모바일 응용 서버의 보안 정책 연구 및 구조 설계

김수형[0] 김중배
한국전자통신연구원
(lifewsky[0], jjkim)@etri.re.kr

A Study and a Design of Mobile Application Server Security Framework

Soo-Hyung Kim[0] Joong-Bae Kim
Electronics and Telecommunications Research Institute

요 약

유·무선 통합 모바일 응용 서버를 위한 보안 구조는 무선 단말의 제한적 리소스와 무선 네트워크의 간헐적 단절성 등과 같은 무선 환경의 제약 사항과 기존 유선 응용과 연동하기 위한 연동 처리 부분 등을 고려하여 설계 되어야 한다. 본 논문에서는 모바일 응용 서버의 보안을 위해 고려해야 할 보안 정책들을 정의하고 그 정책들을 서버 내에서 원활하게 수행하기 위한 보안 구조에 대해 논의하고자 한다.

1. 서 론

무선 단말과 무선 네트워크의 기술 발전에 따라 무선 단말의 사용 범위가 점차 기존 유선 인터넷의 영역으로 확대되고 있으며, 2005년까지 전 세계적으로 10억의 사용자가 무선 단말을 통하여 인터넷에 접속할 것으로 보고되고 있다[1]. 인터넷 사용자의 접근 네트워크가 유·무선으로 다양화 되고, 무선 환경에서의 비즈니스 요구가 발생하며, 좀 더 다양한 무선 응용 서비스에 대한 수요가 증가해감에 따라 이를 지원하기 위한 응용 서버가 무선 인터넷 사용자의 단말적 특성과 네트워크 특성을 고려하여 연구되고 있으며 해외에서는 일부 솔루션을 제공하는 제품들이 이미 개발되어 소개되고 있다.

본 논문은 모바일 응용의 적용 범위를 확대하기 위해서 반드시 요구되는 사용자 인증, 종단간 보안, 접근 제어 등과 같은 보안 서비스를 모바일 응용 서버 내에서 어떤 정책을 가지고 적용할 것인가를 논의하며, 논의된 보안 정책을 바탕으로 모바일 응용 서버 내에 어떻게 구현할 것인지를 소개하고자 한다.

2. 관련 연구 동향

무선 인터넷의 사실상 업계 표준인 WAP 보안에 있어서의 전통적인 문제점은 WAP 게이트웨이의 사용으로 인해 파생된 종단간 보안의 어려움(Security hole)에 있었다[2]. 이러한 문제점은 WAP 포럼에서 제안된 WTLES(WAP Transport Layer End-to-end Security)[3]나 응용 레벨에서의 접근 방법을 통하여, 아직까지는 해결해야 할 난제가 존재하나, 일정 수준 보완되고 있다.

kSSL("kilobyte" SSL)[4]은 무선 단말에서 경량화된 SSL을 사용하여 무선 단말과 서버 간의 종단간 보안을 가능하도록 하도록 한다. 유선 네트워크에서 사용되는 SSL 암호화 알고리즘들 중에서 빈번하게 사용되는 암호화 알고리즘들 만을 채택하여 제공하며 선택사항인 사용자 인증 메커니즘을 제공하지 않는 등의 방법으로 SSL 수행 모듈의 크기를 줄이고, SSL 프로토콜 상에서는 세션 아이디에 기반하여 마스터 키를 재 사용하는 방법을 통해 공개키 계산을 수행하지 않고 클라이언트 서버간의 세션 설정 시간을 단축시키는 방법 등을 제시한다.

서버에 접근하는 무선 단말 사용자의 인증을 위해서 Kerberos 인증 프로토콜을 사용하는 연구도 있는데[5], KDC(Key Distribution Center)와 사용자 단말 사이에 WAP 게이트웨이와 같은 proxy 서버를 두고 사용자 단말에서의 CPU 한계 때문에 발생하는 어려움을 proxy 서버를 통해 극복하는 방법 등을 제시하고 있다.

