RFID 애플리케이션을 위한 상황 인식 보안 아키텍처*

권중규° 정목동
부경대학교 컴퓨터공학과
puker@puker.net° mdchung@pknu.ac.kr

A Context-aware Security Architecture for RFID Application

Jungkyu Kwon° Mokdong Chung
Department of Computer Engineering, Pukyong National University

요 약

동적인 환경 정보를 제공하는 RFID 플랫폼 환경을 위한 보안 서비스를 제공하기 위해서는 동적인 분산 환경에 대한 고려가 필요하고, 한 번의 인증으로 여러 서비스를 이용할 수 있어야 하고, 다양한 자원의 보안 정책을 단순화 시키고, 보안 정책의 설정과 변경이 쉬워야 있어야 한다. 본 논문에서는 RFID 애플리케이션을 위한 상황 인식 보안 아키텍처로서 Single Sign-On 개념을 구현한 Kerberos를 이용한 통합 인증 모델과 단순한 권한 관리를 위해서 RBAC를 이용한 권한 관리 모델을 제시한다.

1. 서 론

향후 유비쿼터스 시대의 응용 및 서비스는 컴퓨팅 및 커뮤니케이션 능력을 가진 스마트 객체들이 동적인 환경 변화를 인식하고 이에 적응할 수 있는 특성을 갖게 될 것이다[1]. 이런 특성은 RFID 플랫폼에서도 일어나고 있으며, RFID 미들웨어를 통해서 동적인 환경 정보를 얻을 수 있다.

또한 유비쿼터스 환경에서는 모든 정보가 공유되고 누구나 쉽게 접근할 수 있다. 그 이면에는 크래킹에 의한 정보 유출, 바이러스 유포, 컴퓨터 범죄, 프라이버시 침해, 저작권 침해 등과 같은 부작용도 일어날 수 있다[2]. 이러한 부작용은 RFID 플랫폼에서도 일어날 수 있으며, 이런 부작용을 방지하기 위해서 인증, 데이터 보호, 접근 제어를 제공해야 한다[3].

따라서 본 논문에서는 RFID 미들웨어에서 제공하는 동적인 환경 정보를 이용하는 상황 인식 보안 아키텍처를 제시한다. RFID 플랫폼에서는 각 시스템에 대한 인증이 아니라 플랫폼 전체에 대한 공통된 인증 메커니즘이 필요하고, 한 번의 인증으로 플랫폼 내의 모든 서비스를 이용할 수 있어야 한다. 또한 동적으로 변화하는 다양한 자원의 보안 설정을 개별적으로 설정하고 관리하는 것은 복잡하고 많은 부담이 따르기 때문에 권한 관리를 단순화 시켜주고 보안정책의 설정과 변경이 쉽고 변경된 보안 정책이 잘 반영 될 수 있는 유동적인 보안 관리 시스템이 필요하다.

본 논문에서는 Kerberos와 RBAC(Role Based Access Control)를 이용한 상황 인식 보안 아키텍처를 제안하고자 한다. 2절에서는 관련연구를, 3절에서는 RFID 애플리케이션을 위한 상황 인식 보안 아키텍처를 제시하고 4절에서 결론 및 향후 연구 방향을 논한다.

2. 관련연구

2.1 EPCglobal Network

EPCglobal Network는 EPC 코드와 RFID 기술을 근간으로 EPC 코드 관련 상품정보를 담고 있는 서버(EPC IS)들을 서로 연결하는 안전한 수단이다. EPCglobal Network에 연결된 기업들은 EPC 코드 관련 정보를 자사의 EPC IS에 저장한다. 로컬 EPC IS에서 상품 정보를 찾지 못할 경우 EPCglobal Network를 통해 ONS(Object Name Service)에 해당 상품 정보를 찾을 수 있는 곳의 위치를 문의해서 그 주소를 통해 해당 상품정보를 얻을 수 있다[4].

EPCglobal Network의 구성요소는 그림 1과 같다.

