한국컴퓨터정보학회 하계학술대회 논문집 제20권 제2호 (2012. 7)

한국 전자여권의 접근제어 메커니즘에 대한 보안성 분석 및 개선†

권근°, 정재욱*, 원동호*††
°*성균관대학교 정보보호연구소
e-mail:{kkwon, jwjung, dhwon}@security.re.kr

Security Analysis and Improvement of Access Control Mechanism in Korean e-Passport

Keun Kwon°, Jaewook Jung*, Dongho Won*††
°*Information Security Group, Sungkyunkwan University

● 요 약 ●

전자여권에 적용된 보안기술인 BAC(Basic Access Control)는 IC칩에 저장된 여권 소지자의 신상정보를 여권을 제출한 상태에서만 확인할 수 있도록 하는 접근제어 기술이다. 하지만 BAC에 사용되는 비밀키의 생성을 위해 여권 소지자의 신상정보가 사용되기 때문에 비밀키에 대한 전수조사 공격에 취약할 수 있다. 이에 본 논문에서는 한국 전자여권의 BAC 과정에서 생성되는 비밀키의 취약성을 분석하고, 전수조사 공격에 대한 보안성을 강화하기 위한 방법을 제안한다.

키워드: 전자여권(E-Passport), MRTD(Machine Readable Travel Document), BAC(Basic Access Control), DES(Data Encryption Standard), SHA-1

I. 서론

전자여권은 기존의 사진전사식 여권에 여권 소지자의 신상정보와 바이오정보를 저장하고 있는 비접촉식 IC칩을 내장하여 위조 및 복제 방지를 강화하고 출입국 관리의 자동화를 실현하기 위해 제안된 여권이다. 현재 전자여권은 미국을 중심으로 도입이 시작되어 전 세계적으로 발급되고 있으며 우리나라는 2008년 8월부터 전자여권 시스템을 도입하여 발급하고 있다.

전자여권의 도입과 함께 전자여권에 저장된 디지털 정보를 보호하기 위한 보안 기술 적용이 요구되었고, 이에 따라 국제 민간 항공기구(ICAO : International Civil Aviation Organization)는 Doc. 9303를 통해 PA(Passive Authentication), BAC(Basic Access Control), AA(Active Authentication)를 제안하였다. 그리고 독일 연방 정보 보안국(BSI : Bundesamt fur Sicherheit in der Informationstechnik)은 바이오정보의 보호를 위한 EAC(Extended Access Control)를 제안하였다[1][2]. 하지만 표준으로 제안된 보안 기술에 다양한 취약점이 존재한다는 것이 여러 연구를 통해 밝혀지고 있다.

특히 접근제어 기술인 BAC에 사용되는 비밀키의 취약성에 따른 전수조사 공격의 가능성이 지속적으로 제기되고 있으며 독일 정부는 이 문제를 해결하기 위해 전자여권번호의 구성 체계를 변경하기도 하였다[3][4][5]. 이러한 취약점은 각 국가의 전자여권 구현방식에 따라 달라질 수 있으므로 우리나라 전자여권의 취약성과 이에 따른 보안강도에 대한 연구가 필수적이라고 할 수 있다.

이에 본 논문에서는 한국 전자여권의 BAC 과정에서 사용되는 비밀키의 보안강도를 측정하고 더 나아가 전수조사 공격에 대한 보안성을 강화시키기 위한 방법을 제안한다.

II. 관련 연구

1. 배경이론

1.1 BAC(Basic Access Control)

BAC 메커니즘은 물리적으로 전자여권을 펼쳤을 때에만 IC칩에 저장된 여권 소지자의 신상정보에 대한 접근이 가능하도록 하는 접근제어 기술이다. BAC 메커니즘은 데이터 암호화를 위해 Triple-DES 대칭키 암호 알고리즘을 사용하며 메시지의 무결성 확인을 위해 ISO/IEC 9797-1 MAC Algorithm 3 을 사용한다. 그림1은 BAC 메커니즘 프로토콜을 나타낸다.

† "본 연구는 방송통신위원회의 방송통신융합미디어원천기술개발사업의 연구결과로 수행되었음" (KCA-2012-12-912-06-003)

†† 교신저자: 원동호(dhwon@security.re.kr)

