모바일 컴퓨팅 환경을 위한 원격지 리소스 접근 방법 구현

이유근°, 김상태, 곽동규, 박원배
경북대학교 정보통신학과
{cinema74°, storm, kwak}@inc.knu.ac.kr, wbpark@ee.knu.ac.kr

Implementation of Remote Resource Access Method for Mobile Computing Environment

Yougeun Lee°, Sangtae Kim, Dongkyu Kwak, Wonbae Park
Dept. of Information and Communications Kyungpook National University

요 약

유비쿼터스 컴퓨팅 환경에서 모바일 디바이스는 Service Controller의 역할을 수행한다. 그러나 모바일 디바이스를 이용하여 원격지 리소스에 접근하는 것은 제약이 따른다. Desktop에서 흔히 쓰이는 FTP와 같은 원격지 접속 기술은 모바일 디바이스에서는 사용 할 수 없다. 또 다른 방안으로 모바일 디바이스에서 Java Application을 이용하여 원격지 컴퓨터에 접속하는 방법이 있다. 그러나 이 또한 Java Security 문제를 해결해야 한다. 모바일 디바이스에서의 Java Security 문제는 그 응용 범위나 필요성에 비해 아직까지 구현 모델은 없다. 따라서 본 논문에서는 Desktop상에서 구현하는 Java Security 접근 방법 모델을 이용하여 모바일 디바이스에서 웹 브라우저를 통해 Java Application으로 원격지 컴퓨터에 접근하는 방법을 구현 한다.

1. 서 론

모바일 디바이스를 이용하여 원격지 컴퓨터의 파일을 읽거나 수정하는 일을 수행하려 한다면 우선적으로 원격지 컴퓨터에 접속을 해야 한다. Desktop 컴퓨터에서는 FTP, Telnet 등을 통하여 원격지 컴퓨터에 쉽게 접속할 수 있지만, PDA와 같은 모바일 디바이스에서는 지원하지 않는다. Java Application은 Desktop 컴퓨팅 환경에서 구현되는 접속기술을 모바일 컴퓨팅 환경으로 구현할 수 있다. 그러나 먼저 원격지 컴퓨터에 접근하기 위해서는 Java Security 문제를 해결해야 한다.

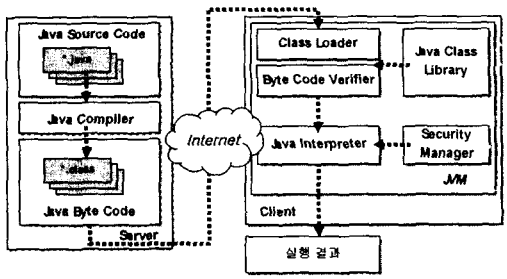
Java는 분산 네트워크 환경에 적합한 프로그래밍 언어로 보안이 중요하다. 보안이 취약하다면 알지 못하는 Remote Code에 의해 원격지의 컴퓨터 시스템이 위험해진다. 따라서 Java는 언어와 런타임 시스템 안에 보안 기능이 설계되어 있기 때문에 외부로부터 전송되어지는 Remote Code는 현실적으로 원격지 컴퓨터의 리소스에 접근 할 수 없고 리소스의 이용도 불가능 하다[1]. 그러나 Java Security API를 이용하여 Java.Policy에 권한을 부여하게 되면 권한이 부여된 항목에 있어서는 사용이 가능해진다. 이러한 원격지 컴퓨터 접근 방법은 썬 마이크로시스템사를 중심으로 Desktop상에서의 활용에 초점을 맞춰 연구가 진행되어져 왔다. 웹의 활용 범위가 넓은 모바일 디바이스를 위한 원격지 컴퓨터 접근 방법에 관한 많은 연구가 요구 된다.

따라서 본 논문에서는 모바일 디바이스에서 Java Security를 이용한 원격지 리소스 접근 방법을 구현 한다. 그리고 모바일 디바이스 상의 웹 브라우저를 통하여 Java Application의 동작 과정과 그 결과를 확인하기 위하여 Java Applet을 사용 한다.

2. 관련 기술

2.1 Applet

Java Applet이란 작은 Application을 의미하며, 웹상에서 웹 페이지와 함께 사용자 측으로 보내질 수 있도록 작게 만든 프로그램을 말하며 애니메이션이나 간단한 계산 그리고 사용자가 서버에 별도의 요청을 하지 않고서도 수행할 수 있는 단순한 작업들을 수행한다.



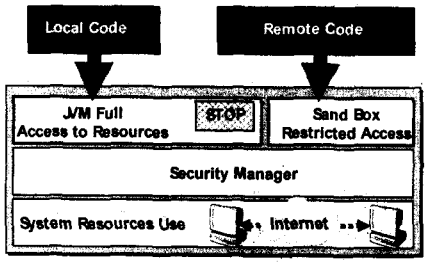
[그림 1] Applet 동작 과정

Java Applet의 동작과정은 그림1과 같다. Java Applet은 서버에서 프로그램이 작성되어 웹을 통해 클라이언트로 전송되어 실행된다.