3. 모바일 응용 서버

본 연구는 모바일 응용 서버에서의 보안 정책과 구조에 대해 논의하고자 하므로 모바일 응용 서버에서 고려해야 할 사항 및 보안과 관련된 몇 가지 응용 서버 모듈에 대해서 소개하고자 한다. 덧붙여서, 기존에 이미 개발되었거나 개발 진행중인 여러 모바일 응용 서버가 존재하지만 본 연구는 유·무선 통합적인 구조의 모바일 응용 서버[6][7]를 바탕으로 하고 있으므로 이와 관련된 내용을 설명한다.

유·무선 통합 모바일 응용 서버 기술 개발 시 고려해야 할 사항으로는 크게 세 가지가 있다. 첫 번째는 무선 단말의 제약 사항에 관한 것으로, 메모리 크기 및 단말의 계산 능력과 같은 열악한 소프트웨어 구동환경, 스크린의 제한된 크기, 입력 수단의 비효율성 등과 관련된 제약 때문에 발생할 수 있는 프로토콜 처리 문제, 세션 유지 문제, 데이터 표현 문제 등을 고려해야 한다. 두 번째는 무선 네트워크와 관련된 것으로, 상대적으로 낮은 대역폭과 간헐적으로 연결이 단절되는 문제로 인한 세션 유지 및 최적으로 데이터를 전송할 수 있는 방법에 대해 고려해야 한다[8]. 세 번째는 기존 시스템과의 연동에 관한 것으로, 레거시 시스템 및 기존 응용 서버와 연동함으로써 보다 다양한 서비스를 무선 단말 사용자에게 제공하는 것을 고려해야 한다.

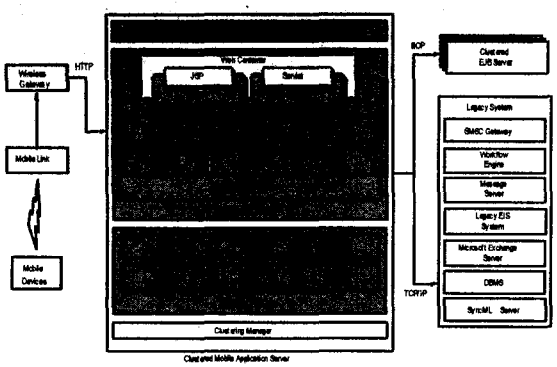

그림 1 모바일 응용 서버 전체 구성도

그림 1은 앞서 언급한 세가지 고려사항을 만족 시켜줄 수 있는 유·무선 통합 모바일 응용 서버의 전체 구성도 이다. 크게, 다양한 모바일 단말기와 무선 네트워크의 간헐적 연결 단절성 등을 처리하기 위한 모바일 환경적응 기술 부분과 기존의 레거시 시스템과 연동하여 확장성을 제공하기 위한 유·무선 연동처리 기술로 구성되어 있다.

전체 모바일 응용 서버 구성 모듈 중에서 보안 관리자와 직접적으로 관련된 모듈들은 세션 관리자와 프로파일 관리자를 들 수 있는데, 무선 네트워크의 간헐적 단절성 문제 등을 처리하기 위한 세션 관리자[6]는 사용자 보안 컨텍스트를 기타 세션 정보와 함께 안전하게 관리하여 보안 관리자에게 필요한 정보를 제공하는 서비스를 제공할 수 있으며, 메모리, 화면 크기, 키보드 타입 등과 같은 컨텐츠 변환을 위한 사용자 단말기의 특성 정보, 컨텐츠 변환기로부터 생성된 변환 프로파일 정보, 사용자 정보 등을 관리하는 프로파일 관리자(Profile Manager)[6]는 접근 제어나 보안 컨텍스트 관리 정책에 필요한 사용자 권한 정보 등을 제공할 수 있다.

3. 보안 정책

유선 환경에서의 응용 서버와 마찬가지로 모바일 응용 서버에서의 보안 정책은 전체 응용 서버의 보안 구조를 설계하는 바탕이 된다. 따라서 본 연구는 모바일 응용 서버의 보안 구조를 설계하기에 앞서, 모바일 응용 서버에서의 보안 정책에 대해 논의 하고자 한다.