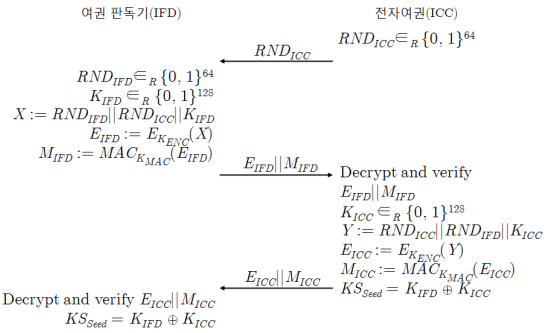

그림 1. BAC 메커니즘 프로토콜
Fig. 1. BAC Mechanism protocol

BAC 메커니즘이 수행되는 과정 중에 ISO 11770-2 키 설정 메커니즘이 사용되어 암호용 키와 MAC용 키를 생성하게 되는데 이때 전자여권의 MRZ(Machine Readable Zone)에 기록된 여권번호, 생년월일, 여권 유효기간 데이터가 사용된다. 즉 여권 내에 기록된 데이터를 기반으로 킷값을 설정하게 되며 따라서 MRZ 데이터의 구성 체계에 의해 암호용 키와 MAC용 키의 엔트로피가 결정된다. 그림 2는 ISO 11770-2의 키 설정 메커니즘을 나타낸다.

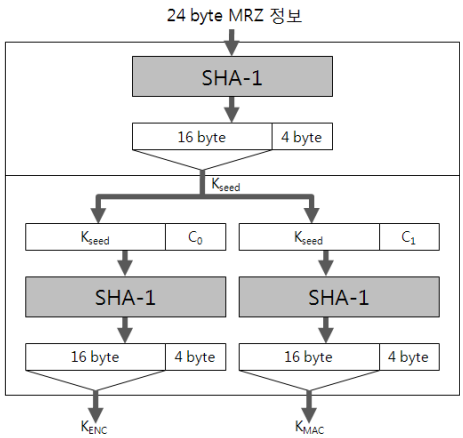

그림 2. ISO 11770-2 키 설정 메커니즘
Fig. 2. ISO 11770-2 Key Establishment mechanism

1.2 BAC 비밀키에 대한 전수조사 공격 방법

1.2.1 전방향 채널 공격

전자여권과 판독기 간의 무선 채널은 비대칭적으로 구성이 된다. 이 때 판독기에서 태그로의 통신채널을 전방향 채널(Forward Channel), 태그에서 판독기로의 통신채널을 후방향 채널(Backward Channel)이라고 하며, 두 채널을 합쳐서 양방향 채널(Two Channel)이라고 한다. 따라서 BAC 비밀키에 대한 전수조사 공격 방법은 전방향 채널 공격과 양방향 채널 공격으로 구분된다.

전방향 채널 공격자는 도청을 통해 $E_{IFD} \| M_{IFD}$ 값을 알아낼 수 있고, $M_{IFD} := MAC_{K_{MAC}}(E_{IFD})$ 이므로 MAC용 키인 K_{MAC}에 대한 전수조사 공격을 시도할 수 있다. 이 때 BAC 메커니즘에서는 ISO/IEC 9797-1 MAC Algorithm 3이 사용되며, 초기 체크 블록 Y_0의 값은 0으로 정해져 있으므로 K_{MAC}에 대한 전수조사 공격이 가능하다.

1.2.2 양방향 채널 공격

양방향 채널 공격에서 공격자는 전방향 채널과 후방향 채널을 모두 도청할 수 있으므로 BAC 메커니즘 프로토콜이 수행되는 동안 양방향 데이터를 모두 도청할 수 있다. 따라서 공격자는 RND_{ICC}, $E_{IFD} \| M_{IFD}$, $E_{ICC} \| M_{ICC}$ 값을 얻을 수 있고 이 값들 중 E_{ICC}의 MSB 8바이트 := $E_{K_{ENC}}(RND_{ICC})$ 이므로 암호용 키인 K_{ENC}에 대한 전수조사 공격을 시도할 수 있다. 이때 암호 알고리즘으로 CBC 모드의 Tripel-DES가 사용되며 IV(Initial Vector)값은 0으로 정해져 있으므로 K_{ENC}에 대한 전수조사 공격이 가능하다. 또한 양방향 채널 공격에서 공격자는 전방향 채널에 대한 도청이 가능하기 때문에 K_{MAC}에 대한 전수조사 공격 방법도 사용 가능하다.

III. 한국 전자여권의 BAC 비밀키 보안성 분석 및 개선

1. 한국 전자여권의 보안성 분석

1.1 한국 전자여권의 BAC 비밀키 엔트로피 측정

BAC 비밀키의 이론적 엔트로피는 MRZ 데이터의 구성 체계에 따라 달라지며 다양한 방법들을 사용하여 이론적 엔트로피의 크기를 줄이는 것이 가능하다. 따라서 한국 전자여권의 보안성을 분석하기 위해서는 여권에 적용된 MRZ 데이터의 구성 체계에 따른 실질적인 비밀키 엔트로피를 측정해야 한다.

표 1은 ICAO Doc.9303에 따른 BAC 비밀키 엔트로피의 이상적인 최대값을 나타내며 표 2, 표 3, 표4는 다양한 조건에서의 한국 전자여권 BAC 비밀키의 엔트로피 측정값을 나타낸다[6].

