암호화된 웹 전화 시스템의 설계

김일민
한성대학교 컴퓨터 공학부
ikim@hansung.ac.kr

The design of an encrypted web phone system.

Ilmin Kim
Computer Engineering Dept. HanSung University

요 약

본 연구에서는 DES 알고리즘과 EDE 알고리즘을 이용한 데이터 암호화와 전자서명 기술을 접목한 인터넷 폰 보안 시스템을 구현하였다. 비밀키 알고리즘의 키 분배 문제를 해결하기 위하여 Diffie-Hellman 알고리즘을 이용한 새로운 키 분배 방법을 제안하였다. 그리고 암호화에 따른 전송지연 시간을 감소시키기 위해 DES 알고리즘의 S-Box와 P-Box를 하나의 테이블로 조합하여 운영하였다. 제안된 인터넷 폰 보안 시스템은 자바로 구현하였으며, 실험결과 DES 알고리즘을 이용할 경우 1.46초, EDE 알고리즘을 이용할 경우 3.25초의 전송지연 시간을 보였다. 제안된 시스템에서 사용된 기술들은 향후 음향제작물의 저작권 보호와 인터넷을 이용하는 데이터의 보호에 적용할 수 있을 것으로 생각된다.

1. 서 론

인터넷을 이용한 전화 서비스는 전 세계가 연결되어 있는 인터넷망을 이용해 전화 서비스를 저렴한 가격에 사용할 수 있다는 장점으로 급속히 보급되고 있다. 사람의 음성 신호를 패킷 형태로 전송한 후 이를 다시 음성 신호로 변화하는 방식으로 이루어지기 때문에 기존 전화와는 비교도 할 수 없을 만큼 저렴한 가격의 서비스가 가능하게 되어 수년 전부터 많은 인터넷 폰이 개발되었다[11]. 대부분의 인터넷폰 서비스는 개방된 상태로 네트워크 경로를 이동하고 있어 도청 또는 변조될 수 있으며 중요한 내용들이 노출되어 많은 피해를 발생시킬 수 있다. 앞으로 인터넷폰이 더욱 보편화됨에 따라 인터넷폰 보안이 절실하게 될 것이다[4,7,14].

웹 보안 기술로서 SSL(Secure Socket Layer), S-HTTP(Secure HyperText Transfer Protocol)가 대표적인 기술로 제안되었다[4,5]. SSL은 사용자의 인증을 위한 전자서명만을 제공하고 메시지에 대한 전자서명을 지원하지 않으며, 암호키의 크기를 40-bit로 제한하여 암호화에 대한 신뢰도가 상대적으로 떨어지며, 채널 자체를 암호화의 대상으로 하기 때문에 서버와 클라이언트간 정보 전달 시 부하가 크다는 단점이 있다[2, 6].

S-HTTP는 HTTP상에서 암호화 모듈을 첨가함으로써 데이터의 기밀성과 무결성을 보장하는 프로토콜이다[4]. S-HTTP는 통신을 수행하기 전에 클라이언트와 서버간에 암호화, 디지털 서명, 인증 중에서 어떤 기능만을 사용할 것인지, 암호화 알고리즘은 무엇을 사용할 것인지, 키 교환은 어떻게 할 것인지를 사용 전에 미리 결정해야 한다[2,6].

본 논문에서는 기존의 인터넷폰에서 불법도청이나 변조를 방지하기 위해 암호화 속도를 향상시킨 64비트 DES알고리즘과 EDE 알고리즘 그리고 Diffie-Hellman 알고리즘을 적용하고 인터넷 환경에서 키 분배가 안전한 인터넷폰 보안 시스템을 제안 및 구현에 대해 논하였으며 구현된 시스템의 개선된 성능에 대하여 기술한다.

2. 관련 연구

2.1 인터넷 폰 시스템

2.1.1 PC-TO-PC 방식의 인터넷 폰

최초의 인터넷폰은 PC와 PC를 연결해서 마이크와 스피커를 통해 음성을 주고 받는 방식이다. 전화통화를 원하는 두 사람이 같은 시간에 인터넷에 접속하고 동일한 프로그램을 통해 통화하는 방식으로 송신자의 PC에서 음성신호를 디지털화하고 이를 압축하여 패킷단위로 인터넷망을 통해 듣는 사람의 PC로 보내면 압축을 풀고 디지털화 된 것을 음성신호로 복원되는 방식으로 통화가 이루어진다.