응용 서버 구축 사유나 전체 네트워크 토폴로지 등이 사용자 인증 방법, 접근 제어 방법, 레거시 시스템 보안 연동 등과 관련된 보안 정책을 결정하는 기준이 된다고 볼 때, 기본적으로 비즈니스 서비스 제공을 목적으로 하면서 다양한 레거시 시스템 연동 방법을 제시하는 유·무선 통합 모바일 응용 서버에서 고려해야 할 보안 정책 요소들은 다음과 같이 정의될 수 있다.

사용자 인증과 관련된 부분은 무선 환경과 사업자의 보안 요구 사항 변화에 적합하도록 (1)기존 유선에서의 다양한 인증 매커니즘들을 그대로 제공할 수 있는 구조를 갖되 무선 환경에 특화된 인증 프로토콜인 경우에도 플러그 인 구조를 제공하여 서비스할 수 있도록 한다. 다양한 인증 방법을 제공하는 구조에서는 시스템 내 보안 처리를 위해 공통된 보안 컨텍스트 흐름이 보장되어야 하는데, 이는 외부 시스템과의 연동을 위해서 뿐만 아니라 사용자들에 대한 일관성 있는 보안 체계를 적용하기 위해서이다. 본 연구에서 보안 대상으로 고려하고 있는 모바일 응용 서버는 하나의 서버 내에 다양한 서비스 및 레거시 시스템 연동 방법을 제공하므로 (2)사용자 별 혹은 사용자 그룹 별 접근 제어 방법을 제공하여야 한다. 응용 서버는 기본적으로 비즈니스 로직의 수행을 고려하고 있으므로 사용자에 대한 접근 제어 방법 제시는 필수적이라 할 수 있다. 레거시 시스템과의 연동을 위해서는 (3)별도의 레거시 시스템 사용자 인증 방법을 적용할 수 있어야 한다. 레거시 시스템은 이미 구축된 인증 체계가 존재할 수 있으므로 그에 준수하는 인증 방안이 제공 되어야 한다. 그리고 마지막으로 모바일 네트워크의 간헐적 연결 단절성과 같은 안정적이지 못한 네트워크 상황을 고려하여 (4)사용자 재 인증 여부 등을 컨트롤 할 수 있는 보안 관리자와 세션 관리자와의 연동 부분을 고려해야 한다.

위에서 정의한 정책 요소들은 모바일 응용 서버 내에서 하나의 보안 정책 관리자에 의해서 관리되도록 한다. (5)정책 관리자는 서비스 특성에 따라 혹은 서버 운영자의 관리 정책에 따라 인증, 접근 제어, 레거시 시스템 연동과 같은 통일된 보안 정책을 갖는 도메인들을 구성하고 관리할 수 있도록 하며 배포 툴에서 규정되는 보안 정보들을 바탕으로 서버에서 필요로 하는 모듈들을 생성하고 관리할 수 있도록 한다.

4. 보안 구조 설계

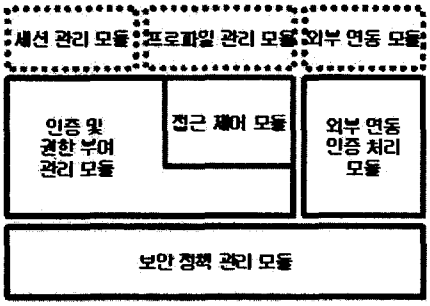

그림 2 모바일 응용 서버 보안 모듈 구성도

앞서 설명한 보안 정책을 수행하도록 하기 위해 본 연구에서는 그림 2와 같은 모바일 응용 서버 보안 모듈들을 구성하였다. 그림 2에서 구성된 보안 모듈 이외에 모바일 응용 서버에서 추가로 필요한 보안 요소는 기타 응용 측 보안 서비스를 제공하기 위하여 암호화 함수 라이브러리 등의 응용을 위한 보안 모듈들이다.