표 1. BAC 비밀키의 이론적 최대 엔트로피
Table 1. Entropy of BAC secret key

MRZ 데이터 항목	가정 사항	경우의 수	엔트로피
여권번호	9자리 영문자, 숫자의 조합	$(26+10)^9$	46.67bit
생년월일	100세 이하	365*100	15.21bit
여권 만료일	발급일로부터 10년	365*10	11.87bit
합계			**73.75bit**

표 2. 한국전자여권 BAC 비밀키의 이론적 최대 엔트로피
Table 2. Entropy of BAC secret key of Korean MRTD

MRZ 데이터 항목	가정 사항	경우의 수	엔트로피
여권번호	한 자리 영문자 + 여덟 자리 숫자	$2*(10)^8$	27.58bit
생년월일	100세 이하	365*100	15.12bit
여권 만료일	발급일로부터 10년	250*10	11.29bit
합계			**53.99bit**

표 3. 생년월일, 여권 만료일이 축소될 경우 키 엔트로피
Table 3. Reduced entropy of BAC key

MRZ 데이터 항목	가정 사항	경우의 수	엔트로피
여권번호	한 자리 영문자 + 여덟 자리 숫자	$2*(10)^8$	27.58bit
생년월일	10년 단위로 예측	365*10	11.83bit
여권 만료일	2년 범위로 가정	250*2	8.97bit
합계			**48.38bit**

표 4. 생년월일 획득, 여권 만료일이 축소될 경우 키 엔트로피
Table 4. Reduced entropy of BAC key

MRZ 데이터 항목	가정 사항	경우의 수	엔트로피
여권번호	한 자리 영문자 + 여덟 자리 숫자	$2*(10)^8$	27.58bit
생년월일	사전에 획득	0	0bit
여권 만료일	2년 범위로 가정	250*2	8.97bit
합계			**36.55bit**

표 4와 같이 한국 전자여권의 BAC 비밀키 엔트로피는 신상정보의 노출 정도에 따라 약 36bit 까지 축소될 수 있다. 따라서 공격자가 3GHz의 PC로 전수조사 공격을 수행할 경우, 약 6시간 내에 킷값을 알아낼 수 있다[7]. 또한 공격자가 전수조사 공격에 COPACOBANA와 같은 키 크랙 전용 머신을 사용할 경우에는 공격 성공 시간은 수분 이내로 줄어들 수 있다[8].

공격자가 킷값을 획득하면 도청공격 시 획득한 전자여권 전송 데이터에 대한 복호화가 가능하고 여권소지자에게 2차적으로 접근해 데이터를 획득할 수 있다. 따라서 여권번호 구성 체계나 BAC 프로토콜을 변경하여 비밀키의 엔트로피를 향상시켜 보안취약점을 개선시켜야 한다[2]. 이에 본 논문에서는 BAC 메커니즘의 MAC 과정 중 사용되는 초기 체크 블록 값과 암호화 과정 중 사용되는 IV(Initial Vector)의 값을 변경하여 전수조사 공격을 무력화 시킬 수 있는 방법을 제안한다.

2. 한국 전자여권의 보안성 개선

2.1 전방향 채널 공격에 대한 보안성 강화

BAC 메커니즘 프로토콜에서 여권 판독기가 MAC 알고리즘의 입력 값으로 사용하는 초기 체크 블록 Y_0은 0으로 설정 되어 있다. 이는 BAC 메커니즘이 시작되기 전에 전자여권과 판독기가 서로 공유하고 있는 난수가 없기 때문이며, 이 값이 0으로 설정이 되어 있기 때문에 공격자는 전수조사 공격을 통해 MAC용 비밀키를 찾아낼 수 있다. 이러한 전수조사 공격을 어렵게 만들기 위해서는 초기 체크 블록 Y_0 값을 전자여권과 판독기가 모두 알고 있는 난수 값으로 변경하여야 하는데 BAC 메커니즘 프로토콜의 첫 단계에서 전자여권이 생성한 난수 RND_{ICC}를 초기 체크 블록으로 사용하면 K_{MAC}에 대한 전수조사 공격을 어렵게 만들 수 있다. 8byte 길이의 RND_{ICC}가 암호학적으로 안전한 의사난수일 경우 264개의 경우의 수를 가지며 K_{MAC}의 전수조사 공격에 필요한 최대 공격횟수가 (후보키의 개수)*264 개로 증가하기 때문이다.

