정책 관련 인증경로검증 알고리즘 분석

고규만*,송주석*

*연세대학교, 컴퓨터 과학과

Analysis of Certification Path Validation Algorithm Related with Policy

K.M. Ko*, J.S. Song*

*Department of Computer Science, Yonsei University

요 약

PKI 구축을 위한 노력이 전 세계적으로 진행되고 있는 가운데 PKI의 계층구조 유형에 따라 인증관리 정책, 인증서 형식 등의 서로 다른 PKI 구성요소를 가진 인증기관(CA)들이 각기 다른 곳에 분산되어 있다. 그러므로, 이러한 CA간의 상호인증 서비스를 어떻게 제공할 것인가를 고려해야 할 필요가 있다. 특히 상호인증 서비스를 제공하기 위한 인증정책, 정책매핑, 정책제한의 확장영역은 인증경로의 유효성을 검증할 때 검증의 성공과 실패에 중요한 영향을 미친다. 본 논문은 ITU-T X.509의 인증경로처리과정에서 정책과 관련된 부분을 살펴보고 ITU-T X.509 3rd Edition의 정책관련 문제점들이 ITU-T X.509 4th Edition에서 어떻게 개선되었는지 몇 가지 예를 통하여 제시하고 앞으로 인증경로처리과정이 어떠한 방향으로 확장되고 응용되어야 할지를 기술한다.

I. 서론

초기의 LAN Protocol(NetBIOS, IPX)은 큰 네트워크에 잘 확장될 수 없었다. 하지만, LAN 프로토콜을 대치하는 Internet TCP/IP 프로토콜을 사용해서 LAN을 WAN에 효과적으로 연결시킨 것은 인터넷의 엄청난 발전을 가져 왔다. 이와 마찬가지로 PKI에서도 신뢰의 전파가 작은 조직에 국한되는 것이 아니라 다른 국가와 전 세계를 통하여 전파된다면 인터넷을 통한 전자상거래가 기밀성, 무결성, 확실성을 기반으로 효율적으로 이루어질 수 있을 것이다. 현재 인증서를 사용하는 많은 시스템이 지금 구현되고 있다. 그들 사이에서 신뢰가 광범위하고도 일관성 있게 전파될 수 있도록 인증경로를 생성하고 검증하는 것은 중요한 문제이다. 공인인증기관을 비롯하여 국가PKI를 원활하게 운영하기 위해서는 정부의 상호인정 지원 및 외국 인증기간의 상호인증 처리를 통한 상호운용성 확보 등의 해결해야 할 문제점을 가지고 있다. 현재 사용되고 있는 공개키 기반 인증서 검증은 인터넷에서 무결성(integrity), 기밀성(confidentiality), 확실성(authenticity)을 제공한다. 여기에 많은 인증기관들이 다양한 서비스를 제공하기 위해 ITU-T X.509 v3. 표준의 확장영역을 이용하고 있으며 또한 서로 다른 정책을 사용하는 도메인간의 상호연동을 위해 정책의 연결이 중요하다. 즉, 서로 다른 인증 체계 영역간 인증서 검증이 단순히 MAC(Message Authentication Code) 검증이나, 기본 유효성 검증만으로 부족하다. 이에 ITU-T와 IETF에서 제시한 확장영역을 사용하여, 인증서 경로의 인증서 정책들이 유효하게 연결되어 있는지를 검증할 필요가 있는 것이다. 인증서의 인증경로 검증에 대해서 IETF RFC2459(01/1999)에서 그 수행절차를 언급하고 있지만 이는 개념적인 기술로만 언급되어 있고 특히 정책매핑(policy mapping)과정이 어제 수행될지 명확하게 언급되어 있지 않으므로 시스템을 실제로 구축해야 하는 구현자에게는 적용하기 어렵다. 이에 IETF Internet-Draft Certificate and CRL Profile(07/2000)에는 정책 매핑과 인증서 정책의 검사 및 수행절차를 좀 더 구체적으로 제시하고 있어 실제로 구현자에게 실제적인 지침이 될 수 있다. 본 논문에서는 ITU-T X.509 3rd Edition(06/1997)와 ITU-T X.509 4th Edition(03/2000)을 중심으로 인증 경로 검증 절차의 차이점을 분석하고 X.509 3rd Edition의 문제점을 X.509 4th Edition에서 어떻게 개정되고 있는 지 가상의 인증경로를 적용해서 알아보고

앞으로의 연구방향에 대해 기술한다.