Java Applet은 웹을 통해 다운로드 되므로 Java Applet에 부여된 Security Permission에 따라 클라이언트에서 수행 할 수 있는 작업이 결정된다[1,2].

2.2 Java Security Model

인터넷의 발달과 더불어 사용자들의 보안에 대한 관심도 커지게 되었다. Java Security Model도 JDK 버전의 발전과 더불어 점점 개선되어 가고 있다.



[그림 2] JDK1.0 보안 모델

JDK1.0 Security Model은 그림 2와 같다.

JDK1.0 보안 모델의 특징은 Local 코드는 Security Manager에서 신뢰하여 컴퓨터의 모든 자원에 접근 가능하도록 하고, Remote 코드는 Security Manager에서 불신하여 Sand Box내에서 정의된 제한된 작업만 실행 가능하도록 한다.

JDK1.1 Security Model의 특징은 JDK1.0에 유연성 추가된 형태로서, Remote 코드에 Sign을 추가하여 인증된 Sign을 가지고 있는 Remote 코드는 Local 코드와 동일한 작업을 수행 할 수 있도록 한다. 따라서 Local 코드, Signed Remote 코드는 Security Manager에서 신뢰하여 컴퓨터의 모든 자원에 접근이 가능하도록 하고 Non-Signed Remote 코드는 Security Manager에서 불신하여 SandBox내에 제한된 작업만 수행 가능 하도록 한다.

JDK1.2 보안 모델의 특징은 Local 코드, Remote 코드에 대해 Scurity Policy를 이용하여 권한을 지정하고 Security Manager에서 허가하면 주어진 권한에 따라 보안 Domain내의 리소스에 접근이 가능하도록 한다[3,4].

3 원격지 리소스 접근 방법 모델의 구성 및 설계

Java 환경이 갖추어져 있는 모바일 디바이스로 Java가 탑재된 원격지 컴퓨터에 접근하기 위해서는 Java Security 문제를 해결해야 한다.

본 논문에서는 인터넷 전용 브라우저가 탑재된 WinCE 기반의 PDA(*Compaq PDA ipaq H3600*)를 이용하여 원격지 컴퓨터에 접속한다. 원격지 컴퓨터의 접속과 접속한 컴퓨터의 자원을 이용하기 위해서 Desktop 환경의 Java Security 기술을 응용하여 모바일 디바이스 기반의 Java Security 기술을 설계 및 구현한다.

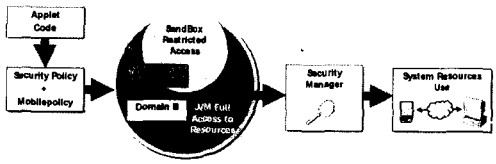
구현 과정에서 실제 모바일 디바이스 환경의 Java Security 기술을 적용 했을 때와 적용하지 않았을 때를 비교한다. Java Security 구현 결과물은 Java Applet을 통하여 모바일 디바이스상의 웹 브라우저로 결과를 확인한다.

3.1 원격지 리소스 접근 방법 모델의 해결 방안

본 논문에서 구현된 모바일 디바이스를 위한 원격지 리소스 접근 방법은 모바일 디바이스 상에 특별히 프로그램의 추가적인 설치 없이 Java 환경이 설치되어 있는 디바이스라면 어디든지 구현이 가능하다. 그리고 Java Security API를 통해 자신이 원하는 작업에 대한 Security Policy만을 구현하여 작업을 수행 할 수 있다.

3.2 원격지 리소스 접근 방법 모델의 구성 및 동작 과정

본 논문에서 원격지 리소스 접근 방법 모델의 구성도는 그림 3과 같다.



[그림 3] 원격지 리소스 접근 방법 모델의 구성도

이 모델의 구성도는 Java Application을 사용하여 모바일 디바이스에서 웹 브라우저를 이용하여 원격지 컴퓨터에 접근하는 과정을 나타낸다. 웹을 이용하기 위하여 인터넷 전용 브라우저가 탑재 되어 있는 WinCE 기반의 Pocket PC를 사용한다. 모바일 디바이스에서 원격지 컴퓨터의 자원을 이용하기 위한 Java Security 문제는 기존 데스크 탑에서 사용되던 Security Policy를 응용함으로써 해결 할 수 있다. 기존 모바일 디바이스에서 사용하던 Java.Policy에 새롭게 구현한 Mobilepolicy를 함께 원격지 컴퓨터로 전송하고, 원격지 컴퓨터에서도 Mobile police를 생성하여 Security Manager에서 원격지 컴퓨터와 모바일 디바이스에서 전송된 Mobilepolicy의 권한을 비교하여 더 제한적인 권한이 최종 권한으로 허가되어 그에 맞는 자원을 가지고 있는 일정 작업을 모아 놓은 장소를 나타내는 Domain을 이용하게 된다.

Security Manager는 Security Class를 이용하여 Policy File의 허가 목록들을 참조하여 어떤 작업들이 허가 되었는지 점검 한다. 여기서는 Java.Policy와 새롭게 작성된 Mobilepolicy를 함께 확인한다. Security Manager에서 최종 허가되면 원격지 컴퓨터의 리소스에 접근 할 수 있다.

