RFID/USN 환경에서 상호 인증 메커니즘 검증·평가

김찬일, 김민경, 신화종, 이완석
한국정보보호진흥원
e-mail: chankim@kisa.or.kr

A Evaluation for Mutual Authentication Protocol In RFID/USN

Chan-Il Kim, Min-Kyoung Kim, Hwa-Jong Shin, Wan S, Yi
Korea Information Security Agency

요 약

유비쿼터스 환경의 센서 네트워크의 보안요소를 살펴보면 센서의 위치, 저전력에 적합한 암호 프리미티브, 초경량의 상호 인증 메커니즘 등이 있다. 그 중 기존의 RFID/USN 환경에서의 식별 및 인증 메커니즘 기법을 살펴보고 RFID/USN 환경에 적합한 상호 인증 메커니즘의 공통된 보안기능요구사항을 본 논문에서는 도출/제시한다. 그리고 RFID/USN 환경에서의 상호인증 기법을 한국정보보호진흥원에서 개발한 평가결과 자동생성도구를 이용하여 실제 검증·평가한다.

1. 서론

IT 환경이 발달하면서 대두되고 있는 유비쿼터스 컴퓨팅 환경은 개방된 환경이기 때문에 데이터에 대한 보호 문제가 발생한다. 이러한 서로 다른 컴퓨팅 환경을 이루는 장치들이 유선과 동일한 형태의 보안을 제공해야 하는 문제점과 개인의 정보를 어디까지 제공하고 보호해야 하는지 등의 보안 문제가 발생될 수 있다[1],[2]

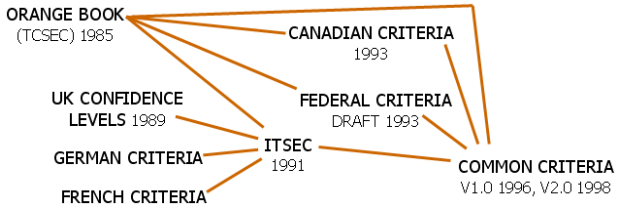
RFID/USN 환경에서 적합하다고 제시하고 있는 기존의 여러 가지 식별 및 인증 메커니즘을 소개하고 또한 기존의 식별 및 인증 메커니즘에서 요구하는 공통된 보안기능요구사항을 분석하고, 본 논문에서 RFID/USN 상에서 적용될 식별 및 인증 메커니즘을 보다 더 안전해질 수 있도록 보안기능요구사항을 도출/제시한다. 그리고 이 보안기능요구사항이 실제 제품에서 어떻게 구현 될 수 있는지를 설명하는 해석을 기술한다. 또한 한국정보보호진흥원에서 개발한 식별 및 인증 기능을 자동으로 평가를 수행하는 평가결과 자동생성 도구를 통하여 실제로 평가를 수행한다.

2. 공통평가기준

2.1. 공통평가기준 소개

IT 제품 또는 시스템의 중요 관심사 중의 하나는 보안 기능성을 보증하는 보안평가이다. IT 보안성 평가에는 ISO 표준(ISO/IEC 15408:1999)인 공통평가기준(CC, Common Criteria)이 널리 사용되고 있다.

IT 보안성 평가를 위한 기준의 개발이 각 국가와 국가들의 연합으로 이루어져 오다가 1993년 6월 국제표준화 기구인 ISO에서 일반 사용자를 위한 '공통평가기준 프로젝트'라고 명명된 프로젝트가 시작되었고 1996년 1월 CC 1.0이 완료되고 1997년 10월 CC 2.0 "베타"가 완료된 이후 검토를 거쳐 CC 버전 2.0이라는 공통평가기준이 발표되었다. 다음 그림은 CC로 통합되어 가는 과정을 보여주는 그림이다.[8, 9]



(그림 1) 공통평가기준 통합 과정

2.2. 공통평가기준 구성

CC는 1부 소개 및 일반모델, 2부 보안기능요구사항, 3부 보증요구사항으로 구성된다. 공통평가기준에서 보안요구사항이란 보안목적을 TOE 보안요구사항과 IT 환경에 대한 보안요구사항으로 정교화한

것으로, 이는 보안요구사항이 만족되면 TOE가 자신의 보안목적을 만족시킬 수 있음을 확인하는 것이다. 이러한 TOE 보안요구사항은 보안기능 요구사항과 보증 요구사항으로 구성되어 있다.

