PMI를 이용한 SLP 클라이언트 접근제어 방안 설계

남윤중° 유황빈
광운대학교 컴퓨터과학과
{nyjcom°, ryou}@kw.ac.kr

Design for Access Control of SLP Client using PMI

Yoon-Joong Nam° Hyang-Bin Ryou
Dept. of Computer Science, Kwangwoon University

요 약

최근 인터넷과 무선통신의 발전으로 많은 외부 클라이언트들이 학교나 공공기관 같은 내부 네트워크를 사용하게 되었다. 이러한 클라이언트들은 내부 네트워크를 사용하게 되면서 여러 가지 서비스를 받기 위해 다양한 서비스의 위치정보를 검색하는데 사용되는 프로토콜인 SLP(Service Location Protocol)를 사용한다. 이 때 악의를 가진 클라이언트가 SLP(Service Location Protocol)를 이용해 서비스 리스트를 얻어 자신이 내부 네트워크의 모든 자원을 사용할 수 있게 만드는 것과 같은 악의적인 행동을 할 수 있는 문제점이 있다.

본 논문은 이러한 문제점을 해결하기위해 PMI(Privilege Management Infrastructure)를 이용하여 내부 네트워크에 들어온 외부 클라이언트에 관해 내부 서비스에 대한 권한을 설정하고자 하는 방안을 제안하고자 한다.

1. 서 론

인터넷과 무선통신의 발전은 클라이언트들이 노트북과 같은 모바일 컴퓨터를 가지고 외부 기관으로 이동할 수 있게 되었다. 클라이언트들은 외부 기관을 다니면서 그 기관의 내부 네트워크를 사용하게 되면서 여러 가지 서비스를 받기를 원하게 된다. 클라이언트는 그 기관의 내부 네트워크의 서비스 위치를 모르기 때문에 SLP를 이용하여 서비스의 위치를 확인할 수 있다. 그러나 악의를 가진 클라이언트가 접근해서는 안 되는 자원의 위치를 파악해서 그 자원을 사용할 수 있도록 만들 수 있다. 예를 들어, 외부에서 들어온 클라이언트가 프린터를 사용할 때 클라이언트가 누군지를 확인 할 수 없으면 클라이언트는 그 프린터를 마음대로 출력하고 싶은 만큼 출력을 할 수 있는 문제점이 생기게 된다. 이러한 사용자를 확인하기 위해 SLP를 사용해서 서비스의 리스트를 클라이언트에 보내기 전에 클라이언트가 서비스 리스트를 요청했을 때 먼저 자신이 누구이고 어느 정도의 권한을 가진 사용자인지를 확인해서 클라이언트가 사용할 수 있는 서비스 리스트만을 보내줄 수 있고 그 클라이언트에 적당한 권한을 부여할 수 있는 시스템을 제안하고자 한다.

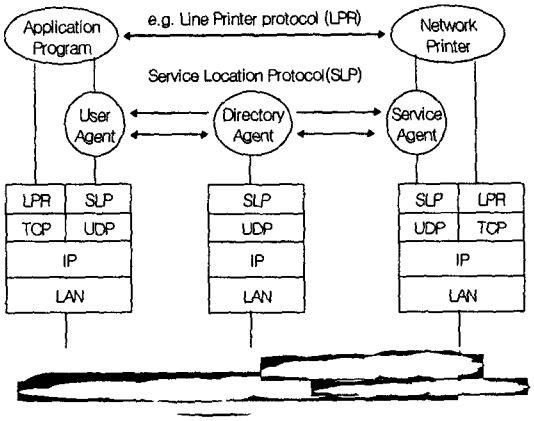
본 논문의 구성은 다음과 같다. 2장에서 관련연구인 SLP와 PMI에 관해 설명을 한다. 3장에서는 제안하고자 하는 시스템을 설명한다. 마지막으로 4장에서는 결론을 맺는다.

2. 관련 연구

2.1 SLP (Service Location Protocol)

SLP는 클라이언트가 원하는 서비스의 위치를 미리 알지 못할 때 그 서비스를 하는 위치 정보를 알아내기 위한 프로토콜이다.

