제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

개방형 서비스 API를 위한 보안모델

이용주*, 최영일*, 이병선*
*한국전자통신연구원
e-mail : silvia@etri.re.kr

A Security Model for Open Service API

Yongju Yi*, Young-il Choi*, Byung-sun Lee*
*ETRI(Electronics & Telecommunications Research Institute,

요 약

개인 정보의 중요성이 커지고, 침입에 대한 기술이 고도화 되어 보안의 필요성이 점점 증가되는 반면, 개방형 네트워크 구조로의 변화는 보안에 더 많은 취약점을 내포하고 있다. 본 논문에서는 개방형 네트워크로의 급속한 변화와 더불어 대두된 개방형 서비스 API 에 대해서 살펴보고, 개방형 서비스 API 보안 모델의 필요성과 현황을 분석하여 요구사항에 대한 모델을 제시하였다. 또한 이미 제정된 보안 모델에서 문제점을 분석하여 앞으로 나아갈 방향을 제시하였다.

1. 서론

인터넷 관련 기술의 급속한 발전으로 데이터, 영상, 화상 등의 다양한 멀티미디어 서비스는 통합 개방형 네트워크로 진화되고 있으며 궁극적으로는 모든 미디어가 하나로 통합되는 NGN(NEXT Generation Network)으로 발전되어 가고 있다.[1] 이러한 개방형 네트워크로의 진화는 경제성과 효율의 증가, 신규서비스의 창출 등 많은 정점을 가지고 있으나 다양한 유무선 통신망의 융합화에 따른 통신망간의 간섭이 증가하고 네트워크 접속점 중심의 통신망간 접속구조가 확대되어 지금까지의 시스템 보안 위주의 단순한 보안기술을 적용하기가 어렵다. 따라서 개방형 네트워크를 효율적으로 보호하는 API 기반의 보안기술이 필요하다. 본 논문에서는 개방형 네트워크 구조에서 보안모델과 API 기반의 보안기술에 대하여 살펴본 후, 요구사항을 분석하여 보안 모델을 제시하고 앞으로의 발전방향을 제시하겠다.

2. 개방형 네트워크와 개방형 서비스 API

시스템의 소프트웨어와 하드웨어를 표준화된 플러그인 들의 집합체 형태로 구성하여 네트워크에 개방성을 부여한 것을 개방형 네트워크라 정의한다. 통신망 사업자로 하여금 가격/ 제품 경쟁력이 있는 여러 벤더들의 제품으로 망구축을 가능하게 하며, 필요에 따라서 망장비 일부 기능의 추가, 교체, 기능 향상을 가능하게 할 것이다. 또한 새로운 신규서비스를 손쉽게 도입할 수 있도록 도와줄 것이다. 그림 1 에서 보는 것과 같이 개방형 시스템은 현재의 수직 구조와는 달리 수평적인 계층 구조를 가지고 있으며 하드웨어와 소프트웨어가 완전히 독립적으로 분리된다.[2]

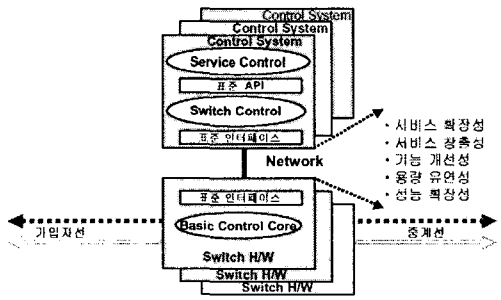

그림 1 : 개방형 네트워크의 구조

개방형 개념은 통신망의 기능에 대한 접근을 가능하게 하는 API(Application Programming Interface) 및 절차에 대한 표준화, 그리고 통신망을 구성하는 교환시스템의 구조 및 통신서비스를 제어하기위한 프로토콜에 대한 표준화를 통해 이루어진다. 이러한 개방형 네트워크 구조를 설계하고 구축할 때 무엇보다 서비스 제공환경에 대한 고려가 필요한데 서비스 제공 환경 측면을 고려해 보면 먼저 서비스 사업자 입장에서는 망의 활용도를 높이기 위한 노력을 기울여야 하며 과

