DNS를 사용한 다중 도메인 환경에서의 CRL 검증에 대한 연구

이건희[0] 유정각 이상하* 김동규
아주대학교, * 동서울대학
(icezzoco[0], kagi, dkkim)@madang.ajou.ac.kr, * shyi@haksan.dsc.ac.kr

A Study about CRL Validation under Multi-Domain Environment using DNS

Geon-Hee Lee[0] Jeong-Gak Yoo Sang-Ha* Yi Dong-Kyoo Kim
Dept. of Information Communication Engineering GSIC AJOU,
*Dept. of Information and Communication, Dong Seoul College

요 약

현재 인터넷 상에서 가장 많이 제공되고 사용 되는 서비스는 전자 상거래에 관련된 서비스이다. 이러한 서비스에서 각 사용자 사이의 신원을 증명해 줄 인증서는 절대적인 위치를 차지하게 된다. 따라서 전자 상거래의 성격에 비추어 그 인증서는 항상 적시에 유지 관리 되어야 하며, 그 상태가 매 순간마다 정확하게 변경되어야 할 것이다. 그리고 그 보안성도 높아야 한다. 이러한 요구사항을 만족하기 위해서 많은 연구가 진행되고 있다. 본 논문에서는 이를 현재 인터넷 환경에서 반드시 사용되어야 하는 DNS 를 이용하여 해결 하는 방법을 제안하고자 한다. 자원레코드의 확장 속성을 사용하여 인증서를 배포하고, 그를 검증하여 안전하고 적시 적용이 가능하도록 한다.

1. 서 론

최근 몇 년 사이에 인터넷 망을 이용한 전자 상거래가 인터넷의 중요한 서비스 중의 하나로 떠오르고 있다. 이러한 e-비즈니스에서 중요한 것이 계약 당사자 간의 인증이다. 계약자와 피 계약자가 서로를 절대적으로 믿고 계약을 할 수 있어야 하는 것이다. 이러한 전자 상거래의 위협 요소를 해결하기 위해서 PKI(Public Key Infrastructure)를 기반으로 하는 인증서를 사용하게 되었다.

이러한 인증서를 사용함에 있어서 고려해야 하는 것 중의 하나가 유효성을 상실한 인증서의 목록을 기록한 인증서 폐지 목록(Certificate Revocation List : CRL)의 관리다. 인증서는 사용자의 필요에 의해서 생성되었다가 다양한 이유로 동일한 사용자에 의해서 폐지될 수 있다. 그런데 폐지된 인증서를 제대로 검증하지 못할 경우, 계약자 상호 간에 신뢰할 수 있는 인증을 할 수 없으므로 PKI 자체의 적용이 어려워지게 된다. 현재 인증서의 유효성 검증을 위해서 가장 많이 쓰이는 기술은 인증서 폐지 목록을 이용하는 것이다. 따라서 폐지 목록의 관리가 중요한 문제점으로 떠오르게 된다.

기존의 CRL을 통한 인증서 검증은 일정 시간 간격마다 폐지된 인증서를 중앙의 디렉토리 서버에 등록하여 게시하는 방법이다. 하지만 전자 상거래는 항상 실시간으로 그 인증서의 유효성을 검증하기를 원하므로, 이 방법은 그 요구사항을 온전히 만족시켜 주지 못하는 단점이 있다.

이러한 CRL을 이용한 방법의 단점을 해결하고자 온라인 인증서 상태 검증 프로토콜(Online Certificate Status Protocol : OCSP)이나 간단한 인증서 검증 프로토콜(Simple Certificate Validation Protocol : SCVP) 등이 제시되고 있다. 하지만 이러한 방법들은 중앙 집중적인 방식을 사용하여 지역 분산에 어려움이 생기게 된다. 또, CRL의 크기가 계속 증가하므로 계속 되는 서버 부하의 증가를 피하기 어렵게 된다. 따라서 본 논문에서는 기존의 안전한 DNS(Domain Name Server)를 이용하여 인증서를 배포하고 CRL을 관리하는 방법에 대해서 논하고자 한다.