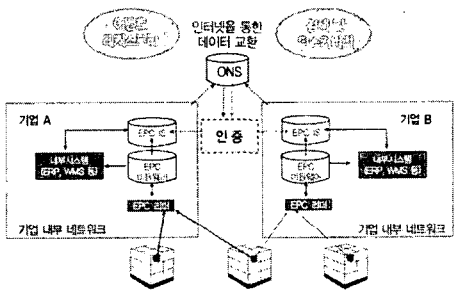

그림 1. EPCglobal Network 구조

2.2 컨텍스트(Context)

Shildt[5]는 컨텍스트의 정의를 사용 장소나 주변의 사람이나 사물의 집합, 또는 시간이 지남에 따른 변화 등을 일컫는다고 컨텍스트를 정의하고 있다. 한편 Dey[6]는 이를 좀 더 일반화 하여 엔티티(entity)의 상태를 특징지을 수 있는 어떤 정보도 모두 컨텍스트로 정의하고 있다. 여기서

* 이 논문은 2005년도 두뇌한국21사업에 의하여 지원되었음

엔티티는 사람이나, 사용자와 애플리케이션 간의 의사소통에 관계되는 사물 등이 될 수 있다고 정의하고 있다.

2.3 Kerberos

Kerberos[7]는 미국 MIT에서 Athena 프로젝트의 일환으로 대칭키 암호화를 이용하여 개방형 분산 환경에서 클라이언트와 서버 간에 인증 서비스를 제공하려는 목적으로 등장한 시스템이다. 분산 환경에서 모든 서버가 직접 클라이언트를 인증하려면 키 관리와 운영에 어려움이 있으므로 중앙에 인증 서버를 두어 서버의 부담을 줄이고, 또한 한 번의 패스워드 인증으로 여러 서버에 반복적으로 접속할 수 있는 싱글사인온(SSO; single sign-on) 개념을 구현하였다. 그리고 Kerberos는 도청과 재전송 공격(replay attack)을 막고, 데이터의 무결성을 보증한다.

2.4 RBAC(Role Based Access Control)

Ravo S. Sandhu에 의해 제안된 RBAC[8]는 사용자의 역할에 기반을 둔 접근 통제 방법으로 조직 내의 사용자 허가 할당에 있어서 복잡성과 비용, 잠재적인 실수를 줄이기 위한 강력한 기법을 제공한다. 또한 조직 수준에서 보안 관리를 증진시키기 위해서 사용자 식별자 수준이 아닌 추상화 수준으로 제공하므로 권한 관리를 매우 단순화 시켜주고, 특정한 보안 정책을 구현하는데 있어서 유연성을 제공하는 장점이 있다.

3. RFID 애플리케이션을 위한 상황 인식 보안 아키텍처

3.1 상황 인식 보안 아키텍처

RFID 애플리케이션을 위한 상황 인식 보안 아키텍처는 그림 2와 같다. 클라이언트, 클라이언트를 인증하는 인증 서버(AS), 접근 제어 서버(ACS), 이용할 서비스로 구성되어 있다.

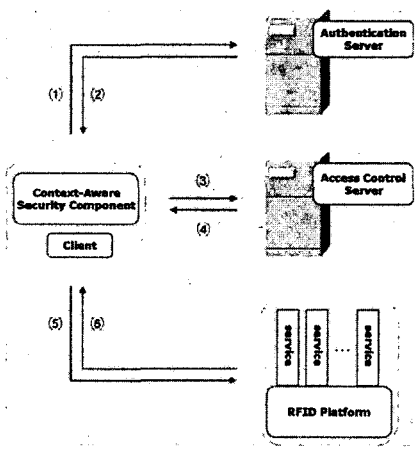

그림 2. 상황 인식 보안 아키텍처

클라이언트 내에는 RFID 미들웨어에서 제공하는 컨텍스트 정보를 이용해서 동적인 보안 서비스를 제공하는 Context-Aware Security Component(CASC)가 존재한다. CASC에서 이용하는 컨텍스트 정보는 RFID 미들웨어에서 제공하는 정보로서 시간(When), 장소(Where), EPC 정보(Who)이다[6].

