IDEF0 모델링을 이용한 인터넷 전자우편 보안시스템 분석

김중인 · 김석우

Systems Analysis of the Internet E-Mail Security Using IDEF0 Modeling

Joong-In Kim · Seok-Woo Kim

〈Abstract〉

The Internet e-mail security software and standards, such as PGP (Pretty Good Privacy) and PEM (Privacy Enhanced Mail), have several limitations that should be overcome for their further applications to the Internet and network environments. In order to improve and reengineer those software, details of the As-Is software processing should be analyzed. One of the possible techniques for software analysis is IDEF0 function modeling. Although IDEF0 has been mainly used for BPR as one of the industrial engineering techniques, it has been rarely applied to the analysis of software processing and reengineering in computer and software engineering fields. Additionally, no sufficient details of PGP and PEM processing are analyzed in the literature. The objective of this paper is to demonstrate the application of the IDEF0 to the systems analysis of the Internet e-mail security software as well as to provide software developers with the basis for software improvements.

1. 서론

인터넷 전자우편을 위한 보안시스템의 de facto 표준인 PGP(Pretty Good privacy)와 IETF(Internet Engineering Task Force)의 de jure 표준인 PEM(Privacy Enhanced Mail)은 개인-대-개인(end-to-end)방식의 아키텍춰, 시스템 요구조건 및 설계규격등을 개발해 왔다 [2, 7, 8, 9, 11, 12, 17, 19, 20, 21, 25]. PGP와 PEM은 둘다 전자우편에 보안서비스를 제공하기 위하여 관용적인 대칭키 암호방식(symmetric cryptoalgorithm)과 공개키(public key)를 사용하는 비대칭키 암호방식(asymmetric cryptoalgorithm)을 혼합하여 사용한다.

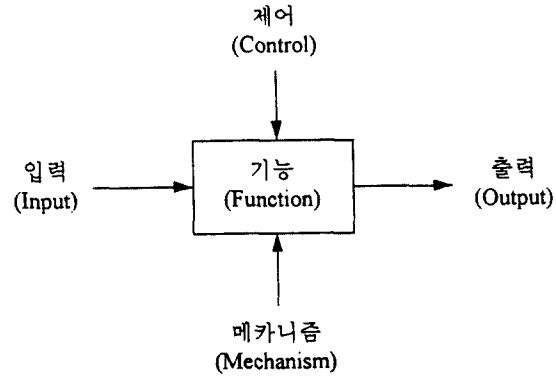
PGP와 PEM에서는 어떻게 한 개인의 공개키가 정말로 그 사람에게 속한 것임을 확인할 수 있는가 하는 것이 중요한 문제가 된다. PGP에서는 이 문제를 각 개인이 직접 다른 사람의 공개키를 보증해주는 personal web of trust방식을 채택하여 해결하고 있다. 그러나, 이 방식은 전자우편을 주고 받는 수 많은 당사자들이 상호간에 상대방의 공개키를 보증하기 위해서 개인적인 접촉을 통해 서로를 소개해야만 한다는 문제점이 있다. 인터넷 보안 연구 그룹에서는 이러한 어려움을 해결하기 위해 PEM(Privacy Enhanced Mail)이라는 표준을 개발하여 신뢰할 수 있는 제삼의 보증기관들(trusted third parties, 즉certification authorities)에서 사용자의 공개키에 대한 보증서(certificate)를 발급해 주도록 하고 있다. 이때, 제삼의 보증기관들은 계층구조를 형성하게 되며, 이러한 계층구조는 PGP의 개인적인 공개키 보증 방식보다 확장성은 좋지만 상당한 하부구조(infrastructure)가 구축되어야만하는 단점이 있다.

한편, PGP와 PEM은 서로 다른 암호알고리즘과 메시지구조를 사용하기 때문에 상호간에 인터넷 전자우편의 호환성이 제공되지 않는다. 또한, PGP와 PEM은 전자우편에 보안서비스를 제공하지만 멀티미디어 데이타를 처리할 수 없고, 멀티미디어 전자우편 프로토콜인 MIME(Multipurpose Internet Mail Extensions)은 보안서비스를 제공하지 못하고 있다. 따라서, 최근에는 PGP와 PEM을 MIME과 통합하기 위한 전자우편 프로토콜로서 PGP/MIME [24]과 PEM/MIME (또는 MMIME Object Security Services: MOSS) [4]이 제안되어 개정중에 있다. 그러나, 새로운 프로토콜들도 멀티미디어만을 추가로 지원했을뿐 앞에서 언급한 기존의 문제점들을 그대로 가지고 있다. 즉, PGP의 personal web of trust 문제, PEM의 계층적 보증기관 구축의 현실적인 어려움, PGP와 PEM의 호환성, 새로운 프로토콜들과 기존의 PGP 및 PEM과의 역방향 호환성(backward compatibility) 등이다. 따라서, 이러한 문제점들을 해결하기 위해서는 PGP와 PEM의 개선이나 새로운 전자우편 보안 시스템의 개발이 필요한 실정이다.