감히 third-party 서비스 솔루션 제공자는 사용자들의 서비스 사용 욕구를 촉진할 수 있는 부가서비스 개발을 진행하여야 한다. 표준화된 개방형 서비스 API 는 바로 차세대 망 구조에 적합한 서비스 제공 환경을 마련해주는 토대가 된다.[3][8]

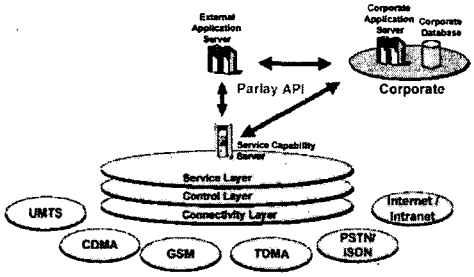

그림 2 : NGN 에서 개방형 서비스 API 의 제공환경

그림 2 에서와 같이 큰 규모의 시장성을 가진 어플리케이션들에 대해서만 관심을 가지는 공중망 사업자들은 소규모의 다양한 서비스를 개발하는 서비스 제공자와 같은 third-party 를 망에 끌어들임으로써, 망의 수입도 올릴 수 있고, 자신들이 개발하지 않는 특정분야의 소규모 서비스를 도입하는데 큰 비용을 투자하지 않아도 된다.

Parlay Group 은 1998 년 3 월 만들어진 비영리 단체로서 공중망 운용자 관리 영역의 외부에 존재하는 어플리케이션을 통신망에서 제공하는 방법을 제시하고 있으며, 소프트웨어 생산자 들에게 다양한 네트워크에 걸친 응용을 개발하도록 하기위한 개방형 구조를 갖는 API 를 정의하고 있다. 규격 정의는 ETSI(European Tel Standard Institute), 3GPP(Third Generation Partnership Project) 등과 공동으로 정의하고, OMG(Object Management Group)의 미들웨어 기술(CORBA)를 채택하고, JAIN(Java APIs for Integrated Network)에서는 Java 언어를 통한 API 의 기술적인 적용을 행한다. 특히 Parlay/ETSI/3GPP 는 Parlay/OSA 규격을 정의하고, Parlay API 는 3GPP 규격으로 재정의된다. 그림 3 은 Parlay API 구현 구조를 보여주고 있다.[4]

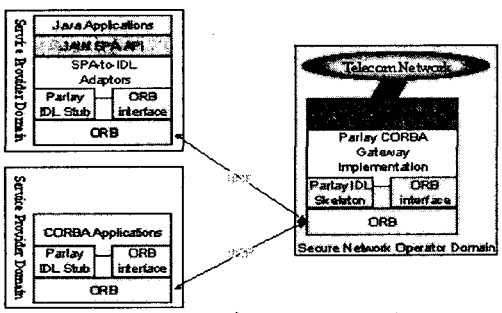

그림 3 : Parlay API Implementation

3. 개방형 API 보안기술

통신 서비스는 Bearer 서비스와 텔레 서비스로 분류된다. 실제 사용자의 데이터가 전달되는 텔레 서비스는 많은 양의 개인적인 데이터를 다루게 되며 하나 이상의 통신 네트워크를 필요로 하게 된다. 텔레 서비스는 터미널 장비나 커미널 노드 안에서 기능을 확장하는데 이는 IN(Intelligent Network)이라 불리는 Value-added service 를 통하여 실현된다. 개인 정보를 보호하기 위한 요구사항은 크게 Confidentiality, Integrity, Availability, Accountability 등으로 나누어 볼 수 있다. 각각의 의미를 따져보면 아래와 같다.

Confidentiality : 정보가 접근허가 받은 사용자에게만 공개된다. Integrity : 정보가 권한 있는 자에 의해서만 변경 될 수 있다. Availability : 권한 있는 사용자가 시스템을 사용 하려할 때 악의적인 목적으로 사용을 방해 받아서는 안 된다. Accountability : 권한 있는 사용자는 보안관련 행동에 대해 책임을 져야 한다.

