AVISPA을 이용한 RFID 보안 프로토콜의 명세 및 검증

강미영° 오정현 이송희 최진영
고려대학교 컴퓨터학과
{mykang°, jhoh, shlee, choi}@formal.korea.ac.kr

The Specification and Verification of RFID Security Protocols Using AVISPA

Miyoung Kang° Jung-Hyun Oh Song-Hee Lee Jin-Young Choi
Dept. of Computer Science and Engineering, Korea University

요 약

최근 유비쿼터스 컴퓨팅에 관한 연구가 활발히 진행됨에 따라 핵심 기술인 RFID 프로토콜에 대한 연구가 활발히 진행되고 있다. 그러나 RF를 사용하여 무선통신을 함으로써 악의적인 공격자에 노출되는 보안상의 문제점이 발생한다. 본 논문은 기존의 RFID 보안 프로토콜의 문제점을 분석하여 새로운 프로토콜을 제안한다. 그리고 제안된 프로토콜을 AVISPA로 정형 명세하고 보안성을 정형 검증하여 안전함을 보여준다.

1. 서 론

최근 유비쿼터스 환경에 대한 연구가 활발히 진행되고 있으며 많은 연구들이 소개되어 있다. 그와 함께 우리 생활의 점점 더 편리해짐에 따라 불의의 사고가 발생할 수 있는 가능성이 높아지고 있다. 그러므로 유비쿼터스 보안 기술이 함께 발전하여야 한다.

RFID는 유비쿼터스의 컴퓨팅의 핵심 기술로 활발히 연구되고 있다. 그러나 Radio Frequency를 사용하여 물리적 접촉없이 물품의 정보를 자동적으로 인식이 가능하고 태그의 정보가 전송될 수 있으므로 과도한 정보 노출에 의한 보안성 문제가 대두된다.

그래서 RFID 시스템의 보안성 문제을 해결하기 위해 다양한 보안 프로토콜들이 제안으나, 보안성을 완벽하게 만족시키지 못하였고 또한 직관적인 방법에 의한 검증으로 보안성을 객관적인 검증이 이루어 졌다고 할 수 없다.

본 논문에서는 보안 프로토콜에 대한 객관적인 검증을 위하여 정형 기법을 사용하였다. 정형기법[CLAR 1996]은 수학적 논리나 이론을 바탕으로 하여 HW 또는 SW 시스템이 주어진 요구사항에 맞게 설계되었고, 안전하게 개발되었는지 확인 및 검증하는 방법론으로, 일반적으로 시스템의 동작 및 특성을 정형적으로 명세하는 정형명세와 정형명세된 시스템이 주어진 요구사항을 만족하는지 정형적으로 검증하는 방법인 정형검증으로 나뉜다.

보안 프로토콜을 정형검증하는 방법은 BAN[ABAI 1989], GNY Logic[GONG 1990] 등을 통한 정리 증명과 SPIN, SMV, FDR, AVISPA등을 이용한 모델체킹 등 다양한 방법들이 있으나 본 논문에서는 AVISPA(Automated Validation of Internet Security Protocols and Applications)를 이용하여 기존 프로토콜의 보안상의 문제점을 정형 검증을 통하여 분석하고 문제점을 해결한 보안 프로토콜을 설계하고 AVISPA로 검증하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 RFID 시스템의 보안 요구 사항을 기술하고 3장에서 관련 연구와 AVISPA의 구조에 대해 설명하고 4장에서는 기존 프로토콜의 문제점 분석과 제안하는 보안 프로토콜의 명세 및 검증을 제시하고 마지막으로 5장에서 결론을 맺는다.

2. RFID 시스템의 보안 요구 사항

리더와 태그간의 무선통신은 불안전한 상태이므로 공격자에 의해 언제나 쉽게 공격당할 수가 있다. 철저한 보안 상태를 유지하지 않는다면 태그의 ID를 추적하여 그와 관련된 개인 혹은 상품 정보를 빼앗길 수도 있다. 좀더 안전한 통신을 위해서 RFID 시스템에서 요구되는 보안 요구 사항으로는 아래 항목을 만족시켜야 한다.

