AVISPA를 이용한 On-Line Secure E-passport Protocol의 명세 및 검증

김현수*, 최진영*
*고려대학교 컴퓨터학과
e-mail:hyunsu@formal.korea..ac.kr

The Specification and Verification of On-Line Secure E-passport Protocols Using AVISPA

Hyun-Su Kim*, Jin-Young Choi*
*Dept. of Computer science, Korea University

요 약

현재 전자여권은 미국을 중심으로 도입이 시작, 전 세계 36개국에서 발행되고 있으며 우리나라도 2008년 시작으로 비자 면제국 가입을 위한 기본 조건으로 전자여권 전환 작업이 진행되고 있다. 전자여권의 도입과 함께 지문 정보 저장에 대한 프라이버시 문제 및 전자여권 내 정보 보호의 문제 등이 대두 되고 있다. 전자여권에서 사용 되고 있는 프로토콜 중의 하나인 OSEP의 취약점 및 문제점을 사전에 알아내 개인 정보 유출을 미연에 방지할 수 있도록 정형 명세 및 검증 도구인 AVISPA를 사용하여 접근해 보았다. 본 논문에서는 AVISPA를 이용한 명세 및 검증을 통해 OSEP(On-Line Secure E-passport Protocol)의 취약점을 효과적으로 발견할 수 있는 방법을 제안한다.

1. 서론

전자여권은 국제민간항공기구(ICAO)와 국제표준화기구(ISO)에서 규정하는 국제 표준에 따라 여권 신청인의 신원정보 및 기타 정보가 저장된 비접촉식 칩(Contactless IC Chip)을 내장한 여권이다. 전자여권에 사용하는 비접촉식 IC칩을 전자여권 IC칩(MRTD Chip)이라 한다. 전자여권 IC팁에는 전자여권 신원정보의 전자적 저장, 가공 처리를 위한 IT 기술 및 정보보호기술을 지원하는 IC 칩 운영체제(COS)와 전자여권 응용프로그램(MRTD Chip Application)이 탑재된다. 전자여권이 비접촉식 통신을 통하여 데이터를 전송하는 만큼, 허가받지 않은 자의 Chip 내 데이터 접근이 가능할 수 있으며, 이를 제한하기 위해여 전자여권의 표준에서는 BAC (Basic Access Control), EAC (Extended Access Control)와 같은 방식의 접근 제한 방식을 두고 있다. BAC 방식은 전자여권 내부에 물리적으로 표시된 88자리의 MRZ 정보를 알고 있는 사람만 Chip내부 정보에 접근 할 수 있도록 하는 것으로, 여권을 소지자로부터 물리적으로 건내받지 않은 상태에서는 정보를 읽지 못하도록 하는 것이다. 또한 MRZ정보로 상대를 확인한 후에는 여권과 판독기 간에 DES알고리즘을 사용한 암호화된 채널을 생성하여 판독내용을 도청할 수 없도록 한다.

EAC 방식은 전자여권 내 삽입된 개인의 지문, 홍채 등의 바이오 정보에 접근하기 위해서 추가적인 접근 통제를 하는 것으로, 국가마다 방식을 지정하도록 되어 있다. 유럽과 우리나라의 경우에는 BAC 보안채널 생성 이후 Diffle Hellman을 사용한 Key Agreement를 통하여 보다 한 단계 더 강력한 보안채널을 생성한 후, 각 여권 발행국 CVCA(Country Verifying CA)가 발급한 인증서가 주입된 판독기(타국가의 출입국 사무소를 포함한)임이 판명된 경우에만 지문 정보를 제공하도록 되어 있다. 허나, BAC, EAC가 모두 필수 사항이 아닌 선택 사항이므로, 각 국가에서 판단하여 사용할 수 있으며, 미국의 경우 BAC 방식이 아닌 차폐막을 사용하여 허가 되지 않은 여권 정보의 접근을 막고 있다.

정형 기법은 설계된 시스템이나 프로그램이 개발자의 요구사항에 맞게 설계된 것인지를 수학적 이론이나 명세 및 검증 도구를 이용하여 검증하는 방법을 말하며, 크게 시스템이나 프로그램의 동작이나 특성들을 정형적으로 표현하는 정형 명세와 명세 된 시스템이 요구사항을 잘 만족하는지 검증하는 방법인 정형 검증으로 나눌 수 있다. 보안 프로토콜의 정형 검증 방법은 수학적 논리를 바탕으로 한 정리 증명과 정형 검증 툴인 FDR, SPIN, AVISPA(Automated Validation of Internet Security Protocols and Applications)[1]를 이용한 모델 체킹 방법이 있는데, 본 논문에서는 인터넷 상의 보안 프로토콜 검증에 적합한 AVISPA를 이용하여 OSEP[2] 프로토콜을 명세 및 분석 하고, 검증 결과를 통해 프로토콜의 안전성을 확인하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 OSEP에 대해서 설명하고 3장에서는 프로토콜을 명세하고 검증하기 위한 AVISPA 및 HLPSL[3]에 대해 소개하며, 4장에서는 HLPSL와 AVISPA를 이용하여 보안 프로토콜의 분석 및 결과에 대해 살펴보고, 마지

막 5장에서는 결론 및 향후 연구 방향을 제시하고자 한다.