3.1 보안 모델의 필요성

인터프라이즈 관리는 IT 시스템을 포함한 비즈니스 자산에 대한 책임이 있으므로 결국 시스템으로부터 정보를 보호하는 것이 최종 목표라 할 수 있다. 즉 최소의 경비로 예측 가능한 모든 위협을 막아야 하며 이런 측면에서 시스템을 보호할 수 있는 정보보호정책이 설정되어야 한다. 여기에는 Access, Audit 등에 관한 정책이 추가 되어야 하며 엔터프라이즈 관리는 API 나 미들웨어 레벨의 보안서비스를 사용하기 어려우므로 자체 보안모델이 필요하다. 최종 사용자 측면에서는 시스템을 사용할 권한을 얻기 위해 인증을 먼저 받게 된다. 각각의 사용자는 시스템에서 다른 객체에 접근하여 서로 다른 일을 수행하기를 원하므로 이러한 Access 에 대한 권한을 얻게 된다.

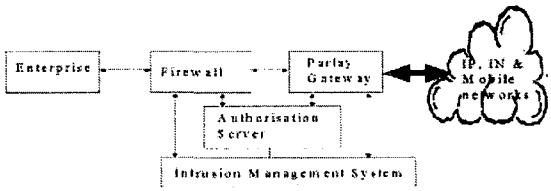

그림 4: Parlay API Security Model

그림 4 는 Parlay Group 에서 정의한 Parlay Security Mechanism 이다. 엔터프라이즈 네트워크와 Parlay Gateway 사이에 방화벽을 이용하여 모든 API 관련 내용을 IP 네트워크 레벨의 트랜잭션 단위로 검증하고, 다른 네트워크 사용자들로부터 사설 네트워크의 자원들을 보호해준다. 방화벽과 Parlay Gateway 사이에는 인증서버와 침입 탐지 시스템 등을 이용하는 구조를 제안하고 있다. 이때 인증 서버는 방화벽에서 검증 받은 함수 호출을 목적지에 전달 하므로서 사용자와 네트워크 기능을 보안등급에 따라 분류하는 기능을 가진다. 게이트웨이나 컨버터 등은 방화벽의 기능을 어플리케이션 레벨의 범위에서 수행하고 침입탐지 시스템은 네크워크 리소스 등에 대한 접근을 제어한다.[7] 또한 MGCP 와 같이 네트워크 계층 프로토콜인 IPSec 처럼 널리 이용되는 보안 인프라를 사용하여 보안 전

문가로부터 검증된 보안 인프라를 사용함으로써 안전성 보장과 개발기간의 단축, 중복투자의 비용을 절감할 수 있다. 이러한 방법은 대부분 응용 프로토콜에서 가장 일반적인 접근 방법으로 이용하고 있으나 기존의 보안 프로토콜을 재사용하는 것을 전제로 하고 있으며 통신용 키 분배 메커니즘이 표준화되어 있지 않으므로 RTP/RTCP 메시지를 보호하기가 쉽지 않다. 또 다른 방법으로는 미들웨어 레벨에서 제공하는 보안 서비스를 이용하는 것이다. 이것은 특정 미들웨어에 의존적이며 미들웨어 레벨에서의 보안은 최상위 레벨의 보안 요구사항에 부족하다.

API 자체의 보안 메커니즘을 사용하여 프로토콜들이 최적의 암호화나 인증방법을 적용할 수 있으므로 보다 효과적인 보안을 제공한다. 각 프로토콜마다 자체의 보안 메커니즘을 따로 설계하는 것은 비효율적이므로 개방형 서비스 API 를 통해 보안 모델을 설계하고 이에 맞는 보안 메커니즘을 제공하는 것이 바람직하다.

