Peer to Peer 환경에서 SNMP를 이용한 보안에 관한 연구

노정희* · 문정환* · 이 준**

* 조선대학교 컴퓨터공학과
** 조선대학교 컴퓨터공학부

A Study on the Security that Using SNMP in Peer to Peer Environment

Jeong-Hee Roh* · Jeong-hwan Moon* · Joon Lee**

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

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

E-mail : bebepig@korea.com

요 약

최근 모자이크의 시대 이후 인터넷의 폭발적인 발달로 인해 Client-Sever의 방식의 네트웍 서비스 방식 뿐만 아니라 P2P(Peer to Peer) 등 분산 서비스 환경이 각광을 받고 있다. 사용자의 직접적인 자료의 공유를 위해서는 Peer to Peer 환경을 설정하여 분산되어진 자료의 효과적인 관리를 위한 통신의 주체가 되는 각각의 에이젼트들 간의 통신과 Sever와 Agent의 통신에 있어 악의적인 침입에 의한 정보누출이 문제가 되고 있다. 본 논문에서는 이러한 문제의 해결방안으로 P2P 환경에 적합한 PKI(공개키 기반구조)를 기반을 이용하여 보안 메커니즘을 설계하였다.

Ⅰ. 서 론

모자이크 시대 이후부터 시작된 인터넷의 폭발적인 성장과 전 세계적인 인터넷의 보급으로 인해 인터넷의 이용자 수가 기하급수적으로 증가하게 되었다.

이러한 발달로 인하여 기본의 Client/Sever 구조의 네트워크에서 사용자들의 특정 서버를 주축으로 종속적이고 수동적인 접근만이 가능하며, 정보의 공유범위 또한 한계가 있었다. [1]

네트워크 서비스로 크게 두각을 나타내고 있는 방식이 Peer To Peer(P2P) 방식이다. P2P는 지금까지 널리 사용되고 있는 클라이언트-서버 방식과 달리 좀 더 자유로운 네트워크를 구성할 수 있고 중앙 서버의 기능을 없애거나 약화시켜서 사용자가 동등하게 참여하는 분산 네트워크 서비스를 편리하게 제공할 수 있다는 장점을 가지고 있어 여러 분야에서 적용되고 있다.[3]

그러나 이렇게 분산된 환경에서 네트워크로 연결된 컴퓨터에서는 자료 전송간 불법적인 침입행위에 의한 오용을 방지하기 위한 보안 시스템이 요구된다. 이러한 보안문제 해결을 위하여 본 논문에서는 PKI(Public Key Infrastructure)를 이용하여 문제점을 해결하려고 한다. [4]

Ⅱ. P2P의 개념과 특징

1. P2P의 개념

Peer-to-peer라는 개념은 정보통신이론이나 컴퓨팅 구조에서는 오래전부터 사용되어온 개념이다. LAN 환경에서 프린터, 스캐너등의 자원을 공유하는 방법으로서도 사용되고, 인터넷을 비롯한 많은 통신프로토콜 등이 P2P 애플리케이션을 기반으로 하여 설계되었지만 네트워크가 성장하면서 점차 비대칭적으로 변형되었다. 이렇듯 인터넷은 소비자를 위한 공간으로 성장하면서 가져온 변화는 P2P 네트워킹을 어렵게 만들었다.[3][5]

네트워크상에서 통신에 참가하는 각 프로그램(혹은 컴퓨터)이 서로 동등한 성능을 가지고 통신하는 방식으로, 하나의 Sever가 다른 Sever와 통신하는 방식을 말한다.[3]

2. Peer to Peer의 모델

(1) Hybird한 방식

PC끼리의 Interaction을 원활하게 해주는 Sever가 개입되는 형태로써 Pure한 모델과는 반대로 Sever가 존재하는 형태이다. Hybrid한 방식은 중앙의 서버에 의존하는 방식으로서 대부분의 작업이 Sever의 전체 네트워크의 성능이나 연결 상태를 파악하거나, 검색의 효율성을 위한 Index Sever의 역할을 하거나, 혹은 Transaction, Billing, AAA 등을 처리하는 역할을 하게 되는 모델이다. 하지만 컨텐츠와 자료정도 등은 각각의 Peer에 위치하는 모델이다.[5]

