HB 프로토콜과 변형된 HB 프로토콜 비교분석†

김수철* , 여상수** , 김성권*

*중앙대학교 컴퓨터공학부 , **단국대학교 정보컴퓨터학부

Comparative Analysis of HB Protocol and Modified HB Protocols

Soo-Cheol Kim* , Sang-Soo Yeo** , Sung Kwon Kim*

*School of Computer Science and Engineering, Chung-Ang University

**School of Information and Computer Science, Dankook University

요 약

무선 주파수 인식(RFID) 기술은 차세대 유비쿼터스 환경에서 가장 핵심적인 기술의 하나이다. RFID 기술의 발전은 다양한 분야에서 인간의 삶에 변화를 줄 것이라 기대된다. 하지만 안전한 유비쿼터스 환경을 위하여 RFID의 보안성이 우선시 되어야 한다. RFID 프라이버시 문제인 태그 내부의 비밀 정보 유출이나 임의의 태그에 대한 위치 추적 가능성을 해결하지 못한다면 RFID 시스템은 사용자의 신뢰를 얻기 힘들 것이다. 이로 인해서 최근 RFID 보안에 관한 연구가 많이 이루어지고 있다. 그 중에서도 최근 Juels가 발표한 Human Based 프로토콜이 많은 관심을 받고 있다. 본 논문에서는 Juels가 제안한 HB, HB+ 이외에 이를 바탕으로 여러 연구자가 제안한 확장된 HB 프로토콜들에 대해서 비교 분석하였다.

I. 서론

가까운 미래에는 사용자가 네트워크나 컴퓨터를 의식하지 않고 장소에 상관없이 자유롭게 네트워크에 접속할 수 있는 유비쿼터스 환경이 구축될 것이라 예상된다. 이와 같이 새로운 형태의 유비쿼터스 네트워크 환경을 구축하기 위해 기본적으로 필요한 핵심적인 기술이 RFID (Radio Frequency Identification)이다.

RFID는 각종 물품에 소형 반도체 칩을 부착해 사물의 정보와 주변 환경정보를 무선주파수로 전송·처리하는 비접촉식 인식시스템이다. 이와 같은 RFID 기술은 기존의 바코드 체계를 대체할 수 있어 개인 생활에 관련된 서비스는 물론 여러 가지 다양한 분야에서 많은 응용 서비스가 가능하다.

RFID 시스템이 많은 장점과 효용성을 가지고 있지만 안정성과 프라이버시 측면에서 문제점이 발생하고 있다. 바코드의 직접적인 접촉방식이 아닌 간접적인 접촉으로 태그를 인식하는 방식이 문제가 된다. RFID의 기본 특성상 태그는 모든 리더에게 자동적으로 응답한다. 그 결과 태그의 비밀 정보를 쉽게 획득 가능한 점과 특정 태그의 위치추적이 용이하다는 점은 사용자 프라이버시에 심각한 문제이다. 그러므로 RFID 시스템의 성공적인 산업화를 위해서는 보안 및 프라이버시 문제 해결이 우선 과제이다.

이와 같은 문제점을 해결하기 위하여 기존의 무선통신 보안책을 사용하기에는 문제가 있다. RFID 태그의 특성상 계산능력, 저장공간과 같은 자원의 한계를 가지기 때문에 태그에 알맞은 경량화된 인증 프로토콜을 만들어야 한다. 그래서 많은 연구자들이 RFID 인증에 대한 프로토콜을 제안하였다.

그 중 본 논문에서는 Ari Juels가 제안한 HB 프로토콜에 중점을 두고자 한다[1]. HB 프로토

† 본 연구는 한국과학재단 특정기초연구 (R01-2005-000-10568-0) 지원으로 수행되었음.

콜에 관련해 많은 연구자들이 변형된 프로토콜을 제안하였으므로 관련된 HB 프로토콜을 모아서 비교 분석해보고자 한다.

II. HB 프로토콜

HB 프로토콜은 Hopper와 Blum이 발표한 HB 프로토콜을 시작으로 Juels와 Weis가 RFID 시스템에 맞게 변형시켜 발표한 HB+, 그리고 Gilbert가 발표한 HB++, 마지막으로 Selwyn이 발표한 변형된 HB++이 존재한다.

2.1 HB 프로토콜

최초의 Human Based 프로토콜은 2001년에 Hopper에 의해 제안되었다[2,3]. HB 프로토콜은 1비트로 상대방을 인증하는 방식이다. 이 방식은 XOR을 사용하여 인증을 하며 그림 1은 HB 프로토콜의 한 라운드를 표시한다.

