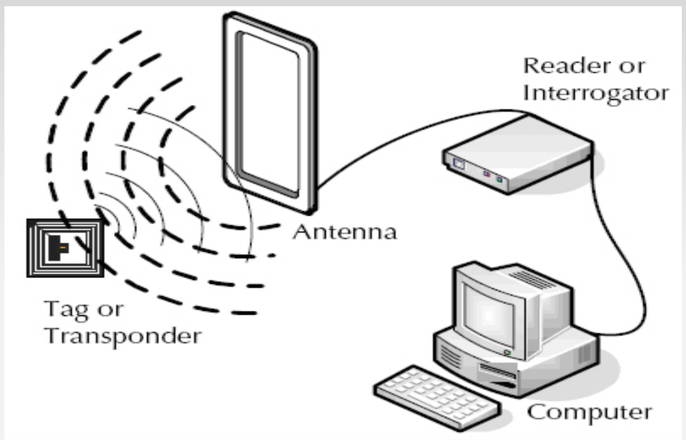
RFID 보안 기법 취약성 분석 및 시뮬레이션

Team – Read Me If You Can
윤자은, 최 경, 김준석
Professor: 송주석 Assistant: 함형민

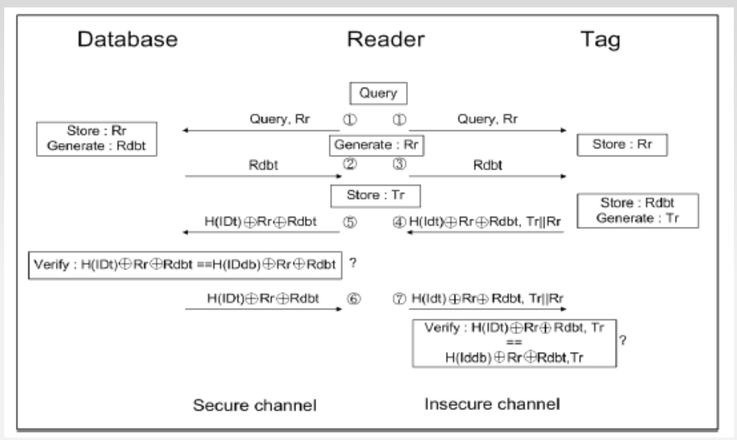
연세대학교 공과대학 컴퓨터과학 전공

1. 연구 주제

'RFID'는 사물의 자동 인식을 위해 무선주파수를 이용하는 기술이며 현재 교통카드, 출입구보안, 재고관리 등 실생활과 산업 전반에서 사용되고 있다.
사물에 부착하는 태그(Tag)와 태그의 정보를 취득하는 리더(Reader)사이 에서 태그의 내장된 정보를 리더가 무선주파수를 이용해 취득하게 되는데 리더와 태그간의 무선 통신 구간에서 보안 문제가 발생하게 된다. 위의 보안 문제에 대한 RFID 보안 기법의 취약성 분석과 시뮬레이션을 통한 연구의 필요성 확인이 우리 연구의 목적이다.