(2) Pure한 방식

Pure한 방법은 쉽게 이야기하면 비슷한 성능을 가진 PC 끼리만 연결된 형태로서는 한 마디로 Server가 없는 모델을 말한다. 모든 Peer가 동등한 조건을 가지고 특정 네트웍을 형성하여 "익명성"이 보장된 형태로, "자료나 리소스"를 공유하는 모델이다. Pure한 방식의 대표적인 예로 Gnutella를 들 수 있다. 중앙에서 관리하는 데이터가 없다. Pure한 방법은 쉽게 이야기하면 비슷한 성능을 가진 PC 끼리만 연결된 형태로서는 한 마디로 Sever가 없는 모델을 말한다. 모든 Peer가 동등한 조건을 가지고 특정 네트워크를 형성하여 "익명성"이 보장된 형태로, "자료나 리소스"를 공유하는 모델이다. [1][5]

3. P2P 방식의 문제점

P2P 모델은 일반적으로 Peer to Peer 구조가 Client/Sever 구조에 대해 가지는 단점을 그대로 계승한다는 피어 프로그램의 유지보수의 부담, 시스템 운영의 안전성과 신뢰도 문제, 개방되고 분산되어 있다. 다른 문제점으로 속도상의 문제이다. 그러나 가장 큰 문제점으로는 보안이다. 서로 연결된 컴퓨터 끼리 과연 믿을 만한 것인가 라는 문제이다.[1]

III. III. PKI의 개념과 특징

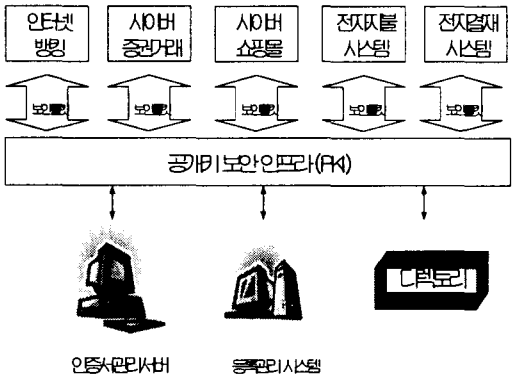
1. PKI의 개념

데이터를 암호화하는 방법에는 공개키와 비밀키방식이 있다. 비밀키 암호시스템이 송수신자 양측에서 똑같은 비밀키를 공유하는 데 반해, 공개키는 암호화와 복호화키가 다르기 때문에 데이터를 암호화하고 이를 다시 풀 수 있는 열쇠가 달라 거의 완벽한 데이터 보완이 가능하고 정보유출의 가능성이 적은 시스템이다. 이를 위해 키의 생성과 인증, 그리고 분배와 안전한 관리를 위한 정보보호표준체계를 마련한 것이 공개키기반구조(PKI)이다. [7][9]

2. PKI의 목표

네트워크를 이용해 전송되는 데이터에는 메시지 도청, 메시지 변조, 메시지 위조, 메시지 송수신 부인 등의 위험요소가 존재합니다. 이러한 위험에 대하여 PKI는 다음과 같은 목표로 서비스를 제공하고 있습니다.[8]

1) 기밀성(Confidentiality) :
거래정보 암호화를 통한 정보보호
2) 무결성(Integrity) :
거래정보의 위/변조 방지
3) 인증(Authentication) :
거래행위자에 대한 신원 확인
4) 부인방지(Nonrepudiation) :
전자서명을 통한 거래 신뢰도 향상
5) 접근제어(Access Control) :
선택된 수신자만이 정보에 접근할 수 있도록 허용



PKI의 개념

3. 인증서비스와 PKI

사이버 공간에서 송.수신되는 전자문서의 송.수신자의 확인 및 송.수신 내용을 확인해 주는 서비스를 인증서비스라 부르며 공개키 암호기술을 사용한다. 공개키 시스템에서는 2종류의 키를 필요로 하는데, 하나는 송신자가 전자서명을 생성할 때 사용하는 Private Key이고 , 다른 하나는 수신자가 송신자의 전자서명을 검증할 때 사용하는 Public Key이다. [6][9]