4. 개방형 서비스 API 보안 모델

그림 5 에서 보는 것과 같이 Parlay API 는 크게 두 가지 범주의 인터페이스로 구성되는데 외부의 어플리케이션들이 네트워크 기반의 Parlay 서비스에 접근할 수 있도록 해주는 프레임워크 인터페이스와 어플리케이션이 네트워크 기능 및 정보를 광범위하게 접근할 수 있게 해주는 서비스 네트워크 등으로 분류된다.

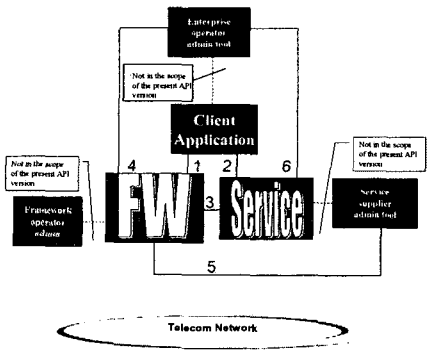

그림 5 : Parlay API 의 구성

프레임워크 API 는 어플리케이션 서버와 프레임워크 간, 혹은 Network Service Capability Server(SCS)와 프레임워크 간의 인터페이스를 제공한다. 현재 Parlay Group 에서 제안한 프레임워크와 어플리케이션 간에 제공되는 보안 메커니즘은 Authentication 과 Authorisation 이다. Authentication 은 오프라인 상에서 등록이 된 후에 어플리케이션이 인증 인터페이스를 통해 인증을 받는 형태이다. 개방형 서비스 API 는 Peer-to-peer 모델을 제시하고 있으며, 다른 API 를 사용하기 전에 받아야 하는 필수 절차이다. 어플리케이션이 프레임워크 API 를 인증 해야 하는지에 대해서는 정책에 따라 달라진다. 필요하다면 상호인증 메커니즘을 사용해야 할 것이다. Authorisation 은 인증을 받은 후에, 인증 받은 사용자가 무엇을 할 수 있는지에 관한 행위에 대한 권한 부여라 할 수 있다. 사용자가 임의의 서비스를 사용하기 위해 사용자 신분을 인증받고, 서비스 사용에 관한 허가를 받게 되며, 모든 것이 성공적으로 끝나면 서비스에 대한 프레임워크 인터페이스를 얻게 된다. 현재 재정된 API Authentication 보안 모델에서는, 보안 도메인 개념을 도입하여 도메인 내의 사용자와 도메인 외부의 사용자로 구분하였다. 보안 도메인 내의 사용자는 특정 인증절차 없이 접근하며 이때 보안 도메인의 정의는 보안 정책 범위에 따라 세가지(Security Policy Domain, Security Environment Domain, Security Technology Domain)로 분류할 수 있다. 각 도메인에 대한 보안 정책은 서비스 제공 업자에 따라 달라지지만 도메인에 대한 명확한 구분과 함께 사용 인터페이스의 구분이 미흡한 실정이다.

Parlay Group 에서 제안하는 API 레벨의 Authentication 실제 모델은 그림 6 과 같다. Authentication A 는 사용자측에서 프레임워크를 인증하고 Authentication B 는 프레임워크 측에서 사용자를 인증하는 상호인증의 형태를 가지는 API 레벨의 인증 모델이다.[6]

