

# RFID 보안 알고리즘 동향 분석

† 박 두진

† 동명대학교 중소기업직업훈련컨소시엄사업단 팀장

**요 약** : 다양한 물류분야에 적용되는 RFID 기술이 보다 확산되기 위해서는 RFID 의 정보의 보안이 선행되어야 한다. 본 발표에서는 RFID 기술의 보안의 취약성과 이를 해결할 수 있는 보안 요구사항을 분석하였다. 또한 RFID 보안 기술과 보안 알고리즘 동향을 분석하였다.

**핵심용어** : RFID, 보안, 알고리즘, 메모리맵

### 1. RFID 보안 취약성 및 고려사항

- RFID 보안 취약성
  - 도청 공격
  - 트래픽 분석
  - 재전송 공격(Replay Attack)
  - 스푸핑(Spoofing) 공격
  - 태그 복제
  - 서비스 거부(DoS, Denial of Service) 공격
  - 물리적인 공격 방법

3

### 2. RFID 보안 요구사항

- RFID 서비스의 보안
- 태그와 RFID 리더 구간 보안
- RFID 미들웨어와 ODS 서버 구간 보안
- ODS 서버 구간 보안
- 정보 서버 또는 응용 서버와 ODS 서버 구간 보안
- RFID 리더와 미들웨어 및 정보 서버와 응용 서버 구간 보안
- 정보 서버 또는 응용 서버와 프라이버시 관리 시스템 구간 보안

5

### 1. RFID 보안 취약성 및 고려사항

- RFID 보안 고려 사항
  - 기밀성(Confidentiality)
  - 무결성(Data Integrity)
  - 인증(Authentication)
  - 인가(Authorization)
  - 부인방지(Non-repudiation)
  - 키 관리(Key Management)
  - RFID 위치추적 프라이버시 보호(Traceability Protection)

4

### 3. RFID 보안 기술 개발 동향

- RFID 보안 기술
  - 수동형 RFID 태그용 보안 모듈
  - 보안 RFID 통합 서비스
  - 전자계보(e-Pedigree) 기술
  - 전자봉인(eSeal) 보안 프로토콜

6

† 교신저자 정회원) djpark@tu.ac.kr

### 3. RFID 보안 기술 개발 동향

#### □ 모바일 RFID 보안 기술

- 모바일 RFID 정보보호 통합 프레임워크
- 모바일 RFID 보안 라이브러리
- 모바일 RFID 보안 미들웨어
- 모바일 WPI 확장 보안 미들웨어 기술
- 모바일 RFID 프라이버시 보호 서비스
- 보안 응용 포탈 게이트웨이 기술
- 정책 프로파일 기반 개인 프라이버시 보호 기술

7

### 4. RFID 보안 알고리즘 동향

#### □ 수동형 RFID 태그와 리더 보안 알고리즘

- 수동형 RFID 태그 메모리맵 정보
- 수동형 RFID 보안 명령/응답 메시지
- 수동형 RFID 보안 프로토콜 동작

10

### 4. RFID 보안 알고리즘 동향

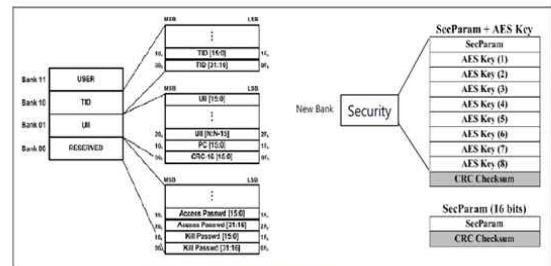
#### □ RFID 태그와 리더간 보안 알고리즘

- 태그와 리더간 도청 방지 기법
  - 트리워킹 알고리즘
  - 난수적 트리워킹 알고리즘
- 태그와 리더간 인증 기법
  - 해쉬락 기법
  - 비대칭키 동의(Asymmetry Key Agreement) 기법

8

### 4. RFID 보안 알고리즘 동향

#### • 수동형 RFID 태그 메모리맵 정보



수동형 RFID 보안태그 메모리맵 구조

11

### 4. RFID 보안 알고리즘 동향

#### □ 트리기반 RFID 보안 알고리즘

- TW (Tree-walking) 알고리즘
- QT (Query Tree) 알고리즘
- AQT (Advanced Query Tree) 알고리즘

9

### 4. RFID 보안 알고리즘 동향

#### • SecParam

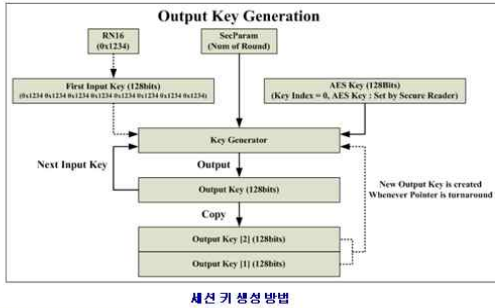
Bit	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
SecParam	SF	KS	RFU[0:1]	Round [0:3]			Key Index [0:7] (EBV)									