2.1.2 PC-TO-Phone 방식의 인터넷 폰

PC와 전화기를 연결하는 방법으로 PC에 해당 프로그

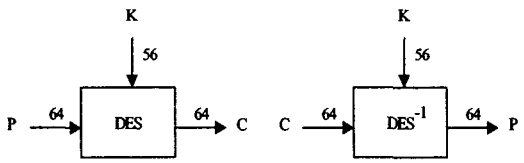
램을 설치하고 인터넷망에 접속한 후에 특정지역에 설치된 IPG(Internet Phone Gateway)라는 장비를 이용해서 전화망을 통해 상대방의 전화와 통화하는 방식이다. PC-TO-PC 방식이 인터넷방식으로 모든 것이 이루어지는 반면에 PC-TO-Phone 방식은 전화를 거는 쪽은 인터넷 방식이고 전화를 받는 쪽은 기존 전화방식으로 통화를 하는 것이다. 즉 IPG의 역할은 인터넷과 기존 전화망을 연결 시켜주는 기능을 하게 된다.

2.1.3 Phone-TO-Phone 방식의 인터넷 폰

기존 전화방식을 대체하기 위하여 PC-TO-Phone 방식의 PC쪽을 전화기로 이용할 수 있도록 전화망과 인터넷망을 연결할 수 있는 Gateway를 설치하는 방법이다. 즉 전화망-인터넷망-전화망 순서로 연결이 되어 전화통화를 할 수 있고 각 망 사이에 망 연결 및 신호감지를 할 수 있는 Gateway가 설치되면 이 방식이 구현되는 것이다[11].

2.2 DES 알고리즘

DES(Data Encryption Standard)는 (그림 1)과 같이 64-bit의 평문을 64-bit의 암호문으로 만드는 블록 암호 알고리즘으로 64-bit의 키를 사용한다. 이 64-bit의 키 중 56-bit는 실제 키가 되고 나머지는 검사용 비트로 사용된다. DES는 16 라운드의 반복적인 암호화 과정을 가지고 있으며, 각 라운드마다 전치 및 대치의 과정을 거친 평문과 56-bit의 내부 키에서 나온 48-bit의 키가 섞여 암호문을 만든다. 복호화는 암호화와 동일하나 키를 역순으로 작용시킨다.[4, 8]. 그림 1에서 P는 평문, C는 암호문, K는 키를 나타낸다.



(그림 1) DES의 기본 구조

2.3 EDE 알고리즘

DES의 약점은 암호 키가 짧다는 것이다. 최근 컴퓨터와 암호 기술이 향상되어, 짧은 키는 해커에게 공격당하기 쉽다. EDE는 암호화의 성능 향상을 위해 첫 번째 64-bit 키로 데이터를 암호화하고, 두 번째 64-bit 키로 이것을 복호화 한 다음, 세 번째 64-bit 키로 이것을 다시 암호화 하는 것이다. 이 방법은 암호화-복호화-암호화형태로 이루어지기 때문에 EDE라고 부른다[8,13].

3 새로운 인터넷 폰 시스템 설계와 구현

3.1 시스템의 전체 구성

인터넷폰 시스템을 구현하기 위하여 PC-TO-PC 방식의 인터넷폰을 자바 언어를 사용하여 구현하였으며, 음성메시지의 실시간 전송을 위해 공개키 방식에 비해 짧은 암복호화 시간을 가지는 비밀키 암호화 방식인 DES를 사용하였다.