3.2 통합 인증 모델

클라이언트 인증 메커니즘은 상황 인식 보안 아키텍처 구성요소를 기반으로 표 1과 같은 인증 프로토콜을 수행한다.

표 1. 통합 인증 프로토콜

Authentication Server Exchange
(1) C → AS: $ID_c \| ID_{acs} \| TS_1$ (2) AS → C: $K_c[K_{c,acs} \| ID_{acs} \| TS_2 \| L_2 \| Ticket_{acs}]$ $Ticket_{acs} = K_{acs}[K_{c,acs} \| ID_c \| AD_c \| ID_{acs} \| TS_2 \| Lifetime_2]$
Access Control Server Exchange
(3) C → ACS: $ID_v \| Ticket_{acs} \| Authenticator_c$ (4) ACS → C: $K_{c,acs}[K_{c,v} \| ID_v \| TS_4 \| Ticket_v]$ $Ticket_v = K_v[K_{c,v} \| ID_c \| AD_c \| ID_v \| TS_4 \| Lifetime_4]$ $Authenticator_c = K_{c,acs}[ID_c \| CI_c \| AD_c \| TS_3]$
Client/Service Authentication Exchange
(5) C → V: $Ticket_v \| Authenticator_c$ (6) V → C: $K_{c,v}[TS_5 + 1]$ $Authenticator_c = K_{c,v}[ID_c \| AD_c \| TS_5]$
표기법
ID_c, ID_{acs}, ID_v 클라이언트, 접근제어서버, 서비스의 식별자 CI_c 시간, 장소, EPC 같은 컨텍스트 정보 AD_c 클라이언트의 주소 TS_k 타임스탬프 L_k 수명 $K_{a,b}$ a와 b 사이의 공유 비밀키 $Ticket_{acs}$ 인증 티켓 $Ticket_v$ 권한 티켓 Authenticator 인증자

인증 프로토콜은 6단계로 이루어져 있으며, 각 단계별 프로토콜의 전송 내용과 처리 방법은 다음과 같다.

(1) 클라이언트 인증 요청(C → AS): 클라이언트가 특정 서비스를 이용하고자 할 때는 먼저 인증 서버로부터 인증을 받아야 한다. 클라이언트는 자신의 식별자, 접근 제어 서버의 식별자, 타임스탬프를 인증 서버에 전송한다.

(2) 인증 티켓 발급(AS → C): 인증 서버는 세션키인 $K_{c,acs}$와 인증 티켓 $Ticket_{acs}$를 생성하여 클라이언트에게 전송한다. 세션키는 인증 서버에 미리 등록되어 있는 클라이언트의 패스워드로부터 유도된 K_c로 암호화한다. 인증 티켓은 인증 서버와 접근 제어 서버 간에 공유한 비밀키 K_{acs}로 암호화한다. K_{acs}는 미리 공유한 것으로 가정한다.

(3) 서비스 권한 부여 요청(C → ACS): 클라이언트는 이용하고자 하는 서비스에 대한 권한 티켓을 얻기 위해 접근 제어 서버에 인증 티켓과 인증자를 전송한다. 인증자에는 클라이언트의 컨텍스트 정보가

포함되어 전송된다.

(4) 권한 티켓 발급(ACS → C): 접근 제어 서버는 비밀키 K_{acs}를 이용하여 인증 티켓을 복호화한다. 또한 인증 티켓에 포함된 세션키 $K_{c,acs}$를 이용하여 인증자를 복호화하여 인증 티켓의 정당한 사용자인지 확인한다. 인증이 성공하면 인증자 내에 컨텍스트 정보를 이용하여 클라이언트가 요청한 서비스 ID_v에 대한 권한 부여 여부를 결정하고 권한 부여 결과인 권한 티켓을 세션키 $K_{c,acs}$로 암호화하여 전송한다. 접근 제어 서버의 권한 관리 모델로는 RBAC를 이용한다.

(5) 서비스 요청(C → V): 클라이언트는 부여받은 권한 티켓과 접근 제어 서버로부터 받은 세션키 $K_{c,v}$로 새로운 인증자를 생성하여 이용할 서비스에 전송한다.

