논문 16-41-03-02 The Journal of Korean Institute of Communications and Information Sciences '16-03 Vol.41 No.03
http://dx.doi.org/10.7840/kics.2016.41.3.298

Full response를 사용하여 중계 공격에 안전한 RFID 거리제한 프로토콜

권 혜 진◆, 김 순 자°

RFID Distance Bounding Protocol to Secure Against Relay Attack by Using Full-Response

Hye Jin Kwon◆, Soon Ja Kim°

요 약

본고에서는 중계 공격 성공확률을 낮추기 위해 RFID 리더가 무요청(void challenge)을 보내더라도 태그가 응답하는 거리 제한 프로토콜을 제안한다. Full challenge 비율에 따른 공격 성공 확률을 분석하고, 기존의 프로토콜과 비교 분석하여 제안 프로토콜의 공격 성공 확률이 낮음을 보인다.

Key Words : RFID authentication, distance bounding protocol, mafia fraud, relay attack, impersonation

ABSTRACT

We propose a RFID distance bounding protocol that RFID tag still responds when reader sends a void challenge in order to reduce the probability of a relay attack. We analyze the success probability of relay attack depending on the full challenge ratio. Our experimental results show that our protocol is secure to relay attack.

Ⅰ. 서 론

중계 공격은 사칭을 목적으로 취하는 공격으로 마피아 공격(mafia fraud)으로도 알려져 있다. 중계 공격의 공격자는 정당한 리더와 리더의 인식 영역 외부에 있는 태그 사이에서 메시지를 그대로 전달(relay)하여 정당한 태그로 사칭하는 것이 목표이다. 일반적인 프로토콜에서는 중계 공격 성공 확률이 100%이지만 거리 제한 프로토콜에서는 메시지 왕복 시간을 통해 거리를 추정하기 때문에 공격자가 메시지를 중계할 경우 메시지 왕복 시간이 길어지게 되어 정당한 리더는 중계 공격이 발생하였음을 인지할 수 있어 공격 성공 확률을 낮출 수 있다. 따라서 공격자는 리더의 질의가 오기 전 태그에게 임의의 챌린지로 질의하여 그 응답에 대한 정보를 얻거나(사전 질의 전략), 리더의 질의에 임의로 응답하는 전략을 취해야 하는데 두 가지 전략 중 공격 성공 확률이 높은 전략을 취해 중계 공격을 시행한다. 이런 거리 제한 프로토콜은 비교적 시간이 소요되는 연산을 통한 인증 정보 생성 등의 거리 측정 사전 준비를 하는 느린 단계와 n 라운드 동안 빠르게 메시지를 교환하여 태그와 리더의 거리 상한선을 계산하고 인증을 수행하는 빠른 단계로 구성된다.

Hancke와 Kuhn은 RFID 거리 제한 프로토콜을 처음 제안하였는데(이하, HK 프로토콜[1]), 이 프로토콜에서 태그는 공격자가 질의를 보내더라도 정당한 응답을 해 중계 공격 성공 확률이 높았다. 이에 Munila와 Peinado는 태그가 공격자의 개입을 감지할 수 있도록 void challenge(무요청)를 사용하는 프로토콜(이하, MP 프로토콜[2])을 제안하였다. void challenge의 비율이 높을수록 태그에게는 공격을 감지 당하기 쉽지만 리더에게 void challenge를 받은 경우 무응답으로 일관하면 되므로 실제로는 공격 성공 확률이 높아진다. 이에 본고에서는 리더가 void challenge를 보내더라도 응답하는 프로토콜을 제안하고 기존의 프로토콜과 성능을 비교 분석한다.

