Walsh 함수를 이용한 RFID 보안 알고리즘

황구연[0] 최진욱 신동규 신동일
세종대학교 컴퓨터공학과
hgy1999@gce.sejong.ac.kr[0], {seekpeace, shindk, dshin}@sejong.ac.kr

The RFID security algorithm using Walsh Function

Guyoun Hwang[0], Jinwook Choi, Dongkyoo Shin, Dongil Shin
Dept. of Computer Engineering, Sejong University

1. 서 론

RFID(Radio-Frequency IDentification)란 무선통신 기술을 사용하여 직접 접촉하지 않고 전파를 이용해 먼 거리에서 정보를 인식하는 기술[1]을 말한다. RFID의 편리한 인식 과정 및 넓은 인식 거리 등 다양한 장점들로 인해 그 활용 범위와 시장규모가 확대되고 있으며 이에 따라 많은 분야에서 위치추적 시스템을 도입하려는 움직임을 보이고 있다. 하지만 RFID의 보안과 관련하여 태그의 변조, 위장된 판독기, 서비스 거부 공격 등 수많은 위협이 예상되고, 특히 산업 정보의 유출과 개인의 프라이버시 보호 문제가 가장 심각한 위협으로 지적되고 있다.

RFID 기술의 부작용에 대한 우려의 목소리가 커지면서 정보유출 및 침해 위협에 대항하기 위한 보안에 관한 연구가 진행 되고 있다. 암호 기법을 적용하여 기밀성과 무결성, 인증을 보장할 수 있으며, 대칭키 암호 기법, 공개키 암호기법, 해쉬 함수 등을 이용하여 암호 프로토콜을 설계할 수 있다. 본 논문에서는 Walsh 함수를 이용하여 보안성을 높이는 알고리즘을 제안한다.

2. 본 론

Miyako Ohkubo는 Hash-Chain을 이용한 보안 프로토콜을 제시했다. 이 기법은 기존에 제안된 다른 프로토콜들에서 해결하지 못 한 전방위 보안성(리더의 요청으로 태그에 보내진 현재 정보가 노출되어도 그 정보로 이전에 생성했던 정보를 알아 낼 수 없도록 하는 것)에 대한 문제를 해결했다. 이 프로토콜은 Hash-Chain을 이용해서 새로운 정보들을 태그에 저장하고 리더에게 보내는 출력 값을 일정하지 않게 보내서 불구분성(태그가 리더의 요청에 의해 전송하는 정보가 동일한 값이 아닌 다른 값을 전송하는 것)을 보장하게 했다. 이 기법은 기존의 Hash-Lock 기법의 위치추적 문제와 Randomized Hash-Lock 기법의 전방위보안성 문제점을 해결했으나 모든 태그에 대해 Hash 연산을 수행하므로 데이터베이스에서 연산이 매우 복잡하고 리더 인증을 실시하지 않는 단방향 인증이어서 정당한 리더라도 태그를 제어하기 곤란하다는 단점[2]을 가진다.

Walsh 함수는 1923년 J.L.Walsh에 의해 직교 함수로 소개되었다. 직교의 의미는 코드 간 상관관계가 "0"이 되어 서로 간섭을 주지 않는다는 것이다. Walsh 함수는 서로 다른 코드를 곱하면(Exclusive OR), 0(또는 -1)과 1이 섞여서 나오고 이를 모두 평균하면 0이 되도록 되어 있고, 같은 코드를 곱하면 모두1이 나와서 전송된 신호에 숨어있는 데이터를 복구할 수 있게 된다. 다른 Walsh 함수를 사용한다면 한번 암호화된 데이터에 다시 암호화를 거치는 과정이 되기 때문에 원래의 신호를 복구할 수 없다. Walsh 함수는 다른 Walsh 함수뿐만 아니라 같은 Walsh 함수라도 한 비트만 동기가 맞지 않아도 다른 Walsh 함수를 곱했을 때와 같은 결과를 주기 때문에 동기를 반드시 일치 시켜야 한다.

