13주 2강.
정보통신 다양한 기술(1)

◆ RFID 정의 및 개요

- RFID
  - RFID(Radio Frequency Identification)는 소형 전자칩과 안테나로 구성된 전자 태그를 사물에 부착하여 전자 태그의 고유 주파수를 통해 사물을 인식하거나 사물이 주위 상황을 인지할 수 있게 하고, 기존 IT시스템과 실시간으로 정보 교환/처리를 할 수 있도록 하는 기술
- RFID 시스템 구성요소
  - RFID 시스템은 리더(Reader 또는 Interrogator), 안테나, 태그(Tag 또는 Transponder)로 구성
- RFID의 방식구분
  - 태그 의 읽고/쓰기 능력, 태그의 전원유무, 리더, 태그간 주파수방식(Air Interface)으로 구분

RFID

- 기본 동작 원리
  - 리더인 RF 캐리어 신호를 태그에 송신하고, 신호를 받은 태그는 RF 신호가 들어오면 이것의 진폭 또는 위상을 변조하여 태그의 저장된 데이터를 리더로 송신한다. 태그로부터 되돌려 받은 변조 신호는 리더에서 복호/복조화되어 태그 정보가 해독된다. 운용 목적에 따라 운용 소프트웨어에 의해 RFID 시스템을 제어한다.
  - 그룹 아이디를 갖는 바코드와 달리 태그는 고유 아이디(Unique ID)를 가진다.
  - 이론적으로 태그의 안테나를 크게 하고 리더의 송신 출력을 크게 하면 태그와 리더 간의 통신거리가 멀어질 수 있으나, 이는 주파수 혼선, 환경 및 인체 영향 문제 등이 발생할 수 있어 국내 전파법 등 전파 관련법에 의해 규제되고 있다.

RFID

RFID 방식별 구분		주요 특징
태그 Read /Write 능력	Read only	. 제조 시 데이터 기록, 정보내용은 변경 불가 . 가격 저렴, 바코드와 같이 단순인식 분야사용
	WORM	. 사용자가 데이터 기록 후 변경이 불가
	Read/Write	. 몇 번이고 기록 및 데이터변경 가능 . 고가이나 다양한 분야에서 고도의 활용이 가능
태그 전원유무	능동형 (Active)	. 태그에 배터리 부착, 수십m 원거리 통신용 . 가격 고가, 수명 제한, UHF대역 이상에서 사용
	수동형 (Passive)	. 태그에 배터리가 없으며, 10m 이내 근거리 통신용 . 가격 저렴, 수명 반영구적(약 10년 이상)
무선 주파수 대역	135kHz이하	. FA용, 동물인식 등 근거리 용도로 활용 . 시스템 가격이 저렴
	13.56MHz	. IC 카드, 신분증 등 1m 이내에서 활용 가능 . 데이터 전송상의 신뢰성이 높음
	UHF	. 433MHz(능동형), 860-930MHz 대역을 이용 . 마이크로파 대역에 비해 무선인식 성능이 우수 . ISO/IEC, EPC 태그 등 국제적으로 활성화 전망
	마이크로파	. 2.45GHz의 ISM 대역 이용 . UHF대역에 비하여 수분,금속 적용환경에서 인식율 저하

RFID

- 바코드
  - 코드를 개별적으로 하나씩 읽어 정보를 수동으로 인식
  - 근거리에서 작동, 재입력이 불가능
  - 제한된 정보만 제공
- RFID 태그
  - 다량의 복수 정보를 동시에 인식하여 읽거나, 입력을 자동화할 수 있다.
  - 무선 신호의 세기에 따라 거리를 자유롭게 조절할 수 있고 다양한 변조방식을 이용하여 비교적 많은 정보를 인식
  - 입력된 정보의 수정 또는 재입력이 가능
  - 정보의 양 수십 Kbyte 가능
  - 가격이 비싸지만 재사용,손상도,활용도,사용기간 등을 고려 경제적
  - 다양한 분야에 응용, 기술 발전 시 대량생산