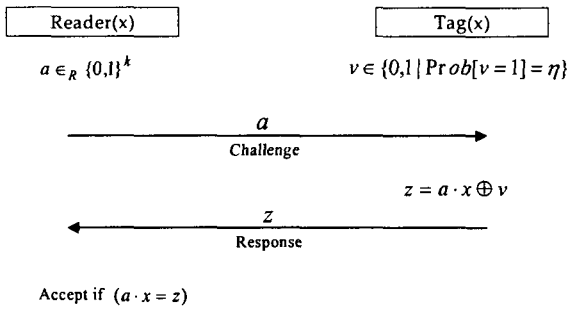

그림 1. HB 프로토콜의 한 라운드

인증하는 과정은 기본적인 도전-응답 방식으로 다음과 같다. RFID 태그와 리더는 서로 비밀값 x를 공유한 상태에서 리더가 태그를 인증하게 된다. 리더가 a 값을 생성하여 태그에게 전송하면 도전이 시작된다. RFID 태그는 $z = a \bullet x$ 값을 생성하여 응답한다. 키의 길이만큼 반복하면 $z = a_1{}^*x_1 + \ldots + a_k{}^*x_k$ 이다. 리더는 태그가 전송해온 값을 받은 후 자신이 저장하고 있는 x값과 a값을 이용하여 생성한 z'값과 받은 z값이 같은지를 확인하다. 이 때 인증의 정확성을 높이기 위해 1비트씩 r번 반복한다. 한번만 보내면 공격자가 확률 1/2로 추측이 가능하지만 위 과정을 r번 반복하면 공격자가 r번 모두 맞게 추측할 확률은 2^{-r}이다. 하지만 이 경우에도 공격자가 a의 비트 길이만큼 도청을 하여 연립방정식을 풀면 x를 알 수 있다. 이를 방지하기 위하여 리더는 도전에 일부러 $\eta \in (0, \frac{1}{2})$ 확률로 노이즈를 넣는다. 이와 같은 인증 과정을 r번 반복하여 그 값이 $\eta \bullet r$ 보다 적게 틀린 경우 정당한 태그로 인증 받는다.

하지만 HB 프로토콜은 공격자가 a 값을 자신에게 유리하게 전송하게 되면 응답값 z 에서 x 에 대한 값을 알아 낼 수 있다. 따라서 Juels는 능동적인 공격에도 안전한 HB+ 프로토콜을 제안하였다[1].

2.2 HB+ 프로토콜

HB+ 프로토콜은 능동적인 공격에 대비하여 HB 프로토콜을 변형시킨 버전이다[1]. 이 방식은 리더와 RFID 태그 간에 비밀값을 x 외에 추가로 y 를 사용한다. 또한 이전 방식와 달리 b 라는 랜덤값을 태그가 전송하면서 프로토콜이 시작한다. 그림 2는 HB+ 프로토콜의 한 라운드를 표시한다.

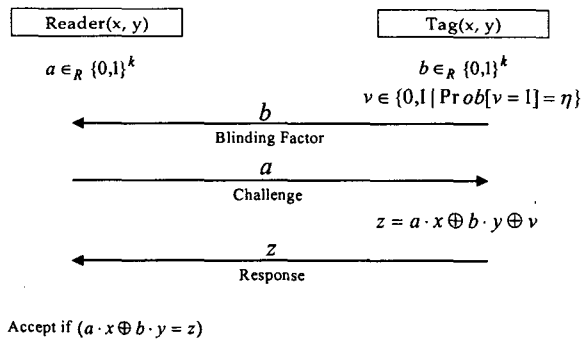

그림 2. HB+ 프로토콜의 한 라운드

HB+의 과정은 다음과 같다. 태그와 리더는 x, y 라는 k비트의 비밀값을 서로 공유한다. 그 후 프로토콜 시작시 태그가 k비트의 b 를 리더에게 전송한다. 그 후 리더는 a 값을 생성하여 태그에게 전송하여 도전을 시작한다. RFID 태그는 a,x,y,b 를 사용하여 $z = a \bullet x \oplus b \bullet y \oplus v$ 를 계산해낸다. 그리고 리더에게 z값을 전송하여 응답한다. 리더는 태그가 전송해온 값과 자신이 가지고 있는 정보를 이용하여 계산한 값을 비교한 후 태그를 인증한다.

Juels는 공격자가 자신에게 유리한 값을 생성하여 공격을 시도할지라도 b 값으로 인해 비밀값 y 에 대한 정보를 얻을 수 없기 때문에 안전하다고 주장했다. 하지만 Gilbert는 HB+ 프로토콜이 단순한 man-in-the-middle 공격에 약하다고 밝혀냈다[4]. 그림 3은 HB+에 대한 능동적인 공격법을 나타낸다. 공격자는 a 값을 보낼 때 δ 값과 XOR해서 보낸다. 그 후 인증단계가 성공하면 높은 확률로 $\delta \cdot x = 0$ 이다. 반대로 실패했으면 높은 확률로 $\delta \cdot x = 1$ 이다. 따라서 x 값을 추측할 수 있다[5].