[그림 1]은 SLP가 유저 에이전트, 디렉토리 에이전트, 서비스 에이전트에서 사용되는 것을 보여주고 있다.



[그림 1] SLP 구성요소

다음은 SLP를 사용하는 주요 구성요소를 설명한다.

- 유저 에이전트는 어플리케이션을 대신해서 사용자 클라이언트에서 실행하는 소프트웨어이다.
- 서비스 에이전트는 서버에서 사용할 수 있는 서비스의 존재와 특성을 알려주기 위해 실행하는 소프트웨어이다. 그리고 서비스 요청 메시지를 보낸 유저 에이전트에게

응답한다.

• 디렉토리 에이전트는 서버에 서비스 에이전트가 없을 때 대신해서 유저 에이전트에게 응답 메시지를 보내기 위해 어떠한 다른 컴퓨터에서 실행하는 소프트웨어이고 서비스를 제공하는 서버의 목록을 가지고 있다.

SLP동작은 다음과 같이 동작한다.

① 각각의 서비스 에이전트는 서버가 지원하는 서비스와 특성을 알리기 위해 디렉토리 에이전트에 등록 메시지를 보낸다.

② 디렉토리 에이전트는 서비스등록 메시지를 보낸 서비스 에이전트에 서비스 승인 메시지를 보낸다.

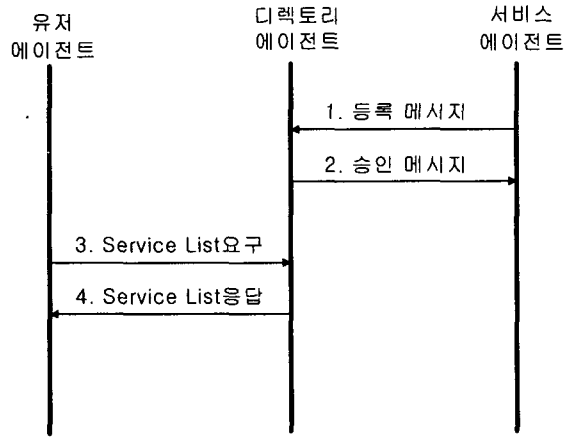
③ 유저 에이전트는 어플리케이션을 대신해서 디렉토리 에이전트에게 사용자가 요구하는 서비스의 설명을 포함한 서비스 요청 메시지를 보낸다.

④ 디렉토리 에이전트는 서비스 요청 메시지에서 나열된 서비스를 이행할 수 있고 네트워크 상에서 사용 할 수 있는 모든 서비스 목록을 포함한 서비스 응답 메시지로서 유저 에이전트에 응답한다.

⑤ 유저 에이전트는 적당한 서버를 선택하고 서비스를 사용하는 클라이언트 어플리케이션에 리스트를 보낸다.

⑥ 나중에 서버를 사용 할 수 없다면 서비스 에이전트는 디렉토리 에이전트에 서비스 등록 취소 메시지를 보낼 수 있다.

[그림 2]는 시스템 동작과정을 도식화한 것이다.



[그림 2] 기존 시스템 동작과정

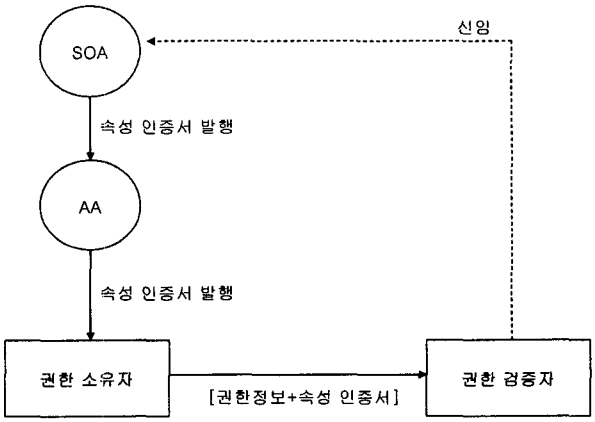
2.2 PMI (Privilege Management Infrastructure)

