인증서 경로검증 알고리즘 평가 도구 개발

정용승*, 이민수*, 황보성**, 이석래**, 이재일**, 박세현*

*중앙대학교, 전자전기공학부

**한국정보보호진흥원

A Development of Evaluation Tool for Certificate Validation Algorithms

Yong Sung Jung*, Min Soo Lee*, Bo Sung Hwang**, Sock Lae Lee**, Jae Il Lee**, Se Hyun Park*

*School of Electronic and Electrical Engineering, Chung-Ang University

**Korea Information Security Agency

요 약

전자상거래, 인터넷뱅킹 등 인터넷이 대중화 된 현재 PKI는 필수적인 요소가 되고 있다. 현재 많은 공인 인증기관에서는 각각의 인증서 경로 검증 알고리즘을 사용하여 인증서 검증에 사용하고 있으나 확실한 표준화가 이루어지지 않은 상황은 유연하고 상호 연동적인 PKI 구축에 많은 어려움을 주고 있다. 이에 본 논문에서는 현재 사용되고 있는 PKI 기반 인증 시스템에서의 경로 검증 모듈의 알고리즘을 평가할 수 있는 평가 항목을 도출하고 이를 기반으로 ITU-T 및 IETF 표준 준수 여부를 평가하는 평가 도구를 구현하여 소개한다. 이 평가 도구는 다가올 유, 무선 PKI 환경 구축에 많은 역할을 할 수 있을 것이다.

I. 서론

최근 전자상거래뿐만 아니라 행정이나 의료 등의 주요 기간 산업과 서비스 분야에 걸쳐 신뢰성 있는 온라인 체계를 갖추기 위해 많은 보안적인 시도가 이루어지고 있다. 이의 대표적인 예가 공개키 기반 구조 (PKI : Public Key Infrastructure)이다. 현재 PKI는 안전한 인터넷 서비스의 필수 요건이 되고 있으나 확실한 표준의 체계화가 이루어지지 않은 시스템과 검증 구조라는 문제점이 대두되고 있다. 특히 공인인증기관에서 사용하고 있는 인증서 경로 검증 알고리즘의 경우 체계적인 표준을 준수하지 않는 실정이라 공인인증기관 사이의 상호인증 등에 많은 어려움이 있다.

본 논문에서는 IETF, ITU-T 규격을 준용해 현재 사용되고 있는 공인인증체계의 인증서 경로검증 알고리즘을 평가할 수 있도록 평가 항목을 제시하고 이에 맞는 평가 도구를 개발하여 본 연구실에서 개발한 검증 알고리즘을 평가하기로 한다.

*본 논문은 한국정보보호진흥원의 지원으로 수행되었음.

II. 경로 검증 알고리즘 구현

기존에 활용되고 있는 경로 검증 알고리즘을 평가하기 위해서는 평가할 기준이 될 검증 알고리즘 구현이 필요하다. 기존에 본 연구실에서 ITU-T의 X.509[1] 표준문서, IETF의 RFC2459[2] 표준문서와 그에 따른 draft[3][4] 문서들의 기반으로 개발된 경로 검증 알고리즘을 이용하여 최근에 공시된 RFC3280[5]의 규격 등을 추가하여 기존의 알고리즘을 제대로 평가할 수 있는 새로운 경로 검증 알고리즘을 구현한다. 구현된 경로 검증 알고리즘은 평가 도구에 삽입되어 평가 항목들에 대한 검증 결과를 생성하고 검증할 소프트웨어의 결과와 비교하여 알고리즘을 평가할 수 있도록 한다. 개발 환경은 windows 2000 Server, 개발 라이브러리는 openssl 0.9.6b[6]을 사용하였다.

III. 평가 항목

현재 인증서 관련 표준화를 진행하고 있는 그룹은 ITU-T와 IETF이다. IETF의 RFC2459와

최근에 공개된 RFC3280의 표준 문서, ITU-T의 X.509, 관련 draft 문서들을 살펴보면 X.509의 기본 구조를 채택하고 있지만 경로검증알고리즘 부분에서 상태변수 이름이나 생성 단계 검증 결과 판단, 확장영역이 없는 인증서 처리 등에서 표준끼리 차이점을 보이고 있다. 본 평가 도구에서는 이 표준들에 준하는 평가 항목을 실정하여 각각의 표준에 준하는 알고리즘을 검증 소프트웨어가 가지고 있는지 평가할 수 있도록 개발하는 것이 목적이다. 구체적인 평가 항목은 다음과 같다.

(1) 기본 인증서 검증

인증서내의 전자서명과 시간항목들이 올바른지에 대한 검증과 name chain 및 인증서 폐지 정보들에 대한 정확한 검증을 수행하여 결과를 도출하는가?

(2) 중계 인증서 검증

인증경로 내의 모든 중계인증서들에 대해 basic constraints 확장영역, name constraints 확장 영역검증 등의 데이터를 바탕으로 정확한 검증을 수행하는가?

