유비쿼터스 협업 환경에서의 Capability 기반 접근 제어 방법

한아름, 김강석, 김기형
아주대학교 일반 대학원 지식정보보안학과
e-mail : likeyong6@ajou.ac.kr, kangskim@ajou.ac.kr, kkim86@gmail.com

Capability based Access Control Mechanism in Ubiquitous Collaboration Environment

Areum Han, Kangseok Kim, Kihyung Kim,
Dept. of Knowledeg Information Security, Graduate School Of Ajou University

요 약

IT 기술의 결정체로 불리는 스마트폰은 보급이 확대됨에 따라 진정한 유비쿼터스 환경 구현을 위한 필수품으로 자리 잡아가고 있다. 이로 인해 시간과 장소에 대한 구애 없이 네트워크에 접속할 수 있는 환경이 조성되어 편의성이 극대화 되었지만, 보안 위험성 증가로 인한 문제점도 가지고 있다. 스마트폰을 통해 제공되는 유비쿼터스 협업(Collaboration)은 프라이버시 침해 문제를 야기할 수 있으며, 이를 완화하기 위한 방법으로 다양한 연구들이 진행되고 있다. 본 논문에서는 Capability 기반의 Access Control 을 제안한다.

1. 서론

IT 와 비즈니스가 융합화되고 실공간과 사이버공간의 자연스러운 연결로 인해 업무환경뿐만 아니라 개인의 관심사 및 정보 관리 방안도 디지털 환경에 맞게 점점 더 다양해지고 있다. 또한 스마트폰의 보급으로 인해 이를 이용한 서비스가 빠르게 확산되고 있고 장소와 시간의 제약이 없는 스마트폰의 특성으로 인해 이용자 수는 계속 증가하고 있다. 이러한 스마트폰은 유선 환경의 디바이스와는 달리 크기가 작아 휴대성이 편리하며, 여러 센서를 활용할 수 있는 장점이 있다. 또한 무선네트워크에 수시로 접속이 가능하여 유비쿼터스 협업화(Ubiquitous Collaboration)에 큰 기여를 하고 있다[1].

한편, 유비쿼터스 환경에서 협업은 중요시되고 있다. 그 이유는 서비스 및 리소스를 성공적으로 제공하기 위해서인데, 어떤 환경에서든 서로 다른 다양한 컴퓨팅 장치들이 원활하게 작용하는 것이 점점 더 요구되기 때문이다[2].

유비쿼터스 협업 환경에서 스마트폰의 보안은 피쳐폰[3]에 비해 여러 가지 문제를 가지고 있다. 그 중 피쳐폰과 차별화되는 보안 위협은 개방성이다. 스마트폰은 무선인터넷 및 외부 인터페이스를 개방하여 제공되고 있으며, 이로 인해 리소스에 누구나 쉽게 접근할 수 있기 때문에 보안에 취약하다[4].

따라서 각 사용자가 자신의 정보나 리소스의 접근에 대한 허가 대상자나 접근이 가능한 리소스를 직접 제어 및 관리 할 수 있어야 한다. 본 논문에서는 접근 제어 중 Capability 기반의 접근 제어를 제안한다.

본 논문의 구성은 2 장 관련연구에서 ACL-based Authorization Infrastructure, RBAC Infrastructure 와 Capability-based Authorization Infrastructure 에 대해 고찰하고 3 장은 제안 방식을 기술하며, 마지막 결론에서는 향후 연구와 보완 사항을 제시한다.

