인터넷 보안을 위한 암호체계

양 종 원* 조 내 현** 채 종 수** 서 창 호***

◈ 목 차 ◈

1. 서 론*

고도로 발달된 인터넷 환경이 첨단 정보사회 구현의 중요한 인프라로서 생활의 편의성을 제공하고 있는 반면, 누구나 쉽게 접근할 수 있는 개방형 환경으로 인해 악의적인 해킹, 바이러스 유포, 지적재산권의 침해, 사이버 범죄 등과 같은 역기능적인 측면이 발생하고 있는 것이 현실이다.

또한 인터넷 보안환경에 전자서명, 키관리 및 인증서비스가 매우 중요하게 부상하고 있으며, 여기에 적용하기 위한 정보보호 기반기술인 암호화 기술, 인증기술, 전자서명, PKI(Public Key Infrastructure) 등이 구축되어 있는 상태이다.

암호화 기술은 합법적 참여자들 간에 메시지 변/복조 규칙에 대한 약속을 정하고, 이 규칙에 따라 송신하려는 메시지를 변조(암호화)시켜 전달 혹은 보관하며, 메시지 수신시 또는 접근 권한이 있는 사람이 필요에 따라 이를 복조(복호화)하도록 하는 기술을 말한다. 인증기술은 어떤 사실을 증명하거나 확인하기 위해 사용되는 기능으로서 전자상거래의 경우 인증 서비스의 목표는 안전한 전자상거래의 보장, 개인 및 기업의 비밀보장, 거래 사실에 대한 증명 등을 위한 것이다.

* 공주대학교 바이오정보학과(정보보호전공) 박사수료
** 공주대학교 군사과학정보학과 박사과정
*** 공주대학교 바이오정보학과 부교수
공주대학교 군사과학정보학과 부교수
chsseo@kongju.ac.kr

본 논문에서는 인터넷 보안을 위한 암호 체계를 통해 사회적으로 사이버 공간에서의 활동증가를 알아본다. 또한 개인 프라이버시 보장 그리고 정보 범죄의 차단 등을 위해 독자적 침해사고 대응환경, 상호 협력관계 유지 및 국가의 중요한 정보기반 구조를 보호하기 위해 필수적으로 인터넷 환경에서 암호체계 구축에 대한 전반적인 것을 알아본다.

본 논문의 구성은, 2장에서 관련연구에 대해 설명하며, 3장에서는 인터넷 보안을 위한 암호체계를 설명하고, 마지막으로 4장에서 결론을 맺는다.

2. 관련연구

2.1 미래인터넷 구조 및 새로운 패러다임

미래인터넷 연구의 가장 큰 핵심은 새로운 인터넷을 위한 구조를 제안하는 것이다. 1970년대 설계된 TCP/IP 프로토콜, IP 어드레싱/라우팅, 패킷 스위칭 기술들로 대변되는 현 인터넷 구조는 미래인터넷을 위한 새로운 패러다임에 의해 재설계되어야 한다. 현재 Clean Slate 설계방법에 따른 미래인터넷의 구조 및 새로운 패러다임 연구 분야는 다음과 같다[1].

- 플로 기반 라우팅/스위칭
- 새로운 네트워크 어드레싱/라우팅
- 동적 서킷 스위칭(Dynamic Circuit Switching)
- 백본 재설계
- 점대점 모델의 재설계