2. OSEP (On-Line Secure E-passport Protocol)

2-1. OSEP 프로토콜의 소개

OSEP은 Pasupathinathan에 의해 정의된 프로토콜로 EAC방식을 통해 능동적인 모니터링 시스템에 사용된다. 각 나라 입국 심사대에서 검증 기관의 인증을 통해 여행자의 신분을 확인 할 수 있는 프로토콜이다. 우선적으로 전자여권 칩에 탑제된 개인 정보 변경 유무의 인증 과정을 거친 후 여행자 신원 정보가 검사시스템에 저장이 된다. 그 후에 가까운 인증기관과의 인증 절차가 이루어진다.

2-2. OSEP 프로토콜의 구성

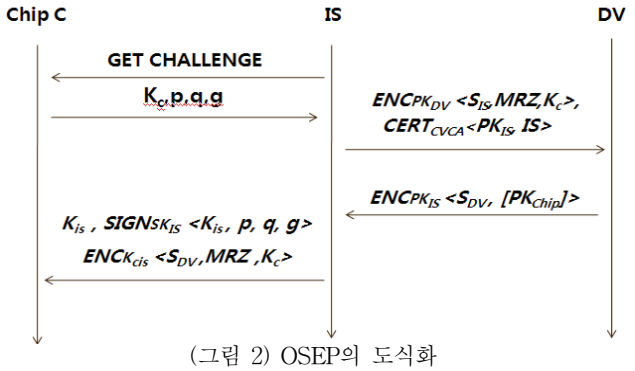
OSEP 프로토콜은 총 3단계로 이루어진다.

- 1단계 : Initial Setup
- 2단계 : IS Authentication (ISA)
- 3단계 : E-Passport Authentication (EPA)

1단계 : Initial Setup
- 프로토콜에서 p, q, g 3개의 공용 값이 필요 - p는 1024bit 또는 그 이상의 소수 - q는 159~160bit 범위의 소수 q|(p-1) - g는 $\forall i < q,\ g^i = 1 \bmod p$. - 각 개체는 자신의 공개키와 비밀키를 갖는다. $PK_i = g^{(Sk_i)} \bmod p$ - 최상위 인증 기관의 증명 표시 $CERT_j <Pk_i , i>$
2단계 : IS Authentication (ISA)
IS → C : GET CHALLENGE C → IS : K_c , p, q, g (S_{IS} = $SIGNSK_{IS}$ <MRZ||K_c>) IS → DV : $ENCPK_{DV}$ <S_{IS},MRZ,K_c>, $CERT_{CVCA}$<PK_{IS}, IS> (S_{DV} = $SIGNSK_{DV}$ <MRZ||K_c||PK_{IS}>,CERTCVCA<PK_{DV} ,DV>) DV → IS : $ENCPK_{IS}$ <S_{DV} , [PK_{Chip}]> IS → C : K_{is} , $SIGNSK_{IS}$ <K_{is} , p, q, g> , $ENCK_{cis}$ <S_{DV} ,MRZ ,K_c>
3단계 : E-Passport Authentication (EPA)
C → IS : $ENCK_{cis}$ <S_C , $CERT_{DV}$ <PK_C> , $CERT_{DV}$ <p, q, g>>

(그림 1) OSEP의 구성

2-3. OSEP 프로토콜의 도식화

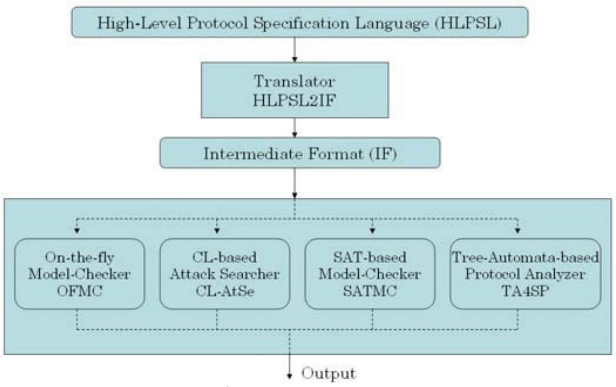


(그림 2) OSEP의 도식화

3. AVISPA와 HLPSL 소개

3-1. AVISPA (Automated Validation of Internet Security Protocols and Applications)