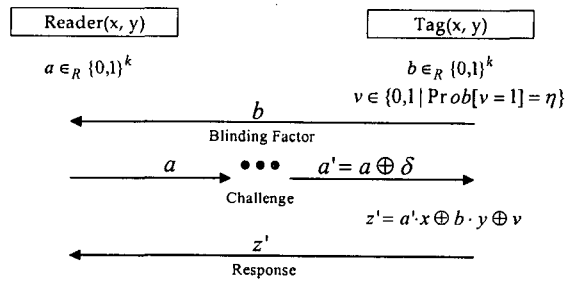

그림 3. HB+ 프로토콜에 대한 능동적 공격

2.3 HB++ 프로토콜

HB+ 프로토콜이 보안에 취약성을 가지기 때문에 Bringer는 두 가지의 HB++ 프로토콜을 제안하였다[6]. 그림 4는 첫 번째 HB++이다.

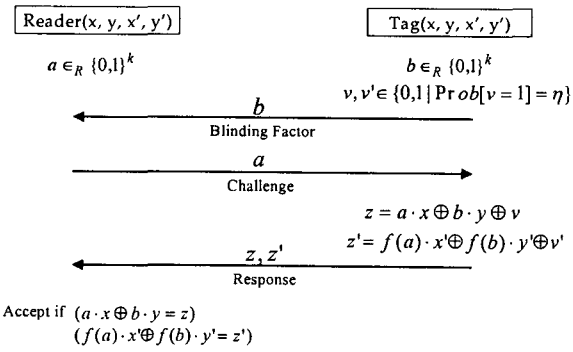

그림 4. 첫 번째 HB++ 프로토콜의 한 라운드

HB+는 side channel 공격이 가능하다[7]. 태그가 전송하는 z 값을 man-in-the-middle 공격으로 쉽게 추측 가능한 점이 문제이다. HB+와 바뀐 점은 기존의 비밀 값 x,y 이외에 추가로 x',y' 를 사용한다. 두 쌍의 비밀값을 이용하여 태그는 z,z' 두 개의 응답값을 만든다.

하지만 이 HB++ 프로토콜도 정당한 리더인척 하는 공격자에게 보안상의 약점이 존재한다. 따라서 Bringer는 두 번째 HB++을 제안하였다. 그림 5가 두 번째 HB++을 나타낸다.

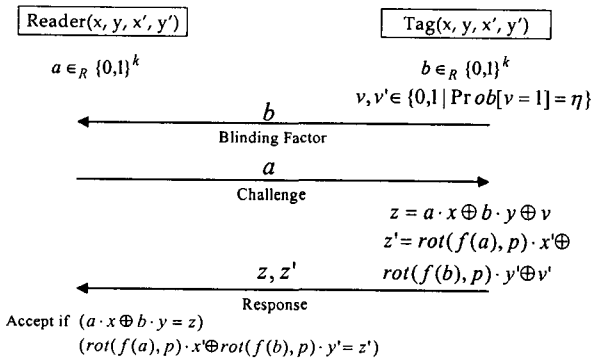

그림 5. 두 번째 HB++ 프로토콜의 한 라운드

하지만 HB++ 프로토콜은 z를 사용하기 때문에 공격 가능한 점이 여전히 남아있다.

2.4 변형된 HB++ 프로토콜

Selwyn은 HB++을 변형한 프로토콜을 제안하였다. Selwyn의 HB++은 그림 6에 나와 있다[8]. 가장 큰 변경점은 다음과 같다. 우선 x,y 를 사용한 z 값이 사라졌다. 이것은 side channel 공격을 예방한다. 그리고 매번 z 를 계산할시마다 p 를 업데이트 해준다. 동일한 p 를 사용하지 않기 때문에 매 라운드마다 다른 결과를 얻을 수 있다.

