論文2000-37TE-5-16

스마트 카드를 이용한 자료 유출 제한 시스템에 대한 연구
(A Study on Conditional Access System for Data Confidential using Smart-Card)

金 信 洪*, 李 佻 濟*
(Sin-Hong Kim and Kwang-Je Lee)

요 약

본 논문에서는 제한 알고리즘을 제안하였다. 이 알고리즘은 개별 네트워크 상의 사용자가 불법으로 자료를 유출하는 것을 제한하기 위하여 별도의 스마트카드와 전자 우편 게이트웨이를 구축하여 개별 네트워크로부터 발송되는 모든 전자우편은 스마트카드에서 인증절차를 거친 후, 전자 우편 게이트웨이로 보내어지게 된다. 전자우편 게이트웨이에서는 외부 인터넷으로 나가는 전자우편을 선별하여 그것을 방화벽 전자우편 처리 프로그램으로 보내게 되며, 송신 메일 중 첨부된 파일이 있는지를 검사하여 첨부된 파일이 있으면 전자우편 데이터베이스에 기록한다. 이때 기록된 내용과 스마트 카드 인증자료를 이용하여 내부 문건 유출시 증거 자료가 되며, 미연에 유출을 자제 할 수 있게 하는 효과도 얻을 수 있다. 뿐만 아니라 본 시스템에서는 전자우편 게이트웨이에서 사원별 필터링 환경을 관리하며 스팸 메일을 방지 할 수 있다.

Abstract

In this paper, we proposed conditional access algorithm for data confidential using smart card. This algorithm is constructed smart card and E-mail gateway for restricting of user's illegal confidential data transmission. After processing of certification procedure in smart card, each E-mail forwarded to E-mail gateway(EG). The EG selects outgoing E-mail and it is sent to fire-wall E-mail processing program, it is checked attached file in transmission mail and if it is attached file, it writes to database. This time, it can be used evidence data about user's illegal confidential data transmission, because of using registered content and smart card certification data in database. in addition to, we can get psychologically effect of prevention to send illegally, and this system can prevent spam mail in EG, also.

Ⅰ. 서 론

6월 말경에 조사기관의 발표에 따르면 인터넷 이용자 1만 명을 대상으로 인터넷 인구센서스 조사를 한 결과 전체 인터넷 인구 1천3백16만7천 여명의 70%인 9백23만2천 여명이 e-메일을 사용하고 있는 것으로 추산됐다. 이 조사에 따르면 e-메일 계정은 평균 2개 정도며, 1주일에 5-6회 e-메일을 보내는 것으로 집계됐다. 그러나 e-메일 남용이 예상보다 훨씬 심각한 수준이다. 미국의 인터넷 보안 컨설팅 업체인 월드토크의 발표자료[1]에 의하면 인터넷 e-메일 남용이 당초 예상보다 훨씬 심각한 수준이라고 발표하였다. 전체 메일 중 스팸메일(상업광고)이 10% 정도이고, 기밀문서에 대한 내용이 9%, 음란내용이 12% 정도이다. 불필요한 e-메일로 인한 기업의 피해는 다음과 같다.

* 正會員, 주성대학 컴퓨터계열
(Computer Div. Juseong College)
※ 본 연구는 학술진흥재단 연구비 지원으로 수행됨
接受日字:2000年 8月29日, 수정완료일 : 2000年11月28日

표 1. 불필요 메일로 인한 피해 사례
Table 1. Case of damage due to spam mail.

피해 내용	피해정도	비 고
시간 낭비	30%	스팸메일로 인한 낭비
스팸메일 여는데 드는 비용	50센트	미국 직원1인당 비용
월간 낭비액	1만5천 달러	천명직원을 가진 기업에 한명의 직원당 10건의 메일이 도착한다는 조건
기밀 문서 발송	산정 불가능	기업의 기밀 내용에 따라 엄청난 피해를 유발 할 수 있음.