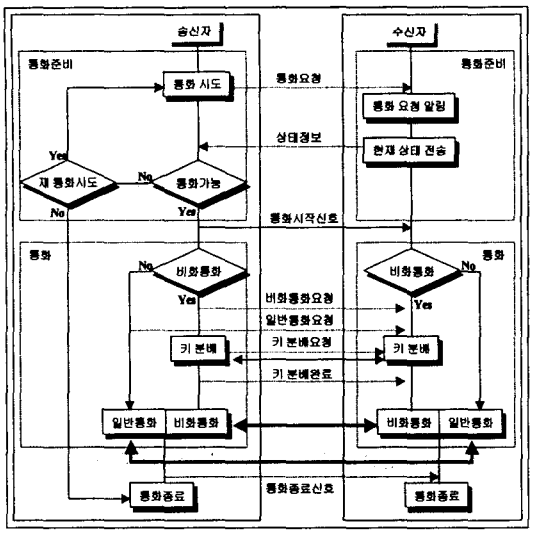
보다 높은 보안을 원하는 경우 EDE 알고리즘을 병행하여 사용할 수 있게 하였다. 비밀키를 안전하게 분배하기 위하여 Diffie-Hellman 키 분배 알고리즘을 사용하였으며 전달되는 메시지의 무결성과 위조방지, 부인방지를 위해 RSA 알고리즘과 MD5 해쉬함수를 이용한 전자서명을 사용하였다. 구현된 시스템은 LAN 환경하의 어떠한 PC에서도 간단한 설치로 안전한 통화가 가능하게 설계되었다.

키 서버는 전자서명을 위한 사용자의 RSA 공개키를 관리한다. 클라이언트에서 새롭게 생성된 RSA의 공개키를 클라이언트로부터 넘겨받아 이를 파일로 기록·보관하며, 클라이언트로부터 요청 받은 특정 사용자의 공개키를 클라이언트에 제공한다. RSA 비밀키는 클라이언트에 DES 암호 방식으로 암호화된 상태로 보관되어 안전하다.

비화통화를 위해서는 먼저 Internet Phone Server에서 통화를 원하는 사용자의 UserID와 IP주소를 획득한 후 키 서버에 전자서명을 위한 상대방의 공개키를 요청한다. 송신 모듈은 사람의 음성을 읽어서 DES 혹은 EDE 알고리즘으로 비화하고 RSA 알고리즘과 MD5 해쉬함수를 이용하여 전자 서명을 한 후 송신한다. 수신 모듈은 수신된 비화 음성 신호를 복호화한 다음, 전자서명 확인 후 출력한다.

3.2 통화순서

(그림 2)은 제안된 인터넷 폰 보안 시스템의 프로토콜을 그림으로 나타낸 것이다. 송신자는 인터넷 폰 서버를 이용하여 수신자가 통화 가능한지 점검한다. 통화가 가능하다면 통화시도를 하고, 수신자가 통화를 허락하면 송신자는 일반통화 또는 비화통화로 수신자와 통화하게 된다. 만일 비화통화일 경우는 송수신자는 키 분배 작업을 먼저 수행한다.



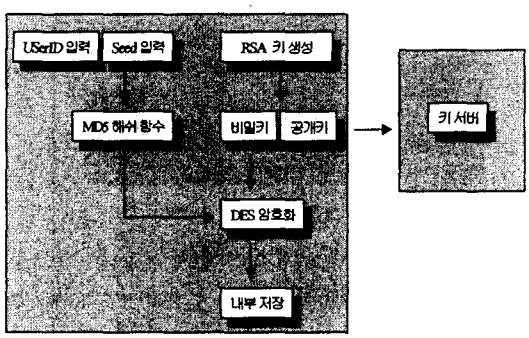
(그림 2) 제안된 시스템의 통화순서

3.3 키 관리

음성데이터를 암호화하기 위해 세 가지의 암호화 알고리즘을 사용한다. 세 가지의 암호화 알고리즘은 음성데이터를 암호화하는데 사용되는 DES, EDE 알고리즘과 전자서명을 위해 사용되는 RSA 알고리즘이다.

3.3.1 RSA 키 관리

전자서명을 위한 RSA 키는 사용자가 인터넷폰 서버에 등록할 때 생성하게 되며, 사용자가 필요시 다시 생성할 수 있다. (그림 3)은 RSA 키의 생성과정을 설명하고 있다.



