전자여권 사용을 위한 향상된 인증 기술

전상엽, 정용훈, 전문석
숭실대학교 일반대학원 컴퓨터학과
e-mail:{yeobi0070, s0178, mjun}@ssu.ac.kr

A Extended Authentication Scheme Using Electronic Passports

Sang-Yeob Jeon, Yong-Hoon Jung, Moon-Seog Jun
Dept of Computer Science, Soongsil University

요 약

최근 미국을 중심으로 전자여권을 도입하기 위한 연구가 활발히 진행되고 있다. 또한 전자여권은 비접촉식 스마트카드 기능의 IC칩에 사용자 정보, 바이오정보 및 여러 보안 기능을 포함함으로써 전자여권의 보안 문제들을 해결하고 있다. 그러나 기존의 RFID 기술에서 발생하는 데이터 위·변조, 무단 복제, 도청 등의 문제점들을 내재하고 있다.

따라서 본 논문에서는 전자여권을 확인 시 전자여권에 포함된 사진의 변경 여부를 확인함으로써 보안의 강도를 강화하는 메커니즘을 제안한다.

1. 서론

전자여권은 기존의 여권정보에 비접촉식 스마트 기능의 IC(Integrated Circuit) 칩을 추가하여 바이오 정보를 탑재한 것이다. 전자여권은 새로운 형태의 출입국 관리 시스템으로 기존의 여권보다 보안 기능이 강화되고 자동화된 출입국 관리를 할 수 있는 장점으로 인해 전 세계적으로 도입하기 위한 연구가 진행되고 있다[1][2].

전자여권을 이용하여 개인 식별 기술은 전자여권 칩과 판독 시스템 사이의 물리적인 접촉 없이 인식이 가능한 장점과 함께 skimming, 데이터의 위·변조, 바이오정보 노출, 여권 복제 등의 개인 신원 정보 침해 문제를 야기할 수 있다. 이러한 문제를 해결하기 위해 ICAO에서는 많은 연구가 진행되어 왔으며, 표준 지침으로 정해지고 있는 PA, BAC, AA와 같은 전자여권 인증 메커니즘이 있다 또한 유럽연합을 중심으로 EAC 메커니즘을 사용하여 사용자의 프라이버시를 보호하고 있다.

그러나 RFID리더기가 암호 키를 제공하기 전에 잠겨있으나 암호 키는 MRZ의 값들의 조합으로 만들어진다. 이에 따라 MRZ조직규칙을 알아낸 후 무차별 공격 프로그램을 사용하여 암호 해독이 가능하다[3].

따라서 본 논문에서는 BAC 메커니즘에 전자여권의 사진정보의 변경여부를 확인함으로써 좀 더 높은 강도의 보안 메커니즘을 제안한다.

2. 관련연구

2.1. 전자여권의 개념

전자여권은 국제민간항공기구와 국제표준화 기구에서 규정하는 국제 표준에 따라 바이오 정보를 내장한 IC칩이 탑재된 기계 판독식 여권을 말한다. 이 칩에는 여권 번호 및 인적 사항 등이 신원 정보면에 기재되어 있는 정보와 바이오 정보가 수록된다.

2.2. 전자여권의 구성

2.2.1 신원정보면

신원정보면(Data page)은 여권번호, 여권사진, 발행국가, 생년월일, 성별, 여권 만기일 등 여권 소지자의 개인 정보를 나타내고 있다.

2.2.2 ICAO 로고

ICAO에서 제정한 국제 로고로서, 여권에 비접촉식 스마트 기능의 IC칩이 내장되어 있음을 의미하며,

전자여권을 발급한 나라의 여권 앞 페이지 하단에 로고를 표시하도록 권고한다[4].

2.2.3 기계판독영역(MRZ)

ICAO에서 표준으로 권고하고 있는 전자여권의 하단에 위치하여 기계가 판독할 수 있도록 인쇄된 영역이다. 기계판독영역은 OCR-B 문자를 사용하여 여권 소지자의 정보를 쉽게 인식할 수 있다. 또한 기계판독영역은 전자여권에 내장되어 있는 IC칩과 판독기 사이의 안전한 메시지 교환을 위해 사요되는 암호 블록 암호 알고리즘 키 쌍인 BAC 세셔키를 생성하는데 사용된다.

2.2.4 비접촉식 IC 칩

비접촉식 스마트 기능의 IC칩은 바이오 정보와 여권 소지자의 개인 정보, 그리고 전자여권의 보안을 위해 사용되는 키들이 탑재되어있다. 또한 비접촉식 IC칩 내의 무결성을 보장하는 개인 신상정보에 대한 해쉬 연산 결과 값을 표준화된 LDS(Logical Data Structure)에 맞게 각각의 DG(Data Group)에 개인 신상정보를 기록한다.

2.3. 전자여권의 보안 기술

2.3.1 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 서명 값의 해쉬를 인증하는 방식은 DOS와 LDS를 비교하여 정보가 일치하였을 경우 데이터가 변경되지 않았음을 증명함으로써 인증을 수행한다[5].

