RFID 플랫폼 환경을 위한 통합 인증 모델 설계*

권중규° 안규희 이현동 정목동
부경대학교 컴퓨터공학과
puker@puker.net° {heeya0101, win4class}@hanmail.net mdchung@pknu.ac.kr

Design of Integrated Authentication Model for RFID Platform Environment

Jungkyu Kwon° Kyuhee Ahn Hyundong Lee Mokdong Chung
Department of Computer Engineering, Pukyong National University

요 약

RFID 플랫폼 환경을 위한 인증 서비스를 제공하기 위해서는 동적인 분산 환경, 한 번의 인증으로 여러 서비스를 이용할 수 있어야 하고, 많은 데이터 처리와 열악한 컴퓨팅 환경에 대한 고려가 있어야 한다. 본 논문에서는 RFID 플랫폼 환경을 위한 통합 인증 모델로서 Kerberos Version 4를 이용하여 Single Sign-On 개념을 적용하고 대칭키 인증 시스템을 사용한다. 또한 단순한 권한 관리를 위해서 RBAC를 이용한 권한 관리 모델을 제시한다.

1. 서 론

인간 중심의 미래 컴퓨터 환경인 유비쿼터스 컴퓨팅(ubiquitous computing) 환경 실현을 위한 연구 개발이 활발히 진행되고 있다. Mark Weiser에 의하여 제창된 유비쿼터스 컴퓨팅의 주요 개념 중 하나인 고요한 상거래(silent commerce)를 가능하게 하는 차세대 핵심 기술로 RFID(Radio Frequency Identification) 기술이 주목받고 있으며, RFID를 기반으로 하는 유비쿼터스 서비스 환경 구축을 위한 연구 개발이 진행되고 있다[1].

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

본 논문에서는 RFID 플랫폼 환경에 필수적인 보안서비스 중에서 인증에 대한 모델을 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 RFID 플랫폼 환경의 특성상 많은 양의 데이터와 분산 환경의 디바이스의 컴퓨팅 능력이 부족할 수 있으므로 공개키 암호화 알고리즘과 같은 복잡한 연산의 알고리즘은 적용하기 어렵다.

따라서 RFID 플랫폼 환경에서는 위와 같은 고려 사항을 만족 시키려면 Single Sign-On의 개념과 대칭키 기반의 인증 프로토콜이 필요하다. 본 논문에서는 Kerberos Version 4를 이용한 통합 인증 모델을 제안하고자 한다. 2절에서는 관련연구를, 3절에서는 RFID 플랫폼 환경을 위한 통합 인증 모델을 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.

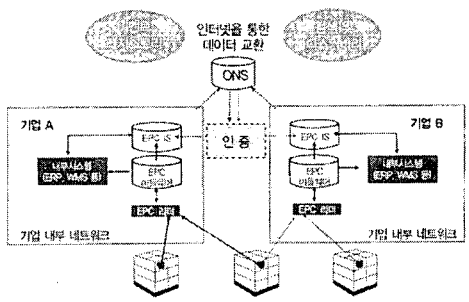

그림 1. EPCglobal Network 구조

EPC 코드는 사물을 고유하게 식별하는 EPC 식별자와 태그 판독의 효율성을 높이기 위해 사용되는 필터 값으로 구성된다. EPC 식별자는 메타 코딩 체계이다.

대부분의 RFID 태그는 반도체 칩과 안테나가 달린 송

* 본 연구는 교육부에서 주관하는 "차세대물류IT기술연구사업단"에 의해 지원 받은 연구임.

수신기로 구성된다. RFID 태그는 손상될 염려가 적고, 극히 빠른 속도로 다수의 태그를 동시에 판독할 수 있으며, 태그와 리더 사이에 장애물이 존재하여도 판독이 가능하며, 읽기/쓰기 기능을 가지게 할 수 있으므로 태그를 재사용할 수 있다.

리더는 EPC 코드를 태그로부터 읽어 들이는 장치이며 안테나와 제어장치로 구성된다. 제어장치는 인코딩 및 디코딩, 데이터 체크 및 저장, 태그 및 호스트와 통신 등을 관장한다.

EPC 미들웨어는 EPCglobal Network의 중추신경과 같은 존재로서 리더와 기업 정보 시스템 간에 데이터 교환을 가능하게 해 주는 장치이다. 미들웨어는 실시간 판독 상황을 감독하고, 경고 메시지를 발송하며, EPC IS나 기타 기업 정보 시스템에 전송할 신시간 판독정보를 관리한다. RFID 태그와 리더, 그리고 현장의 각종 시설을 통합하고 제어한다.

