제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

인증서 폐기 메커니즘의 최근 동향 분석

황 원 섭*, 김 자 영*, 정 수 민*, 윤 동 식*
* 안동과학대학 사이버테러대응학과

요 약

Kohnfelder는 1978년 그의 학사논문 "Towards a Practical Public-Key Cryptosystem"을 통해 처음으로 서명된 데이터구조, 즉 믿을 수 있는 사람에게 공개키를 전달할 수 있는 인증서의 개념을 소개했다. 따라서 20년이 넘도록 이 개념은 무결성 관점에서 공개키를 필요한 사용자에게 전달하기 위해 필요한, 확장 가능하고 안전한 방식으로 인정받고 있다. 간단히 말하면, 공개키 인증서는 사용자의 이름이나 사용자와 연관된 어떤 특성을 사용자의 공개키와 연결하는데 사용된다. 현재 공개키 기반의 인증서는 인터넷뱅킹, 전자상거래 분야뿐만 아니라 개인 식별을 위해 주민등록번호 대신 사용되는 등 그 활용범위가 넓어지고 있다. 인증서가 만료되지 않았더라도 발급된 인증서가 더 이상 유효해서는 안 되는 경우가 있을 수 있다. 따라서 인증서가 유효기간이 종료되기 전에 공개키 인증서를 폐기할 수 있도록 효율적이면서 신뢰할 수 있는 방식이 필요하며, 이에 대한 다양한 방식이 제안되고 있다. 인증서 폐기는 PKI의 광범위한 사용에 따라 점차 중대한 문제가 되어가고 있다. 그러므로 본 논문에서는 지금까지 발표된 인증서 폐기 메커니즘 및 최근 동향에 대하여 분석하고자 한다.

Recent Trend Analysis of Certificate Revocation Mechanism

Hwang Won Seop*, Kim Ja Young*, Jeong Soo Min*, Yun Dong Sic*
* Andong Science College Dept. of Cyberterror Defense

ABSTRACT

The notion of a certificate was introduced by Kohnfelder in his 1978 MIT bachelor's thesis. The idea, now common, was that a certificate is a digitally signed statement binding the key-holder's name to a public key. With the increasing acceptance of digital certificate, there has been a gaining impetus for methods to nullify the compromised digital certificates and enable the end user to receive this information before be trusts a revoked certificate. The problem of certificate revocation is getting more and more crucial with the development of wide spread PKIs. In this paper, we investigate recent trend of certificate revocation mechanism.

1. 서 론

인터넷의 발달과 함께 전자상거래가 활성화되고 안전한 네트워크 환경의 구현에 공개키 기반 구조의 응용이 확대됨에 따라 통신에 있어서의 신뢰성을 충족시키기 위해 인증서가 사용되었다.

이러한 인증서의 사용이 증가함에 따라 인증서의 효력정지 및 폐기상태에 관한 정보를 효율적으로 제공하기 위한 연구가 활발히 진행되고 있으며, 그 결과로 다양한 인증서 폐기 메커니즘들이 IETF(Internet Engineering Task Force)의 PKIX(Public Key Infrastructure based on X.509) 워킹그룹의 표준화 작업을 거쳐 발표되고 있다.

본 논문에서는 현재까지 발표된 RFC와 Draft 문서를 바탕으로 인증서 폐기 메커니즘의 최근 동향에 대하여 논의 하고자 한다.

본 논문의 2장에서는 지금까지 발표된 인증서 폐기 메커니즘에 대해서 살펴본다. 3장에서는 기존 메커니즘들을 비교분석한다. 끝으로 4장에서는 결론을 맺는다.

2. 인증서 폐기 메커니즘

2.1 IETF PKIX 주요 표준화 문서

[표 1] PKIX RFCs

분야	내용	문서번호
기반 분야	PKI 인증서 및 인증서 폐기 목록 프로파일	RFC3280 (2459대체)
	PKIX암호 알고리즘과 확인자	RFC3279
	PMI 속성 인증서 프로파일	RFC3281
	자격 인증서 프로파일	RFC3739 (3039대체)
	CMP를 이용한 인증서 관리 메시지	RFC2797
	Diffie-Hellman 개인키 소유증명 알고리즘	RFC2875
	인증서 요구 메시지 형식	RFC2511
	인증서 관리 프로토콜	RFC2510
	KEA 키 표현	RFC2528
운영	운영 프로토콜 LDAPv2/FTP/HTTP/ LDAPv2 Schema	RFC3494 (2559대체), 2585, 2587
인증서 검증	OCSP/DPD-DPV/SCVP	RFC2560, 3379, Drafts
인증서 정책	인증서 정책, 속성 인증서 정책	RFC3647 (2527대체)
데이터 검증	타임스탬프/데이터 검증 및 인증 서비스	RFC3161, 3029, 3628