RFID

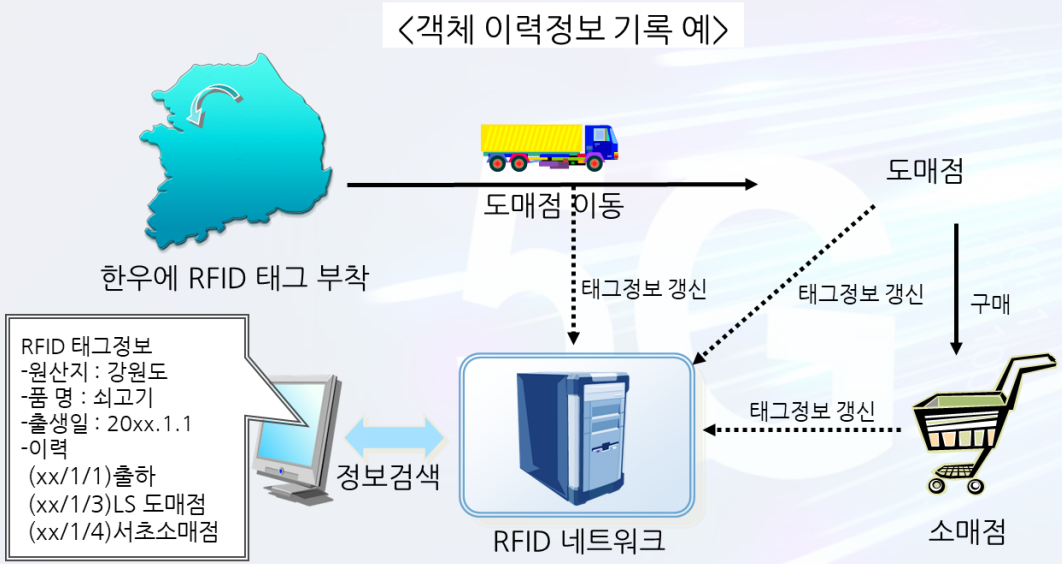
- 전력 공급 방식에 따른 분류
  - 수동형 태그 : 일반적으로 사용되는 저렴한 태그. 리더로부터 전력을 공급받음. 리더로 후방 산란 변조를 통해 데이터를 전송.
  - 능동형 태그 : 내장 배터리 사용. 능동 송신부 내장으로 향상된 인식거리, 배터리 수명에 따라 사용기간 제한됨. 크기와 무게가 크고 가격도 올라감.
  - 반수동형 태그 : 자체 전원을 내장하고 있어 태그의 일부 기능을 리더와 독립적으로 수행. 통신은 수동형 태그와 같이 후방 산란 변조 사용

RFID

- 주파수에 따른 분류
  - LF (125, 135KHz) 와 HF (13.56 MHz) 대역
    - 코일을 이용한 유도성 결합(inductive coupling) 방식
    - 인식 거리가 제한되고, 데이터 양과 전송속도의 한계
    - 액체나 인체 등에 영향을 받지 않으나 전도성 물체에는 영향을 받음
  - UHF (433, 910MHz)와 마이크로파 (2.45GHz) 대역
    - 안테나를 이용한 전자파 결합(Electromagnetic coupling) 방식
    - 먼 거리 통신이 가능하고 데이터 처리량과 속도가 빠른 장점
    - 도체 기술의 발전에 따라 최근 저가격의 태그에 대한 관심이 증대됨

- RFID 네트워크 개요
  - 정의 : RFID 태그가 부착된 객체(예 : 물품 등)의 정보가 저장된 시스템
  - 구성요소 : RFID 디렉토리 시스템과 RFID 정보 서버로 구성

- RFID 네트워크가 필요한 이유
  - RFID 태그 메모리 사이즈의 한계
  - 객체 정보의 변동이 있을 경우 저비용으로 정보의 실시간 Update 가능



- 주파수에 따른 RFID 특성

구 분	LF	HF	UHF		마이크로파
	125.134KHz	13.56MHz	433MHz	900MHz	2.45GHz
액체	거의 없음	거의 없음	크게 받음	크게 받음	크게 받음
목재	받지 않음	받지 않음	받지 않음	받지 않음	받지 않음
금속	거의 없음	크게 받음	크게 받음	크게 받음	크게 받음
유리 (無코팅)	거의 없음	거의 없음	거의 없음	거의 없음	거의 없음