위의 피해 사항 중 무엇보다도 심각한 피해는 대외비로 되어있는 기업의 기밀문서들이 e-메일을 통해 손쉽게 유출되고 있다는 사실이다. 이는 기업의 막대한 투자를 통해 이루어 놓은 기술정보들이 하루아침에 도용되고 낭패를 초래할 수 있다는 것이다.

본 논문에서는 이러한 기밀문서의 내부자 발송을 방지할 수 있는 알고리즘과 스팸메일 방지 알고리즘을 제안하고, 2장에서는 자료유출시스템 관련 연구이고 3장에서는 자료 유출 제한시스템의 하드웨어 구성도와 알고리즘을 제안하고 4장에서는 실험 및 결과, 5장에서는 결론 및 향후 연구방향을 제시한다.

Ⅱ. 관련 연구

1. 방화벽 설계

방화벽은 그림에 나타나 있는 것처럼 여러 가지의 주요 기능들을 수행하는 요소들로 구성되어진다. 방화벽을 설치하는 가장 기본적인 목적은 교환되는 모든 패킷들을 검사하여 오직 인가된 패킷들만이 방화벽을 통과할 수 있게 하는 것이다[2]. 따라서 방화벽은 개별 네트워크와 인터넷간에 교환되는 모든 패킷을 중간에 가로채어 사전에 정해진 규칙에 따라 패킷의 처리 여부를 결정하게 되는 패킷 필터링을 수행하게 된다.

그림 1은 방화벽의 기능을 나타내며, 그 기능을 좀 더 살펴보면 다음과 같다.

(1) 응용 게이트웨이(Application Gateway)

응용 게이트웨이는 TCP/IP 응용계층에서 사용자에 대한 실체 인증을 수행한다. 이 응용 게이트웨이의 기능은 종종 프락시 서버(proxy server)에 의해서 제공되는데, 개별 네트워크 상의 사용자는 먼저 프락시 서버에 연결되어 인증과정을 거치게 된다. 이 인증과정이 성공적으로 행해진 다음에 사용자는 인터넷상의 다른 호스트와의 연결이 가능하게 된다. 여기서 프락시 서버는 telnet과 ftp 프락시 서버를 포함하고 있다.

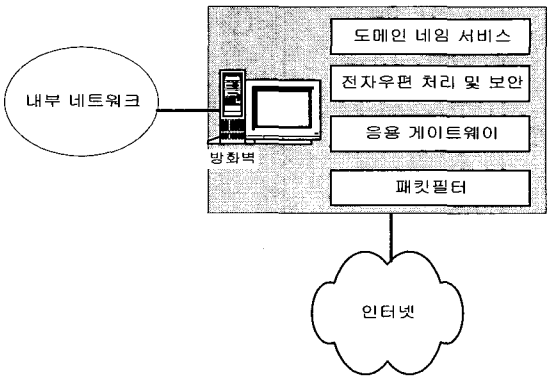

그림 1. 방화벽 구성도
Fig 1. The structure of fire-wall.

(2) 도메인 네임 서비스

도메인 네임 서비스를 통해서 개별 네트워크 상의 호스트의 IP 주소가 외부로 노출되지 않게 한다.

(3) 전자우편 처리 서비스

SMTP(Simple Mail Transfer Protocol)에 기반을 둔 전자우편은 인터넷 사용자들이 상호간에 메시지를 교환하기 위한 수단으로 사용한다. 전자우편 처리 서비스를 통해서 개별 네트워크와 인터넷간의 전자우편 교환이 항상 방화벽을 통해서 이루어지게 하고 있다. 전자우편 데몬 프로그램인 SENDMAIL의 취약점은 이미 널리 알려져 여전히 공격자들에 의한 주된 대상이 되고 있다. 전자우편 시스템으로부터 개별 네트워크를 보호하기 위한 방안 중의 하나는 개별 네트워크 상에 전자우편 게이트웨이를 구축하여 개별 네트워크로부터 발송되는 모든 전자우편은 먼저 전자우편 게이트웨이로 보내어지게 된다. 게이트웨이는 외부 인터넷으로 나가는 전자우편을 선별하여 그것을 방화벽 전자우편 처리 프로그램으로 보내고 반대로 방화벽은 외부 인터넷으로부터 수신된 전자우편을 개별 네트워크의 전자우편 게이트웨이로 보내게 된다. 방화벽은 이와 같이 다양한 보안 서비스를 제공하고 있지만 개별 네트워크 상의 사용자에 의해서 자행되는 공격은 방어할 수 없다. 방화벽은 단지 개별 네트워크와 인터넷간의 통신만을 보호 대상으로 하고 있기 때문이다.

