情報保護學會論文誌
第12券 第4號, 2002. 8

델타 CRL 운영 기술 개발*

김 락 현**, 엄 희 정***, 염 흥 열**

Development on the Operating Technique for Delta CRL

Rack-Hyun Kim**, Hee-Jung Um***, Heung-Youl Youm**

요 약

본 논문은 현재 국내·외에서 개발되었고 개발되고 있으며, 이미 표준화 단계를 앞두고 있는 인증서 발급 시스템 중에 인증서가 폐지되었을 경우에, 발급하는 인증서 폐지 목록(CRL)을 발급하는 시스템의 부하를 줄이고, 발급되는 CRL의 크기를 감소시키며, 또한 전체 CRL의 발급 시간을 늘일 수 있는 Delta-CRL 발급 시스템의 개발 및 방안 연구를 목적으로 한다. 이를 이용하여 유·무선 통신상에서의 인증서 발급의 단점을 해소하고, 인증서를 보관하고 있는 인증서 보관소에 대한 문제를 해소할 수 있다.

ABSTRACT

The purpose of this paper is to present both the specification of delta-CRL and the polices for delta CRL in order to solve the problem involved in issuing and maintaining the certificate revocation lists for the mobile communication network. If the user request to revoke the certificate issued by certification authority, the certificate should be revoked and listed up in the certificate revocation list. In general, the certificate revocation list is issued regularly. Therefore PKI application should download the CRL and prove the validity of CRL. The traffic size of the exchanged traffic should be reduced for the mobile communication environment. The result if this paper can be used for the mobile communication various environments to reduce the size of CRL.

Keyword : *CRL/CARL, Full-CRL/CARL, Base-CRL/CARL, Delta-CRL/CARL, Indirect-CRL/CARL*

Ⅰ. 서 론

인터넷과 무선 통신을 이용한 전자 상거래가 급격히 확장됨에 따라 인터넷과 무선 통신의 정보보호의 근간이 되는 인증 기반 기술에 대한 연구의 중요성이 증가하고 있다. 따라서 국내의 인증 기반 기술에 대한 전반적인 동향을 분석하고, 이를 기반으로 인증서 관리 분야 중 중심이 되는 인증서 폐지 목록(CRL) 관련 분야의 연구는 인터넷 전자 상거래 및 전자 정부 구성을 위한 국가 경쟁력 강화를 위해 꼭 필요한 연구이다.

본 논문의 목적은 인증서 발급 시스템 중에서 인증서가 폐지되었을 경우에 발급하는 인증서 폐지 목록(Certificate Revocation List : CRL)을 발급하는 시스템의 부하를 줄이고, 발급되는 CRL의 크기를 감소시키며, 또한 전체 CRL의 발급 시간을 늘일 수 있는 Delta-CRL 발급 시스템의 개발 및 방안 연구를 목적으로 한다.

* 본 연구는 한국정보보호진흥원 외부수탁과제(전자서명 인증연구 01-02)로 수행하였습니다.
** 순천향대학교 공과대학 정보보호학과(rhkim70@orgio.net, hyyoum@sch.ac.kr)
*** KSIGN PKI개발팀(crow@ksign.com)

1.1 필요성

주체가 인증서를 발행 받은 후, 인증서를 발행 받은 주체의 이름이 변경되거나, 주체가 인증서를 발행했던 조직에서 퇴직하거나 변동이 있거나, 인증서의 공개키에 대응되는 개인키가 누설되거나 도난 당했을 경우에 주체에게 발행된 인증서를 폐지하게 된다. 이때 폐지된 인증서는 CRL 형태로 공개적으로 관리 분배된다. 폐지된 인증서는 CRL에 그 내용을 목록화하여 발급함으로써 해당 인증서가 불법적으로 사용되거나 도용되는 것을 방지 할 수 있다. 그러나 인증서 발행의 수적 증가로 인해 폐지된 인증서 또한 기하급수적으로 증가하게 되고, 이는 분산된 통신상에서 트래픽의 증가와 CRL 데이터베이스의 저장 공간을 증가시키는 문제를 낳고 있다.[1]

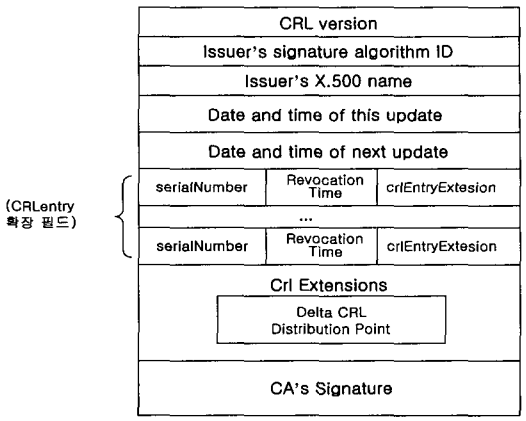
Delta-CRL은 Full-CRL이 발행된 이후로 발행한 인증서 상태가 변경된 인증서들의 목록만을 포함하며, 이로 인해 Full-CRL에 비해 상대적으로 크기가 작은 Delta-CRL은 데이터 저장 장소 크기 감소와 데이터 전송시 소요되는 전송 부하량이 줄어든다.

제안된 시스템은 Delta-CRL과 관련된 여러 문제를 해결하는 방법을 제시하고 있다. Delta-CRL을 폐지된 인증서의 Scope 별로 구분해 발행함으로써 CRL 데이터베이스의 저장 용량을 줄이는 방법을 제안한다. Scope 별로 발행함으로써 장점은 디렉터리 구조나 데이터 베이스상에서 CRL을 검색하여 조회하는 경우에 시간의 손실을 줄일 수 있다는 것이다.

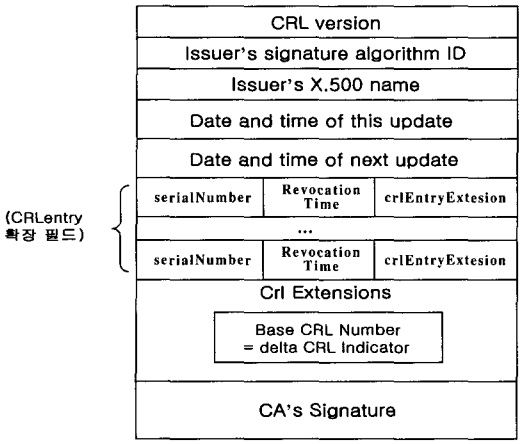
본 논문에서는 Delta-CRL에서 필요한 확장자들에 관한 내용과 기존의 Delta-CRL을 발급하는 세 가지 방법에 대하여 분석하고, 현재까지 체계화되지 않았던 인증기관의 Delta-CRL발급 정책을 제시한다. 그리고 Scope 별 Delta-CRL 발행 구조 및 시스템 구조를 정의하고 그에 따른 운영 방안을 제안한다.

