P2P 서비스를 이용한 효율적인 인증서 폐지 목록 배포에 관한 연구

김현철*, 백주호*, 김정재*, 오해석*
*숭실대학교 컴퓨터학과
e-mail:dmzpolice78@korea.com

A Study on Efficient Certificate Revocation List Distribution using P2P Service

Hyun-Chul Kim*, Ju-Ho Baek*, Jeong-Jai Kim*, Hae-Seok Oh*
*Dept of Computer Science. SoongSil University

요 약

공개키 기반의 인증서 상태 검증 시스템은 사용자 인증서에 대해 전자 서명을 수행함으로써 사용자 중요 정보의 대한 무결성, 인증, 부인방지, 기밀성 등을 보장해 준다. 이와 같은 인증서 상태 검증 서비스를 제공하기 위해 인증서 상태 검증 시스템은 하루에 한번씩 인증기관(CA)으로부터 디렉토리 서버에 개시된 인증서 폐지 목록을 다운 받아야 한다. 하지만 현재 사용되고 있는 인증서 폐지 목록 배포 시스템은 특정시간에 다수의 인증서 상태 검증 서버가 디렉토리 서버에 접속해 인증서 폐지 목록을 다운 받아야 하기 때문에 네트워크에 대한 과부하로 인한 인증서 폐지 목록 다운로드 시간이 많이 소요된다는 단점과 디렉토리 서버의 처리량의 초과로 인한 서버가 다운될 수 있는 문제가 발생할 수 있다. 따라서 본 논문에서는 기존의 인증서 폐지 목록 배포 방식에 대한 분석과 더불어 위와 같은 문제를 해결하기 위한 Peer-to-Peer 서비스를 이용한 효율적인 인증서 폐지 목록 배포 시스템을 제안 하고자 한다.

1. 서론

공개키 기반의 전자 서명 검증 기술은 자신의 공개키를 외부에 공개한 후, 이를 이용하여 자신의 신원을 상대방에게 입증시키는 기술이다. 그러나 공개키는 누구나 쉽게 획득 할 수 있도록 공개된 장소에 등록되어 있기 때문에 중요 정보의 노출, 중요 정보의 위·변조등과 같은 문제가 발생할 수 있다.[1]

이러한 중요 정보의 보호를 위해서는 정보의 위조 및 변조 여부를 판단하는 무결성(Integrity), 전송된 정보의 송신자와 수신자를 확실하게 증명해주는 인증(Authentication), 정보의 송신자와 수신자 사이에 송신과 수신한 사실을 부인하지 못 하도록 하는 부인방지(Non-Repudiation), 모든 정보 교환에 대하여 중요 정보의 불법 노출을 방지하기 위한 기밀성(Confidentiality)등의 기능들이 기본적으로 제공되어야 한다.[2]

PKI기반의 인증서 상태 검증 시스템은 사용자의 인증서에 대한 전자 서명을 수행함으로써 사용자 인증서에 대한 무결성, 인증, 부인방지, 기밀성등을 보장하여 준다. 하지만 현재 사용하고 있는 인증서 상태 검증 시스템은 디렉토리 서버에 개시된 인증서 폐지 목록을 특정시간에 다수의 인증서 상태 검증 서버들이 접속해서 인증서 폐지목록을 다운 받아야 하기 때문에 네트웍에 대한 많은 부하가 걸리며 그에 따른 결과로 인증서 폐지 목록 다운로드 시간이 많이 소요된다는 단점이 있다. 그와 더불어 디렉토리 서버의 처리량 초과로 인한 디렉토리 서버가 다운될 수 있는 문제가 발생할 수 있다.[4]

본 논문에서는 기존의 인증서 폐지 목록 배포 방식에 대한 분석을 통한 문제점을 제시하고 문제점을 해결하기 위한 P2P 서비스를 이용한 효율적인 인증서 폐지 목록 배포에 관한 새로운 방안을 제안하고자 한다.

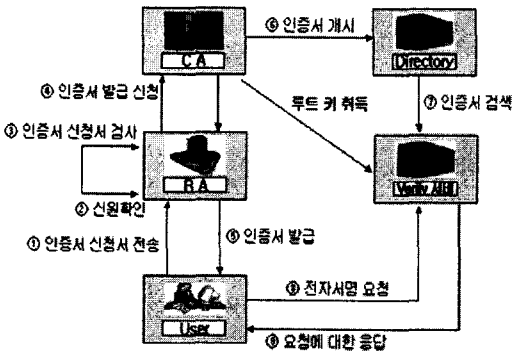
본 논문에 구성은 2장에서 관련연구를 기술하고 3장에서 제안하는 시스템인 P2P 서비스를 이용한 효율적인 인증서 폐지 목록 배포에 관하여 제시한다.

