2002년도 대한전자공학회/대한전기학회 시스템 및 제어분야 합동 추계학술대회 논문집(2002.11.30)

Mobile-Grid 환경에서의 통합 보안 모델

강 수 연, 이 승 룡
경희대학교 전자계산학과
전화 : 031-201-2950

Intergrating Security Model for Mobile-Grid

Su Youen Kang, Sungyoung Lee
Dept. of Computer Science, Kyunghee University
E-mail : {onmoon, sylee}@oslab.kyunghee.ac.kr

Abstract

Grid provides integrating system that enables to use distributed computing resource and services as adapts traditional infrastructures to overcome the distributed computing environments. But, computing today is moving away from a restriction of the desktop, becoming diffused into our surrounding and onto our personal digital devices. In such mobile computing environments, users expects to access resource and services at any time from anywhere in such Mobile-Grid computing. This expectation results security issues, since the computing environments is expanded. This paper describes the security challenges in Mobile-Grid computing, explaining why traditional security mechanism fail to meet the demands of these environments. This paper describes policy diriven security mechanism enabled entity to use service and data in trust Mobile-Grid environments and a set of security service module that need to be realized in the Mobile-Grid security architecture, presents a set of use pattern that show how these modules can be used for billing service in a secure Mobile-Grid environments.

I. 서론

컴퓨팅 환경은 초고속 네트워크와 프로세스 성능의 향상으로 인하여 다양한 컴퓨팅 리소스들로 인해 이기종적인 특성을 가진 노드들로 구성된 그리드같은 통합적 분산 환경으로 변화되었다[1]. 이러한 변화는 무선 네트워크 기술과 이동 디바이스의 발전으로 한 단계 더 진보된 컴퓨팅 환경을 맞이하게 되었다. 이동성은 컴퓨팅 환경의 패러다임을 바꾸어 놓았다. 기존의 사용자는 다양한 서비스와 정보를 얻기 위해 컴퓨터가 있는 곳으로 이동하지만 이동 컴퓨팅 환경은 사용자가 원하는 곳 어디서나 온라인상의 다양한 서비스들의 사용을 가능하게 하였다. 사람들은 고정된 데스크탑을 벗어나 비행기, 기차, 거리에서조차 핸드폰이나 PDA를 이용하여 은행, 증권거래, 결재 및 예약 등의 서비스를 이용한다. 이러한 변화는 기존의 PC중심에서 사용자 중심으로의 변화와 고정된 유선 기반의 컴퓨팅 환경의 확장을 나타내고 있다. 하지만 확장된 컴퓨팅 환경에서의 편리함과 융통성은 한 가지 사실을 가정하고 있는데 이는 신뢰성 있는 보안 정책기반의 컴퓨팅 환경이다. 만약 누군가 핸드폰을 이용하여 결재를 한다면, 이 과정에서 사용자는 중요한 개인적인 정보들을 전송하게 된다. 이때 실수로 사용자의 개인 정보나 신용정보 등이 유출되어 큰 피해를 입게 된다면 이 사람은 이동 기기를 사용한 서비스 사용을 꺼리게 될 것이다[2]. 하지만 기존의 유선 환경 기반의 보안 메카니즘은 이동 컴퓨팅 환경의 자원 제약적인 특성상 적용하기가 어려우므로 새로운 보안 모델이 필요하다. 또한 현재 이동 컴퓨팅 환경은 분산된 이기종적 이동 디바이스간의 통합을 위해 자동차 내에서의 제어 유닛을 이용한 텔레메틱스나 가정에서의 홈 네트워크뿐만 아니라, 다양한 이동 디바이스들 간의 통합적 플랫폼 등의 이동 분산 환경에서의 통합을 위해 많은 노력을 기울이고 있다. 이를 위해 이동 분산 환경의 보안 모델은 유선 기반의 분산 컴퓨팅 환경에서의 요구사항들도 고려해야 한다[3].

본 논문에서는 이동 컴퓨팅 환경에서의 편리하고 유

용한 서비스의 안전한 사용과 사생활 보호를 위해 이동 환경의 고유한 특징과 분산 환경과의 공통적 특징을 모두 고려하여 이동 분산 컴퓨팅 환경에 적용 가능한 사용자 중심적인 보안 정책과 이동 환경에서 필요한 보안 서비스에 대해 정의하고, 자원 제약적인 이동 환경에 적용 가능한 보안 기술들을 사용하여 확장된 컴퓨팅 환경을 위한 신뢰성 있는 보안 모델을 제시한다.