- 크로스-계층 설계(Cross-Layer Design)
- 네트워크 가상화
- 새로운 보안구조의 설계

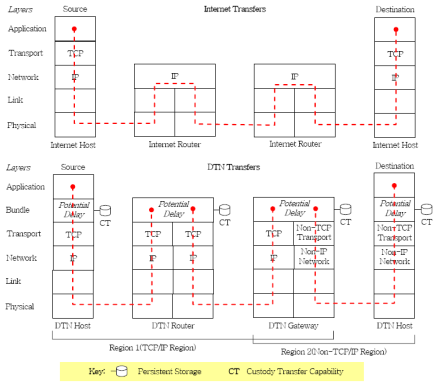
현재 진행되고 있는 대표적인 연구들만 살펴보면, 최근 IETF[2], IRTF[3]를 중심으로 인터넷상의 가장 큰 문제인 라우팅과 어드레싱의 확장성을 높이는 연구가 진행되고 있다. 이동성, 멀티호밍, PI 라우팅 등의 증가로 인한 라우팅 테이블 엔트리의 증가는 현재 인터넷에서 가장 시급히 개선되어야 할 문제 중 하나로 인식되고 있다. 이러한 문제는 현재 사용되는 IP 어드레스에 식별자(ID: Identifier)와 로케이터(Locator) 기능이 함께 사용되기 때문이며, 이를 해결하기 위해 현재 어드레스 개념에서 ID와 로케이터를 분리하거나, 혹은 ID를 근본적으로 다시설계하려는 연구가 진행중에 있다. ID/Locator 분리 작업에 대한 연구 및 표준화는 IETF RoAP BoF 등을 통해 추진중에 있다. 현재 제안된 솔루션으로는 호스트-기반 방식과 네트워크-기반 방식으로 나누어 분류되며, 대표적으로 LISP, PASH, HIP, SHIM6 방법 등이 연구되고 있다. 이러한 솔루션들은 현 인터넷 구조에 일부 호환(backward-compatibility)을 고려하여 제안된 보다 현실적인 방식들이다. 이 와 동시에 IRTF RRG에서는 Clean Slate 접근 방식에 따른 새로운 구조 등도 함께 연구되고 있다[4].

현 인터넷의 패킷 스위칭 기술은 네트워크 계층상에서 비상태보존(stateless) 라우팅 시스템의 구현을 가능하게 했으며, 이를 통해 라우터는 별도의 연결 상태를 유지하지 않는다는 장점을 가지고 있었다. 이러한 순수 패킷 스위칭 방식은 액세스 단에서는 아직도 올바른 방법으로 인식되고 있으나, 코어단으로 갈수록 서비스 품질 제어나 트래픽 엔지니어링, 패킷의 그룹핑을 처리하는 데 있어 많은 제약을 가져왔다. 이를 해결하기 위해 모든 경로의 광-기반 스위칭의 도입 혹은 동적 서킷 스위칭에 대한 연구도 함께 진행중에 있다[5].

또 다른 미래인터넷의 새로운 패러다임 중 하나는 프로그램-가능 네트워크의 적용이다. 초기 인터넷 장비들은 각 기능들이 정적인 형태로 구현되어 사용되어 왔으나, 미래인터넷의 장비들은 새로운 프로토콜이나 서비스들을 프로그램하여 네트워크 상에 플러그-인 형태로 추가, 확장할 수 있도록 하는 연구가 진행중에 있다. 이러한 연구는 예전 능동 네트워크(active network) 혹은 최근 개념 등과 함께 활발히 연구가 진행되고 있다.

마지막으로 DTN에 대한 개념은 현재 인터넷 환경하에서는 상시 연결성(always-on)만을 고려할

때 제공하기 어려운 간헐적, 확률적 연결(intermittent/ opportunistic connection), 장시간 지연 등의 응용 등을 처리하는 데 획기적인 아이디어로 고려되고 있다. 초기 DTN은 ISOC의 IPN 프로젝트내 행성간 연결성 지원을 위해 설계된 것이었으나, 최근 무선/이동 센서 등의 등장으로 인해 그 용도가 크게 중요시 되고 있다. 기본 개념은 TCP/IP 점대점 모델 대신 번들(bundle) 프로토콜을 기반으로 하는 메시지-기반 오버레이 방식의 전송 모델을 사용하는 것으로, DTN의 장점은 TCP/IP가 아닌 다른 네트워크/수송계층 프로토콜을 사용하는 어느 단말 사이에서도 비동기(asynchronous) 형태로 통신이 가능하게 할 수 있다는 데 있다. (그림 2)는 기존 TCP/IP 라우팅과 DTN 라우팅의 차이를 나타낸 것이다[6].