(4) 전자우편 보안

전자우편의 사용의 빈도 및 중요성에 비해 보안성에 있어서 취약점을 지니고 있다. 어느 사용자가 다른 사용자에게 보낸 전자메일은 목적지에 도달 할 때까지 많은 게이트웨이를 거치게 된다. 전자우편은 보내는 사람의 주소뿐만 아니라 내용까지도 그대로 보이는 구조를 가지고 있기 때문에 이런 과정에서 얼마든지 탈취, 변조될 가능성을 항상 가지고 있다. 이러한 상황에서 전자우편의 보안을 유지하는 길은 같은 내용을 암호화하여, 중간에서 가로챈다 하더라도 다른 사람은 알아볼 수 없게 만드는 방법뿐이다[2].

현재 인터넷에서 사용하는 보안 기법은 PGP(Pretty Good Privacy)와 PEM(Privacy Enhanced Mail)등의 전자우편 보안 도구로 사용되고 있다. PGP와 PEM은 보내고자 하는 내용을 암호화 알고리즘을 이용하여 암호화함으로써 내용을 볼 수 없도록 하는 것이다. 본 논문에서는 전자우편 이용시 첨부한 메일을 함부로 유출하는 것을 제한하기 위한 알고리즘을 제안한다.

(5) CAS 알고리즘

기존 관련제품에서는 아직까지 CAS 알고리즘이 적용되지 않고 있다. 기존 제품에서는 첨부파일을 암호화하거나 스마트카드를 이용한 인증하는 기능을 사용하고 있다.

본 논문에서는 개별 네트워크 상의 내부 사용자가 불법으로 자료를 유출하는 것을 제한하기 위하여 별도의 스마트카드(사원카드) 인증시스템과 전자 우편 게이트웨이를 구축하여 개별 네트워크로부터 발송되는 모든 전자우편을 인증절차를 거친 후, 전자 우편 게이트웨이로 보낼 수 있도록 설계하였다. 게이트웨이는 전자우편을 선별하여 외부 인터넷으로 발송이 허가된 전자메일을 방화벽 전자우편 처리 프로그램으로 보내게 된다.

Ⅲ. 자료유출 제한 시스템 알고리즘

본 연구에서는 자료 유출을 방지하기 위하여 스마트카드를 이용한 사용자 인증과 기존의 방화벽 알고리즘인 스크린 호스트 알고리즘을 변형한 CAS 알고리즘을 제안한다.

1. CAS 하드웨어 구성도

그림 2에서 나타낸 바와 같이 외부 인터넷에서 내부 네트워크로 들어오는 것과 외부로 나가는 패킷에 대하여 CAS 알고리즘을 적용한다.

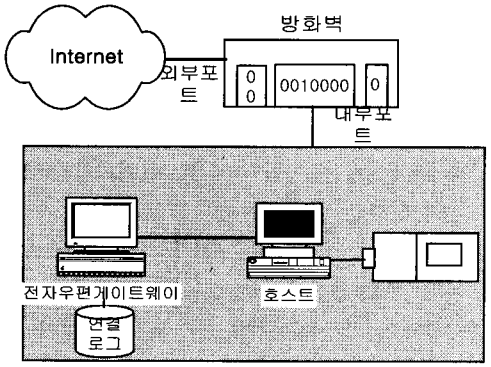

그림 2. 자료유출 제한시스템 구성도
Fig. 2. The structure of CAS.

