FM 부가방송 기반에서의 인증서 유효성 검증에 관한 연구

장홍종[0] 이성은 이정현
행정자치부, 인하대학교
realking@gcc.go.kr

A Study on the Cert-Validation of Certification based on FM Subcarrier Broadcasting

Hong-Jong Chang[0] , Seong-Eun Lee , Jung-Hyun Lee
Dept. of Government Computer Center , MOGAHA

요 약

공개키 기반 인증시스템에서 사용자의 실수로 비밀키가 노출되었거나 자격의 박탈, 유효기간 만료 등의 이유로 인증서를 폐지해야 할 경우가 있다. 이에 따라서 각 사용자는 수신한 인증서가 유효한 것인지를 확인해야만 한다. 이 인증서 폐지 여부를 확인하는 방법으로는 CRL, Delta-CRL, OCSP 등의 방식이 개발되었다. 하지만 이 모든 방식에서의 인증서 유효성 검증은 실시간으로 처리해야 하므로 많은 통신량을 발생시키는 문제점을 가지고 있다. 본 논문에서는 CRL관리의 문제점인 전송시점 차이에 따른 무결성 문제와 실시간 처리로 인한 서버와 네트웍의 과도한 트래픽 발생을 해결한 FM Subcarrier Broadcasting을 이용한 효율적인 CRL 구축 방안을 제안하였다.

1. 서 론

공개키 기반 인증시스템[1]에서 사용자의 실수로 비밀키가 노출되었거나 자격의 박탈, 유효기간 만료 등의 이유로 확인서를 폐지해야 할 경우가 있다. 따라서 각 사용자는 수신한 인증서가 유효한 것인지를 확인해야 하며 이는 인증기관이 폐지된 확인서에 대한 정보를 공개하거나 사용자가 원하는 확인서의 상태를 인증기관에 직접 의뢰를 함으로써 알 수 있다[2]. 이 폐지 여부를 알 수 있는 가장 일반적인 방법으로 확인서 폐지목록(CRL : Certification Revocation List) 방식이 있다. 이 방법은 간단한 반면 확인서 폐지 목록을 다운로드 해야 하며, 파일의 크기가 커지는 단점이 있으며 목록에서 대상이 되는 확인서가 존재하는지 확인해야 하므로 많은 부하가 걸린다. 이를 개선하기 위해 전체 CRL을 다루지 않고 CRL이 발행된 시점에서 새로운 CRL이 발행된 시점까지의 목록을 모아둔 delta-CRL 방식이 있으나 이 또한 이전 목록은 저장하고 있어야 한다. 또한 인증기반의 확산으로 CRL, delta-CRL 모두 전송량이 늘어나고 있으며 전송시간 역시 일정시간의 간격을 두고 이루어지고 있어 많은 문제점이 발생되고 있다. 최근 이들의 단점을 보안하여 실시간으로 전송하도록 개선한 OCSP(Online Certification Status Protocol)라는 새로운 방식이 개발되었다. 하지만 이 방식은 인증서의 유효성 검증을 실시간으로 처리해야 하므로 많은 통신량을 발생시키는 또 다른 문제점을 가지고 있다.

본 논문에서는 이와 같은 CRL 관리의 문제점인 전송시점 차이에 따른 무결성 문제와 실시간 처리로 인한 서버와 네트웍의 과도한 트래픽 발생을 해결한 FM Subcarrier Broadcasting system을 이용한 효율적인 CRL 구축 방안을 제안하였다.

2. DARC

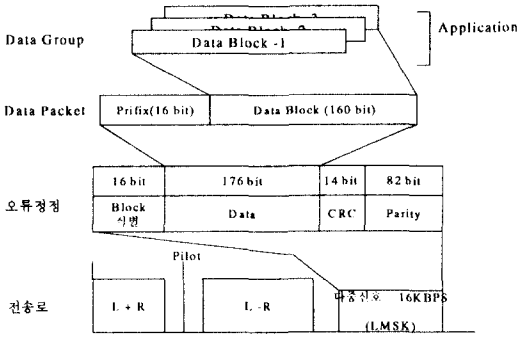
FM 부가방송은 하나의 FM 방송채널에 할당된 대역폭 중 미 사용중인 53~100KHz의 대역에 음성 또는 디지털 데이터를 다중화하여 방송함으로써 FM 방송 수신자에게 부가적인 서비스 즉, 자동공조, 프로그램 자동선국, 시간정보, 교통정보, 날씨정보, 주식동향 등의 실시간 사회정보, 무선호출, 비상경보, 그리고 자동주행 시스템의 교통 데이터 제공등의 높은 부가가치의 서비스를 제공하는 부가적인 방송서비스를 지칭한다[3]. Darc의 계층 구조는 [그림 1]과 같다.