II. 본문

ITU-T X.509(1997)	ITU-T X.509(2000)
Authority Key Identifier Subject Key Identifier Key Usage Extended Key Usage Priviate Key Usage Period **Certificate Policyes** **Policy Mapping**	Authority Key Identifier Subject Key Identifier Key Usage Extended Key Usage Priviate Key Usage Period **Certificate Policyes** **Policy Mapping**
Subject Alternative Name Issuer Alternative Name Subject Directory Attributes	Subject Alternative Name Issuer Alternative Name Subject Directory Attributes
Basic Constraints Name Constraints **Policy Constraints**	Basic Constraints Name Constraints **Policy Constraints** **Inhibit Any Policy**
CRL Distribution Points	CRL Distribution Points Freshest CRL

그림 1: X.509 인증서 확장 필드 비교

1. 인증정책 관련 확장필드

인증정책 관련 확장 필드에는 Certificate Poicies, Policy Mapping, Policy Constraints, inhibit Any Policy 있으면 특히 inhibit Any Policy는 ITU-T X.509 4th Edition에 추가된 확장 필드이다.

1) certificate Policies(인증서 정책)

인증서를 생성하기 위한 규칙들의 집합으로서, 인증서 발행에 사용된 정책 및 인증서 사용목적 등을 나타낸다. 인증서 사용자가 수신된 인증서가 특정응용에 적용 가능한지를 결정하기 위한 판단 기준이 된다. 일반적으로 인증서 정책은 OID로 공표되며 특정의 OID와 정책을 기술하는 문서는 1:1 대응 관계가 있다. PolicyIdentifier는 인증서 정책의 OID이고 PolicyQualifiers는 인증서 정책의 구체적인 명칭 또는 이를 나타내는 방법이다

2) Policy Mappings(정책 매핑)

Issuing CA의 정책과 Subject CA의 정책이 서로 동등함을 나타내고 CA 인증서에만 사용된다. issuerDomainPolicy는 인증서를 발급하는 Issuer CA의 정책 OID고 subjectDomainPolicy는 인증서를 발급받은 Subject CA의 정책 OID다.

3) Policy Constraints(정책 제한)

정책 검사 및 정책매핑 제한을 통하여 경로의 유효성을 제한하고 CA 인증서에만 사용된다. requireExplicitPolicy는 인증경로상에서 현재 이후로 acceptable policy 이외의 정책이 허용되는 횟수를 SkipCerts 값에 지정하고 지정된 횟수 이후로는 모든 인증서가 acceptable policy를 가져야 한다. acceptable policy는 사용자가 받아들일 수 있는 정책으로 정책매핑에서 동치로 판단된 것도 포함한다. inhibitPolicyMapping은 인증경로 상에서 현재 이후로 정책매핑이 허용되는 횟수를 SkipCerts값에 지정하고 지정된 횟수 이후로는 Policy Mapping이 금지된다. SkipCerts값은 인증경로에서 제한이 적용되기 전까지 스킵하는 인증서의 수를 나타낸다.

4) Inhibit Any Policy

anyPolicy가 인증경로 상에 있는 모든 인증서의 정책들과 연결 되는 것을 제한한다.

2. 인증경로 검증 파라미터 비교

	ITU-T X.509(1997)	ITU-T X.509(2000)
Input	• 인증경로를 구성하는 인증서들의 집합 • trusted public key value or key identifier • initial-policy-set • initial-explicit-policy • initial-policy-mapping-inhibit • 현재 날짜 및 시간	
		• initial-inhibit-any-policy
Output	• 인증경로 유효성의 성공과 실패 여부 • 실패한 경우 실패한 이유 • 인증경로가 유효할 때 authorities-constrained policies 집합 또는 any-policy • 정책매핑에 대한 자세한 내용	
		• user-constrained policies 집합 (authorities-constrained-policy-set ∩ initial-policy-set • explicit-policy-indicator
state variables	• authorities-constrained-policy-set • permitted-subtrees • excluded-subtrees • explicit-policy-indicator • policy-mapping-inhibit-indicator • pending-constraints (explicit-policy-pending,policy-mapping-inhibit-pending)	
	• user-constrained-policy-set	• path-depth • inhibit-any-policy-indicator • pending-constraints (inhibit-any-policy-pending)

