한국 전자여권의 접근제어 메커니즘에 대한 보안성 분석[1)]

권근°, 이광우*, 정재욱*, 원동호*[2)]
°*성균관대학교 정보보호연구소
e-mail : {kkwon, kwlee, jwjung, dhwon}@security.re.kr

Security Analysis of Access Control Mechanism in Korean e-Passport

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

● 요 약 ●

전자여권에 적용된 보안기술 중 BAC(Basic Access Control)는 전자여권의 IC칩에 내장된 여권 소지자의 신상정보를 여권을 제출한 상태에서만 확인할 수 있도록 하는 접근제어 메커니즘이다. 하지만 BAC에 사용되는 비밀키의 생성을 위해 전자여권 내의 MRZ 정보를 구성하고 있는 여권 소지자의 신상정보가 사용되기 때문에 비밀키에 대한 전수조사 공격에 취약할 수 있다. 이에 본 논문에서는 한국 전자여권의 BAC 과정에서 사용되는 비밀키의 보안성을 분석한다.

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

I. 서 론

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 본격적으로 전자여권 시스템을 도입하였다.

전자여권의 도입과 함께 전자여권에 저장된 여권 소지자의 신상정보와 바이오정보의 보호를 위한 다양한 보안 기술들의 필요성이 대두되었고, 이에 따라 국제 민간 항공기구(ICAO : International Civil Aviation Organization)에서는 전자여권의 보안기술에 대한 국제표준을 마련하였다. ICAO의 국제표준 문서인 Doc. 9303에 제안되어 있는 전자여권의 보안기술에는 전자여권 인증 메커니즘인 PA(Passive Authentication), BAC(Basic Access Control), AA(Active Authentication)가 있으며, 독일 연방 정보 보안국(BSI : Bundesamt fur Sicherheit in der Informationstechnik)은 바이오정보의 보호를 위한 EAC(Extended Access Control)를 제안하였다[1][2].

전자여권을 발급한 각국 정부들은 위와 같은 보안기술들을 근거로 하여 전자여권의 보안강도가 충분하다고 판단하였으나 최근의 연구결과를 통해 다양한 취약점들이 밝혀지고 있는 것이 사실이다. 특히 BAC 메커니즘에 사용되는 비밀키의 낮은 엔트로피에 따른 전수조사 공격의 가능성이 지속적으로 제기되고 있으며 독일 정부는 이 문제를 해결하기 위해 전자여권번호의 구성 체계를 변경하기도 하였다[3][4][5]. 이러한 취약점들은 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 엔트로피를 측정하여 보안강도를 분석한다.

II. 관련 연구

1. 배경이론

1.1 BAC(Basic Access Control)

전자여권은 비접촉식 IC칩을 내장하여 여권 판독기와 무선으로 데이터를 주고받기 때문에 도청공격과 스키밍 공격에 취약할 수 있다. 따라서 전자여권을 제출한 상태에서만 여권 내의 IC칩에 저장된 여권 소지자의 신상정보에 대한 접근이 가능하도록 해야 하는데 이러한 접근을 제어하는 보안기술이 BAC(Basic Access Control) 메커니즘이다. 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.

1) "본 연구는 지식경제부 및 정보통신산업진흥원의 "대학 IT연구센터 육성·지원사업"의 연구결과로 수행되었음" (NIPA-2012-C1090-1001-0004)