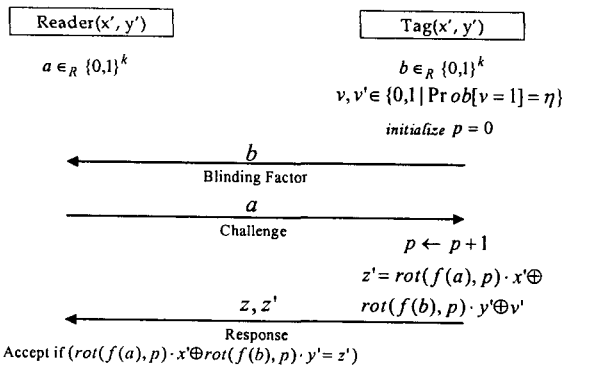

그림 6. 변형된 HB++ 프로토콜의 한 라운드

III. 분석

지금까지 HB 프로토콜과 변형된 HB 프로토콜에 대하여 알아보았다. 아래의 표1은 위에서 설명한 각 HB 프로토콜에 대하여 비교분석한 것이다. 각 프로토콜의 기본 정보와 요구하는 하드웨어 사항, 그리고 보안에 대하여 표로 정리하였다.

표 1. HB 관련 프로토콜 비교 분석

	HB	HB+	HB++	m-HB++
active attack	X	△	○	○
M-I-M attack	X	X	○	○
side channel	X	X	X	○
비밀값 수	1	2	4	2
하드웨어 요구사항	$\cdot, \oplus$	$\cdot, \oplus$	$\cdot, \oplus, rot, f(x)$	$\cdot, \oplus, +, rot, f(x)$

각 프로토콜들은 HB를 시작으로 하여 그전 단계의 약점을 수정하여 나온 프로토콜들이다. 따라서 단계마다 그전 프로토콜의 취약점은 보완되었다. 하지만 프로토콜이 변경됨에 따라 기존의 장점이었던 하드웨어 요구사항이 점점 높아진 것이 새로운 문제점이다.

HB와 HB+ 프로토콜은 보안상에 약점이 있지만 최소한의 하드웨어로 인증을 구현한 점이 인상적이다. 그리고 HB++와 변형된 HB++은 기존의 약점을 없애려는 시도는 좋았지만 프로토콜 구현을 위해 태그가 가져야할 하드웨어 요구사항이 HB 프로토콜의 목표점을 벗어난 것 같다.

IV. 결론

본 논문에서는 최근 이슈가 되고 있는 HB 프로토콜과 여러 변형된 프로토콜들에 대하여 비교 분석을 하였다. RFID 프라이버시 보호에 관한 연구에서 핵심사항은 경량화된 인증이다. 수동형 RFID 태그는 하드웨어 자체의 한계가 있기 때문에 최소한의 하드웨어 구현만으로 안전한 보안을 제공해야만 한다. 따라서 태그에 최소한의 하드웨어만 요구하는 HB 프로토콜은 주의 깊게 살펴볼 가치가 있다.

하지만 HB 프로토콜이 완벽하지는 않아서 많은 연구자들이 변형된 형태의 HB 프로토콜을 제안하고 있다. 따라서 여러 가지 형태의 HB 관련 프로토콜을 모아서 비교분석하였다. HB 프로토콜은 RFID의 보안 요구 사항을 어느 정도 만족하는 가능성이 보이는 프로토콜이다. 그러나 HB 프로토콜은 1비트 인증이기 때문에 다수의 태그를 관리하는 환경에서는 부적합한 단점이 있다.

앞으로 HB 프로토콜을 기본 개념으로 하며 보안 요구 사항을 만족하는 경량화된 프로토콜에 대한 연구가 지속적으로 필요하다고 본다.

[참고문헌]

[1] A. Juels and S. Weis. Authenticating Pervasive Devices with Human Protocols, in Adcanced in Crytology - CRYPTO'05, LNCS 3126, pp. 293-308, 2005.

[2] N.J. Hooper and M. Blum. A Secure Human-Computer Authentication Scheme, Technical Report CMU-CS-00-139, Caranegie Mellon University, 2000.

[3] N.J. Hooper and M. Blum. Secure Human Identification Protocols. Advances in Cryptology - ASIACRYPT 2001, LNCS vol. 2248, pp. 52-66, 2001.

[4] H. Gilbert, M. robshaw, and H. Sibert. An Active Attack Against HB+ - A Provably Secure Lightweight Ptotocols. Cryptology ePtint Archive, Report 2005/237, 2005.

[5] J. Katz and S. Ji Sun. Parallel and Concurrent Security of the HB and HB+ Protocols, In Advances in Cryptology - EUROCRYPT'06, LNCS, 2006.

[6] J. Bringer, H. Chabanne, and E. Dottax. HB++: a Lightweight Authentication Protocol Secure Against Some Attacks, In SecPerU, 2006.

[7] R.C.-W.Phan and S.-M. Yen. Amplifying Side-Channel Attacks with Techniques from Block Cipher Cryptanalysis, In CARDIS'06, 2006.

[8] P. Selwyn, HB and Related Lightweight Authentication Protocols for Secure RFID Tag/Reader Authentication, In CollECTeR 2006, 2006.