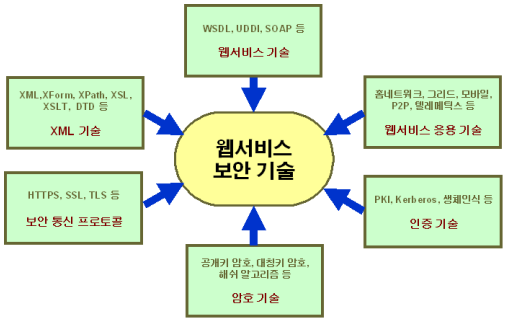
(그림 1) TCP/IP 라우팅과 DTN 라우팅 비교

2.2 웹서비스 보안기술

웹서비스 보안기술은 기술 특성에 따라 XML 정보보호 기술, 웹서비스 보안 프레임워크 기술, 웹서비스 응용보안 기술로 구분되며, XML 정보보호 기술은 XML 기반 서비스나 시스템을 위한 보안 기반 기술로

인증, 인가, 기밀성, 무결성, 부인봉쇄 등의 보안서비스 및 보안정보 관리 기능을 제공하며, 세부기술로는 XML 전자서명 및 암호화 기술, XML 기반 보안정보 교환기술, XML 기반 접근제어기술, XML 기반 공개키 관리기술 등이 있다.

웹서비스 보안 프레임워크 기술은 XML 정보보호 기술을 기반으로 웹서비스에서 안전하게 정보를 교환하고 자동화된 방법으로 상호의 보안 정책을 처리하여, 안전하고 통합된 비즈니스를 가능하게 하며, 세부기술로는 통신보안 기술, 보안정책 기술, 프라이버시 보호 기술, 보안세션 관리 기술, 신뢰관리 기술 등이 있다.



(그림 2) 웹서비스 보안 연관기술 관계도

3. 인터넷 보안을 위한 암호체계

현 인터넷의 시초가 된 1969년 미 국방성 주도의 ARPANet이란 대규모시험 네트워크 선행 도입, 1990년대 이를 NSF 주도의 NSFNet 학술연구망으로 발전시켜 기 개발된 각종 프로토콜/응용들을 시험적으로 운용, 단계별로 발전시킴으로써 현재의 글로벌 인터넷 구조를 가능하게 했다는 점이며, 1993년 사용자 응용의 혁명을 가져온 WWW이 개발된 후, TCP/IP 응용이 글로벌 네트워크의 사용자 환경을 통합하는 대표적인 수단으로 자리잡게 된 점을 들 수 있다. 사실 1990년대 초반까지만 해도 각 나라별로는 OSI 7계층 모델에 따라 GOSIP라는 실행표준에 의해 정보 네트워크를 OSI로 구축하려는 시도가 있었으나[7], 현재는 "네트워크"라고 하면 "인터넷"만을 언급한 정도로 현 인터넷은 가파른 성공과 성장세를 유지하고 있다.

처음 인터넷이 제안될 당시 설계 목표와 요구사항은 다음과 같이 7가지로 정리된다[8],[9].

- 네트워크간 연결
- 생존성(Survivability)
- 다중 유형의 서비스 지원
- 다양의 물리계층의 지원
- 분산 관리 허용
- 비용 절감(Cost-Effective)
- 자원 책임(Resource Accountability) 허용

이러한 목표 및 요구사항을 만족하기 위해 현 인터넷은 다음과 같은 5가지 설계철학을 가지고 구현되었다.

- 계층화(Layering)
- 패킷 스위칭
- 네트워크의 네트워크
- 네트워크의 단순화 및 단말의 지능화
- 점대점 통신(End-to-End Argument)

이러한 현 인터넷의 설계철학은 네트워크와 이를 구현하는 프로토콜들을 단순화시켜 다양하고 복잡한 네트워크와 네트워크간의 연결을 더욱 간편하게 하였고 인터넷 발전의 원동력으로 인식되어 왔다.