전자우편 게이트웨이에서 연결 요청이 오면 TCP의 패킷 헤더를 분석하여 근원지/목적지의 주소와 포트번호, 제어 필드의 내용을 분석하고, 이들을 패킷 필터 규칙에 적용하여 계속 진입시킬 것인지, 아니면 거절할 것인지를 판별한다. 연결 요청 패킷의 진입이 허가되면 이후의 모든 패킷은 연결 단절이 발생할 때까지 모두 허용된다.

전자우편 게이트웨이에서는 사용자 레벨과 응용 프로토콜 레벨에서 접근 제어를 제공한다. 그리고 모든 응용 사용에 대한 기록을 유지하도록 설계되는데 특히 전송되는 모든 트래픽을 기록하고 제어 할 수 있다.

2. CAS 프로시저

단계 1. 자료를 전송하기 전에 스마트카드 리더에 삽입된 스마트카드와 ID/Password를 입력하여 사용자 인증을 요청한다.

단계 2. 사용 가부를 통보한다.

단계 3. 메일 송신시 첨부 파일을 포함시킬지를 응용계층에서 확인하고 제어필드의 첨부파일 유무 표시 필드에 기록하고 EG(전자우편 게이트웨이)로 전송한다.

단계 4. 전자우편 게이트웨이는 스마트 카드가 연결된 호스트로부터 스마트 카드 인증 패킷을 받는다.

단계 5. 전자우편 게이트웨이에서 사용자 응용 계층의 트래픽을 제어하며 첨부 파일 유무표시 필드

를 체크한다. 첨부 파일이 있는 경우 첨부 파일 및 인증 정보를 함께 하드디스크에 기록한다. 그리고 통과된 트래픽은 목적지로 전송된다.

단계 6. 전자우편 게이트웨이에서는 수신 트래픽에 대한 패킷 필터링 알고리즘을 적용한다. 포트 번호, 프로토콜 플래그, 행위(허가/거절) 등을 이용한다.

a. 패킷 필터링은 근원지 주소, 근원지의 포트번호, 목적지 주소, 목적지

b. 인터넷 주소에 적용하는 허가/거절 조건의 순차적인 액세스 집합인 액세스 리스트를 정의한다. 신규등록은 각 사용자 별 문답에 의해 추가 될 수 있다.

c. 이러한 액세스 리스트를 가지고 처리되며, 패킷을 허가 혹은 거절할 것인지를 액세스 리스트에 있는 정의에 의해서 순차적으로 결정되며, 패킷에 해당하는 액세스 리스트가 나타날 때까지 혹은 마지막 액세스 리스트에 도달할 때까지 순차적으로 점검한다.

단계 7. 전자우편 게이트웨이를 통과한 트래픽만이 송수신 될 수 있다.

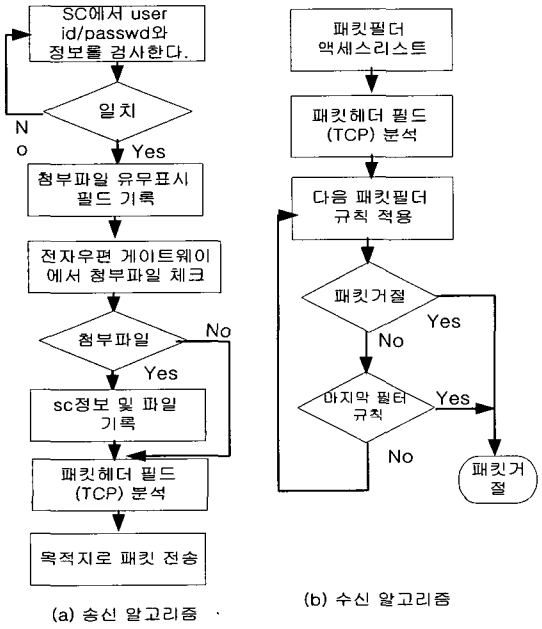

그림 3. CAS 알고리즘 순서도
Fig. 3. The flowchart of CAS algorithm.