2. 기존의 인증서 검증 방법

2.1 CRL을 이용한 방법

디렉토리 서버를 통해서 직접 CRL을 내려 받아서 해당되는 인증서의 유효성을 검증하는 것이 된다. 이를 사용할 경우 구현이 간단하다는 점은 있지만, CRL이 점차 증가함에 따라서 네트워크 트래픽의 증가를 부르게 된다. 또, CRL이 커지면 인증서 유효성의 검증을 위해서 클라이언트가 해야 할 일이 많아지게 된다. 이를 보완하기 위해서 delta-CRL을 사용하지만 그 효율성에 대해서는 그리 높지 않다고 한다. 또 실시간으로 업데이트가 되지 않으므로 실시간 처리가 중요시 되는 서비스에서는 그 보안성에 문제가 된다.

2.2 온라인 인증서 상태검증 프로토콜 (OCSP)

OCSP는 클라이언트가 CRL을 요청하지 않고 유효성을 검증하고자 하는 인증서의 현재 상태를 검증하는데 사용하는 프로토콜이다. 이는 CRL을 통한 인증서 검증보다 인증서의 상황을 더 적시에 얻을 수 있어서 계약의

적시성이 크게 요구되는 시스템에 사용될 수 있다. 일례로 고액의 자금이체나 주식 거래 등에 이용될 수 있다.

클라이언트가 정해진 포맷으로 OCSP 응답 서버에게 상태를 요청하게 되면 OCSP 응답 서버는 이 요청이 정당한지를 가려 요청한 인증서의 상태에 대해서 응답을 해 준다. 이때 인증서의 상태는 양호(good), 폐기(revoked), 알려지지 않음(unknown) 등의 세 가지가 있다. 이러한 상태 정보를 통해서 해당하는 인증서의 유효성을 결정하게 되는 것이다.

2.3 간단한 인증서 검증 프로토콜(SCVP)

OCSP가 단순하게 사용할 인증서의 현재 상태를 검증하는 것이라면, SCVP는 서버에서 인증서의 경로 검증(path validation)을 대행함으로써 클라이언트의 오버헤드를 줄이기 위한 프로토콜이다. 현 draft에서는 서버와 클라이언트간의 메시지 정의는 되어 있지만 메시지 핸들링이나 서버의 역할에 대한 자세한 정의와 설명이 되어있지 않다. 이 프로토콜을 통해서 SCVP 서버는 클라이언트에게 인증서의 유효성 여부와 trusted root까지의 인증서 체인 등의 정보를 제공한다.

3. DNS를 이용한 인증서 검증 방법

기존의 인증서 검증 방식의 경우에 모두가 중앙 집중적인 방식을 사용한다. 따라서 이미 앞에서 밝힌 바와 같이 지역적인 분산이 필요하게 되므로 각 서비스를 제공하는 서버들의 보안이 매우 중요하다. 따라서 본 논문에서는 현재 인터넷을 적용하는데 있어 지역 분산이 잘 되어 있고 안전한 DNS를 이용한 인증서의 검증 방법을 제시하고자 한다.

3.1 DNS를 이용한 인증서 적용

우선 DNS의 구조가 PKI의 구조와 상이하다는 데서 출발하게 된다. 현재 인터넷 상의 DNS들은 각 도메인별로 DNS Master 서버가 존재하고, 그 아래에는 서브 네임 서버들을 두는 방식을 사용한다. 따라서 각 사용자가 인증서를 요청하게 되면 당연히 DNS를 통해서 CA(Certificate Authority)의 역할을 하는 서버로 이동을 하게 될 것이며, 이를 통해서 인증서를 받아오게 된다. 따라서 클라이언트가 요청하는 순간 DNS Master 서버에서 요청한 인증서를 받아서 보관을 하고, 이를 클라이언트가 속해 있는 해당 서브 네임 서버로 인증서를 전송한다. 서브 네임 서버 역시 이를 DNS에 보관하고, 이를 요청한 클라이언트에게 인증서를 보내 준다. 이 때 DNS 마스터 서버와 서브 네임 서버 사이에는 DNS의 존(zone) 전송을 이용하여 인증서를 분산시킨다. 그림 1이 이를 나타내고 있다.

이러한 방법을 사용함에 있어서 DNS의 보안 확장에서 제공하는 기존의 자원 레코드 외에 CERT RR이 추가된다. 이 CERT RR의 구조는 그림 2와 같다. Type 필드는 인증서의 타입을 나타내며, key tag 필드는 인증서에 포함되어진 키를 계산해서 얻어낸 16bit의 값이고, 알고리즘(algorithm) 필드는 키를 생성한 알고리즘을 나타낸다. 그리고 인증서의 적시의 업데이트를 위해서 DNS의 동적 업데이트 기능을 사용한다.