보안기능 요구사항은 IT 보안성을 뒷받침하기 위해 TOE 기능에 요구되는 것으로, 필요한 보안 행동을 정의한다. 보안기능 컴포넌트는 가정된 TOE 운영환경의 위협에 대처하고 조직의 보안정책과 가정사항을 만족시키기 위한 보안요구사항을 표현한다.

보안기능들이 제대로 동작하는지에 대한 증거를 보증 요구사항을 통해 제시한다. 이러한 보안기능 요구사항들과 보증 요구사항들은 평가의 기본적인 토대가 되고 보증 요구사항의 제시에 따라서 평가 등급이 결정된다.

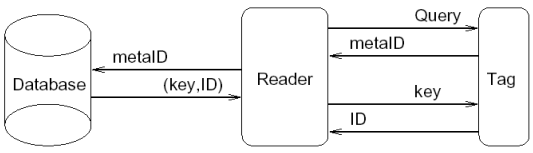
3. 기존의 RFID/USN 환경에서의 식별 및 인증 메커니즘

본 논문에서는 RFID/USN 환경에서 적합한 상호인증 메커니즘을 검증·평가 방법에 관하여 기술하고자 한다. 먼저 RFID/USN에서 사용되고 있는 식별 및 인증 기법은 저전력, 저컴퓨팅 능력 같은 여러가지 사항을 고려하여야 한다. 이중 가장 고려되어야 할 사항은 저전력이고 이 저전력을 고려한 해쉬함수 기반의 식별 및 인증 기법이 연구되고 있다.

3.1 Hash-Locking 식별 및 인증방식

RFID에서 중요한 정보을 가진 태그의 데이터에 대한 식별 및 인증 방법은 해쉬함수를 기반으로 식별 및 인증을 수행하여 데이터에 접근 허용 여부를 결정하는 방법이다.

태그 데이터의 접근을 허용하기 위해서는 리더기는 태그로부터 MetaID 값을 쿼리를 하고 리더기는 MetaID를 이용하여 Back-end-데이터베이스에서 Key를 찾는다. 태그는 Key를 전송받아 그 값을 해쉬하여 MetaID와 비교하여 정확여부를 확인하고 정확하게 매치 될 경우는 태그의 데이터 접근을 허용하고 그렇지 않을 경우에는 태그의 데이터 접근을 허용하지 않는다. 그 절차를 다음 그림에서 표시하고 있다.

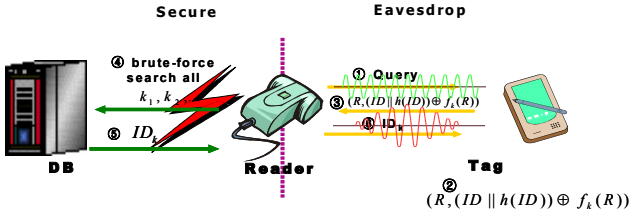


(그림 2) Hash-Locking 식별 및 인증 절차

3.2 Randomized Hash-Locking 식별 및 인증방식[4]

위에서 설명한 Hash-Locking 식별 및 인증 방식은 실제 식별 및 인증을 담당하는 ID인 MetaID값과 Key 값이 노출되는 위험이 존재한다. 그래서 이런 취약점을 해결하기 위하여 태그는 램덤 값을 생성하여 리더기에 전달하는 스킴인 Randomized Hash-Locking 식별 및 인증 방식을 여기서 설명한다.

태그의 데이터에 접근을 허용하기 위해서는 리더기는 태그로부터 (R, (ID||h(ID))⊕fk(R))값을 쿼리를 하고 Back-end-데이터베이스에서 램덤값과 태그와 공유하고 있는 Key값들을 이용하여 fk(R)을 계산하고 (ID||h(ID))⊕fk(R)과 XOR를 수행하여 (ID||h(ID))을 찾는다. 이것을 수행한 후 ID/Key 쌍으로 저장된 Back-end-데이터베이스에서 ID||h(ID) 값을 비교하여 ID값을 찾는다.