- 대상에 따른 적재 및 부착

대상 물체	특성	예시
전파를 반사하는 물체	- RF 영역 내의 물체는 전파를 반사한다. - 대상물 건너편의 태그 인식 불가	철제 제품
전파를 반사하지 않는 물체	- 전파가 물체를 통과 하거나 아주 극소량 반사된다. - 건너편의 태그를 판독 할 수 있다.	플라스틱, 목재
전파를 흡수하는 물체	- 전파를 흡수한다. - 건너편의 태그를 거의 읽지 못한다.	탄소 함유량이 많은 제품, 물
전파를 흡수하지 않는 물체	- 전파가 대상물을 통과한다. - 건너편의 태그를 판독 할 수 있다.	철제 제품이 아니거나 탄소 함유량이 많지 않은 제품

RFID 보안

- RFID 프라이버시 정의 및 특징
  - 프라이버시 : 개인에 관한 정보
  - RFID와 프라이버시의 연계 : RFID 리더 통해 판독되는 해당 개인정보 일체
- RFID 태그 정보와 개인정보와의 연계 예시
  - 백화점, 마트 등 매장의 물품판매 목록과 고객정보 연계
  - 공공도서관에서 특정 도서와 대여한 사람의 개인정보 연계
  - 병원에서 수술, 응급 환자의 병력정보와 환자정보 연계

- RFID 프라이버시 위험요인

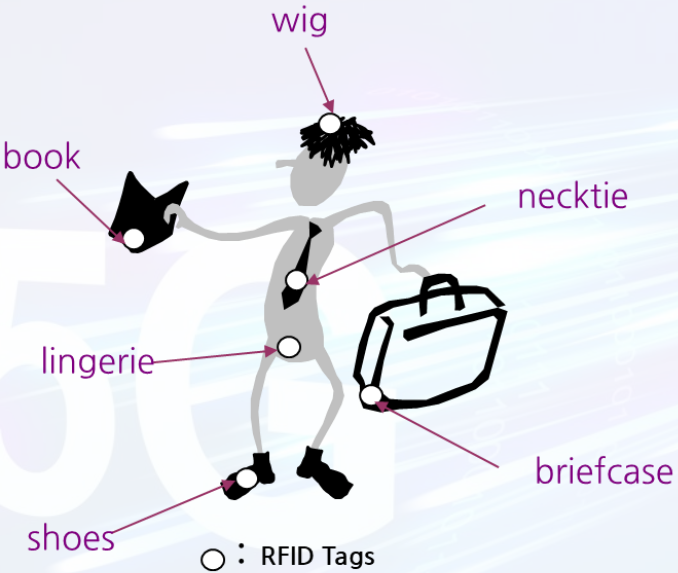
(1)