이러한 전자우편 보안시스템의 개선이나 리엔지니어링을 위해서는 As-Is 소프트웨어 기능(functions) 또는 처리절차(procedures)가 자세히 분석되어야만 한다. 기능 분석을 위한 모델링 기법으로는 IDEF0(ICAM DEFinition 0 또는 Integration DEFinition 0 for function modeling)와 DFD(Data Flow Diagram)가 사용될 수 있다. IDEF0는 산업공학적 기법의 하나로써 미국과 유럽에서 BPR(Business Process Reengineering)과 기업 모델링(enterprise modeling)에 주로 쓰여왔지만 [1, 5, 6, 10, 13, 14, 15, 16, 18, 22, 23], 정보통신, 전산 및 소프트웨어 공학분야에서는 거의 소개되지 않은 상태이고 소프트웨어 기능 분석, 소프트웨어 개발 및 리엔지니어링에의 응용은 찾기가 매우 어렵다. 대신 이 분야에서는 DFD가 주로 사용되어 왔으며 최근에는 객체지향 기법들이 사용되고 있다 [16]. 한편, PGP와 PEM에 대해 다루고 있는 문헌들에서는 소프트웨어 개발자 및 프로그래머들을 위한, 기술적으로 자세한 소프트웨어 처리절차에 대한 분석이 나타나 있지 않아서 이들의 개선 및 리엔지니어링을 위해서는 소스코드 수준의 분석이 필요한 실정이다. 특히, 전자우편 보안을 포함한 각종 정보보안시스템에 대한 DFD와 IDEF0를 이용한 분석은 현재까지 존재하지 않고 있다. 따라서 본 연구는 산업공학적 기법인 IDEF0를 인터넷 전자우편 보안시스템의 기능 분석에 적용한 예를 제시하고, 소프트웨어 개발자 및 프로그래머들이 필요로 하는 자세한 소프트웨어 처리절차를 제공하는 데 목적이 있다.

2. 시스템분석을 위한 IDEF0 모델링기법

IDEF0 기능 모델의 기본 단위는 〈그림 1〉에 나타나 있는 하나의 기능 단위이다. 〈그림1〉의 나타난 기능의 이름은 대개 [동사+명사]의 형식을 따른다 (예를 들면, Perform Analysis). 입력(input)과 제어(control)는 둘 다 기능 수행에 필요한 정보 및 개체들을 나타내는데, 차이점은 입력은 기능에 의해 그 속성, 성질 또는 정보값 등이 변환되는데 반해, 제어는 기능에 의해 변환되지 않고 단지 기능을 수행하는데 필요한 정보, 제어 또는 정책 등을 나타낸다. 메카니즘(mechanism)은 기능을 수행하는데 필요한 자원(resource)으로서 소프트웨어, 장비등을 나타낸다.



〈그림 1〉 IDEF0 기능 단위

IDEF0 모델에서의 기능들은 〈그림 2〉에 나타난 바와 같이 ICOM (Inputs, Controls, Outputs 과 Mechanisms) 흐름들에 의해 상호연결되며, 하위수준의 서브-기능들로 더 자세하게 하향식으로 분해(top-down