2.2 인증서 구조 및 의미

X.509가 인증서의 표준항목 및 확장과 관련된 어떤 요구조건을 정의하고 있더라도, 다른 인증서는 상호운용에 있어서의 고려사항을 완전하게 다루기 위해 특정한 프로파일(profile)에서 개선되어야 한다. IETF(Internet Engineering Task Force)의 PKI X.509(PKIX) 워킹그룹은 1999년 1월에 이러한 프로파일을 RFC2459에서 소개했지만, 2002년 4월에 RFC3280으로 대체되었다. RFC3280은 인터넷 커뮤니티를 목적으로 하고 있지만, RFC3280의 여러 가지 권고사항이 기업 환경에 똑같이 적용될 수 있으며, 가능한 일관성이 유지되어야 한다.

[그림 1]은 X.509 공개키 인증서 버전3의 일반적인 구조를 보여준다.

Version
Serial Number
Signature
Issuer
Validity
Subject
Subject Public Key Info
Issuer Unique Identifier
Subject Unique Identifier
Extensions

[그림 1] 공개키 인증서 구조(버전3)

- Version : X.509의 버전으로 0은 버전1, 1은 버전 2, 2는 버전 3을 의미
- Serial Number : 발행기관이 생성한 각각의 인증서에 대한 유일 식별자
- Signature : 발행기관이 인증서를 서명하는데 사용한 알고리즘
- Issuer : 인증서를 서명하고 생성한 자의 ID로서, X.500에 정의된 계층적인 명명법인 DN
- Validity : 인증서의 유효기간
- Subject : 공개키 소유주의 ID, X.500 명명 방식을 따름
- Subject Public Key Info : 사용자의 공개키와 공개키에 대한 정보(알고리즘과 파라미터)
- Issuer Unique ID : 버전2 이상 사용, 발행기관의 부가적인 정보 포함
- Subject Unique ID : 버전2 이상 사용, 공개키 소유주의 부가적인 정보를 포함
- Extensions : 인증 정책 등 여러 가지 사항을 포함

2.3 인증서 폐기 목록(CRL)

CRL은 폐기된 인증서의 목록을 가지고 있는 서명된 데이터 구조이다. [그림 2], [그림 3], [그림 4]는 X.509 표준[X509-00]에 정의된 인증서 효력정지 및 폐기 목록 프로파일 구조, 확장을 나타내었다.

Version
Signature
Issuer Name
This Update
Next Update
Revoked Certificates User Certificates Revocation Date CRL Entry Extensions
CRL Extensions

[그림 2] CRL 버전2의 기본구조

Reason Code
Hold Instruction Code
Invalidity Date
Certificate Issuer

[그림 3] CRL Entry Extensions

Authority Key Identifier
Issuer Alternative Name
CRL Number
Delta CRL Indicator
Issuing Distribution Point
Freshest CRL
CRL Scope
Status Referrals
CRL Stream Identifier
Ordered List
Delta Information
Base Update

[그림 4] CRL Extensions

일반적인 CRL 검증 기술은 CRL 갱신 주기(정책) 기반 인증서 상태정보 DB를 scanning 후 CRL생성후 디렉토리에 게시한다. 이는 폐기 인증서 증가에 따른 CRL 크기 문제와 CRL 갱신 주기에 따른 실시간 인증서 검증 문제가 발생된다.

2.4 CRL Distribution Point

CRL 분배점은 하나의 CA 영역 내에 있는 폐기 정보가 다중의 CRL에 기입될 수 있도록 한다.

폐기 정보는 CRL의 규모가 커지는 것을 막기 위해서 관리가 가능한 크기로 분할될 수 있고, 인증서는 CRL 분배점의 위치를 지정할 수 있기 때문에 신뢰할 수 있는 사용자는 특정한 인증서에 대한 폐기 정보의 위치를 사전에 알아야 할 필요가 없다.