2. 관련 연구

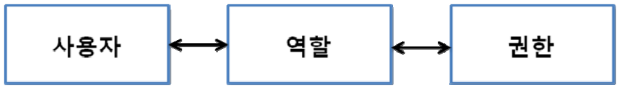
2.1 ACL-based Authorization Infrastructure

ACL-based model[5]에서 리소스 노드는 매번 요청을 인증하고 허가하는 데 책임을 가지고 있다. 만약 요청이 동일한 클라이언트에게 인증과 허가가 반복되어서 연속된다는 것을 가정할 때, 이 시스템은 확장성 문제(Scalability Problem)에 민감할 수 있고 DoS 공격이 가능하게 만들 수 있다. [그림 1]은 ACL 기반의 권한 부여 구성도(ACL-based Authorization Infrastructure)를 나타내고 있다. 리소스 공급자와 권한이 각기 분리되어 있으므로 Workflow 가 비교적 무거운 편이다[6].

(그림 1) ACL based Authorization Infrastructure

2.2 RBAC Infrastructure

RBAC(Role-based Access Control)[5]은 권한부여가 사용자가 아닌 역할이 기반이기 때문에 효율적인 권한 관리를 가능케 하지만, 역할간 계층구조로 인해 권한 상속(Permission Inheritance)이라는 특징을 가지고 있어 상위 역할일 수록 필요 이상의 권한을 부여하게 되는 문제가 있으며, 제약이 복잡해지거나 바뀔 경우, 적용이 번거롭고 어려울 수도 있다. [그림 2]는 각 사용자의 역할에 따라 권한이 적용되는 RBAC 의 Infrastructure 를 나타내고 있다[7].



(그림 2) RBAC Infrastructure

2.3 Capability-based Authorization Infrastructure

Capability 는 접근 행렬을 행 단위로 컨트롤하는 방법으로 각 주체는 하나의 능력 리스트-Capability List-와 관계되는 것이다[8].

능력 기반 권한 부여 구성도(Capability-based Authorization Infrastructure)는 앞의 모델과는 달리, 리소스 공급자가 권한을 갖고 있어서 혼동된 대리인 문제(Confused Deputy Problem) 가 없다는 장점을 가지고 있다. 또 다른 장점은 발행된 능력 토큰(Capability Token)을 통해 다중 접속으로 재사용이 가능하다는 것이다. [그림 3]은 능력 기반 권한 부여 구성도(Capability-based Authorization Infrastructure)를 나타내고 있다. 사용자는 첫 번째로 리소스 공급자에게 요청을 보낸다. 리소스 공급자는 이 요청을 그 사용자의 능력(Capability)에 따라 승인한다[6].

(그림 3) Capability-based Authorization Infrastructure

3. 제안 방식

리소스 공급자는 인증된 사용자에게만 권한을 주어 불필요한 사용자의 접근을 방지할 수 있어야 한다. 따라서 차별화된 정책(Policy)을 가지고 권한을 주어 리소스 접근 방식을 강화시켜야 한다.

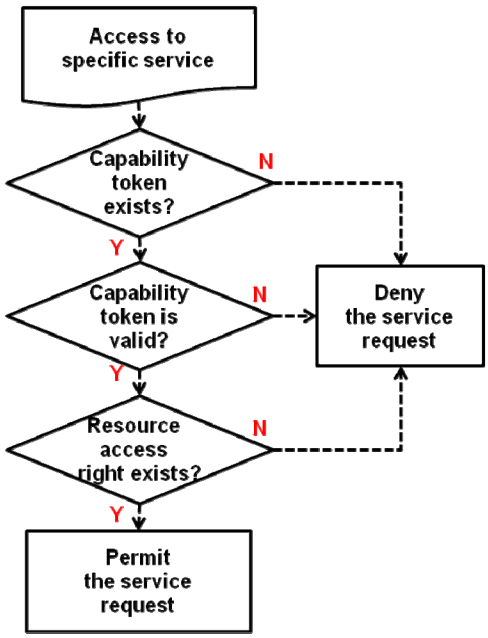
이를 기반으로 제안한 스마트폰 유비쿼터스 협업 환경에서의 권한 접근 방식은 다음 [그림 4]와 같다.