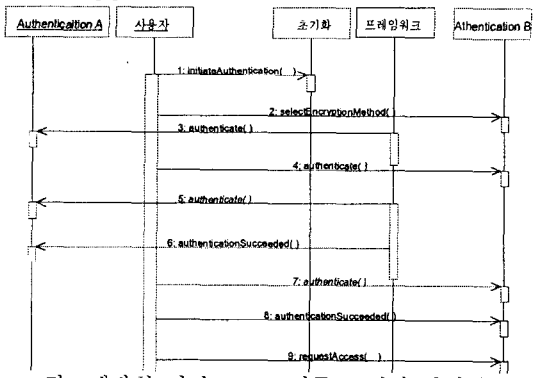

그림 6:개방형 서비스 API 인증 모델의 다이어그램

그림 6 에서 사용자가 먼저 프레임워크의 초기 작업을 한 후에 암호화 메소드 협상작업을 하게 된다. 성공적으로 협상이 된 후에 상호 인증 메소드를 실행하게 되며 이러한 메소드는 상위 인터페이스의 콜백 기능을 비롯한 여러 메소드를 상속 받아 이루어진다. 이 인증 모델의 안정성은 선택되는 암호 알고리즘에 달렸으므로 암호 키의 최소길이 지정 등이 필요하며 개방형 서비스 API 레벨의 보안 모델이라는 점에서 큰 의미가 있지만 리소스 보호 등을 위해 프레임워크에 의해 제어되는 강력한 인증 모델이 필요하다.[9]

현재 Parpay Group 에서 제안하는 보안모델의 수준은 극히 미약하며 시작 단계에 불과하다. 인증 받은 사용자가 자신에게 맞는 Authorication 을 부여 받기 위해서는 Access Control Model 이 필요하다. 즉 각각의 사용자 마다 혹은 객체마다 차별화 된 Authorization 을 제공하기 위해서는 차별화 된 Access Control 정보를 얻을 수 있는 모델이 필요한 것이다. 프레임워크는

두 개의 레이어를 대표할 수 있는 인터페이스를 생성하여 하나는 클라이언트 측의 호출에 관한 Access Decision 을 담당하게 하고 다른 하나는 API 측의 호출에 대한 Access Decision 을 담당하게 하는 모델을 제안한다. 이러한 보안 모델 구조 속에서 각 서비스 제공 업자들은 각각에 맞는 보안 정책을 설정하여 Access Decision 을 이용하여 다양한 기능을 제공할 수 있다. 그리고 이러한 Access Decision 구조와 Audit 를 병행하면 보다 조직적인 보안모델로 발전시킬 수 있다. 그림 7 은 앞서 설명한 구조를 보여주고 있다.

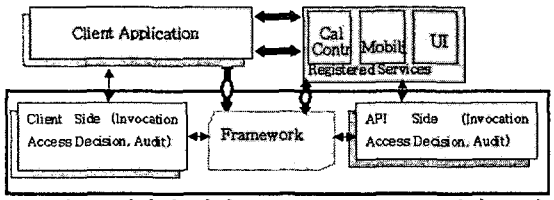

그림 7: 개방형 서비스 API Audit, Access 제안 모델

메시지의 무결성을 위한 메커니즘이 필요하다. 현재 미들웨어 레벨에서 제공되는 메시지 무결성은 각각의 오퍼레이션과 파라미터의 쌍에 타겟 ID, 서비스 정보, 호스트 주소 등의 헤더를 붙여 메시지의 변경 여부를 체크 한다. 이것으로 API 레벨의 메시지 무결성 까지 체크 할 수는 없기 때문에 이를 위한 모델이 제시 되어야 한다.[5]

다음은 Delegation 모델에 대해서 살펴보겠다. 개방형 서비스 API 모델은 객체지향 모델을 기반으로 설계되었다. 객체 기반의 호출과 객체와 객체사이의 통신은 필수이며 하나의 객체가 콜을 완수하지 못한 경우 미리 형성된 콜 체인을 통해 다른 객체에게 위임할 수 있다. 이때 사용되는 콜 체인은 앞서 필요한 Access Control Model 과 조화되어 수행되어야 한다. 체인을 형성하는 각각의 객체에서 Access Decision 이 수행되어야 하며 Privilege Delegation 개념을 이용하여 특정 상황에서 초기와 과정 시 Access control 정보로 체인을 형성하는 객체에게 이에 대한 증거물을 줄 수도 있다. 이러한 방법을 사용하면 보안 도메인을 사용하는 인증 모델과 함께 수행되어 보다 효과적으로 사용할 수 있다.