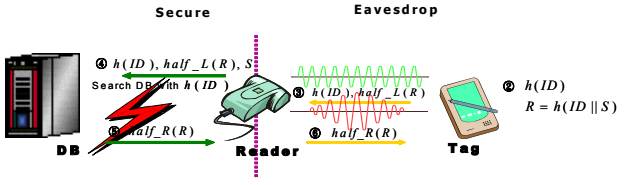


(그림 3) Randomized Hash-Locking 식별 및 인증 절차

3.3 향상된 hash 기반 식별 및 인증방식[3]

위에서 설명한 Randomized Hash-Locking 식별 및 인증 스킴은 여전히 Spoofing 취약성을 보여주고 있다. 이런 취약성을 제거하기 위하여 향상된 Hash 기반 식별 및 인증 방식이 연구되고 있다.

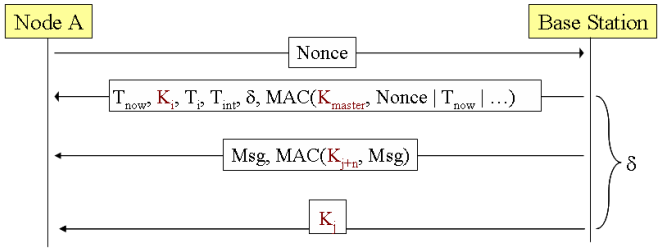
리더기에서 생성한 램덤 값 S를 각 태그에 쿼리를 보내면 각 태그는 h(ID) 값과 ID와 S를 덧붙여서 h(ID‖S) 한 후 나온 값중 왼쪽 반만 리더기에 h(ID)와 함께 보낸다. 그리고 리더기는 받은 왼쪽 반값과 h(ID), S 값을 Back-end-데이터베이스에 보내 ID 값을 찾고 h(ID‖S) 한 후 나온 값중 오른쪽 반값을 받아 태그에게 보낸다. 이와 같은 방법으로 리더기와 태그는 식별 및 인증이 이루어진다. 하지만 여전히 취약성이 남아 있다.



(그림 4) 향상된 hash 기반 식별 및 인증 절차

3.4. µTESLA 방식의 식별 및 인증방식[5,6,9]

µTESLA 방식은 USN 환경에서 Broadcast 인증 방식으로써 해쉬함수의 특징과 일정한 시간이 경과 후 Key을 공개하여 식별과 인증하는 방식이다. Base Station에서 분할된 시간 단위에서 생성된 hash-chain의 key들을 생성하고 K0는 모든 Node에 분배가 된 상태에서 다음과 같은 절차로 인증이 된다. Node에 램덤값을 받은 서버는 현 시간Tnow과 Base Station을 인증할 수 있는 Ki와 시간간격이 시작하는 시간 Ti와 시간 간격인 Tint 와 일정 시간이 경과후 Key 값을 공개하는 시점인 δ를 Node에게 알려 준다. Node은 Ki값으로 Base Station을 인증하고 δ기간중에 오는 Msg를 보관하고 있다가 Base Station에서 오는 Kj 값을 받아 저장하고 있는 Msg를 인증한다.



(그림 5) µTESLA 식별 및 인증 절차

4. 공통된 보안기능요구사항

유비쿼터스 환경의 센서 네트워크의 보안요소를 살펴보면 센서의 위치, 저전력에 적합한 암호 프리미티브, 초경량의 상호 인증 메커니즘 등이 있다.

RFID/USN 환경에서 적합한 경량화된 상호인증기술을 3장에서 소개하였다. 본 논문에서는 높은 안전성을 요구하는 RFID/USN 환경 대상으로 필요한 보안기능요구사항을 도출하고, IT 제품의 보안기능을 평가하기 위해 공통평가기준의 보안기능 컴포넌트로 보안기능요구사항을 다음 표와 같이 제시한다.

(표 1) RFID/USN 상의 식별 및 인증기능의 보안기능요구사항

보안기능 클래스	보안 기능 컴포넌트	
식별 및 인증	FIA_AFL.1	인증 실패 처리
	FIA_ATD.1	사용자 속성 정의
	FIA_SOS.1	비밀정보의 검증
	FIA_UAU.2	모든 행동 이전에 사용자 인증
	FIA_UAU.4	재사용 방지 인증 메커니즘
	FIA_UID.2	모든 행동 이전에 사용자 식별

FIA_AFL.1 : 인증 실패 - RFID/USN 환경에서 센스와 서버의 상호 인증의 실패 처리를 탐지 할 수 있어야 하고 이중 실패 횟수가 명세된 값을 넘기면 센서 또는 Base-Station의 대응행동이 있어야 한다.

