정리증명을 이용한 RFID 인증 프로토콜 설계 및 검증

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

Safety Analysis and Design of the RFID Authentication Protocol Using Theorem Proving

Junghyun Oh°, Jinyoung Choi
Dept. of Computer Science and Engineering, Korea University

요 약

RFID기술은 RF를 이용하여 자동적으로 사물의 정보를 획득할 수 있는 매우 편리한 기술이다. 하지만 악의적인 공격자에 의해 사물의 의도적으로 노출이 될 수 있는 문제를 지니고 있다. 이러한 RFID 시스템의 보안적 취약점을 보안하기 위해 많은 프로토콜들이 제안되었지만, 아직까지 완벽하게 보안성과 경제성을 모두 만족시키지 못하였고, 직관적인 방법에 의해 제안 프로토콜들을 검증하여 명확한 검증이 이뤄졌다고 할 수 없다. 본 논문에서는 새로운 RFID 인증 프로토콜을 제안하고 직관적인 검증이 아닌 정형기법을 이용하여 프로토콜의 보안성을 검증하였다.

1. 서 론

RFID 시스템은 Radio Frequency를 사용하여 물리적인 접촉이 필요 없이 물품의 정보를 자동적으로 읽어 들이는 유비쿼터스 기술 중에 하나이다. 하지만 시스템을 구성하는 요소간의 통신 채널이 무선환경이라는 특수성 때문에 도청을 통한 위조 또는 추적 등 보안적인 취약점을 내포하고 있다. 더하여 태그를 구성하는 하드웨어의 제약으로 유선 통신 환경에서 사용하는 암호화 방법들을 사용할 수 없기 때문에 보안성과 경제성을 모두 만족시키는 인증 프로토콜의 개발이 필요하게 되었다.

이에 해쉬함수 기반 인증 기법 또는 질의-응답 인증 기법(Challenge-Response) 등, 다양한 프로토콜들이 제안되었으나, 보안성 및 경제성을 완벽하게 만족시키지 못하였고, 또한 직관적인 방법에 의해 프로토콜들의 보안성을 검증하여 명확한 검증이 이뤄졌다고 할 수 없다.

본 논문에서는 RFID 시스템의 보안적 취약점을 보완하고 경제성 및 신속을 만족시켜주는 해쉬기반 보안 프로토콜을 설계하고 정형기법을 사용하여 보안성 만족 여부를 검증하였다.

정형기법[1]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.

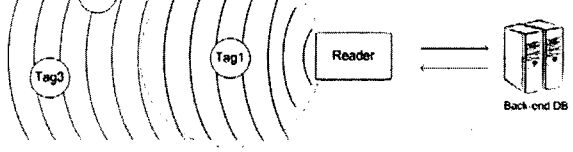
보안 프로토콜을 정형검증 하는 방법은 BAN[2], GNY Logic[3] 등을 통한 정리증명과 SPIN, SMV등을 이용한 모델체킹 등 다양한 방법들이 있으나, 본 논문에서는 GNY Logic을 이용한 정리증명으로 보안성을 검증하였다.

본 논문은 2장에서 관련 연구를 소개하고, 3장에서 프로토콜을 제안하고 정리증명을 통한 보안성을 검증하며, 4장에서 결론 향후과제에 대해서 언급하는 것으로 구성되어 있다.

2. 관련연구

2.1 RFID 시스템

일반적으로 RFID 시스템은 태그와 리더 그리고 데이터베이스 서버로 구성되어 있다 (그림 1).



(그림 1) RFID 시스템

RFID 시스템은 통신환경의 특수성 때문에 도청이 매우 용의하여 이를 통한 정보 누출(Data Leakage)과 누출된 정보를 통해 정보추적(Traceability)이 가능하다는 취약점을 갖고 있다.

2.2 보안적 요구사항

RFID 시스템의 보안적 취약점을 제거하기 위해 RFID 보안 프로토콜은 다음과 같은 요소들을 만족시켜야 한다.

