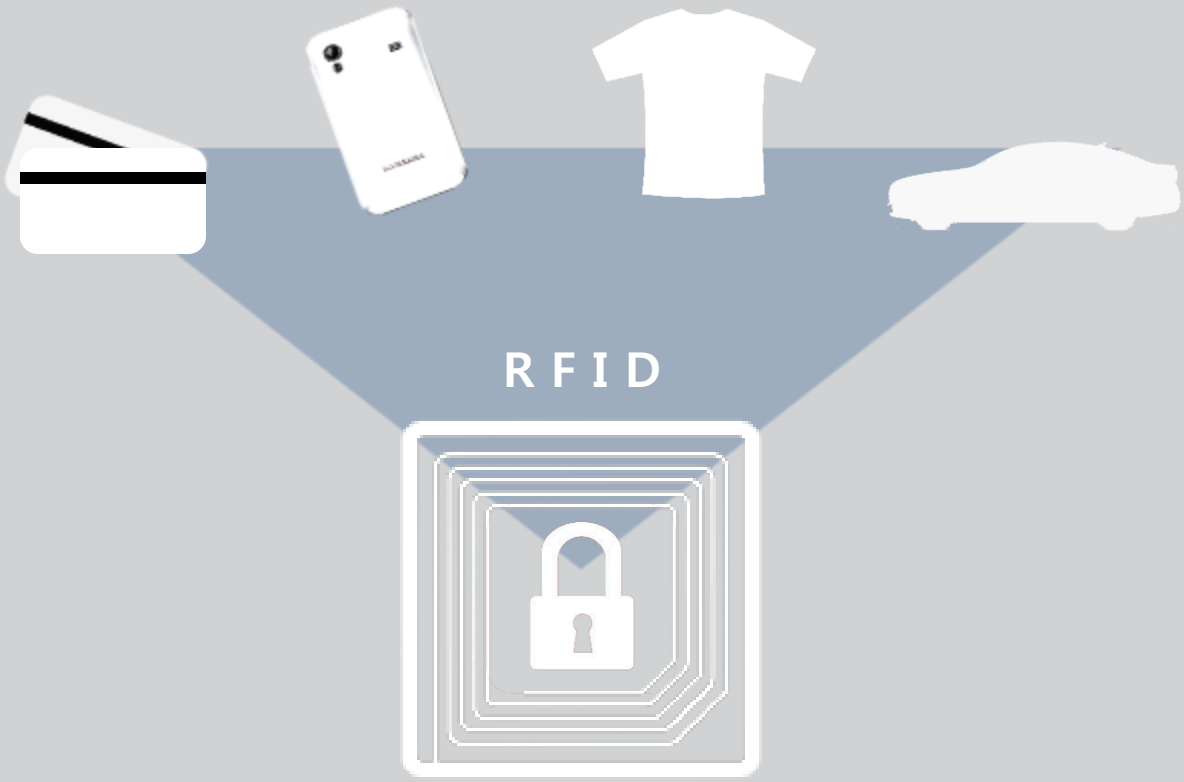
2013 2학기 소프트웨어 종합설계



RFID Security :
Enhanced Improved eMARP

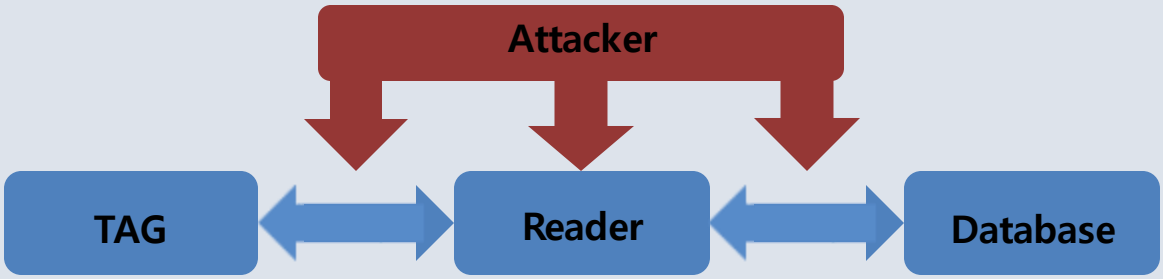
연세대학교 컴퓨터과학

신재석 심규동 정수호

지도: 송 주 석 교수님

소개

RFID (Radio Frequency Identification : 전자 태그) 는 현재 뜨거운 관심을 받고 있는 기술로, 비교적 큰 용량, 싼 가격, 무선 인식 가능 등의 장점을 가지고 있어 유통관리, 생활의 편의 등 다양한 부분에서 기존에 존재하던 바코드나 IC카드를 대체할 수 있을 것이라 큰 기대를 받고 있다.