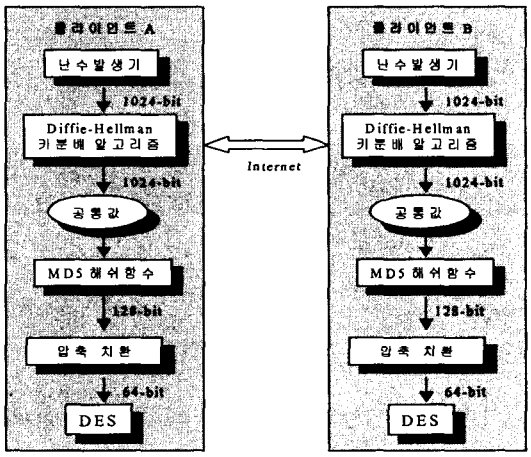
(그림 3) RSA 키의 생성

512-bit 크기의 RSA 비밀키와 공개키는 자바의 SecureRandom 클래스를 이용하여 생성된다. 그 중에 공개키는 키 서버의 공개키를 모아두는 파일에 저장되고 비밀키는 사용자가 입력한 Seed로부터 MD5 해쉬함수를 통해 생성된 64-bit 키를 사용하여 DES 암호 방식으로 암호화 한 후 클라이언트에 저장된다. 이때 Seed의 길이는 제한이 없으며 비밀키는 암호화되어 클라이언트에 저장되므로 외부로 노출될 가능성을 최소화하였다.

클라이언트와 키 서버간의 통신에서는 높은 신뢰성이 요구되므로 신뢰성이 높은 point-to-point 통신을 지원하며 패킷손실을 방지하는 자바의 TCP방식인 Socket 클래스를 사용하였다.

3.3.2 DES와 EDE 키 관리

음성 데이터의 암호화에 사용되는 64-bit DES 키는 필요시 자동으로 생성되었다가 통화가 끝남과 동시에 소멸된다. 즉, 새로운 통화가 시작될 때마다 새롭게 키가 생성됨으로 보다 안전한 통화가 가능해진다. (그림 4)는 시스템의 키 생성과정을 설명하고 있다. 난수 발생기는 JCE(Java Cryptography Extension)에 포함된 SecureRandom 클래스를 사용하여 1024-bit 크기의 난수를 생성한다.



(그림 4) DES 키의 생성

보다 높은 비도를 위해 사용된 EDE 알고리즘에 필요한 세 개의 키는 위의 과정을 세 번 반복하여 세 개의 64-bit 키를 생성하여 사용한다. 키 생성 부분은 모든 과정이 클라이언트 측의 어플리케이션에서 이루어지며 키 서버와 인터넷폰 서버와는 어떠한 정보도 교환하지 않으므로 보다 안전한 키 관리가 가능하다.

3.4 비문 송수신

비문 송수신은 양방향(Full duplex) 전송을 지원해야 하기 때문에 송신용 스레드와 수신용 스레드가 동시에 수행된다. 송신 스레드는 음성 데이터를 44096-bit 단위로 캡쳐하여 전자 서명을 한다. 전자서명 한 음성 데이

터는 DES 또는 EDE 알고리즘을 이용하여 암호화되어 전송된다. 수신 스레드는 암호문을 수신하여 복호하고 전자서명을 확인 후 음성 데이터를 출력한다. 음성 데이터의 암/복호화와 송수신은 모든 루틴이 클라이언트에서 이루어지며, 이는 클라이언트에서 음성 데이터가 완벽하게 암호화 된 상태에서 전송되어 패킷이 경유하는 어떠한 곳에서도 도청되는 것을 방지하기 위함이다.

메시지의 무결성을 보장하기 위한 인증과 송신부인 방지를 위한 전자 서명 기능을 가지기 위해서는 RSA 알고리즘과 MD5 해쉬 함수가 사용된다. 전자서명 과정은 먼저 원문을 해쉬 함수를 이용하여 128-bit로 축약한다. 그리고 축약문을 송신자의 비밀키로 암호화 한 후 원문에 추가하여 전송하게된다.

수신 측에서는 첨가된 축약문을 분리한 후 이것을 송신자의 공개키로 복호화 한다. 그리고 수신한 원문을 해쉬함수를 이용하여 128-bit로 축약해 복호화한 축약문과 비교하여 중간 변조 여부와 정당한 송신자가 보낸 것인지를 확인할 수 있다[3].