II. 관련연구

2.1 엑스닷컴-M-월릿페이펄 서비스

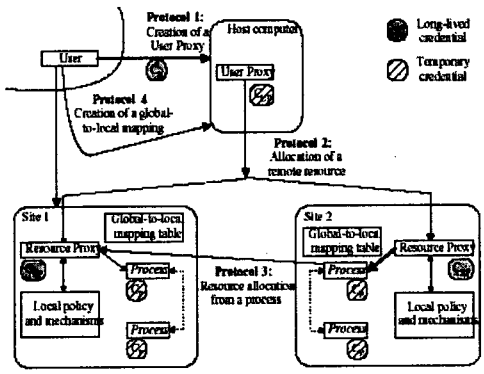
엑스 닷컴은 330만 명 이상의 고객을 확보한 최대의 보안 지불 네트워크를 제공하고 있다. 엑스닷컴의 개념은 매우 단순하다. 서비스 사용자와 제공자가 각각 페이펄에 계정을 만들고, 사용자는 사용한 서비스에 대한 지불은 페이펄과 서비스 제공자 사이에 이루어진다. 때문에 사용자는 자신의 정보를 교환하지 않고 원하는 서비스를 사용할 수 있어 계좌 번호나 주민번호 같은 중요한 자신의 개인 정보가 유출될 위험을 덜게 된다. 또한 서비스 제공자 또한 페이펄을 통해서 결재가 이루어지므로 사용자의 부인봉쇄를 막을 수 있다. 이러한 방법은 사용자와 제공자 모두에게 보안에 대한 불신을 덜어주게 된다. 하지만 이러한 서비스는 단순히 결재를 위한 보안 방법으로써 다양화된 이동 통합 환경으로의 적용을 위해서는 분산 환경에 특징을 고려한 서비스가 필요하다.

2.2 도코모의 I-Mode의 보안 서비스

도코모는 도코모 네트라고 하는 기밀성 보장이 높은 사설 네트워크 망처럼 폐쇄된 도코모의 서버 안에서 운영되기 때문에 일반 인터넷에 비해 신뢰성이 높다. 그리고 각각의 사용자에게 전화번호를 이용하여 ID가 생성되고 한 대의 단말기 이외에는 접속이 불가능하기 때문에 패스워드나 아이디를 훔쳐 악용하는 행위를 막을 수 있다. 또한 단말기 분실로 인한 개인 정보의 유출을 막기 위해 ' i모드 잠금' 이라고 하는 보안 기능이 장착되어 있어 간단한 조작으로 사용자 이외의 디바이스를 통한 보안 위험성을 줄일 수 있다. 때문에 I모드의 사용자층은 계속 확대되어 가고 있는 추세이다. 하지만 I모드는 단말기를 중심으로 서비스가 이루어지고 있어 기타 다른 이동 디바이스에 대한 보안 정책에 대한 고려가 부족하다.

2.3 글로버스 보안 서비스

그리드 에서는 여러 지역 참여 노드들로 구성되어있다. 때문에 다양한 자원 공유와 여러 계층적 커뮤니케이션이 일어나게 된다. 이러한 대규모적 분산 시스템 내에서는 기존의 보안 서비스와는 다른 복잡한 메커니즘이 필요하다. 우선 서비스를 제공받는 사용자의 신원 확인을 위한 인증, 또한 다수의 특정 사용자를 위한 허가, 대규모의 네트워크 안의 다양한 노드들의 관리하기 위한 계정관리, 뿐만 아니라 대용량의 자원의 사용에 대한 모니터링과 기록을 위한 감사 등 다양한 기능들을 포함하고 있다. 그리드 미들웨어인 GLOBUS의 보안 아키텍처는 이러한 기능들을 위해 GSI(Grid Security Infrastructure)를 구현하고 있다. 이는 기존의 인프라를 최대한 변경하지 않고 사용할 수 있도록 공개키 기반구조와 SSL 프로토콜을 이용하고 있다. 하지만 그리드 에서는 아직 이동환경을 위한 보안 서비스를 고려하지 않고 있어 이에 대한 연구가 필요한 실정이다. 아래 그림은 글로버스의 보안 구성도 이다.