2.2 양방향 채널 공격에 대한 보안성 강화

BAC 메커니즘에서 데이터의 암호화에 사용되는 CBC모드의 Triple-DES 알고리즘은 IV값으로 0을 사용한다. 따라서 공격자는 K_{ENC}에 대한 전수조사 공격에 성공할 수 있다. 그러므로 IV값을 전자여권과 여권 판독기 모두 알고 있는 난수로 변경할 필요가 있는데 여권 판독기에서 생성한 RND_{IFD}가 적절한 대안이 될 수 있다. RND_{IFD}는 여권 판독기에서 전자여권으로 전송될 때 암호화되어 전송되기 때문에 공격자는 이 값을 알 수 없고 RND_{ICC}와 마찬가지로 264개의 경우의 수를 가지므로 K_{ENC}에 대한 전수조사 공격을 어렵게 만들 수 있다.

하지만 RND_{ICC}는 전자여권에서 여권 판독기로 전송되는 데이터이므로 양방향 채널 공격자에 의해 도청 될 수 있다. 따라서 앞서 제안한 방법대로 여권 판독기가 이 값을 MAC 과정의 초기 체크 블록으로 사용한다 하더라도 K_{MAC}에 대한 전수조사 공격을 어렵게 할 수 없는 한계점이 있다.

2.3 보안성 비교 분석

BAC 메커니즘의 MAC 과정 중 사용되는 초기 체크 블록 Y_0의 값과 암호화 과정 중 사용되는 IV의 값을 변경하면 비밀키의 전수조사 공격에 대한 안전성이 높아지는 것을 확인하였다. 이것을 기존의 방법과 비교하여 나타내면 표 5와 같다. 기존처럼 두 값을 모두 0으로 설정하여 BAC 메커니즘을 수행하면 전방향 채널 공격자는 K_{MAC}에 대한 전수조사 공격을 성공할 수 있고 양방향 채널 공격자는 K_{MAC} ,K_{ENC}에 대한 전수조사 공격을 성공할 수 있다. 하지만 초기 체크 블록Y_0 과 IV 대신에 각각 RND_{ICC} ,RND_{IFD}를 사용하면 양방향 채널 공격자는 K_{MAC}에 대한 전수조사 공격만 성공할 수 있고 특히 공격 가능성이 더 높은 전방향 채널 공격자는 그 어떤 키에 대한 전수조사 공격도 성공하기 어려워진다.

표 5. 보안성 비교 분성
Table 5. Security analysis

공격 형태	양방향 채널 공격		전방향 채널 공격	
공격 키 / Y_0, IV 값	K_{MAC}	K_{ENC}	K_{MAC}	K_{ENC}
Y_0 = 0 IV = 0	O	O	O	X
Y_0 = RND_{ICC} IV = RND_{IFD}	O	X	X	X
비고	신상정보 획득 가능		킷값만 획득 가능	

※ O : 전수조사 공격 가능 / X : 전수조사 공격 불가능

Ⅳ. 결론

본 논문에서는 전자여권 시스템에서 발생할 수 있는 보안 취약점을 해결하기 위하여 전자여권에 적용된 보안기술 중 하나인

BAC 메커니즘의 안전성을 분석하고 한국 전자여권의 BAC 메커니즘에 사용되는 비밀키의 엔트로피를 측정하였다. 그리고 낮은 엔트로피로 인한 취약점 때문에 발생할 수 있는 도청 공격과 전수조사 공격의 가능성을 RFID 시스템의 특성에 맞추어 분석하였다. 또한 분석한 결과를 바탕으로 비밀키 전수조사 공격에 대한 보안성을 강화시킬 수 있는 방법을 제안하였다. 하지만 전자여권 보안을 위해 반드시 도입되어야 할 비인가 판독기의 접근 제어에 대한 고려가 부족하였다. 앞으로 부족한 부분에 대한 연구를 추가적으로 실시하여 여권 소지자의 신상정보가 담긴 전자여권의 보안성을 더욱 강화시켜야 할 것이다.

참고문헌

[1] ICAO, Machine Readable Travel Documents, Doc 9303, Part 3 vol2 Third Edition 2008.

[2] BSI, Advanced Security Mechanisms for Machine Readable Travel Documents–Extended Access Control v2.05 2010.

[3] Juels, A., Molnar, D., Wagner, D. “Security and Privacy Issues in E-passports.”, Cryptology ePrint Archive, Report 2005/095 2005.

[4] B. Jacobs, J. Hoepman, E. Hubbers., “Crossing borders: Security and privacy issues of the european e-passport”, IWSEC 2006

[5] Ivo Pooters, “Keep Out of My Passport: Access Control Mechanism in E-passport”

[6] Keun Kwon et al., “Security Analysis of Access Control Mechanism in Korean e-Passport”, KSCI 2005

[7] Robroch, H., “ePassport Privacy Attack”, Presentation at Cards Asia Singapore 2006

[8] Yifei Liu et al., “E-Passport: Cracking Basic Access Control Keys. In”, OTM Confederated International Conferences CoopIS, DOA, ODBASE, GADA, and IS 2007, Vilamoura, Portugal, November 25-30, 2007

[9] KISA, ePassprot Protection Profile V2.1, 2010