하지만, 물리적인 접촉 없이 인식이 가능하다는 점에서 통신내용의 탈취가 쉬우며, 요청에 대해 자신이 가진 고유값을 그대로 응답하기 때문에 큰 프라이버시 문제를 갖는다.

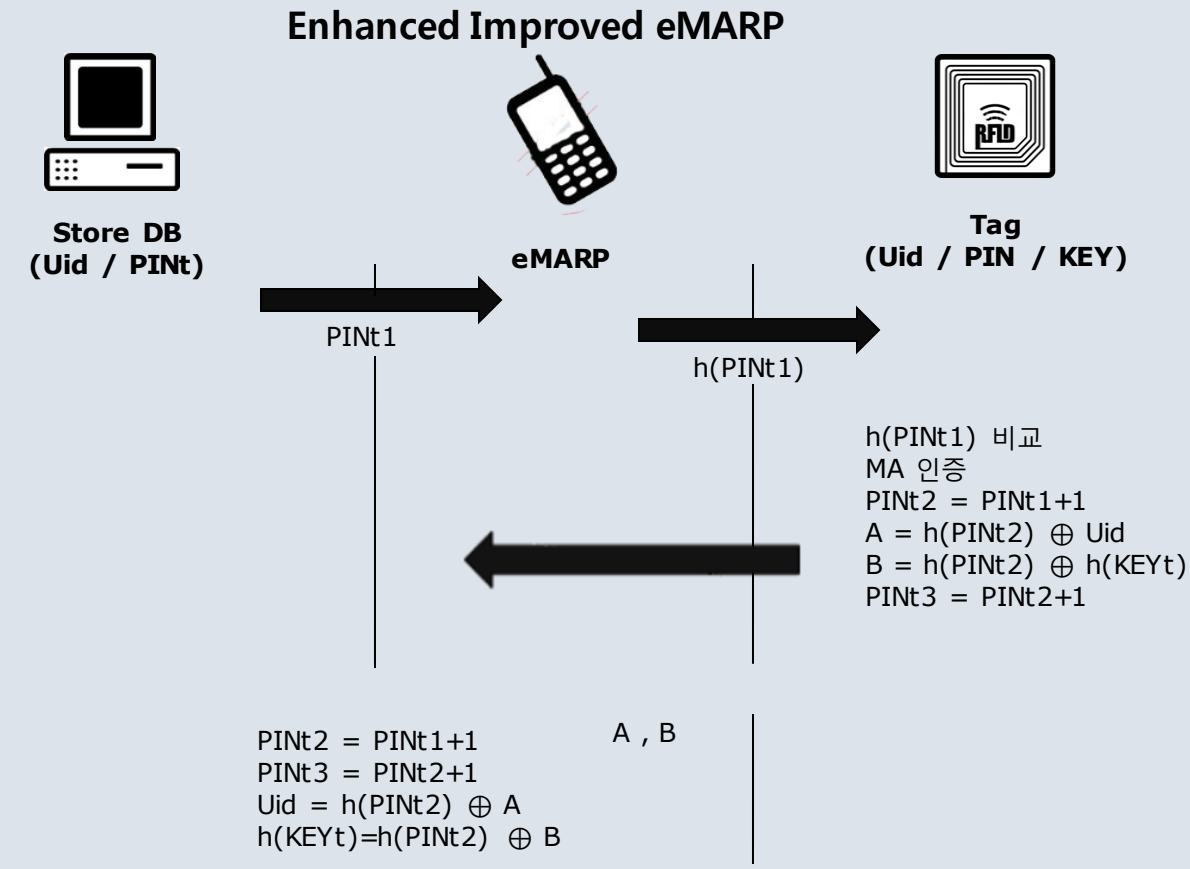
방향성

보안문제 해결에 대해 많은 방향이 있다. 하지만 하드웨어적인 제약사항을 가진 TAG 내부에서의 해결이 아닌 높은 성능을 이용할 수 있는 모바일 에이전트 기법이 주된 연구의 방향이다. 많은 개선사항들이 있었지만. 우리의 연구에서는 최근 제시된 eMARP와 Improved eMARP는 모바일 에이전트 기법을 개선하였다. 성능, 비용적인 측면에서의 보완 뿐만 아니라 보안적 이슈로 부터 안전하고 효율적인 프로토콜을 제시하고자 한다.