(그림 4) 능력(Capability) 기반 접근 권한 구조도

리소스 공급자는 리소스를 가지고 있고 사용자가 접근하고자 할 때, 제안하는 방식의 단계별 요청을 살펴보면 다음과 같다.

1. 리소스 공급자에게 사용자가 리소스를 요청할 경우, 스마트폰 사용자는 능력 토큰(Capability Token)과 시간상의 제한 요소(Time Validation)들을 포함한 리소스 정보를 리소스 공급자에게 보낸다.
2. 리소스 공급자는 사용자로부터 받은 요청의 적합성을 판단하기 위해 능력 토큰의 유효성, 시간 제약성, 접근 권한을 순차적으로 검증하여 유효하다고 판단되면 해당 사용자에게 리소스 접근 권한을 부여하고 이에 대한 응답을 보내준다.

이에 대한 상세한 순서도는 [그림 5]와 같다.



(그림 5) 능력(Capability) 기반 접근 권한 순서도

리소스 공급자에 유효한 능력 토큰이 존재하고 정당한 리소스가 접근하면, 정책에 따라 리소스 요청을 허용하고, 이를 만족하지 않으면 모두 거부한다.

스마트폰 사용자들은 이와 같은 Capability 기반의 접근 권한을 적용함으로써 화이트 보드, Audio/Video Conferencing, 게임 등의 다양한 서비스를 안전하게 활용할 수 있다.

4. 결론 및 향후 연구

최근 스마트폰의 보급이 늘어남에 따라 그 보안에 대한 관심과 염려 역시 비례적으로 증가하고 있다. 접근 제어를 하지 않으면 허가되지 않은 무단 사용자의 접근이 늘어나고 이에 따라 리소스의 낭비가 많아질 것이다. 따라서 리소스에 대한 접근 권한이 필요하다. 여러 가지 접근 권한이 있지만, 그 중 Capability를 제안한 이유는 Token 의 폐지 문제(Revocation Problem)만 다룬다면 점점 심각화 되어가는 DoS 공격에 좋은 메커니즘이며, 혼동된 대리인 문제(Confused Deputy Problem)가 없다는 장점을 가지고 있고 또 재사용을 할 수 있어서 다중 접속이 가능하기 때문이다.

이에 따른 향후 연구 방향은 Audio/Video Conferencing(유비쿼터스 협업)을 위한 어플리케이션으로써 안드로이드 환경에서 구현된 화이트 보드에서 Capability 정책을 정의하고, 구현해봄으로써 효율성을 분석해보고자 한다.

참고문헌

[1] Feature Phone, Wikipedia, [online], http://en.wikipedia.org/wiki/Feature_phone

[2] 박상준, 이건수, 김민구, “유비쿼터스 환경에서 협업 수행을 위한 의존성 기반 역할 할당 방법”, 한국컴퓨터종합학술대회 논문집 Vol.36, NO.1(B), 2009

[3] 스마트폰과 유비쿼터스, [online], http://shadowshow.blog.me/70107715461, 2011.04.16

[4] 강동호, 한진희, 이윤경, 조영섭, 한승완, 김정녀, 조현숙, “스마트폰 보안 위협 및 대응 기술”, 전자통신동향분석 제 25 권 제 3 호 통권 123 호 (2010 년 6 월) pp.72-80 ISSN 1225-6455

[5] Fischer, Robert J., Halibozek, Edward, Green, Gion, “Introduction To Security”, Butterworth-Heinemann, 2008

[6] Liang Fang and Dennis Gannon, “XPOLA – An Extensible Capability-based Authorization Infrastructure for Grids”, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, IL 60439, 2005

[7] 이상하, 조인준, 천은홍, 김동규, “역할기반 접근통제에서 역할 계층에 따른 접근권한 상속의 표현”, 한국정보처리학회 논문지 제 7권 제7호(2000. 7)

[8] 이종주, “다중영역환경을 위한 무결성 보호 모델에 관한 연구”, 동국대학교, 2010