II. Base-CRL 및 Delta-CRL의 확장

본 장에서는 Base-CRL 및 Delta-CRL에 관련된 확장자를 분석한다. Delta-CRL을 발행할 경우, 그에 따른 Base-CRL과 인증서가 같을 경우에는 Delta-CRL Indicator에 의해 Delta-CRL의 위치, 즉 Delta-CRL의 URL을 파악하여 발급을 받는다. [그림 1]은 Base-CRL의 필드들을 나타낸 것이다.



[그림 1] Base CRL의 구조



[그림 2] Delta CRL의 구조

그림에서 보는 바와 같이 Base-CRL은 CRL 확장 필드 내에 Delta-CRL Distribution Point라는 서브 필드를 포함하고 있어야 한다. [그림 2]에서 알 수 있듯이 각각의 Delta-CRL은 Delta-CRL Indicator 역할을 하는 Base-CRL Number 필드를 포함하고 있다.

2.1 CRL Distribution Points

CRL 분배 점은 어떻게 CRL 정보를 획득할 것인지를 확인하는 확장자를 지적한다. 이 확장자는 non-critical 이다. 그러나 PKIX 프로파일에서는 인증기관들과 응용이 이 확장자를 지원할 것을 권고한다.

cRLDistributionPoints 확장자는 Distribution-Point의 SEQUENCE OF 타입이다. Distribution-Point는 URL 형태의 분배점을 포함하는 distribution-Point, 폐지 범위를 나타내는 reasons, 그리고

cRLIssuer 등의 3개의 서브필드들로 다시 구성되는데, 각 서브필드는 선택적이다. 그러나, 이 필드들은 선택적이지만, DistributionPoint는 오직 reasons 필드만으로 구성되어서는 안되고, distributionPoint 또는 cRLIssuer 중 하나가 반드시 존재해야 하며, 인증서 발행자가 CRL 발행자가 아니면 cRLIssuer 필드는 반드시 존재해야 하고 CRL 발행자의 이름을 포함해야 한다. 만약 인증서 발행자가 CRL 발행자이라면, cRLIssuer 필드는 생략되어야 하고, distributionPoint 필드는 존재해야 한다. 만약 distributionPoint 필드가 생략된다면, cRLIssuer는 반드시 존재해야 하고, CRL이 위치하는 X.500 또는 LDAP 디렉토리 엔트리에 대응되는 이름을 포함해야 한다.[2,3]

2.2 Delta-CRL Indicator

Delta-CRL Indicator는 현재 CRL이 Delta-CRL임을 확인하는 critical 확장자이다. Delta-CRL은 폐지된 모든 인증서 폐지 목록을 가지고 있는 것이 아니라, 이전에 발행된 기반 CRL 이후에 상태가 변한 인증서 목록만을 포함한다. Delta-CRL의 사용은 어떤 환경에서 상당히 망 부하와 처리 시간을 줄일 수 있는 특징이 있다. Delta-CRL은 일반적으로 Full-CRL보다 크기가 작다. 그러므로 Delta-CRL을 획득하는 것이 대응되는 Full-CRL을 획득하는 방법보다 망 대역폭을 감소시킬 수 있다.[4,5] Delta-CRL Indicator 확장자는 BaseCRLNumber의 일련번호를 포함한다. 이 CRL 번호는 Delta-CRL을 생성하기 위한 시작점으로 사용된 주어진 범위에 대한 Base-CRL을 확인한다. CRL issuer는 참고된 Base-CRL을 Full-CRL로 공표한다. Delta-CRL은 동일한 범위에 대한 폐지 상태의 모든 갱신 정보를 포함한다. Delta-CRL과 참조된 Base-CRL이 결합된 Full-CRL은 Delta-CRL이 공표된 시점에서 주어진 범위에 대한 Base-CRL과 등가이다.[4]

Delta-CRL은 Delta-CRL에 대응되는 Base-CRL과 동일한 범위를 갖는다. 즉, Delta-CRL의 범위는 기반으로 참조하는 완전한 CRL의 범위와 등가가 됨을 의미한다. 이 참조된 Base-CRL과 Delta-CRL은 distribution point 확장자를 제거해야 하거나 동일한 issuing distribution point 확장자를 포함해야 한다.[9]

2.3 issuing distribution point

issuing distribution point는 특정 CRL을 위한 CRL 분배점과 범위를 확인하기 위한 critical 확장자이다. 그리고 issuing distribution point는 이 CRL이 최종 개체만을 위한 폐지인지, 인증기관만을 위한 폐지인지, 또는 제한된 사유들의 집합을 갖는 폐지인지를 나타낸다. 이 확장자는 critical이지만 호환 실현은 이 확장자를 지원하도록 요구되지 않는다.[8]

분배점과 연관되는 사유 부호들은 onlySomeReasons 서브 필드에 규정되어야 한다. 만약 onlySomeReasons가 나타나지 않는다면, 이 분배 점은 모든 사유 부호에 대한 폐지를 포함해야 한다. 인증기관은 손상이나 정기적인 폐지에 바탕을 둔 CRL을 다시 세부적으로 분할하기 위하여 CRL 분배 점들을 사용해야 한다. 이러한 경우, 사유 부호 keyCompromise(1)(개인키 누설), cACompromise(2)(인증기관 개인키 손상), 그리고 aACompromise(8)(속성 인증서 폐지) 인 폐지는 하나의 분배 점에서 나타나고, 다른 폐지 사유들을 갖는 폐지는 또 다른 분배점에서 나타낸다.[9]

III. CARL/CRL과 Delta-CARL/CRL 발급 정책

본 장에서는 인증기관에 적용 가능한 CRL과 Delta-CRL 관련된 인증서 정책을 제안한다. 이를 위하여 두 가지 인증서 폐지 목록의 유형을 정의한다. 하나는 root CA가 인증기관에게 발행한 인증서 중에서 폐지된 인증서 목록을 나열한 것으로, root CA에 의하여 발행되는 인증기관을 위한 인증기관 폐지 목록(CARL:Certification Authority Revocation List)이다. 다른 하나는 인증기관이 고객에게 발행된 인증서들 중에서 폐지된 인증서 목록으로써, 인증기관에 의하여 발행되는 인증서 폐지 목록(CRL : Certification Revocation List)이다.

root CA는 CARL를 발행해야 하고, 인증기관은 CRL을 발행해야 한다.