가) 상호인증(Mutual Authentication)

무선통신구간에서는 공격자가 태그나 리더로 위장하여 전송되는 통신내역의 도청이나 위조가 가능하므로, 태그와 리더는 서로의 존재에 대해서 정당한지를 검토하고 인증해야 한다.

나) 불추적성(Untraceability)

기밀성(Confidentiality)과 익명성(Anonymity)을 포괄하는 개념으로 공격자가 어떤 공격기법을 통해서도 태그를 추적하지 못해야 한다. 기밀성이란,

태그가 소유자의 개인 정보 처리에 절대 관여하지 말아야 한다는 것이다. 즉 태그에 저장된 정보는 인증되지 않은 리더 혹은 태그와 소유자와의 관계를 추적할 수 있는 자료의 수집이 이루어지지 않아야 한다는 뜻이다. 익명성이란, 태그마다 존재하는 고유한 식별정보를 공격자가 알아내지 못하도록 보호를 하는 게 중요하다는 의미이다.

다) Spoofing 공격 방지

공격자는 특정한 리더로 위장하여 태그로부터 전송되는 통신내역을 수집한 후에 그 자료를 이용하여 정당한 리더로부터 인증을 받으려는 Spoofing 공격을 시도할 수 있다. 따라서 리더는 태그가 정당한지를 판단하고 공격을 차단할 수 있어야 한다.

라) 재생공격(Replay Attack) 방지

공격자가 특정 리더와 태그간의 통신 내역을 도청하여 수집한 내용을 가지고 나중에 리더로부터 인증을 받아서는 안 된다. 장시간 동안 통신 내용을 수집하여 분석한 공격자는 정당한 리더에게 재전송을 할 수 있으므로 이를 방지해야 한다.

RFID 시스템 구성요소들 중에서 리더와 서버의 통신은 유선 통신이므로 기존의 유선망에서 사용되는 보안 프로토콜들을 사용이 가능하기 때문에 보안성문제가 해결되었다고 가정한다. 그러나 태그와 리더간의 통신 채널은 무선 통신이기 때문에 무선 통신이 갖는 정보 누출과 태그 정보를 통한 위치 추적의 문제가 발생한다. 그러므로 RFID 시스템에 보안 프로토콜이 필요하게 되었으며, 보안 프로토콜을 설계 시 고려사항은 기밀성, 무결성, 익명성이다.

가) 기밀성(Confidentiality)

기밀성은 수동적 공격으로부터 데이터를 보호하는 것이다. 정당한 권한을 가진 사용자만이 데이터의 내용을 확인 할 수 있어야 한다. 무선으로 주고받는 정보는 도청 가능하다. 도청이 가능하더라도 데이터의 내용은 알 수 없어야 한다.

나) 무결성(Integrity)

무결성은 수신자 입장에서 송신자가 보낸 메시지가 제 삼자에 의해서 생성된것인지 또는 변조된 것인지에 대해서 확인 가능해야 한다. RFID환경에서는 메시지를 주고 받는 것은 누구나 도청 가능하기 때문에 메시지를 변조하여 태그와 통신을 시도 할수 있다. 그러므로 인가 받은 개체만이 전송하는 데이터가 변조 되었는지 확인 할 수 있어야 한다.

다) 익명성(Anonymity)

익명성은 프로토콜에서 사용되는 자료에 의해 태그의 정보를 추적할 수 없어야 한다. 인가받지 않은 사용자는 전송된 데이터에서 태그의 중요한 정보를 얻을 수 없어야 한다.

3. 관련 연구

RFID 시스템의 보안성 문제를 해결하기 위해 다양한 보안 프로토콜들이 제안되었다. 대표적인 보안 프로토콜은 Weis가 제안한 Randomized 해쉬 락 프로토콜[WEIS 2003], Okubo가 제안한 해쉬 제인 프로토콜[OHKU 2004], 그리고 Henrici가 제안한 해쉬 기반 프로토콜[HENR 2004]등이 있다. 하지만 이들은 태그의 정보 익명성을 제대로 보장해주지 못해 위치 추적이라는 문제점을 제거하지 못했다.