4장에서 본 연구 결과로 얻을 수 있는 기대효과에 대하여 기술하고 5장에서 결론을 맺고자 한다.

2. 관련연구

2-1 PKI(Public Key Infrastructure)기반구조

공개키 알고리즘을 통한 암호화 및 전자서명을 제공하는 복합적인 보안시스템으로서 암호화와 복호화 키로 구성된 공개키를 이용하여 송수신 데이터를 암호화하고 디지털 인증서를 통해 사용자를 인증하는 시스템 구조를 공개키 기반 구조 다시 말해 PKI 기반 구조라 한다. [그림 1]은 공개키 기반구조 구성도를 보여주고 있다.[1][2]



[그림 1] 공개키 기반구조

2-2 공개키 기반구조 구성요소

① 인증기관(CA)

CA는 Certificate Authority의 약어로서 다른 인증기관에게 인증서를 발행해 주는 신뢰성이 보장된 실체로서 인증기관은 인증서를 발급하고 폐지하며 또한 디렉토리에 인증서 및 인증서 폐지 목록을 개시하는 역할을 한다.[3]

② 등록기관(RA)

등록기관 RA는 Registration Authority의 약어로서 인증기관과 인증서 주체가 될 실체 사이의 중간 매개체 역할을 수행하는 실체이다. 또한 등록기관은 사용자의 신분을 확인하는 역할뿐만 아니라 인증기관으로부터 권한을 위임받아 사용자에게 인증서 발급 신청을 접수받으며 접수받은 인증서 발급을 인증기관에 요청한다. RA는 선택적 요소이며 RA가 없을 때에 인증기관(CA)은 RA에 기능을 수행한다.[3]

③ Directory

인증서와 사용자 관련 정보, 상호 인증서 쌍 및 인증서 폐지 목록 등을 개시하고 개시된 정보를 저장 · 검색하는 장소이다.[3]

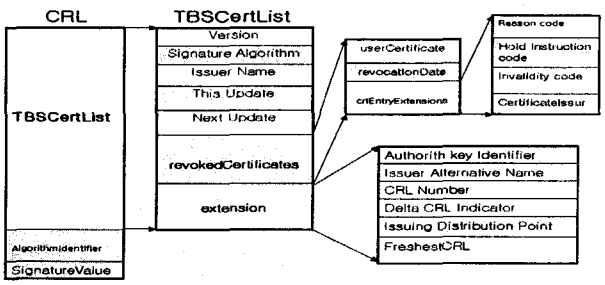
④ USER

인증서를 사용하는 실제 사용자.[3]

2-3 인증서 폐지 목록(CRL)

인증서 폐지 목록 CRL은 Certification Revocation List의 약어로 인증서는 사용자가 해당 인증서에 대한 취소를 요청 했을 경우, 사용자의 개인키가 노출되었을 경우, 사용자가 인증서를 발행 했던 기관으로부터 퇴직 했을 경우 등과 같이 여러 가지 이유로 인증서 유효기간 이전에 폐지될 수 있는데 이렇게 폐지된 인증서를 모아놓은 리스트를 의미한다.

현재 사용되고 인증서는 CCITT에서 제정한 X.509V3이며 X.509 CRL방법은 1993년 X.509 version2에서 CRL version1이 제정되었고, 1997년 X.509 version3에서 CRLversion2가 제정되었다. 현재 RFC2459에서 CRL 프로파일을 규정하고 있다. CRL포맷은 [그림 2]와 같다.[1][5]



[그림 2] X.509v3 CRL 포맷

CRL 포맷의 각 필드의 내용을 살펴보면 아래와 같다.

① Version : 인코딩된 CRL의 버전을 의미

② Signature Algorithm : CRL을 서명하기 위해 사용된 알고리즘을 나타낸다.

③ Issuer Name : CRL을 발행하고 서명한 발급자 이름을 나타낸다.

④ This Update : CRL의 현재 발행 일자를 나타낸다.

⑤ Next Update : 현재 CRL에 다음 CRL이 발행 일자를 나타낸다.

⑥ revoked certificates : 폐지된 인증서를 나타낸다.

⑦ extension : CRL에 추가적인 속성을 나타낸다.