[그림 1] 글로버스 보안 구성도

III. 이동 분산 환경의 통합 보안 모델

3.1 이동 분산 환경을 위한 보안 서비스 및 정책

사용자에게 더욱더 편리한 서비스를 제공하기 위해 이동 컴퓨팅 환경은 통합적 시스템 구현을 위한 다양한 시도가 이루어지고 있다. 하지만 이러한 편리한 시스템이 구축되더라고 개인정보의 보호와 안전한 서비스의 보장이 없다면 이는 무용지물이 된다. 때문에 안정되고 명확한 보안 정책은 이동 컴퓨팅 환경의 확장을 위해 꼭 필요한 요소이다. 만약 디바이스 및 서비스 사용의 안전성과 사생활 보호 문제가 해결되지 못한다면, 이러한 편리한 시스템들은 무용지물이 되어버린다.

아래의 내용은 이러한 문제점을 고려하여 이동 컴퓨팅 환경에서 요구되어 져야할 보안 서비스이다.

- 무선네트워크상의 전송되는 데이타의 기밀성
- 이동디바이스 분실시 사용자 정보의 무결성
- 이동 환경에서의 서비스사용을 위한 상호인증
- 유료서비스 사용시의 부인 봉쇄

▪ 이동 디바이스의 가용성

이러한 서비스들이 이동 분산 환경에서 상호 협력적으로 이루어지기 위해서는 이동 분산 환경의 특성을 고려한 명확한 정책이 필요하다. 먼저 분산 환경의 특징으로는 기존의 지역 노드들이 사용하고있는 보안 인프라(Kelberos, PKI)가 존재하므로 이러한 시스템을 무시하고, 전혀 새로운 시스템을 구축하는 것은 비용적인 측면에서 매우 비합리적이다. 때문에 현재 사용되고 있는 기반 시스템들을 기초로 한 통합적인 서비스의 제공이 필요하다. 또한 유선 기반의 분산 환경의 이동 환경으로의 확장된 컴퓨팅 환경에서의 상호 연동성은 유연한 보안 정책을 위해서 꼭 필요한 특성 중 하나이다. 또한 이동 환경의 자원 제약적인 특성을 고려한 개인화된 프로파일특성을 해야 한다.

- 다중 접근권한 정책 (Certification Policy)
- 프록시 정책 (Proxy Policy)
- 개인화 정책 (Privacy Policy)
- 매핑 정책 (Mapping Policy)

위의 정책을 살펴보면, 우선 다중 접근 권한 정책은 다양한 서비스를 위한 다중의 보안 관리 영역의 편리한 접근을 위하여 지역 보안 정책과 글로벌 보안 정책으로 구분된 접근 권한 정책이 필요하다. 예를 들어 Kerberos 원리나, 유닉스 시스템에서 지역 아이디 권한을 가지고 있는 사용자는 지역 보안 관리 정책을 사용하게 된다[8]. 이를 통해 파일이나 디스크 등의 접근 권한을 얻게 된다. 이동 환경에서는 이외에도 디바이스 분실로 인한 사용자 정보의 유출을 막기 위해 디바이스 아이디 통해 사용자의 아이디를 보호하도록 한다. 또한 프록시 정책은 다양한 자원들로의 접근의 편리성을 위해 여러 번의 인증을 과정을 막기 위해 프록시 정책을 사용한다. 사용자는 프록시 인증서를 생성하여 사용자가 여러 번의 인증과정을 거치지 않고도 자원을 사용할 수 있도록 한다. 단 프록시를 통한 거부된 사용자의 접근 권한을 막기 위해 유효 기간을 설정하도록 한다. 이상의 정책들은 기존의 분산 환경에서의 보안 문제점을 위해 공통적으로 적용될 수 있다. 하지만 이동 환경에서 고려해야할 또 하나의 문제점은 디바이스 분실로 인한 사용자 정보의 유출이다. 이러한 문제를 해결하기 위하여 기본적인 사용자 아이디 이외에 디바이스 아이디를 생성하여 디바이스 아이디를 통해서 서비스나 자원 사용이 가능해 지도록 한다. 사용자의 정보는 디바이스 아이디를 인증만 할 뿐 디바이스에 저장되어 이용할 필요가 없다. 그리고 이동 환경의 가장 큰 특성인 자원 제약적인 디바이스들에 알맞은 개인화된 정책사용으로 사용자 환경의 수용능력과 요구사항에 따른 보안 정책을 따르도록 한다. 이외에도 매핑 정책은 이러한 여러 정책들을 관리하고 서로 상호 호환될 수 있도록 관리하는 역할을 한다. 이러한 여러 가지 정책들을 이용하여 실행되는 보안 서비스 모듈은 다음절에서 상세하게 기술하도록 하겠다[6][7].

