유도 코일 등을 사용하여 도청하는 수법을 말한다.

4. 컴퓨터 파괴

컴퓨터 파괴란 컴퓨터 하드웨어의 파괴뿐만 아니라 컴퓨터에 수록되어 있거나 보조기억장치 등에 내장되어 있는 데이타, 소프트웨어 등의 파괴를 모두 포함한다. 컴퓨터 시스템에 대한 고의적인 파괴행위는 파업에 의한 사례보다 외부인에 의한 소행으로 발생한 경우가 많이 있다. 특히 테러조직에 의한 소행이 많이 있다.

5. 서비스 중단

서비스 중단이란 전산화되어 있는 서비스들을 불법적으로 중단하는 행위이다. 은행을 비롯하여 오늘날 대기업의 회계 및 고객, 물품 등 관리업무는 전산화되어 이들이 파업을 할 경우 기업 전체의 활동이 정지되고 커다란 사회적, 경제적 혼란과 손실을 가져온다.

6. 불법 복사

불법 복사란 시장에서 판매가 이루어지고 있는 소프트웨어를 합법적으로 취득하지 않고 불법적인 방법으로 복사판을 만들어 이용하는 것을 말한다. 특히 최근 PC가 널리 공급됨에 따라 수천 종의 소프트웨어 패키지가 개발 판매되고 있는 PC 소프트웨어 시장의 경우 해적판의 범람은 PC 소프트웨어 개발업계가 직면한 가장 큰 문제로 제기되고 있다.

3. 컴퓨터 범죄의 방지대책

일반적으로 사람들은 세가지 이유로 범죄 행위를 자제하고 있다. 첫째로는 도덕적 양심때문이며, 둘째로는 범죄를 일으킬 기회가 사실상 없기 때문이며, 셋째로는 범죄 수행 후 발각되어 처벌받을 것이 두렵기 때문이다. 이에 따라 컴퓨터 범죄를 막기 위해서는 다음과 같은 점을 고려해야 한다. 첫째, 내부 직원 또는 사회인의 도덕성을 높여야 한다. 둘째, 범죄를 일으킬 수 있는 기회를 가능한 한 줄임으로써 범죄 충동을 줄여야 한다. 셋째, 범죄 수행 후 발각될 가능성을 높이고 그것이 발견되는 경우 적절한 처벌을 함으로써 범죄에 대한 두려움을 높여야 한다.

이와 같은 세가지 사항에 근거하여, 컴퓨터 범죄로부터 시스템을 보호하기 위한 방지대책을 그림 1과 같이 4가지의 계층으로 나누어 생각할 수 있다. 즉, 기술적인 통제 방안을 이용하는 기술적 방지대책, 물리적으로 시스템 환경을 안전하게 보호하기 위한 물리적 방지대책, 컴퓨터 시스템의 관리 및 운영적인 측면에서의 관리적 방지대책, 마지막으로 국가적인 차원에서 지원해야 하는 법적/제도적 방지대책 등으로 나누어 진다.

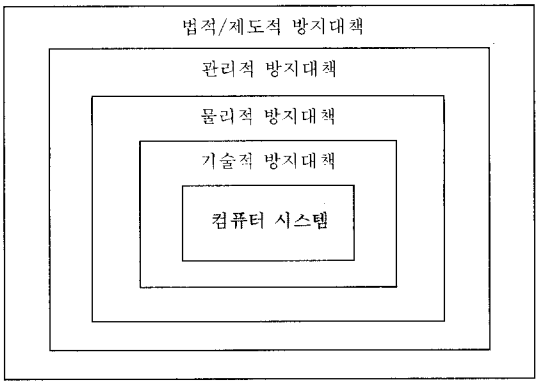


그림 1 컴퓨터 범죄의 방지대책

Fig. 1. The protection scheme of computer crime

4. 컴퓨터 통신망의 보호모델

컴퓨터 통신망의 보호서비스들로는 비밀보장, 신분인증, 접근제어, 데이타 무결성, 그리고 부인봉쇄 서비스가 있다. 사용되는 메카니즘들로는 암호화, 인증, 데이타 무결화, 접근제어, 디지탈서명, 트래픽 패딩, 경로제어 그리고 공증 메카니즘이 있다[1]. 전형적인 OSI 참조모델과 호환되는 보호모델의 구조와 각 계층의 보호 프로토콜은 그림 2와 같다.

