# SNMP환경에서 공개키 기반구조에 관한 설계

노정희* · 문정환* · 이종은* · 이정기* · 이 광** · 이 준***

*조선대학교 컴퓨터공학과 · **청주과학대학 컴퓨터과학과 · ***조선대학교 컴퓨터공학부

# SNMP Key Security Mechanism Design using the PKI

Jeong-hee Roh* · Jeong-hwan Moon* · Chong-eun Lee* · Jeong-ki Lee* · Kwang Lee** · Joon Lee***

*Dept of Computer Engineering Chosun University, Gwangju 501-759, Korea

**Dept of Computer Scoemce, College School, Chongju University

***School of Computer Engineering Chosun University, Gwangju 501-759, Korea

E-mail : bebepig@korea.com

## 요 약

초고속 통신망을 이용한 인터넷의 대중화와 더불어 인터넷을 기반으로 하는 SNMP가 활발해 지고 있다. SNMP에 있어서는 민감한 정보의 기밀성과 사용자 인증의 확보가 필수적이며, 이를 위해서는 전자서명 기술을 포함하고 있는 공개키 기반의 인증서 관리 체계의 확립이 선결되어야 한다. 본 논문에서는 인증, 기밀성 및 무결성 문제를 해결하기 위하여 PKI 기반 인증서의 생성, 관리 기능과인증서를 상호 교환하여 매매 협상을 하는 에이전트 중재에 의한 보안 애플리케이션을 설계하고 이에 대하여 기술한다.

## I. 서 론

모자이크 시대 이후부터 시작된 인터넷의 폭발적인 성장과 보급으로 전 세계적으로 이용자수는 기하급수적으로 증가하게 되었다.

이러한 인터넷의 발달로 인하여 Client/Sever 구조의 네트워크에서 사용자들의 특정 서버를 구축으로 종속적일 수동적인 접근만이 가능하며, 정보의 공유범위 또한 한계가 있다.

인터넷의 특성인 개방성과 표준성은 그 사용주체가 기업이건 개인이건 간에 정보교환과 정보공유의 벽을 허물어 버렸다. 반면에 정보의 보호와 커뮤니케이션 측면에서 근본적인 취약점은 산업발전에 걸림돌이 되고 있다. 이러한 취약점을 해결하기 위해 다각적인 노력의 일환인 공개키 기반 구조가 적용되고 있다.

이러한 보안 문제를 해결하기 위하여 본 논문에서는 PKI(Public Key Infrastructure)를 이용하여 보안관리 측면의 SNMPv3 보안기능의 문제점을 분석하고, 통신망 보안의 중앙관리를 위한 보안관리정책의 필요성, 수립된 보안관리정책을 효과적으로 실행하기 위한 역할기반 보안관리모델에 대하여 기술한다.

## II. 보안 위협

중요한 정보를 가공, 전달, 저장하는 도중에 발생되는 위협으로부터 불법적인 제 3자와 합법적인 통신 상대방에 의해 행위로 구별되며 제 3자에 의한 보안 위협으로 3가지로 나눌 수 있다.

(1)기밀성의 상실 : 정보가 부당하게 노출됨

(1)무결성의 상실 : 정보가 불법개조, 변조됨

(1)가용상의 상실 : 보존된 정보나 자산이 제 3자의 컴퓨터에 부당하게 사용됨.

정보보안의 대표적인 4가지 특성을 들자면, 첫째 컴퓨터를 기반으로 한다는 것, 둘째, 전자화된 정보를 근간으로 한다는 것, 셋째, 네트워크를 이용한다는 것, 넷째, 사용자들의 익명성이 보장된다는 것으로 요약할 수 있다. 위와 같은 특성들 때문에 권한이 없는 자에 의한 자료의 완벽한 복제와 타인의 시스템으로의 불법적인 침입 등이 가능하게 되었고, 이러한 가능성은 결국 정보보안의 존립과 효용성을 위태롭게 하고 그 활성화에 걸림돌이 되어있다.

## II. PKI의 구조와 특성

### 2.1 PKI관련 보안 서비스

정보보안은 각종위협으로부터 안전지대를 구축하는 개념으로 정의된다. 컴퓨터에 저장된 정보는 문서나 데이터의 형태로 저장되고, 이러한 정보에

대한 정당하지 않은 행위를 가하는 것을 위협이라고 정의할 수 있다. 도청, 권한위조, 변조, 서비스 거부 등의 위협에 대응하는 보안정책을 설정하는 것을 보안서비스라고 하는데, PKI는 그 중에서 대표적으로 다음 서비스를 실현하는 체제이다.