3.2 통합 보안 모델의 서비스 모듈

앞의 절에서 이동 분산 환경의 보안 정책에 대해서 정의하였다. 이러한 정책을 기반으로 이동 디바이스나, 통합적 이동 플래폼에서 서비스나 정보를 제공받기 위한 보안 서비스 모듈들로는 인증 서비스, 어트리뷰트 서비스, 권한 맵핑 서비스, 권한 대행 서비스들이 있다. 아래의 내용은 이 서비스들에 대한 기능들에 대한 설명이다.

■ 인증 서비스

암호나 디지털 서명을 위해 공개키 암호를 사용하는 대부분 RSA 알고리즘을 사용하지만 RSA를 위한 비트 길이는 최근 수년 동안 증가되어 왔고, 이것은 자원 제약적인 이동 디바이스에게 매우 많은 양의 처리 시간과 자원을 요구하게 된다. 이러한 문제는 온라인 상 서비스 사용을 위해 안전한 거래를 요구할 때 자주 일어나게 된다. 분산 이동 컴퓨팅 환경에 알맞은 XML인증 방식을 이용한다. 이때 사용가능한 서명방식은 RSA, DES, HMAC 알고리즘을 인증자로 이용 할 수 있다. 아래 코드는 HMAC을 이용한 XML서명 이다.

```
<Signature>
<SignedInfo>
 <CanonicalizationMethod Algorithm=
  .... >
 <SignatureMethod Algorithm=
  .... >
        <HMACOutputLength>..
        </HMACOutputLength>
 </SignatureMethod >
 <Reference ...>
 </Reference>
</SignedInfo>
...
<Signature>
```

[그림 2] XML-HMAC 인증 코드

■ 어트리뷰트(Attribute) 서비스

이동 환경에서의 사용자는 서비스를 사용하기에 앞서 자신을 확인시키는 인증과정이 필요하다. 그래서 사용자 한사람만이 가지고 있는 유일한 정보를 가지고 있어야 한다. 이러한 도구로는 사용자의 주민번호나, 혹은 차량번호, 단말기의 고유번호, 또는 지문, 홍채 같은 사람의 생체매트릭스 정보 등이 이용 될 수 있는데, 사람의 생체인식 정보나 주민번호는 도난 시 매우 큰 위

험이 발생할 수 있다. 따라서 차량 번호나 단말기의 고유번호 정보 등을 이용하여 자신의 어트리뷰트 문서를 생성시킬 수 있다. 이를 통해 사용자는 서비스 제공자에게 자신이 누구임을 확인 시켜주게 된다.

■ 서비스 제공자와 사용자간의 접근권한 맵핑 서비스

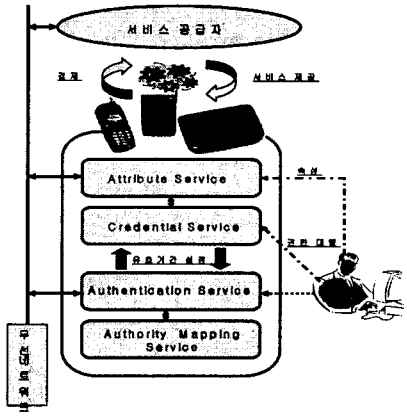
각각의 디바이스는 자신의 고유한 특성에 맞는 프로파일 보안 메카니즘이 존재하게 된다. 따라서 디바이스 사용자가 상위 계층의 서비스를 필요로 하거나, 디바이스 프로세서를 통해 작업을 해야 하는 경우 자신의 디바이스 권한과 상위의 글로벌 네트워크 그룹 안에서의 권한 맵핑이 필요하게 된다. 이때 사용자의 아이디와 패스워드 정보 등의 디바이스 고유의 정보를 통해 권한 맵핑을 이루게 된다. 이때 고려해야 할 점은 디바이스 분실시 사용자의 정보 등이 유출되어 원하지 않는 작업을 수행하게 된다면 그로 인한 피해는 매우 클 것이다. 단말기에서는 이러한 문제를 해결하고자 사용자 자신의 정보 대신에 단말기 정보를 이용하게 되어 단말기를 분실하더라도 가입국에 의해 단말기의 사용이 금지되어질 수 있다.