RFID Reader

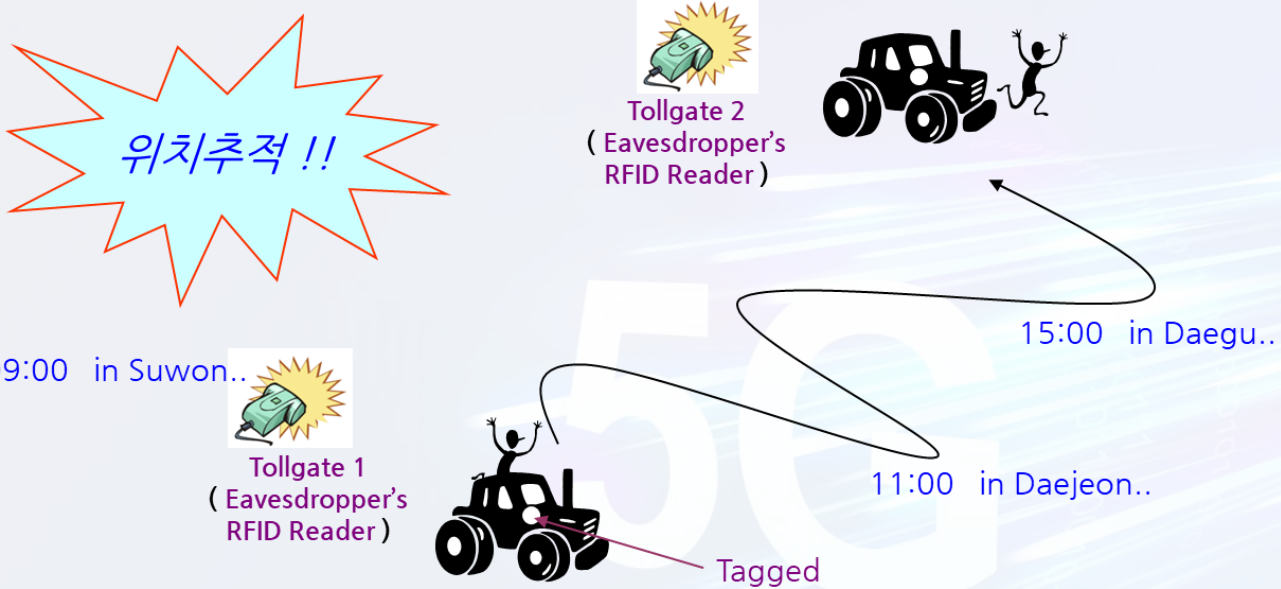
⋮

- book - *yellow journal…*
- shoes - *imitation leather…*
- lingerie - *maker, size…*
- wig - *nylon.. bald head…*
- necktie - *maker, price…*
- briefcase - *imitation…*

⋮



(2)


18:00 in Busan..
위치추적 !!
Tollgate 2
(Eavesdropper's
RFID Reader)
15:00 in Daegu..
09:00 in Suwon..
Tollgate 1
(Eavesdropper's
RFID Reader)
11:00 in Daejeon..
Tagged

RFID 보안

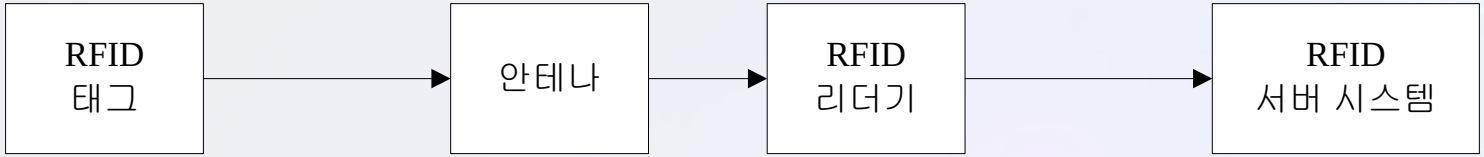
- 프라이버시 보호 가이드라인의 필요성 및 성격
  - RFID는 사물에 대한 정보를 효율적으로 처리할 수 있도록 하여, 물류·운송·유통·내부 재고관리 등에 획기적인 개선을 가져올 것이 예상 되는 반면, 개인이 RFID 태그가 부착된 사물을 착용·휴대할 경우, RFID 태그 내 고유 정보가 판독되어 개인에 대한 성향 파악 및 위치추적 등에 오·남용되거나, 개인 프라이버시를 침해할 수 있다는 우려 증대 이에 따라 가이드라인은 RFID 태그, 리더기를 비롯한 전체 시스템을 취급함에 있어 준수하여야 할 기준을 제시함으로써 취급사업자는 제시된 기준 하에서 사업을 안정적으로 추진할 수 있고 이용자는 프라이버시에 대한 우려를 최소화할 수 있음. RFID를 활용한 신규 서비스 증가로 프라이버시 침해 우려가 높아짐에 따라, 법적 규제, 가이드라인이 필요

RFID 보안

- RFID 프라이버시 보호 원칙
  - 공정 정보 규정의 원칙
    - 개방성 혹은 투명성
    - 목적에 대한 기술
    - 수집 제한
    - 책임
    - 안전 보호 RFID 사업 추진 시 프라이버시 보호 원칙의 적용
  - RFID 도입 단계 : 개인 정보 기록의 제한
    - RFID 부탁/ 탈착 : 부착 사실 등 설명, 표시
    - RFID 수집(Reading) : 개인 정보 수집 제한
    - RFID 연계 : 물품 정보와 개인정보의 연계 제한
    - RFID 저장 / 이용 / 제공 : 개인정보의 이용 / 제공 제한

