모바일에이전트를 이용한 SLP 보안

황영덕° 조인휘
한양대학교 정보통신대학원
usei°@ihanyang.ac.kr iwjoe@hanyang.ac.kr

Security of Service Location Protocol using MobileAgents

Youngdeok Hwang° Inwhee Joe.
Graduate School of Information and Communications, Hanyang University

요 약

현재의 사용자 컴퓨팅 환경은 점점 방대해지고 복잡해지고 있으며, 이동중에 업무를 신속하게 처리해야하는 경우가 많아지면서, 이동 컴퓨팅환경에 대한 편리성과 신뢰성의 요구가 증가하고 있다. 사용자는 언제 어디서나 필요한 서비스를 제공 받을 수 있어야 한다.

이 논문에서는 서비스와 자원탐색을 자동으로 해주는 SLP(Service Location Protocol), 필요한 코드와 데이터를 원격으로 보내 처리하는 모바일에이전트(Mobile Agents) 기술의 문제점을 해결하고 상호 연동하여 보완한다.이 기술의 보편화를 저해하는 보안에 대한 문제점을 분석하여 이것을 해결할 하나의 모델을 제시함으로써 편리하고 안정적인 응용을 보이고자 한다.

1. 서 론

현재의 사용자 컴퓨팅 환경이 점점 방대해지고 복잡해 지면서, 원하는 서비스와 정보를 찾기위해 사용자는 복잡한 설정을 일일이 지정해야 하며, 원하는 정보를 찾기 위해 많은 노력을 기울여야만 한다. 특히, 이동성이 잦은 장비들은 더더욱 이러한 작업이 귀찮아진다.

SLP는 IETF 표준[1]이며 무선 또는 기타 연결 방식을 가진 장치의 수동 구성을 간편하게 해주는 프로토콜이다. 이 프로토콜을 이용하면 프린터, 서버, 팩스기기, 비디오 카메라, 백업 테이프등의 자원과 서비스의 위치를 자동으로 검색하고 설정할 수 있게 된다. 하지만 악의적인 서버가 등록하거나, 정상적이지 않은 사용자가 서비스를 이용할 수 있는 문제점이 발생한다.

모바일 에이전트(Mobile Agents) 기술은 에이전트(agent)가 다른 실행 환경에 이동해 처리를 행하는 것에 의해, 원격실행, 비동기실행, 분산 프로그래밍의 간단화 등이 실현된다. 또한, 에이전트(agent) 관리자는 자기 대신에 모바일 에이전트(agent)에게 네트워크(network)를 사용한 번잡한 작업의 처리를 맡길 수 있다. 한편, 악의를 가진 실행 환경이 에이전트(agent)의 데이타(data)에 대하여, 도청· 수정한 문제도 발생한다.

2. 관련 연구

2.1 SLP(Service Location Protocol)

2.1.1 개념

그림 1은 SLP의 기본 동작원리를 보여주는 것으로서 UA(User Agent), SA(Service Agent), DA(Directory Agent)의 3가지 에이전트로 구성되어 있다.

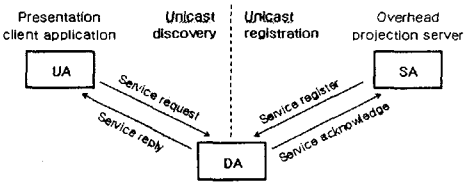

그림 1. SLP의 기본구성

UA는 어플리케이션을 대신해서 사용자 클라이언트에서 실행하는 소프트웨어로서 자원이나 서비스를 요청하고 응답을 받는다.

SA는 자원이나 서비스 서버에서 사용할 수 있는데, 자신의 존재와 특성을 알려주기 위해 DA로 등록 메시지를 보내게 된다.

DA는 서버의 SA의 등록을 받는 일종의 데이터베이스로서 UA가 요청한 적절한 서비스를 알려주기도 한다.

2.1.2 SLP의 문제점

기존의 SLP프로토콜은 UA의 인증없이 요청을 받아들이고 SA 역시 모든 등록 요청을 수락하게 된다.

이런 상황에서 네트워크가 점점 대형화 되어 악의적

인 사용자가 나타나게 되고 악의적인 사용자에 의하여 서버의 서비스가 무차별적으로 이용되어 서비스를 필요로하는 요구자에게 피해를 줄 수 있는 문제가 발생할 수 있다.

또한, 거짓으로 서버가 SA를 통하여 등록 메시지를 볼 수 있다. SA는 인증되지 않은 서버의 등록을 DA로 보내고 서비스를 제공하지 않고도 UA를 끌어들일 수 있게 된다.

2.2 모바일에이전트(MobileAgents)

2.2.1 개 념

이동 에이전트란 자율성을 가지고 비동기적으로 수행이 가능한 개체로, 선택적으로 지능을 가지고 특정 작업을 수행하기 위해 네트워크 상의 한 호스트에서 다른 호스트로 이동할 수 있는 개체라고 정의 할 수 있다.