2) 교신저자 : 원동호(dhwon@security.re.kr

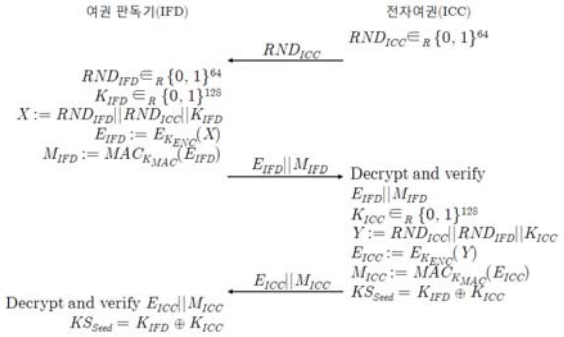

그림 1. BAC 메커니즘 프로토콜
Fig. 1. BAC Mechanism protocol

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

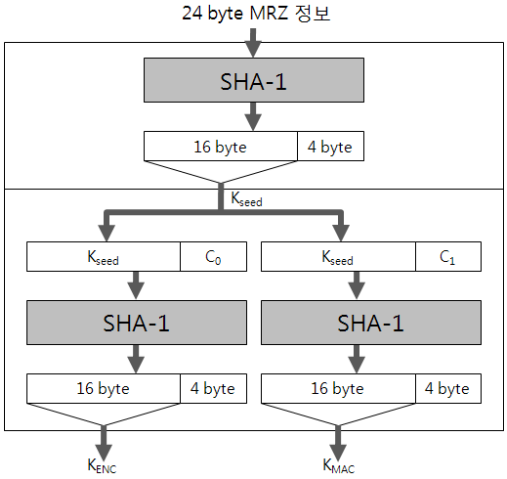

그림 2. ISO 11770-2 키 설정 메커니즘
Fig. 2. ISO 11770-2 Key Establishment mechanism

1.2 RFID 통신 채널 공격법

전자여권 시스템은 무선으로 데이터를 주고받기 때문에 도청공격에 취약하다. 특히 IC칩이 내장된 RFID 태그는 판독기의 요청에 수동적으로 반응하므로 별도의 정보보안 기능이 갖추어져 있지 않다면 내부에 저장된 데이터가 쉽게 유출 될 수 있다.

전자여권에 사용되는 RFID 태그는 내부전원을 사용하지 않는 수동형 태그이다. 따라서 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.

공격자는 RFID 시스템에 대한 도청공격 시 전방향 채널 공격과 양방향 채널 공격을 시도할 수 있으며 특히 신호의 강도가 높은 전방향 채널에 대한 공격 가능성이 더 높다. 따라서 안전한 RFID 시스템을 구성하기 위해서는 전방향 채널 공격을 어렵게 만드는 보안기술의 도입이 반드시 필요하다.

1.3 BAC 비밀키에 대한 전수조사 공격 방법

BAC 비밀키에 대한 전수조사 공격은 전자여권과 여권 판독기에 대한 도청공격을 통해 얻어낸 데이터를 사용하여 수행된다. 이 때 공격자가 도청에 사용하는 안테나의 성능에 따라 전자여권과 여권 판독기 간에 구성되는 양방향 채널이 모두 도청 가능한지, 아니면 전방향 채널만 도청 가능한지가 결정되며 전수조사 공격방법 또한 어떤 채널을 도청했느냐에 따라 달라질 수 있다.

1.3.1 전방향 채널 공격

공격자는 전방향 채널을 통해 $E_{IFD} \| M_{IFD}$ 값을 도청할 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 체크블록 Y_0의 값은 0으로 정해져 있으므로 K_{MAC}에 대한 전수조사 공격이 가능하다.

1.3.2 양방향 채널 공격

양방향 채널 공격에서 공격자는 전방향 채널과 후방향 채널을 모두 도청할 수 있으므로 BAC 메커니즘 프로토콜이 수행되는 동안 여권 판독기가 전자여권에 보내는 데이터와 전자여권이 여권 판독기에 보내는 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.

2. 연구 동향

2.1 국외 연구 동향

1.1절에서 살펴보았듯이 BAC 메커니즘은 암호용 키와 MAC용 키를 설정하는 과정에서 MRZ 데이터를 입력 데이터로 사용하기 때문에 MRZ 데이터의 구성 체계에 따라 BAC 메커니즘의 보안 강도가 결정된다. 이에 따라 ICAO Doc. 9303 표준문서에서는 BAC 과정에서 사용되는 비밀키의 이론적 최소 엔트로피를 Triple-DES 암호 알고리즘의 키 길이와 동일한 56bit 이상으로 권고하고 있다[1]. 하지만 다양한 방법을 통해 이론적 엔트로피를 낮추는 것이 가능하기 때문에 BSI에서는 비밀키에 대한 이론적

엔트로피가 73bit 이상이 되도록 권고하고 있다[2][6].

