인트라넷 환경을 위한 PKI 인증서 유효목록 검증 시스템에 관한 연구

김종권
고려대학교 컴퓨터정보통신대학원 디지털정보미디어공학과
e-mail : happytg2@gmail.com

A Study on the list of valid PKI certificate verification system for intranet environments

Jong-Kwon Kim
Dept. of Digital Information & Media Engineering ,
Graduate School of Computer & Information Technology, Korea University

요 약

기 구축된 Public Key Infrastructure(이하 PKI) 에서 발급된 디지털인증서를 외부 네트워크와 단절된 인트라넷 환경에서 사용하기 외부 네트워크에 지정된 인증서 검증 서버에 접속할 수가 없기 때문에 인증서 유효성 검증의 문제를 발생시켜 사용이 불가능하다. 이러한 문제점을 해결하기 위해 인트라넷 환경을 위한 인증서유효목록 검증 시스템을 제안한다. 인증서유효목록 검증 시스템은 기존의 PKI 에서 인증서 검증을 위해서 사용하는 Certificate Revocation List (이하 CRL)를 대체하는 Certificate Valid List (이하 CVL)를 사용하여 외부 네트워크와 접속이 단절된 인트라넷 환경에서도 기 구축된 PKI 에서 발급된 디지털 인증서의 유효성을 검증할 수 있다. 인증서유효목록 검증 시스템은 CVL 의 생성을 위한 Certificate Valid List Manager (이하 CVLM)와 주기적인 CVL 발급 및 게시를 위한 Certificate Valid List Issuer (이하 CVLI), 응용서비스에서 사용하는 User Agent (이하 UA) 를 포함한다.

1. 서론

PKI 란 개방형 또는 분산형 네트워크 시스템에서 보안 요구사항을 만족시키기 위해 만들어진 인증 암호체계 기반의 구조이다. 이 인증체계는 이미 국내외에 구축되어 이용되고 있으며, 특히 국내에서는 많은 사용자가 공인인증기관으로부터 인증서를 발급받아 인터넷 뱅킹, 전자문서결재, 보험서류서명 등 다양한 분야에서 이용하고 있다.[1]

PKI 에서 공개키와 개인키는 같은 알고리즘을 통하여 한 쌍으로 동시에 만들어지며, 개인키는 사용자에게 주어지고 공개키는 상기 디지털 인증서에 포함된 정보로 공개된다. 개인키를 이용하여 예컨대 어떤 데이터에 서명을 하면, 반드시 쌍이 되는 공개키로만 검증이 가능하므로 개인키 소유자만 할 수 있는 전자서명이 된다. 따라서 본인 인증과 정보에 대한 무결성 검증 및 본인 실행에 대한 추후 부인방지 등이 가능하게 된다. 여기에서 본인에 대한 확인은 공개키가 포함된 상기 디지털 인증서의 소유자가 누구인지를 통해 확인이 가능하다. [4]

이러한 PKI 인증서 기반의 사용자 인증은 현재 각종 서비스에서 흔하게 적용되어 있다. 그리하여 사용자는 인증서를 통하여 본인임을 확인시켜줌으로써, 그 사용자에게 부여된 권한에 따라 각종 서비스를 수행할 수가 있게 된다.

문제는 이러한 과정 중에서 상대방의 디지털 인증서가 유효한 지에 대한 검증이 불가능할 경우이다. 디지털 인증서에 대한 검증을 수행하지 않을 경우 마치 실제 유효한 인증서와 같은 가짜 인증서를 만들어 제공함으로써 상대방이 실제 당사자인 것처럼 믿게 할 수 있다. 가짜 인증서를 만드는 방법은 인터넷 등에 게시된 많은 도구와 방법을 이용할 경우 어느 정도의 지식을 가진 사람은 구현이 가능하다.

인터넷 접속이 가능한 온라인 상태에서는 공인인증기관 등 각종 디지털 인증서 관련 서비스를 하는 기관에서 인증서의 유효성에 대한 확인이 가능하도록 서비스를 제공하고 있다. 이러한 서비스를 이용하여야만 실제 전자서명을 수행한 상대방이 유효한지에 대한 확인이 가능하다.