2.5 Base/Delta CRL

Delta CRL 역시 CRL의 크기 증가 문제를 줄이기 위한 대안이나 CRL 분배점과 다른 점은 인증서 일련번호나 인증서폐기사유에 따라 CRL을 나누는 것이 아니라 CRL의 일정 크기에 따라 Base CRL과 그 나머지가 되는 Delta CRL로 나눈다는 것이다. 당사자들은 최근 CRL 갱신시 Delta CRL만을 다운로드 받음으로써 다운로드의 부하를 감소시키는 방식이다. CRL 확인 시에는 기존의 Base CRL을 반드시 함께 사용해야만 한다.

2.6 Over-issued CRL

일반적인 CRL 메커니즘의 경우 주기적으로 발행되는 다음 갱신주기(next update) 시간에 CRL 발행기관은 급작스러운 자원 사용에 따른 통신과부하 상태에 이르게 된다. 이러한 문제를 해결하기 위하여 CRL 발행기관은 주기적 발행뿐만 아니라 비주기적(실시간) CRL 발행을 통하여 동일 시간 내에 여러 개의 유효한 CRL을 사용 가능하게 한다. 이를 통하여 해당 CRL 발행기관은 갑작스런 통신 과부하 문제로부터 벗어날 수 있다.

2.7 Indirect CRL

간접 CRL은 인증기관이 아닌 CRL 전문 발행기관이 다수의 인증기관을 대행하여 CRL을 발행하는 메커니즘으로써 이를 통하여 신뢰 당사자는 여러 개의 CRL을 관리하는 어려움으로부터 벗어날 수 있게 된다.

2.8 Dynamic CRL Distribution Point

동적 CRL 분배점은 기존 CRL 분배점이 갖고 있는 초기 분배 간격 설정 후 변경할 수 없는 분배 간격의 문제를 동적 방법으로 해결해 주는 방식이다. 이를 통하여 CRL 발행자는 운영 중에도 인증서 발행 추이에 따라 동적으로 분배 간격을 조정할 수 있다.

2.9 Online Certificate Status Protocol

신뢰 당사자가 인증서의 상태 검증을 원하는 경우 해당 인증서의 일련번호를 OCSP 서버로 전송하면 OCSP 서버는 인증서 상태 확인 후 전자서명된 상태 결과를 신뢰 당사자에게 되돌린다. 그러므로 신뢰 당사자는 CRL의 시간격차 문제없이 인증서 상태 검증을 수행할 수 있다. 그러나 OCSP는 서버가 해당 결과에 전자서명을 수행하는 방식이기 때문에 OCSP 서버와 수신자 모두에게 전자서명 생성 및 검증에 따른 과부하를 발생시키게 된다.

2.10 Simplified Certificate Validation Protocol

SCVP는 OCSP의 기능 외에도 추가적으로 인증서 경로 검증에 대한 기능도 신뢰 당사자에게 제공한다. 그러므로, 신뢰 당사자는 SCVP를 이용하여 자신이 수행해야 할 인증서 상태 및 경로검증의 부하를 모두 줄일 수 있게 된다. 그러나, SCVP 역시 OCSP와 동일한 문제점을 갖게 된다. 옵션사항으로서 전자서명이 없는 결과 메시지 전송이 가능하도록 정의되어 있기는 하지만 이것은 안전성을 보장할 수 없는 트랜잭션이기 때문에 실제 사용하기 어려운 옵션이 된다.

3. 특징 분석

[표 2]에서는 지금까지 살펴본 인증서 폐기 메커니즘을 요약 정리해 보았다.

[표 2] 인증서 폐기 메커니즘

메커니즘	특 징
Over-issued CRL	• 갱신주기에 집중적인 자원 사용으로 인한 통신과부하 상태에 빠지는 문제를 해결 • 비주기적인 CRL 발행을 추가하여 동일 시간 내에 여러 개의 유효한 CRL을 사용
CRL DP	• CRL의 크기를 줄이기 위한 방법 • 폐기된 인증서의 일련번호 등을 기준으로 다수의 CRL을 생성/분산하여 공개 저장소에 게시
Delta CRL	• CRL 크기 증가 문제를 해결하기 위한 방식
Indirect CRL	• CRL 관리를 위한 인증기관의 부담을 줄이기 위해서 제안된 방식 • CRL 전문 발행기관이 다수의 인증기관을 대행하여 CRL 발행
Dynamic CRL DP	• 분배를 위한 초기 기준과 간격을 설정 후 서비스 운영 과정에서 인증서 발행 및 폐기의 추이에 따라 동적으로 분배 간격을 조정
OCSP	• 주기적 갱신에 의한 시간격차 문제로 발행하는 문제를 해결하기 위한 방식 • OCSP 서버는 검증 대행에 요청에 대한 응답으로 인증서의 상태를 확인한 후 그 결과를 전자서명하여 사용자에게 전송
SCVP	• OCSP의 기능 이외에도 추가적으로 인증서 경로 검증 기능 제공