인터넷 프로토콜의 보안성을 정형 검증하는 도구로 상용 프로토콜을 보안의 문제점을 지적하고 있다. AVISPA Tool은 독립적으로 개발된 모듈로 구성되어 있다. 툴의 입력으로 사용되는 High-Level Protocol Specification Language(HLPSL)은 표현력이 뛰어 나고, 모듈로 구성되어 있고, role-based인 정형언어이다. HLPSL은 HLPSL2IF 변환기를 통하여 Intermediate Format(IF)으로 자동 생성되어 OFMC, CL-AtSe, SATMC, TA4SP의 입력으로 사용된다.



(그림 3) AVISPA Tool

On-the-fly Model-Checker (OFMC) [4] 요청 조절 방법(demand-driven way)안에서 IF 명세에서 변환 시스템을 탐구함으로써 프로토콜 변조와 부분적 검증을 수행한다. OFMC 많은 정확성과 완전성을 가진 상징적 기술을(symbolic techniques) 구현한다. 암호적 동작과 타입과 타입이 없는 프로토콜 모델의 수학적 특성 명세를 지원한다.

Constraint-Logic-based Attack Searcher (CL-AtSe) 효과적이고 간결한 heuristics과 중복제거 기술 같은 강제적인 해결책을 제공한다.[5] CL-AtSe는 모듈화 되어 있고 암호적 동작에 수학적 속성을 다룰 수 있다. 정형화된 오류를 추출하고 메시지 연결성을 조절하는 것을 지원한다.

SAT-based Model-Checker (SATMC) IF에 의해 명세된 변환 관계의 제한된 전개를 암호화된 명제식으로 만든다. 보안 속성의 침해를 표현하는 초기상태와 상태집합을 표현한다. 명제식은 최

신 기술의 SAT에 제공된다.

TA4ST (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols)back-end[6]는 정규 트리 언어와 개서를 사용한 침입자 지시 지식에 근접한다. 보안 속성을 위해, TA4SP는 프로토콜에 결점이 있는지 없는지와 어떤 세션이 안전한지 아닌지를 보여줄 수 있다.

3-2. HLPSL(High Level Protocols Specification Language)

HLPSL은 role을 기반으로 하는 언어로써, 각각의 role들은 서로 독립되어 구성이 되어있고, channel을 통해 의사소통을 한다. role은 역할에 따라 두 가지로 나누어 구분할 수 있는데, 프로토콜을 구성하는 각각의 개체들을 기술하는 basic role과 basic role들의 시나리오를 기술하기 위한 composition role로 구성된다. basic role은 각 개체들이 가지고 있는 정보를 표기하고, SND와 RCV 명령어를 이용하여 다른 개체들과 서로의 정보를 교환하여 의사소통을 한다. composition role은 전체 프로토콜의 구성을 나타내는 role로써 각 role들이 가지고 있는 각각의 구조와 공격자(intruder)가 가지고 있는 정보, 프로토콜의 검증 속성을 포함하는 goal들을 표기한다.

4. AVISPA를 이용한 OSEP 위험성 분석

4-1. OSEP 명세

다음은 OSEP을 HLPSL로 명세한 부분 중에 CHIP에 대한 role의 명세부분이다.

```
role CHIP(C, IS, DV: agent,
                PK_dv, PK_is,
                PK_chip,PKc : public_key
                K_cis : symmetric_key

                ) played_by C def=
local S : nat,
      Get_chall,P,Q,G,MRZ : text,
      Kc,Kis,K_cis : symmetric_key,

      SND, RCV: channel (dy)

init S := 0
transition
% C =|> IS
1. S = 0 ∧
   RCV(Get_chall')
   =|>
   S' := 1 ∧
   Kc' := new() ∧
   P' := new() ∧
   Q' := new() ∧
   G' := new() ∧
   SND(Kc, P,Q,G)

   secret(P,t_p,{C,IS,DV}) ∧
   secret(Q,t_q,{C,IS,DV}) ∧
   secret(G,t_g,{C,IS,DV}) ∧
   witness(C,IS,key_k,Kc)

% C =|> IS
2. S = 1 ∧
RCV(Kis.{Kis.P,Q,G}_inv(SignSK_IS).{Sdv.MRZ.Kc}_
ENCK_cis)
   =|>
   S' := 2 ∧
   Sc' := new() ∧
SND({Sc.CERTdv<PKc>}ENCK_cis.CERTdv<P,Q,G>
)

requset(IS,C,key_k,Kc)

end role
```