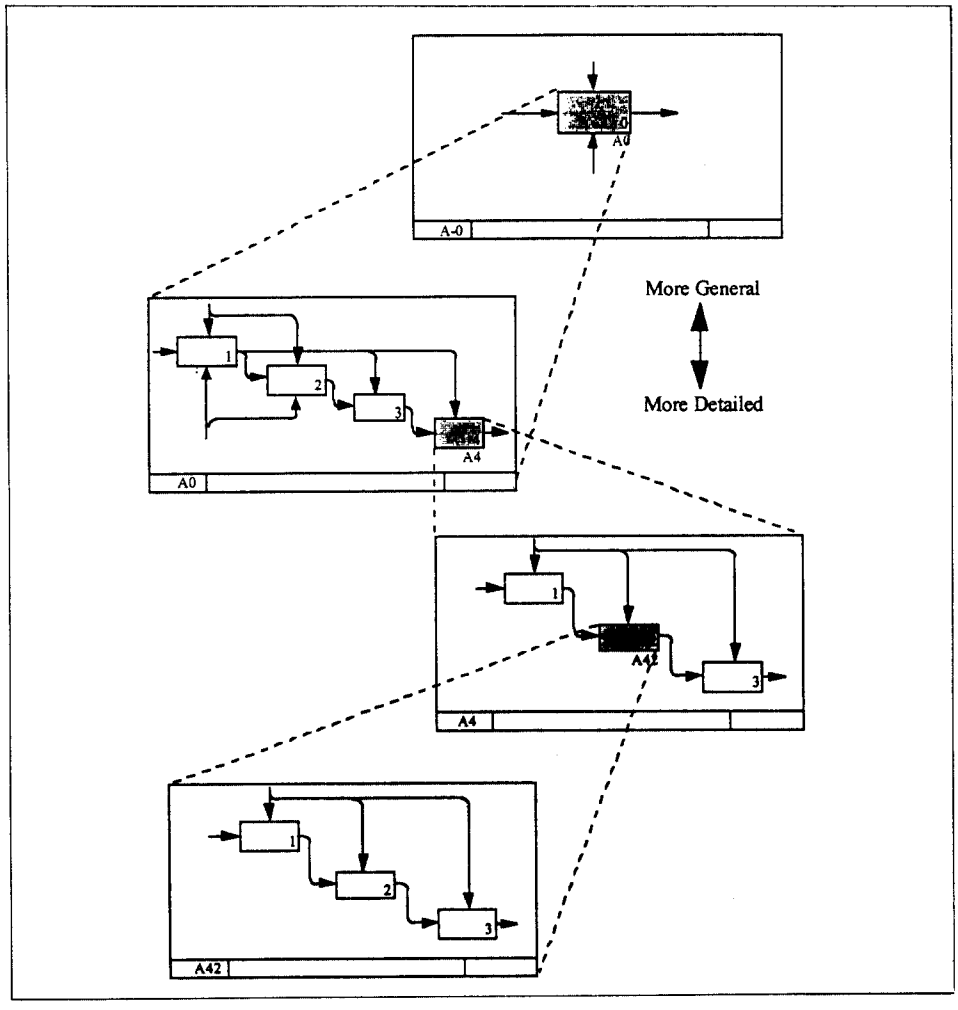
decomposition)되는데 이러한 분해작업은 어떤 특정 프로젝트에서 필요한 만큼의 기능들이 파악되고 문제영역(problem domain)이 필요한 만큼 분석될 때까지 계속된다.

3. PGP와 PEM에서 제공되는 보안과 통신 서비스

PGP와 PEM은 인터넷 전자우편에 데이타 비밀성(confidentiality), 데이타 발신자 인증(data-origin authentication), 데이타 무결성(data integrity), 그리고 발신자 부인 봉쇄(non-repudiation with proof of origin)와 같은 보안 서비스들을 제공한다. 또한 PGP와 PEM은 canonicalization 및 인코딩(encoding)과 같은 통신 서비스도 제공하는데, 특히 PGP는 한 컴퓨터내에 있는 파일들과 디렉토리 전체를 암호화하는 기능 및 메시지의 압축(compression)과 분할(segmentation) 서비스를 추가로 제공한다.

데이타 비밀성은 전자우편 메시지의 내용을 통신로상에서나 사용자의 전자우편함에서 발생할 수 있는 불법적인 노출로부터 보호하는 서비스이다. 즉, 메시지는 발신자와 수신자만이 읽을 수 있도록 한다.

데이타 발신처 인증은 수신자로 하여금 메시지의 발신자가 정말로 메시지를 보낸 사람인지를 확인할



〈그림 2〉 하향식(top-down) 기능 분해

수 있도록 하는 서비스이다. 만일 중간 수신자가 다시 다른 수신자에게 메시지를 재전송(forwarding)했을 경우에는 원 발신자대신에 중간 수신자(즉, 재전송된 메시지의 발신자)를 확인할 수 있도록 해준다.

데이타 무결성은 메시지가 불법적으로 변경되지 않았음을 확인할 수 있도록 하는 서비스이다. 즉, 수신자가 메시지의 변경여부를 확인할 수 있도록 한다.