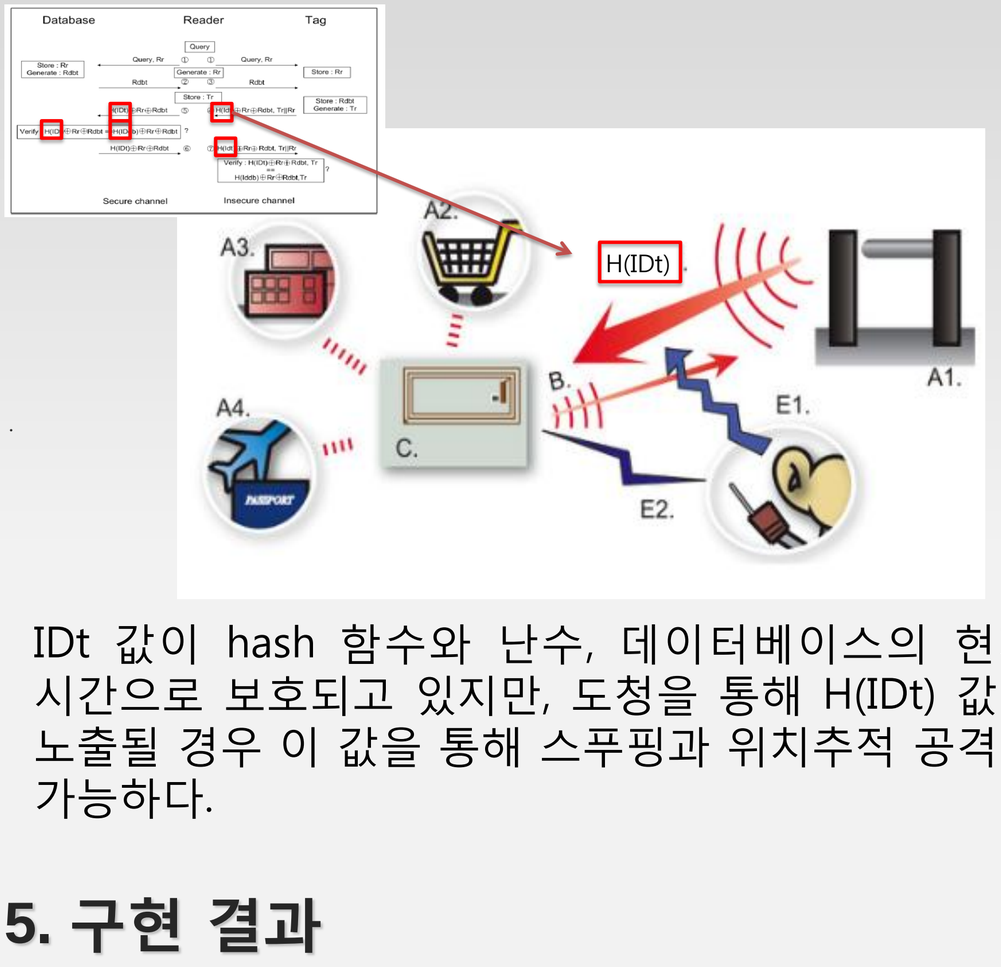
2. 기존 보안 기법 분석



우리가 분석한 보안 기법은 '해시함수 기반의 새로운 저비용 RFID 상호인증 프로토콜' 이다. 이는 RFID의 보안 기법으로써 태그 고유의 비밀 인증 정보 IDt를 태그와 리더가 사전에 공유한다는 가정으로부터 시작된다.

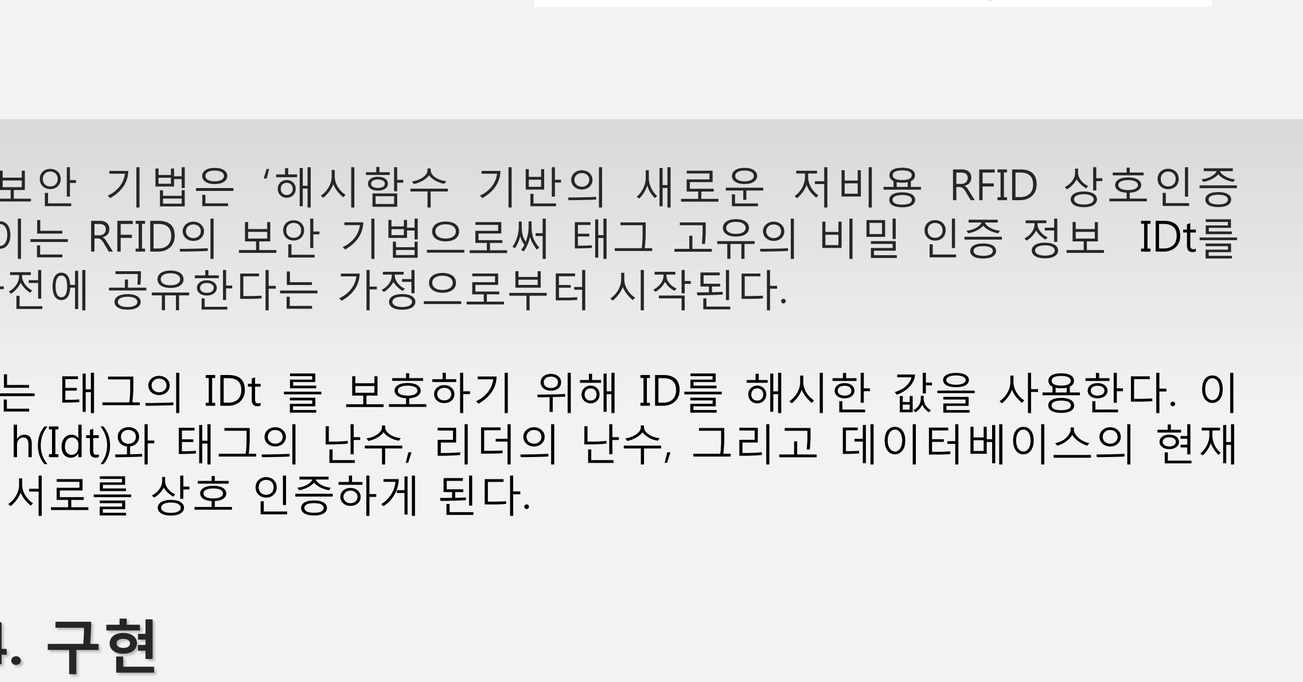
이 프로토콜에서는 태그의 IDt 를 보호하기 위해 ID를 해시한 값을 사용한다. 이 IDt를 Hash한 값 h(Idt)와 태그의 난수, 리더의 난수, 그리고 데이터베이스의 현재 시간을 이용하여 서로를 상호 인증하게 된다.