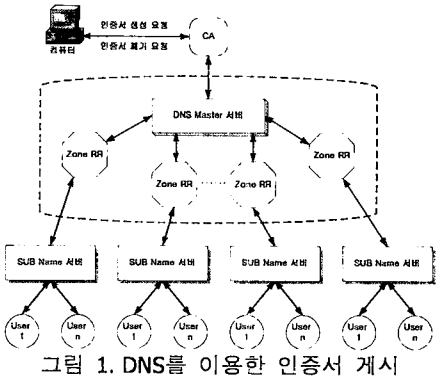

그림 1. DNS를 이용한 인증서 게시

클라이언트가 상대의 인증서를 요청하는 일은 DNS를 사용하는 것과 마찬가지다. 일단 사용자가 상대방과 통신을 위해서 단순하게 주소를 요청하는지, 인증서도 같이 요청하는 지를 구분한다. 그런 다음 인증서도 함께 요구하는 것이라면 서브 네임 서버의 CERT RR을 살핀다. 이때 이 전에 인증서가 캐쉬되었다면 해당하는 인증서가 되돌려 지게 될 것이다. 그렇지 않다면 최상위의 DNS를 통해서 다음 단계의 DNS로 계층적으로 내려오면서 인증서를 요청하게 된다.

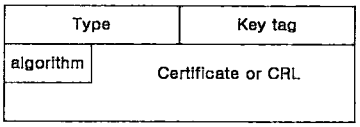

그림 2. CERT Resource Record

예를 들어 ajou.ac.kr에 속해 있는 B 사용자의 인증서를 A 사용자가 요청한다고 가정하자. 처음 연결하는 상태라면 DNS를 통해서 kr을 관장하는 DNS로 쿼리를 전송하게 되고, kr에서는 다시 ac를 관장하는 DNS로 전송하며, 마지막으로 ajou를 관장하는 DNS에서 원하는 B 사용자의 인증서를 획득하게 된다. 이 인증서는 인증서를 요청한 A 사용자가 속해있는 서브 네임 서버로 전송되어 CERT RR의 인증서 필드에 캐쉬되고 사용자에게 전송된다. 이렇게 해서 얻어진 인증서를 A 사용자가 검증하기 위해서 다음 절의 검증 방법을 사용한다.

3.2 DNS를 이용한 검증

3.1 절에서 언급한 방법으로 인증서를 관리하게 된다면 기존의 CRL 검증이 아닌 다른 방법을 적용할 수 있다. 기존의 CRL 검증법에 이용되는 CRL DP(Distribution Point) 정책이 있다. CRL을 이용한 검증법에서 CRL이 커질 경우의 네트워크 부하를 줄이기 위해서 자신이 사용하는 인증서의 CRL이 게시된 지점을 존 별로 나누어 게시하고 클라이언트가 CRL을 검사해야 할 경우 해당되는 지점으로 가서 CRL을 받아서 검증하게 하는 방법이다.

본 논문에서는 이를 응용하여 다음과 같은 방법을 제시한다.

3.1 절에서 언급한 CERT RR의 마지막 필드에 인증서나 CRL을 저장하게 되어 있다. 이 필드에 CRL 검증을 위해서 인증서가 폐기 될 경우 CRL을 넣어야 하지만, CRL이 커지면 그 효율은 떨어지게 된다. 따라서 도메인 CRL DP를 이 필드에 게시한다. 그리고 처음부터 CRL은 DNS의 도메인에 따라서 발급된다고 가정한다. 즉, ajou.ac.kr이라는 도메인 상의 사용자들에 대한 인증서 폐지 목록과 dsc.ac.kr이라는 도메인 상의 사용자들에 대한 인증서 폐지 목록은 따로 발급하는 것이다.

이 경우 클라이언트가 인증서의 유효성을 검증하기 위해서 CRL을 요청할 경우에 서브 네임 서버에 요청을 전송하게 되고, DNS에서는 이미 지니고 있던 도메인 CRL DP에 의해서 해당되는 CRL을 지니고 있는 곳으로 이동한다. CRL이 보관된 DNS 서버에서는 검증을 하기 위해서 하나씩 추적하고, 이 결과를 검증을 요청한 클라이언트에게 전송한다.