(6) 상호 인증(V → C): 서비스는 전송받은 권한 티켓을 복호화하여 세션키 $K_{c,v}$를 얻고 이 세션키를 이용해서 인증자를 복호화하고 클라이언트가 권한 티켓의 정당한 사용자인지를 확인한다. 그리고 (TS_5 + 1)을 세션키 $K_{c,v}$로 다시 암호화하여 클라이언트에게 전송하여 클라이언트가 서비스를 인증을 할 수 있게 한다.

통합 인증 프로토콜의 결과로 클라이언트와 서비스를 상호 인증을 할 수 있고, 동일한 공유 비밀키를 가지게 된다. 이렇게 생성된 공유 비밀키를 통해서 향후에는 비밀통신을 할 수도 있다.

3.3 권한 관리 모델

다양한 환경 요소가 동적으로 변화하는 RFID 플랫폼 환경에서 다양한 자원의 보안 설정을 개별적으로 설정하고 관리하는 것은 복잡하고 많은 부담이 따른다. 따라서 RBAC 모델을 적용하면 권한 관리를 단순화 시켜주고 보안 정책의 설정과 변경이 쉽고 변경된 보안 정책이 잘 반영 될 수 있는 유동적인 보안 관리 시스템을 제공 할 수 있다.

서비스에 대한 접근 제어는 보안 정책에 따라 결정된다. 보안 정책은 사용자 역할(Role), RFID 미들웨어에서 제공하는 컨텍스트 정보로 구성된다.

표 2는 보안 정책의 전형적인 예이다. 표 2에 기술된 역할과 컨텍스트 정보가 조건을 만족하면 서비스 A를 읽을 수 있다.

표 2. 서비스 A에 대한 보안 정책 예

A Security Policy for Managed Service A	
Security Service	Reading
Role	administrator; user;

Security Contexts	epc = *.*.*.[24662089-24662200];
	readingtime ≥ 09:00;
	readerlocation = Door/Shelf;

4. 결론 및 향후 연구 방향

본 논문에서는 RFID 미들웨어에서 제공하는 동적인 환경 정보를 이용하는 상황 인식 보안 아키텍처를 제시하였다. RFID 미들웨어에서 제공하는 상황 정보를 시간(When), 장소(Where), EPC 정보(Who)의 3가지 컨텍스트로 분류하였고, 동적이고 분산 환경인 RFID 플랫폼 환경을 고려하여 각각의 서비스가 세부적인 로그인 과정을 수행하지 않도록 인증 서버를 두는 Kerberos 기반 통합 인증 모델을 사용하였다. 또한 분류한 컨텍스트 정보와 RBAC 모델을 이용하여 동적인 권한 관리 모델을 제시하였다.

하지만 본 논문에서는 컨텍스트 정보를 모델링하지 않았고, 다소 제한적인 컨텍스트 정보를 이용하였다. 또한 다른 영역간의 인증은 고려하지 않았다. 따라서 향후에는 컨텍스트 정보에 대한 모델링과 더 많은 컨텍스트에 대한 고려가 필요하며, 통합 인증 모델에 대한 연구도 필요하다. 또한 권한 관리 모델로서 제안한 RBAC에 대한 개선도 필요하다.

[참고문헌]

[1] 김재호 외, 상황인식 서비스 기술 연구 동향, 주간기술동향 제1178호, 2004.

[2] 윤정로, 최장욱 역, 유비쿼터스, 21세기북스, 2003.

[3] Securing RFID Data for the Supply Chain, http://www.verisign.com/epc.

[4] 한국유통물류진흥원, http://www.gslkr.org.

[5] B.Schildt and M.Theimer, "Diseminating Active Map Information to Mobile Hosts," IEEE Networks, 8(5), 1994.

[6] A.K.Dey, Providing Architectural Support for Building Context-Aware Applications, PhD Thesis, College of Computing, Georgia Institute of Technology, 2000.

[7] William Stallings, Cryptography and Network Security, Pearson Education, Inc. Prentice Hall, 2003.

[8] R. S. Sandhu, et al., "Role-based access control models," IEEE Computer, Vol. 29, No. 2, 1996.