RFID 보안

- RFID 시스템에서의 주요 침해 기술들



위조
물리적 공격

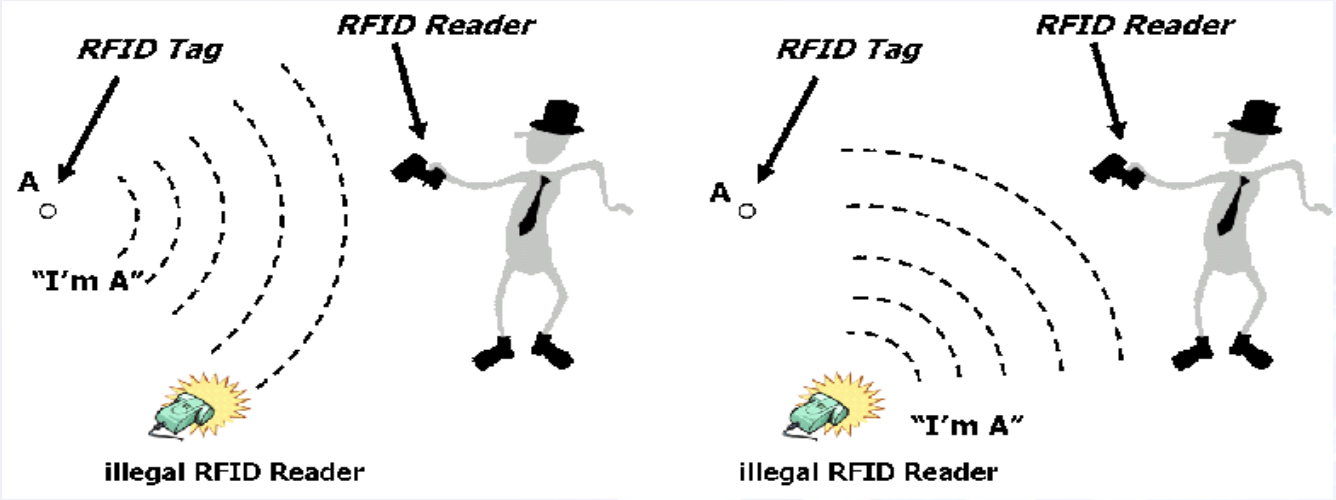
도청공격
트래픽 분석
가로채기
재생고격
중간자 공격

스니핑
스프핑
스캐닝
서비스 거부 공격
버퍼오버플로우

RFID 보안

- RFID에 대한 일반적인 공격기법

도청공격과 재전송 공격

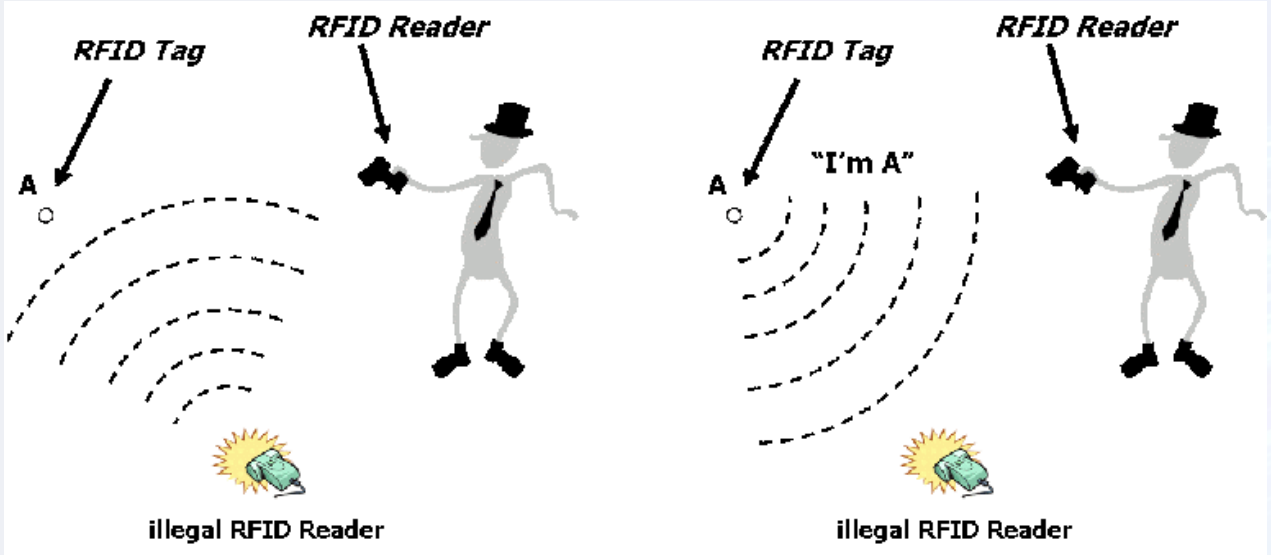


(a) 도청 (b) 재전송

RFID 보안

- RFID에 대한 일반적인 공격기법

RFID 시스템에 대한 스푸핑 공격



(a) 불법적인 스캔 (b) 태그의 응답

RFID 보안

- RFID에 대한 일반적인 공격기법
  - 스니핑(Sniffing, 엿보기) : 네트워크상의 전송되는 패킷 정보 또는 모든 정보를 송수신자가 인지하지 못하는 상태에서 읽어 보는 것
  - 스푸핑(Spoofing, 위장하기) : 승인 받은 사용자인 것처럼 가장하여 시스템에 접근하려는 행위, 네트워크상에서는 허가된 주소로 가장하여 접근 통제를 우회할 수 있음
  - 서비스 거부(DoS; Denial of Service)공격 : 공격자가 여러 대의 장비 또는 시스템을 이용해 표적 시스템이 처리하지 못할 정도의 엄청난 데이터를 집중적으로 전송함으로써, 표적 시스템의 정상적인 기능을 방해하는 것

RFID 보안

- 물리적인 공격 방법
  - 단순 전력분석 (SPA, Simple Power Analysis) 및 차분 전력분석 (DPA, Differential Power Analysis) : 암호 알고리즘 계산 시 사용되는 암호키 값에 따라 소모 전류 변화를 이용한 공격