⑧ Authorith key Identifier : 개인키에 대응하는 공개키를 구분하는 수단

⑨ Issuer alternative name : 추가적인 Identity가 CRL 발행자와 연결될 수 있도록 한다.

⑩ CRL Number : non-critical CRL의 확장

⑪ Delta CRL 지시자 : Critical CRL에 확장으로 delta-CRL을 구분한다.

⑫ Issuing Distribution Point : critical CRL의 확장으로 특정 CRL에 대한 분배점을 알 수 있게 한다.[1][5]

2-4 Delta-CRL

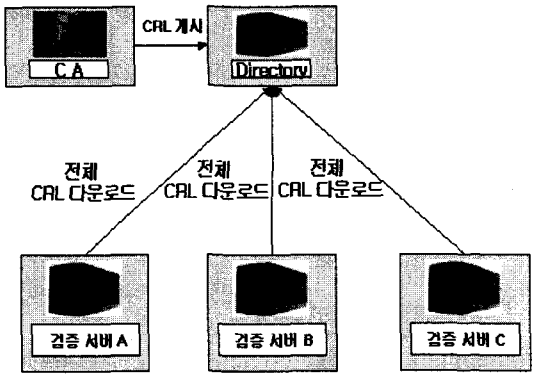
CRL의 주기적인 갱신기간(24시간) 동안 현재성 문제를 보완하기 위해서 제안된 방식으로 Delta-CRL은 가장 최근 폐지된 인증서만을 포함하는 인증서 폐지목록이다. 즉 CRL이 생성된 때부터 다음 CRL생성까지의 포함된 폐지 인증서와의 차이만큼을 포함하는 인증서 폐지목록이다. 따라서 사용자는 전체 CRL을 다운 받을 필요 없이 가장 최근에 발급된 CRL과 그 이전에 발급된 CRL과의 차이만큼을 다운 받아서 사용하기 때문에 CRL을 저장하기 위한 공간을 줄일 수 있으며, CRL 갱신 이전에 폐지목록을 제공하기 때문에 CRL에 현재성 문제를 해결할 수 있다는 장점이 있다. [그림3]는 Delta-CRL 포맷이다.[5]

<table>
<tr><td colspan="3">CRL version</td></tr>
<tr><td colspan="3">Issuer's signature Algorithm ID</td></tr>
<tr><td colspan="3">Issuer's X.500 Name</td></tr>
<tr><td colspan="3">Date and time of This Update</td></tr>
<tr><td colspan="3">Date and time of Next Update</td></tr>
<tr><td>Serial</td><td>Revocation Time</td><td>crlEntryExtion</td></tr>
<tr><td colspan="3">Crl Extensions</td></tr>
<tr><td colspan="3">CA Signature</td></tr>
</table>

[그림 3] Delta-CRL 포맷

3. 제안하는 시스템

기존의 인증서 폐지 목록 분배 방식은 인증서 폐지 목록이 인증기관(CA)로부터 디렉토리 서버에 개시되고 인증서 상태 검증 서버는 인증서 폐지 목록을 다운로드 하기 위해 동시에 디렉토리에 서버에 접속 인증서 폐지 목록을 다운 받는 방식이다. 하지만 현재 사용되고 있는 인증서 폐지 목록 배포 시스템은 특정시간에 다수의 인증서 상태 검증 서버가 디렉토리 서버에 접속해 인증서 폐지 목록을 다운받아야 하기 때문에 네트워크에 대한 과부하로 인한 인증서 폐지 목록 다운로드 시간이 많이 소요된다는 단점과 디렉토리 서버의 처리량의 초과로 인한 서버가 다운될 수 있는 문제가 발생할 수 있다. [그림 4]는 현재 사용되고 있는 인증서 폐지 목록 배포 시스템을 보여주고 있다.

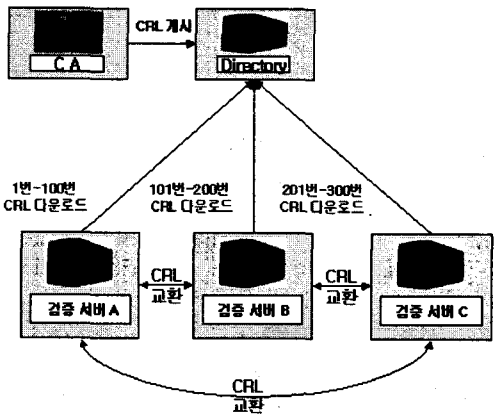


[그림 4] 기존의 인증서 폐지 목록 배포 방식

본 논문에서는 기존의 인증서 폐지 목록 배포 방식의 효율성 증진을 위한 방법으로 P2P 서비스를 이용한 인증서 폐지 목록 배포에 관한 새로운 모델을 제안하고자 한다.