특히 계층화, 패킷 스위칭, 네트워크의 단순화의 개념은 새로운 프로토콜 설계시 결코 버려서는 안될 인터넷의 가장 중요한 핵심철학으로 자리잡게 되었다. 그러나, 현 인터넷 주변의 환경은 다음과 같이초기 인터넷이 설계되었을 때는 상당히 다른 모습으로 변화되어 발전되어 왔으며[10],

- 통신환경: 신뢰 → 비신뢰
- 사용자환경: 전문연구 집단 → 일반 소비자
- 망사업자: 비영리 → 영리
- 통신주체: 호스트-중심 → 데이터-중심
- 연결성: 점대점 연결 → 간헐적 연결

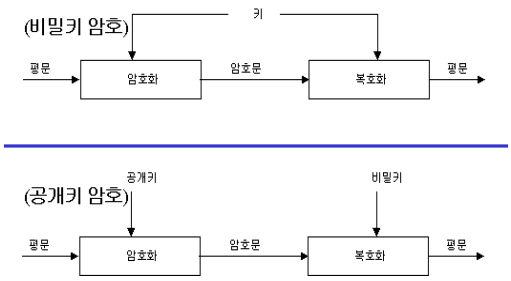
특히 2000년에 들어서면서부터 센서와 같은 다량의 단말 접속, 다양한 무선구간의 확장, 다중인터페이스 단말의 등장, 빠른 이동단말의 지원, 안전한 전자거래, 네트워크에서의 서비스 품질보장, 비즈니스 측면 보완 등 현 인터넷 기술에 대한 문제 제기 및 이를 보완, 대체하기 위한 다양한 연구들이 진행되어 왔다. 특히 정보보호에 대한 관심은 최근에 매우 중요하게 여기게 되었으며, 정보보호 중에서도 암호에 대한 체계는 미래인터넷기술 뿐만 아니라, 현 인터넷 환경에서도 중요한 역할을 수행을 하고 있다.

3.1 인터넷 환경에서의 암호의 중요성

(표 1) 암호의 기능

인증식별	정보의 송·수신 또는 정보시스템의 신원을 확인하는 것으로 패스워드 방식에 비해 안정성이 높은 방식으로 공개키 방식에 기반한 인증방식.
무결성과 전자서명	전송 또는 보관중인 정보를 비인가자가 인가되지 않은 방법으로 위·변조할 수 없도록 보호하는 것으로 전자 서명방식 사용.
부인방지	사용자가 정보를 송·수신하거나 시스템을 처리한 사실을 나중에 부인하지 못하게 하는것.

인터넷은 그 특성상 Open시스템일 수 밖에 없으며, 또한 이로 인하여 해킹·바이러스, 정보유출 등 사이버 범죄나 개인정보 유출 등에 취약한 구조를 지니고 있다. 인터넷상에서의 전자거래 혹은 e-Mail 등에는 타인의 해킹·도용 등으로부터 자신을 보호하는 수단으로 암호화기술이 각광받고 있으며, 암호의 기능인 인증식별, 무결성과 전자서명, 그리고 부인방지 등은 선택이 아니라 필수가 되어가고 있다[표 1].



(그림 3) 대칭키 및 공개키 방식

3.1.1 암호화 알고리듬

① 대칭키 암호화

대칭키 암호 알고리듬은 비밀키 암호 알고리듬 혹은 단일키 암호 알고리듬이라고 불리기도 하는데 이 방식은 송·수신자가 동일한 키에 의해 암호화 및 복호화 과정을 수행하며, 암호화하는 데이터를 변환하는 방법에 따라 블록 암호 알고리듬과 스트림 암호 알고리듬을 분류한다. 대표적으로 DES, 3DES, AES 등이 사용한다.