Ⅱ. 연구 배경

HK 프로토콜[1]에서 리더와 태그는 비밀 정보 K를 공유하며, 느린 단계에서 리더가 생성한 난수 N_R을 교환한 후 라운드 수의 두 배인 $2n$비트의 해시 값 $h(K\|N_R)=R^0\|R^1$을 생성한다. 해시 값을 생성한 후 리더는 태그에게 1 비트의 질의(challenge)를 보내 빠른 단계를 시작한다. i라운드에서 리더의 질의 C_i

※ 이 논문은 2012학년도 경북대학교 학술연구비에 의하여 연구되었음.
◆ First Author : College of IT Engineering, Kyungpook National University, heyjk90@gmail.com, 정회원
° Corresponding Author : College of IT Engineering, Kyungpook National University, sjkim@ee.knu.ac.kr, 종신회원
논문번호 : KICS2016-01-021, Received January 29, 2016; Revised February 24, 2016; Accepted February 25, 2016

$(1 \le i \le n)$는 0 또는 1이 되며, 리더는 C_i를 보낸 직후 타이머를 작동시킨다. 이 C_i를 받은 태그는 즉시 R^{C_i}로 응답하고, 응답을 받은 리더는 타이머를 정지시키고 메시지 왕복 시간을 통해 거리의 상한선을 계산하고 R^{C_i}가 올바른지 확인한다. 만약 거리의 상한선이 일정 수준 이상이거나 태그의 응답이 올바르지 않을 경우 리더는 중계 공격이 발생한 것으로 간주하고 프로토콜을 종료한다.

사전 질의 전략에서 공격자는 정당한 리더와 태그 사이에서 오가는 메시지를 전달하여 느린 단계를 중계(relay)한 후, 리더가 빠른 단계를 시작하기 전 태그에게 먼저 챌린지 C_1^A를 보내 빠른 단계를 진행한다. 그 후 정당한 리더가 보내는 챌린지가 자신이 보낸 챌린지와 일치하는 경우 태그의 응답을 그대로 전달하고, 일치하지 않는 경우 임의의 비트로 응답한다. 공격자가 리더의 챌린지가 오기 전 미리 태그에게 챌린지를 보내 그에 대한 응답을 받아놓기 때문에 메시지 왕복 시간이 짧다. 이로 인해 리더는 응답을 하는 태그가 근방에 있다고 간주하고 인증을 수행하며 이때 공격자의 성공 확률은 $\left(\frac{3}{4}\right)^n$이 된다. 사전 질의 없이 공격할 경우 빠른 단계의 리더의 챌린지에 임의로 응답하며 이 경우 공격 성공 확률은 $\left(\frac{1}{2}\right)^n$이 되어 공격자는 HK 프로토콜을 공격할 때 성공 확률이 높은 사전 질의 전략을 취해 중계 공격을 수행하며 공격 성공 확률은 $\left(\frac{3}{4}\right)^n$이 된다[1].

MP 프로토콜[2]에서 리더와 태그는 느린 단계에서 각각 난수 N_R, N_T를 생성하고 교환한 후 사전에 공유한 비밀 키 K를 통해 $h(K\|N_R\|N_T) = P\|v$를 생성한다. 빠른 단계에서 리더는 P가 0일 경우 요청을 보내지 않고, 1일 경우에만 0 또는 1로 요청을 보낸다. 이로 인해 태그는 P가 0임에도 리더가 요청을 보내거나, P가 1임에도 요청을 보내지 않으면 공격자가 개입된 것으로 간주하고 프로토콜을 종료한다. 이 외에 리더의 요청이 0인 경우 v의 가장 오른쪽 비트를, 1인 경우 v의 가장 왼쪽 비트를 보낸 후 사용한 비트는 비트열에서 삭제한다. 또 리더의 요청이 없는 경우 태그도 응답하지 않는다[2].