3. 취약성 분석



IDt 값이 hash 함수와 난수, 데이터베이스의 현재 시간으로 보호되고 있지만, 도청을 통해 H(IDt) 값이 노출될 경우 이 값을 통해 스푸핑과 위치추적 공격이 가능하다.

4. 구현



통신 프로토콜을 구현하여 리더의 태그 인식 및 정보 취득을 확인하고 주요 보안 취약점인 스니핑 공격과 스푸핑 공격의 구현을 통해 RFID의 보안 문제와 연구의 필요성을 확인한다.

5. 구현 결과

결론: Hash 함수를 이용하여 Data를보호하여도 Spoofing 공격에 취약하다.

Basic Mode

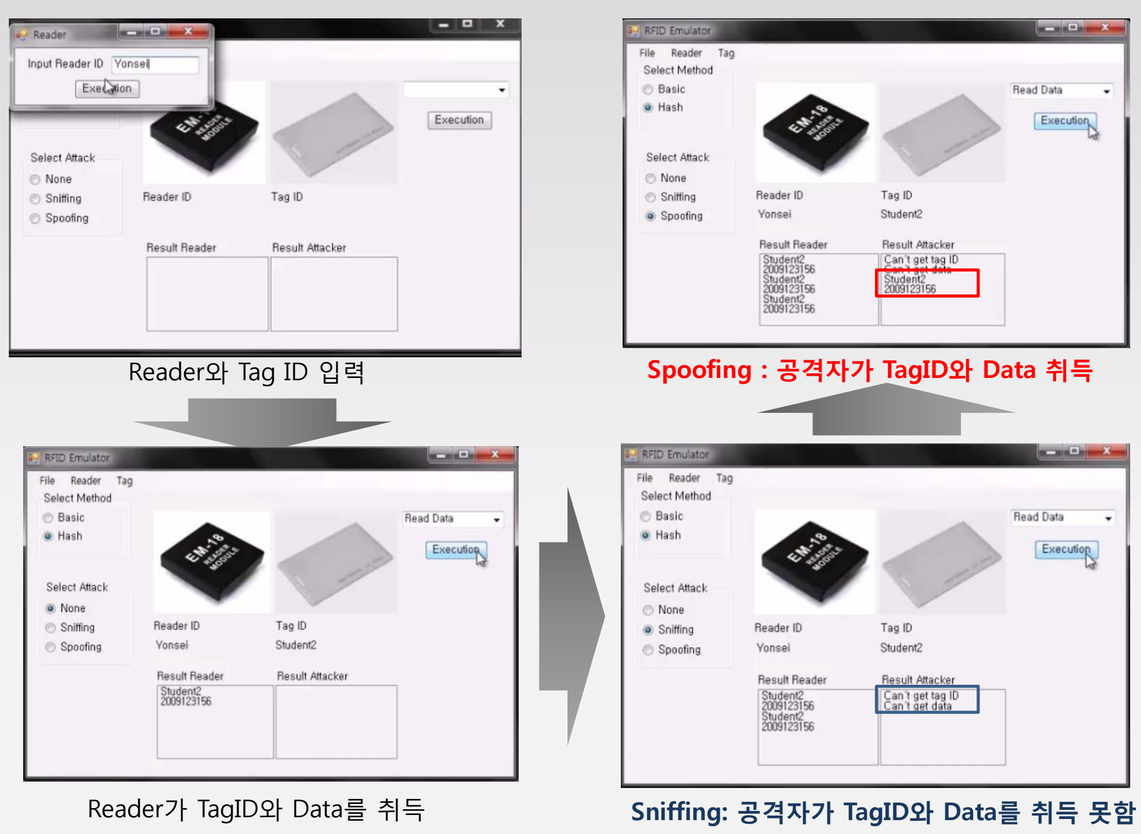
Reader와 Tag ID 입력

Spoofing 공격: 공격자가 TagID와 Data 취득

Reader가 TagID와 Data를 취득

Sniffing 공격: 공격자가 TagID와 Data를 취득

Hash Mode



Reader와 Tag ID 입력

Spoofing : 공격자가 TagID와 Data 취득

Reader가 TagID와 Data를 취득

Sniffing: 공격자가 TagID와 Data를 취득 못함