그림 2: 인증경로검증에서 입출력 파라미터 비교

• initial-policy set

인증경로 처리과정에서 인증서 사용자가 받아들일 만한 인증서 정책을 나타내는 인증정책 ID의 집합, any-policy를 가질 수 있다.

• initial-explicit-policy

받아들일 만한 정책들이 경로의 모든 인증서 정책확장 영역에 명시적으로 나타나야 함을 지시하는 값

• initial-policy-mapping-inhibit

인증경로에서 정책매핑의 허용여부를 나타낸다

• initial-inhibit-any-policy

인증서 정책 확장영역에 anyPolicy가 나타날 때 이 anyPolicy가 제한된 정책의 특정한 정책과 연결되어야 할 지를 나타낸다.

• user-constrained-policy-set

인증경로에서 인증서 사용자가 받아들일만한 인증서 정책 집합이다. X.509 3rd에서는 initial-policy-set로 초기화되며 검증과정에서 인증경로를 따라 생성되는 authorities-constrained-policy-set과 비교하여 검증의 성공과 실패가 결정되고 X.509 4th에서는 검증의 최종단계에서 authorities-constrained-policy-set과 initial-policy-set의 교집합으로 결정된다.

- **authorities-constrained-policy-set**

인증경로에서 인증기관이 받아들일만한 인증서 정책 집합이다. X.509 3rd와는 달리 X.509 4th에서는 테이블 형태로 표현되고 있는 것이 큰 특징이다. 테이블에서 행(row)는 정책, 정책 한정자(qualifier), 연결내력(history)을 나타내고 열(column)은 인증경로에서 처리되는 인증서를 나타낸다.

- **explicit-policy-indicator**

인증경로에서 받아들일만한 정책들이 모든 인증서에 명시적으로 나타나야 할지를 지시한다. X.509 3rd에서는 이 값이 경로검증과정의 모든 인증서마다 체크되어 경로의 유효성을 판단한다. X.509 4th에서는 출력값이 true라면 authorities-constrained-policy-set이 empty인지 검사한다.

- **policy-mapping-inhibit-indicator**

정책 매핑이 금지될 경우 사용한다.

- **inhibit-any-policy-indicator**

anyPolicy가 어떤 특정한 인증정책과 연결하는 것을 금지할 경우 사용한다.

- **pending-constraints**

explicit-policy-pending, policy-mapping-inhibit-pending, inhibit-any-policy-pending로 구분되며 explicit-policy-indicator, policy-mapping-inhibit-indicator, inhibit-any-policy-indicator가 사용되지 않을 수 있는 인증서의 최대 개수를 나타낸다. inhibit-any-policy-pending는 X.509 4th에서 추가된 것이다.

3. 기본 인증서 체크

```
PolicyBasicCheck();
IF(explicit_policy_indicator == TRUE
  AND user_constrained_policy_set != any-policy)
    IF(certificate policies extension is present AND
      (extension_policy_set∩user_constrained_policy_set !==NULL))
      CHECK1=SUCCESS  ELSE CHECK1=FAIL
    END IF
IF(certificate policies extension is present
  AND criticality flag == TRUE)
    authority_constrained_policy_set
    =authority_constrained_policy_set∩extension_policy_set
    IF(authority_constrained_policy_set∩user_constrained_policy_set !=NULL)
      CHECK2=SUCCESS  ELSE  CHECK2=FAIL
    END IF
IF(CHECK1==FAIL or CHECK2==FAIL)
    RETURN FAIL
END IF
```