MP 프로토콜에 대한 중계 공격 성공 확률은 비트열 P에서 요청(full challenge)의 비율(p_f)과 라운드 수에 따라 달라진다. 사전 정보 없을 때 공격 성공 확률은 $\left(1-\frac{p_f}{2}\right)^n$이 되며, 사전 질의 전략을 취할 경우 공격 성공 확률은 $\left(\left(1-\frac{p_f}{4}\right)\left(1-2p_f+2p_f^2\right)\right)^n + \sum_{i=1}^{n} 2p_f(1-p_f)\left(1-2p_f+2p_f^2\right)^i\left(1-\frac{p_f}{4}\right)^{i-1}\left(\frac{1+p_f}{2}\right)\left(1-\frac{p_f}{2}\right)^{n-i}$이 된다. 공격자의 성공 확률을 낮추기 위해서는 두 전략 모두 성공 확률이 낮아야 한다. 그림 1에서 MP 프로토콜의 빠른 단계가 20, 50 라운드로 구성될 때 풀 챌린지의 비율 p_f에 따른 공격 성공 확률을 보여준다. 태그에게 사전 질의를 할 때의 공격 성공 확률로 무요청의 비율$(1-p_f)$이 클 경우 무응답으로 대답하는 비율이 크므로 공격 성공 확률이 높아짐을 볼 수 있으며 요청의 비율(p_f)이 1에 가까울수록 태그가 공격자의 존재를 감지할 확률이 낮아지면서 태그로부터 얻을 수 있는 정보가 많아져 공격 성공 확률이 높아짐을 볼 수 있다. 사전 정보 없이 공격하는 경우에는 p_f가 클수록 응답을 예측해야하는 횟수가 많아지므로 성공 확률이 낮아짐을 볼 수 있다.

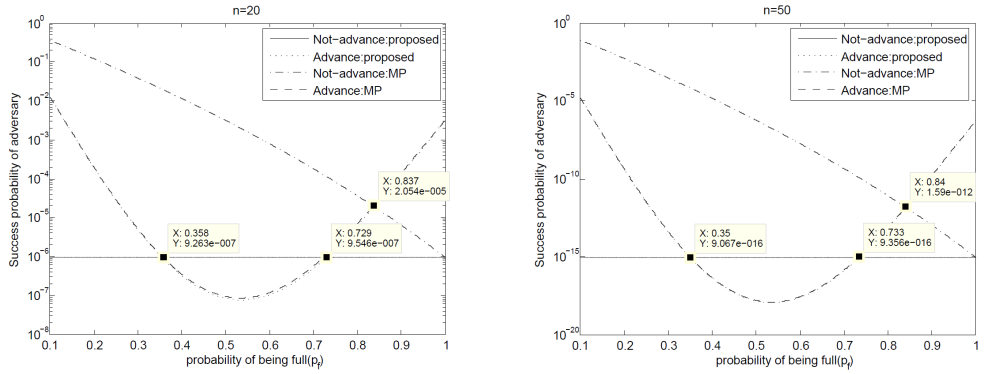

그림 1. 라운드 별 MP프로토콜과 제안 프로토콜의 전략별 공격 성공 확률 비교
Fig. 1. Comparison of Adversary's success probability

Ⅲ. 제안하는 프로토콜

우리는 앞 장에서 MP 프로토콜을 따를 경우 리더가 무요청을 보낼 경우 태그도 무응답하여 공격자가 사전질의 없이 공격할 때 공격 성공확률이 높아짐을 확인하였다. 이에 이 장에서는 리더가 무요청(void challenge)하더라도 태그는 사전 계산 정보를 통해 응답을 전송하는 프로토콜을 제안한다. 우선 느린 단계에서는 HK 프로토콜과 같이 리더와 태그는 리더가 생성한 난수 N_R을 공유하고, 비밀 키 K를 통해 $2n$ 비트 해시 값 $h(N_R \| K) = P \| Q$을 생성한다. 빠른 단계에서 리더는 n 비트열 P를 통해 요청을 할 것인지 ($P_i = 1$) 무요청을 할 것인지($P_i = 0$) 결정하고 요청을 보낸다면 타이머를 작동시키고 태그의 응답이 오면 타이머를 정지시켜 거리 추정과 인증을 수행한다. 태그는 $P_i = 1$인데 리더가 요청을 보내지 않거나, $P_i = 0$인데 요청을 보내는 경우는 공격자가 개입된 것으로 간주하고 프로토콜을 종료한다. 그 외에 $P_i = 0$이고 리더가 요청을 보내지 않은 경우나 $P_i = 1$이고 리더의 요청이 0인 경우에는 Q_i로 응답하며, $P_i = 1$이고 리더의 요청이 1인 경우에는 $Q_i \oplus K_i$로 응답한다.