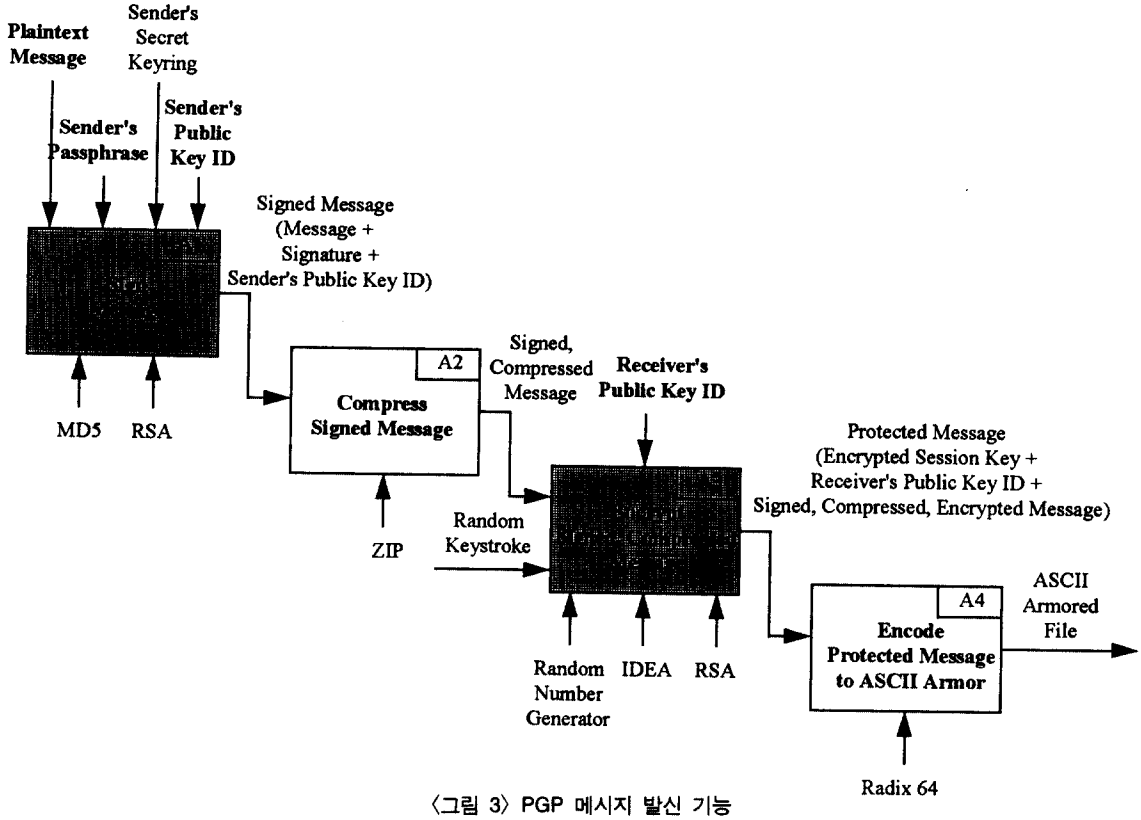
발신자 부인봉쇄는 발신자가 메시지를 보내고도 나중에 특별한 사건이 발생했을 때 메시지를 보내지 않았다고 거짓으로 부인하는 것을 방지하기 위한 서비스이다. 이런 일이 발생했을 경우에 수신자는 신뢰할 수 있는 제삼자에게 메시지를 재전송하여서 제삼자가 발신자를 확인할 수 있는 메카니즘을 제공한다.

한편, 인터넷상에서 공개키를 사용함으로 인하여 공개키의 관리기능들이 필요하다. 이러한 관리기능에는 공개키/비밀키 쌍의 생성 및 분배, 공개키 인증, 공개키 확인, 공개키의 취소, 공개키의 저장 및 유지/변경 등이 필요하다.

