부하감소를 위한 분산 OCSP 서버 그룹화 모델 제안

최선묵° 서동린, 이금석
동국대학교 컴퓨터공학과, 동서울대학 컴퓨터소프트웨어과, 동국대학교 컴퓨터공학과
tashcom@dongguk.edu°, drsuh@dsc.ac.kr, kslee@dongguk.edu

A Proposal on Grouping Model of Distributed OCSP Server for Reduced Load

Seonmook Choi° Dongreen Suh, Keumsuk Lee
Dept. of Computer Engineering Dongguk Univ. Dept. of Computer Software Dongseoul Coll.
Department of Computer Engineering Dongguk University

요 약

PKI(Public Key Infrastructure)에서 인증서 상태 검증은 네트워크 환경에서의 거래에 신뢰성과 안전성 및 기밀성, 무결성 등의 서비스를 제공한다. 인증서 검증 방식은 CRL, OCSP, SCVP, DVCS 등이 있다. CRL은 시간이 지남에 따라 CRL의 크기가 증가하여 검증 시간이 지연되고 실시간 검증을 할 수 없는 단점을 가지고 있다. OCSP는 CRL을 이용하지 않고 거의 실시간에 가깝게 인증서를 검증하지만 서버의 부하 증가와 느린 검증 등의 단점을 가지고 있다. 분산 OCSP는 OCSP 서버를 분산시킨 후 CRL을 중복하여 보관하거나 분배하여 보관한 상태에서 검증하는 방식으로 대리검증에 따른 느린 검증과 CA의 부하부담 등의 단점을 가지고 있다. 본 논문에서는 제기된 단점들을 해결하여 빠른 검증과 부하 분산 효과를 얻을 수 있도록 분산된 OCSP 서버를 그룹으로 분류하고, 그룹 내의 각 서버에 인증서 폐지 정보를 중복 저장하여 부하분산, 빠른 검증, CRL을 Delta CRL 방식으로 OCSP 서버에 전송하여 네트워크 부하를 감소할 수 있도록 그룹 분산 OCSP 방식을 제안하고자 한다.

1. 서 론

네트워크 환경에서 정보의 위변조 및 누출, 부인 등의 위협으로부터 정보를 안전하게 보호하고 신뢰성 있는 거래를 위한 기술로 PKI가 이용되고 있다. PKI가 제공하는 서비스는 기밀성, 부인방지, 무결성, 인증 등이 있다. PKI는 사용자의 공개키와 인증서를 사용할 수 있도록 기반을 제공하는 구조로, 인증서(Certificate)는 신뢰할 수 있는 기관에서 사용자의 신분과 공개키를 CA의 개인키로 서명하여 발행하고 공개한다. 발행된 인증서는 유효기간 이전에도 사용자의 신원변경, 개인키 노출, 자격박탈 등의 이유로 인증서의 효력이 정지되거나 폐지될 수 있다. 인증서 상태 검증은 PKI를 이용한 거래에서 필수적이며 중요한 과정으로 CRL, OCSP, SCVP, DVCS 방식 등이 있다[1].

CRL은 주기적으로 인증서 폐지정보를 발행하여 DS에 공개하고, 검증 시 CRL 전체를 클라이언트로 가져가 실시한다. OCSP는 CRL을 이용하지 않고 CA가 실시간에 가깝게 발행하는 CRl를 OCSP 서버로 가져와 요청된 검증 서비스를 실시한다. SCVP는 인증서 폐지정보 및 전체 인증서에 대한 간단한 검증 서비스까지 제공하는 프로토콜이다. DVCS는 인증서 데이터의 소유 증명 및 인증서 검증으로 부인방지 서비스를 제공한다.

CRL 방식은 CRL 크기가 증가함에 따라 검증 시간이 오래 걸리며, 주기적 처리에 의한 시간차(time gap) 등의 이유로 OCSP가 사용된다. OCSP 서버 방식은 검증이 한 곳에 집중되어 서버 부하가 증가되어 검증 시간 지연 등의 문제가 제기된다. 분산 OCSP 서버 방식은 분산된 OCSP 서버에 CRL를 중복 저장하거나 분배 저장할 경우 안전성에는 유리하지만, 검증 시간 및 네트워크 송수신 등의 문제, 대리검증에 따른 검증 시간 지연 등의 문제점이 발생된다.

본 논문에서 제안한 서버 그룹핑 기법은 분산된 OCSP 서버들을 그룹으로 나누고, 그룹 내의 OCSP 서버들에게 인증서 폐지 정보를 중복 저장하고, 부하분산 모듈을 이용하여 그룹 내에서 부하가 가장 적은 서버가 검증을 실시하도록 하여 빠른 검증 결과를 얻을 수 있게 하였다.