3. CRL전송 및 수신

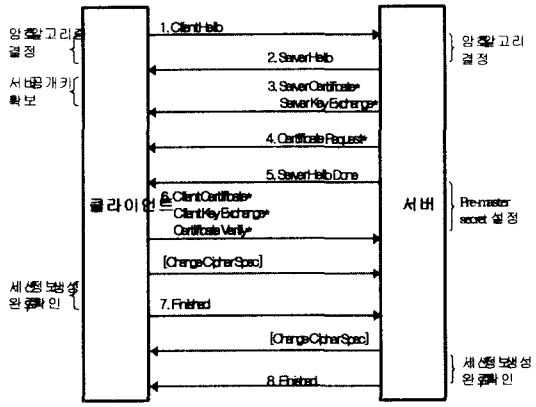
DARC을 이용한 CRL 전송시스템에서 전송될 CRL의 유무를 체크하고 발생 시 CRL을 DARC서버에 송신한다.

인터넷상에서 제공되는 데이터 중에서도 상호보안이 유지되는 상태에서 전송되어야만 하는 경우가 존재한다.

예를 들어 전자상거래나 온라인 뱅킹, 인증기관에 이르기까지 정보가 누출되어서는 안 되는 경우가 있다. 이러한 경우에는 일반적으로 사용되어지는 HTTP Protocol이 아닌 특별한 종류의 Protocol을 필요로 하며, 가장 널리 사용되어지는 방법이 SSL을 이용한HTTP



[그림 1] Darc의 계층구조



[그림 2] CA CRL송신 서버와 DARC서버와의 핸드쉐이크

Protocol이다. SSL 서버에서 제한된 클라이언트에게만 접근을 허용하는 경우에도 사용되어진다.

예를 들어 서버는 클라이언트에게 인증서를 요구할 수 있으며, 클라이언트의 인증서를 바탕으로 하여 접근여부를 판단할 수 있다.

이에 따라 본 논문에서도 DARC서버에 CRL 전송에는 CA의 CRL전송서버와 DARC서버간에 SSL을 이용하여 안전하게 전송한다.

CRL서버를 클라이언트, DARC서버를 서버라 하면 SSL을 이용한 클라이언트와 서버간의 전송 Operation은 크게 [그림 2]과 같은 순서로 이루어진다.

첫째, 클라이언트는 서버에게 Client Hello message를 전송한다.

둘째, 서버는 클라이언트에게 Server Hello message와 서버인증서를 전송하고, 만약 클라이언트인증서가 필요한 경우에 인증서 요청도 함께 전송한다.

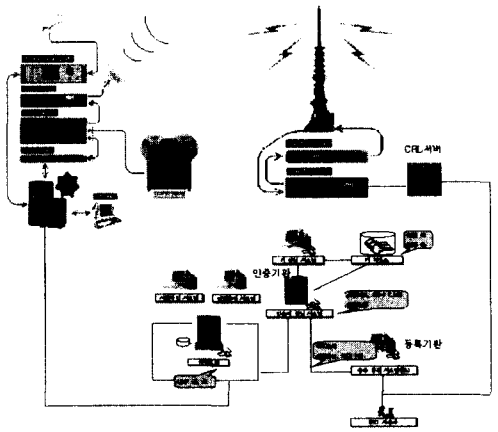
셋째, 클라이언트는 암호화에 사용되는 세션키와 함께 클라이언트에서 지원하는Cipher Suite를 서버로 전송, 서버가 인증서를 요청한 경우에는 클라이언트의 인증서도 함께 전송한다.