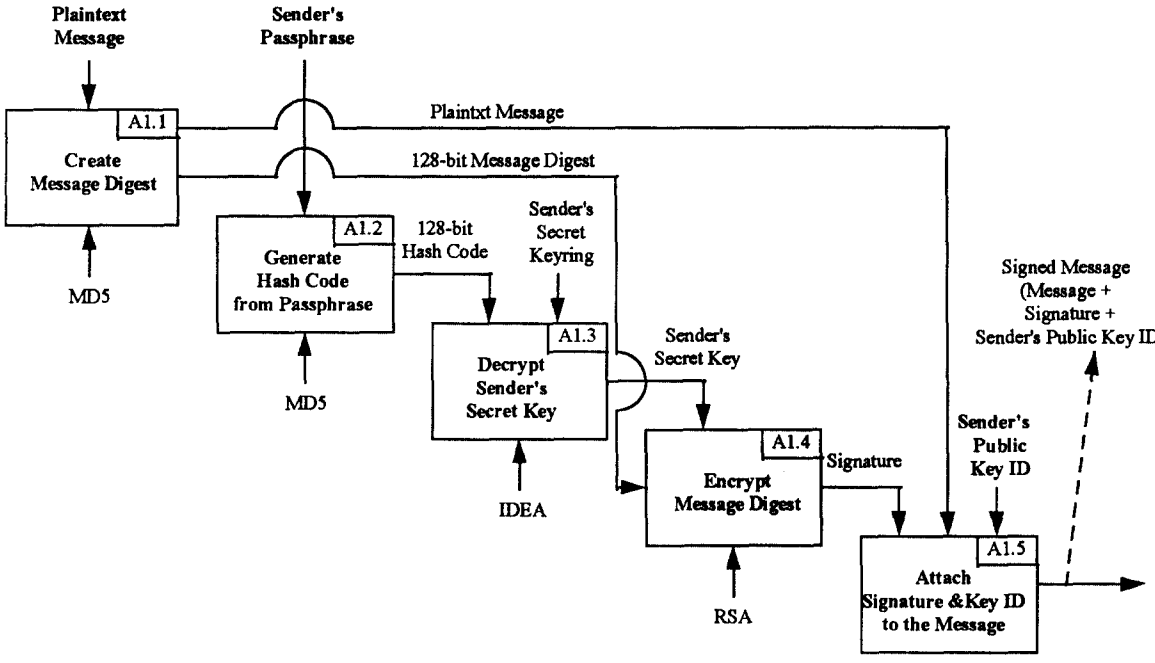
보안서비스이외에도 통신기능을 위하여 제공되는 서비스로는 먼저 canonicalization이 있다. Canonicalization은 운영체제들 사이의 연동성(interoperability)을 위한 것으로서 메시지가 어떤 문서편집기나 전자우편 소프트웨어에 의해 작성되었던 간에 공통의 네트웍 표준 형태로 메시지를 변환하여 줌으로써 인터넷상의 다양한 컴퓨터 기종과 플랫폼에서도 호환될 수 있도록 해준다.

인코딩은 데이타 비밀성을 위하여 암호화된 메시지가 이진(binary) 형태이므로 이를 ASCII 문자열로 변화시켜준다. 현재 사용되고 있는 대부분의 전자우편 시스템이 텍스트 메시지는 변경없이도 처리할 수 있지만 이진 메시지는 시스템에 따라 각각 다른 형태로 변경되어 처리되기 때문에 8비트의 이진 스트림(binary stream)형태의 메시지를 ASCII 문자열로 변환하여 줌으로써 완벽한 메시지 호환성을 제공하고 메시지의 복호화에 문제가 없도록 하기 위함이다.