*본 연구는 문화체육관광부 및 한국콘텐츠진흥원의 2009년도 문화콘텐츠산업기술지원사업의 연구결과로 수행되었음

Reader and Tag exchanged Message
IF($Walch\,\mathrm{Pr}\,oof\,(msgs, wcode_i)) == +1$)
return $wcode_i + random(WC)$
Else donothing

리더와 태그는 key와 Walsh 함수를 이용, 이것을 비교 판단하여 서로의 인증과정을 거치며 정보를 전송할 때마다 Walsh 함수를 사용, 매번 다른 코드를 보내고 있다. 공격자가 도청을 하더라도 Walsh 함수를 알지 못하므로 어떠한 정보인지 알지 못 한다. 리더와 태그의 정보교환이 이루진 후에 태그는 새로운 key를 갱신하여 사용함으로 공격자로부터의 접근을 차단한다. 다음과 같은 세부 단계를 거친다.

1단계 : 리더가 자신의 탐지 범위 내의 태그에게 Hash Chain 함수를 이용해 생성한 Tag Search Message를 전송한다. 메시지를 주고받을 때, 경로의 양쪽 끝에서 메시지에 대한 해쉬 값을 구해서, 보낸 쪽과 받은 쪽의 값을 비교하면 메시지를 주고받는 도중에 여기에 변경이 가해졌는지 어떤지를 알 수 있다. 불가역적인 일방향 함수이기 때문에 해쉬 값에서 원문을 재현 할 수는 없다. 또한 같은 해시 값을 가진 다른 데이터를 작성하는 것도 극히 어렵다.

2단계 : 태그는 초기화 단계에서 저장 되어 있는 Tag Search Message에 대한 해쉬 값이 일치하는지 체크한다. 동일한 값을 갖는다면 타 간섭으로 인한 메시지의 변경이 없는, 리더로부터 전송된 메시지임을 인증하며 walsh 함수를 사용하여 Response Message를 전송한다. 만약 일치하지 않는다면 공격자가 임의로 스푸핑 공격을 한 것으로 판단하고 대응하지 않는다.

3단계 : Response Message를 받은 리더는 Walsh 코드를 가진 데이터에 같은 코드를 곱하면 모두 +1이 되어 데이터를 복구할 수 있다는 성질을 이용하여 메시지의 증명과정을 거친다.
태그에서 사용된 동일한 Walsh 코드를 곱해주면 결과 값에는 모두 + 값만을 가지고 그 외 공격 신호들은 0 또는 - 값이 되어버리므로 + 값을 가진 메시지만 태그에서 보낸 메시지임을 인증한다.
0 또는 -1이라면 공격자의 재전송 공격, 또는 스푸핑으로 판단하여 데이터를 받아들이지 않는다.

4단계 : 리더와 태그는 Walsh 함수를 이용하여 Encryption ↔ Decryption 단계를 거치며 정보 전송을 한다. 역시 +1의 결과 값이 아니라면 재전송 공격, 또는 스푸핑으로 간주한다.

5단계 : 리더로부터 Complete Contact Message를 받으면 교신을 완료하고 해쉬 체인의 key를 갱신하여 리더의 Search를 기다리며 공격자의 공격에 대비한다.

3. 결 론

본 논문에서는 RFID의 보안성을 높이기 위해 기존의 Hash Chain기법에 Walsh 함수를 사용하여 상호인증을 거치며 도청공격, 재전송 공격, 스푸핑 공격, 트래픽 분석 공격, 위치 트래핑 공격 서비스 거부 공격 등에 안전할 뿐만 아니라 전방향 안전성을 제공하는 알고리즘을 제안하였다.
향후 연구로는 본 논문에서 제안한 알고리즘의 성능을 평가하기 위하여, 기존에 제안된 해쉬 기반의 알고리즘들과 비교분석을 수행할 예정이다.

[1]K. Finkenzeller, "RFID handbook", John Wiley & Sons, 1999.
[2]이병주(Byeung-Ju Lee), 송창우(Chang-Woo Song), 정경용(Kyung-Yong Chung), 임기욱(Kee-Wook Rim), 이정현(Jung-Hyun Lee), RFID 시스템에서 Hash-Chain기반 Tag-Grouping을 이용한 안전하고 효율적인 데이터베이스 검색, 한국콘텐츠학회논문지 제9권 제9호, 2009. 9