- SF(Secure Function) 비트
- KS(Key Setting) 비트
- Round[0:3]
- Key Index[0:7]

12

#### 4. RFID 보안 알고리즘 동향

##### • AESKey



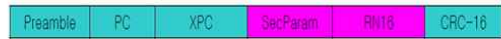
13

#### 4. RFID 보안 알고리즘 동향

##### • ACK 명령의 태그보안 응답메시지



ACK 명령에 따른 기존 응답

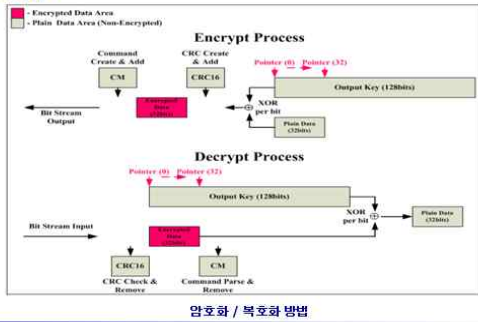


ACK 명령에 따른 보안 응답

16

#### 4. RFID 보안 알고리즘 동향

##### • AESKey



14

#### 4. RFID 보안 알고리즘 동향

##### • Update\_Key 명령/응답메시지

Update_Key Command (16+8+16+16+16 = 72 bits, Word Pointer(0x00) - SecParam)				
Command	WordPr	SecParam	RN	CRC-16
# of bits	16	8	16	16
description	0x00	handle	0x00000000	handle

Update_Key Command (16+8+16+16+16 = 72 bits, Word Pointer(0x01-0x1F) - AESKey(0x))				
Command	WordPr	AESKey	RN	CRC-16
# of bits	16	8	16	16
description	0x00	handle	0x00000000	handle

Update_Key Fauch Command (72 bits, Word Pointer(0x00) - AESKey is completed)				
Command	WordPr	CRC of AESKey	RN	CRC-16
# of bits	16	8	16	16
description	0x00	handle	0x00000000	handle

Update_Key Fauch Command (72 bits, Word Pointer(0x00) - AESKey is failed)				
Command	WordPr	AESKey	RN	CRC-16
# of bits	16	8	16	16
description	0x00	handle	0x00000000	handle

Update_Key Reply (1+16+16 = 33 bits, Reply Time(T1) within 20 ms)				
Header	RN	CRC-16		
# of bits	1	16	16	
description	0 or 1	handle	handle	

WordPr(0) Bit position (C: Completed, F: Failed)

Bit position	C	F	C	F	C	F	C	F	C	F
Word Pointer of All Reply	0	1	0	1	0	1	0	1	0	1

Fauch with Completed (C: 1, F: 0)

Bit position	C	F	C	F	C	F	C	F	C	F
Fauch with Failed (C: 0, F: 1)	0	1	0	1	0	1	0	1	0	1

17

#### 4. RFID 보안 알고리즘 동향

##### • 수동형 RFID 보안 명령/응답메시지

- ACK 명령의 태그 보안 응답 메시지
- Update\_Key 명령과 응답 메시지
- Get\_SecParam 명령과 응답 메시지
- Sec\_ReqRN 명령과 응답 메시지
- Req\_Auth 명령과 응답 메시지

15

#### 4. RFID 보안 알고리즘 동향

##### • Get\_SecParam 명령/응답메시지

Get_SecParam Command (16+16+16 = 48 bits)				
	Command	RN	CRC-16	
# of bits	16	16	16	
description	0xE101	handle	handle	

Get_SecParam Reply (1+16+16+16 = 49 bits)				
	Header	SecParam	RN	CRC-16
# of bits	1	16	16	16
description	0 or 1	SecParam	handle	handle

18

#### 4. RFID 보안 알고리즘동향

##### • Sec\_ReqRN 명령/응답메시지

Sec\_ReqRN Command (16+16+16+16 = 64 bits)

	Command	Challenge	RN	CRC-16
# of bits	16	16	16	16
description	0xE102	RN 16	handle	

Sec\_ReqRN reply (16+16+16 = 48 bits)

	Challenge	RN	CRC-16
# of bits	16	16	16
description	RN 16	handle	

: Plain Data
  : Encrypted Data

19

#### 4. RFID 보안 알고리즘동향

##### • Req\_Auth 명령과 응답메시지

Req\_Auth Command (16+16+16 = 48 bits)

	Command	Handle	CRC-16
# of bits	16	16	16
description	0xE103	Encrypted newRN16	

Req\_Auth reply (16+16 = 32 bits)

	Auth_data	CRC-16
# of bits	16	16
description	Ch 16 @ newRN16	

: Plain Data
  : Encrypted Data

20