실제 공인인증기관 또는 정부인증기관등 인증기관에서는 이러한 서비스를 위하여 CRL 을 주기적으로 생성하여 게시하거나, Online Certificate Status Protocol(이하 OCSP) 를 통해 인증서의 실시간 상태 확인을 수행해 준다. [5][8]

CRL 이란, 유효기간이 남아 있는 전체 인증서 중에서 여러 가지 이유로 이용할 수 없는 인증서의 정보들을 리스트로 만들어 발급 인증기관의 전자 서명키로 서명하여 게시하는 것으로 보통 1~2 일 정도의 유효기간을 가지고 있다. 이에 따라 거의 비슷한 주기

로 발급을 한 다음 특정 URL 또는 LDAP 등에 게시하도록 하고 있다.

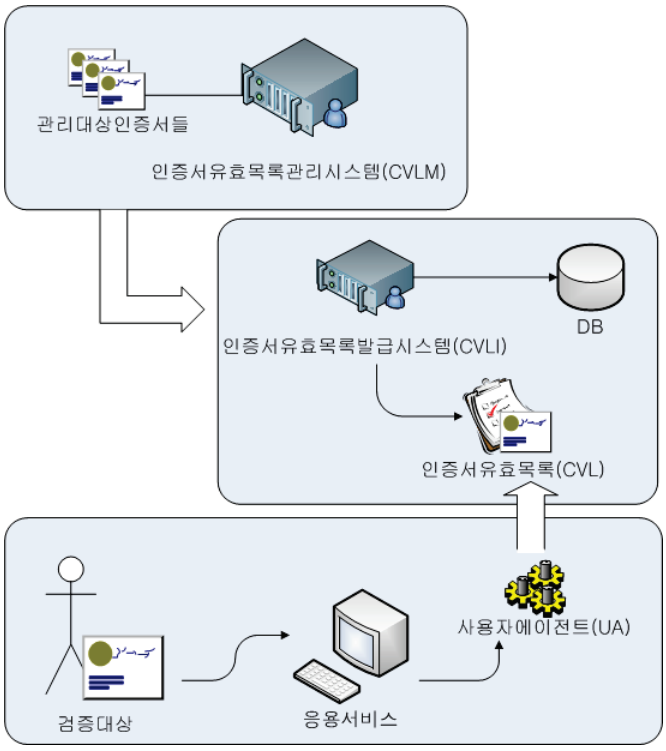
그러나, 인트라넷과 같은 외부와 단절된 네트워크 환경에서는 이러한 서비스를 받을 수 없으며, 따라서 디지털 인증서 기반의 각종 서비스를 원래의 목적한 바대로 수행할 수 없게 되는 것이다.

일반적으로 인증시스템이 인증서폐지목록을 운영하는 이유는 발급한 인증서의 개수가 많으며 유효한 인증서가 유효하지 않은 인증서보다 많기 때문에 효율적이기 때문이다. 또한 인증서폐지목록에는 순수한 폐지 정보뿐만 아니라, 효력정지, 폐지 사유 등 다양한 정보가 들어가 있어 추가적인 활용이 가능하다. 그러나 인트라넷에서는 이러한 인증서폐지목록을 이용하기에는 적절치 않다. 외부 망으로부터 주기적으로 다운로드 하여 내부 망으로 전달하는 것도 쉽지 않을 뿐 아니라, 다양한 내부 망 서비스를 위해 특정 위치에 게시하는 것도 인증서 내부의 인증서폐지목록 참조 값과 일치하지 않으므로 쉽지 않다. 또한 별도로 인증서폐지목록을 내부에서 생성하여 처리하는 것도 인증서폐지목록 대상 전체를 알아야 하므로 불가능하다.

본 논문에서는 외부의 접속이 원활치 않은 인트라넷 환경에서 기 발급된 디지털인증서의 유효성 확인을 할 때에 효과적으로 적용할 수 있는 시스템 및 방법을 제안하고자 한다.

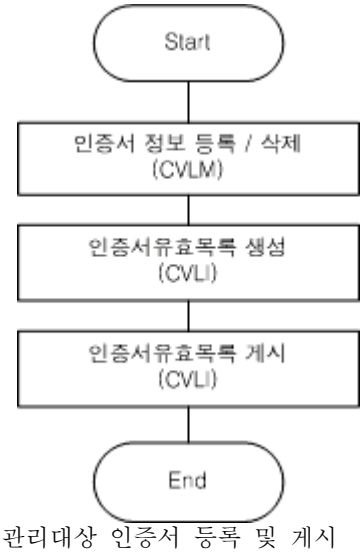
본 논문의 구성은 다음과 같다. 2 장에서는 본 논문에서 제안하는 인증서유효목록 검증 시스템의 구성 및 업무흐름을 설명하고 4 장에서는 결론을 맺는다.