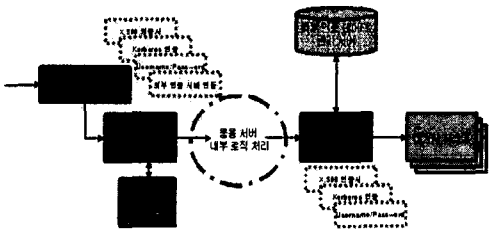

그림 3 모바일 응용 서버 보안 모듈 흐름도

그림 3은 모바일 응용 서버 내에서 보안 컨텍스트의 흐름도를 나타낸다. 인증 처리 모듈에서 외부 요청에 대한 다양한 인증 방법에 대한 인증 요청을 처리하고 인증이 정상적으로 완료되면 사용자 정보, 인증 정보, 접근 권한을 바탕으로 보안 컨텍스트를 구성한다. 구성된 보안 컨텍스트는 응용 서버 내 루틴을 따라 전달되어, 필요 시 접근 제어나 내부 응용 루틴에서 사용되며 외부 레거시 시스템 연동을 위해서 사용될 수 있다. 사용자 보안 컨텍스트는 사용자 정보, 인증 정보, 접근 권한 정보, 레거시 시스템 보안 연동 정보 등으로 구성되며 응용을 위해 필요한 보안 컨텍스트 접근 API를 제공한다.

종합하면, 모바일 응용 서버의 보안 관련 모듈은 그림 2와 같이 보안 정책 관리 모듈, 인증 및 권한 부여 관리 모듈, 접근 제어 모듈, 외부 인증 처리 모듈 등으로 구성되며, 아래에서 설명되는 바와 같은 역할을 수행한다.

4.1 보안 정책 관리 모듈

보안 정책 관리 모듈은 사용자 인증, 접근 제어, 레거시 시스템 연동 방법 모듈 등의 전반적인 보안 정책을 구성하고 서비스 및 어플리케이션의 보안 관련 도메인을 형성할 수 있도록 한다. 보안정책은 관리자에 의해 XML 파일로 기술할 수 있도록 하고 이는 배포 툴에서 종합적으로 관리되도록 한다.

4.2 인증 및 권한 부여 모듈

사용자에 대한 인증은 응용 서비스와 무선 단말기, 무선 사업자의 보안 인프라에 따라 다양한 방법으로 수행될 수 있으므로 다양한 인증 메커니즘을 지원할 수 있는 구조를 제공하여야 한다. 따라서 ID/Password, Kerberos, X.509 인증서 등의 기본적인 인증 처리 모듈을 제공하며 특정 무선 인증에 특화된 인증 서비스를 가능하게 하기 위해 플러그인 구조를 갖는다. 무선 단말과 서버 간의 인증 프로토콜 수행 과정에서 프락시 서버의 역할이 있을 수 있으나 이는 앞서 기술한 기존 인증 처리 모듈에서 처리하거나 특화된 인증 처리 모듈에서 처리할 수 있다. 추가로, 통신 사업자가 응용 서버로의 사용자 접근 전에 독자적인 인증을 수행하고 통신 사업자의 서버와 응용 서버간에 신뢰성 있는 통신 채널이 설정되어 있다면, 응용 서버에서 인증 과정을 생략하기 위해, 이미 인증된 정보의 안전한 보안 컨텍스트 전파 (Propagation)를 처리할 수 있는 모듈이 필요로 할 수 있다.

사용자 인증이 정상적으로 이루어진 시점에서 모바일 네트워크의 간헐적 단절성을 고려하여, 보안 컨텍스트를 세션 매니저에 위임하여 관리되도록 하여 사용자의 인증 부담을 덜어 줄 수 있는 방법을 제공한다. 또한 사용자 요청 메시지에서 보안에 필요한 사용자 정보를 얻기 위해 프로파일 매니저로부터 필요한 정보를 요청할 수도 있다.

4.3 접근 제어 모듈

응용 서버는 무선 비즈니스 영역의 서비스를 기본적으로 고려하고 있으므로 접근 제어 모듈은 사용자의 응용 로직 처리 루틴 접근 가능 여부와 레거시 시스템 접근 가능 여부를 판단할 수 기능을 제공하며, 이를 위해 관리 정책과 사용자의 접근 권한에 대한 정보를 사용한다.