② 공개키 암호화

공개키 암호 알고리즘을 사용하는 시스템은 암·복호화에 사용되는 키셋(Key Set)을 다르게 생성 ,배포 및 관리함으로 높은 수준의 보안유지가 가능하다. 공개키 암호 시스템은 두 개의 키셋을 생성하여 그중 하나를 공개하고(Public Key), 나머지 하나는 비밀키로 자신이 보관하여(Private Key) 사용하는 암호 시스템 방식이다. 따라서 공개키 암호 시스템의 사용자는 오직 자신의 비밀키만 보관하면 되므로 대칭키 암호 시스템에 비해 적은 수의 키로 시스템 유지가 가능하며, 또한 공개키 암호 시스템은 전자 서명을 사용하는데 상대적으로 효율적이고 간단한 시스템 구축이 가능하다. 대표적으로 복잡한 인수분해 기법을 적용한 RSA(Rivest-Shamir-Adleman)와 이산대수의 난해성을 기반을 둔 ECC(Elliptic Curve Cryptosystem)이 많이 활용되고 있다.

3.1.2 TLS & PGP

TLS(Transport Layer Security) 는 웹 트랜젝션 보안용으로 널리 사용되고 있는 SSL(Secure Session Layer)을 IETF에서 표준화시킨 것으로 TCP상의 응용 프로토콜에 대한 암호화나 무결성 등의 보안서비스를 제공해 주는 Client-Server 모델의 보안 프로토콜이다. SSL은 서버와 클라이언트 간에 인증(Certification)으로 RSA방식과 X.509를 사용하고, 실제 암호화된 정보는 새로운 암호화 소켓채널을 통해 전송하는 방식이다. SSL은 특히 네트워크 계층의 암호화 방식이기 때문에 HTTP 뿐만 아니라 NNTP, FTP등에도 사용할 수 있는 장점이 있다. SSL은 기본적으로 신분확인(Authentication), 암호화, 그리고 메시지의 무결성을 보장해 주며, 이는 인터넷간의 채널을 통해 비밀 보장 서비스 제공한다.

PGP(Pretty Good Privacy)나 S/MIME은 주로 E-mail 보안용으로 널리 사용되는 응용 계층 보안 프로토콜로 메시지에 대한 암호화나 인증, 서명 등의 기능을 제공한다. 특히 PGP는 Web of Trust 형의 분산구조 공개키 인증 방식을 택해 별도의 공개키 기반구조 없이도 동작한다는 잇점으로 가장 널리 사용되는 응용 보안 프로토콜이다.

3.2 네트워크 보안을 위한 암호체계

네트워크 시스템은 일반적인 컴퓨터 시스템과 비교하여 보다 복잡한 시스템이라고 간주할 수 있다. 따라서 운영체제에 적용되는 대다수의 보안 개념과 보안 통제들은 네트워크 시스템에도 그대로 적용될 수 있다. 네트워크 시스템에서 제공되는 기본적인 정보 보안 서비스로는 인증, 접근 통제 비밀 보장, 무결성, 부인 방지 등을 들 수 있다. 네트워크 보안이란 네트워크에 연결된 컴퓨터 시스템의 운영 체제, 서버, 응용 프로그램 등의 취약점을 이용한 침입을 방지하는 것이다. 일반적으로 네트워크 보안을 위해서 방화벽을 주로 사용한다.

또한, 네트워크 보안 요구사항으로 비밀성 유지 및 보장, 무결성의 유지 및 보장, 데이터 발신처 처리 및 가용성 확인 그 외 통신 사실의 부인 방지, 사용자 신분 확인 및 인증, 인가된 접근의 허용 등이 있다.

3.2.1 암호화

암호화는 프라이버시, 인증, 무결성 및 데이터에 대한 제한적 접근을 제공하는 강력한 수단이다. 네트워크 환경에서 암호화는 두 개의 호스트간에, 혹은 두 개의 응용 시스템간에 적용될 수 있다.