본 논문에서 제안하는 P2P 서비스를 이용한 인증서 폐지 목록 배포 방식은 각각의 서버가 전체크기의 인증서 폐지 목록을 다운 받는 방식이 아닌 인증서 폐지 목록을 일정 크기로 구분하여 다운로드 하는 방식이다. 즉 인증기관(CA)은 인증서 폐지 목록을 일정 크기로 구분해서 디렉토리 서버에 개시한다. 그 후 각각의 인증서 상태 검증 서버는 자신에게 해당되는 일정 크기에 인증서 폐지 목록만을 다운로드 받는다. 자신이 다운로드 하지 않은 인증서 폐지 목록을 획득하기 위해 연결된 다른 인증서 상태 검증서버와 P2P 서비스를 이용해 자신이 다운받지 않은 인증서 폐지 목록에 대한 교환을 통한 인증서 폐지 목록을 획득한다.

본 논문에서 제안하는 방식을 위해 몇가지의 전제조건이 필요하다. 먼저 인증기관(CA)에서 인증서 폐지 목록을 디렉토리 서버에 개시 할 시점에 인증서 폐지 목록을 일정 크기로 구분해야 한다. 또한 P2P 서비스를 이용하기 위해 각각의 인증서 상태 검증 서버간에 데이터베이스는 공유되어야 한다. 본 논문에서 제안하는 시스템의 구성도는 [그림 5]와 같다.



[그림 5] 제안하는 시스템

4. 기대효과

본 논문에서 제안하는 P2P 서비스를 이용한 인증서 폐지 목록 배포 시스템은 전체 인증서를 다운 받는 기존 방식에서의 문제점인 네트워크 과부하 문제로 인한 인증서 폐지 목록 다운로드 시간을 감소시키기 위해 인증서 폐지 목록을 일정 크기로 구분해 다운로드 함으로서 네트워크 과부하 문제를 해결할 수 있으며 그로 인한 부과적인 효과로 인증서 폐지 목록 다운로드 시간을 감소 시킬수 있다.

또한 각각의 인증서 상태 검증 서버간의 P2P 서비스를 이용 자신이 다운받지 않은 인증서 폐지 목록을 다른 인증서 상태 검증 서버와 교환함으로써 디렉토리 서버에게 집중되는 현상을 다른 인증서 상태 검증 서버에게 분산 시켜줌으로서 디렉토리 서버에 대한 Access 효율을 증가 시킬 수 있다. 결과적으로 디렉토리 서버 처리용량 초과로 인한 디렉토리 서버 다운 문제를 해결할 수 있다.

5. 결론

본 논문에서는 기존의 인증서 폐지 목록 배포 방식에 대해 기술하였고 또한 철저한 분석을 통해 네트워크에 대한 과부하로 인한 인증서 폐지 목록 다운로드 시간이 많이 소요된다는 문제와 디렉토리 서버의 처리량의 초과로 인한 서버가 다운될 수 있는 문제를 제시하였다.

본 논문에서는 위와 같이 문제점으로 지적된 문제를 해결하고 보다 효율적인 인증서 폐지 목록 배포를 위한 P2P 서비스를 이용한 인증서 폐지 목록 배포 시스템을 제안하였다. 향후 본 논문의 연구 결과를 바탕으로 실제 공개키 기반 구조 시스템에 적용할 수 있도록 연구를 계속 진행해 나갈 것이다.

참고문헌

[1] 이만영, 원동호, 이민섭, 송주석, 임종인, 박춘식 " 현대 암호학 및 응용" 생능출판사. 2002

[2] 권태경, 강명호, 김승주, 서정욱, 진승헌 "정보 보 호 표준 개론" 한국정보통신기술협회. 2002

[3] "정보보호기술 용어집" 한국정보보호진흥원. 2002

[4] Chu Yae Liau, Stephane Bressan, Kian-Lee Tan "Efficient Certificate Revocation : A P2P Approach" ASIAN 2002 Workshop on Southeast Asian Computing Research. (ASIAN 2002).

[5] J. Willemson "Certificate Revocation Paradigms" Technical Report, Cybernetica. 1998