4.4 외부 연동 보안 모듈

외부 연동 보안 모듈의 기본적인 기능은 외부 연동 시스템에 보안 컨텍스트를 전파하는 것이다. 하지만 이미 구축된 인증 서비스 및 보안 서비스를 가지고 있는 레거시 시스템으로의 사용자 접근을 위해서는 그에 적합한 인증 처리 루틴이 필요로 할 수 있다.

별도의 사용자 인증이 필요한 경우, 레거시 시스템 접근을 위한 사용자의 인증 정보를 보호하기 위해 외부 보안 서버에 필요한 정보를 저장할 수 있다. 이를 위해, 보안 서버와 연동하여 레거시 시스템에 대한 사용자 인증을 수행하는 구조를 필요로 할 수 있다.

5. 결론 및 향후 연구

무선 통신 단말과 무선 네트워크의 발달이 전체 유선 서비스의 무선 서비스로의 전이를 의미하는 것은 아닐 것이다 무선 서비스는 단말을 통한 사용자의 의사 전달에 대한 어려움, 사용자에게 전달되는 정보량의 한계, 사용자의 이동성(mobility)과 접근 편이성 등에 기반하여 좀 더 사용자 중심적인 형태로 제공되지 않을까 생각한다. 이러한 서비스가 업무와 관련된 비즈니스를 로직을 처리하기 위해 제공될 수도 있고 생활의 편의성과 활력을 위한 콘텍츠를 제공하기 위해서 일수도 있다. 여기서 중요한 것은, 무선 환경에서 제공되는 서비스가 단순한 정보의 브라우징을 제공하는 것에서 벗어나기 위해서는 유선과 마찬가지로 보안의 큰 틀 속에서 보호되어야 한다는 것일 것이다.

본 연구는 모바일 서비스 제공자의 위와 같은 다양한 서비스 제공 요구를 만족시켜줄 모바일 응용 서버에서의 보안 특성과 정책 그리고 구조에 대해 소개하였다.

향후 과제는 레거시 시스템과의 연동 부분에서의 안전한 사용자 인증 정보 관리 방법에 대한 연구가 필요할 것으로 보이며, WTLES를 위해 WAP 스택을 일부 응용 서버 구조에 포함시키는 등의 무선 특화된 보안 모듈을 적절하게 응용 서버 내에 포함시키는 방법 등이 연구되어야 한다.

6. 참고 문헌

[1] Geoff Johnson, "m-Commerce Scenario," Gartner Group, 2001

[2] Ashley P, Hinton H, Vandenwauver M. "Wired versus wireless security: the Internet, WAP and iMode for E-commerce," Proceedings 17th Annual Computer Security Applications Conference. IEEE Comput. Soc., pp.296-306. 2001

[3] "Wireless Application Protocol Transport Layer End-to-End Security Specification," WAP forum, 2001

[4] Vipul Gupta, "Bringing Big Security to Small Device," http://java.sun.com/javaone/javaone2001/pdfs/2246.pdf, JavaOne Conference, 2001

[5] Alan Harbitter , Daniel A. Menascé, "The performance of public key-enabled kerberos authentication in mobile computing applications," Proceedings of the Conference on Computer and Communications Security, pp.78 - 85 , 2001

[6] 김성훈, 장철수, 정승욱, 서범수, 노명찬, 박중기, 이경호, 김중배, "유무선 통합 모바일 응용서버에 관한 연구," 정보과학회지, v.20, n.6, pp.20-31, 2002

[7] 오동익, 이종섭, 이경호, 김중배, "모바일 응용서버의 구조에 관한 연구," 한국멀티미디어학회지 제6권 제 1호, pp.45-55, 2002

[8] Jeffrey M Capone, "Extending J2EE for Mobile Application Development," http://www.oreillynet.com/pub/a/onjava/2001/10/17/mobilej2ee.html, 2001