- 자료의 비밀성 - 태그 관련 자료는 악의적인 공격자에게 노출되어서는 안된다
- 자료의 무결성 - 태그 관련 자료는 악의적인 공격자에 의해 임의적으로 수정되어서는 안된다
- 자료의 익명성 - 프로토콜에서 사용되는 자료에 의해 태그가 추적되어서는 안된다

2.3 기 제안된 프로토콜

해쉬 락 기법[4]은 태그의 잠금 상태를 해제하는 키값이 공격자에게 노출되고, 태그, 리더 및 서버간 주고받는 데이터의 값이 고정 값이기 때문에 추적이 이것을 통해 추적이 가능하다는 문제점이 있다. 위에서 언급한 태그의 추적 가능성을 제거하기 위해 Randomized 해쉬 락 기법[5]이 제안 되었으나, 리더가 태그가 보내온 ID값과 서버로부터 받은 ID값 중에서 매칭되는 것을 찾아야 하는 부담과, 리더가 찾은 ID값을 태그에게 다시 보내는 과정에서 ID값이 노출된다는 문제점이 있다. 이에 다시 해쉬 체인 기법[6]이 제안 되었으나, 단위 태그당 서버가 계산해야 하는 해쉬값 계산이 너무 많고, 한 세션 내에 인증이 끝나지 않았을 경우 이 방법도 태그의 익명성을 보장해주지 못한다. 해쉬 기반 ID Variation 기법[7]도 마찬가지로 태그가 태그의 ID를 해쉬함수 암호값을 취해 리더에게 보내게 되는데, 인증 세션이 종료되지 않는 상태일 때에는 이 값이 고정 값이기 때문에 부분적인 태그의 추적이 가능하다. 또한 서버가 분산되어 있는 환경에서 분산된 서버간 실시간적인 자료 갱신이 되지 않아 서버간의 데이터 베이스 정보의 차이로 문제가 발생될 수 있다. 이런 문제점을 해결하기 위해 질의-응답 기법[8]을 사용한 프로토콜들이 다시 제안되었으나, 프로토콜이 직관적인 방법에 의한 프로토콜의 보안성이 검증되어 보안성이 명확하게 검증되었다고 볼 수 없다.

2.4 GNY Logic

정리증명은 정형검증 방법의 하나로써 시스템 동작 및 특성을 정형적으로 명세한 후 수학적 또는 논리적으로 주어진 시스템이 주어진 요구사항을 만족하는지 유도하여 증명하는 방법이다. 정리증명을 이용한 보안 프로토콜의 검증에는 BAN Logic, GNY Logic 등 다양한 방법이 있으나, GNY Logic을 이용한 검증이 가장 성공적인 방법으로 알려져 있다.

GNY Logic을 이용한 보안 프로토콜의 검증은 다음과 같은 절차를 거쳐 이뤄지게 된다.

- 단계 1 프로토콜 메시지의 정형화
- 단계 2 초기 가정의 명세
- 단계 3 요구사항 명세
- 단계 4 논리식을 이용한 증명

GNY Logic에는 프로토콜의 메시지의 정형화와 논리적인 증명을 위해 간단한 기호와 논리식을 정의하고 있다.

다음은 GNY Logic에 정의된 논리식 중에서 제안 프로토콜을 검증하는데 사용된 논리식들을 정리한 것이다.

- Being Told Rule T1 : $\dfrac{S \lhd *X}{S \lhd X}$

S가 자신이 보내지 않은 데이터 X를 받았다는 것은 자신이 데이터 X를 받았다

- Possession Rule P1 : $\dfrac{S \lhd X}{S \ni X}$

S가 데이터 X를 받았다는 것은 자신이 이제 데이터 X를 갖게 되었다.

- Freshness Rule F10 : $\dfrac{S \models \#(X),\ S \ni X}{S \models \#(H(X))}$

S가 데이터 X를 갖고 있고, 과거에 사용된 적이 없다는 것 인정할 수 있다면, 데이터 X의 해쉬값도 과거에 사용된 것이 없다는 것을 인정할 수 있다.

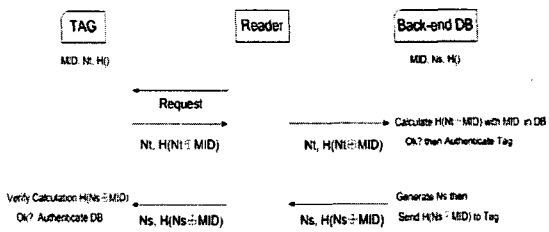
- Message Interpretation Rule I3

$$\frac{S \lhd *H(X,<MID>),\ S \ni (X,MID),\ S \models S \xleftrightarrow{MID} T,\ S \models \#(X,MID)}{S \models T \vdash (X,<MID>)\quad S \models T \vdash H(X,<MID>)}$$

S가 H(X,<MIID>)를 받았고, X,MID를 갖고 있고, S와 T는 MID를 사용하여 상호 인증할 수 있으며, 받은 값들이 과거에 사용되지 않았다는 것을 인정할 수 있다며, S는 (X,<MID>)와 H(X,<MID>)값이 T가 보낸 데이터임을 인정할 수 있다.