기존 내용	
eMARP : Privacy는 보호하지만 위치추적에 취약 -> RFID의 성능을 유지하면서 보안성 요구	**Improved eMARP :** eMARP의 단점을 보완했으나 연산량이 많음 -> 보안성을 만족하면서 효율성이 필요

개선 방향
Enhanced improved eMARP : 이전의 eMARP 시스템과 비슷한 연산량을 통해 효율성 증대 및 알고리즘 수정을 통한 보안의 강화

구현내용



STEP1 DB -> Mobile agent

- DB에서 모바일 에이전트로 태그 PIN 전송.

STEP2 Mobile agent -> Tag

- DB로 부터 받은 값을 해시하여 해시된 PIN 을 보내 인증을 받음.

STEP3 Tag 내 인증 / 업데이트

-모바일 에이전트의 인증.
(불일치시 업데이트 과정 없이 무반응)
-PIN 값의 업데이트를 통해 재전송 공격 방지.
-XOR 연산 및 eMARP / Store DB로의 전송.
-PIN 값의 업데이트 / 무응답 모드 전환.

STEP4 Tag -> Mobile agent

- PIN 값을 두 번 업데이트.
- 자신의 DB에 Uid, h(KEYt), PINt3 저장.
- 정당한 PIN 값에 대해 태그가 무응답일 경우 업데이트 후 처음부터 다시 실행.

STEP5 Cycle

- MA->Tag 인증 PIN값의 재조정.

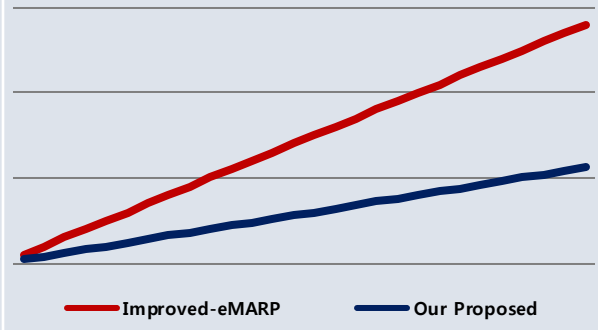
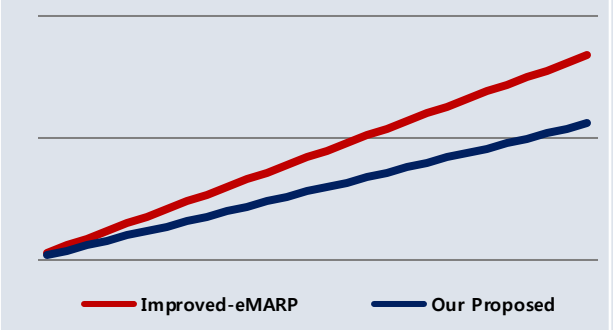
기호	설명
Uidt	태그의 유일한 아이디
KEYt	인증을 위한 태그의 비밀 값
PINt	태그 모드 변경을 위한 키
||	문자열 연접 연산
⊕	XOR 연산
h(-)	일방향 해시 함수
PINt i	I번째 수행되는 태그 모드 변경 키

분석

Security Feature

	eMARP	Improved eMARP	Our Proposed
Eavesdropping	No	No	**No**
Spoofing Attack	No	No	**No**
Tag forgery	No	No	**No**
Location Tracking	Yes	No	**No**
Disclosure	Yes	No	**No**

Performance

Tag Computation	Traffic
	

Our Proposed (= eMARP) < Improved – eMARP (≒ 40%)

Our Proposed < Improved – eMARP (= eMARP) (≒ 33%)

보안적 이슈에 대해 안정성을 지니면서 효율성이 증가

결론 / 기대효과

- **기존 기술이 가지고 있는 문제점 및 위험성에 대해 분석.**

- **새로운 기술을 제시하고** Enhanced improved eMARP**에 대해 보안 및 적합성을 분석 / 효율적인 결과의 도출.**

- **최신 기술에 대해 장단점을 파악하고 이를 보안하는 새로운 방안을 탐구 및 논문 작성.**
  (RFID 프라이버시 보호를 위한 모바일 에이전트 향상 프로토콜 2013.12)

- **RFID Mobile agent를 활용하는 분야에 대해 보다 효과적인 기술 응용이 가능할 것으로 기대.**