RFID 네트워크 보안분석을 위한 정형적 방법론 [1)]

Formal Methodology for Analysis of the Network Security on RFID

김현석 김일곤 오정현 최진영
Hyun-Seok Kim Il-Gon Kim Jung-Hyun Oh Jin-Young Choi
고려대학교 정형기법 연구실
{hskim, igkim, jhoh, choi}@formal.korea.ac.kr

ABSTRACT

무선주파수 식별자(RFID: Radio Frequency Identification)의 연구에 있어 보안에 관한 부분은 학계 및 개발자들에게 중요한 부분이다. 특히 기술적인 이슈인 개체인증을 통한 데이터의 보안은 아직도 신뢰성을 얻지 못하고 있다. 본 논문에서는 RFID 기반 네트워크 시스템의 취약성을 분석하고 정형적 방법론의 적용사례를 통해 적용가능성을 타진해 보고자 한다.

Keywords : RFID, Formal methods, CSP, FDR

1. 서 론

RFID(Radio Frequency Identification)는 모든 사물에 RFID 태그를 부착하고 이를 통해 사물의 인식정보를 기본으로 주변의 모든 정보를 탐지 및 이를 실시간으로 네트워크에 연결하여 정보를 관리하는 것으로 먼저 인식정보를 제공하는 RFID를 중심으로 발전하고 이에 감지기능이 추가되어 이들간의 네트워크가 구축 되는 USN 형태로 발전할 것으로 전망되고 있다. 그러나 이러한 자동화되고 손쉽게 정보를 얻을 수 있는 환경에서는 보안에 있어 심각한 결과를 초래할 수 있다.

즉, RFID 태그의 사용에 있어서 사용자 개인의 프라이버시 문제(위치정보)와 RFID 태그의 ID가 쉽게 식별되는 문제 및 태그가 사용자가 알지 못하는 사이에 모든 리더에게 자동적으로 응답하는 문제가 인식된다.

이러한 궁극적인 보안문제를 해결하기 위한 방법으로서 보안프로토콜[1]이 제안되어 왔으며 시스템의 설계단계에서부터 사용자와 개발자에게 안전성과 신뢰성을 제공하기 위해 대표적으로 정형기법이라는 연구를 안전성 및 보안성을 검증하고자 하였다.

이러한 방법론은 정형 명세와 정형 검증의 두 가지 방법으로 구분된다.

정형 명세는 개발하고자 하는 시스템의 동작 및 시스템이 만족해야 하는 특성을 정형적인 표현방법을 이용해 모델링하는 방법이고, 정형 검증은 정형적으로 명세된 시스템을 대상으로 그 시스템이 정확한지 혹은 그 시스템의 요구사항으로 주어지는 특성을 만족하는지를 논리적으로 증명하는 방법이다.

정형 검증은 정리증명과 모델체킹 기법으로 구분되며, 전자는 BAN[2], GNY 와 같은 보안 로직을 이용하여 특정한 논리식으로 시스템을 명세하고 정확한 논리증명단계로써 정확성을 증명하는 방식이고, 후자는 프로토콜의 인증과정을 유한상태 기계의 형식으로 모델링하고 그 모델이 만족해야 하는 요구사항이나 특성을 모델에서 만족되는지를 검증도구를 이용해 자동으로 증명하는 방식으로 ESTEREL, Murphi, NRL protocol Analyzer [3]와 FDR[4][5]과 같은 도구들이 있다.

본 논문에서는 RFID 의 보안 문제점 및 목표를 알아보고 해결방안으로서 정형검증도구인 FDR 을 이용한 보안프로토콜의 검증사례를 통해 RFID 환경에 적합한 분석 방법론을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2 장에서는 RFID 네트워크 시스템의 보안 문제점과 요구사항을 알아보고, 3 장에서는 이러한 문제점에 대한 관련연구에 대해 살펴보며, 4 장에서는 RFID 네트워크 시스템의 분석방법론으로서 모델체킹 도구를 소개하고, 5 장에서 이에 대한 사례를 제시하며, 6 장에서는 결론 및 향후 연구방향을 제시하고자 한다.

2. RFID 네트워크시스템의 보안 문제와 요구사항

2.1. RFID의 보안 문제

RFID 시스템은 다음 세가지 구성요소로 이루어져있다.