최근 태그의 익명성을 보장하기 위한 보안 프로토콜들이 제안되었는데 Tsudik이 제안한 YA-TRAP 프로토콜과 Chatmon이 제안한 O-TRAP 프로토콜[CHAT 2006]등이 있다. 이들은 Challenge-response 기법을 기본으로 사용하고, 리더와 태그간 Time-stamp 또는 약속된 난수값을 사용하는 데이터를 통해, 태그와 리더간의 상호인증을 할수 있도록 설계되어 있다. 하지만 공격자에 의한 광범위한 Time-stamp 공격에 매우 취약하고, 태그와 리더가 사용하는 난수값을 수정하면, 서버에 저장되어 있는 해쉬테이블 전체의 내용이 갱신되어야 하기 때문에 효율성에 문제가 있다.

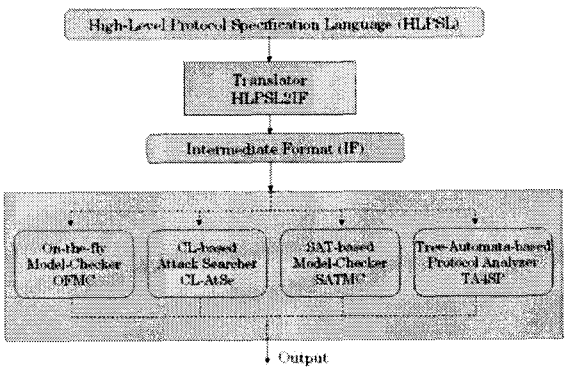
국내에서 GNY 로직을 이용하여 정형 검증한 프로토콜[OH 2007]을 제시하였고 FDR를 이용하여 모델 체크한 보안 프로토콜[KIM 2007]를 제안하였다.

본 논문에서는 AVISPA를 이용하여 Ari Juels 프로토콜[JUEL 2003]을 보안성을 검증하여 기밀성의 문제를 찾아내고 이를 보완하여 현실성있는 보안 프로토콜을 제안하였다. 제안된 보안 프로토콜을 AVISPA를 이용하여 보안성에 안전한지를 정형 검증하였다.

3.1 AVISPA

인터넷 프로토콜의 보안성을 정형 검증하는 도구로 상용 프로토콜[AVIS]을 보안의 문제점을 지적하고 있다.

AVISPA Tool은 독립적으로 개발된 모듈로 구성되어 있다. 툴의 입력으로 사용되는 High-Level Protocol Specification Language(HLPSL)L은 표현력이 뛰어나고, 모듈로 구성되어 있고, role-based인 정형언어이다. HLPSL은 HLPSL2IF 변환기을 통하여 Intermediate Format(IF)으로 자동 생성되어 OFMC, CL-AtSe, SATMC, TA4SP의 입력으로 사용된다[그림1].



[그림 1]AVISPA 툴의 구조

On-the-fly Model-Checker (OFMC) [BASI 2004] 요청 조절 방법(demand-driven way)안에서 IF 명세에서 변환 시스템을 탐구함으로써 프로토콜 변조와 부분적 검증을 수행한다. OFMC 많은 정확성과 완전성을 가진 상징적 기술을(symbolic techniques) 구현한다. 암호적 동작과 타입과 타입이 없는 프로토콜 모델의수학적 특성의 명세를 지원한다.

Constraint-Logic-based Attack Searcher (CL-AtSe) 효과적이고 간결한 heuristics과 중복제거 기술 같은 강제적인 해결책을 제공한다. [CHEV 2002], CL-AtSe는 모듈화 되어있고 암호적 동작에 수학적속성을 다룰수 있다. 정형화된 오류를 추출하고 메시지 연결성을 조절하는 것을 지원한다. .

SAT-based Model-Checker (SATMC) [ARMA 2004] IF에 의한 명세된 변환 관계의 제한된 전개을 암호화된 명제식으로 만든다. 보안 속성의 침해를 표현하는 초기 상태와 상태집합을 표현한다. 명제식은 최신 기술의 SAT에 제공된다.