3.5 시스템 구현

(그림 5)는 본 시스템을 구현하기 위하여 사용된 도구 및 테스트를 위한 동작환경을 나타내었다. 인터넷폰 서버와 키 서버는 편의상 실험실에서 운영되는 서버(optosys.kmu.ac.kr)를 사용하였다.

- 개 발 도 구 : JDK 1.2.2, JMF 1.2
- 테스트 환경
  - 클라이언트
    - 기종 - Intel PentiumIII 450Mhz
    - OS - Windows 98
  - 키 서버 : optosys.kmu.ac.kr
    - 기종 - Pentium MMX 160MHz
    - OS - Windows NT Server 4.0
  - 인터넷폰 서버 : optosys.kmu.ac.kr
    - 기종 - Pentium MMX 160MHz
    - OS - 윈도우NT Server 4.0

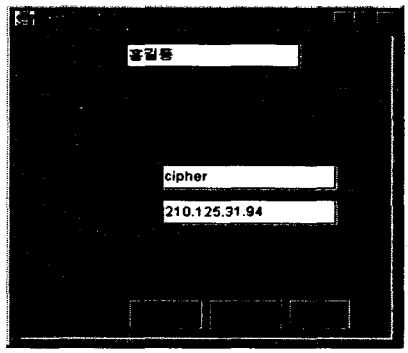
(그림 5) 개발 및 테스트 환경

4 시스템의 구현 결과와 평가

4.1 시스템의 구현결과

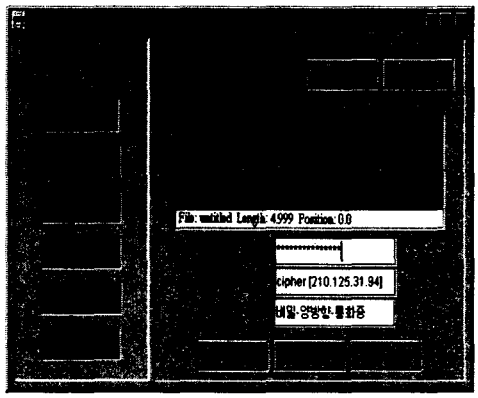
개발된 인터넷폰 보안 시스템은 Intel Pentium 450MHz, 64M 메모리의 두 대의 PC상에서 실험되어졌다. 암호 통신을 하기 위해서는 먼저 새로운 사용자에 대한 RSA 키를 생성해 키 서버와 인터넷폰 소프트웨어에 등록하는 작업을 거쳐야 한다.

RSA키 발생화면에서 사용자의 이름과 사용자 ID 그리고 Seed 값을 입력 후 "키생성" 버튼을 누르면 새로운 RSA 키가 생성된다. 이때 사용자 ID는 각 개인의 키를 식별할 목적으로 사용되므로 유일해야 한다. 키 생성 후 "키저장" 버튼을 누르면 생성된 RSA 공개키는 키 서버에 저장되어 사용자의 요청이 있으면 특정 사용자의 공개키를 제공해준다. RSA 비밀키는 입력된 Seed 값을 이용하여 생성된 값을 암호 키로 사용하여 암호화된 후 사용자의 프로그램 상에 저장된다. (그림 6)은 인터넷폰 사용자가 통화를 시작하기 위해 수신자의 전화번호를 검색하는 화면이다.



(그림 6) 전화번호 검색 화면

(그림 7)은 정당한 사용자가 자신의 Seed 값을 입력 후 전화번호 검색을 이용하여 검색 된 "cipher" 라는 사용자와 통화하는 화면이다.



(그림 7) 본 시스템을 이용한 통화

정당한 사용자의 Seed 값을 입력 후 "전화통화" 버튼을 누르면 수신자의 인터넷폰 보안 시스템에 통화요청을 알리는 벨이 울린다. 수신자의 통화허락으로 일반통화가

시작되며 비화통화를 원할 때 "비밀통화" 또는 "극비통화" 버튼을 누르면 먼저 내부적으로 키 분배 알고리즘에 의해 수신자와 공통값을 교환하게 된다. 교환된 공통값은 암복호화 키로 만들어져 비화통화에 사용된다. 통화의 보안 정도에 따라 비밀통화와 극비통화를 구분하여 사용할 수 있게 구현함으로서 암호화에 의한 전송지연시간을 줄이며 용도에 맞는 통화를 가능하게 하였다.