  - 칩 내부 공격 (Chip rewriting attack) : 마이크로 컨터롤러의 공격, ROM Overwrite 공격, EEPROM 변형 공격
  - 메모리 잔류정보 분석 공격 (Memory remanence attack) : RFID 태그 내부의 관련 데이터를 삭제하여도 삭제된 흔적(미량 전류자기)이 남는다. 데이터가 완벽하게 지워지지 않는다는 사실을 이용하여 적절한 측정 장치를 가지고 거의 모든 종류의 저장 장치에 대한 정보를 복구하는 것이 가능하며, 심지어는 여러 번의 쓰고 지우기를 반복한 후에도 이러한 공격은 유효하다.

RFID 보안

- 물리적인 공격 방법
  - 타이밍 분석 공격 (Timing analysis attack) : 암호화적 계산에 소요되는 시간이 다양하다는 사실을 이용한 공격
  - 비파괴 공격 (Non-Invasive attack) : 갑작스런 전원 이상을 이용
  - 배터리 소진 공격(Battery Burn-out attack) : RFID 리더 장치의 배터리를 짧은 시간 내에 방출시켜 장치를 더 이상 사용하지 못하게 만드는 것. 공격자는 계속적으로 리더 장치에게 데이터 전송 요청이나 연결 요청을 보내어 배터리를 소진하게 함

RFID 보안

- 주요 보안 취약점
  - 정보 유출 (데이터 보안 문제)
  - 추적 가능성 (위치 프라이버시 문제)
  - 전방향 프라이버시 (Forward Privacy) 문제 : 일시적으로 공격자에게 태그의 비밀 정보가 노출되었다고 하더라도, 그로 인하여 그 태그와 관련된 사용자에 대한 이전의 모든 행적이 다 노출될 수 있다.