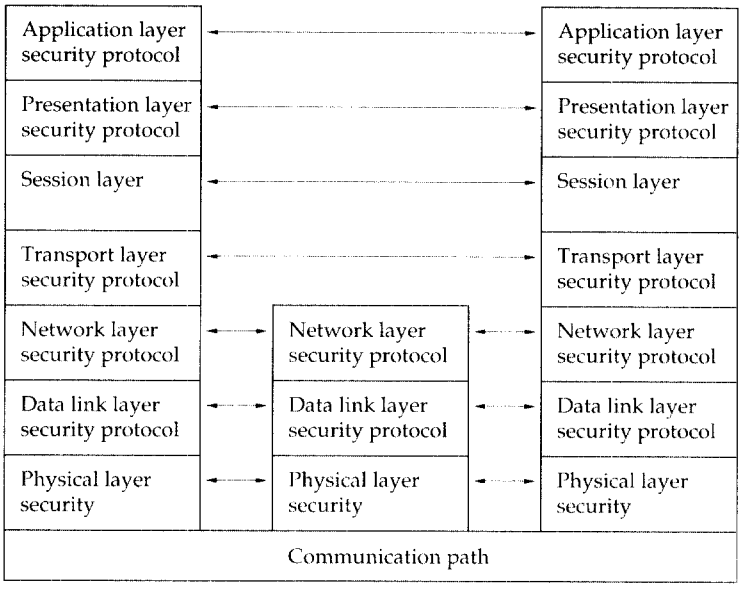


그림 2 OSI참조모델에서의 보호프로토콜

Fig. 2. Placement of security protocols in OSI 7-layer

물리계층에서의 보호는 ISO 9160[9]에서 정의하고 있으며 전송되는 모든 비트를 암호화한다. 데이타 링크 계층의 보호에 대해서는 보호서비스는 규정되어 있으나, 다양한 프로토콜에 사용될 수 있는 구체적인 보호메카니즘은 정해지지 않고 있다. 반면에, 근거리 통신망에서의 보호 위해 IEEE 802.10[10]은 제 2계층 보호 프로토콜을 규정하고 있다. 네트워크 계층과 트랜스포트 계층에서의 보호는 SDNS(secure data networksystem)[11] 프로젝트에 의해 SP3(security protocol 3)[12]과 SP4(security protocol 4)[13]가 정의되었다. ISO와 IEC의 JTC1/SC6에서는 네트워크 계층과 트랜스포트 계층 보호 프로토콜의 표준화를 추진하고 있다[14][15]. 세션 계층에서는 보호서비스가 제공되지 않고 있다. 프리젠테이션 계층에서 제공되는 기능들은 암호에 기초한 데이타의 구문적인 부호화이다. 응용 계층에서의 보호는 MHS(message handling system) 보호[16], FTAM(file transfer, access, and management) 보호와 디렉토리 보호 등이 있으며 현재 CCITT X.400, ISO 8571, CCITT X.507 등에서 연구중이다.

각 계층에 보호서비스와 메카니즘을 할당하는데 고려될 사항은 다음과 같고, 표 1은 OSI 참조모델 각 계층과 보호서비스 그리고 보호메카니즘 간의 관계를 나타낸 것이다.

1) 최소화된 방법으로 보호서비스가 구현되야 한다.
2) 한 계층이상에서 보호서비스가 제공되어도 보호시스템의 구성이 가능해야 한다.
3) 보호를 위한 추가기능은 OSI의 기존 기능

과 중복되어서는 안된다.

4) 계층의 독립성을 위반하지 않아야 한다.5) 보호해야 할 기능의 양은 최소화되어야 한다.

6) 한 실체가 하위 계층의 실체에 의해 제공되는 보호메카니즘에 종속적인 경우, 중간 계층들의 보호에 위반되지 않아야 한다.