TA4ST (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols) back-end [BOIC 2004]는 정규 트리 언어와 개서를 사용한 침입자 지시 지식에 근접한다. 보안 속성를 위해, TA4SP는 프로토콜에 결점이 있는지 없는지와 어떤 세션이 안전한지 아닌지를 보여줄 수 있다.

3.2 AVISPA에서 보안성 검증

```
Goal

% Confidentiality
  secrecy_of sec_k1, sec_k2
       secret(ID,sec_k1,{T,R})

% Message authentication
  authentication_on na
       request(R,T,na,Na)
       witness(T,R,na ,Na')
end goal
```

위의 명세된 HLPSL의 goal에서 보안성의 요건인 기밀성(confidentiality)와 상호 인증(authentication)을 만족하는지 검증한다.

secret(ID,sec_k1,{T,R}) T와 R사이에 ID가 안전한지(노출이 안되었는지) sec_k1를 통해 검증한다.

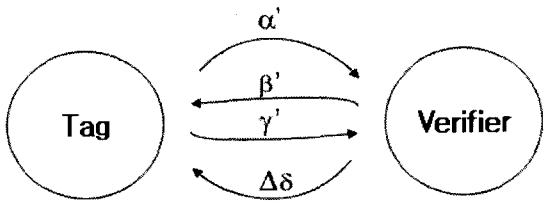
request(R,T,na,Na) R이 T에게 Na를 가지고 인증을 받겠다고 요청한다.

witness(T,R,na ,Na') T가 Na를 가지고 R이 맞다는 것을 확신한다.

4. 제안 프로토콜

4.1 기본 모델

Ari Juels[JUEL 2003c]는 One-Time Padding 기법을 사용하여 태그에 Padding Factor를 두어 태그와 검증자간의 인증 세션이 성공적으로 종료되었을 경우 이를 사용하여 태그와 리더에 저장된 비밀키와 Padding Factor를 가지고 XOR 계산을 시켜서 업데이트 시키는 방법이다.



[그림 2] Ari Juels 프로토콜

주어진 프로토콜은 Challenge-Response 기법의 종류로써, 태그는 K개의 비밀키 $k=\{\alpha_i\}\cup\{\beta_i\}\cup\{\gamma_i\}$(단, $1\le i\le k$)와 m개의 Padding Factor $\delta = \{\delta_1, \delta_2, \cdots, \delta_m\}$를 검증자와 상호 공유하고 있으며, 카운터(c)를 두어 비밀키와 Padding Factor 선택에 사용한다. 검증자는 내부에 모든 태그에 대한 비밀키들과 Padding Factor들을 저장하여, 태그 인증에 이를 사용한다.

4.2 Ari Juels 모델의 보안성 분석

AVISPA를 이용한 정형 검증은 주어진 프로토콜이 정상적으로 상호인증을 하는지와 사용되는 비밀키가

공격자에게 노출되지 않는지를 HLPSL로 명세한다.

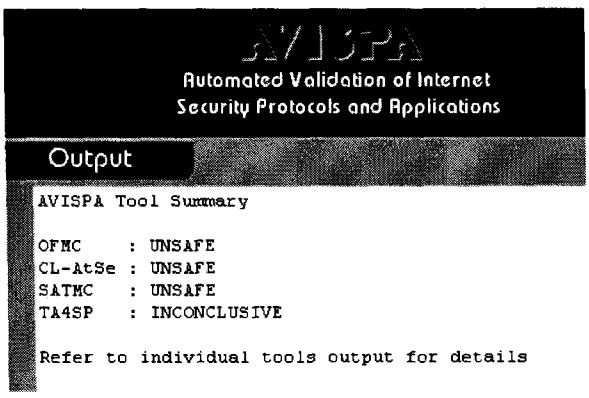
```
role tag (
    T,V : agent,
    SND,RCV     : channel(dy)
        )
played_by T def=
local
      A,B,C,Na     : text,
      State        : nat
const sec_k1 : protocol_id
init  State := 0
transition
1. State   = 0 /\ RCV(start) =|>
    State':= 1 /\ SND(A)
2. State = 1 /\ RCV(B) =|>
    State' := 2 /\ Na':= new()
                /\ SND(C)
                /\ secret(C,sec_k1,{T,V})
                /\ witness(T,V,na ,Na')
end role
```

위의 기술은 두개의 role인 Tag, Verifier 중 Tag부분이다. 전체 프로토콜 기술은 지면상 생략하였다. 아래의 두가지 속성(properties)을 검증한다.

secret(C,sec_k1,{T,V}) Tag와 Verifier사이에 C가 안전한지(노출이 안되었는지) sec_k1를 통해 검증한다.