그림 3: X.509 3rd 기본 인증서 체크

```
PolicyBasicCheck();
IF(certificate policies extension is not present)
  authorities_constrained_policy_set = NULL
  by deleting all rows from the authorities-constrained-policy-set table
END IF
IF(certificate policies extension is present)
  anyPolicy가 아닌 확장영역의 각 policy P에 대해
  P를 포함하는 authorities-constrained-policy-set table의
  [path-depth] column entry의 각 row에 P와 관련 있는 policy qualify를 첨가해라.
  IF(authorities_constrained_policy_set[0,path-depth]==any-policy 인 것을 제외하고
    P를 포함하는 authorities-constrained-policy-set table의
    [path-depth] column entry의 row가 없다.)
    0번째 row를 복사해서 새로운 row를 만들고
    그 row의 [path-depth]column entry에 P와 P와 관련 있는 policy qualify를 쓰라.
END IF
IF((certificate policies extension is present AND
  (extension_policy_set∩any-policy==NULL)OR(inhibit_any_policy_indicator==TRUE))
  extension_policy_set 중 어느 하나도 포함하지 않는 [path-depth] column의
  row를 지우고 any-policy를 포함하는 [path-depth] column의 row를 지우라
END IF
IF(certificate policies extension is present AND
  (extension_policy_set∩any-policy!=NULL) AND inhibit_any_policy_indicator=FALSE)
  any-policy나 extension_policy_set에 없는 값을 포함하는
  authorities-constrained-policy-set table의 [path-depth] column entry의
  각 row에 any-policy와 관련 있는 policy qualify를 첨가하라
END IF
```

그림 4: X.509 4th 기본 인증서 체크

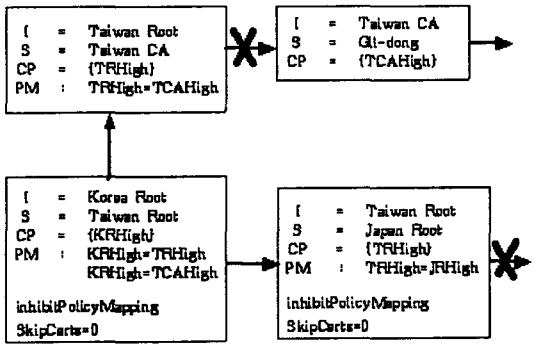
4. 인증서 경로 검증

인증경로를 구성하기 위해 몇 가지 가정과 제한을 둔다.

- 각각의 인증서에 대한 기본 검증의 결과는 유효하다
- I : Issuer, S : Subject, CP : Certificate Policies, PM : Policy Mapping
  ACPS : authorities-constrained-policy-set
  UCPS : user-constrained-policy-set
- 인증정책 확장영역은 critical이고 initial-policy-set은 any-policy이다.

인증서에 inhibitPolicyMapping 확장영역이 있거나 initial-policy-mapping-indicator가 true일 때 모든 정책매핑이 중단된다. inhibitPolicyMapping확장영역과 관련하여 X.509 3rd의 인증정책처리는 신뢰당사자(relying party)가 주어진 경로가 유효하다고 하고 싶지만 그 경로를 거부하는 결과를 초래한다. inhibitPolicyMapping 확장영역 문제를 설명하기 위해 다음 예를 사용할 것이다. Korea Root의 신뢰당사자는 Taiwan Root과 다른 정책을 사용하고 있지만 Taiwan 인증서 주체(Subject)까지의 인증경로를 유효하게 판단하기 위해 Korea Root는 Taiwan Root와 상호인증하기를 희망한다. 동시에 Korea Root에서 non-Taiwan Root까지의 경로는 Korea 신뢰당사자들에게 유효하지 않아야 한다. Korea Root가 Taiwan Root에게 발급한 인증서에는 inhibitPolicyMapping 확장필드를 이용하여 Korea 신뢰당사자들이 Taiwan 신뢰도메인을 빠져나가는 경로의 유효성을 인정하지 않기 위해