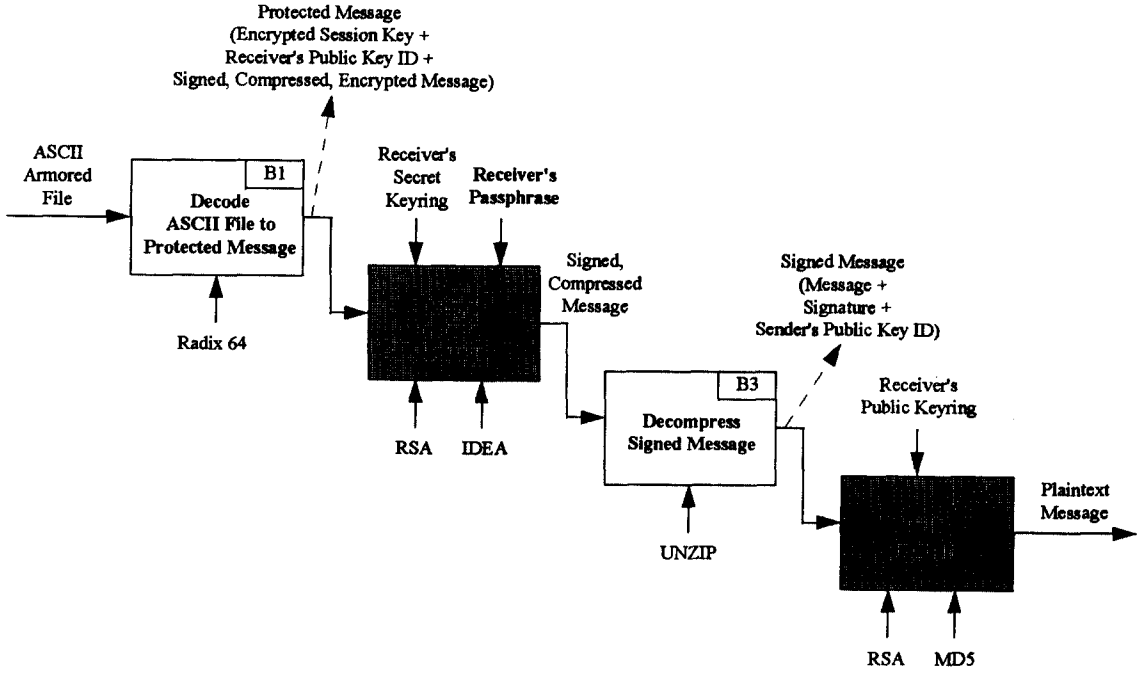
압축은 전송되는 메시지를 보다 작은 크기로 압축



〈그림 3〉 PGP 메시지 발신 기능



〈그림 4〉 Sign Message (A1) 기능의 분해된 모델

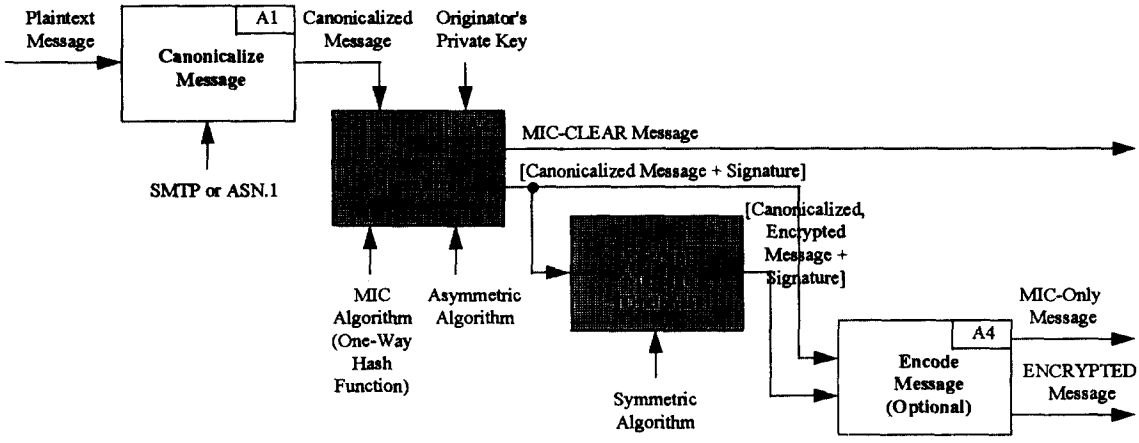


〈그림 5〉 PGP 메시지 수신 기능

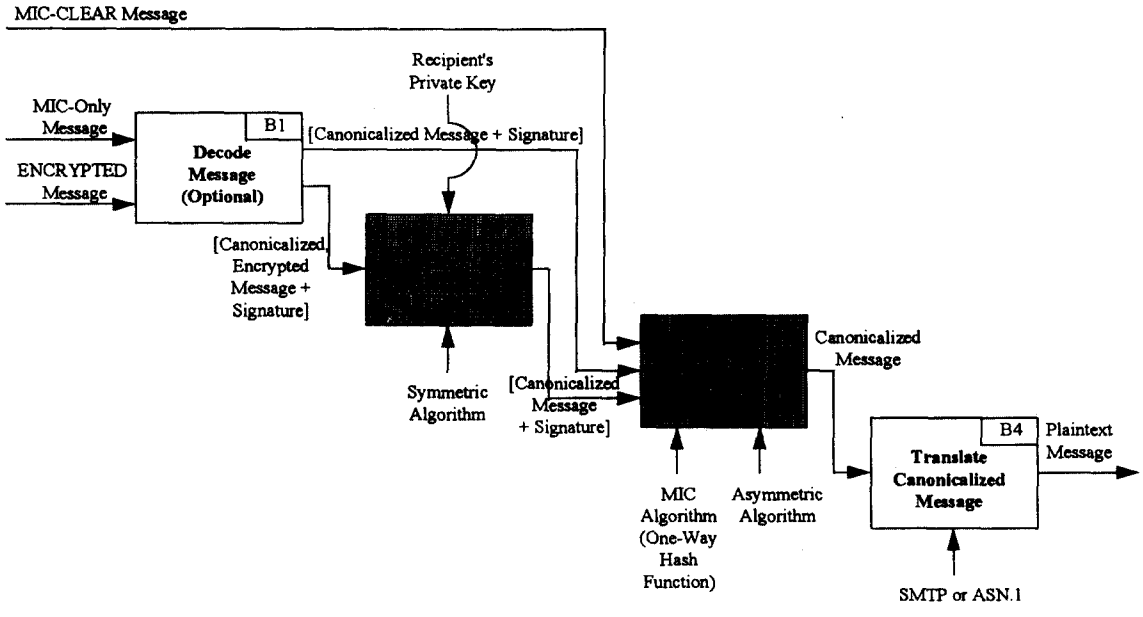
하여주며, 분할은 현재 인터넷 전자우편의 메시지 크기가 최대 50,000 바이트로 제한되어 있으므로 그 이상 크기의 메시지를 작은 단위의 세그먼트로 분할하여 전송하는 기능을 말한다.

4. PGP와 PEM 기능에 대한 IDEF0 모델

〈그림 3〉부터 〈그림 5〉까지는 바로 앞에서 설명한 PGP에서 제공하는 보안 및 통신 서비스들 중에서 PGP 메시지의 발신과 수신 처리절차에 대한 상위수준의 IDEF0모델과 발신 모델내에서의 첫번째 기능인 Sign Message (A1) 기능을 하향식으로 분해한 IDEF0모델



〈그림 6〉 PEM 메시지의 발신 기능



〈그림 7〉 PEM 메시지의 수신 기능

을 예로서 보여주고 있다. 또한 〈그림 6〉과 〈그림 7〉은 PEM의 보안 및 통신 서비스들 중에서 PEM 메시지의 발신과 수신 처리절차에 대한 상위수준의 IDEF0 기능모델을 예시하였다. 이 그림들에서 굵은 글자체로 표시된 제어(control)정보들은 PGP와 PEM의 사용시 사용자가 입력해야 되는 데이타들로서 사용자의 입력데이타와 소프트웨어가 내부에서 처리하는 데이타를 구분하여 줌으로써 소프트웨어 설계 및 프로그래밍 단계에 도움을 줄 수 있다. 