(그림 4) OSEP의 HLPSL 명세 코드

4-2. OSEP 분석

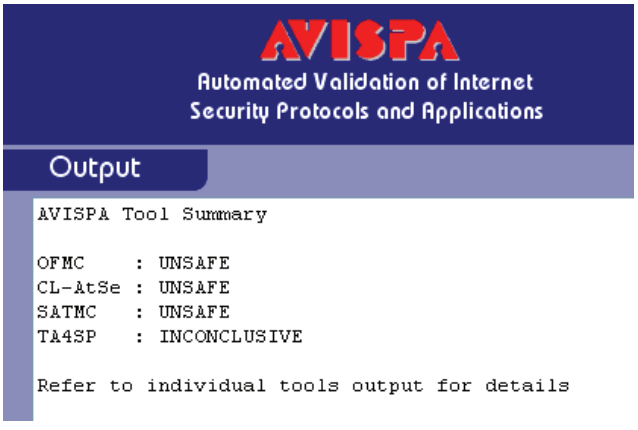
(그림 4)의 명세는 최초 칩과 검사시스템 간의 통신에 있어서 개인 정보를 통신하는 부분이다. 이 부분에서 공격자에 의해 개인 정보 유출이 발생 할 수 있는 경우를 secret(), witness(), request() 함수를 이용해 보안과 인증 속성을 검증해 보았다. 위에 명세 된 코드에서의 각 함수의 의미는 다음과 같다.

secret(P,t_p,{C,IS,DV}) : 칩(C)과 검사시스템(IS)과 검증기관(DV) 사이에 개인정보(P)에 대해 보안요구 사항 중 기밀성이 만족 되는지를 검증한다. t_p는 goal 부분에 명세 하기 위한 ID값이다.

witness(C,IS,key_k,Kc) : Kc의 값에 대해서 IS에 의한 C의 약한 인증(weak authentication)을 의미 하며, key_k는 goal에 명세하기 위한 ID값이다.

request(IS,C,key_k,Kc) : Kc의 값에 대해서 IS에 의한 C의 강한 인증(strong authentication)을 의미 하며, key_k는 goal에 명세하기 위한 ID값이다.

4-3. OSEP 검증 결과



(그림 5) AVISPA의 검증 결과

OFMC, CL-Atse, SATMC UNSAFE로 검증한 결과는 안전하지 않다는 결과가 나온다. 공격자가 중간자 공격을 통하여 C와 IS, IS와 DV간의 인증 세션을 종료시키지 않으면서 중간에서 값을 획득할 가능성이 있다는 것을 보여준다. 위의 결과를 통해 C와 IS, IS와 DV간의 안정성에 취약한 부분이 있다는 것을 확인 할 수 있다.

5. 결 론

전자여권은 전 세계 어디에서나 통용되어 사용되는 신분증이다. 개인의 신분증이 본인을 확인하기 위한 정보를 오픈하는 것은 당연한 사항이나, 사용 용도에 맞게 개인의 정보가 제한되어 오픈될 필요가 있으며, 특히 개인의 민감한 데이터인 바이오 정보는 여권 발행국에서 허용된 국가의 정보기관만이 판독 할 수 있도록 제한되어야 한다. 보안 프로토콜 검증 도구인 AVISPA를 이용하여 전자여권의 보안상 취약점과 해킹 방지 및 위변조 방지등 큰 사고에 대비 할 수 있는 명세 및 검증 방법을 제안한다.

보안 프로토콜의 취약한 부분을 찾고 검증 하는 방법으로 AVISPA를 이용한 방법을 소개 하였고 향후에 더 강력한 프로토콜을 제시 하여 명세 및 검증 할 수 있도록 연구하고자 한다.

참 고 문 헌

[1] AVISPA. "AVISPA v1.1 User Manual", Available at http://www.avispa-project.org, 2006.

[2] V. Pasupathinathan, J. Pieprzyk, H. Wang, "On-Line Secure E-Passport Protocol" Book Chapter in Information Security Practice and Experience Volume 4991/2008, pages 14-28, Springer Berlin / Heidelberg, 14th March 2008.

[3] AVISPA. "HLPSL Tutorial : A Beginner's Guide to Modelling and Analysing Internet Security Protocols", Available at http://www.avispa-project.org, 2006.

[4] D. Basin, S. Modersheim, L.Vigano, "OFMC: A Symbolic Model-Checker for Security Protocols", International Journal of Information Security, 2004

[5] Y. Chevalier and L. Vigneron, "Automated Unbounded Verification of Security Protocols", In Proc. CAV'02, LNCS 2404. Springer, 2002

[6] Y. Boichut, P.C. Heam, O. Kouchnarenko,F. Oehl. "Improvements on the Genet and Klay Technique to Automatically Verify Security Protocols. In Proc. AVIS'04, ENTCS, 2004