3.3 원격지 리소스 접근 방법 모델의 구현

본 논문에서 구현된 시스템의 환경은 다음과 같다.

- OS: Windows 2000 Server, WinCE 3.0
- Java: JDK 1.3.1, Personal Java
- Servlet: Jsdk 2.1
- Mobile Device: Compaq PDA(*PocketPC H3600*)
- Java Virtual Machine: Jeode VM, JVM

구현된 접근 방법 모델의 실행 과정은 아래와 같다.

① 아래의 소스 코드는 모바일 다바이스 이용자가 원격지 컴퓨터에 접속하여 자원을 이용하기에는 불충분한 Java.Policy에 추가적으로 자원을 이용하기 위해 충분한 권한을 부여한 Mobilepolicy의 소스 코드이다.

본 구현에서는 특정한 File에 대한 권한의 한 예로 FilePermission을 이용한다.

```
/* 사용자가 필요로 하는 작업에 대한
권한을 명시 */
grant {
  permission java.io.FilePermission "test.txt",
"read";
};
```

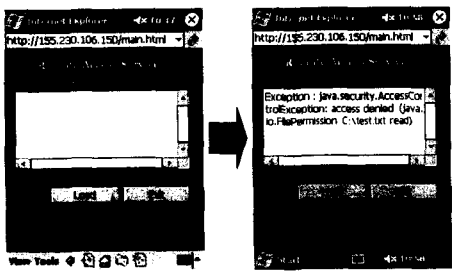
② 아래는 Java.Security의 정책 코드이다.

Java.Policy와 함께 Mobilepolicy의 경로를 지정함으로써 Security Manager에서 권한 부여 시 Mobilepolicy도 함께 참조하도록 한다.

```
/* Provider는 암호 알고리즘을 구현한
클래스의 집합 */
policy.provider=sun.security.provider.PolicyFile
security.provider.1=sun.security.provider.Sun
security.provider.2=com.sun.net.ssl.internal.ssl.
                    Provider
security.provider.3=com.sun.rsajca.Provider
security.provider.4=com.sun.crypto.provider.SunJCE
security.provider.5=sun.security.jgss.SunProvider

/* Policy.url은 Java.Policy의 경로 지정 */
/* 순서대로 참조*/
policy.url.1=file:${java.home}/lib/security/java.policy
policy.url.2=file:${user.home}/.java.policy
policy.url.3=file:/Windows/lib/security/Mobilepolicy
```

③ 그림 4는 Security Manager에서 부여한 File Policy에 관련된 권한 없이 모바일 디바이스에서 원격지 컴퓨터 리소스에 접근하려 했을 때 Java Security Exception이 발생하는 화면이다.

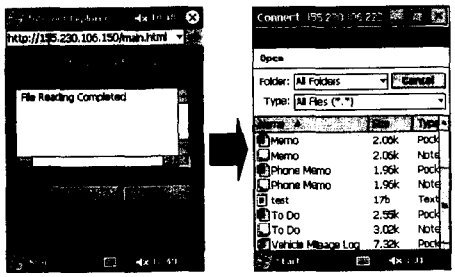


[그림 4] Java Security Exception 발생 화면

File Policy에 관련된 권한이 없어서 발생한 Security Exception의 내용은 아래와 같다.

```
Exception : java.security.AccessControlException:
access denied (java.io.FilePermission
C:₩test.txt read)
```

④ 그림 5는 Security Manager에서 부여한 권한으로 모바일 디바이스에서 원격지 컴퓨터에 정상적으로 접속한 모습을 구현한 화면이다.



[그림 5] Java Security Policy가 적용된 화면

4. 결론

본 논문에서는 모바일 컴퓨팅 환경에서 웹을 통해 Java Application을 이용하여 원격지 컴퓨터 리소스에 접근 할 경우, 모바일 디바이스 상에 Java Security Permission을 부여함으로서 모바일 디바이스로 원격지 컴퓨터 리소스에 접근이 가능하도록 하였다.

위 접근 방법은 모바일 디바이스에서 네트워크를 이용하여 원격지 리소스에 접근이 가능하고, 유비쿼터스 컴퓨팅 환경에 접목시킬 수 있다.

향후 모바일 디바이스를 이용하여 홈 네트워킹에 산재되어 있는 많은 디바이스를 사용자가 쉽게 접근 할 수 있도록 모바일 컴퓨팅 환경을 위한 Security에 관한 연구가 지속적으로 수행 되어져야 할 것이고, 아울러 모바일 디바이스 사용자가 쉽게 Java Security를 사용 할 수 있게 하는 연구도 병행 되어야 할 것이다.

5. 참고 문헌

[1] Sun Microsystems, "FAQ Applet Security" *http://java.sun.com/sfaq/*
[2] terms, *http://www.terms.co.kr*
[3] securingjava, "The Base Java Security Model: The Original Applet Sandbox" *http://www.securingjava.com/chapter-two/chapter-two-5.html*
[4] Java World, "Understanding the keys to Java security - the sandbox and authentication" *http://www.javaworld.com/javaworld/jw-05-1997/jw-05-security_p.html*