위와 같은 BAC 비밀키 엔트로피의 취약점은 A. Juels 등에 의해 제기되었으며, H. Robroch 는 비밀키의 이론적 엔트로피를 낮추어 일반적인 PC시스템을 사용한 BAC 비밀키 전수조사 공격이 효율적인 시간 내에 가능함을 보였다[3][7]. 또한 Y. Liu 등은 키 크랙 전용 머신인 COPACOBANA를 사용하여 수 분 이내에 BAC 비밀키에 대한 전수조사 공격에 성공할 수 있음을 보였다[6].

이와 같이 BAC 비밀키에 대한 공격이 성공하게 되면 전자여권과 여권 판독기에 전송되는 암호화된 데이터를 도청하여 복호화하는 것이 가능해지기 때문에 여권 소지자의 신상정보가 유출될 수 있다. 따라서 BAC 비밀키의 이론적 엔트로피를 높이거나 전수조사 공격을 어렵게 하는 방법이 필요하다.

III. 한국 전자여권의 접근제어 메커니즘에 대한 보안성 분석

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.

전자여권의 MRZ 데이터는 여권번호, 생년월일, 여권 만료일로 구성되는데 이 때 여권번호는 9자리 영문자, 숫자의 조합으로 이루어져있고 여권 소지자의 나이는 100세 이하, 여권 만료일은 여권 발급일로부터 10년 후라고 가정하여 BAC 비밀키의 이론적 최대 엔트로피를 구하면 표 1과 같다. 하지만 한국 전자여권은 여권번호가 한 자리의 영문자와 여덟 자리의 숫자로 이루어져 있기 때문에 비밀키의 이론적 최대 엔트로피가 줄어들게 된다. 이 때 첫 영문자는 복수여권일 경우 M, 단수여권일 경우 S로 표기되므로, 결국 2*(10)8 개의 경우의 수를 가지게 된다. 또한 한국에서는 공휴일에 여권이 발급되지 않으므로 가능한 여권 만료일의 날짜는 250개로 한정된다. 표 2는 이러한 가정 사항을 반영한 한국 전자여권 BAC 비밀키의 이론적 최대 엔트로피를 나타낸다.

BAC 비밀키의 엔트로피는 여권 소지자의 생년월일과 여권만료일의 범위를 축소함으로써 더 줄어들 수 있고, 표 3과 같이 나타낼 수 있다. 또한 사회 공학적 기법 등을 사용하여 여권 소지자의 생년월일을 알아냈을 경우 키 엔트로피는 더 줄어들 수 있으며 표 4와 같이 계산될 수 있다.

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

1.2 한국 전자여권의 BAC 비밀키 보안강도 분석

앞서 살펴본 바와 같이 한국 전자여권의 BAC 비밀키 엔트로피는 최대 약 36bit 까지 줄어들 수 있다. 따라서 도청을 통한 비밀키 전수조사 공격을 할 경우 공격자는 유의미한 시간 내에 키값을 얻어낼 수 있다.[6] 일단 키값이 획득되면 도청공격 시 획득한 전자여권 전송 데이터에 대한 복호화가 가능하고 여권소지자에게 2차적으로 접근해 비인가 리더기를 사용하여 데이터를 획득할 수 있다. 따라서 여권번호 구성 체계를 변경하여 엔트로피를 향상시키거나 BSI에서 제안한 PACE(Password Authenticated Connection Establishment)를 도입하여 비밀키의 보안취약점을 개선시켜야 한다.[2]

IV. 결 론

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 전수

조사 공격의 가능성을 RFID 시스템의 특성에 맞추어 분석하였다.

본 논무에서 분석한 내용을 기반으로 기존에 보급된 전자여권 시스템에 대한 변경 없이 BAC 비밀키의 엔트로피를 향상시킬 수 있는 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] 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

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

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