(3) 인증 경로 정책 연결 검증

경로상의 인증서 내의 policy set 값들과, initial-explicit-policy, requireExplicitPolicy값들의 설정 값에 의해 Authority constrained policy set, User constrained policy set, Explicit policy indicator를 제대로 실정하고 올바른 검증결과를 도출하는가?

(4) Path length 관련 검증

특정한 path length constraint를 감안한 path length를 계산하여 경로 검증 성공 여부를 정확하게 판별하는가? 다양한 path length의 경우와 그에 따른 여러 경우의 path length constraint를 실정하여 테스트한다.

(5) Directly Issued Full CRL 검증

CRL들의 전자 서명, issuer name, 폐기, 시간 정보들과 확장영역에 대한 정확한 검증결과를 도출하는가?

[표 1]에 평가 도구가 평가할 항목을 나타내고 있다.

CRITERIA
[illegible]
전자 서명 검증
notBefore 항목 검증
notAfter 항목 검증
name chain 검증
인증서 폐지 정보 검색
폐지된 인증경로의 인증서 검증
[illegible]
기본 제한 확장영역 검증
기본 제한 확장영역과 cA 컴퍼넌트 검증
pathLenConstraint 영역 검증
기본 제한 확장영역과 키 사용 확장 영역 검증
키 사용 확장 영역 검증
CRL singer 의 공개키 검증
nameconstraints 검증
[illegible]
authority constrained policy set 검증
policy와 policy qualifier 검증
policy mapping 검증
inhibit policy mapping state variable 검증
explicit policy indicator state variable 검증
authority constrained policy set 검증
user constrained policy set 검증
explicit policy indicator state variable 검증
검증 결과 검증
[illegible]
permitted path length 검증
[illegible]
전자 서명 검증
issuer name 검증
폐기된 인증서 검증
nextUpdate 검증
daltaCRLIndicator 검증
issuingDistributionPoint 검증

표 1: 평가 항목

위의 평가항목들을 적용하기 위한 인증서 및 CRL들은 NIST의 인증경로 적합성 테스트(NIST PKI Program X.509 Path Validation Test Suite, Version 1.07)에서 사용되는 것을 기본으로 구성하였고 추가할 항목들을 설정하여 구성한다. 평가항목을 만족하기 위해서 적합한 인증서와 CRL들을 사용하여 테스트 시나리오를 설정하고 테스트 항목들을 생성한다. 생성된 테스트 항목들은 검증의 중요도에 따라 각각의 level이 부가된다. 정확한 검증데이터를 얻기 위해 하나의 평가항목은 여러 개의 테스트 항목으로 나누어진다.

IETF의 RFC 2459, RFC 3280, ITU-T의 X.509 표준에 따라 평가항목의 테스트 시나리오는 분류를 하고 평가 도구는 각각의 표준을 평가할 수 있도록 분류된 시나리오 테스트 항목을 이용하여 각각의 표준을 제대로 준수하는지 테스트한다.

IV. 평가 도구의 설계 및 구현

경로검증 알고리즘의 평가를 위해서는 검증한 소프트웨어와 평가 도구 사이의 인터페이스 구현

이 필요하다. 현재 쓰이는 경로검증 소프트웨어들은 정형화된 입력값이나 출력값이 없는 실정이므로 평가를 위해서 이 논문에서 하나의 인터페이스를 제시하고 검증을 위해서 인터페이스를 따르게 하기로 한다. 먼저 검증할 소프트웨어의 입력값은 검증할 인증서와 그에 따른 경로상의 모든 인증서, CRL들이 필요하다. 평가 도구에서는 이 모든 입력들을 REQ 확장자를 가진 하나의 파일을 사용하기로 하며 출력값은 검증 테스트에 필요한 인자들을 ASN.1의 규격에 따라 RES 확장자를 가진 하나의 파일로 만들 수 있도록 인터페이스를 구현한다. RES 파일의 구조를 목적에 맞게 설계하여 상태변수를 비교할 수도 있으며 검증 결과의 성공여부만으로도 알고리즘을 평가할 수 있다. 검증 받을 소프트웨어는 도구에서 제공하는 REQ 파일들을 가지고 검증하고 그 결과로 나온 RES 파일들을 이용하여 평가 도구가 결과를 출력할 수 있도록 해야 한다. [그림 1]은 평가 도구의 경로 검증 알고리즘 평가 절차를 나타내고 있다.

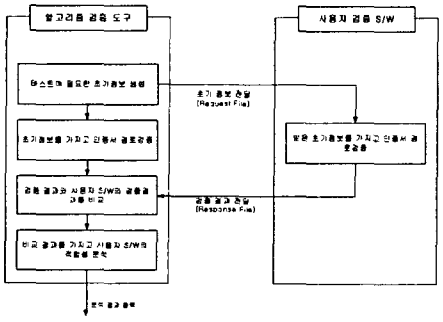

그림 1: 경로 검증 알고리즘 평가 절차

평가도구는 크게 다음과 같은 모듈로 나누어진다.