본 논문의 구성은 2장에서는 관련연구에 대해 알아보고, 3장에서는 제안된 모델의 구조 및 분석, 결과를 알아본다. 마지막으로 4장에서는 결론을 맺는다.

2. 관련연구

PKI에서 인증서의 사용은 필수적이며, 사용 전 반드시 인증서 상태를 점검하여야 한다. 인증서 상태 점검 방법인 CRL, OCSP, 분산 OCSP에 관해 살펴본다.

2.1 CRL

CA는 주기적으로 폐지되거나 효력이 정지된 모든 인증서의 일련번호, 폐지시간, 폐지이유 등을 CRL에 기록하여 DS에 공개하고 보관한다[2]. 공개된 CRL은 클라이언트로 가져다 검증에 이용한다. 한 개의 인증서를 검증할 경우에도 CRL 전체를 다운로드해야 하므로, 사용자의 증가로 CRL의 크기도 증가하여 네트워크 부하 및 검증시간의 지연, 시간 차 등의 문제가 있을 수 있다.

2.2 OCSP

온라인상에서 OCSP 서버와 OCSP 클라이언트간에 수행되는 프로토콜로 인증서의 폐지상태 및 효력정지 여부를 CRL을 사용하지 않고 실시간에 가깝게 확인하는 프로토콜이다[2]. ORS, DPD, DPV 등의 서비스를 통해 클라이언트 요구를 단일 서버가 검증하여 응답한다[1][3][4][5]. 단일 OCSP 서버에 검증이 집중되어 부담이 가중되고 검증시간 지연 등의 문제가 발생될 수 있다.

2.3 Distributed OCSP

단일 OCSP 서버의 부담 증가와 검증시간 지연 등을 해결하기 위해 서버를 여러 곳에 분산할 필요가 있다[6]. 분산된 각 OCSP 서버에 CRl를 중복 보관하여 인증서 상태 검증을 실시한다[7]. 중복 보관할 경우 안전성에는 유리하지만 검증시간 지연, 네트워크 부하 증가 등의 문제가 발생될 수 있다.

3. 제안 모델

분산 OCSP 서버에 CRl를 중복하여 보관하거나 분배하여 보관할 경우 발생할 수 있는 문제는 사용자 급증에 의한 CRL 크기 증가로 인증서 상태 검증 시간의 지연(중복보관과 분배보관), CA와 OCSP 서버간의 CRl 전달에 따른 네트워크 부하증가(중복보관), 특정 서버에 검증이 집중될 경우 다른 서버에 검증을 요청하고, 요청 받은 서버는 인증서 정보를 CA로부터 가져와 검증하는 대리검증에 따른 시간 지연(분배보관) 등이 있을 수 있다. 제안 모델은 부하분산을 통해 검증 시간 단축에 효과가 있는 방법을 제안한다.

3.1 제안모델의 구성

그림 1은 제안모델의 구성도로 분산된 OCSP 서버들을 OCSP 클라이언트 특성 및 분포, 네트워크 환경, 거리 등을 고려하여 그룹으로 나누고, 그룹에 속한 모든 OCSP 서버에는 동일한 인증서 효력정지 및 폐지 목록을 중복하여 저장한다. 검증 시 부하가 가장 작은 OCSP 서버가 검증을 실시한다.

3.2 제안모델의 효과

CA와 OCSP 서버간의 인증서 효력정지 및 폐지 정보는 Delta CRL을 이용하여 새롭게 발행된 정보만을 전송함으로써 네트워크 부하를 감소하게 한다. CRL 전체를 다운로드하지 않고 새롭게 갱신된 정보만을 받기 때문에 OCSP 서버가 다운로드하는 시간을 줄일 수 있다.

분산 OCSP 방식에서 CRL 중복보관은 급증하는 CRL 크기에 의한 네트워크 및 OCSP 서버의 부하 증가, 검증 지연 등의 문제는 CRL을 분배하여 저장함으로 해결할 수 있다. 그러나 CRL을 분배하여 보관할 경우에 발생되는 문제 중에서 대리검증은 인증서 정보를 가지고 있는 서버가 부하 증가로 검증 작업을 처리할 수 없을 때, 다른 서버에 검증을 부탁하는 동작이다. 부탁받은 OCSP 서버는 검증하려는 인증서 정보가 없기 때문에, CA에 검증하려는 인증서 정보를 요청하여 검증하고, 검증 결과를 부탁한 OCSP 서버에 전송하는 관계로 검증 시간의 지연이 발생된다.