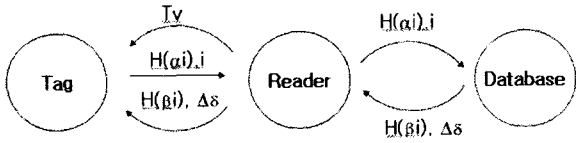
witness(T,V,na,Na') T가 Na'를 가지고 V이 맞다는 것을 확신한다.

검증한 결과는 안전하기 않다는 결과가 나온다. 공격자가 중간자 공격을 통하여 tag와 verifier간의 인증 세션을 종료시키지 않으면서 중간에서 값을 획득했음을 보여준다. 위의 결과를 통하여 a_i, β_i 까지 안전하지 않음을 유추 할 수 있다.



[그림 3] AVISPA의 검증 결과

4.3 제안 프로토콜



프로토콜 절차는 다음과 같다.

가) 리더

ㄱ) quary와 Tv(Time-stamp)를 태그에게 보낸다.

나) 태그

ㄱ) i=(Tv mod m)+1 을 계산

ㄴ) i번째 Padding Factor를 검색

ㄷ) $\alpha_i = \alpha \oplus \delta_m$, $H(a_i)$을 검색

ㄹ) $H(\alpha_i)$와 i를 리더에게 보낸다.

다) 리더

ㄱ) $H(\alpha_i)$와 i를 데이터베이스에게 보낸다.

라) 데이터베이스

ㄱ)저장된 값 중에서 α_i와 동일한 값이 있는지 확인

ㄴ) 있으면 태그 인증 성공

대칭되는 β_i 값을 찾아 $H(\beta_i)$ 및 Padding Factor를 갱신하기 위해 $\Delta\delta$를 송신

ㄷ) 없으면 세션 종료

마) 리더

ㄱ) $H(\beta_i)$와 $\Delta\delta$을 태그에게 보낸다.

바) 태그

ㄱ) $H(\beta_i)$와 $\Delta\delta$를 받으면 상호 인증 성공

ㄴ) $\delta_m = \delta_m \oplus \Delta\delta$ 계산

4.4 AVISPA를 이용한 보안 프로토콜 명세 및 검증

다음은 수정된 보안 프로토콜을 HLPSL로 명세한 것으로 리더가 추가되었다. role로는 태그, 리더, 데이터베이스를 사용하고 보안성 검증을 하였다. 보안성 검증은 동일하게 비밀키의 기밀성과 이를 이용한 효과적인 상호 인증 가능 여부에 대하여 실시하였다. Role reader이외의 명세는 지면상 생략 하였다.

```
role reader (
    R,T,DB : agent,
    H          : hash_func,
    SND,RCV    : channel(dy)
    )
played_by R def=
```

```
local
  A,B,Na    : text,
  State     : nat

init  State := 0

transition

1. State = 0 /\ SND(start) =|>
   State' := 1 /\ RCV(H(A))

2. State = 1 /\ SND(H(A)) =|>
   State' := 2 /\ RCV(H(B))

3. State = 3 /\ SND(H(B)) =|>
   State' := 3 /\ request(R,T,na,Na)

end role
```

정형적으로 명세된 프로토콜을 AVISPA로 보안성을 검증한 결과 문제가 없음을 확인하였다.

5. 결론

유비쿼터스 컴퓨팅 환경을 구현하기 위해 필수적인 기술로 대두되는 RFID에 대한 연구가 많이 진행되고 있다. RFID 시스템은 사용자들의 생활의 편리함 뿐만 아니라 물류비용 절감등과 같은 경제적인 측면에서도 크게 기여할 것으로 기대된다. 그러나 보안적 문제들을 해결하지 않으면 큰 문제가 발생할 수도 있다.