인증기관은 선택적으로 Delta-CRL 발행을 지원할 수 있다. 인증기관은 자신의 인증서 정책에 따라 선택적으로 Delta-CRL을 발행할 수 있다.

CARL과 CRLs 내에 존재하는 내용은 포함되기 전에 철저히 검증되어야 한다. 검증은 부적절하게 생성된 CARL 또는 CRL에서 오류를 찾기 위한 소

프트웨어를 이용하거나 다른 신뢰적인 수단을 이용하여 수행되어야 한다.

3.1 인증기관 CARL 또는 Delta-CRL 발행 주기

Root CA는 인증기관이 개인키 손상 사유로 인증서 폐지를 요청하면, 인증기관 인증서 폐지 요구의 정당성을 확인하고, 요구를 수신시간부터 6시간 이내에 관련 폐지 명단을 CARL에 공개해야 한다.

Root CA는 정기적으로 발행되는 CARL과 개인키 손상으로 발행되는 CARL을 유지해야 한다. Root CA는 인증기관 CRL 정보를 시기적절하게 당사자에게 제공하기 위하여 CRL을 폐지 정보의 변경이 없을 때라도 주기적으로 발행해야 한다. Root CA는 인증서 상태 정보를 [표 1]에서 규정된 발행 빈도보다 더 자주 발행해야 한다.

표 1 CARL 발행 주기

	정기적인 발행	개인키 손상으로 인한 발행
CARL	적어도 하루 한번	6시간

Root CA는 정기적인 발행의 경우, 하루에 한번씩 CARL을 발행해야 한다. 또한 Root CA는 인증기관의 개인키의 손상으로 인한 경우, 인증기관에 의한 폐지 요구를 수신한 후 6시간 이내에 개인키 손상 범위를 갖는 CARL을 발행해야 한다. Root CA는 개인키 손상 CARL 요구사항을 만족하기 위하여 6시간마다 개인키 손상의 범위를 갖는 CARL을 발행하거나, 하루에 한번 CARL을 발행하고 6시간마다 Delta-CARL을 발행할 수 있다. 따라서 Root CA는 두 범위에 대한 Delta-CRL을 선택적으로 발행할 수 있음을 의미한다.

인증기관은 자신의 인증서 정책으로 CRL 발행 주기와 CRL 범위(scope)를 결정해야 한다.

그리고, CRL/CARL 은 계획된 다음 갱신 일시보다 빨리 발행되어야 한다. 신뢰 당사자는 오프라인으로 인증서 상태 정보를 자국에 저장할 수 있다. 이전 인증서 폐지 목록은 최근 인증서 폐지 목록으로 대체되어야 한다.

3.2 Delta-CARL/CRL 범위

Root CA는 Delta-CARL을 선택적으로 지원한다. Delta-CARL 발행주기는 6시간 단위로 한다. Delta-CARL의 범위(scope)는 전체 폐지 사유와 개인키 손상으로 한정한다. 따라서 CRAL 역시 두 가지 범위로 발행한다.

인증기관의 Delta-CRL 발행 정책은 인증기관의 자율로 결정한다.

Ⅳ. Delta-CRL 운영방안

4.1 Delta-CRL 발급 시스템의 개요

제안된 발급 시스템의 구조는 [그림 3]과 같다.

4.1.1 Delta-CRL 발급 시스템 구조

- 사용자가 인증기관으로부터 인증서를 발급 받음.
- 사용자가 인증서의 폐지를 해당 인증기관에 인가된 방법으로 요청하면 인증기관은 CRL에 해당 인증서를 포함함.
- 인증서 발급 및 폐지 방법은 PKIX의 CMP 프로토콜을 이용함.

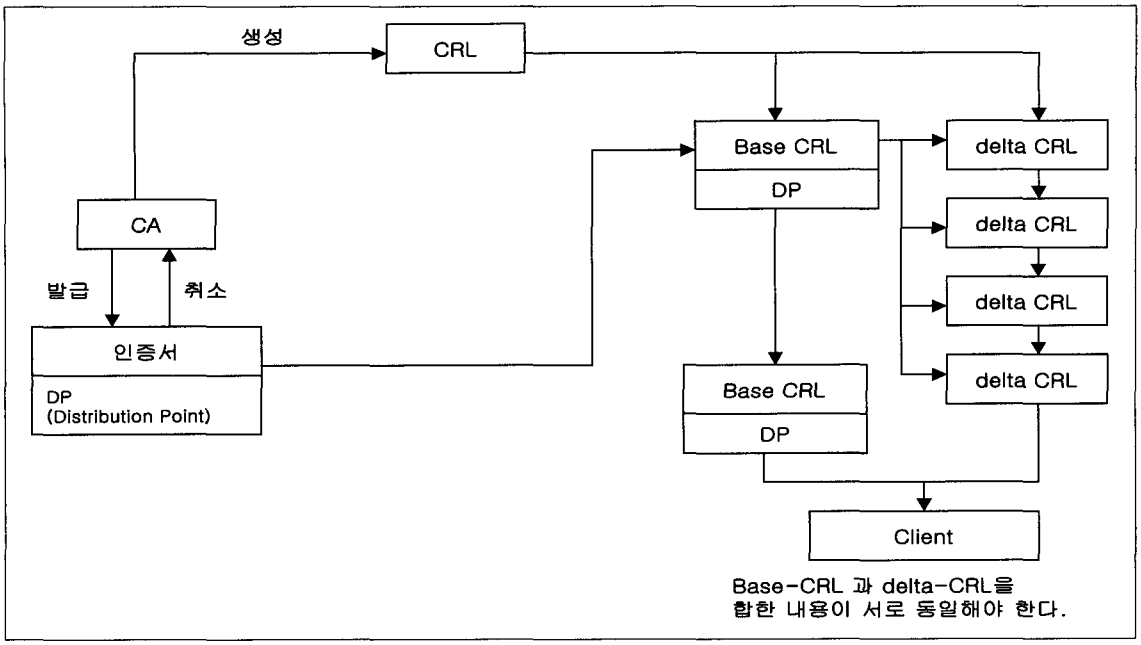
4.1.2 Base-CRL과 Delta-CRL 생성 방안

- Base-CRL과 Delta-CRL 구조 : CRL 구조가 서로 다르며, 인증서내에서는 각각의 DP(Distribution Point)에 의해 구분된다.
- Client는 Full-CRL을 얻기 위하여 Base-CRL과 Delta-CRL을 결합함.
- FULL-CRL과 Base-CRL 그리고 Delta-CRL은 디렉토리 서비스 또는 웹을 이용하여 공개함.