- RFID labels(트랜스폰더)
- RFID label 리더 또는 트랜시버
- Application system

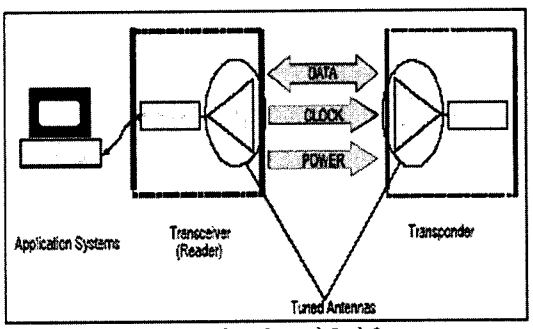

그림 1. RFID 컴포넌트 상호작용도

이러한 환경하에서 RFID의 보안 문제는 다음과 같이 정리할 수 있다.

■ 위조 : 태그에는 메모리에 데이터 항목이 존재한다. 이 항목은 항상 공격자의 공격대상이 될 수

1) 본 연구는 산업자원부 및 고려대학교 RFID 연구센터 성장동력기술개발사업의 연구결과로 수행되었음.

있으며 공격자는 데이터 항목을 지우거나 대신할 수 있는 방법을 사용할 수 있다. 이것은 리더와 태그간의 통신에 잘못된 데이터를 서로 교환 가능하게 함으로써 치명적인 위협이 존재한다. 또한, 리더의 위조로 인해 태그의 데이터 항목이 노출되는 위험이 존재한다.

■ 트래픽 분석 : 리더와 태그간 통신중 트래픽 분석을 통한 위협이 존재한다. 공격자가 어떤 특정 지역 내지 특정 태그에서 리더와 태그간의 트래픽을 분석할 수 있다면, 그 지역에서 어느 정도의 물품 이 존재하고, 빠져나가는지에 대해서 알 수 있다. 또한, 트래픽 분석을 통해서 위치 추적이 가능하다. 아무리 패킷내용이 암호화되어 있을지라도 같은 비트 패턴의 태그가 이동하는 것을 알 수 있기 때문에 개인의 움직임을 알 수 있다. 더 나아가 개인의 신상정보까지 노출될 수 있는 위협이 존재한다.

■ 도청 : RFID 시스템은 바코드 시스템과 달리, 효율성을 높이기 위해 수 미터의 범위 내에서도 리더와 태그간에 통신이 가능하도록 되어 있기 때문에 악의적인 사용에 의해 보안 문제점을 노출시킨다. 공격자가 리더를 이용해 태그를 스캐닝하는 적극적 공격과, 리더와 태그간 통신을 RF 수신하는 수동적 공격이 있다.

■ 서비스 거부(Denial of Service) 공격 : 리더가 태그간에 질의와 반응의 메커니즘이 존재한다. 이러한 특징을 이용하여 공격자가 리더를 가지고 수많은 질의를 리더 및 태그에게 보낸다면 리더와 태그는 많은 질의에 대해서 일일이 반응해야 된다. 이는 너무 많은 계산이 요구되고, 리더와 태그가 정상적인 기능을 못하게 만드는 결과를 초래한다. 서비스 거부 공격은 RFID 시스템이 작동을 못하도록 하는 위협이다.

2.2. RFID의 보안 요구사항

위 4가지 RFID 보안 문제들을 해결하기 위하여 RFID는 RF 태그와 리더 등 구성환경에 대해 다음과 같은 사항을 고려해 보안 목표를 설정할 수 있다.

■ 인증이 되지 않은 리더에게 정보유출이 되지 않아야 하며, 태그와 그 소유자 사이에 긴 시간 동안의 추적(long-term tracking)이 불가능해야 한다.

■ 태그의 내용은 근제한기법 (access control)에 의해 질의채널 (interrogation channel)이 안전하지 않다고 예상되면 암호화되어야 한다.

■ 태그와 리더는 모두 상호 신뢰해야만 한다.

■ 태그와 리더 어느 쪽이든 스푸핑이 어려워야한다.

■ 추적을 막기 위해서 보유자는 그들이 보유한 태그를 감지하거나 사용불가로 만들 수 있어야 한다.

■ 공개적으로 사용 가능한 태그의 결과는 랜덤화되거나 태그와 보유자 사이의 장기간 관련성(long-term association)을 회피하기 위해 쉽게 수정이 가능해야 한다.

■ 태그와 리더 사이에는 상호인증(mutual authentication)이 제공되어야 한다.

■ 전원공급차단에 의해 프로토콜이 손상 또는 가로채기 공격(hijack)에 노출되지 않아야 한다.

■ 태그와 리더 모두 재생공격(replay attack) 및 공격자 중간공격(man-in-the-middle attack)에 저항력이 있어야 한다.

3. RFID 네트워크 시스템 보안문제 해결에 관한 관련연구

RFID 시스템에서 사용자 프라이버시의 보호를 위한 많은 연구들이 진행되어 오고 있다. 현재 진행되어 왔던 연구결과 중, Kill 명령어의 접근법, Blocker 태그 기법, 해쉬락(Hash-Lock)기법[6], 랜더마이즈드 해쉬락 기법[7], XOR 기반 원타임 패드 기법[8], 외부재암호화 기법, 해쉬 체인(Hash-Chain) 기반 기법등이 있다.