2.3.2 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

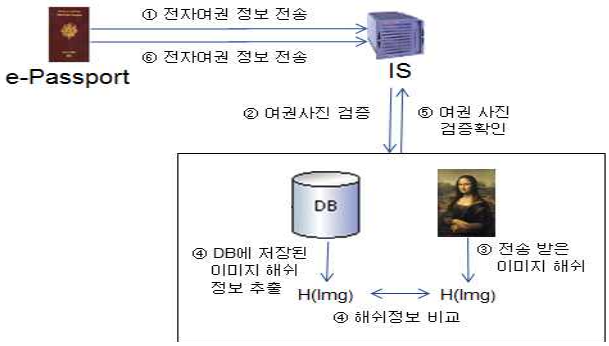
BAC(Basic Access Control)는 전자여권 칩에 저장된 데이터들이 공격자들에게 불법적으로 읽히는 것을 방지하고, 전자여권 칩과 판독시스템 간에 전송되는 정보를 도청하지 못하도록 전자여권 칩과 판독시스템 간 안전한 통신 채널을 구성하기 위한 접근통제 메커니즘이라 할 수 있다.

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[6].

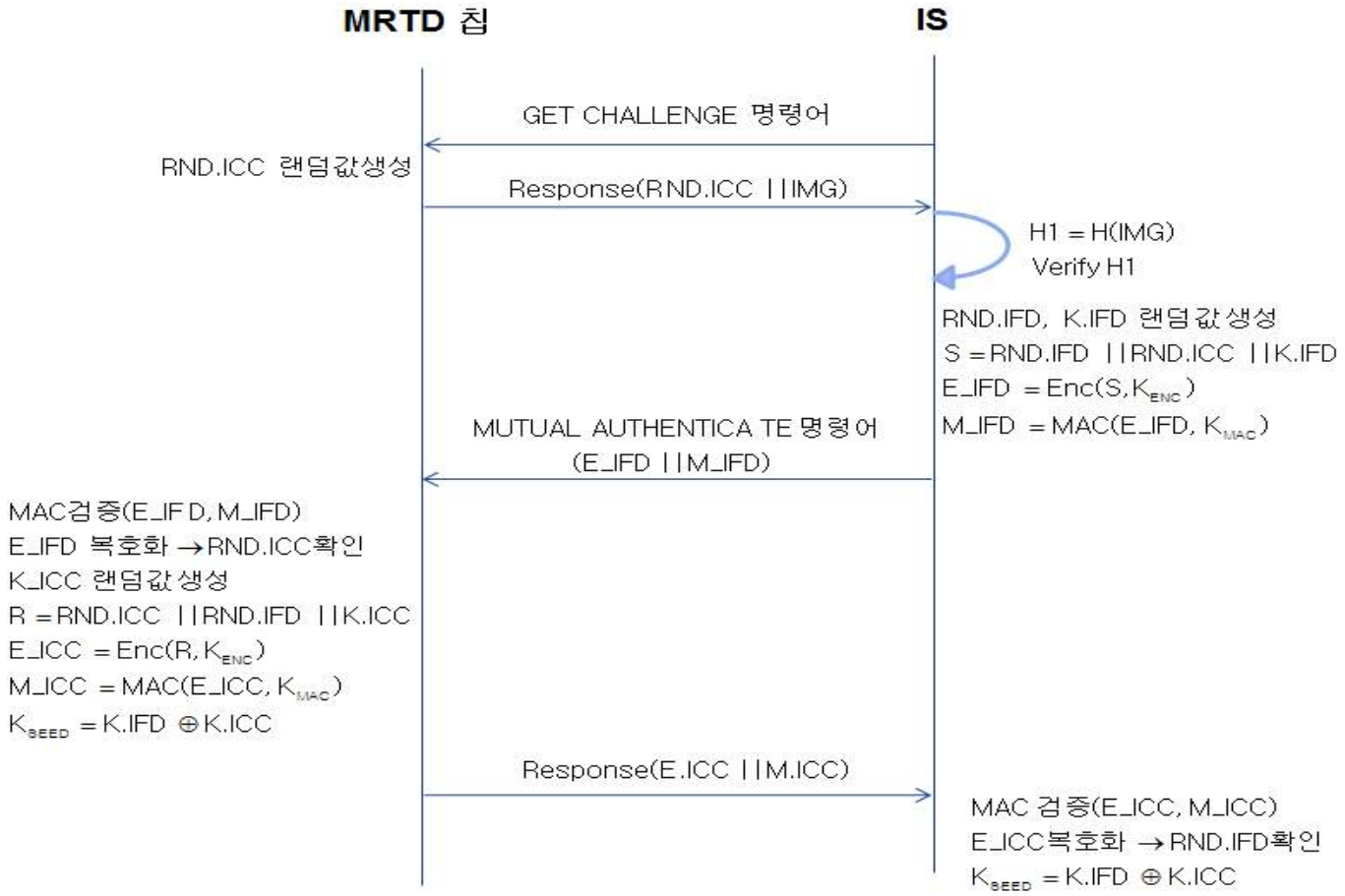
2.1.4 확장 접근 제어

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][7].