Private Key 는 인감 등과 마찬가지로 개인이 안전하게 보관하는 키 정보인 반면, 공개키는 네트워크 상의 누구나 접근할 수 있도록 공개해 놓는 키 정보이다. 이 두가지 키 쌍의 합치 여부를 통하여 송.수신 메지시의 위변조를 확인하는 서비스이다. [6][10]

4. PKI 의 구성요소

가. 인증기관(CA; Certification Authority)

PKI의 핵심 객체로서 인증서 등록 발급 조회 시 인증서의 정당성에 대한 관리를 총괄하는 시스템을 말한다. Public Key는 공개된 저장소에 누구나 접근 가능하도록 공개해 놓아야 한다. 이를 공개함에 있어서 신뢰할 수 있는 제 3자가 해당 키 소유자의 신원 정보 등을 확인한 후, 불특정 다수가 그 키를 믿고 사용하여도 좋다는 보장을 기관에서 인증해 주어야 하는데, 이러한 역할을 하는 기관을 인증기관이라고 하며, 이때 사용되는 시스템을 인증시스템이라고 부른다.

다른 CA, 사용자, 등록기관에게 인증서 발급 및 분배.[6][7]

나. 등록기관(RA; Registration Authority)

사용자가 인증 서비스를 사용하기 위해서는 반드시 물리적인 신원을 확인하는 절차가 필요하다. 이 신원확인은 인증기관으로부터 받는 것이 원칙이지만, 지역적으로 멀리 떨어져 있는 사용자들이 중앙의 인증기관에 일일이 방문하는 것은 현실적으로 불가능한다. 따라서 이러한 인증기관의 신원확인 업무를 대행해 주는 기관이 바로 등록기관(Registration Authority: RA)이며, 이때 사용되는 시스템을 등록관리 시스템이라 부른다. [6][8]

- 다른 CA, 사용자, 등록기관에게 인증서 발행 및 분배
- CA에 인증 요청을 전송

다. 디렉토리(Directory)

사용자가 전자서명 검증키를 공개하기 위해 인증기관에 요청한 키 정보에 대하여 인증기관에서 인증서를 발급한 후 이를 공개된 저장소에 등재하게 되는데, 이 공개된 저장소가 바로 디렉토리이다. 이 디렉토리 기능을 담당하는 시스템을 디렉토리 서버 또는 디렉토리 시스템이라고 부른다.[7][8]

- 인증서 및 인증서 취소목록 등 PKI관련된 정보들이 저장 및 검색하는 장소

라. 사용자(User)

PKI 내의 사용자는 사람뿐만 아니라 사람이 이용하는 시스템 모두를 의미한다.[7]

일반적인 사람뿐 아니라 PKI를 이용하는 시스템을 포함하여

- 서명 생성 및 검증
- 인증서 요구 생성
- 인증서 취소요구
- 인증서 갱신 요구

5. 인증서

인증서는 사용자의 신분과 공개키를 연결해주는 문서로 인증기관의 비밀키로 전자서명하여 생성한다. 즉, 인증서는 사용자의 공개키가 실제로 사용자의 것임을 증명하는 것이다.[9]

PKI에서 인증서의 발행 대상은 인증기관, 사용자, 서버 등으로 인증기관에게는 상위 인증기관이 인증기관의 적법성을 증명하기 위해 발행하고 사용자와 서버에게는 사용자의 신원, 서버 등의 적법성을 증명하기 위해 인증기관에서 발행한다.[8][10]

VI. SNMP를 이용한 보안문제 해결

1. SNMP의 보안

SNMPv3 개발의 주요 목적중의 하나는 SNMP를 이용한 통신망 관리의 보안기능을 향상시키는 것으로, 강화된 데이터 출처 인증(Data origin authentication), 데이터의 암호화, 데이터 스트림 변경 방지, MIB에 대한 접근 통제 기능들이 추가되었다. SNMPv3의 보안 서비스는 비인가된 사용자에 의한 데이터의 변경(무결성 침해), 도청(비밀성 침해), 재사용 공격에 대응하는 기능을 제공하는 사용자기반 보안모델(User-based Security Model)과 인가된 사용자의 MIB 접근을 통제 기능을 제공하는 뷰기반 접근통제 모델에 의해 제공된다. [9]

a) 기존 SNMP 망관리 구성과 키관리

SNMP에서 키를 사용하는데는 두가지 단계를 거친다. 보통 사용자는 패스워드를 사용하듯이 자신의 비밀번호를 유지하고 사용한다. 사용자가 패스워드를 넣으면 사용자의 패스워드를 반복시켜서 220 octet사이즈로 만든다. 그런 다음 해쉬함수를 거치면 이것이 바로 User Key이다.p10[

- SNMP Key Management의 문제점

가. 통합적인 키관리가 부족하다.