7) 보호기능이 추가될 때는 가능한 한 독립된 모듈로서 실현될 수 있도록 정의되어야 한다.

표 1. OSI 참조모델 각 계층에서의 보호서비스 및 보호서비스와 보호메카니즘간의 관계

Table 1. Security services in OSI reference model and the relationships between security services and mechanisms.

	Layer							Mechanisms							
Service	1	2	3	4	5	6	7*	E	D.S.	A.C.	D.I.	A.E.	T.P.	R.C.	N
Peer entity authentication	·	·	Y	Y	·	·	Y	Y	Y	·	·	Y	·	·	·
Data origin authentication	·	·	Y	Y	·	·	Y	Y	Y	·	·	·	·	·	·
Access control service	·	·	Y	Y	·	·	Y	·	·	Y	·	·	·	·	·
Connection confidential	Y	Y	Y	Y	·	·	Y	Y	·	·	·	·	·	Y	·
Connectionless confidential	·	Y	Y	Y	·	·	Y	Y	·	·	·	·	·	Y	·
Selective field confidential	·	·	·	·	·	·	Y	Y	·	·	·	·	·	·	·
Traffic flow confidential	Y	·	Y	·	·	·	Y	Y	·	·	·	·	Y	Y	·
Connection integrity with recovery	·	·	·	Y	·	·	Y	Y	·	·	Y	·	·	·	·
Connection integrity without recovery	·	·	Y	Y	·	·	Y	Y	·	·	Y	·	·	·	·
Selective field connection integrity	·	·	·	·	·	·	Y	Y	·	·	Y	·	·	·	·
Connectionless integrity	·	·	Y	Y	·	·	Y	Y	Y	·	Y	·	·	·	·
Selective field connectionless integrity	·	·	·	·	·	·	Y	Y	Y	·	Y	·	·	·	·
Non - repudiation, origin	·	·	·	·	·	·	Y	·	Y	·	Y	·	·	·	Y
Non - repudiation, delivery	·	·	·	·	·	·	Y	·	Y	·	Y	·	·	·	Y

Where,

Y : Yes

· : Not provided

* : It should be noted, with respect to layer 7, that the application process may, itself, provide security services

E : Encipherment, D.S. : Digital signature, A.C : Access control

D.I. : Data integrity, A.E. : Authentication exchange,

T.P : Traffic padding. R.C. : Routing control, N. : Notarization

Note, The presentation layer contains a number of security facilities which support the provision of security services by the application layer.

표 1에서 하나의 서비스에 대해 타당한 메카니즘이라고 표시한 것이 절대적인 것은 아니다. 즉, 타당하다고 표시된 메카니즘은 그 메카니즘 하나 혹은 표시된 다른 메카니즘과 함께 적용될 수도 있다.

5. 컴퓨터 범죄의 기술적 대처방안

컴퓨터 범죄의 유형은 2장에서 기술한 바와 같이 경험적 기준에 의하여 컴퓨터 횡령, 컴퓨터 자원의 절취, 해커, 컴퓨터 파괴, 서비스 중단, 그리고 불법 복사로 구분하였다. 이러한 컴퓨터 범죄로부터 시스템을 보호하기 위한 방지대책으로는 기술적 방지대책, 물리적 방지대책, 관리적 방지대책, 그리고 법적/제도적 방지대책으로 나누어진다. 표

2는 컴퓨터 범죄와 이의 방지대책간의 관계를 나타낸 것이다.

표 2. 컴퓨터 범죄와 방지대책간의 관계

Table 2. The relationship between computer crime and its prevention scheme.