3. 제안하는 메커니즘



[그림 1] 전자여권의 사진정보 확인



[그림 2] 제안하는 인증 메커니즘

3.1 인증 과정

(1) 판독시스템에서 GET CHANLLENGE 명령어로 MRTD칩에 임의 값(RND.ICC)을 요청

(2) MRTD칩에서 8bit의 임의 값을 생성 후 여권의 사진 정보를 판독시스템에 전송

(3) 판독시스템에서의 수행 동작

ⓐ 전송받은 사진(IMG)를 해쉬하여 판독시스템에 저장되어 있는 사진의 해쉬정보와 비교하여 무결성을 확인

ⓑ 8bit 임의 값(RND.IFD)과 키를 만들기 위한 16bit 임의 값(K.IFD)을 생성

ⓒ RND.ICC, RND.IFD, K.IFD를 연접하여 S 값을 생성

ⓓ 사전에 공유된 K_ENC를 이용하여 S값을 암호화하여 E_IFD를 생성

ⓔ E_IFD를 해쉬하여 M_IFD를 생성

ⓕ E_IFD와 M_IFD를 연접하여 MRTD칩으로 전송

(4) MRTD칩에서의 수행 동작

ⓐ E_IFD의 해쉬 값인 M_IFD를 검증하여 무결성 확인

ⓑ E_IFD를 복호화 하여 RND.ICC를 추출

ⓒ 키를 만들기 위한 16의 임의 값(K.ICC)을 생성

ⓓ RND.ICC, RND.IFD, K.ICC를 연접하여 R 값을 생성

ⓔ 사전에 공유된 K_ENC를 이용하여 R값을 암호화하여 E_ICC를 생성

ⓔ E_ICC를 해쉬하여 M_ICC를 생성

ⓕ K.IFD와 K.ICC를 ⊕연산을 통해 K_{SEED}를 생성

ⓖ E.ICC와 M.ICC를 연접하여 판독시스템으로 전송

(5) 판독시스템에서의 수행 동작

ⓐ E_ICC의 해쉬 값인 M_ICC를 검증하여 무결성 확인

ⓑ E_ICC를 복호화 하여 RND.IFD를 추출

ⓒ K.IFD와 K.ICC를 ⊕연산을 통해 MRTD 칩과 판독 시스템 사이의 공유된 K_{SEED}를 생성

4. 안정성 비교

ICAO에서 표준화한 인증 메커니즘은 PA, BAC, AA, EAC가 있으나 현재 BAC와 PA 인증 메커니즘이 필수적으로 적용되고 있다. 따라서 본 절에서는 BAC 메커니즘의 안전성을 제안 메커니즘과 비교 분석 한다. BAC 인증 메커니즘의 안전성을 분석하기 위해서 도청 공격, 재생 공격, 중간자 공격, 데이터 위·변조 공격, 에 대해 안전성을 비교 한다.

4.1 안정성 비교

BAC 메커니즘과 제안하는 메커니즘을 아래의 [표 2]와 같이 비교한다. 우선 도청공격과 중간자 공격에 대해서는 각각 안전하였으나 데이터 위·변조 공격에서는 BAC 메커니즘에서는 취약한 반면 제안 메커니즘에서는 사진정보를 이용하여 전자여권의 무결성을 확인함으로써 데이터 위·변조 공격에 안전하다는 장점을 가진다.

[표 1] 안전성 평가

분류	BAC	제안 메커니즘
도청 공격	○	○
재생 공격	○	○
중간자 공격	○	○
데이터 위·변조 공격	×	○

4. 결론

현재 전자여권 취약점 및 효율성 제고를 위해 전자여권 보안 기술 연구가 활발히 진행 되고 있으며 더욱 안전한 전자여권 시스템의 개발이 요구되어 지고 있다.

기존의 전자여권에서의 취약점들을 해결하기 위해 ICAO에서 표준화한 인증 메커니즘 중 BAC 메커니즘은 전자여권 칩과 판독 시스템 사이의 안전한 통신을 제공하였다. 그러나 리더기 취소 공격 및 데이터 위·변조 공격에 대해 문제점을 갖고 있다. 그리하여 본 논문에서는 좀 더 안전성을 높이는 방법을 제안하였고, 앞으로 전자여권 보안 이슈에 대해 더 많은 연구가 진행되어야 할 것이다.

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] http://www.computerworld.com/s/article/9012406/Crack_Security_expert_hacks_RFID_in_UK_passport?source=rss_news50

[4] ICAO, "Use of Contactless Integrated Circuits In Machine Readable Travel Documents,", Version 4.0, 5 May 2004

[5] ICAO, "Development of a Logical Data Structure-LDS for Optional Capacity Expansion Technologies", Revision 1.7, 2004

[6] ICAO, ‘PKI for Machine Readable Travel Documents offering ICC Read-Only Access', Version 1.1, 2004.

[7] NIST, "Recommendation for Key Management. Technical Report Special Publication 800-57 Draft", 2005