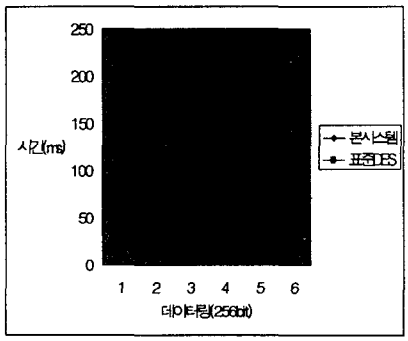
<표 1>은 각 통화별 사용된 암호화 알고리즘과 전송지연시간을 나타내었다. 전송지연시간은 암호화 시간과 전송시간 그리고 복호화 시간을 포함한다.

<표 2 > 통화 단계별 특징

특징 / 통화구분	암호 알고리즘	전송지연 시간	비도
일반통화	없음	0.62초	낮음
비밀통화	DES	1.46초	보통
극비통화	EDE	3.25초	높음

4.2 인터넷 폰 보안 시스템의 평가

개발된 시스템을 평가하기 위해 기존제품과의 비교와 비도 그리고 암호화 속도 측면을 고려하였다. 음성 데이터를 암호화하는데 사용한 64-bit의 DES 키는 8-bit의 패리티 비트를 제외하면 72×10^{15} 개의 키를 생성 할 수 있다. 이것은 하나의 키를 검사하는데 1㎲이 걸리는 시스템을 사용한다면 적용된 비밀키를 알아내는 데에는 약 1000년이 걸리게 된다. 또한 통화내용의 중요도에 따라 EDE 알고리즘을 사용할 경우 비도는 DES의 9.17 배가 된다[8]. (그림 8)은 인터넷 폰 보안 시스템에서의 개선된 DES와 표준 DES의 암호화 속도를 Pentium III 450MHz의 PC에서 자바 Date 클래스를 이용하여 측정하였다.



(그림 8) 암호화 속도의 비교

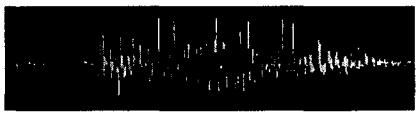
개선된 DES 알고리즘은 표준 DES의 확장순환, S-box, P-box를 조합하여 하나의 테이블 만듦으로써 데이터량의 증가에 비례해 암호화 속도가 뚜렷하게 차이 난다. <표 2>는 현재 개발되어 있는 인터넷폰 시스템과 본 암호 시스템을 비교한 것이다.

<표 3> 주요 인터넷폰과의 비교

특징 / 제품명	PC2 PC	PC2 폰	폰2 폰	전화 번호	프로토콜	인증 / 비화
본 시스템	O	×	×	IP주소	UDP	O
다이얼 패드	O	O	×	IP주소	UDP	×
Net2 Phone	×	O	O	E-mail 주소	TCP	×
DigiPhone	O	×	×	IP주소	UDP	×

현재 개발되어 있는 인터넷폰 시스템 중 Third Planet 사의 DigiPhone은 인증 서비스를 제공하고 있으며, Net Speak사의 Web Phone이 암호화를 제공 하지만 암호화에 사용되는 키가 통화자간에 고정되어 있어 키가 노출되었을 경우 많은 위험이 따르며 키를 바꾸기 위해서는 키를 구두나 다른 안전한 방법으로 교환하여야 한다.