대책 / 유형	기술적 방지대책	물리적 방지대책	관리적 방지대책	법적/제도적 방지대책
컴퓨터 횡령	Y	Y	Y	Y
컴퓨터자원 절취	Y	Y	Y	Y
해커	Y	N	Y	Y
컴퓨터 파괴	N	Y	Y	Y
서비스 중단	N	N	Y	Y
불법 복사	Y	N	Y	Y

Y : 가능, N : 불능

물리적 방지대책은 건물, 사원, 혹은 방문자의 출입관리나 데이타 및 프로그램의 보호관리로 이루어지며 컴퓨터 횡령, 컴퓨터자원절취, 컴퓨터 파괴와 같은 물리적 접근에 의해 이루어지는 컴퓨터 범죄는 막을 수 있으나 해커, 불법 복사, 서비스 중단과 같은 유형은 막을 수 없다. 관리적 방지대책은 안전한 조직체계 설계 및 정보의 기밀 등급 분류로 이루어지며 효율적인 관리로 모든 범죄 유형이 발생할 수 있는 기회를 줄이도록 한다. 법적/제도적 방지대책은 컴퓨터 범죄가 발생하였을 경우 이를 적절하게 처벌할 수 있는 법적 근거를 마련하여 범죄에 대한 두려움을 높여 컴퓨터 범죄를 막는 것이다. 기술적 방지 대책은 컴퓨터 범죄를 암호학에 기초하여 대처하며 컴퓨터 횡령, 컴퓨터자원절취, 그리고 불법 복사 등의 범죄를 막

표 3. 컴퓨터 범죄의 기술적 보호방안

Table 3. Technical prevention schemes of the computer crime.

범죄유형	범죄방법	보호서비스	메카니즘	계층
컴퓨터 횡 령	입력조작	접근제어 부인봉쇄	접근제어 서명, 공증	3,4,7 7
	데이타변조	접근제어 신분인증 비밀보장 무결성 부인봉쇄	접근제어 인증, 서명, 암호화 암호화 무결화, 서명 서명, 공증	3,4,7 3,4,7 1,2,3,4,7 3,4,7 7
	출력조작	접근제어 서명	접근제어 서명, 공증	3,4,7 7
컴퓨터 자 원 절 취	데이타절취	접근제어 신분인증 비밀보장	접근제어 인증, 서명, 암호화 암호화	3,4,7 3,4,7 1,2,3,4,7
	서비스부정 사용	접근제어 신분인증	접근제어 인증, 서명, 암호화	3,4,7 3,4,7
	Tapping	비밀보장	암호화	1,2,3,4,7
	트레픽분석	비밀보장	암호화, 트래픽패딩	1,2,3,4,7
해 커	데이타변조	접근제어 비밀보장 무결성 부인봉쇄	접근제어 암호화 무결화, 서명, 서명, 공증	3,4,7 1,2,3,4,7 3,4,7 7
	데이타절취	접근제어 신분인증 비밀보장	접근제어 인증, 서명, 암호화 암호화	3,4,7 3,4,7 1,2,3,4,7
	서비스부정 사용	접근제어 신분인증	접근제어 인증, 서명, 암호화	3,4,7 3,4,7
컴퓨터 파괴	물리적파괴	-	-	관리적, 법적대응
서비스 중단	물리적중단	-	-	관리적, 법적대응
불법 복사	S/W 복사	-	-	관리적, 법적대응

을 수 있으며 가장 효율적인 대책이라 할 수 있다.

본 논문에서는 컴퓨터 범죄의 각 유형에 대해 대처할 수 있는 보호서비스와 보호메카니즘 그리고 적용 가능한 OSI 참조모델 계층을 종합적으로 분석, 제시하며 표 3에 나타낸다.

표 3에서 컴퓨터 횡령 범죄의 한 유형인 입력조작의 경우에는 접근제어와 부인봉쇄 서비스로 대처할 수 있으며 접근제어 서비스는 접근제어 메카니즘으로 그리고 부인봉쇄 서비스는 서명 메카니즘으로 구현 가능하고 적용할 수 있는 계층은 각각 3,4,7 그리고 7계층이다. 표 3의 내용을 고찰하면 컴퓨터 파괴, 서비스 중단 및 불법 복사와 같은 범죄는 제도적 혹은 법적 대응이 효과적이고 데이타 조작 등과 같은 일반적 컴퓨터 범죄는 기술적인 보호방법이 효과적이나 기술적, 물리적, 관리적, 그리고 법적/제도적 방지대책이 적절하게 병행되어질때 컴퓨터 범죄에 보다 효율적으로 대처할 수 있다. 표 3에서 알 수 있듯이 제 3계층은 혹은 제 4계층에서는 부인봉쇄 서비스를 제외한 모든 보호서비스가 제공될 수 있어 이 계층에 보호시스템을 우선적으로 구축하는 것이 매우 효과적이다. 단, 부인봉쇄 서비스는 제 7계층에서 제공되도록 해야한다.