제안 프로토콜에서 사전 정보 없이 공격할 경우 무요청에도 응답해야 하므로 공격 성공 확률은 $\left(\frac{1}{2}\right)^n$이며, 요청(full challenge)의 비율을 p_f라 하고 태그에게 사전 질의를 하는 전략을 취할 때 중계 공격 성공 확률은 $\left(\left(1-\frac{p_f}{4}\right)\left(1-2p_f+2p_f^2\right)\right)^n +$ $\sum_{i=1}^{n} 2p_f(1-p_f)\left(1-2p_f+2p_f^2\right)^i\left(1-\frac{p_f}{4}\right)^{i-1}\left(\frac{1}{2}\right)^{n-i+1}$이 되며 이들은 그림 1의 그래프로 보여진다. 공격자는 성공 확률이 높은 전략을 통해 공격을 시도하므로 p_f를 0.36~0.7로 설정하면 공격 성공 확률이 가장 낮출 수 있다. 일반적으로 해시를 통해 생성되는 비트열에서 1의 비율은 0.5이고 이는 0.36~0.7의 범위에 들어가므로 별 다른 p_f 조정 과정이 필요 없다. 그러나 MP 프로토콜에서 두 전략의 공격 성공 확률이 모두 낮아지는 때는 p_f가 약 0.84인 경우이다. 그러나 p_f를 0.84로 설정하는 것은 현실적으로 어렵기 때문에 Munila와 Peinado는 NAND 연산을 통해 p_f를 0.75로 조정했다. 그림 1에서 보는 바와 같이 사전 질의를 할 경우 p_f에 따른 공격 성공 확률은 제안 프로토콜과 MP 프로토콜이 큰 차이가 없이 두 프로토콜 모두 낮은 공격 성공률을 보여준다. 그러나 사전 정보 없는 전략의 경우 MP 프로토콜이

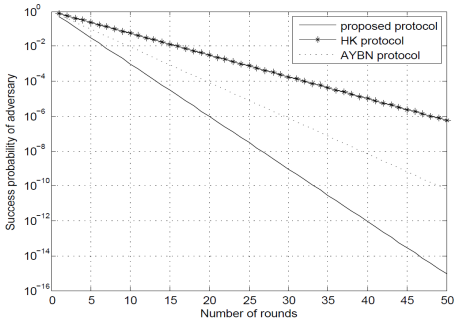

그림 2. 중계 공격 성공 확률 비교
Fig. 2. Comparison of adversary's success probability

공격 성공 확률이 높기 때문에 공격자는 성공 확률이 높은 사전 정보 없는 전략으로 접근하여 결과적으로 높은 공격 성공률을 보이게 된다.

그림 2는 각 프로토콜의 p_f를 최적으로 설정했을 때의 각 프로토콜의 라운드별 공격 성공 확률을 보여준다. 라운드 수가 커질수록 공격 성공 확률은 낮아지며 라운드 수에 관계없이 제안 프로토콜의 공격 성공 확률이 낮음을 확인할 수 있다. 즉, 같은 수준의 중계 공격에 대한 안전성을 얻기 위해 기존의 프로토콜보다 상대적으로 적은 라운드를 수행해도 됨을 의미하여 효율적임을 보여준다.

Ⅳ. 결 론

본고에서는 RFID 거리 제한 프로토콜에서 리더의 무요청에도 태그가 응답하여 중계 공격에 대해 $\left(\frac{1}{2}\right)^n$의 낮은 성공 확률을 보장하는 프로토콜을 제안하였다. 이로 인해 기 제안 프로토콜과 비교하여 같은 라운드를 수행할 경우 공격 성공률이 낮으며, 같은 공격 성공 확률을 보장하기 위해 보다 작은 라운드를 수행해도 됨을 실험 결과를 통해 보였다.

References

[1] G. P. Hancke and M. G. Kuhn, "An RFID distance bounding protocol," in *1st Int. Conf. Security and Privacy for Emerging Areas in Commun. Netw. (SecureComm 2005)*, pp. 67- 73, Sept. 2005.

[2] J. Munilla and A. Peinado, "Distance bounding protocols for RFID enhanced by using void challenges and analysis in noisy channels," *Wirel. Commun. Mob. Comput.*, vol. 8, no. 9, pp. 1227-1232, 2008.