2.2.1 개요

공개키 기반구조에서 신원확인을 위해 사용하는 공개키 인증서와 구분하여 권한관리 기반구조에서 사용되어 속성 관계를 보증하는 인증서를 'PMI 인증서' 또는 '속성 인증서(Attribute Certificate)'라 부른다. 공개키 인증서는 인증기관에서 사용자에 대한 신원을 확인한 후 발급하는 반면, 속성 인증서는 각 해당 속성을 관리하는 기관에서 해당 속성 정보를 바탕으로 발급하게 된다. 따라서 사용자의 신원확인을 위해서는 기존의 공개키 인증서를 그대로 활용하고 사용자의 속성 정보를 확인하기 위해서는 속성 인증서를 검증하면 되는 것이다. 이러한 검증 과정에서 권한 검증자는 속성 인증서와 그것이 가리키는 공개키 인증서를 연결하여 해당 사용자가 정당한 권한을 가지고 있는지 판별하게 된다.

2.2.2 구성요소

[그림 3]는 권한관리 기반구조의 전반적인 구조를 나타내고 있다. 여기서 SOA(Source Of Authority)는 공개키 기반구조의 루트 CA와 유사한 역할을 하는 자로서 권한 검증자가 무조건 신뢰하는 AA(Attrivute Authority)이다. AA는 SOA로부터 권한의 전부 또는 일부를 위임받아 인증서 발급 업무를 수행한다. 권한 소유자(Privilege Holder)는 인증서를 통해 AA로부터 권한에 대한 소유권을 보증 받은 자로서 PKI의 End-entity에 해당한다. 권한 검증자(Privilege Verifier)는 속성 인증서를 받아 이것을 어플리케이션에 맞게 사용하는 자로 권한 주장자가 권한을 정당하게 소유하고 있는지 확인한다.

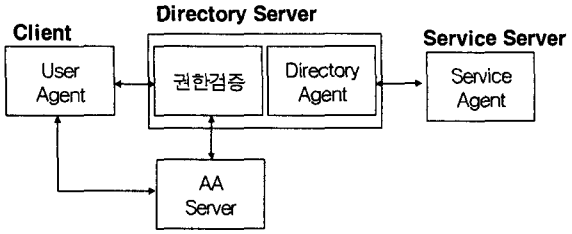


[그림 3] PMI 구조

3. 제안 시스템

3.1 시스템 구조

앞에서 말한 SLP는 유저 에이전트, 디렉토리 에이전트, 서비스 에이전트만을 가지고 있어서 악의 적인 클라이언트가 사용할 수 있는 권한을 설정 할 수 없었다. 제안하고자 하는 시스템은 [그림 4]에서 보여주는 것과 같이 유저 에이전트, 디렉토리 에이전트, 서비스 에이전트 뿐 아니라 속성인증서를 발급하는 AA 서버와 권한을 검증할 수 있는 모듈로 구성되어 있다. 권한검증 모듈은 유저 에이전트가 서비스 요청 메시지를 보낸 것을 감지하고 유저 에이전트에 속성인증서 요구를 하게 되고 AA 서버는 각 클라이언트에 맞는 속성인증서를 발급하게 된다. 그러므로 클라이언트에 대한 권한 설정을 할 수 있게 하였다.



AA Server : Attribute Authority Server

[그림 4] 제안 시스템 구조

3.2 시스템 동작

처음 클라이언트가 새로운 네트워크에 들어 왔을 때 클라이언트는 자신이 필요한 서비스를 찾기 위해 SLP를 사용하여 자신이 원하는 서비스를 찾으려 할 것이다. 다음은 제안하는 시스템에서 클라이언트가 필요한 서비스를 SLP를 통해 찾는 과정을 말한다.

① 유저 에이전트는 디렉토리 에이전트에 SLP를 사용해서 서비스 리스트를 요청한다.

② 요청메시지를 받은 디렉토리 서버는 권한검증 모듈에서 유저 에이전트 속성인증서의 권한을 확인하기 위해 속성인증서를 요청한다.