① 링크 암호화

링크 암호화(link encryption)는 물리적인 통신 회선으로 전달되기 바로 직전에 데이터를 암호화한다. 즉, 링크 암호화는 OSI 참조 모델의 제 1계층(물리계층) 혹은 제 2계층(데이터 링크 계층)에서 이루어진다. 복호화는 통신 데이터가 수신 컴퓨터에 들어가는 시점에서 이루어진다. 따라서 데이터는 두 개의 컴퓨터간에 전송되는 동안에는 암호화에 의해 보호되지만, 호스트 상에서는 평문으로 존재한다. 링크 암호화는 사용자에게 투명하다. 링크 암호화는 하위 계층의 네트워크 프로토콜에 의해 수행되는 전송 서비스가 된다. 링크 암호화는 특히 통신 회선이 취약할 때 적합하다.

②단대단 암호화

단대단 암호화(end-to-end encryption)는 OSI 참조 모델의 가장 높은 계층, 즉 제 7계층(응용계층)이나 제 6계층(표현 계층)에서 사용자에 의해 수행된다. 단대단 암호화는 사용자와 호스트간에서 하드에어에 의해 이루어질 수도 있으며, 호스트 컴퓨터에서 수행되는 소프트웨어에 의해서도 이루어질 수 있다.

단대단 암호화는 모든 라우팅과 전송 처리에 앞서 암호화가 이루어지기 때문에, 메시지는 암호형태로서 네트워크를 통하여 전달한다. 만약 네트워크에서 보안 유지에 실패하여 데이터가 노출된다 하여도, 데이터의 비밀성은 위협을 받지 않는다.

3.2.2 전자 서명

전자 서명은 데이터에 대한 서명과 서명된 데이터에 대한 검증의 절차로서 정의된다. 서명은 서명자의 비밀 정보인 공개 키 암호 알고리즘의 비밀 키를 사용함으로써 데이터의 암호화 및 검사값을 생성하는 과정이며, 검증은 서명자의 공개 정보를 사용하여 정보를 보낸 사람이 누구인지를 알아내는 과정이다.

전자 서명 메커니즘의 본질적인 특성은 비밀 키의 소유자가 아니면 어느 누구도 서명된 데이터를 생성할 수 없어야 한다. 또한 서명자는 그 데이터에 서명하고 송신했음을 부인할 수 없어야 하고, 데이터를 받은 사람은 서명된 데이터를 변조 및 위조할 수 없어야 한다.

3.2.3 접근제어

접근 통제는 사용자의 접근 권한을 결정하거나 사용자에게 접근 권한을 부여하기 위하여 사용자의 고유성, 사용자에 관한 정보 또는 사용자의 자격 등을 이용한다. 만약 사용자가 비인가된 자원에 대하여 접근을 시도하거나 인가된 자원일지라도 불법적인 방법으로 접근하고자 한다면 접근 통제 기능은 그러한 접근 시도를 거부하여야 한다.

접근 통제 메커니즘은 통신의 종단 지점이나 중간 지점에서 적용될 수 있다. 통신의 발신이나 중간 지점에서 적용된 접근 통제는 송신자가 수신자와 통신하기 위하여 인증되어야 하는지, 또는 요구된 통신 자원을 사용하기 위하여 인증되어야 하는지를 결정하기 위해 사용된다.

3.2.4 데이터 무결성

데이터 무결성은 네트워크 상에서 데이터의 정확성을 점검하는 메커니즘으로 송신자와 수신자가 각각 무결성을 결정하게 된다. 송신자는 데이터 자체에 대한 특정 값을 계산하여 무결성 기능을 제공하는데, 이에는 주로 DES를 이용한 메시지 인증 코드와 조작 점검 코드(MDC: Manipulation Detection Code)등이 사용된다. 수신자는 수신한 데이터와 관계가 있는 무결성 정보를 발생시켜 수신한 무결성 정보와 비교하여 데이터의 변경 여부를 결정한다.

그러나 이러한 방식으로는 데이터의 재사용을 방지할 수는 없다. 접속형 데이터 전송의 경우는 데이터의 순서 무결성을 제공하기 위하여 데이터 단위의 순서 번호와 타임스탬프 등과 같은 부가적 기능을 사용할 수 있으며, 비접속형 데이터 전송의 경우는 각 데이터의 재사용을 막기 위하여 타임스탬프를 사용할 수 있다.