3.3 검증 알고리즘

```
procedure CertValidation()
x ← RRTypeCheck()
if x ≠ "good"
   then return CRLValidation(x)
   else return x

procedure RRTypeCheck()
if CERT_RR[type] = 1
   then return "good"
   else if CERT_RR[type] = 0
      then return CERT_RR[crl_zone]

procedure CRLValidation(crl_zone)
list ← crl[crl_zone]
x ← head[list]
while x ≠ NULL
   do if cert_A[serialNumber] = x[serialNumber]
         then return x[reasonCode]
         else x ← next[list]
return "unknown"
```

그림 3. 인증서 검증 알고리즘

3.2절에서 언급한 검증 과정을 거치기 위해서는 그림 3과 같은 알고리즘이 필요하다. 본 고는 이 알고리즘을 몇 가지 전제하에 제시한다.

첫째, 모든 사용자들이 사용하는 개인 인증서의 변동 및 폐기는 즉시 각 도메인을 관장하는 CA에게 알려지고, 이를 신고 받은 CA는 해당 DNS의 동적 업데이트 기능을 통해서 즉시 도메인 내에 알린다.

둘째, 클라이언트가 인증서를 생성하면 해당 DNS의 CERT RR의 인증서 필드에 인증서가 기록되며, 폐기를 할 경우에 DNS 서버는 CERT RR의 동일한 필드에 도메인 CRL DP를 보관한다.

셋째, 모든 사용자들이 사용하는 인증서를 폐기할 경우 CRL에 게시가 되며, 이는 연결 리스트(linked-list) 형태로 관리된다.

넷째, 인증서가 있는 DNS를 찾는 것은 DNS를 통해서 IP 주소를 연결 짓는 것과 유사하다.

다섯째, CERT RR의 type 필드가 예약된 값인 0을 도메인 CRL DP로 정의한다.

3.1절에서 언급한대로 B 사용자의 인증서를 획득한 A 사용자가 B 사용자에게 자신의 인증서와 자신의 주소를 보내어 둘 사이의 연결을 성립하고자 하면, B 사용자는 그림 3의 알고리즘을 이용해 이를 검증한다. 이 결과는 OCSP에서 사용하는 세 가지 상태 중 하나를 돌려준다. 이 결과를 통해 B는 A의 인증서가 유효한지를 결정한다.

위의 알고리즘에서 CERT_RR은 CERT 자원레코드를 의미하며, crl_zone은 각 존 별로 나누어진 도메인을 의미한다. A가 속해 있는 최종 네임 서버까지 url을 통해 추적한 다음 최종 네임 서버에 존재하는 CERT_RR의 type 필드를 검사하여 인증서를 포함하는지 도메인 CRL DP를 포함하는지를 결정한다. 인증서를 포함하면 인증서가 유효하다는 의미며, 도메인 CRL DP가 있을 경우 해당 존으로 넘어가서 CRL에 A의 인증서가 들어 있는지 비교하게 된다. 존재하면 CRL의 폐기 이유 코드를 넘겨주고 그렇지 않으면 unknown 필드를 넘겨 준다.

4. 결 론

본 논문에서 인증서를 검증함에 있어서 DNS의 사용에 대하여 논의하였다. DNS를 이용한 검증을 할 경우에 인증서 검증에서 중요하게 다루어지는 적시성과 분산화가 적절히 이루어 질 수 있다는데 큰 장점이 있다. DNS의 동적 업데이트를 통해서 항상 최신의 CRL 정보를 유지할 수 있다. 또, 각 도메인 별로 인증서와 CRL을 관리할 수 있고, 그를 다시 존으로 나눌 수 있으므로 부하를 분산 시킬 수 있다.

하지만 DNS를 CA와 같은 수준으로 보호해야 한다는 단점이 있을 수 있다. 이를 해결하는 해결책을 생각해야 할 것이며, DNS를 통한 경로 검증법을 추가하는 것도 생각해 볼 수 있다.

5. 참고문헌

[1] D. Eastlake, "Domain Name System Security Extensions", rfc2535, 1999. 03.
[2] D. Eastlake, O. Gudmundsson, "Storing Certificates in the Domain Name System (DNS)", rfc2538, 1999. 03.
[3] B. Wellington, "Secure Domain Name System (DNS) Dynamic Update", rfc3007, 2000. 11.
[4] ITU-T , Draft ITU-T RECOMMENDATION X.509 version 4, ITU-T Publications, 2001. 5. 3