개방형 서비스 API 를 이용해 여러 서비스 제공업자와 망사업자, 사용자가 공존하는 구조에서 무엇보다 중요한 것이 Non-Repudiation 모델이다. 이는 어떤 행위에 대해 책임을 지게 하는 보안 기능으로서, Accountability 을 제공하기 위한 가장 중요한 보안 기능이다. 특히 API 서비스 레벨의 메소드 실행이 사용자의 요금과 관계되는 환경에서는 필수라 할 수 있다. 믿을 만한 제 3 자를 이용하는 방법도 이용할 수 있으나, 본 논문에서는 현재 개방형 서비스 API 구조에 맞추어 프레임 워크 API 에서 타 서비스 API 와 사용자 사이의 Non-Repudiation 을 제공할 수 있는 구조를 제안하겠다.

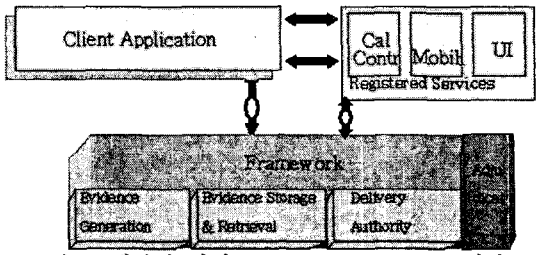

그림 8: 개방형 서비스 API Non-repudiation 제안모델

그림 8 과 같이 서비스 이용 및 메소드 사용과 관련된 증거를 생성 및 검증하는 부분과 저장하는 부분 문제가 생겼을 경우 이를 해결하는 부분 등으로 인터페이스를 나누어 설계할 수 있다. 현재 개방형 서비스 API 에서는 서비스를 사용하기 위한 사용자의 등록을 비롯한 기능들이 프레임워크에 있다. 위의 구조를 따를 경우 기존의 프레임워크에서 제공되는 보안 모델의 구조를 변경하지 않고 타 서비스 API 의 사용과 관련된 모든 행위에 대하여 송/수신 Non-Repudiation 보안기능을 제공할 수 있다.

5. 결론

개방형 네트워크로의 변화로 인해, 필요성이 제기되어 꾸준히 규격이 제정되고 있는 개방형 서비스 API 의 모델과 구조에 대해서 살펴보았다. 개인 정보의 중요성이나 침입에 대한 기술이 점점 고도화 되어 보안의 필요성이 점점 더 커지고 있는 반면 개방형 구조로의 변화는 보안에 더 많은 취약점을 내포하고 있다. 이에 따른 보안 모델이 시급한 실정이며 본 논문에서는 그 필요성과 현황을 분석하여 요구사항에 대한 보안모델을 제시하였다. 또한 이미 규격으로 제정된 보안 모델에서의 문제점을 분석하여 앞으로 나아갈 방향을 제시하였다. 향후 본 논문에서 제안한 모델을 세분화하여 인터페이스와 메소드에 대한 정의를 위한 연구가 요구되며, 각 모델 별로 필요로 하는 보안 정책에 관한 연구도 활발히 진행되어져야 한다.

참고문헌

[1] 이근호, 이송희 외 3 인, "VoIP 를 위한 보안기술 현황과 전망", 한국통신학회비 제 19 권 8 호, 2002.
[2] 강선무, "개방형 네트워크기술의 표준화동향" NONF, Sep, 2002.
[3] 이병선, 최영일 외, "차세대 개방형 네트워크 포럼 보고서", NONF, Dec, 2001.
[4] 김경미, "Parlay Group 기술 표준화 동향", 2002.
[5] OMG "CORBA Security Specification", 2001.
[6] The Parlay Group, "Open Service Access Specification", Dec, 2001.
[7] Reiner Sailer, "Security Service in an Open Service Environment", IEEE megazine, Sep, 2000.
[8] Wolfgang Kellerer, "Intelligence on Top of the Networks", IEEE IN Workshop, May, 2001.
[9] Nevin Heintze, " A model for Secure Protocols and Their Compositions", AT&T Bell Lab Report, Mar, 2002.