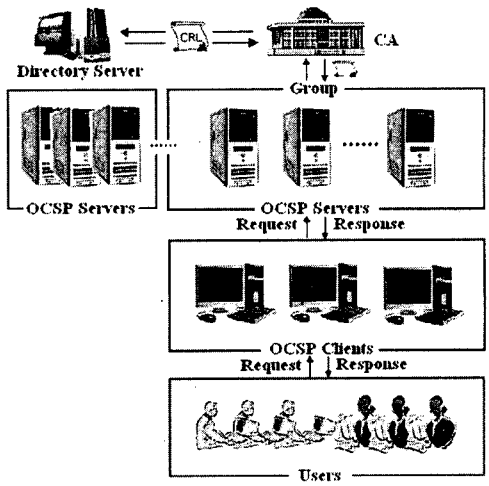

그림 1 제안모델 구성도

제안 모델은 그룹에 속한 모든 OCSP 서버에 동일한 CRL 정보를 중복 보관하고, 검증 요청 시 부하가 가장 적은 OCSP 서버를 선택하여 검증하게 함으로써 대리검증이 필요 없기 때문에 빠른 검증 결과를 얻을 수 있다. 이 같은 효과는 그룹에 속한 모든 OCSP 서버 중에서 부하가 가장 적은 서버를 찾기 위해 모든 OCSP 서버의 부하를 지속적으로 측정하여 기록하는 부하 모니터링 모듈과, 측정된 부하량을 이용하여 부하가 가장 적은 OCSP 서버를 선택하여 요청된 검증을 실시하도록 지시하는 부하균형 모듈이 필요하다.

3.3 제안모델의 처리모듈

CA는 인증서를 발행하고 인증서 발행 정보를 보관할 그룹에 전송한다. 발행된 인증서 정보가 어느 그룹에 보관되었는지 테이블에 기록하여 보관한다. CA는 테이블에 기록된 정보를 이용하여 각 그룹에 인증서 정보가 균등하게 보관되도록 한다. 발행된 인증서에는 정보가 보관된 그룹의 주소가 확장 필드에 기록된다. 즉, 인증서 생성 시 CA는 각 그룹에 보관된 인증서 수를 확인하여, 가장 적은 수를 보관하고 있는 그룹에 인증서 사용자의 정보와 공개키를 CA의 개인키로 서명하여 발행하고 보관한다. 확장 필드에 기록된 그룹 주소는 차후 인증서 검증 시, 클라이언트가 인증서 정보가 보관된 그룹을 검색하는데 이용된다. 그림 2는 제안 모델의 처리모듈을 나타낸 것이다.

OCSP 클라이언트는 사용자가 검증을 요청할 경우 인증서 처리모듈 정책에 따라 OCSP 형식에 맞추어 OCSP 서버에 검증을 요청하고, 동시에 DPD와 DPV에 의해 인

증서 경로 검색 및 인증서 경로 검증을 OCSP 서버에 위임한다. 이 때 인증서에 기록된 그룹 주소를 가지고 검증에 필요한 정보가 어느 그룹에 보관되었는지 확인하고, 검증을 요청한 인증서를 해당 그룹에 전달한다.

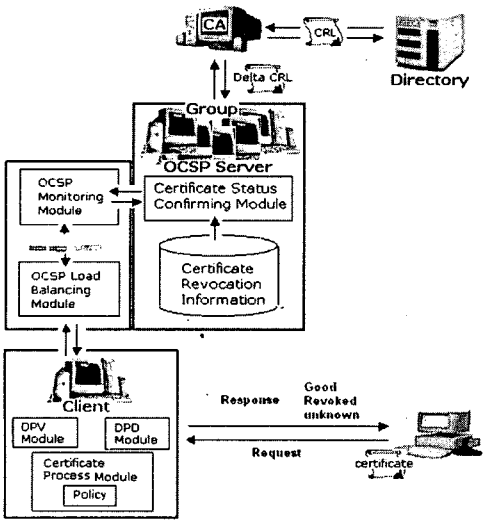

그림 2 제안모델의 처리모듈

OCSP 모니터링 모듈은 지속적으로 그룹에 속한 각 OCSP 서버들의 부하량을 임계값을 기준으로 측정하여 보관한다. 보관된 각 OCSP 서버들의 부하량은 인증서 상태 검증이 요청될 때, OCSP 서버 부하균형 모듈이 그룹에 속한 OCSP 서버 중에서 부하량이 가장 적은 OCSP 서버를 선택하여 검증을 실시하도록 수신된 정보를 전달한다. 지정된 OCSP 서버는 인증서 효력정지 및 폐지목록을 확인하여 검증하고, 그 결과를 요청한 OCSP 클라이언트에 전송한다.