4. 결론 및 향후 연구

1974년 인터넷 개념이 처음 제안된 이후, 급격한 통신환경의 변화 및 다양한 사용자 요구사항의 증대로 인해 현재 인터넷이 갖는 근본적인 보안에 대해 심각한 고민이 발생하고 있다. 특히, 전자상거래의 증가 및 글로벌한 인터넷 환경에서 불특정 다수에게 막대한 피해를 주는 바이러스 및 해커들의 공격은 나날이 발전하고 있는 상황이다.

본 논문에서는 현재 인터넷 보안을 위한 암호체계를 분석하고, 어떠한 방향으로 가야하는지에 대해 논하였다.

향후 미래인터넷 요구사항인 확장성, 재설정/자동설정, 이동성, 상황인지 등에 맞는 암호체계를 분석할 예정이다.

참 고 문 헌

[1] Standford Univ., “Clean Slate Designs for the Internet,” http://cleanslate.stanford.edu.

[2] IETF, http://www.ietf.org.

[3] IRTF, http://www.irtf.org.

[4] 신명기, Future Internet Research in IETF Perspective, 미래인터넷포럼 정기총회 발표자료, 2007, http://anf.ne.kr/fif/meetings.html.

[5] D. Clark, “Contemplating a Future Internet,” in Proc. Internet Innovation Workshop, 2007.

[6] F. Warthman, Delay-Tolerant Networks(DTNs): A Tutorial v1.1, 2003, http://www.dtnrg.org.

[7] 김대영, “미래네트워크,” TTA 저널: 표준화논단, No.112, 2007, pp.12-15.

[8] D. Clark, “The Design Philosophy of the DARPA Internet Protocols,” in Proc. ACM SIGCOMM, 1998.

[9] A. Feldmann, “Internet Clean-Slate Design: What and Why?,” ACM SIGCOMM Computer Communication Review, Vol.37, No.3, 2007, pp.59-64.

[10] S. Shehnker, “We Dream of GENI: Exploring Radical Network Designs,” CRA Computing Community Consortium at(FCRC) 2007, 2007.

◐ 저 자 소 개 ◑

양 종 원(Jong-Won Yang)

2003년 : 공주대학교 전자계산학과(학사)
2005년 : 공주대학교 일반대학원 컴퓨터공학과 (공학석사)
2005년 : 공주대학교 일반대학원 바이오정보학과 박사수료
2006년~현재 : 한국전자통신연구원 위촉연구원
<관심분야> 시스템 보안, 생체인식, 암호 알고리즘 등
e-mail: nobody@kongju.ac.kr

조 내 현(Nae-Hyun Cho)

1987년 : 국방대학원 운영분석(석사)
2007년 : 공주대학교 일반대학원 군사정보과학(정보보호전공) 박사과정
<관심분야> 무선 인터넷 보호, 군사암호 등
e-mail: cjooonh@hanmail.net

채 종 수(Chae - Jong Soo)

2003년 : 전남대학교 컴퓨터공학(석사)
2008년 : 공주대학교 일반대학원 군사정보과학(정보보호전공) 박사과정
<관심분야> NCW, C4I, 국방인터라넷 정보보호, 무선암호 등
e-mail : jsc0230@hanmail.net

서 창 호(Chang-Ho Seo)

1990년 : 고려대학교 수학과(학사)
1992년 : 고려대학교 일반대학원 수학과 (이학석사)
1996년 : 고려대학교 일반대학원 수학과 (이학박사)
1996년~1996년 : 국방과학연구소 선임연구원
1996년~2000년 : 한국전자통신연구원 선임연구원, 팀장
2000년~현재 : 공주대학교 응용수학과(정보보호전공) 부교수
2001년~현재 : 공주대학교 바이오정보학과 부교수 및 군사정보과학 부교수
<관심분야> 암호 알고리즘, PKI, 무선 인터넷 보호 등
e-mail: chseo@kongju.ac.kr