네트워크 상의 호스트는 이러한 이동 에이전트가 실행 할 수 있는 환경을 제공하여 이질적인 하드웨어와 운영체제로 구성된 분산 컴퓨팅 환경에 동적인 이식을 가능케 하여(Portability) 서로 이질적인 분산 환경에서도 에이전트가 실행할 수 있는 환경을 제공하여 주는 에이전트 시스템의 역할을 수행한다. 이러한 에이전트는 특정 작업을 수행하기 위해 자신을 복제(Clone)하여 작업 부하를 분산시킬 수 있으며 자신의 현재 실행 상태를 저장하여 네트워크를 통해 이동하며(Code mobility) 상태를 다시 복원함으로써 해당 작업에 대한 실행을 재개할 수 있어 과부하 된 호스트의 부하를 줄여 수행의 효율성을 높이는 기능을 제공 할 수 있다[2][3]. 다음 그림에서 모바일 에이전트의 기본 동작원리를 나타냈다.

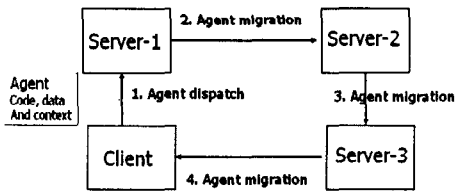

그림 2 MobileAgent

클라이언트에서 모바일 에이전트가 코드와 데이터를 가지고 각 서버를 이동하는 모습을 보여주고 있다.

2.2.2 MobileAgent의 문제점

이동 에이전트는 인터넷과 같은 공개 네트워크 상의 호스트들을 직접 이동해 다니면서 주어진 작업을 수행하기 때문에, 에이전트의 상태, 실행 가능한 코드, 이전 호스트로부터 얻은 데이터를 공격자로부터 안전하게 보호하느 것이 중요 관심사이다. 그러나, 현재 대부분의 공개 네트워크는 안전하지 않은 것으로 알려져 있고 모바일 에이전트가 실행되는 호스트 또한 반드시 정직하다는 것을 보장할 수 없기 때문에 이동 에이전트에 대한 공격에 대해 분석한 후 적절한 대응이 필요하다[4].

3. SLP상에서 모바일에이전트의 보안

3.1 목 표

SLP의 문제점을 해결하기 위해 UA와 SA를 이용하는 호스트들을 인증하기 위한 AA(Authorization Agent)를 둠으로서 이 문제를 해결하고, 또한 이동성을 중요시하는 시스템에서 SLP를 이용하기 위하여 모바일 에이전트와 협력할 수 있도록 함으로서 실제 응용을 보이고자 한다.

3.2 제안 시스템

이 시스템은 모바일에이전트와 협력하여 이동성을 지원한다. 이동형 클라이언트 1이 네트워크 상태가 좋지 않더라도 작업할 수 있도록 모바일 에이전트(MobileAgent)를 유선으로 연결된 클라이언트 *n* 으로 보내게 된다. 유선상의 클라이언트는 직접 DA에게 보내도록 한다.

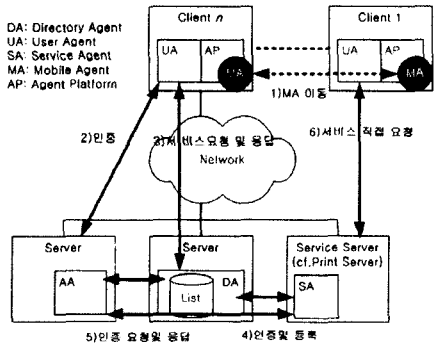

그림 3 제안시스템의 구조

이때 1)에서 MA는 UA와통신할 코드와 출발지정보, 출발지서명, 요청 서비스타입, 문서등의 민감한 자료를 XML 보안방식의 데이터로 묶어 출발한다. 보내고난 Client 1에서는 접속이 끊어져도 상관없다.결국 MA가 DA로 옮겨와서 모든처리를 하도록 하게 할 수 있도록 한다. 2)에서 XML 보안 인증 방식으로 AA에 인증을 받도록 한다. 여기서 MA는 출발지 서명을 가져오므로 부인 봉쇄기능을 하게 되고 무결성을 입증한다. 이후 인증을 마치고 서비스를 알게되면 6)에서 UA와 협업하여 해당 서비스를 요청하고 DA로부터 해당 서비스 목록을 가져와서 적절한 서비스 서버를 MA가 이용하게 된다. 4), 5)에서도 마찬가지로 SA의 서버를 인증하도록 한다.

3.2.1 XML Security

XML Security이란 XML 구조에 적용된 보안 기술의 어플리케이션이라고 할수 있다. 이 기술을 이용하여

데이터 보호와 인증을 적용 하였다. XML Security는 대단한 유연성을 제공하는데 기존의 바이너리 형태의 인증 및 암호화방식을 텍스트 기반의 솔류션으로 변경된 것이다. 이것으로 데이터들의 관계를 더욱더 쉽게 표현할 수 있게 한다.