3. 송신메일 제어필드 구성

사용자 호스트에서 EG로 전송되는 PDU는 다음과 같다.

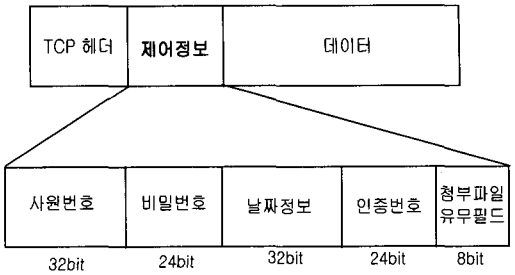

그림 4. 송신제어필드 구성
Fig. 4. The construct of transmission control field.

액세스모드 리스트의 구성은 다음과 같다.

00 : 메일 송신 요청, 01 : 액세스 리스트 요청, 02 : 리스트 추가 요청, 03 : 리스트 삭제 요청으로 구성된다.

4. 스마트 카드 오퍼레이션

(1) 스마트카드에 로그인 프로시저

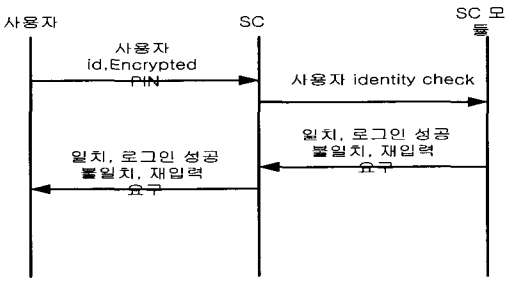

그림 5. 스마트카드 로그인 프로시듀어 조회
Fig. 5. The smart card login procedure retrieval.

(2) 스마트 카드를 이용한 사용자 프로파일

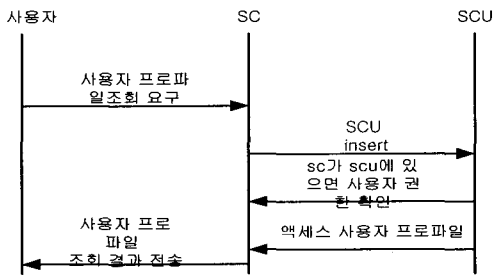

그림 6. 사용자 프로파일 조회
Fig. 6. The user profile retrieval

(3) 스마트카드 및 사용자 프로파일 생성

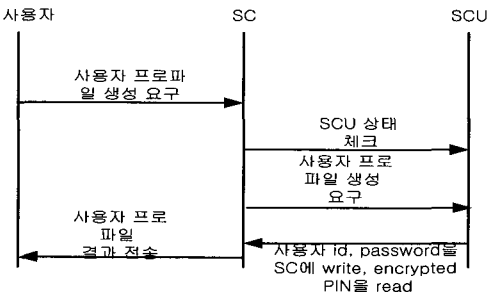

그림 7. 스마트카드 카드 및 사용자 프로파일 생성
Fig. 7. The generation of smart card and user profile.

Ⅳ. 분석 및 결과

1. 네트워크 구성 사례

그림 8은 호스트와 전자우편게이트로 구성된 네트워크이다. 131.44.0.0에 있는 모든 호스트는 인터넷의 모든 tcp서비스를 액세스 할 수 있다.

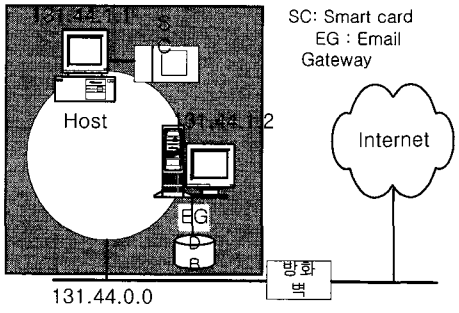

그림 8. 네트워크 구성사례 1
Fig. 8. The case of network construct(1).