이 점은 IDEF0를 소프트웨어 기능 분석에 적용할 때에 얻을 수 있는 장점중의 하나로서, 기존의 IDEF0관련 문헌들에서는 제시된 바가 없다. 또한, 그림들에서 어둡게 칠해진 기능들은 하위수준의 서브-기능들로 분해된 기능들을 나타낸다.

본 원고에서는 PGP와 PEM의 전체 보안 및 통신 서비스들에 대한 하향식 IDEF0모델들의 예시와 모델들에 대한 설명은 생략하였는데, 이는 원고의 분량이 너무 커지게 되고, IDEF0 모델의 장점이 말로된 설명이 필요없이도 쉽게 이해할 수 있는 (앞의 2절에서 설명된) 간단한 형식을 따른다는 점 때문이다. 모델에 나타난 용어의 정의 및 알고리즘등에 대한 설명은 PGP와 PEM에 관한 참고문헌[2, 7, 8, 9, 11, 12, 17, 19, 20, 21, 25]을 참조할 수 있을 것이다.

5. 결론

본 연구에서는 산업공학적 기법의 하나인 IDEF0를 인터넷 전자우편 보안시스템의 분석에 적용한 결과를 제시하였다. 인터넷 전자우편뿐만이 아니라 최근 관심과 수요가 증대하고 있는 각종 보안시스템의 개발 및 구축에 IDEF0를 이용한 시스템 분석이 중요한 역할을 할 수 있을 것으로 기대된다. 또한, IDEF0 이외에도 IDEF1x 정보 모델링 (또는 데이타 모델링) 및 객체지향 모델링 기법등을 보안시스템의 분석 및 설계에 적용한 연구도 찾아보기 어려우므로 이에 대한 향후 연구가 요구된다.