Full-CRL을 구하기 위하여 Delta-CRL이 Base-CRL과 결합(Combine)될 때, Base-CRL은 Delta-CRL과 동일한 CRL number 번호 체계를 유지해야 한다. 또한, Base-CRL은 지금 발행 일시인 thisUpdate와 다음 발행 예상 일시인 nextUpdate 필드를 갖는다. 거기에 더하여 Base-CRL은 issuing distribution point를 이용하여 특정 범위로 발행된 특정 범위의 Delta-CRL을 확인할 수 있다.[7]

4.1.3 Base-CRL과 Delta-CRL의 결합을 위한 4가지 조건

- Base-CRL과 Delta-CRL이 동일한 발행자를 갖는다.
- Base-CRL과 Delta-CRL은 동일한 범위를 갖는데, 두 CRL 들이 다음의 조건을 만족해야만 한다.



〔그림 3〕 delta CRL 발급 시스템

- issuingDistributionPoint 확장자가 Base-CRL과 Delta-CRL에서 공히 생략되어 있다.
- issuingDistributionPoint 확장자가 Base-CRL과 Delta-CRL에서 공히 존재하고, 확장자들에서 필드들의 각각의 값들이 동일하다.

- Base-CRL의 CRL 번호가 Delta-CRL에서 정의된 BaseCRLNumber 보다 같거나 커야 한다.
- Base-CRL의 CRL 번호가 Delta-CRL 번호보다 작아야 한다. 이는 Delta-CRL이 번호 순서에서 Full-CRL을 따르는 것을 의미한다.

위의 Delta-CRL 발급시스템을 좀 더 자세히 살펴보면 〔그림 4〕와 같다.

2.1절에서 설명했듯이 DistributionPoint 확장자를 살펴보면 distributionPoint, reasons, 그리고 cRLIssuer의 세 개의 필드로 구성되어 있음을 알 수 있다. 그 중에서 reasons 필드는 다음과 같은 폐지 사유들을 포함하고 있다.

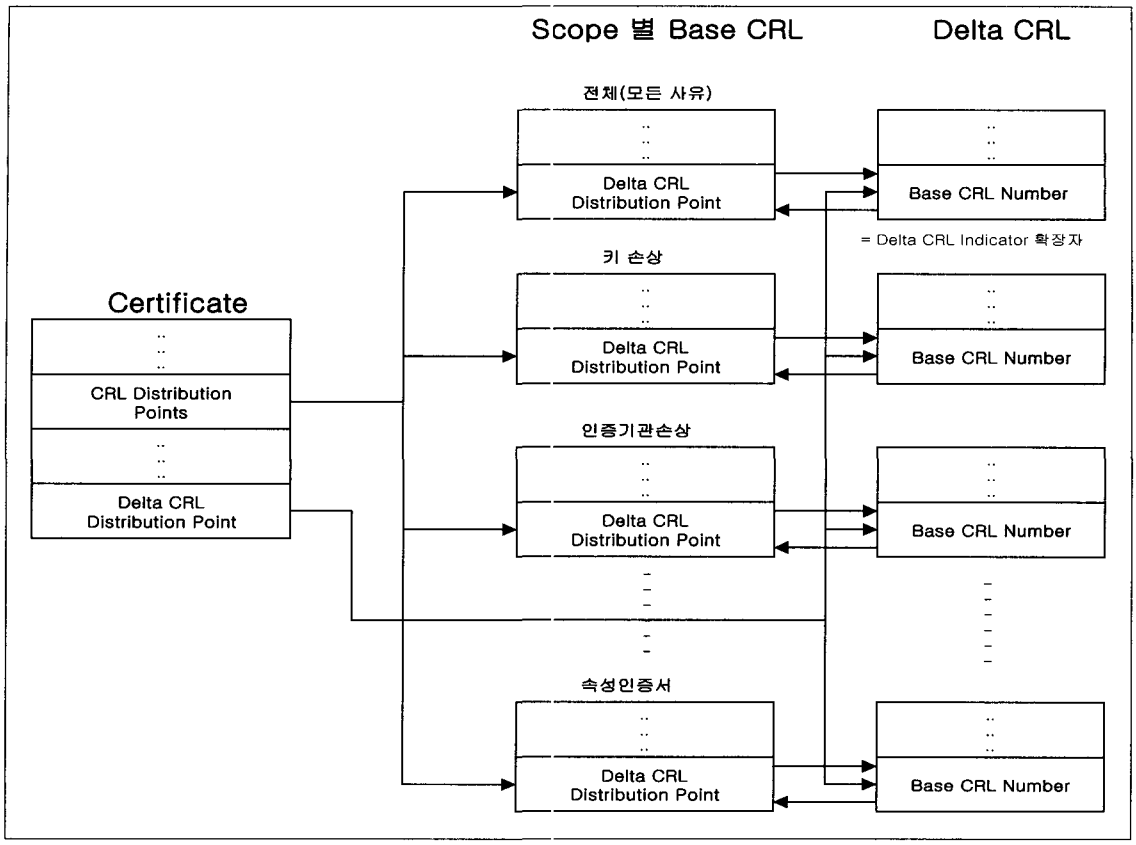
ReasonFlags ::= BIT STRING {
unused (0), //사용 않함
keyCompromise (1), //키 손상
cACompromise (2), //인증기관 손상
affiliationChanged (3), //직장 변경
superseded (4), //지위 박탈
cessationOfOperation (5), //동작 중단
certificateHold (6), //인증서 정지
privilegeWithdrawn (7), //특권 폐지
aACompromise (8) } //속성인증서손상

만약 DistributionPoint가 reasons 필드를 생략하면, CRL은 모든 이유들을 갖는 폐지 정보를 포함한다.

Delta-CRL 발급 시스템의 운영 방침은 기본적으로 다음과 같은 원칙을 따른다.