본 논문에서는 RFID 기술의 보안성에 대한 문제를 분석하고 분석한 문제에 대한 정형적 검증 방법을 소개하였다.

기존의 Ari Juels 프로토콜은 데이터의 기밀성을 만족시키지 못한다는 것을 AVISPA를 통하여 검증할수 있었다. 확인된 문제점을 개선하여 프로토콜을 제안하였다. 제안하는 프로토콜에 현실성을 고려하여 검증자를 분리시켜 태그, 리더, 데이터베이스로 구성하였다. 그리고 다시 정형 검증을 통하여 보안성 검증을 하여 문제가 없음을 확인하였다.

앞으로 연구 과제로써 제안된 보안 프로토콜이 구현될수 있도록 태그 메모리의 용량 문제에 대해 연구하고자 한다.

참고 문헌

[ABAI 1989] M. Abaid, M.Burrow, and R. Needham, "A Logic of Authentication, Proceedings of the Royal Society, Series A, pp.233-271, December 1989

[ARMA 2004] A. Armando and L. Compagna. SATMC: a SAT-based Model Checker for Security Protocals. In Proc. JELIA'04, LNAI 3229. Springer, 2004

[Auto-ID] Auto-ID Center, "860MHz-960MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Proposed Recommendation Version 1.0.0", Technical Report MIT-AUTOID-TR-007, Nov. 2002

[AVOI 2005] G. Avoine, P. Oechslin, "A Scalable and Provably Secure Hash-based RFID Protocol", IEEE PerSec 2005, March 2005.

[AVIS] http://www.avispa-project.org/

[BASI 2004] D. Basin, S. Modersheim, L.Vigano, "OFMC: A Symbolic Model-Checker for Security Protocols", International Journal of Information Security, 2004

[BOIC 2004] Y. Boichut, P.C. Heam, O. Kouchnarenko, F. Oehl. "Improvements on the Genet and Klay Technique to Automatically Verify Security Protocols. In Proc. AVIS'04, ENTCS, 2004

[CHAT 2006] C. Chatmon, T. Le, and M. Burmester, "Secure Anonymous RFID Authentication Protocols", Technical Report TR-060112, Florida State University, Department of Computer Science, Tallahassee, Florida, USA, 2006

[CLAR 1996]E. Clarke and J. Wing, "Formal Methods: State of the Art and Future Directions", ACM Computing Surveys, vol. 28, No.4, pp.626-643, 1996

[CHEV 2002] Y. Chevalier and L. Vigneron, "Automated Unbounded Verification of Security Protocols", In Proc. CAV'02, LNCS 2404. Springer, 2002

[GONG 1990] L. Gong, R. Needham, R, Yahalom, "Reasoning about Belief in Cryptographic Protocols", IEEE, 1990

[HENR 2004] D. Henrici, P. Muller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops(PERCOMW'04), pp.149-153, IEEE, 2004

[KIM 2007] H. Kim, J. Oh, and J. Choi, "The Design and Verification of RFID Authentication Protocol for Ubiquitous Computing", WICS, DEXA, Germany, Sep. 2007

[KINO 2003] S. Kinoshita, F. Hoshino, T. Komuko, A. Fujimura and M. Ohkubo, "Nonidentificable Anonymous-ID Scheme for RFID Privacy

Protection", Proc. Of CSS 2003, pp.497-502, IPSJ, Oct. 2003

[JUEL 2003] A. Juels, "Minimalist Cryptography for Low-Cost RFID Tags", RSA Laboratories, 2003

[OH 2007] J. Oh, H. Kim, J. Choi, "Light-weight Security Protocol for RFID system using One Time Pad", The 1st International Conference on Ubiquitous Information Technology, ICUT 2007, Dubie(UAE), February 2007, pp 51-60

[OHKU 2004] M. Ohkubo, K. Suzuki and S. Kinoshita, "Efficient Hash-Chain Based RFID Privacy Protection Scheme", Ubicamp 2004, 2004

[WEIS 2003]Weise, S. et al, "Security and Privacy in Radio-Frequency Identification Devices", Massachusetts Institute of Technology, 2003