넷째, 클라이언트는 Finished message를 서버로 전송하고 데이터 전송단계로 이동한다.

다섯째, 서버는 Cipher Suite를 받아들이고(또는 거부하고) Finished message를 클라이언트로 전송한 후 데이터 전송단계로 이동하고 상호 합의한 Cipher Suite에 의해서 암호화된 메시지를 교환한다.

이러한 절차에 따라 DARC서버에 수신된 CRL은 DARC송신 시스템에 의해 브로드 캐스팅 된다. CRL전송은 1시간 간격으로 전체 CRL을 브로드캐스팅하고 발생하는 CRL은 발생 즉시 브로드캐스팅 한다.

DARC에 의해 브로드캐스팅된 CRL은 DARC 수신기에 의해 수신되고 세션키로 복호화 된 후 데이터베이스에 저장된다.



[그림 3] 제안시스템 구성도

4. 인증서 유효성 검증

데이터베이스화된 CRL은 수신된 인증서의 확인을 위해 사용된다. 전송된 인증서의 유효성을 검증하기 위해서는 현재상태의 CRL을 필요로 한다. 인증서 발급번호로 로컬 데이터베이스에 저장된 CRL을 확인하고 인증서의 유효성 여부를 확인한다. 본 논문에서 제안하는 시스템의 구성도는 [그림 3]과 같다.

5. 실험 및 평가

5.1 기본가정

본 논문에서는 통신량을 분석할 때 필요한 인증기관의 구성은 하나 이상의 인증기관이 존재할 수 있다고 가정하며 디렉토리는 각 인증기관에 속해 있을 수도 있다. 즉, 인증기관과 디렉토리간 또는 사용자와 디렉토리간의 통신량을 생각 할 때 어느 특정 디렉토리를 대상으로 하는 것이 아니고 전체 디렉토리에 대해서 네트워크 상에서 발생되는 통신량을 고려한다. 즉, 디렉토리가 전체에 하나가 있다고 가정하는 것과 동일하다. 발생되는 통신량을 분석하기 위해 <표 1>과 같은 표기를 사용하며 1일을 기준으로 통신량을 나타낸다. 일반적으로 인증서가 폐지되는 비율은 10% 정도로 한다[4].

<표 1> 표 기

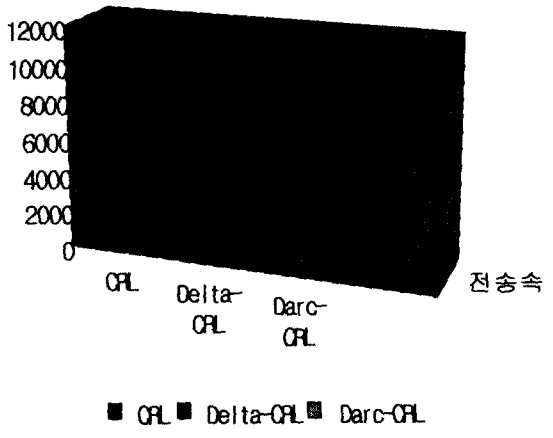
n	전체 총 인증서의 수
k	한 인증기관에 속한 평균 인증서 수
p	폐지되는 인증서의 비율
r	폐지된 인증서의 수 (r=n×p)
T	폐지 리스트의 1일 갱신 횟수
l	인증서의 일련번호를 나타내는 비트 수
q	사용자들이 인증기관에 인증서의 유효 여부를 질의하는 횟수(1일)

5.2 실험 및 평가

요구되는 통신량을 계산해보면 인증기관과 디렉토리사이에는 하루에 폐지된 인증서에 대해서 갱신 횟수만큼 목록을 전송해야 하므로 T×r×l=T×n×p×l 만큼의 비트를 전송해야 하며 디렉토리가 1일 동안 사용자들에게 전송해야 하는 양은 q×p×k×l 비트이다.

