안전한 전자여권 사용을 위한 인증 기술 연구

전상엽*, 박정효*, 장승재*, 전문석*
*숭실대학교 일반대학원 컴퓨터학과
e-mail : {yeobi0070, helios914, hezc81, mjun}@ssu.ac.kr

The authentication technology Research for using secure e-passports

Sang-yeob Jun*, Jung-hyo Park*, Seung-jae Jang*, Moon-Seog Jun*
*Dept of Computer Science, Soongsil University

요 약

최근 전 세계적으로 전자여권을 도입하기 위한 연구가 미국을 중심으로 활발히 진행되고 있다. 또한 전자여권은 비접촉식 스마트카드 기능의 IC(Integrated Circuit) 칩에 사용자의 정보와 바이오정보 그리고 여러 보안 기능들을 포함함으로써 기존의 여권에서 발생하는 문제점들을 해결하고 있다.

그러나 기존의 RFID(Radio Frequency Identification) 기술에서 발생하는 데이터 위변조, 도청, 무단 복제 및 바이오정보 노출 등의 문제점들을 아직 내재하고 있다.

따라서 본 논문에서는 현재 필수로 적용되는 BAC 메커니즘을 조금 더 안정적이고 효율적으로 개선한 EBAC 메커니즘을 제안한다.

1. 서론

UN 산하 국제민간항공기구에서는 ISO/IEC JTC1 SC17 Doc 9303 국제 규격에 따라 기존의 사진 전사식 여권에 비접촉식 스마트카드 기능을 가지고 있는 IC 칩을 추가하여 바이오정보를 탑재한 전자여권 형태 및 기능, 구성 등에 대하여 발표하였다. 이에 국내에서도 미국의 비자면제 프로그램 참여를 위해 보안기능을 제공하는 전자여권을 발급하기 위한 연구가 진행되고 있다[1][2].

그러나 전자여권을 이용한 개인 식별 기술은 전자여권 칩과 판독시스템 사이의 물리적인 접촉 없이 인식이 가능하다는 장점과 함께 도청 공격, 데이터 위변조, 바이오정보 노출, 전자여권 복제 등의 개인 신원 정보 침해 문제를 발생 시킬 수 있다. 이러한 개인 신원 정보 침해 문제를 해결하기 위해서 ICAO 에서는 많은 연구가 진행되어 왔으며, 필수적으로 사용되는 BAC와 선택적으로 사용하는 PA, AA와 같은 전자여권 인증 메커니즘들이 있다. 또한 유럽연합을 중심으로 EAC 인증 메커니즘이 제안되고 있다.

본 논문에서는 기존의 전자여권과 검증기관 사이에 단방향 인증과 기존의 세션이 계속 유지되는 단점을 보완하기 위해 BAC 메커니즘을 보안한 EBAC를 제안한다.

2. 관련연구

1.1. 전자여권의 개념

전자여권이란 바이오정보를 내장한 IC 칩이 탑재된 기계판독식 여권을 말한다. 전자여권의 외형상 현행 사진전사식 여권과 큰 차이는 없으며, 다만 여권의 뒷표지 속에 IC 칩이 내장되게 된다. 이 칩에는 여권번호 및 인적사항 등 신원정보면에 기재되어 있는 정보와 바이오정보가 수록된다.

1.2. 전자여권의 구성

[그림1] 전자여권 구성

[그림1]은 전자여권의 구성을 보여주고 있으며, 전자여권의 구성은 그림에서와 같이 신원정보면, ICAO 로고, 비접촉식 IC 칩, MRZ로 구성된다[3].

2.1. 전자여권 보안 기술

2.1.1 수동적 인증

PA(Passive Authentication)는 전자여권 칩의 LDS에 포함되어 있는 정보가 수정되지 않았음을 알려주며, 이 메커니즘은 Document Security Object를 사용한다. 이것은 전자여권 발행 기관이 암호화 방식을 적용하여 여권 속의 칩에 대한 정보를 저장하고, 해쉬를 이용하여 전자적인 서명을 통해 칩 안의 정보를 암호화 한다.

Document Security Object 서명값의 해쉬를 인증하는 방식은 DOS와 LDS를 비교하여 정보가 일치하였을 경우 데이터가 변경되지 않았음을 증명함으로써 인증을 수행한다. 예를 들어 공격자가 칩 안에 임의의 데이터를 삽입하고 전자여권을 위조한 경우, 전자여권 내의 칩에 저장되어 있는 정보에 대한 서명값이 일치하지 않기 때문에 PA 기술에 의해 전자여권의 내용이 바뀌었음을 알아낼 수 있다. 그러나, PA 기술의 단점은 전자여권 내의 칩에 대한 복제를 막을 수 없다는 것이다[4].