보호메카니즘을 구현하는데 사용될 대표적인 보호알고리듬에는 DES(data encryption standard), FEAL(fast encryption algorithm), key-escrow system, ZKIP(zero knowledge interactive proof), SHA(secure hash algorithm), MD5(message digest algorithm)와 DSS(digital signature standard)등이 있으며 표 4는 보호메카니즘과 대표적 보호알고리듬간의 관계를 나타낸 것이다. 구현에 사용될 대표적 알고리듬인 DES, FEAL-8, SHA, MD5와 디지탈 서명의 연산인 모듈라 곱 알고리듬의 수행시간은 표 5와 같이 80486 PC(50 MHz)상에서 수 *ms*에서 수십 *ms* 이므로 실시간 구현이 가능하다.

표 4. 보호메카니즘과 구현에 사용될 대표적 보호알고리듬
Table 4. Security mechanism and representaive security algotithm for implementation.

보호메카니즘	보호알고리듬
암호화	DES, FEAL, RSA, Key-escrow system
인증	D-H, RSA, ZKIP, DES, FEAL
접근제어	DES, FEAL
데이타 무결화	SHA, MD5
디지탈 서명	DSS, RSA
트래픽 패딩	DES, FEAL
공증 메카니즘	DSS, RSA, DES, FEAL, SHA, MD5
경로제어	-

표 5. 대표적 보호알고리듬의 수행시간(80486 PC (50 MHz))
Table 5. Excution time of the representive security algorithm in 80486 PC(50 MHz).

보호알고리듬		수행시간 [ms]	비고
DES		16.40	입출력 : 64 비트 데이타 : 512 비트
FEAL-8		6.53	입출력 : 64 비트 데이타 : 512 비트
MD5		2.34	입력 : 512 비트 출력 : 128 비트
SHA		2.48	입력 : 512 비트 출력 : 160 비트
모듈라 곱	Yang	3.32	곱셈시간 (512 비트)
	Montgomery	3.10	곱셈시간 (512 비트)

6. 결 론

본 논문에서는 컴퓨터 통신망에 관련된 범죄를 유형별로 구분하고 이에 대한 기술적 방지대책을 구체적으로 제시하였다. 컴퓨터 범죄를 경험적인 기준에 의하여 컴퓨터 횡령, 컴퓨터 자원의 절취, 해커, 컴퓨터 파괴, 서비스 중단, 그리고 불법 복사로 구분하였다. 컴퓨터 파괴, 서비스 중단 및 불법 복사와 같은 범죄는 제도적 혹은 법적 대응이 효과적이고, 컴퓨터 횡령, 컴퓨터 자원의 절취와 해커 같은 컴퓨터 범죄에 대한 방지는 기술적인 대응이 효과적이나 기술적, 물리적, 관리적, 그리

고 법적/제도적 방지대책이 적절하게 병행되어질 때 컴퓨터 범죄에 보다 효율적으로 대처할 수 있다. 전형적인 OSI 참조모델에 기초한 보호모델 구조와 컴퓨터 범죄의 각 유형에 대해서 대처할 수 있는 보호 서비스 및 메카니즘 그리고 적용 가능한 계층을 분석 제시하였다. 또한 보호메카니즘을 구현하는데 사용될 대표적 보호알고리듬인 DES, FEAL, SHA, MD5와 디지탈 서명의 연산인 모듈라 곱 알고리듬의 수행시간은 80486 PC (50 MHz)상에서 수 *ms*에서 수십 *ms*이므로 실시간 구현이 가능하다.

참 고 문 헌

[1] ISO, Information Processing - Open System Interconnection-Basic Reference Model - Part 2 : Security Architecture, ISO 7498-2, 1989.

[2] D. B. Parker, Computer Abuse Assessment, SRI, 1975.