4.1.4 Delta-CRL 발급 시스템 운영 원칙

- CRL distribution point 확장자의 reasons 필드를 이용 Scope 별 Full CRL을 발행.
- 인증서에 Base-CRL을 지적하는 CRL Distribution Point와 Delta-CRL 지적하는 Delta-CRL Distribution Point 확장자를 이용하여 위치 확인.
- 각각의 Distribution Point는 CRL이 저장되어 있는 디렉토리 위치 또는 파일을 얻을 수 있는 URL 형태임.
- Delta-CRL을 이용하는 인증서는 확장 영역내에 Delta-CRL DP 확장자를 가지고 있음.
- Base-CRL은 독립적인 번호 체계를 유지함.



〔그림 4〕 delta CRL 발급 시스템의 체계

- Delta-CRL은 자신이 참조하는 기반 CRL을 나타내기 위한 Base-CRL Number 확장 필드를 가지고 있음
- Base-CRL과 Delta-CRL의 발급은 다음 장부터 설명되는 방식으로 하되, 발행 간격 등은 인증기관 정책에 의하여 결정됨.

4.2 Delta-CRL 발급시스템의 동작방법

본 절에서는 지금까지 발표된 대표적인 세 가지 Delta-CRL 동작 방법을 분석한다. 첫 번째 방법은 Full-CRL은 3시간마다 한번씩 발행되고 Delta-CRL은 1시간마다 한번씩 발행되어 3시간마다 Delta-CRL의 Base-CRL 번호가 바뀌는 전형적인 방법이다. 이 방법은 기본적인 시스템 구조를 제안한 것으로 실제 시스템에 연동하기 위해서는 데이터 량이 많은 Delta-CRL을 생성하고, 고객이 Delta-CRL을 조회하도록 환경을 제공해 주는 전파지연 시간이 고려되어야 하므로 다음 두가지 방법으로 보완한다. 두 번째 방법은 Full-CRL의 이력을 3시간에서 6시간으로 늘리는 슬라이딩 윈도우 방식을 채택한 방법, 그리고 세 번째 방법은 슬라이딩 윈도우 방식을 사용한 복사/전달 지연 시간을 고려하여 발행하는 방법이다.

아래의 세 가지 방법을 설명 효율적으로 설명하기 위하여 폐지 사유에 대한 용어를 다음과 같이 정의하였다.

```
· 폐지 사유
  a : 직장변경
  k : 키 손상
  h : 인증서 효력정지
  r : 효력 정지된 인증서 폐지 목록을 CRL로부터
      제거함(복구)

폐지 사유와 부호는 인증기관 정책에 따라 변경될 수
있음.
```

4.2.1 전형적인 Delta-CRL 발급 방법

Full-CRL은 3시간마다 한번씩 발행하고 Delta-CRL은 시간마다 한번씩 발행한다. 발행의 편이를 위하여, 발행자는 첫 번째 Full-CRL을 발행함과 동시에 Delta-CRL을 발행하기 시작하고 Delta-CRL은 항상 이전에 발행된 Full-CRL을 기반으로 사용할 수 있다. Delta-CRL 번호 4로부터 시작하여, Full-CRL과 동시에 발행되는 Delta-CRL은 Base-CRL로 이전에 발행되었던 Full-CRL을 사용한다. 그러나 Delta-CRL들은 3시간 이상의 이력을 제공하지 않는다.

4.2.1.1 [표 2]에 발행된 Delta-CRL 관련 사건 일지

- 인증서 14는 첫 CRL이 발행된 12:00 이전에 키 손상으로 폐지되었다.
- 인증서 124는 12:00에서 13:00 사이에서 키 손상으로 폐지되었다.
- 인증서 39는 14:00 에서 15:00 사이에 효력이

[표 2] 전형적인 Delta-CRL 발급 방법

Current time	Revoked certificates	Full CRL	Delta-CRL
12:00	{14k}	cRLNumber=1 thisUpdate=12:00 nextUpdate=15:00 CertificateList={14k}	cRLNumber=1 thisUpdate=12:00 nextUpdate=13:00 BaseCRLNumber=1 CertificateList={}
13:00	{14k, 124k}		cRLNumber=2 thisUpdate=13:00 nextUpdate=14:00 BaseCRLNumber=1 CertificateList={124k}
14:00	{14k, 124k}		cRLNumber=3 thisUpdate=14:00 nextUpdate=15:00 BaseCRLNumber=1 CertificateList={124k}
15:00	{14k, 124k, 39h}	cRLNumber=4 thisUpdate=15:00 nextUpdate=18:00 CertificateList={14k, 124k, 39h}	cRLNumber=4 thisUpdate=15:00 nextUpdate=16:00 BaseCRLNumber=1 CertificateList={124k, 39h}
16:00	{14k, 124k, 39h, 67a}		cRLNumber=5 thisUpdate=16:00 nextUpdate=17:00 BaseCRLNumber=4 CertificateList={39h, 67a}
17:00	{14k, 124k, 67a}		cRLNumber=6 thisUpdate=17:00 nextUpdate=18:00 BaseCRLNumber=4 CertificateList={39r, 67a}
18:00	{14k, 124k, 67a}	cRLNumber=7 thisUpdate=18:00 nextUpdate=21:00 CertificateList={14k, 124k, 67a}	cRLNumber=7 thisUpdate=18:00 nextUpdate=19:00 BaseCRLNumber=4 CertificateList={39r, 67a}
19:00	{14k, 124k, 67k}		cRLNumber=8 thisUpdate=19:00 nextUpdate=20:00 BaseCRLNumber=7 CertificateList={67k}

정지되었다. 그리고 이 정지는 16:00와 17:00 사이에 폐지되었다.

- 인증서 67은 15:00에서 16:00사이에 직장 변경으로 폐지되었다. 인증서 67의 폐지 사유는 18:00에서 19:00 사이에 키 손상으로 변경되었다.

4.2.2 슬라이딩 윈도우 방식을 이용한 Delta-CRL 발급방법

아래의 예는 Delta-CRL을 발행하는 "슬라이딩 윈도우" 방법을 나타낸다.