3.4 제안모델의 분석결과

제안한 서버 그룹핑 모델은 분산된 OCSP 서버들을 그룹으로 묶고, 각 그룹의 OCSP 서버들에게 새롭게 갱신된 CRI만을 Delta CRL 기법으로 전송하여 전송 시간 단축 및 네트워크 부하 감소 효과가 있다. 또 한 요청된 검증을 그룹 안에서 처리하도록 그룹에 속한 모든 OCSP 서버에 동일한 CRI를 저장하고, 부하가 가장 적은 OCSP 서버를 찾아 검증하므로 빠른 검증 결과를 얻는다. 표 1은 단일 OCSP, 분산 OCSP CRL 중복, 분산 OCSP CRL 분배 및 제안모델을 네트워크 부하, 지연시간, 대리검증, 응답시간으로 비교한 것이다.

네트워크 부하는 단일 OCSP와 분산 OCSP CRL 중복은 CRL 전체를 가져오는 관계로 가장 많고, 분산 OCSP CRL 분배보다 제안 모델이 아주 적은 것은 새롭게 갱신된 정보만을 가져오기 때문이다. 지연시간은 CRL을 읽는 시간으로 전체 CRL을 읽어야 하는 단일 OCSP와 분산 OCSP CRL 중복이 길고 갱신된 정보만을 읽는 제안 모델이 가장 짧다. 대리검증은 분산 OCSP CRL 분배에

표 1 검증기법별 분석비교

	네트워크 부하	지연시간	대리검증 시간	응답시간
단일 OCSP	아주 많다	길다	없음	아주 느리다
분산 OCSP [CRL 중복]	아주 많다	길다	없음	아주 느리다
분산 OCSP [CRL 분배]	적다	짧다	길다	느리다
제안 모델	아주 적다	아주 짧다	없음	빠르다

서만 발생된다. 응답시간은 단일 OCSP와 분산 OCSP CRL 분배는 전체 CRL을 참조하고 실시간에 가깝게 전체 CRI를 전송받기 때문에 아주 느리며, 제안 모델은 분산 OCSP CRL과 같이 분배된 CRL을 참조하지만 대리검증이 없는 제안 모델의 응답시간이 더욱 빠르다.

4. 결론

PKI를 이용한 거래에서 인증서 상태검증은 필수적인 것으로, 실시간에 가깝게 정확한 검증과 빠른 응답이 요구된다. CRL, 단일 OCSP, 분산 OCSP 기법의 네트워크 부하량 증가, 느린 다운로드 시간, 느린 검증 시간 등을 해결하기 위해 서버 그룹핑 모델을 제안하였다. 제안된 모델은 대리검증을 없애고 부하를 분산하여 빠른 검증 결과를 얻는 효과를 낼 수 있다. 향후 연구과제는 급증하는 인증서 폐지에 따른 CRL 크기 증가로 네트워크 부하량 증가, 느린 검증 시간 등을 해결하기 위해 CRL 구조 변경, Disk에서 정보를 가져오지 않고 메모리에서 가져오는 방법 등에 대해 더 연구가 필요하다.

참고문헌

[1] M.Myers et al, "Draft, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol", version 2, IETF, 2002

[2] R.Housley, W.Ford, T.Polk, D.Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC2459, Jan. 1999

[3] M.Myers, S.Farrel, C.Adams, "Delegated Path Discovery with OCSP", IETF Draft, draft-ietf-pkix-ocsp-path-00.txt, Sep. 1999

[4] M.Myers, C.Adams, S.Farrell, "Delegated Path Validation", IETF Draft, draft-ietf-ocsp-valid-00.txt, Aug. 2000

[5] D.Pinkas, "Delegated Path Validation and Delegated Path Discovery Protocol", IETF Draft, draft-ietf-pkix-dpv-dpd-00.txt", Jul. 2001

[6] C.Popescu, B.Crispo, S.Tanenbaum, "A Certificate Revocation Scheme for a Large-Scale Highly Revocation Distributed System", IEEE, 2003

[7] 고훈, 장의진, 신용태, "PKI환경의 OCSP 서버 부하 감소를 위한 OCSP 분산 기법", 정보보호학회 논문지, 제13권 6호, 2003. 12