XML 형태로 표현된 데이터는 서명 데이터 외에도 검증이나 관련된 모든 정보(X.509인증서)를 담을 수 있게 된다. XML 서명 문법은 <Signature> 앨리먼트와 <SignedInfo>앨리먼트로 구성되어 있다. 아래에 예시를 보인다.

```
<Signature>
  <SignedInfo>
    <SignatureMethod
        Algorithm =
      " http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
  <Reference URI=" file:///C:Wcheck.txt" >
  <DigestMethod
  Algorithm=" http://www.w3.org/2000/09/xmdsig#sha1" />
  <DigestValue>aZh8Eo2aLike1D5NMW+q3iHrRPQ=
  </DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>
          M16rfg4Xwdf3erf…
</SignatureValue>
</Signature>
```

표 1 XML Document

3.2.2 Authorization Agent의 구조

UA나, SA는 AA를 통해 자신의 서버가 인증된 시스템으로 등록되어야만 UA와 SA의 기능을 수행하도록 한다. 적절한 호스트로 인정 받기 위해서는 인증서를 통하여 호스트의 서명을 검증하고 판단할 수 있도록 한다. 이것은 사용하고자하는 어플리케이션의 신뢰성을 판단할 수 있는 기준으로 작용한다. XML 입력으로 <KeyInfo> 앨리먼트를 이용하며, 그 앨리먼트를 기준으로 해서 신뢰성 여부를 판단하게 된다. 그림 4 에서는 XML 문서를 AA가 입력 받아 <Signature> 앨리먼트 안에 <KeyInfo>앨리먼트를 분리해 내고, 그것을 바탕으로 신뢰 여부를 판단하는 과정을 보여준다.

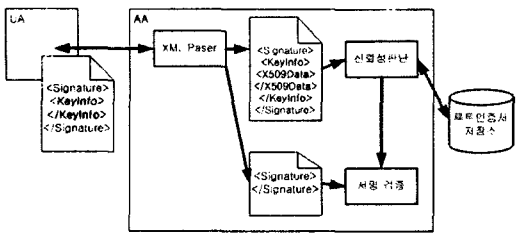

그림 4 AA의 신뢰성여부 판단

이 예에서 <KeyInfo>앨리먼트는 X.509인증서를 가지고 있으며, 이 인증서는 <KeyInfo>앨리먼트에 담겨서 '신뢰성 판단' 엔진 으로 넘겨지게 된다. 그리고, 신뢰 여부에 대한 판정 결과는 서명 검증 컴포넌트로 넘어간다. <KeyInfo> 내부의 인증서는 신뢰된 루트 인증서 저장소의 인증서와 대조해 보게 된다.

4. 구현 및 결론

SLP상에서 MA를 이용하므로서 클라이언트의 이동성을 보장하고 네트워크가 끊어진 상태에서도 원하는 서비스를 찾고 이용할 수 있도록 하였다.

본 논문에서는 SLP프로토콜의 취약점인 인증부분을 보완하는 AA를 제안하고 설계하였다. AA는 XML형태로 인증서데이터와 문서데이터를 같이 포함할 수 있으며, 텍스트 방식으로 인하여 유연성과 데이터무결성을 제공하게 되었다. Ichiro의 Agentspace를 확장하여 Editor의 문서를 SLP를 이용하여 프린터 자원을 찾는 과제를 수행하였다.

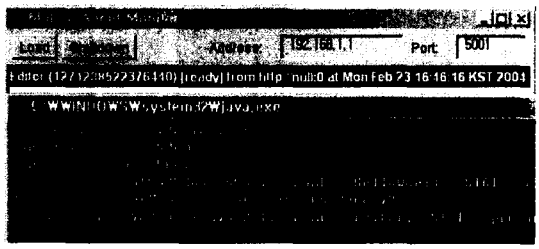

그림 5 Agentspace를 이용한 수행

인증되지않은 서버나 클라이언트는 AA에 의해 차단되어지게 되고 모바일 에이전트를 이용해 네트워크 소통량을 감소하며, 끊어진 상태에서도 요청된 서비스를 수행하게 된다.

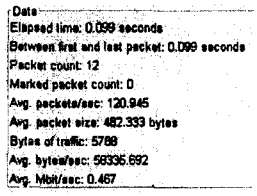

그림 6 MA전송시 패킷량

향후 체인체인을 이용하여 변경된 MA를 검출하며, 자원 등급과 MA의 여행리스트에 대해 동적구성을 하도록 하는 연구가 필요하다. 이 연구를 통하여 MA에 대한 자체 보안능력을 향상시킬 계획이다.

[1] E. Guttman, C. Perkins, J. Veizades, and M. Day, " Service Location Protocol, Version 2" IETF, RFC 2608, June 1999.
[2] D. Chess, C. Harrison, A. Kershenbaum. " Mobile agents : Are they a good idea?, In Mobile Object Systems: Towards the Programmable Internet" , Vol. 1222 of Lecture Notes in Computer Science, Spring-Verlag, 1997.
[3] Anny B.Lange , Mitsuru Oshima , " Programming and Deploying Java Mobile Agents with Aglets," AddisonWesley, 1998.
[4] Michael S. Greenverg, Jennifer C. Byington, " Mobile Agents and Security," IEEE Communications Magazine, 1998