RFID 보안

- 비암호학적인 방법
  - Kill tag, Faraday Cage, Active Jamming, Blocker Tag, etc.
  - XOR, concatenation, etc.
- 암호학적인 방법
  - Hash Lock, Hash Chain, Randomized Hash, External Re-encryption, etc.
  - 대칭키 사용, 비대칭키 암호 사용, etc.
- 보안 기술
  - 미들웨어에 대한 접근 제어, 리더 인증, 통신 채널 보안, 리더 관리 등
  - EPC IS에 대한 접근 제어, 사용자 인증, 응용 서비스 접근 제어, XML 보안 등
- 프라이버시 보호 기술
  - RFID 기술에 대한 프라이버시 보호를 위한 법/제도 및 기술적인 해결책 제시필요

- 태그 기능 정지 방안

Kill 명령어 기법

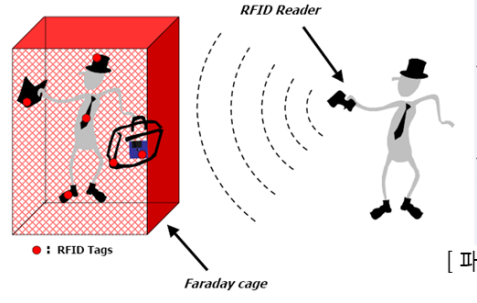
Sleep 명령과 Wake 명령어 기법

- Kill 명령의 단점 보완 위해 태그 기능을 잠시 정지 후 다시 동작하도록 하는 명령

RFID 보안

- 물리적 해결방안

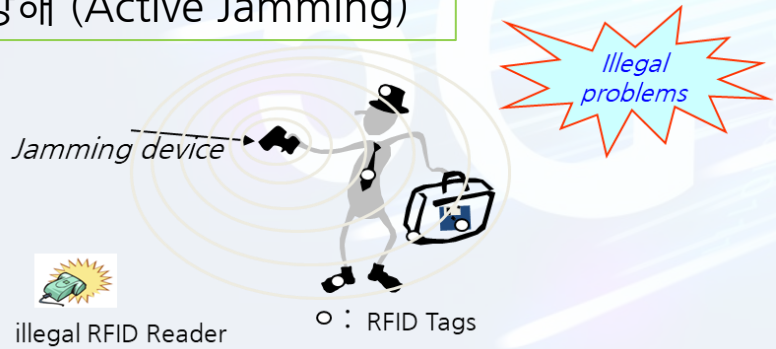
태그 차폐 (Shield the Tag)



- 전파 차단막,특정 주파수가 통과할 수 없도록
- 단점 : 도난 물건에 악용

[패러데이 케이지(Faraday Cage)]

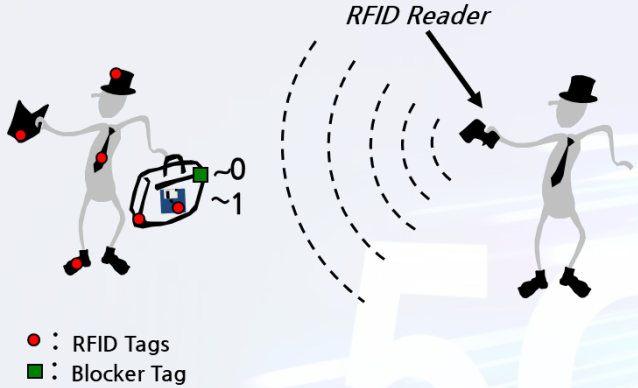
능동형 전파방해 (Active Jamming)



RFID 보안

- 물리적 해결방안

블로커 태그 (Blocker Tag)



프록싱(Proxying) 접근

- 일반 장소에 설치되어 있는 RFID 리더를 통한 정보의 보호를 대신하여 소비자들이 직접 자신만의 RFID 시스템 하의 프라이버시 보호를 위한 장비를 가지고 다니는 것

RFID 보안

- 소프트웨어적인 방법
  - 배타적 논리합(XOR), 익명(Pseudonym) 등의 저연산 기법
  - 해시 기반 및 난수 등을 이용한 기법
  - 암호화 알고리즘을 이용한 기법

수고하셨습니다.