2.1.2 능동적 인증

AA(Active Authentication)는 적법한 전자여권의 데이터를 수집하여 동일한 데이터와 기능을 가지는 칩을 복제하는 것을 방지하는 보안 메커니즘이다. AA 기술은 칩안에 내장된 키 쌍을 이용해 판독기와 전자여권 내의 칩과 질의-응답 방식의 인증 방법을 사용하여 칩이 복제되지 않았음을 알아내게 된다.
이 방법은 전자여권 내의 LDS 구조 중 DG15의 공개키정보를 이용하여 해쉬값 생성후 Document Security Object에 저장하고, 해쉬값에 발행 국가의 전자서명을 포함한다. 이 과정에서 비밀키는 전자여권에 내장된 칩의 안전한 메모리 영역에 보관되어 노출되지 않는다.

2.1.3 기본 접근 제어

BAC(Basic Access Control)는 전자여권 칩에 저장된 데이터들이 공격자들에게 불법적으로 읽히는 것을 방지하고, 전자여권 칩과 판독시스템 간에 전송되는 정보를 도청하지 못하도록 전자여권 칩과 판독시스템 간 안전한 통신 채널을 구성하기 위한 접근통제 메커니즘이라 할 수 있다.
판독시스템은 전자여권 신원정보면의 기계판독영역 정보에서 여권번호, 생년월일, 여권 만기일과 각각의 검증 숫자를 OCR 리더로부터 읽어 들인다. 이를 통해 판독기와 전자여권 칩 사이에서 안전한 메시지 교환을 위해 사용되는 세션키를 유도해 내고, 전자여권 칩과 판독기간 안전한 통신채널을 구성하게 된다[5].

2.1.4 확장 접근 제어

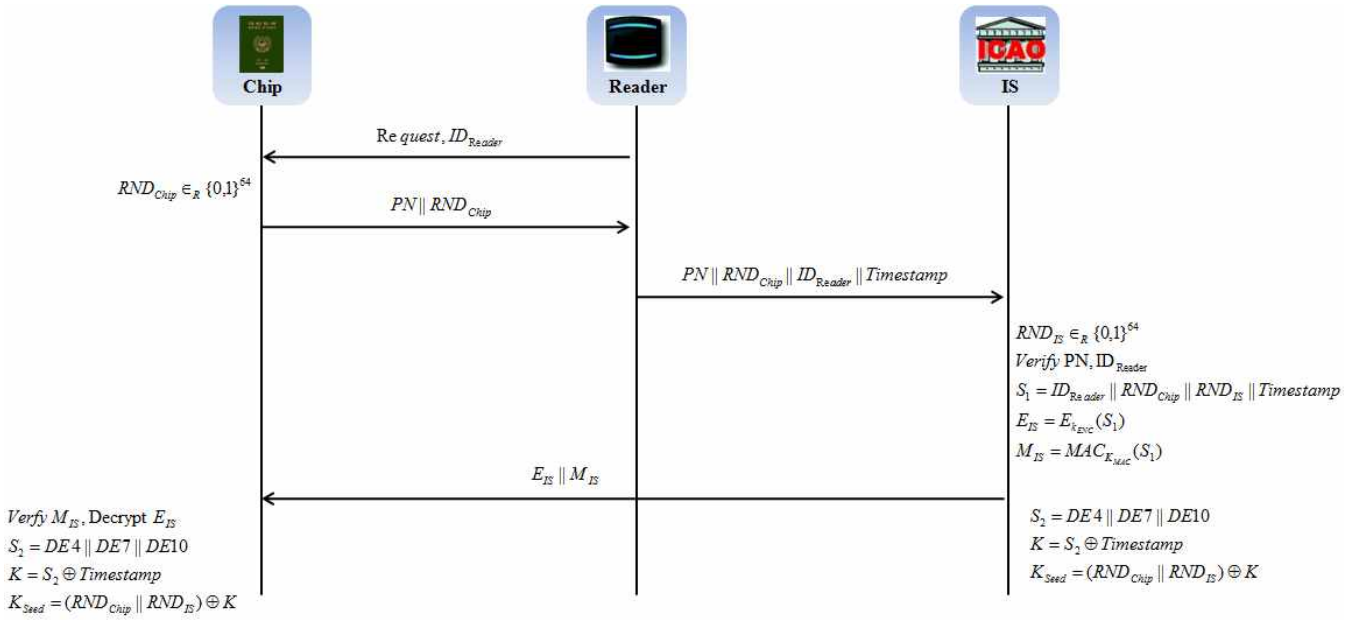
EAC(Extended Access Control)은 전자여권 칩에 저장된 바이오 정보를 권한이 없는 국가에게 정보를 열람할 수 없도록 방지하는 접근통제 메커니즘이다. BAC 보안 채널 생성 이후 Diffie-Hellman 알고리즘을 사용한 키 동의 방식을 통해 더욱 더 안전한 보안 채널을 생성한다. 그 후, 각 여권 발행국 CVCA가 발급한 인증서가 탑재된 판독기임이 판명된 경우에만 바이오 정보를 제공하도록 되어 있다. 즉 검증할 수 있는 키를 제공받은 국가들에게만 전자여권 칩 내에 저장되어 있는 바이오 정보들을 제공하게 된다[2][6].