3. 제안 프로토콜

본 논문에서 제안하는 프로토콜은 해쉬함수 기반 프로토콜로서, 물류창고의 입·출고 과정에서 서버에 저장되어 있는 태그의 정보가 정상적으로 업데이트될 수 있도록 하기 위해, 인증과정을 통해 정상적인 태그의 정보가 서버 내에서 갱신되고, 태그는 자신이 보낸 데이터가 정상적으로 서버에게 전달되었음을 확인할 수 있도록 하였다. 또한 이 과정에서 구성요소들이 주고받는 데이터들의 익명성과 비밀성을 보장할 수 있도록 설계하여, 악의적인 공격자가 주고받는 데이터의 내용을 이해할 수 없어 이를 통한 악의적인 정보노출 및 정보추적의 가능성을 제거하였다.



(그림 2) 제안 프로토콜

Nt, Ns : 태그와 서버가 생성한 난수
MID : 태그와 서버가 공유하고 있는 비밀값
H() : 해쉬 함수
⊕ : XOR

주어진 프로토콜은 수동형 RFID 태그를 사용하는 시스템을 전제로 설계된 프로토콜이며, 리더와 서버간의 통신 채널은 안전하고, 태그와 리더의 통신채널은 안전하지 않다는 가정을 둔다. 태그와 서버는 MID를 비밀값으로 공유하고 있으면서 태그와 서버가 상호 인증을 할 때 사용하며, 성공적인 인증이 종료되면 태그와 리더는 미리 정해진 규칙에 의해 MID 값을 변경한다. 태그와 서버는 상호 주고받는 데이터의 익명성 보장을 위해 난수를 생성하여 사용한다. 서버는 자신과 연결된 많은 리더들이 보내오는 자료를 처리해야하여 단위 태그당 사용될 난수를 생성하는 것이 사실상 어렵다. 그러므로 리더들로부터 받는 태그자료들이 서버에 입력되는 순서를 기억하여 해당 태그로 보내는 난수로 사용하는 방법을 이용할 수 있다.

3.1 인증절차

- 단계 1 : 리더는 태그에게 Request를 보낸다.
- 단계 2 : 태그는 난수 Nt와 H(Nt⊕MID)를 리더를 통해 서버에게 보낸다.

• 단계 3 : 서버는 리더로부터 Nt와 H(Nt⊕MID)를 받아 MID를 계산하여 태그를 인증한 후 DB내의 자료를 업데이트한다.
• 단계 4 : 서버는 난수Ns와 H(Ns⊕MID) 를 리더를 통해 태그
에게 보낸다.
• 단계 5 : 태그는 리더로부터 Ns와 H(Ns⊕MID)를 받아 MID 계산하여 자신이 보낸 자료가 정상적으로 전달되었음을 인증한다.

3.2 보안성 검증

다음은 GNY Logic을 이용하여 단계적으로 프로토콜의 보안성 검증을 실시한 것이다..

① 프로토콜 메시지의 정형화

M1 : $S \lhd *(Nt, H(Nt \oplus MID))$
M2 : $T \lhd *(Ns, H(Ns \oplus MID))$

서버와 리더의 통신채널이 안전하고, 리더는 자료를 건네주는 역할만 하므로 정형화 과정에서 생략되었다.

② 초기 가정의 명세

$S \ni Ns, MID$ $\quad$ $T \ni Nt, MID$
$S \models \#(Ns)$ $\quad$ $T \models \#(Nt)$
$S \models \#(MID)$ $\quad$ $T \models \#(MID)$
$S \models S \xleftrightarrow{MID} T$ $\quad$ $T \models S \xleftrightarrow{MID} T$

서버는 난수 Ns를 갖고 있고 이 값이 과거에 사용된 적이 없음을 알고 있다. 마찬가지로 태그도 난수 Nt를 갖고 있으며 이 값이 과거에 사용된 적이 없음을 알고 있다. 더하여 서버와 태그는 MID를 비밀 값으로 공유하고 있으며, 이 값으로 상호 인증할 수 있음을 나타내고 있다.