나. 키의 노출이 쉽다.[11]

b) PKI 기능이 추가된 SNMP 키관리

위에서 지적한 SNMP의 Key 관리의 문제점을 해결하기 위해 PKI에서 사용되는 인증서의 개념을 도입하여 해결하도록 하였다. 위에서 살펴본 대로 인증서는 통신하고자 하는 주체를 인(인증)하는데 있어서 확실한 방법을 제공해 준다. PKI의 인증서를 다루기 위해서는 전체 PKI표준을 따르는 방대한 부분을 다루어야 한다.

-인증서 발급 및 검증

공개키 기반구조가 구축되고 나면 사용자는 인증기관에서 인증서를 발급 받아 인터넷을 통한 전자 거래

시 이를 사용할 수 있다.[10]

-. PKI 기능이 추가된 SNMP 키관리

가. 인증서 발행과정

각각의 대상들은 자신의 공개키를 이용해서 CA에 등록하고 인증서를 발급받는다.

나. 인증서 교환과정

인증서에는 각자의 공개키가 들어 있으므로 인증서를 교환하고 서로의 공개키를 확인한 다음 이 공개키를 이용해서 필요한 데이터를 암호화해서 보낸다. 이 과정에서 실제 데이터 통신을 위한 대칭키 생성이 이루어진다.

다. 데이터 교환과정

인증서 교환과정을 거치면서 생성된 대칭키를 이용해서 실제 데이터의 교환이 이루어진다.

V. 결 론

본 논문에서는 기존의 Client/Sever 구조의 네트워크 환경이 가지는 문제점을 해결하는 모델로 새롭게 제시되고 있는 Peer to Peer 환경을 소개하고, 현재의 Peer to Peer 환경의 문제점을 분석한 후 보안 문제점을 PKI환경을 이용하여 해결하고자 한다. PKI환경에서 네트워크를 이용해 전송되는 데이터에는 메시지 도청, 메시지 변조, 메시지 위조, 메시지 송수신 부인 등의 위협요소를 인증, 부인봉쇄, 무결성, 기밀성등의 서비스로서 보안부분을 해결하고자 한다.

본 연구에서는 PKI에서 SNMP알고리즘을 이용하여 이러한 보안 문제를 해결하고 향후 인증 서비스를 위한 연구를 계속 진행하고자 한다.

참고문헌

[1] 문형남, "P2P 향후전망", 매경 이코노믹, 2000, 11
[2] 이경전, "P2P 비즈니스모델" , 고려대학교, 2000,10.
[3] 이경전, 삼성종합기술원, "P2P Networking", 2000,11
[4] 문형남, 안은정 "P2P를 적용한 인터넷 비스니스의 가능성에 관한 연구", 2000,11
[5] Ganchev.Philpip, "Clusters-a P개 posed Topology for a Peer -to-Peer Network", Unversity a Pittsburgh, 2000,10.
[6] 이병천, 김광조, "사용자 위주의 새로운 공개키 기반구조 제안"
[7] Public-Key-Infastucture (X.509) (PKIX), http://www.ietf.org/html.charter/pkix-charter.html
[8] Simple Public Key Infrastructure (SPKI), http://www.ietf.org/html.charters/spki-charter.html
[9] 오중효, 박기철, 이국희, 조갑환, 문상재, "공개키 확인서 취소 방식의 비료", CISC '98 논문집 , PP, P-20
[10] 이계환, 장재준, 서승호, 김호철, 김영탁, "TINA/CORBA - SNMP 연동을 위한 SNMP Trap Server 설계 및 구현(Design and Implementation of a SNMP Trap Server for TINA/CORBA - SNMP interworking)", KNOM review 제3권 제2호, 2000. 11.
[11] "SNMP 분석 파라미터를 이용한 WWW 기반의 네트워크 관리 환경 설계", 영남대학교 정보통신연구소 논문집, 8권 2호, pp. 59-70, 2001.