FIA_ATD.1 : 사용자 속성 정의 - RFID/USN 환경에서 센스와 Base-Station의 보안 속성이 정의 되어야 한다. 각각의 식별 및 인증 메커니즘에 따라 인증에 필요한 보안속성은 다르게 정의 될 수 있지만 센스별 또는 Base-Station별로 보안속성은 Base-Station에서 관리 될 수 있어야 한다.

FIA_SOS.1 : 비밀정보의 검증 - 허용 기준을 만족시키는 비밀정보를 검증하는 메커니즘이 요구되고 관리되는 기능이 제공되어야 한다. (RFID/USN 환경에서 비밀 정보 검증 메커니즘의 허용기준은 대표적으로 해쉬의 길이 또는 key 길이 등이 될 수 있고 이와 동등한 보안강도 및 비밀정보를 검증하는 메커니즘이 될 수 있다.)

FIA_UAU.2 : 모든 행동 이전에 사용자 인증 - 모든 행동 이전에 센스 또는 Base-Station의 상호 인증을 요구한다. Base-Station에서 인증 실패에 대한 감사기록이 남아야 하고 센스에서는 명세된 기간동안 인증 실패의 감사기록이 남아야 한다.

FIA_UAU.4 : 재사용 방지 인증 메커니즘 - 재사용 인증 메커니즘은 일회용 인증 데이터와 동작하는 인증 메커니즘을 요구한다.

FIA_UID.2 : 인증을 요구하는 다른 모든 행동을 수행하기 전에 사용자를 식별하는 요구 조건이 요구된다. RFID/USN 환경에서 센스를 식별할 수 있는 ID와 서버를 식별할 수 있는 램덤 값 등이 이에 해당 될 수 있다.

5. 식별 및 인증 메커니즘 검증·평가

식별 및 인증 보안기능을 검증·평가를 수행하기 위한 한국정보보호진흥원에서 자체 개발한 평가결과 자동생성 도구를 이용하여 실제 평가하였다. 평가를 수행할 제품의 부재로 인하여 공통평가기준에서 요구하는 보안목표명세서 수준으로만 실제 평가를 수행하였다. 다음은 실제 평가를 위하여 보안목표명세서의 보안기능요구사항을 본인이 직접 작성하여 보안기능요구사항 대상으로만 실제 평가를 수행하였다.

FIA_AFL.1 인증 실패 처리

계층관계 : 없음

FIA_AFL.1.1 TSF는 [ID, 패스워드가 일치하지 않으면]에 관련된 [3회] 번의 실패한 인증 시도가 발생한 경우 이를 탐지해야 한다.

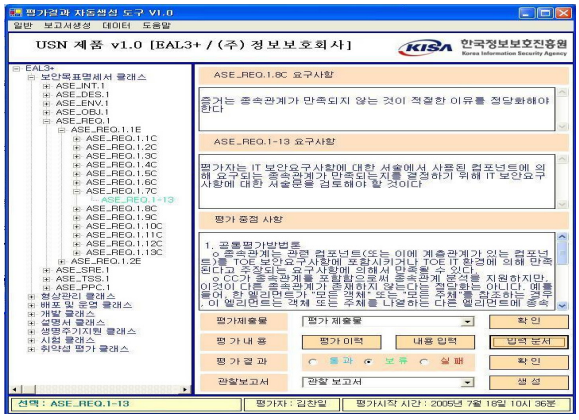
FIA_AFL.1.2 실패한 인증 시도가 정의된 횟수에 도달하거나 초과하면, TSF는 [인가된 관리자가 대응행동을 취할 때까지 해당 사용자 인증 방지, 접속 시도한 센서는 30초동안 접근거부가 이루어져야 한

다.]을 수행해야 한다.