한 인증기관에 속한 평균 인증서 수가 3,500만건 취소되는 인증서의 비율을 10% 라고 하면 취소되는 인증서의 수는 350만건, 취소리스트의 1일 갱신 횟수를 12회, CRL의 크기를 35byte, 사용자들이 인증기관에 확인서의 유효여부를 질의하는 횟수를 350만회라 하면 기존의 CRL 방식의 전체 전송량은 350만×0.1×3,500만×35byte= 428.75 Tbyte 이다. 10Mbps로 전송한다면 전체전송시간은 11,909시간이다. 또한 delta-CRL 방법으로 전송 시에도 전체 전송량 중 시간당 145,833건 발생하고 이를 다시 24시간을 기준으로 계산하면 18Tbyte 가되며, 만약에 10Mbps로 전송한다면 전체 전송시간은 496시간이다. 실제의 전송속도는 네트워크 부하나 시스템의 부하에 의해 더욱더 나쁜 결과를 도출한다.

본 논문에서 제안한 방법은 인증서가 폐지될 때마다 실시간으로 전송되고 한번의 전송으로 가정한 350만의 사용자에게 브로드캐스팅 되므로 실제 전송량은 350만건 × 35byte = 122.5Mbyte이다. 16Kbps로 전송 시 2시간 13분이면 전송을 완료 할 수 있다. 이것은 시간당 145,833건의 CRL이 발생한 것과 같으며 이것의 전송은 약 5.4분만에 전송이 가능하다. 이 들의 전송시간을 비교 도식화하면 [그림 4]와 같다. 또한 검증을 위해 폐지목록을 다운 받기 위한 대기시간 없이 즉시 검증이 가능하다. CRL과 delta-CRL은 전송주기에 따른 자료의무결성이 발생하나 본 논문에서 제안한 방법은 실시간으로 인증서의 유효성을 검증할 수 있다. 또한 CRL의 확장필드를 이용하여 그룹을 분리하여 이용자가 필요한 그룹을 선택적으로 수신할 수 있어 이용자에게 더욱더 효율적인 방법을 제공할 수 있다.



[그림 4] 전송시간 비교도

예를 들어 전자상거래를 하는 기업이 주고객의 CRL를 직접 보관 관리 운영함으로써 주고객의 신뢰성을 사전에 확보하고 상거래를 함으로써 고품질의 서비스가 가능하다. 이를 위한 프로파일은 <표 2>와 같이 구성하였다.

<표 2> Darc-CRL 프로파일 추가 부분

Field	C	CRL	비고
darcCRLGroup	O		추가
CRLGroupIdentifier			추가
FrequencyIdentifier			추가
CRLClassification			추가

(1) darc 사용 확인 필드(Darc CRL Group)
darc의 사용 유무를 확인한다. 이 필드는 시스템 구성에 따라 사용여부를 결정한다.

(2) 그룹 분류를 위한 필드(CRL Group Identifier)
이 필드는 CRL이 필요한 그룹을 분리 서비스가 가능하도록 한다.

(3) 주파수 구분 필드 (Frequency Identifier)
주파수 대역의 확인용 필드이다.

(4) CRL 구분 필드(CRL Classification)
이 필드는 CRL 과 Delta-CRL을 구분하는 필드이다.

6. 결 론

본 논문에서는 CRL관리의 문제점인 전송시점 차이에 따른 무결성 문제와 실시간 처리로 인한 서버와 네트웍의 과도한 트래픽 발생을 해결하기 위하여 DARC를 이용한 인증서 유효성 검증방안을 제안하였다. 또한 현재 제안되어진 인증서 유효성 검증방법의 장단점을 분석하여 각각의 단점을 배제하고 장점을 수용한 방법을 제안함으로써 효율적인 인증서 유효성 검증 체계를 제안하였다.

참 고 문 헌

[1] ITU-T Recommandation X.509 (1997) ISO/IEC 9594-8 . 1997, Information Technology -Open Systems Interconnection The Directory : Authentiation Framework, 1997.

[2] IETF, Online Certification State Protocol

[3] Linda Zeger, "Analysis and simulation of Multipath Interference of FM Subcarrier Digital Signal" Proc. of the third IEEE Symposium on Computer and Communication, pp. 35-41, June 1998.

[4] S. Micali, Efficient Certificate Revocation Technical Memo MIT/ LCS/TM-524b, 1996.