1)기밀성(confidentiality)
1)무결성(integrity)
1)인증 (authentication)
1)부인방지(non-repudiation)
1)접근제어(access control)

2.2 PKI의 시스템 구성

시스템을 구성하는 요소로는 인증서를 구축하는 개념으로 정의된다. 컴퓨터에 저장된 정보는 문서나 데이터의 형태로 저장되고, 이러한 정보에 대한 정당하지 않은 행위를 가하는 것을 위협이라고 정의할 수 있다. 도청, 권한위조, 변조, 서비스 거부 등의 위협에 대응하는 보안정책을 설정하는 것을 보안서비스라고 하는데, PKI는 그 중에서 대표적으로 다음 서비스를 실현하는 체제이다.

2.3 PKI의 적용의 문제점

- ■Public Key 분배방식의 안전성을 확실하게 보장할 수 있고 , 이를 공식적으로 인증 할 수 있어야만 한다.
- ■Private Key의 안전한 보관과 사용을 위해 제 3의 key의 저장장치가 필요하다.
- ■Encryption과 Decryption에 대한 속도문제와 Secrecy와의 관계가 Trade-off임으로 Performance를 향상시킬 대안이 필요하다.

## III. SNMPv3 보안모델 구조 및 특성

본래 OSI(Open System Interconnect) CMIP(Common Management Information Protocol)의 개발까지 잠정적인 통신망 관리 프로토콜로 개발되었던 SNMP(Simple Network Management Protocol)는 사용의 편리성과 함께 지속적인 기능향상에 의해, 현재는 단순한 네트워크로부터 네트워크 구성 요소들로 이루어진 복잡한 대규모 네트워크 관리까지 통신망 관리의 핵심 프로토콜로서 자리잡아 가고 있다.

SNMP는 통신망 관리 프로토콜뿐만 아니라, 통신망 구성요소의 기술과 관리정보 스키마 명세를 위한 규칙들, 그리고 통신망 구성 요소들의 관리정보 저장소인 관리 정보 저장소인 관리 정보베이스로 구성된다.

SNMP를 이용한 일반적인 통신망 관리 시스템은 관리시스템은 관리시스템-관리대상시스템으로 이루어진 2계층 구조를 가지며, SNMP 프로토콜에서 제공되는 프리미티브들을 이용해 통신망에 대한 구성관리, 장애관리, 성능관리 , 보안관리, 과금 관리 기능을 수행한다.

3.1 통신망 및 통신망관리시스템 보안

통신망을 대상으로 일반 시스템과 같은 비밀성, 무결성, 가용성에 대한 보안위협이 가능하며, 특성에 따라 수동적 위협과 능동적 위협으로 구분된다. 수동적위협으로는 전송중인 데이터의 내용을 불법적으로 도청하는 행위와 시간대별 통신량과 통신패턴 등을 이용한 통신패턴 등을 이용한 통신 트래픽 분석행위 등이 있다. 수동적 위협이 데이터의 전송을 차단하거나 전송중인 데이터의 내용을 변화시키지 않는데 비하여, 능동적 위협은 데이터의 전송 차단, 데이터의 변경과 위조 등 보다 적극적인 보안위협을 포함한다.

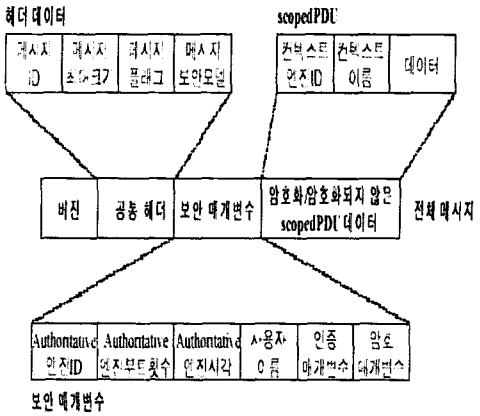


그림 1. SNMPv3 의 메시지 구조

3.2 SNMPv3 보안서비스

1.1.1.49.SNMPv3 개발의 주요 목적중의 하나는 SNMP를 이용한 통신망 관리의 보안기능을 향상시키는 것으로, 강화된 데이터 출처 인증, 데이터의 암호화, 데이터 스트림 변경방지, MIB에 대한 접근 통제 기능들이 추가되었다. SNMPv3 보안서비스는 비 인가된 사용자에 의한 데이터의 변경, 도청, 재사용 공격에 대응하는 기능을 제공하는 사용자기반 보안모델과 인가된 사용자의 MIB 접근을 통제기능을 제공하는 뷰 기반 접근통제 모델에 의해 제공된다.