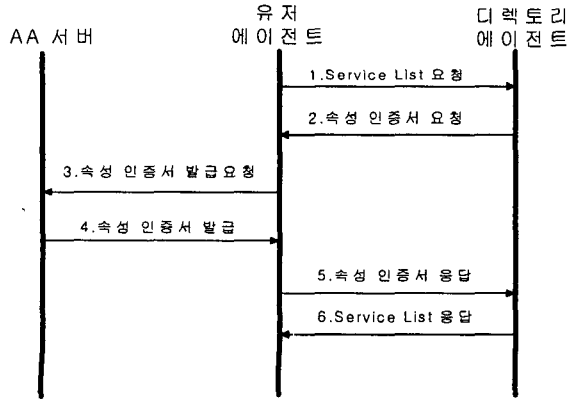
③ 클라이언트의 속성인증서 소유여부

ⓐ 클라이언트가 자신이 들어온 내부 네트워크에 해당되는 속성인증서를 가지고 있다면 그 인증서로 응답한다.

ⓑ 그렇지 않다면 클라이언트는 3.3절에서 설명할 속성인증서 발급과정을 통해 속성인증서를 발급받고 그 속성 인증서로 디렉토리 서버에 응답한다.

④ 디렉토리 서버는 속성인증서에 명시되어 있는 클라이언트의 권한에 맞는 서비스 리스트를 응답한다.

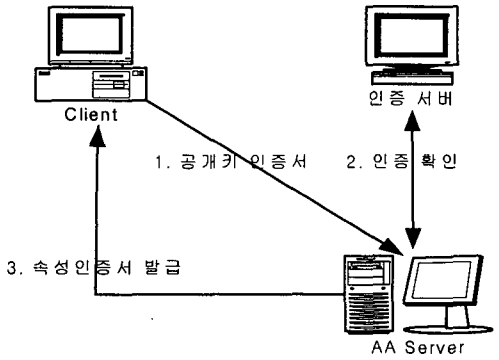
위 과정을 통하게 되면 클라이언트가 접근이 불가능한 서비스 위치 자체를 노출 시키지 않기 때문에 클라이언트가 접근 불가능한 곳에는 아무런 피해를 주지 않게 된다. [그림 5]는 이러한 시스템 동작과정을 도식화한 것이다.



[그림 5] 제안 시스템 동작과정

3.3 속성인증서 발급과정

속성인증서 발급과정은 먼저 클라이언트가 내부 네트워크의 속성인증서를 가지고 있지 않으면 속성인증서를 발급받아야 한다. [그림 6]은 속성인증서 발급과정을 보여준다.



[그림 6] 속성인증서 발급과정

4. 결론 및 향후 연구과제

본 논문에서는 악의적인 클라이언트가 자신이 새로이 들어간 내부 네트워크에서 서비스의 위치를 확인하기 위해 SLP를 사용하여 자신이 접근해서는 안 되는 서비스 위치에 접근하는 문제점을 해결하고자 PMI를 적용하여 속성인증서를 발급받아 디렉토리 서버로부터 서비스 위치를 제공받을 때 클라이언트가 사용해도 되는 서비스 위치 리스트만을 보내주는 시스템을 설계하였다.

향후 연구과제로서 이 논문에서 제안된 시스템의 목적은 클라이언트의 권한을 설정해서 서버에 접근을 막는 것인데, 어떠한 서버에 접근 권한을 가진 클라이언트가 접근하여 악의 적인 행동을 할 경우 그 클라이언트에 대한 예방책에 대한 연구가 진행되어야 할 것이다.

5. 참고 문헌

[1] James D. Solomon, "Mobile IP", PTR Prentice Hall, 1998.

[2] J. Veizades and E. Guttman and C. Perkins and S. Kaplan, "Service Location Protocol", RFC 2165, June 1997. available on line at http://www.ietf.org/rfc/rfc2165.txt.

[3] S. Farrell and R. Housley, "An Internet Attribute Certificate Profile for Authorization" RFC 3281, April 2002. available on line at http://www.ietf.org/rfc/rfc3281.txt.

[4] Joon s. Park and Ravi Sandhu, "Binding Identities and Attributes Using Digitally Signed Certificates", IEEE communication Magazine, September, 2000.

[5] P. Yee, "Attribute Certificate Management Messages over CMS", March 2002, Draft-ietf-pkix-acmc-01.txt