EPC DS는 사용자가 특정 EPC 코드에 대한 데이터를 찾아 그 데이터에 대한 접근할 수 있도록 지원하는 종합 서비스를 말한다. ONS는 일종의 디렉토리 서비스로서 EPC 코드를 인터넷 상의 URL로 변환시켜 준다. EPC IS는 상품 정보를 관리하고 정보 제공 요구가 있을 때 이를 제공한다.

2.2 사용자 인증 프로토콜

네트워크에 연결되어 있는 기존의 분산서비스 환경에서는 서버로부터 제공되는 서비스에 접속하기 위한 다양한 사용자 인증 프로토콜이 존재한다. 이러한 인증 프로토콜들은 메시지 암호화의 관점에서 대칭키 또는 비대칭키의 사용 유무에 따라 그리고 당사자(principal)간의 안전한 통신을 위해 미리 정의된 일을 수행하는 TTP(trusted third party)의 존재 유무에 따라 다음과 같은 네 가지로 분류된다[5, 6].

① Symmetric Key without Trusted Third Party
② Symmetric Key with Trusted Third Party
③ Public Key
④ Hybrid Protocols

첫 번째 인증 프로토콜은 당사자간에 안전한 통신을 위한 별도의 TTP를 사용하지 않고, 암호화된 메시지를 생성하기 위해 대칭키를 사용한다. 대표적인 프로토콜로는 ISO의 One-pass Symmetric Key Unilateral Authentication Protocol이 있다.

두 번째 인증 프로토콜은 당사자간에 안전한 통신을 위한 별도의 TTP를 사용하고, 암호화된 메시지를 생성하기 위해 대칭키를 사용한다. TTP는 당사자간에 암호화된 통신을 위해 세션키와 이 세션키의 전달을 위해 티켓을 생성 배포한다. 이 티켓을 이용해서 세션키를 공유하게 되고 이를 사용하여 안전한 통신을 할 수 있게 된다. 여기서 이 세션키를 재사용할 수 있도록 설계된 프로토콜을 반복 인증 프로토콜(repeated authentication protocol)이라 하며, 대표적인 프로토콜로는 Neuman과 Stubblebine의 인증 프로토콜과 MIT에서 개발한 Kerberos 프로토콜이 있다.

세 번째 인증 프로토콜은 메시지의 암호화를 위해 공개키 기반 구조(PKI)를 사용한다. 즉 메시지를 암호화하는데 있어 공개키를 사용하고, 인증서를 기반으로 사용자 인증을 수행한다. 대표적인 프로토콜로는 CCITT의 X.509에서 정의한 인증 프로토콜이 있다.

네 번째 인증 프로토콜은 메시지의 암호화를 위해 공개키 및 대칭키를 동시에 사용한다. 일반적이지는 않지만, 메시지는 공개키를 사용하여 암호화하고 공개키를 배포하는데 대칭키를 사용한다. 대표적인 프로토콜로는 EKE(Encrypted Key Exchange) 프로토콜이 있다.

3. RFID 플랫폼 환경에서 통합 인증 모델

통합 인증 모델의 구성요소는 그림 2와 같다. 클라이언트, 클라이언트를 인증하는 인증 서버(AS), 접근 제어 서버(ACS), 이용할 서비스로 구성되어 있다.

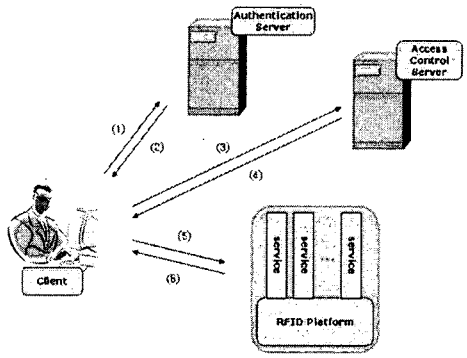

그림 2. 통합 인증 모델 구조

클라이언트 인증 메커니즘은 통합 인증 모델 구성요소를 기반으로 표 1과 같은 인증 프로토콜을 수행한다.