3.2.1 사용자기반 보안 모델

사용자기반 보안모델에서는 데이터 출처 인증, 데이터 암호화, 데이터 스트림 변경방지 기능을 위한 보안 서비스를 제공한다.

3.2.2 뷰기반 접근 통제

1.1.1.55.뷰-기반 접근통제 모델은 사용자 이름과 보안모델로 구성되는 그룹, 보안 레벨, 컨텍스트, MIB 뷰, 뷰 모드를 입력으로 사용자가 접근

하려는 관리정보에 대한 접근 통제 기능을 수행한다.

3.3 SNMPv3 보안특성 분석

사용자기반 보안 모델과 뷰기반 접근 통제 모델에 기반한 SNMPv3의 보안서비스는 보안 서비스를 거의 제공하지 않았던 이전 SNMP버전에 비해 인증과 암호화를 이용한 매우 강화되고 MIB 뷰 기반의 세분화된 접근 통제 기능을 제공하는 특징을 가진다.

■인증-암호화-접근통제를 이용한 여러 강도의 보안 서비스 제공
■사용자 그룹기반의 접근 통제
■세분화된 접근통제 명세기능

3.3.1 인증 및 암호화를 위한 패스워드 관리 문제

SNMPv3 사용자 기반 보안 모델은 인증과 데이터 암호화 과정에서 관리시스템과 관리 대상 시스템이 공유하는 인증용 패스워드, 암호용 패스워드로부터 각각 생성된 인증키, 암호키를 사용한다. 이를 위하여, 통신망 관리 시스템의 초기화 단계에서 관리시스템과 관리 대상 시스템에는 동일한 인증용, 암호용 패스워드를 설정하는 과정이 필요하며, 관리기능 수행 중의 인증키 또는 암호키의 변경은 이미 설정된 인증키와 암호키를 이용하여 새로운 값으로 'SET SNMP' 연산을 통해 이루어진다.

3.3.2 중앙집중방식의 보안관리기능 부재

SNMPv3 보안 서비스의 다른 문제점은 통신망 관리자에 의해 결정된 보안정책을 통신망 관리에 적용하고 관리할 수 있는 중앙집중방식의 보안관리기능이 제공되지 않는 점이다. 그리고 통신망 관리자별 인증키/암호키 정보, 통신망 관리자 그룹, 통신망 관리자 그룹별 절근가능 MIB에 분산 저장, 관리되어 통신망에 대한 일관된 보안정책의 명세, 변경된 정책의 반영, 그리고 현재 통신망 보안정보 파악에 대한 중앙집중방식의 보안관리가 불가능한 문제점이 있다.

마지막으로 통신망 관리자 그룹간 관계를 정의하는 기능을 제공하지 않아서 관리대상 시스템의 계층적 관리가 불가능한 문제점이 있다. 대규모 기업의 통신망을 고려할 때, 통신망 구성요소가 수행하는 기능의 중요도에 따라 관리대상 시스템을 그룹화하고 각 그룹에 대해 관리자 또는 관리자 그룹을 배정할 수 있다.

SNMPv3의 보안 관리 기능 문제를 정리하면 다음과 같다.

■관리대상 시스템 MIB에 통신망 관리자 보안 정보의 중복 저장
■통신망 보안관리정보의 중앙 집중방식의 관리기능 부족
■통신망 관리자간, 관리자 그룹간 계층구조 미지원으로 인한 효과적 권한부여 관리의 어려움

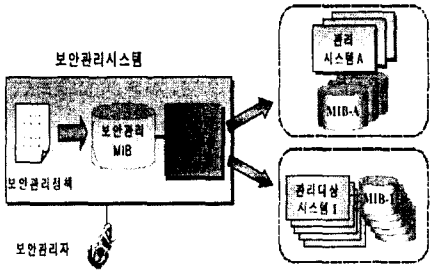


그림 2. 역할기반 보안관리모델 구성요소

3.4 SNMP Key Management의 문제점

1. 통합적인 키 관리가 부족하다.

하나의 관리 시스템이 많은 수의 관리대상 시스템과 통신하기 위해서 모든 관리대상 시스템에 자신의 키를 생성해야 한다.

2. 키의 노출이 쉽다.