(1) REQ 파일 생성 모듈

평가항목을 실제로 테스트하기 위해 적합한 인증서와 CRL들을 사용하여 하나의 시나리오를 작성하는데 사용되는 부분이다. 인증서와 CRL을 삽입하여 하나의 경로 검증을 위한 입력 REQ 파일을 생성할 수 있다. 여기서 생성된 REQ 파일은 평가 도구에서 제공되는 인터페이스를 사용하여 검증할 소프트웨어와 평가 도구의 입력값으로 사용된다.

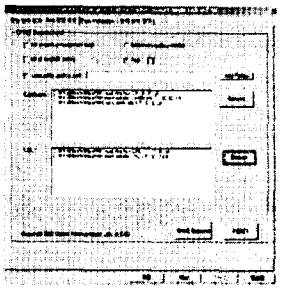

그림 2: REQ 파일 생성 모듈

(2) 인증서 경로 검증 모듈

평가항목 별로 생성된 REQ 파일을 이용하여 경로 검증 결과를 도출할 수 있는 부분이다. 평가항목에 준하여 생성한 REQ 파일을 입력값으로 사용하여 예상한 결과가 나오는지 확인하여 평가항목의 유효성을 확인한다. 결과값으로 RES 파일을 생성한다.

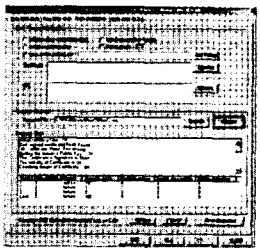

그림 3: 인증서 경로 검증 모듈

(3) RES 파일을 이용한 세부 평가 모듈

검증할 소프트웨어와 도구에서 생성된 두개의 RES 파일을 이용해 검증 과정, 상태 변수 설정들을 세부적으로 알 수 있는 기능을 제공하는 부분이다.

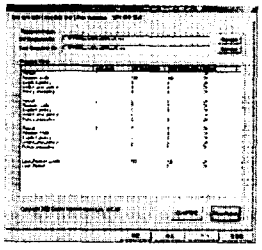

그림 4: RES 파일을 이용한 세부 평가 모듈

(4) RES 파일들을 이용한 전체 평가 모듈

모든 평가항목에 의해 생성된 RES 파일들을 이용하여 검증할 소프트웨이가 얼마나 평가항목들을 만족하고 있는지를 알 수 있게 해주는 부분이다.

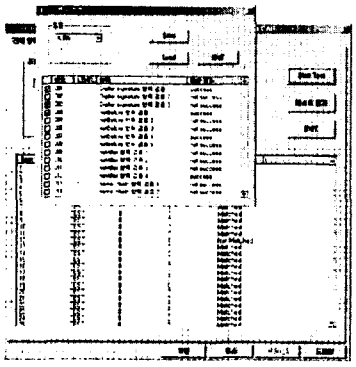

그림 5: RES 파일들을 이용한 전체 평가 모듈

V. 평가 도구 결과 분석 및 고찰

구현된 평가 도구의 성능을 분석하기 위해 기존에 본 연구실에서 개발했던 경로 검증 알고리즘을 평가하였다. 검증대상의 경로 검증 알고리즘은 RFC 2459의 요구사항을 만족하며 개발 당시 공시되었던 draft 문서의 요구사항을 대부분 만족시킨다. 하지만 name constraints 확장 처리 부분과 issuingDistributionPoint 검증 부분은 처리를 하지 않는다.

평가 도구의 결과는 처리 모듈이 없는 name constraints 부분과 issuingDistributionPoint 검증 항목에서 예상 결과와 일치하지 않는 결과를 보였다.

VI. 결론 및 향후 연구 과제

본 논문에서는 현재 이용되고 있는 PKI 모듈중 경로 검증 알고리즘의 적합성을 평가 할 수 있도록 평가항목을 설정하고 평가도구를 구현하였다.

본 논문에서 구현된 인증서 경로 검증 평가 도구를 사용하여 서비스를 시행하고 있거나 개발중인 경로검증 모듈의 적합성을 평가하여 보다 상호연동적이며 유연성을 가질 수 있는 PKI 환경을 구축할 수 있게 될 것이다.

향후 연구과제로는 보다 완전하고 손쉽게 현재 사용되고 있는 공인인증기관의 인증서 경로검증 알고리즘을 평가할 수 있도록 체계화된 새로운 평가 항목 도출과 그에 따른 테스트 시나리오를 보강해 나가는 것이 필요하다.

참고문헌

[1] ITU-T Recommendation X.509, "Information technology - Open systems interconnection - The directory : public-key and attribute certificate frameworks", 2000

[2] IETF Network Working Group, "[RFC 2459] Internet X.509 Public Key Infrastructure Certificate and CRL Profile", 1999

[3] IETF PKIX Internet Draft, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", 2001. 1

[4] IETF PKIX Working Group, "[Internet-Draft] Internet X.509 Public Key Infrastructure Certificate and CRL Profile", 2000

[5] IETF Network Working Group, "[RFC 3280] Internet X.509 Public Key Infrastructure Certificate and CRL Profile", 2002

[6] http://www.openssl.org