이 방법에서, Full-CRL들은 3시간마다 한번씩 발행되고, 델타는 매 한 시간마다 한번씩 발행된다. 발행자는 full-CRL과 동시에 Delta-CRL 발행을 개시한다고 가정한다. cRLNumber 7부터 시작하여, full CRL과 동시에 발행된 Delta-CRL은 Base-CRL로서 이전에 발행된 full CRL을 이용하지 않고 대신에 이전 CRL을 이용한다. 이 Delta-CRL들은 6시간 이상의 이력을 제공하지 않는다.[10]

〔표 3〕 슬라이딩 윈도우 방식을 이용한 Delta-CRL 발급방법

current time	Revoked certificates	Full CRL	Delta-CRL
12:00	{14k}	cRLNumber=1 thisUpdate=12:00 nextUpdate=15:00 CertificateList={14k}	cRLNumber=1 thisUpdate=12:00 nextUpdate=13:00 BaseCRLNumber=1 CertificateList={}
13:00	{14k, 124k}		cRLNumber=2 thisUpdate=13:00 nextUpdate=14:00 BaseCRLNumber=1 CertificateList={124k}
14:00	{14k, 124k}		cRLNumber=3 thisUpdate=14:00 nextUpdate=15:00 BaseCRLNumber=1 CertificateList={124k}
15:00	{14k, 124k, 39h}	cRLNumber=4 thisUpdate=15:00 nextUpdate=18:00 CertificateList={14k, 124k, 39h}	cRLNumber=4 thisUpdate=15:00 nextUpdate=16:00 BaseCRLNumber=1 CertificateList={124k, 39h}
16:00	{14k, 124k, 39h, 67a}		cRLNumber=5 thisUpdate=16:00 nextUpdate=17:00 BaseCRLNumber=1 CertificateList={124k, 39h, 67a}
17:00	{14k, 124k, 67a}		cRLNumber=6 thisUpdate=17:00 nextUpdate=18:00 BaseCRLNumber=1 CertificateList={124k, 39r, 67a}
18:00	{14k, 124k, 67a}	cRLNumber=7 thisUpdate=18:00 nextUpdate=21:00 CertificateList={14k, 124k, 67a}	cRLNumber=7 thisUpdate=18:00 nextUpdate=19:00 BaseCRLNumber=1 CertificateList={124k, 39r, 67a}
19:00	{14k, 124k, 67k}		cRLNumber=8 thisUpdate=19:00 nextUpdate=20:00 BaseCRLNumber=4 CertificateList={39r, 67k}

4.2.2.1 〔표 3〕에 발행된 Delta-CRL 관련 사건 일지
- 인증서 14는 첫 CRL이 발행된 12:00 이전에 키 손상으로 폐지되었다.
- 인증서 124는 12:00 13:00 사이에서 키 손상으로 폐지되었다.
- 인증서 39는 14:00 에서 15:00 사이에 효력이 정지되었다. 그리고 이 정지는 16:00와 17:00 사이에 취소되었다.
- 인증서 67은 15:00에서 16:00사이에 직장 변경으로 폐지되었다. 인증서 67의 폐지 사유는 18:00 에서 19:00 사이에 키 손상으로 변경되었다.

4.2.3 복사/전달 지연 시간을 고려한 Delta-CRL 발급 방법

이 방법에서, full-CRL과 Delta-CRL은 저장소 시스템 도처에 복사될 것이다. 데이터는 파일의 크기에 따라서 다른 속도로 시스템 도처에 복사될 것이다. CA 관리자는 full-CRL이 3시간 이내에 시스템 전반에 유용하다고 추정한다. Delta-CRL은 15분 이내에 유용하다.(초기 CRL은 작고, Delta-CRL 같이 전파될 것이다.)[10]

이 방법은 Delta-CRL을 발행하는 "슬라이딩 윈도우" 방법을 사용한다. 그러나 전파를 고려하여 thisUpdate와 nextUpdate 시간을 중복되도록 한다. 이 예제에서, full-CRL은 매 3시간마다 한번씩 발행되고, Delta-CRL은 매 45분마다 한번씩 발행된다. 일관성을 위하여 발행자는 full-CRL과 동시에 delta-CRL의 발행을 시작한다. cRLNumber 7로 시작하여, full CRL과 동시에 발행된 Delta-CRL은 기반으로 직전에 발행된 full CRL을 이용하는 대신에 이전 CRL을 이용한다. 이 Delta-CRL은 6시간 이상의 이력은 제공하지 않는다.

4.2.3.1 〔표 4〕에 발행된 Delta-CRL 관련사건 일지
- 인증서 14는 첫 CRL이 발행된 12:00 이전에 키 손상으로 폐지되었다.
- 인증서 124는 12:00 에서 13:00 사이에 키 손상으로 폐지되었다.
- 인증서 39는 14:00 에서 15:00 사이에 효력이 정지되었다. 그리고 이 정지는 16:00와 17:00 사이에 폐지되었다.
- 인증서 67은 15:00에서 16:00사이에 직장 변경으로 폐지되었다. 인증서 67의 폐지 사유는 18:00 에서 19:00 사이에 키 손상으로 변경되었다.

V. 구현 및 실현

5.1 OpenSSL 기반 구조

이 장에서는 이미 앞 단원에서 제안한 Delta-CRL의 정책과 규정을 적용하여 구현한 내용을 설명한다. 구현의 단계는 CRL에 명시된 Delta-CRL의 distribution point의 삽입 단계와 Delta-CRL의 생성, 그리고 Delta-CRL검증 단계로 구성되며, 소스로는 Open-SSL v0.96b를 이용하여 Delta-CRL 루틴을 삽입하였다. 기존의 인증서 발행과 폐지를 관리하기 위한 인증 서버의 역할을 하는 OpenSSL은 소스가 공개 되어 있어 있을 뿐만 아니라, 프로그래머가 소스를 분석하고, 수정, 개발 할 수 있도록 각종 문서를 제공하고 있다. 또한 이미 개발되었고, 개발되고 있는 인증서 관련 제품들의 기반이 되고 있는 소스이다.

OpenSSL 시스템에 적용 가능한 Delta-CRL은 OpenSSL의 특성에 따라 windows 환경, Linux 환경, UNIX 환경 모두에서 동작하며, 이는 OpenSSL 설치의 경우에 소스를 컴파일 하여 운영체제에 상응하도록 설치만 하면 된다. 현재 OpenSSL의 최신 버전은 0.96b 이다.