[3] L. Rohner, Computerkriminalitat, Schulthess Polygraphischer Verlag AG, 1976.

[4] U. Sieber, Computerkriminalitat und Strafrecht, Carl Heymanns, 1980.

[5] K. Tiedemann, Wirtschaftsstrafrecht unt Wirtschaftskriminalitat, 1976.

[6] U. Sieber, The International Handbook on Computer Crime, Jon Wiley & Sons Ltd., 1986.

[7] J. A. Schweitzer, Computer Crime and Business Information : A Practical Guide for Managers, Elsevier, 1986.

[8] 門田 涉, "我の國におけるコソピュータ犯罪の現狀," 警擦公論, 1985年 7月

[9] ISO, Information Processing - Data Encipherment - Physical Layer Interoperability Requirements, ISO 9160, Feb. 1988.

[10] IEEE, Standard for Interoperable Local Area Network Security (SILS), IEEE 802.10/D6, Sep. 1989.

[11] R. Nelson and J. Heimann, "SDNS architecture and end - to - end encryption," CRYPTO 89', pp. 356-366, Aug. 1989.

[12] SDNS Program Office, Security Protocol 3 (SP3), SDN.301, Revision 1.5, May. 1989.

[13] SDNS Program Office, Security Protocol 4 (SP4), SDN.401, Revision 1.3, May. 1989.

[14] ISO/IEC JTC 1/SC 6, Information Technology - Telecommunications and Information Exchange Between Systems - Nework Layer Security, DIS Ballot Text of ISO/IEC 11577, Jan. 1993.

[15] ISO/IEC JTC 1/SC 6, Information Technology - Telecommunications and Information Exchange Between Systems - Transport Layer Security, Draft of the New DIS Test, Oct. 1992.

[16] CCITT, Message Handling system : EDI Messaging System, Draft Recommendation X.435, Version 6.0, Nov. 1990.

□ 著者紹介

박 영 호 (정회원)

1989년 2월 경북대학교 전자공학과 (공학사)
1991년 2월 경북대학교 전자공학과 (공학석사)
1991년 3월 ~ 현재 경북대학교 전자공학과 박사과정

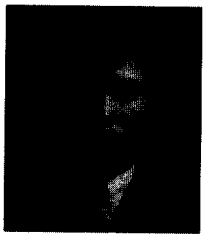
문 상 재 (종신회원)

1948년 4월 20일생
서울대학교 공업교육과 (전자전공 학사)
서울대학교 대학원 전자공학과 (석사)
미국 UCLA 공학박사 (통신공학 전공)
금성 전기주식회사 근무
미국 UCLA 연구조원 근무
미국 Satellite Tech. Management Inc. 근무/ 미국 UCLA Postdoctor 근무 (Dept. of Elec. Eng.)/
미국 OMNET 주식회사 Consultant 근무
경북대학교 전자공학과 부교수
※ 주관심분야 : 부호기술 및 디지탈통신 등

김 세 헌 (종신회원)

서울문리대 물리학과 졸업
미국 Standford대학교 (경영과학 석사 및 박사)
미국 System control, Inc사 근무
현재 한국과학기술원 경영과학과 교수, 본 학회 편집위원장
※ 주관심분야 : 컴퓨터 범죄와 프라이버시 침해 방지 대책, 정보시스템 보안, 암호학

□ 著者紹介



강 신 각 (정회원)

1984년 2월 충남대학교 전자공학과 (공학사)
1987년 8월 충남대학교 전자공학과 (공학석사)
1984년 3월 ~ 현재 한국전자통신연구소 정보통신표준연구센터 선임연구원

임 주 환

1972년 2월 서울대학교 공업교육과 (전자전공, 공학사)
1979년 2월 서울대학교 대학원 (공학석사)
1984년 7월 독일 Braunschweig 공대 (공학박사)
1978년 ~ 1979년 한국통신기술연구소 연구원
1979년 ~ 1984년 독일 Braunschweig 공대 통신시스템연구소 연구원
1984년 ~ 현재 한국전자통신연구소 (책임연구원)
ISDN 연구부장, 교환연구부장, 정보통신표준연구센터장 역임
현재 교환기술연구단장