RFID 네트워크 시스템의 보안을 위한 공개키 알고리즘의 하드웨어적인 구현은 2004년 Rabin, NTRU, ECC등의 공개키 알고리즘에 대한 구현 결과 제시에 의해 NTRU의 경우 20μW의 저전력에 3000개의 게이트만 필요하며, 경량화된 센서 노드에 탑재 가능한 것으로 알려져 있다[9]. 그러나 현재는 기존의 알고리즘을 개선하여 사용하고 있으며 향후에는 새로운 알고리즘 개발이 요구된다. 그룹키 관리를 위해 대칭키 방식 적용시 리더와 태그간의 키를 공유해야하며, 각 태그마다의 유일한 키를 관리하는 등의 많은 계산량 때문에 사용하기 어려우며, 키의 유출에 의한 태그 무력화, 장기간의 사용에 따른 노출 가능성등의 문제가 있다. 또한, 태그에 암호키를 탑재하는 방식은 에칭(etching), 탐침 등의 물리적공격에 취약하며 암호키의 노출 가능성이 있다. 버클리 대학의 SmartDust 프로젝트에서 채택한 센서네트워크의 보안 프로토콜인 SPINS(Security Protocol for Sensor Network)[10]은 μTESLA와 SNEP로 구성되어 있으며 메시지 인증, 무결성, 기밀성, 적시성 등의 서비스를 제공하고 있다. 랜덤키 사전 분배방식은 키 DB을 선택하고 무작위로 키를 선택하여 센서 노드에 할당하며, 두 개의 노드는 자신의 키 DB를 탐색하여 상대방이 같은 공통키를 소유하고 있으면 이 키를 세션키로 사용하는 방식이다.

4. CSP and FDR

4. 1 CSP(Communicating Sequential Process)

CSP[11]는 프로세스 알제브라 언어로서, 병렬성을 갖는 통신 프로토콜의 동작을 효율적으로 명세하기 위한 언어이다. 최초 일반 통신 프로토콜 및 제어 시스템의 명세를 위해 사용되어 졌으나, 점차 보안 프로토콜의 명세를 위한 영역으로 확대되어 가고 있다. CSP 에서 제공하는 pure synchronization(|||)과 Interleaving parallelism (||) 개념을 사용하여 분산 시스템 환경하에서 동작하는 클라이언트 서버와 공격자 모델을 정형적으로 표현할 수 있는 장점을 갖고 있다. 예를 들어, 분산시스템 환경하에서 동작하는 보안 시스템은 다음과 같이 간략히 표현할 수 있다.

SYSTEM = CLIENT1 ||| CLIENT2||| SERVER || INTRUDER

4.2 FDR(Failure Divergence Refinement)

FDR 은 모델체킹 도구로서, CSP 언어를 입력 받아 구현된 보안 모델에 대해 비밀성, 인증과 같은 보안 속성의 만족여부를 체킹하는 도구이다. 이를 통해 해당 속성을 만족시키지 못할 경우 반례를 보여주어, 공격 시나리오의 가능형태를 분석해 준다. 즉 보안 프로토콜이 반드시 갖추어야 하는 요구사항인 비밀성, 무결성, 인증, 부인방지와 같은 보안속성의 만족여부에 대한 검사 도구이다.

5. CSP and FDR 을 이용한 검증 사례

RFID 환경에 적용할 수 있는 멀티캐스트 통신에서 TESLA 와 같은 보안프로토콜을 검증하여 SPINS 프로토콜을 검증할 수 있는 기반을 마련한 연구가 진행되었다. TESLA 를 간단히 설명하면, 대칭키 암호화 방법으로, 공유키에 의한 공격을 방지하기 위하여 'loose time synchronization'과 'delayed key disclosure' 개념을 사용한다. 즉, 송신자는 'K_n, K_{n-1}..., K_0'의 일련키들을 형성하고 역으로 'K_0,...,K_n'의 순서로 키를 전송한다. 그리고 패킷을 전송시, 패킷 전송 후(packet delivery time + a)에 전송될 키 (K_i)로 MAC 값을 계산하여 함께 전송한다. 그러면 수신자는 패킷을 받았을 때,key K_i가 아직 전송되지 않았다는 상황을 확인하고, 확인되면 송신자가 K_i 를 전송할 때까지 패킷을 버퍼링해 두었다가, key 전송 후 패킷을 인증하게 된다. 이렇게 하면, 패킷이 전송되는 중간에는 공유키가 유출되지 않으므로 공격을 방지할 수 있게 된다. 이를 아래와 같이 CSP 언어로 명세하고 FDR 을 이용해 안전성을 입증하였다.[12]

```
SENDER_n(S, R, k_prev, k_curr) =
  [] k_next : FKey |~| m_curr : Packet
  output.S.R.(Msg3a, Sq.<m_curr, Hash.(f, <k_next>),
  k_prev>,<>) ->
  output.S.R.(Msg3b, Hash.(mac,<k_curr,m_curr,Hash.(
  f,<k_next>)>),<>) -> forget.k_prev.S.SENDER_role
  -> tock -> SENDER_n(S, R, k_curr, k_next)
```