5.2 CA 구현 및 실현

주체의 인증서를 사유로 인하여 폐지하는 경우 인증기관은 CRL를 발행하고, 이를 공개적으로 관리하고 분배한다. 그러나 현재 통신 시스템에서의 운영을 보면 인증서 검증을 위해 CRL을 수신한다는 것에는 문제점이 발생한다. 첫째로 인증서 폐지 시 발행하는 CRL의 크기는 기하급수적으로 크기가 증가한다. 이때 사용자가 인증서 검증을 위해, CRL을 수신하는 경우 통신 선로상의 트래픽 부하가 발생한다. 또한 CA는 CRL을 보관하기 위한 데이터베이스의 저장 공간의 부족 현상이 발생할 가능성 또한 높다 할 수 있다. 이를 보완하기 위한 방법이 Delta-CRL을 이용한 방법이다. Delta-CRL은 CRL의 분산점을 통해 지적되며, Delta-CRL은 scope 별로, 자신에게 주어진 폐지 인증서만을 관리한다. 상대적으로 CRL 보다 크기를 줄일 수 있다. 또한 Delta-CRL은 Base-CRL 보다 상대적으로 짧은 발행주기를 갖는다.

본 논문에서는 첫 번째로 CA가 자체 서명한 CA

〔표 4〕 복사/전달 지연 시간을 고려한 Delta-CRL 발급방법

Current time	Revoked certificates	Full CRL	Delta-CRL
12:00	{14k}	cRLNumber=1 thisUpdate=12:00 nextUpdate=18:00 CertificateList={14k}	cRLNumber=1 thisUpdate=12:00 nextUpdate=13:00 BaseCRLNumber=1 CertificateList={}
12:45	{14k, 124k}		cRLNumber=2 thisUpdate=12:45 nextUpdate=13:45 BaseCRLNumber=1 CertificateList={124k}
13:30	{14k, 124k}		cRLNumber=3 thisUpdate=13:30 nextUpdate=14:30 BaseCRLNumber=1 CertificateList={124k}
14:15	{14k, 124k}		cRLNumber=4 thisUpdate=14:15 nextUpdate=15:15 BaseCRLNumber=1 CertificateList={124k}
15:00	{14k, 124k, 39h}	cRLNumber=5 thisUpdate=15:00 nextUpdate=21:00 CertificateList={14k, 124k, 339h}	cRLNumber=5 thisUpdate=15:00 nextUpdate=16:00 BaseCRLNumber=1 CertificateList={124k, 39h}
15:45	{14k, 124k, 39h, 667a}		cRLNumber=6 thisUpdate=15:45 nextUpdate=16:45 BaseCRLNumber=1 CertificateList={124k, 39h, 67a}
16:30	{14k, 124k, 67a}		cRLNumber=7 thisUpdate=16:30 nextUpdate=17:30 BaseCRLNumber=1 CertificateList={124k, 39r, 67a}
17:15	{14k, 124k, 67a}		cRLNumber=8 thisUpdate=17:15 nextUpdate=18:15 BaseCRLNumber=1 CertificateList={124k, 339r, 67a}
18:00	{14k, 124k, 67a}	cRLNumber=9 thisUpdate=18:00 nextUpdate=24:00 CertificateList={14k, 124k, 67a}	cRLNumber=9 thisUpdate=18:00 nextUpdate=19:00 BaseCRLNumber=5 CertificateList={124k, 39r, 67a}
18:45	{14k, 124k, 67k}		cRLNumber=10 thisUpdate=18:45 nextUpdate=19:45 BaseCRLNumber=5 CertificateList={39r, 67k}

인증서를 발행하고, 이를 이용하여, 사용자 요청에 의한 사용자 인증서를 발행한다. 현재 논문에서 다루고 있는 시스템의 운영체제는 윈도우즈를 이용한다.(단, OpenSSL v0.96b를 이용하여 구현하였으므로, UNIX, LINUX, MAC 등의 시스템에도 탑재가 가능하다)

5.3 Delta-CRL 운영 시나리오

Delta-CRL의 운영의 대표적인 잇점은 Full-CRL을 이용하는 경우와 비교하여, CRL 저장공간의 문제를 해결하고, 통신 선로에서의 데이터 전송의 부하를 줄일 수 있다는 잇점이 있다.

본 절에서는 Delta-CRL을 적용한 시스템의 시나리오를 살펴본다.

[가정 1]

Full-CRL은 3시간 마다 한번씩 발행하고, Delta-CRL은 한 시간마다 한번씩 발행한다.

[가정 2]

발행자는 첫 번째 Full-CRL을 발행함과 동시에 Delta-CRL을 발행하기 시작한다.

[가정 3]

클라이언트에서 Base-CRL과 Delta-CRL을 이용하여 Full-CRL과 비교 검증한다.

① 주체의 요청에 의하여 인증기관이 인증서를 발행한다.
② 발행된 인증서는 주체의 이름이 변경되거나, 주체가 인증서를 발행했던 조직에서 퇴직 또는 변동이 생길 경우, 인증서의 공개키에 대응되는 개인키가 누설되거나 도난당했을 경우에 인증기관에 의해 폐지된다.
③ 인증기관은 발행주기에 따라, 4장에서 제시한 방법으로 Full-CRL과 Base-CRL, Delta-CRL을 발행한다.
④ 주체가 인증서를 사용할 경우, 인증서의 유효성을 검증하기 위해 Base-CRL과 Delta-CRL을 결합하여 Full-CRL을 검증한 후, 인증서의 유효성을 판단한다.

다음은 클라이언트에서 Base-CRL과 Delta-CRL을 결합하여 Full-CRL을 검증하는 과정이다.

① Base-CRL의 서명 검증
② Delta-CRL의 서명 검증
③ Full-CRL의 조건 검사
  (1) 발급자 동일성 검사
  (2) crl scope 검사
  (3) Delta-CRL의 번호가 Base-CRL보다 작은지 검사
  (4) Delta-CRL의 BaseCRLNumber가 Base-CRL의 crlNumber 보다 작은지 검사
④ Base-CRL 폐지 목록 검증
⑤ Delta-CRL 폐지 목록 검증
⑥ 인증서의 유효성 판단

5.4 Delta-CRL 적용 시스템의 통신 부하량 비교

Delta-CRL 적용 시스템의 최대의 잇점은 통신 선로상의 부하 감소이다. Full-CRL을 고객의 요청에 따라 인증서 검증시 단말기로 다운로드 할 경우, 크기가 큰 Full-CRL을 받아야 하는 통신 선로의 부하 부담이 발생한다. 이의 단점을 보완하기 위해 Delta-CRL을 이용한 인증서 유효성 검사 시, 통신 부하량을 비교 하고자 한다.