키의 생성과정이 아무리 복잡하더라도 결국 사용자의 패스워드에서부터 규칙을 통해서 만들어진다. 또한 이 사용자 패스워드는 양쪽이 모두 같은 값을 가지고 있어야 하므로 관리대상 시스템에 사용자의 패스워드를 전달해 주어야 하는데 이 과정에서 스니핑 같은 공격기법이나 패킷캡쳐 등의 방법에 의해서 유출되기가 쉽다.

3. PKI기능이 추가된 SNMP 키관리

위에서 지적한 SNMP의 Key관리의 문제점을 해결하기 위해 PKI에서 사용되는 인증서의 개념을 도입하여 해결하도록 하였다. 위에서 살펴본대로 인증서는 통신하고자 하는 주체를 인증하는데 있어서 , 확실한 방법을 제공해 준다. PKI의 인증서를 다루기 위해서는 전체 PKI 표준을 따르는 방대한 부분을 다루어야 한다.

PKI기법이 적용된 SNMP에서는 크게 세단계로 나뉜다. 첫번째 단계는 CA로부터 각자의 인증서를 받아보는 단계이다. 두번째 단계는 통신하고자 하는 대상끼리 서로의 인증서를 교환하고 데이터 통신을 위한 대칭키를 만들어 내는 과정이다. 마지막으로 생성된 대칭키로 데이터를 교환하고 데이터 전송이 끝나면 데이터가 사라진다.

## IV. SNMPv3 Key Management 문제점 해결

서버가 클라이언트의 연결을 기다리기 위한 소켓을 설정을 하게 된다.

설정 한 후에 RSA를 초기화 시킨 다음 snmpd

의 실행 여부를 확인한 수 실행되어 있지 않으면 실행시킨 후 PID를 받아 온다.

암호화된 세션키를 보낼 경우

```
Sent_size = write(client_sockfe,
Skey_Encrypted, Skey_Encrypted_len);
If(sent_size <= 0) {
Printf( "[서버]: 암호화된 세션키를 보내지 못했습니다. \n" );
Exit(1);
else
printf ( [서버]: 암호화된 세션키를 처음보낸 정송크기? %d\n , sent_size);
```

서버에서 인증서가 도착했을 경우

```
If(read_size <= 0)
{printf( [SERVER] : Cant Aceept Client_Certificates size.?n );
exit(1);}
else
{printf( [서버]:처음 받은 인증서파일크기의 전송크기 : %d\n,read_size);
while(read_size<sizeof(int))
{temp_size=read(client_sockfd, &int_read, -read_size);
if(temp_size<sizeof9int))
{printf( [서버] : 인증서 파일 크기를 받지 못했습니다.(중간)·.\n );
exit(1);
read_size +=temp_size;}
```

## V. 결 론

SNMP 통신망 관리 프레임워크를 제시한 SNMPv3는 인증과 데이터 암호기능, 데이터 재사용 방지기능을 제공하는 사용자기반 보안 모듈과 사용자그룹 기반의 뷰기반 접근 통제 모델을 통해 융통적이며 매우 강화된 보안 서비스를 제시함으로써, 이전 SNMP 버전들이 제공하지 못했던 안전한 통신망 관리를 위한 기반 기술을 제공하였다. 본 논문에서는 SNMPv3가 제공하지 못하는 보안관리기능을 공개키 기반구조로 관리하기 위한 보안관리모델을 제시하였다. 제시된 보안관리모델은 보안관리자에 의해 기술된 보안관리정책과 보안관리 MIB 데이블을 보안관리 시스템에서 중앙관리한다.

향후 제안된 보안관리 모델에 대한 보완연구와 함께 보안관리 MIB 테이블들을 관리 시스템과 관리대상 시스템에 안전하게 전송하는 프로그램 설계 및 구현에 대한 연구가 필요하다.

## 참고문헌


[1] 이병천, 김광조, "사용자 위주의 새로운 공개키 기반 구조 제안"

[2] Public Key Infrastructure (X.509), http://www.ietf.org/html.charters/spki-charter.html

[3] dhwbdgy, 박기철, 이국희, 조갑환, 문상재, "공개키 확인서 취소 방식의 비교", CISC' 98 논문집, pp, P-20

[4] "SNMP 분석 파라미터를 이용한 WWW 기반의 네트워크 관리 환경 설계" :, 영남대학교 정보통신연구소 논문집 8권2호, pp. 59-70, 2001.

[5] 이형효, 이동익, 노봉남 "역할기반 접근통제 모델을 이용한 SNMPv3 보안관리기능 설계

[6] William Stallings, SNMP, SNMPv2 and RMON, Addison-Wesley, 1996