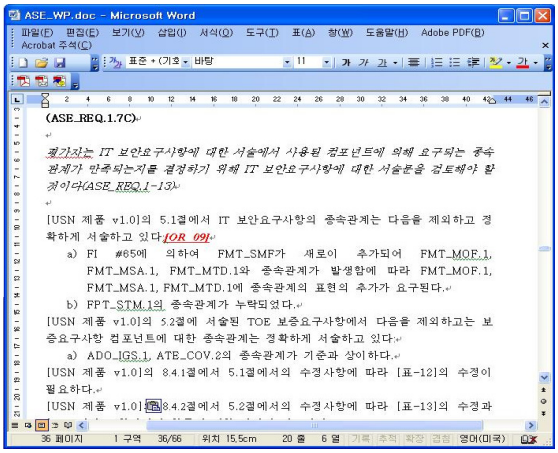
종속관계 : FIA_UAU.1 인증

실제 평가를 수행한 평가항목의 평가방법은 보안기능요구사항에 관련된 것만 선택하여 다음과 같이 기술하였고 실제 이 항목으로 평가를 수행하였다, 실제 보안 기능의 동작 여부는 공통평가기준 part3의 시험 부분 중 ATE_FUN, ATE_IND에서 확인해야 하지만 본 논문에서 실제 구현된 제품이 존재하지 않아 시험은 생략한다.

실제 평가는 다음과 같은 평가결과 자동생성 도구를 이용하여 평가를 수행하였고, 실제 보안 기능의 동작 여부는 공통평가기준 part3의 시험 부분 중 ATE_FUN, ATE_IND에서 확인해야 하지만 본 논문에서 실제 구현된 제품이 존재하지 않아 시험은 생략한다.



(그림 6) 평가결과 자동생성 도구 실행 모습



(그림 7) 평가결과 자동생성 도구로 실제 평가한 결과물

6. 결론 및 향후 과제

RFID/USN의 환경에서 식별 및 인증이 보안제품에 가장 중요한 요소이고 이런 보안제품을 구현하기 위해서 본 논문에서 식별 및 인증 메커니즘의 보안기능요구사항을 정의하였고 실제로 보안기능이 구현될 수 있도록 상위수준으로 보안기능요구사항을 보안목표명세서에 기술하였다. 마지막으로 실제 보안제품으로 보안기능을 평가하지 않았지만 보안목표명세서의 보안기능요구사항을 간접적으로 평가하여 RFID/USN 상에서 요구되는 식별 및 인증 기능의 보안성을 평가하였다.

본 논문에서 제시한 보안기능요구사항이 높은 보안성을 요구하는 RFID/USN 환경에서 식별 및 인증 메커니즘의 보안기능을 모두 포함하고 있다고 생각하지 않는다. 다만 지금 시점에서는 본 논문에서 제시한 보안기능요구사항 정도만 만족하며 최소한의 보안기능이 구현되었다고 할 수 있고, 제시된 보안기능요구사항을 만족할 수 있는 식별 및 인증 메커니즘 연구가 필요하고 차후 더욱더 나아가 보다 안전한 보안기능을 위해서 새로운 보안기능요구사항 도출이 필요할 것이다.

참고문헌

[1] 강전일, 박주성, 양대헌, “RFID 시스템에서의 프라이버시 보호기술”, 정보보호학회지, 24(6), 2004, 12

[2] 임지형, 이병길, 김현곤, 정교일, 양대헌, “유비쿼터스 및 Ad Hoc 네트워크 망에서의 정보보호 분석”, 정보통신연구진흥원, 주간기술동향 1160, 2004, 8.

[3] 황영주, 이수미, 이동훈, 임종인, “유비쿼터스 환경의 RFID Low-cost 인증프로토콜 ”, CISC'S04, pp 149-153 2004. 6.

[4] Dirk Henric, and Paul Muller, “Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers”, PerSec'04, pp. 149-153, 2004. 3

[5] M. Ohkubo, K. Suzuki and S. Kinoshita, “Cryptographic Approach to "Privacy-Friendly" Tags, ” RFID Privacy Workshop, http://www.rfid.edu.com, 2003.

[6] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, “Cryptographic Approach to "Privacy-Friendly" Tags, ”SPIN: Security Protocols for Sensor Networks”, Mobile Computing and Networking 2001 Rome, Itally Copyright 2001 ACM

[7] Ari Juels. “Minimalist Cryptography for Low-Cost RFID Tags”, RSA Laboratory

[8] 한국정보보호진흥원, “정보보호시스템 신분확인기능 및 무결성기능 평가방법 연구”, 최종 연구보고서, 1999년 12월.

[9] 한국정보보호진흥원, “정보보호 시스템 보안정책 모델 평가 방법론 연구”, 최종 연구보고서, 2004년 11월.

[10] 조영복, 김동명, 이상호, “유비쿼터스 네트워크에서의 상호인증 프로토콜”, 한국정보과학회 가을 학술발표논문집, 31(2), 2004.