다음 [표 5]는 Full-CRL을 이용한 인증서 유효성 검사에서의 통신 부하량과 Delta-CRL을 이용한 인증서 유효성 검사에서의 통신 부하량을 비교한 것이다. 유선 통신로에서 1000개의 인증서를 발급하고, 일정 시간 간격으로 500개의 인증서를 폐지한 후, 단말기에서 Full-CRL과 Delta-CRL을 다운로드하여 각각의 통신 선로의 CRL 전송량 부하를 측정한 것이며, 인증서 발급과 폐지 시스템에 관하여는 언급하지 않는다.

표 5 통신 부하량 비교(단위 : Kbyte)

유효성 검사횟수 / CRL 방식	10회	1000회	1000000회
Full-CRL	709	71,726	70,985,000
Delta-CRL	50.13	6,015.6	899,200

위 표에서 보면, Full-CRL을 직접 이용한 시스템에서는 인증서의 유효성을 검사 할때 마다 Full-CRL을 인증 기관으로부터 수신받아 인증서 유효성을 검증한다. 그러나 Delta-CRL을 적용한 시스템에서는 Base-CRL을 기반으로 Delta-CRL을 이용하기 때문에 Full-CRL을 적용한 시스템보다 현

저히 작은 통신량으로도 인증서 유효성 검증이 가능한 것으로 판단된다. 또한 Full-CRL을 일정한 시간 간격을 두고 생성하지 않고, 크기가 작은 Delta-CRL을 이용함으로써 CRL의 크기를 현저히 감소시킬 수 있다.

Ⅵ. 결 론

인터넷과 무선 통신을 이용한 전자 상거래가 급격히 확장됨에 따라 인터넷과 무선 통신의 정보보호의 근간이 되는 인증 기반 기술에 대한 연구가 중요성이 증가하고 있다. 따라서 국내의 인증 기반 기술에 대한 전반적인 동향을 분석하고 이를 기반으로 인증서 관리의 분야 중 중심이 되는 인증서 폐지 목록(CRL) 관련 분야의 연구는 인터넷 전자 상거래 및 전자 정부 구성을 위한 국가 경쟁력 강화를 위해 꼭 필요한 연구이다.

이에, 본 논문은 현재 국외와 국내에서 개발되었고 개발되고 있으며, 이미 표준화 단계를 앞두고 있는 인증서 발급 시스템 중에 인증서가 폐지되었을 경우에 발급하는 인증서 폐지목록(Certificate Revocation List : CRL)을 발급하는 시스템의 부하를 줄이고, 발급되는 CRL의 크기를 감소시키며, 또한 전체 CRL의 발급 시간을 늘일 수 있는 Delta-CRL 발급 시스템의 개발 및 운영 방안을 제안하였다.

본 논문은 OpenSSLv0.96b를 이용하여 인증기관에서 자체 서명한 인증서를 발행하고, 이를 이용하여 사용자의 인증서를 발행하며, 인증서 폐지 사유가 발생하면 인증서를 폐지하고 인증서 폐지 목록을 생성한다. 이때 인증서 폐지 목록 운영의 문제점을 극복하기 위한 Delta-CRL을 이용하여 전송 선로에서의 트래픽 부하를 감소시키고, 인증서 폐지 목록을 저장하는 저장 공간의 부족 문제를 해결하였다.

참 고 문 헌

[1] David A. Cooper, "A More Efficient Use of Delta-CRLs", *Proceeding of 2000 IEEE Symposium on Security and Privacy, 2000.*

[2] IETF homepage, http://www.ietf.org/, 1999.

[3] C. Adams, S. Farrell, Certificate Management Protocols, http://www.ietf.org/internet-drafts/*draft-ietf-pkix-ipki3cmp-08.txt*, 1998. 5.

[4] David A. Cooper, "A Model of Certificate Revocation", *Proceeding of Fifteenth Annual Computer Security Applications Conference*, 12. 1999.

[5] Public-Key Infrastructure(X.509) (pkix), http://www.ietf.org/html.charters/pkix-charter.html, 1998. 4

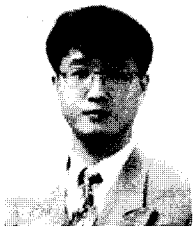
[6] IETF, Security Area, "X.509(pkix) Document", http://www.ietf.org, 1999. 7.

[7] ITU and ISO/IEC Final Proposed Draft Amendment on Certificate Extensions April 1999.

[8] R. Housley, W. Ford, W. Polk, D. Solo "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", http://www.ietf.org/internet-drafts/draft-ietf-pkix-new-part1-08.txt, 7, 2001.

[9] IETF Internal Document, IETF Society, 2001.

〈著者紹介〉



김 락 현 (Rack-Hyun Kim)
1997년 2월 : 순천향대학교 전자공학과 졸업
1999년 8월 : 순천향대학교 일반대학원 전기·전자공학과 석사 졸업
2000년~현재 : 순천향대학교 정보보호학과, 청운대학교 인터넷컴퓨터학과, 홍성기능대학교 전자계산기학과 외래강사
2001년 2월~현재 : 순천향대학교 일반대학원 정보보호학과 박사과정
〈관심분야〉 암호 이론, 공개키 기반구조, 전자상거래 보안

엄 희 정 (Hee-Jung Um)
2000년 2월 : 수원대학교 이과대학 전자계산기학과 졸업
2000년 3월~현재 : KSIGN PKI 개발부 연구원
2001년 9월 : 순천향대학교 산업정보대학원 정보보호학과 석사과정
〈관심분야〉 통신공학, 정보보호, 암호프로토콜

염 흥 열 (HeungYoul Youm)
1981년 : 한양대학교 전자공학과 졸업
1983년 : 한양대학교 대학원 전자공학과 석사
1990년 : 한양대학교 대학원 전자공학과 박사
1982년~1990년 : 한국전자통신연구소 선임연구원
1990년~현재 : 순천향대학교 공과대학 정보기술공학부 교수, 정보보호학과 학과장
1997년~2000년 : 순천향대학교 산업기술연구소 소장
2000년~현재 : 순천향대 산학연컨소시엄센터 소장
1997년~현재 : 한국통신정보보호학회 총무이사, 학술이사, 교육이사
〈관심분야〉 네트워크 보안, 전자상거래 보안, 공개키 기반 구조, 부호이론, 이동통신보안