【참고문헌】

[1] Bravoco, R.R. and Yadav, S.B., A Methodology to Model the Functional Structure of an Organization, Computers in Industry, Vol. 6, pp. 345-361, 1985.

[2] 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.

[3] Crocker, D., Standard for the Format of ARPA Internet Text Message, RFC 822, 1982.

[4] Crocker, S., Freed, N., Galvin, J., and Murphy, S., MIME Object Security Services, RFC 1848, 1995.

[5] Crossley, T.R., Koriba, M., and de Hoxar, R.A., Justification of CIM Using Business Models Based on the IDEF0 Methodology, Proceedings of the 4th International Conference on Simulation in Manufacturing, pp. 251-262, 1988.

[6] Harley, M. and Cooney, B., An SADT Representation of a Production Activity Control (PAC) System, ESPRIT CIM, B. Hirsch and M. Actis-Dato (Eds.), Elsevier Science Publishers B.V. (North-Holland), 1987.

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

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

[9] Kent, S.T., Internet Privacy Enhanced Mail, Communications of the ACM, Vol. 36, No. 8, pp. 48-60, August 1993.

[10] Kim, J.I., Function, Information, Dynamics, and Organization Integrated Modeling Methodology for Enterprise Systems Integration, Ph.D. Dissertation, Arizona State University, Department of Industrial & Management Systems Engineering, 1995.

[11] Linn, J., Privacy Enhancement for Internet Electron-

ic Mail: Part I, Part II, Part III, Part IV, Network Working Group, RFC 1421, 1422, 1423, 1424, February 1993.

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

[13] Mackulak, G.T., High Level Planning and Control: An IDEF0 Analysis for Airframe Manufacture, Journal of Manufacturing Systems, Vol. 3, No. 2, pp. 121-133, 1984.

[14] NIST (National Institute of Standards and Technology), Integration Definition for Function Modeling (IDEF0), FIPS Publication 183, December 1993.

[15] Oestreich, K.P., IDEF Is Not a Four-Letter Word, 1988 Proceedings of the Production and Inventory Control, pp. 291-292, 1988.

[16] Savolainen, T. and Mattila, V., Models Required for Logistics Network Engineering, Proceeding on the Third International Conference on FAIM: Flexible Automation and Integrated Manufacturing 1993, M.M. Ahmad and W.G. Sullivan (Eds.), 1993, pp. 78-87.

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

[18] Shunk, D.L., Sullivan, B., and Cahill, J., Making the Most of IDEF Modeling-The Triple-Diagonal Concept, CIM Review, pp. 12-17, Fall 1986.

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

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

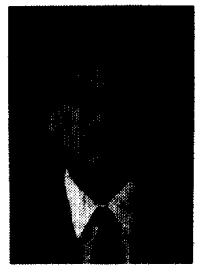
[21] Stallings, W., Protect Your Privacy: The PGP Users Guide, Prentice Hall PTR, Englewood Cliffs, New Jersey, 1995.

[22] U.S. Air Force, Integrated Computer-Aided manufacturing (ICAM) Architecture, PartII, Volume IV: Function Modeling Manual (IDEF0), AFWAL-TR-81-4023, Wright-Patterson Air Force Base, Ohio, 45333, June 1988.

[23] Wu, C., Chen, Y., and Cai, X., The State CIMS-ERC of China and Application of Integration Methodologies/Technologies, Proceedings of the 5th CIM Europe Conference, pp. 211-220, 1989.

[24] Yamamoto, K., An Integration of PGP and PEM, IEEE Proceedings of the Simposium on Network and Distributed Systems Security96, pp. 17-24, 1996.

[25] Zimmermann, P.R., PGPTM Users Guide, Phils Pretty Good Software, 1994.



김중인

1987년 한양대 산업공학과 (학사)
1989년 한양대 산업공학과 (석사)
1995년 Arizona State University 산업공학과 (박사)
1995-1996 한국전자통신연구소 선임연구원
현 재 홍익대학교 경영정보학과 전임강사
관심분야: CALS/EC, Systems & Enterprise Modeling, Object Technology, Systems Integration, Information & Network Security

김석우

1979년 항공대 통신정보공학과 (학사)
1989년 New Jersey Institute of Technology 전산학과 (석사)
1995년 아주대학교 컴퓨터공학과 (박사)
1986-1988 AT&T Bell Lab. 방문연구원
현 재 한국전자통신연구소 책임연구원
관심분야: Computer Security, Network Security, Information Security