대용량 인증 서비스 환경으로 변화함에 따라 폐기 인증서의 증가와 더불어 CRL의 크기가 증가한다. 또한 모든 인증서 검증 사용자가 수신한 인증서 검증을 위해 모든 인증서 폐기 정보를 획득하는 것은 비효율적이며, 실 시간적 인증서 폐기 정보 획득의 필요성이 증대된다.

전통적인 CRL방식은 인증서를 검증하고자 할 때마다 인증서 폐기 목록 전체를 다운받아야 하고 인증서 폐기목록의 크기가 커질수록 다운받아야 하는 목록의 크기가 커짐에 따라 다운받는 시간과 통신량의 증가로 이어진다는 단점을 가지고 있다. 이런한 단점을 보완하기위해 인증서 및 CRL의 확장 그리고 새로운 형태의 메커니즘들이 제안되고 있다.

4. 결론

본 논문에서는 IETF RFC 표준안을 근거로 하여 다양한 인증서 폐기 메커니즘에 대하여 살펴보았다.

국내에 이미 활성화된 PKI 서비스의 종류는 상당히 다양하게 나타난다. 이렇게 활용범위가 넓어지면서 PKI 토폴로지는 단순 계층구조에서 메시(Mesh)구조 즉, 네트워크형 PKI 구조로 변화하게 되고 상호인증 방법과 구현방식이 다양하게 발전하게 된다. 이런 PKI를 기반으로 하는 인증서 및 인증서 폐기 목록 메커니즘 역시 끊임없이 변화한다.

앞에서도 살펴보았듯이 어떤 기술은 어떤 환경에 매우 적합하지만, 다른 환경에서는 적합하지 않다. 따라서, PKI 업체는 주어진 PKI 영역에 대하여 가장 좋은 폐기 전략을 제공할 수 있어야 한다.

참고문헌

[1] R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 3280, April 2002

[2] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999

[3] D. Pinkas, R. Housley, "Delegated Path Validation and Delegated Path Discovery Protocol Requirements", RFC 3379, September 2002

[4] C. Adams, S. Lloyd , "Understanding PKI : Concepts, Standards, and Deployment Consid

erations ", Addison-Wesley, 2002
[5] 염흥열, "PKIX 표준화 동향", 정보보호기술 표준 워크숍(ISSW), 2002.12.3
[6] 윤이중, 한재우, 한대완, 류재철, "타원곡선 암호를 이용한 효율적인 인증서 폐지 메커니즘", 정보보호학회지, 2001
[7] 곽진, 이승우, 조석향, 원동호, "온라인 인증서 상태 검증 프로토콜(OCSP)의 최근 연구 동향에 관한 분석", 정보보호학회지, 2002
[8] 이용준, 정재동, 오해석, "검증자목록을 이용한 실시간 인증서 폐지 정보 전송의 설계", 정보보호학회지, 2003
[9] 최영철, 박상준, 원동호, "클라이언트-서버환경에 적합한 효율적인 인증서상태 및 경로검증 시스템", 정보보호학회지, 2003
[10] A. Malpani, R. Housley, T. Freeman, "Simple Certificate Validation Protocol (SCVP)", IETF Draft, draft-ietf-pkix-scvp-14.txt, 2004

황 원 섭

2004년 ~ 현재 안동과학대학 사이버테러대응학과 재학

김 자 영

2004년 ~ 현재 안동과학대학 사이버테러대응학과 재학

정 수 민

2004년 ~ 현재 안동과학대학 사이버테러대응학과 재학

윤 동 식

1992년 관동대학교 전자계산학과(공학사)
1994년 관동대학교 컴퓨터공학과(공학석사)
2000년 관동대학교 컴퓨터공학부(공학박사)
1999년 ~ 현재 안동과학대학 사이버테러대응학과 교수