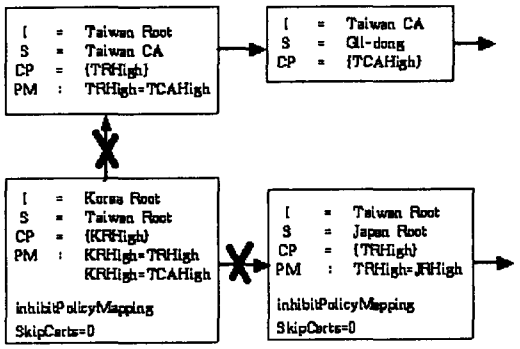
정책매핑을 금지시켰다. X.509 3th과 X.509 4rd의 인증경로처리방법으로 Korea Root를 시작하여 Gil-dong에게 발급된 인증서까지의 인증경로(**Path1**)와 Korea Root를 시작하여 Japan Root에게 발급된 인증서까지의 인증경로(**Path2**)의 유효성을 검증한다. 기대되는 검증결과는 **Path1**은 **Success**되고 **Path2**는 **Fail** 되어야 한다.



	Path1	Path2	
초기값	ACPS={any-policy} UCPS={any-policy}	초기값	ACPS={any-policy} UCPS={any-policy}
Korea Root	ACPS={KRHigh,TRHigh,TCAHigh} UCPS={any-policy}	Korea Root	ACPS={KRHigh,TRHigh,TCAHigh} UCPS={any-policy}
Taiwan Root	ACPS={TRHigh} UCPS={any-policy}		
Gil-dong 인증서	ACPS={} UCPS={any-policy}	Japan Root 인증서	ACPS={TRHigh} UCPS={any-policy}
검증결과	Fail	Success	

그림 5: X.509 3rd 인증서 검증결과

위의 결과에서 알 수 있듯이 **Path1**과 **Path2**의 검증결과가 기대했던 것처럼 나오지 않았음을 알 수 있다. Korea Root가 inhibitPolicyMapping의 사용을 통해 신뢰의 확산을 올바르게 제한하지 못했다 .



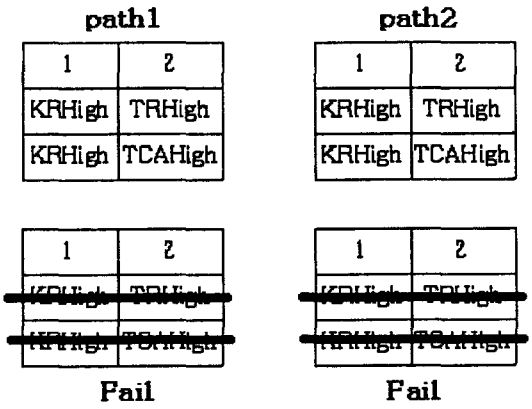


그림 6: X.509 4th 인증서 검증결과

X.509 4th 인증서 검증결과에서 **Path2**에서는 원하는 결과를 얻을 수 있었지만 **Path1**에서는 X.509 3rd에서와 같이 검증이 성공하지 못했다. X.509 3rd에서 policy checking이 policy mapping보다 먼저 수행됨으로 인해 유효하지 않는 인증경로를 받아들이는 경우가 발생했는데 X.509 4th에서 이 문제를 해결함으로 **Path2**에 대한 검증결과 바르게 나왔다.

Ⅲ. 결론

본 PKI의 원활한 운영을 위해서 인증서 확인 검증 절차에 대한 표준화 작업이 계속 되어야 한다. 본 논문에서는 정책부분과 관련하여 X.509 3rd와 4th의 차이점을 분석하고 인증경로 검증 예를 통해서 어떠한 부분이 개정되었는지 알 수 있었다. 아직 X.509 4th에서도 정책매핑이 먼저 수행되어 Mapping 과정에서 문제가 발생되는 경우 인증경로 전체를 거부해 버리는 문제를 해결해야 한다. 앞으로 다양한 PKI구조에 효율적으로 대응할 수 있도록 하기 위해 현재 거론되고 있는 문제점을 수정한 인증경로 알고리즘이 제시되어야 한다.

참고문헌

[1] Housely, R., W. Ford, W. Polk, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile draft-ietf-pkix-new-part1-08",July 2001

[2] ITU-T Recommandation X.509(1997)| ISO/IEC 9594-8:1997,"Information technology-Open Systems Interconnection-The Directory:Authectication Framework",August 1997