■ 사용자 권한 대행 서비스

사용자가 작업을 수행할 때 모든 작업마다 프로세스가 승인을 받고 수행한다면 심각한 오버헤드가 예상된다. 때문에 프로세스는 사용자의 권한을 가지고 마치 사용자 인 것처럼 서비스를 자원이나 서비스들에게 접근 할 수 있게 된다. 이때 고려 할 점은 사용자가 프로세스를 통해 권한 대행을 하고 있는 도중 디바이스 분실하면 획득한 제 3자에 의해 오용될 수 있다. 때문에 유효기간이 있는 권한 대행을 실행하게 된다. 만약 유효기간이 지난 후에도 작업이 완료되지 못하면 이 프로세스는 다시 사용자에게 패스워드와 아이디를 묻게 될 것이다.

IV. Moblie-Grid 보안 결재 시나리오

이동 환경에서 가장 유용하게 쓰이는 서비스 중 하나가 바로 결재(Billing)과정이다. 결재 과정은 통합 보안 모델의 4가지 서비스를 통해 이루어지게 된다. 아래 그림을 살펴보면, 사용자는 모바일 다바이스에게 인증을 받고 서비스 사용을 위해 속성값을 설정하게 된다. 이때 인증 서비스는 사용자의 아이디와 패스워드를 확인하고 사용자에게 디바이스 사용 권한을 허락한다. 사용자는 원하는 서비스를 수행하기 위해 프로세스들은 사용자의 권한을 대행하여 사용자로부터 불필요한 인증 과정을 줄여주게 된다. 하지만 디바이스 분실시 이를 악용할 수 있으므로 프로세스가 가지는 권한은 사용자가 임의로 정하거나 기본값을 설정으로 제한적이다.
서비스 공급자는 결재 대행 서비스를 이용하거나 혹은 직접적으로 소비자와 결재처리 과정을 거치게 된다. 이때 제공자는 사용자의 속성 값과 디바이스의 프로세스의 대행권한의 유효기간을 확인하고 서로 통신하게 된다.



[그림 3]Mobile-Grid 보안결재 서비스구성도

V. 결론

보안 문제는 기술 이상으로 중요한 이슈이다. 그리고 프라이버시 문제는 보안 문제 이상으로 중요한 이슈이다. 프라이버시는 사업의 윤리적 중심이다. 또한 정보가 어떻게 수집되었는가 보다는 어떻게 쓰여 지는가와 보다 밀접한 연관성을 지니고 있다. 다른 컴퓨터 기술들과 마찬가지로 보안 기술도 항상 변화하고 있다. 컴퓨팅 자원이 사용되는 목적이나 상황에 따라 보안 등급이 달라지기 때문에 적절한 보안 기술들을 적용하여 자신이 원하는 서비스를 제공하고 제공받게 된다[4].
앞으로 컴퓨팅 환경은 더욱 확장될 것이고 이때의 보안 서비스는 필수적이다. 이러한 변화된 컴퓨팅 환경에서는 범용적 이고 명확한 보안 정책이 필요하다. 이러한 정책들은 언제, 어디서나 컴퓨팅 자원의 사용이 가능한 환경에서 매우 중요한 요소가 된다. 때문에 향후 이러한 환경에 적용 가능하도록 정책을 수정하고 보안하고, 새로운 환경에 알맞은 사용자의 다양한 입력 정보를 통한 보안 인터페이스 연구가 필요하다.

참고문헌

[1] Andrew S.Tanenbaoum, " Ddistributed Systems Principles and Paradigms" , Prentice Hall, 2002.
[2] M. McCarthy, S. Cambell "Security Transformation", McGraw-Hill 2001.
[3] R. Kalakota, "The Mobile Economy", McGraw-Hill 2002.
[4] Ken SAKAMURA "Ubiquitous Computer Kakumei", Kadoka Washoten 2002