③ 요구사항 명세

$S \models \#(H(Nt \oplus MID))$
$S \models T \vdash H(Nt \oplus MID)$
$T \models \#(H(Ns \oplus MID))$
$T \models S \vdash H(Ns \oplus MID)$

프로토콜이 만족하고자 하는 요구사항을 명세한 것이다. 서버와 태그는 자신이 받는 데이터가 일회성 데이터로 예전에 이 값이 사용되지 않았다는 것과, 이 데이터는 정상적인 태그 그리고 서버로부터 받은 것임을 인정한다는 것을 명세한 것이다.

④ 논리식을 이용한 증명

M1 : $S \lhd *(Nt, H(Nt \oplus MID))$

• T1 논리식을 적용하여 S ◁ {Nt, H(Nt⊕MID)}을 유도
• P1 논리식을 적용하여 S ∋ {Nt, H(Nt⊕MID)}을 유도
서버는 난수 Nt와 H(Nt⊕MID)를 갖게 되었다. 서버는 MID를 갖고 있으므로 H(Nt⊕MID)를 계산할 수 있다.
• 초기 가정에서 S ⊨#(MID)임을 알 수 있다.
• F1 논리식을 적용하여 S ⊨#(Nt⊕MID)을 유도
• F10 논리식을 적용하여 S ⊨#(H(Nt⊕MID))을 유도
서버는 이제 자신이 받은 데이터가 과거에 사용되지 않은 일회성 데이터임을 인정할 수 있다.
• I3 논리식을 적용하여 S ⊨T ⊢H(Nt⊕MID)을 유도
서버는 이제 자신이 받은 데이터가 정상적인 태그가 보내온 데이터임을 인정할 수 있다.

M2 : $T \lhd *(Ns, H(Ns \oplus MID))$

• 위와 똑같은 방법으로 논리식을 적용하면 태그는 자신이 받은 데이터가 과거에 사용되지 않은 일회성 데이터임을 인정한다는 의미를 갖고 있는 T ⊨#(H(Ns⊕MID))와 태그는 자신이 받은 데이터가 서버가 보내온 데이터임을 인정한다는 의미를 갖고 있는 T ⊨ S ⊢H(Ns⊕MID)를 유도해낼 수 있다.

4. 결론

RFID 시스템의 보안적 취약점을 보안하기 위해 제안되었던 많은 프로토콜들이 완벽하게 취약점을 보안하지 못하였고, 보안성 검증 또한 직관적인 방법에 의존에 검증되었었다. 본 논문에서 제안된 해쉬기반 프로토콜은 인증과정에 통해 서버에 저장된 태그의 정보가 정상적으로 업데이트되고, 태그와 서버가 공유된 비밀값과 난수를 사용하여 데이터를 주고받도록 하여 악의적인 공격자가 중간에 데이터를 획득한 후 태그 또는 서버로 위장하여 재생공격을 하더라도 MID값을 알지 못하므로 인증을 받을 수 없도록 설계 되어 있다. 또한 제안 프로토콜은 설계된 프로토콜이 RFID 시스템의 보안적 요구사항의 만족여부를 정형기법을 이용하여 완벽히 만족하고 있음을 증명하였다.

5. 참고문헌

[1] E. M. Clarke and J. M. Wing, "Formal Methods: State of the Art and Future Directions", ACM Computing Surveys, vol. 28, No. 4, pp.626-643, 1996
[2] M. Abaid, M. Burrow, and R. Needham." A Logic of Authentication", Proceedings of the Royal Society, Series A,426,1871,pp.233-271, December 1989
[3] L. Gong, R. Needham, R, Yahalom, "Reasoning about Belief in Cryptographic Protocols", IEEE, 1990
[4] S.E. Sarma. Weis, and D.W. Engels, "RFID systems, Seucrity and Privacy Implications", White Paper MIT-AUTOID-WH-014, AUTO-ID CENTER, 2002
[5] S.A. Weis, "Security and Privacy in Radio Frequency Identification Devices", MS Thesis, MIT, May 2003
[6] M. Ohkubo, K Suzuki, and S, Kinochita, "Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low Cost RFID", Proceedings of the SCIS 2004, pp.719-724, 2004
[7] 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
[8] Keunwoo Rhee, Jin Kwak, Seungjoo, Dongho Won, "Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment", SPC 2005, pp.70-84, 2005