이는 키값을 n 번째 받아 확인하는 과정을 설명하고 있으며 해쉬함수가 사용됨을 알 수있다.

```
Spec_1(S,m_prev) =
  signal.Sent.S?m_curr-> (signal.Accept?R!S.m_prev -> tock -
  > Spec_1(S,m_curr) |~| tock -> Spec_2(S)) |~|
  signal.Accept?R!S.m_prev -> signal.Sent.S?m_curr ->
  tock -> Spec_1(S,m_curr)
```

위 표현은 송수신자 사이의 통신시 정보의 안전성 속성을 표현하고자 하였다.

6. 결론 및 향후 연구방향

RFID의 정보 활용의 유용성은 반대급부로 정보노출이라는 보안 취약점을 야기시키며, 이러한 정보노출은 기존의 컴퓨터 정보의 유출만이 아닌 위치, 건강상태, 활동방식 등 우리의 전반적인 생활정보의 유출을 의미하게 된다. 현재 RFID의 보안 요구 사항 으로 태그 정보의 보호, 임의의 태그에 대한 추적방지 등이 제시되고 있다. 가장 최근에 연구되고 있는 프라이버시 보호를 위한 해쉬체인 기법 등의 연구는 RFID의 보안 요구사항을 어느 정도 만족하고 있다. 그러나 연산량의 줄이는 방법, 초경량 해쉬 함수의 구현문제 사항들이 더욱 연구되어야만 한다. 또한, 재기록이 가능한 태그(rewritable tag)에 대한 무결성 보장등도 병행되어야 한다.

아직까지는 표준화된 RFID의 보안 요구사항에 대한 정의 및 정형화된 기법은 존재하지 않고 있다. 따라서 보안에 대한 기술적 접근과 더불어 RFID 보안 연구에 있어 표준화 작업도 다각적으로 전개될 전망이다. 향후 연구분야로서 매우 가변적인 네트워크 보호를 위한 라우팅 보호프로토콜, 부채널 공격에 대한 RFID 보안기술 연구를 진행하고자 한다.

7. 참고문헌

[1] H.S.Kim, I.G.Kim, and J.Y. Choi, "Analysis of Security Protocols with Certificate over Open Networks: Electronic Payment System", Proceedings of the 25th IEEE International Conference on Distributed Computing Systems ICDCS-2005, pages 217-223, June, 2005.

[2] M. Abadi, M. Burrows, and R. Needham. "A Logic of Authentication", Proceedings of the Royal Society, Series A,426, 1871, pages 233-271, December 1989.

[3] Philip E.Varner, "Formal Methods as and Environmental Catalyst for Emergent Security in System Design and Construction", December 12, 2002.

[4] Gavin Lowe, "Breaking and Fixing the Needham-Schroeder Public-Key Protocol using FDR"

[5] H.S. Kim, I.G. Kim, and J.Y. Choi, "Analysis of the Application of E-Commerce System in Wireless Network", Proceedings of the 2th IEEE International Workshop on Mobile Commerce and Services, pages 112-121, July, 2005

[6] S. Sarma, S. Weis, and D. Engels, "Radio Frequency Identification : Security Risks and Challenges", Crypto Bytes, 2003.

[7] S. Weis, S. Sarma, R. Rivest, and D.Engels, "Security and privacy aspects of low-cost radio frequentcy identification systems", Proceedings of the 1st Security in Pervasive Computing, 2003.

[8] A. Juels, Privacy and authentication in low-cost RFID tags, In submission, Available at http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/

[9] G. Gaubatz, J. Kaps, and B. Sunar, "Public Keys Cryptography in Sensor Networks Revisited", Proceedings of the 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004).

[10] A. Perrig, et al., "SPINS : Security Protocols for Sensor Networks", Mobile Computing and Networking 2001.

[11] C.A.R. Hoare, Communicating Sequential Processes, Prentice-Hall, 1985

[12] Philippa, Hopcroft, and G. Lowe, "Analysing a stream authentication protocol using model checking", proceedings of LNCS, 19 August 2004