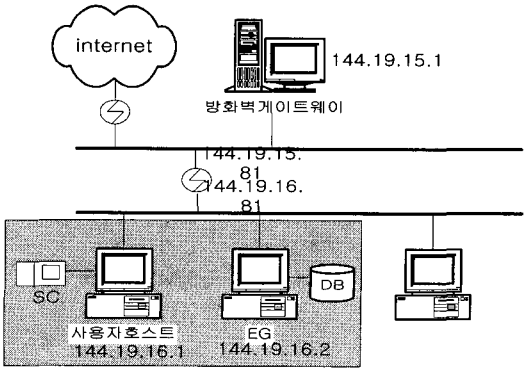

그림 9. 네트워크 구성사례 2
Fig. 9. The case of network construct(2).

그림 9는 두 개의 서브네트워크를 이용한 144.19.0.0을 나타낸다. 서브네트워크는 내부 네트워크와 외부 네트워크로 구성이 된다. 서브네트워크 15는 외부 네트워크이고 서브네트워크 16은 내부 네트워크이다. 호스트가 서브네트워크 16에 있고 IP 주소 144.19.15.81을 갖는다. 서브네트워크 15와 15에 접속된 내부 라우터의 IP 주소 세그먼트 144.19.15.81과 144.19.16.81를 갖는다. 그림 8, 그림 9인 경우 CAS 알고리즘을 적용하면 다음과 같다.

단계 1. 사용자는 우편 호스트에서 스마트 카드를 이용하여 인증 절차를 거친 후에 메일을 보낸다.

단계 2. 메일은 전자우편 게이트웨이로 보내게 되고 첨부 파일을 체크한다. 첨부 파일이 있으면 데이터베이스에 저장하고 외부 네트워크로 가는 메일을 선별하여 외부 방화벽으로 전송한다.

단계 3. 전자우편 게이트웨이에서는 전자우편에 대한 통제를 중앙 집중적으로 함으로써 개별 네트워크에 침투되는 유해한 소프트웨어를 효율적으로 통제한다.

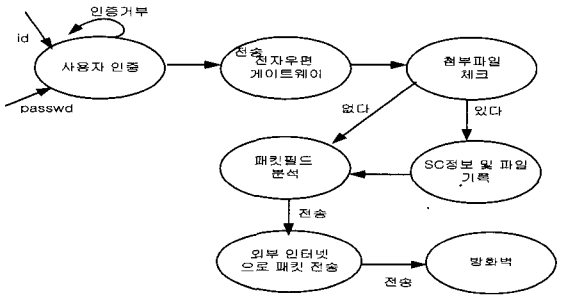

그림 10. 송신 알고리즘의 자료흐름도
Fig. 10. The data flow diagram of transmission algorithm.

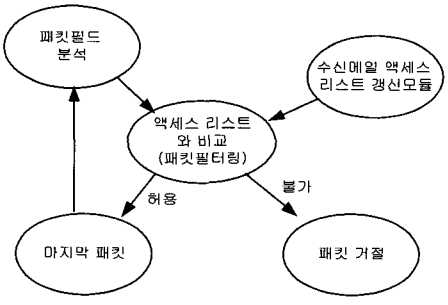

그림 11. 수신 알고리즘의 자료흐름도
Fig. 11. The data flow diagram of receive algorithm.

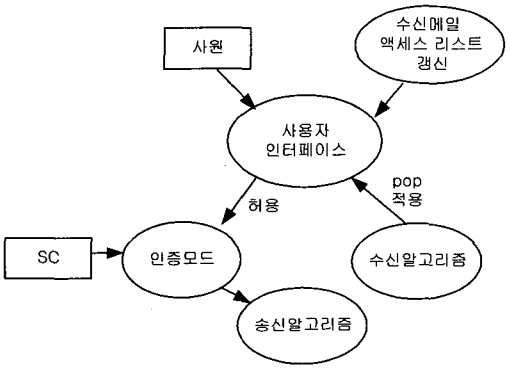

그림 12. 응용 프로그램의 자료 흐름도
Fig. 12. The data flow diagram of application program.