3. EBAC 메커니즘

EBAC(Extended Basic Access Control) 메커니즘은 기존의 인증 메커니즘들의 보안 문제점인 단방향 인증과 세션 관리를 해결하기 위함이고, 또한 성능면에서의 개선을 중점으로 하였다.

3.1. 시스템 파라미터

- ID_{Reader} : 리더기의 고유 식별 ID
- RND_{Chip} : 칩에서 생성하는 임의 값
- RND_{IS} : 판독시스템에서 생성하는 임의 값
- PN : 여권 번호
- Timestamp : 키 생성을 위한 시간
- E_{IS} : 판독시스템에서 S_1을 K_{ENC}로 암호화한 값
- M_{IS} : Inspection System에서 S_1을 K_{MAC}을 계산한 값
- S_1 : 리더기의 ID, 칩과 판독시스템의 임의 값, Timestamp를 연접한 값
- S_2 : DG1 그룹의 여권번호, 생년월일, 여권만기일을 연접한 K_{Seed} 생성에 사용되는 값
- K : S_2와 Timestamp를 XOR 하여 생성한 값
- K_{Seed} : 칩과 판독시스템의 임의 값을 연접한 결과와 K를 XOR 하여 생성한 SEED 값



[그림 2] EBAC 인증 메커니즘

3.2. EBAC 인증 과정

(1) 리더기는 자신의 고유 식별 ID을 전송함과 동시에 임의 값을 요청
: Request, IDReader

(2) 칩은 8바이트의 임의 값을 생성
: $RND_{Chip} \in_R \{0,1\}^{64}$

(3) 여권번호와 칩의 임의 값을 연접하여 리더기에 전송
: $PN||RND_{Chip}$

(4) 리더는 칩에게서 받은 여권번호와 임의 값과 리더기 고유 식별 ID와 현재 시간을 연접하여 판독시스템에 전송
: $PN||RND_{Chip}||ID_{Reader}||Timestamp$

(5) 판독시스템은 8바이트의 임의 값을 생성
: $RND_{IS} \in_R \{0,1\}^{64}$

자신의 시스템에서 여권번호와 리더기의 고유 식별 ID를 확인
: Verify PN, ID_{Reader}

리더기의 고유 식별 ID와 칩과 판독시스템의 임의 값과 Timestamp를 연접하여 S_1을 생성
: $S_1 = ID_{Reader}||RNDChip||RND_{IS}||Timestamp$

BAC 인증용 암호키인 K_{ENC}를 이용하여 S_1을 암호화
: $E_{IS} = E_{KENC}(S_1)$

BAC 인증용 해쉬키인 K_{MAC}을 이용하여 해쉬 값을 생성
: $M_{IS} = MAC_{KMAC}(S_1)$

(6) 암호 값과 무결성 확인을 위해 해쉬 값을 연접하여 전송
: $E_{IS}||M_{IS}$

(7) 암호 값을 복호 후, 무결성 비교
: Verify M_{IS}, Decrypt E_{IS}

DG1의 4,7 그리고 10번째 값인 여권번호, 생년월일, 여권만기일을 연접
: S_2 = DE4||DE7||DE10

16바이트 키를 생성하기 위해 S_2와 Timestamp를 XOR 연산
: $K = S_2 \oplus Timestamp$

칩과 리더기의 임의 값을 연접한 결과에 K를 XOR 하여 K_{Seed} 생성
: $K_{Seed} = (RND_{Chip}||RND_{IS}) \oplus K$