본 시스템에서는 Diffie-Hellman 알고리즘을 이용하여 매 통화 시 새로운 키를 생성하여 보다 안전한 통화를 보장하며 PC-TO-PC방식을 지원함으로써 별도의 사용료 없이 인터넷에 연결된 PC에서 간단한 소프트웨어의 설치로 안전한 통화가 가능하다. 하지만 본 시스템은 통화 시 음질이 네트웍의 전송속도에 많은 영향을 받으며, 통화하고자 하는 사람의 PC에 같은 소프트웨어가 설치되어야 하며, 온라인 상태에 있어야 한다는 단점이 있다. (그림 9)는 개발된 시스템의 음성 출력을 측정한 화면이다.



a) 원문 음성신호

b) 비화 된 음성신호

c) 다른 키로 복호한 음성신호

d) 전자서명 확인이 되지 않은 음성신호

e) 정상적으로 복호된 음성신호

(그림 9) 인터넷폰 보안 시스템의 출력

5. 결 론

본 논문에서는 음성 데이터의 단계별 암호화를 이용하여 암호화된 음성데이터를 인터넷을 통해 전달하는 PC-TO-PC 방식의 인터넷폰 보안 시스템을 구현하였다. 통화 내용의 기밀성을 보장하기 위한 방법으로 DES 알고리즘을 사용하였으며, 보다 높은 보안을 유지하기 위해 EDE 알고리즘을 병행하여 사용하였다.

또한 음성데이터의 실시간 전송을 위해 빠른 암/복호화 시간이 요구되는데, 이를 위해 DES의 S-Box와 P-Box를 하나의 테이블로 통합하는 방법을 사용하였다. 제안된 시스템은 기존의 기술들이 보안을 고려하지 않고 전송지연 시간과 음질에 중점을 두고 있는데 비해 빠른 속도로 음성 데이터를 암호화함으로서 통화내용의 보호와 더불어 전송지연 시간의 증가를 막았다. 또한 기존의 암호화를 제공하는 인터넷폰 시스템의 키 분배 문제를 해결함으로써 어떠한 장소에서도 간단하게 시스템을 설치해 안전한 통화를 손쉽게 할 수 있으며, 새로운 통화를 시작할 때는 항상 새로운 키를 사용함으로써 통화의 비도를 증가시켰다.

본 논문에서 제안된 시스템에서 EDE 알고리즘을 이용하는 경우, 속도 향상을 위한 연구가 앞으로 수행되어져야 할 것이다. 현재 시스템은 PC-TO-PC 방식의 인터넷폰 서비스의 보안을 목적으로 하고 있으나 향후 다른 방식의 인터넷폰 서비스와 일반 전화기 또는 인터넷 팩스에 보안 기능에 적극 활용 될 수 있을 것으로 사료된다.

참고문헌

[1] 강신각, 박정수. "월드 와이드 웹(WWW) 보안기술". 정보처리 제7권 제2호, pp. 41-47, 2000. 3.

[2] R. Stinson,D., *Cryptography : Theory and Practice*. CRC Press, 1995.

[3] 박동욱. 박재희, 김진상, 김일민. "PGP 방식을 이용한 웹 기반 전자우편 보안 시스템". 한국 정보 처리 학회 논문지 제8-C권, pp16-22, 2001.

[4] 박창섭. 「암호이론과 보안」. 대영사, 1999.

[5] 송상헌, 박정수, 강신각, 김재명, 안은미, 류재철. "웹 보안을 위한 사용자 인증과 암호화 통신 구현.". 제7회 통신정보합동학술회의, 1997.

[6] 이은성, 박현동, 류재철. "안전한 WWW통신을 위한 NetCrypt 설계." 「한국통신 정보보호 학회 종합학술발표회논문집」, pp.191-200, 1998.

[7] 장윤희, 박선종. 「인터넷 보안 가이드」. 위저드, 1998.

[8] Schneier,B., *Applied Cryptography : Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, Inc., 1994.

[9] 최완용. "음성 DSP칩을 이용한 패킷 음성 통신의 구현". 한남대학교 석사 학위 논문, 1996.

[10] 충남대학교 정보보호연구실. "Pretty Good Privacy". http://espresosun.chungnam.ac.kr/~hdpark/PGP/signature.html, 1998.

[11] 한국전산원. "A Study on the Internet Telephony and Internet TV Standatds". 1999.

[12] 한국전자통신연구원. 「암호학의 기초」. 경문사, 1999.

[13] Biham,E., Shamir,A., "Differential Cryptanalysis of DES-like Cryptosystems". Journal of Cryptology, vol.4, no.1, pp.3-72, 1997.

[14] Siyank,K., Hare,C., *Internet Firewalls and Network Security*. New Riders, Publishing, 1995.