표 1. 통합 인증 프로토콜

Authentication Server Exchange
(1) C → AS: $ID_c \parallel ID_{acs} \parallel TS_1$ (2) AS → C: $K_c[K_{c,acs} \parallel ID_{acs} \parallel TS_2 \parallel L_2 \parallel Ticket_{acs}]$ $Ticket_{acs} = K_{acs}[K_{c,acs} \parallel ID_c \parallel AD_c \parallel ID_{acs} \parallel TS_2 \parallel Lifetime_2]$
Access Control Server Exchange
(3) C → ACS: $ID_v \parallel Ticket_{acs} \parallel Authenticator_c$ (4) ACS → C: $K_{c,acs}[K_{c,v} \parallel ID_v \parallel TS_4 \parallel Ticket_v]$ $Ticket_v = K_v[K_{c,v} \parallel ID_c \parallel AD_c \parallel ID_v \parallel TS_4 \parallel Lifetime_4]$ $Authenticator_c = K_{c,acs}[ID_c \parallel AD_c \parallel TS_3]$
Client/Service Authentication Exchange
(5) C → V: $Ticket_v \parallel Authenticator_c$ (6) V → C: $K_{c,v}[TS_5 + 1]$ $Authenticator_c = K_{c,v}[ID_c \parallel AD_c \parallel TS_5]$
표기법
ID_c, ID_{acs}, ID_v 클라이언트, 접근제어서버, 서비스의 식별자 AD_c 클라이언트의 주소 TS_k 타임스탬프 $Lifetime_k$ 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. 인증 티켓과 인증자는 암호화되어 전송되기 때문에 네트워크 상에서의 기밀성과 무결성을 보장한다. 또한 인증자의 TS_3은 매번 달라지는 값이므로 재전송 공격(replay attack)을 방지할 수 있다.

(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 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 RBAC(Role Base Access Control)[7]를 이용한다. RBAC는 사용자의 역할에 기반을 둔 접근 통제 방법으로 조직 내에서의 역할은 사용자 교체, 업무(task) 재할당에 비해 상대적으로 변화가 적기 때문에 권한 관리를 매우 단순화 시켜주고, 특정한 보안 정책을 구현하는데 있어서 유연성을 제공하는 장점이 있다. 다양한 서비스들이 빈번히 추가되는 RFID 플랫폼 환경에 RBAC를 이용한 권한 관리 모델은 서비스에 대한 개별적인 보안 설정의 복잡함을 상당히 줄여줄 수 있다.

(5) 서비스 요청(C → V): 클라이언트는 부여받은 권한 티켓과 접근 제어 서버로부터 받은 세션키 $K_{c,v}$로 새로운 인증자를 생성하여 이용할 서비스에 전송한다. 새로운 인증자에는 TS_5를 포함하고 있으므로 재전송공격을 방지할 수 있다.

(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.

4. 결론 및 향후 연구 방향

본 논문은 RFID 플랫폼 환경을 위한 통합 인증 프로토콜을 제안하였다. RFID 플랫폼 환경을 고려하여 각각의 서비스가 세부적인 로그인 과정을 수행하지 않도록 인증 서버를 두었고, 각각의 서비스에 대한 권한 관리를 위해서 RBAC를 이용한 권한 관리 모델을 제시하였다. 또한 RFID 플랫폼 환경의 많은 데이터 처리와 분산 환경의 디바이스의 열악한 컴퓨팅 능력을 위해 복잡한 연산을 수행하는 공개키 기반의 인증 대신에 대칭키를 사용한 인증을 사용함으로써 좀 더 빠르고 좀 더 적은 시스템 자원을 사용하도록 하였다.

하지만 본 논문에서는 다른 영역간의 인증은 고려하지 않았으며, 인증 서버와 접근 제어 서버간의 미리 공유된 비밀키가 있다고 가정하였다. 따라서 향후에는 이에 대한 연구와 권한 관리 모델로서 제안한 RBAC에 대한 연구도 필요하다. 또한 제안한 통합 인증 프로토콜에 대한 실제 구현도 필요하다.

[참고문헌]

[1] 원종호 외, 유비쿼터스 컴퓨팅 환경을 위한 RFID 기반 센서 데이터 처리 미들웨어 기술 동향, 전자통신동향분석 제19권 제5호, 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] John Clark and Jeremy Jacob, "A Survey of Authencition Protocol Literature: Version 1.0," University of York, Department of Computer Science, 1997.

[6] 전경석 외, "OSGi 서비스 플랫폼 환경에서의 사용자 인증 메커니즘," 정보과학회논문지 제9권 제2호, 2003.

[7] R. S. Sandhu, et al., "Role-based access control models," IEEE Computer, Vol. 29, No. 2, pp. 38-47, 1996.