(8) DG1의 4,7 그리고 10번째 값인 여권번호, 생년월일, 여권만기일을 연접
: S_2 = DE4||DE7||DE10

16바이트 키를 생성하기 위해 S_2와 Timestamp를 XOR 연산
: K = $S_2 \oplus$Timestamp

칩과 리더기의 임의 값을 연접한 결과에 K를 XOR 하여 K_{Seed} 생성
: K_{Seed} = $(RND_{Chip}||RND_{IS}) \oplus K$

4. 성능분석

ICAO에서 표준화한 인증 메커니즘은 PA, AA, BAC, EAC가 있으나 필수적용 사항은 BAC와 PA를 기본적으로 사용한 메커니즘이다. 하지만 BAC와 PA의 인증 메커니즘으로는 리더기 취소 문제와 단방향 인증만 가능하다는 문제점들이 존재한다. 이러한 문제점들은 보완하기 위해 BAC를 향상시킨 EBAC를 제안하였고 안전성과 성능에 대해 분석하였다.

4.1. 안전성 비교

BAC의 도청 공격, 리더기 취소 문제, 쌍방향인증 문제점들을 고려하여 EBAC를 제안하였다. EBAC에서 KSeed를 생성할 때 시간을 사용함으로써 도청 공격과 리더기 취소문제를 고려하였고, 칩에서의 인증과 판독시스템 사이의 인증을 각각 함으로써 기존의 단방향 인증을 쌍방향시스템으로 보완하였다.

[표 1] 안전성 비교 표

안전성 비교	BAC	EBAC
도청 공격	×	○
리더기 취소	×	○
중간자 공격	○	○
쌍방향 인증	×	○
재생 공격	○	○

4.2. 성능 비교

기존의 BAC에서는 칩과 판독시스템 사이에 암·복호화 과정이 2회씩 실행되고, MAC 생성·검증 또한 총 2회가 실행되며, 임의 값 생성은 총 4회가 실행된다. 그에 비해 제안하는 시스템인 EBAC에서는 암호화 과정 및 MAC 생성이 판독시스템에서만 1회씩 수행되고, 복호화 과정 및 MAC 검증 또한 칩에서만 1회 수행된다. 그리고 임의 값 생성은 칩과 판독시스템에서 1회씩만 생성됨으로 기존의 BAC에 비해 계산량을 감소시킬 수 있는 장점을 가진다.

[표 2] 성능 비교 표

성능 비교	전자여권 칩과 판독시스템 사이의 계산량				
	암호화	복호화	임의 값 생성	MAC 생성	MAC 검증
BAC	2	2	4	2	2
EBAC	1	1	2	1	1

5. 결론

현재의 전자여권 보안 기술에 대한 연구가 더욱 더 활발히 진행되고 있으며, 그에 따른 보안 취약점과 효율성 제고를 위한 분석을 통해 안전한 전자여권 시스템의 개발이 요구되고 있다.
기존 전자여권 시스템에서의 보안 취약점들을 해결하기 위해 ICAO에서 표준화한 인증 메커니즘들 중에 BAC를 중점으로 하여 전자여권 칩과 판독시스템 사이의 안전한 통신을 제공하였다. 하지만 도청 공격과 리더기 취소, 쌍방향 인증의 문제점을 고질적으로 갖고 있었다. 그리하여 본 논문에서는 향상된 EBAC를 사용하여 안전성을 높이고, 성능을 개선을 위한 방법을 제안하였다.

참고문헌

[1] 문지현, “전자여권 융합기술 및 국제표준”, IT Forum Korea, 1999.
[2] ISO, "ISO/IEC 7816 Identification Cards-Integrated Circuit(s) Cards with Contacts. Technical Report", ISO JTC1/SC 17
[3] ICAO, "Development of a Logical Data Structure-LDS for Optional Capacity Expansion Technologies", Revision 1.7, 2004
[4] Gaurav S., Kc and Paul A., Karger., "Security and privacy issues in machine readable travel documents (MRTDs)", IBM Technical Report (RC23575). IBM T. J., Watson Research Labs, April, 2005.
[5] ICAO, ‘PKI for Machine Readable Travel Documents offering ICC Read-Only Access', Version 1.1, 2004.
[6] NIST, "Recommendation for Key Management. Technical Report Special Publication 800-57 Draft", 2005