2. 기대효과

스마트 카드를 이용함으로써 내부 문건 유출시 증거 자료가 남게되므로 사전에 방지할 수 있다. 그리고 사원카드를 스마트카드로 활용함으로써 별도의 스마트카드를 제작할 필요가 없다. 그리고 전자우편 게이트웨이에서 사원별 필터링을 함으로써 스팸메일을 사전에 방지할 수 있는 효과가 있다. 기존 제품은 첨부파일을 체크하여 암호화하는 기법이다. 이 방법은 암호화 및 복호화 하는 처리시간이 추가로 소요된다. 그리고 암호화는 하지만 자료유출은 피할 수 없다.

표 2. 제품 비교분석
Table 2. The analysis of product comparison.

제품명	자료유출	자료유출제한 방법	기능
A	유출	-	첨부파일암호화
B	유출	-	인증
C	방지	CAS	CAS알고리즘적용

V. 결론 및 향후 연구 방향

본 논문에서는 개별 네트워크 상의 사용자가 불법으로 자료를 유출하는 것을 제한하기 위하여 자료유출 제한 알고리즘을 제안하였다. 가상적으로 네트워크를 구성하여 CAS 알고리즘을 적용해 본 다면, 모든 메일은 사용자 인증을 거치므로 일차적으로 누가 메일을 보냈는지에 대한 기록이 남게 된다. 그리고 첨부된 파일은 전자우편 게이트웨이의 데이터베이스에 저장되므로 누가 불법으로 어떤 파일을 보냈는가에 대한 자료가 남게 되므로 자료유출을 방지하는데는 매우 효과적이라고 할 수 있다. 향후 연구방향은 전자우편 게이트웨이의 데이터베이스 용량 한계를 극복할 수 있는 방안을 계속 연구해야 한다. 그리고 사용자 인증 등 여러가지 절차를 거치면서 복잡성과 처리속도 문제 등 같이 계속적으로 연구가 이루어져야 할 것이다.

참 고 문 헌

[1] 중앙일보 1999.4.19
[2] 박창섭, 암호인론과 보안, 대영사, 1999
[3] 강신각, 박정수, "월드와이드 보안기술", 정보처리학회지, vol. 7, no. 2. 2000.3
[4] 이제광 외 2명, 인터넷 방화벽과 네트워크 보안, 1996
[5] 김신홍, "DBS 시스템에서 효율적인 자원관리를 위한 RRMC 구현에 관한 연구", 한국정보처리학회 논문지 제4권 제12호 1997
[6] 김경신외 2명, "스마트 카드를 이용한 유료 방송 한정 수신 시스템", 제6회 통신정보 합동학술 대회 논문집, 1996
[7] 하재철외 2명, "인증서명 키분배를 통합하는 개인정보에 기초한 암호시스템", 제6회 통신정보 합동학술 대회 논문집, 1996
[8] 김종율, "인터넷과 스마트카드 상승효과 가속", 하이테크호 61 1997
[9] 탁승호, "강좌 : IC카드 금융, 전자상거래용 IC카드", GKDLXPZM/164하이테크호, 1997
[10] 정보통신정책연구원, "향후 5년간 인증시장 규모 추정 : 1999년-2003년의 인증서비스 시장", 1999
[11] 한국전자통신연구원, "전산망 보호를 위한 방화벽 시스템", 주간기술동향, 1996

저 자 소개

金 信 洪(正會員)

1986년 2월 울산대학교 전자계산학과 졸업. 1990년 8월 인하대학교 대학원 전자계산학과 졸업. 1999년 2월 충남대학교 컴퓨터공학과 박사 수료. 1999년 2월 한국전자통신연구원 선임연구원. 1999년 3월~현재 주성대학 전임강사. 주관심분야 : 보안, 소프트웨어 엔지니어링

李 佾 濟(正會員)

2000年 3月 第37卷 TE編 第1號 參照