2. 인증서유효목록 검증 시스템 구성



(그림 1) 인증서유효목록 검증 시스템 구성도

(그림 1) 을 참조하면, 본 논문의 시스템은 CVLM, CVLI 및 UA 로 구성된다. 본 시스템의 사용자는 이미 PKI 기반의 인증체계에서 발급받은 인증서를 소유한 자이다. 또한, 본 논문의 시스템을 이용하는 응용서비스와 응용서비스가 검증하고자 하는 검증 대상과 검증 대상의 인증서 등이 있다.

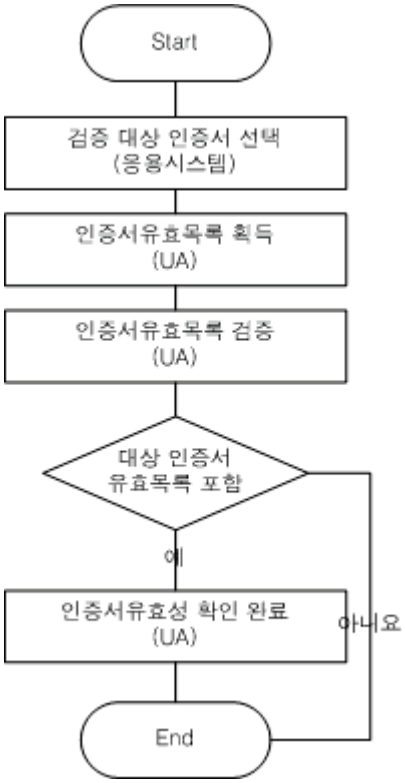


(그림 2) 관리대상 인증서 등록 및 게시

(그림 2) 를 참조하면, 상기 CVLM 를 통해 관리자는 관리 대상 인증서들을 CVLI 에 등록한다. 이 때 등록하는 것은 인증서 자체를 등록할 수도 있고, 인증서 정보일 수도 있다. 여기서 인증서 정보란 유효인증서목록 생성에 필요한 인증서 구별 정보들로서, 인증서의 발급자 정보와 인증서의 시리얼번호 등이 대상이 될 수 있다. 또는 인증서 구별 정보로는 인증서 자체 또는 인증서 내부 공개 키를 해시 함수를 이용하여 산출한 해시 값일 수도 있다. 또한 CVLM 은 CVLI 와 독립된 별도의 시스템이거나 또는 CVLI 의 일부로서 등록 기능을 수행하는 모듈일 수 있다. 또한 관리자는 CVLI 를 통해 필요에 따라 새로운 인증서 또는 인증서 구별 정보를 등록할 수 있으며 또는 기 등록된 인증서 또는 인증서 구별 정보를 CVL 생성의 대상에서 제외될 수 있다. 상기 CVLI 는 전달받은 인증서 또는 인증서 구별 정보를 Database 등을 통해 관리한다. 인증서가 전달되었을 경우에는 인증서로부터 인증서 구별 정보를 획득해 놓는다. 발급 주기가 되면 CVLI 는 CVL 발급 대상이 되는 모든 인증서 구별 정보를 모아 CVL 로 발급하고 특정 위치에 게시한다. 여기서 특정 위치란 UA 가 접근 가능하고 미리 알고 있는 위치를 말하며 웹 서비스, FTP 서비스, LDAP 등의 다양한 방법을 이용할 수 있다. 또한 CVLI 에 직접 접속하여 획득할 수도 있다.

(그림 3)을 참조하면, 상기 UA 는 응용 서비스로부터 전달 받은 인증서 검증 대상의 디지털 인증서가 유효한지를 상기 CVLI 가 게시해 놓은 CVL 를 통해 확인한다. 응용 서비스는 UA 의 인증서 검증을 통해 유효 여부를 확인한 후 서비스 제공 여부를 판단하게 된다. 이때 UA 입장에서는 CVL 의 전자서명 자체의 유효성을 확인할 수 없는 문제가 발생하게 된다. 이

러한 문제는 UA 가 CVLI 의 인증서 또는 인증서 정보를 기 획득해 놓음으로써 해결이 된다. 즉, UA 가 가지고 있는 신뢰할 수 CVLI 의 인증서로 전자 서명된 CVL 을 신뢰할 수 있게 된다.



(그림 3) 검증 대상 인증서 유효성 검증

상기 CVL 의 구성은 유효기간, 다음 발급 일시, 발급 대상이 되는 인증서 구별정보 목록 등으로 이루어질 수 있으며, 발급자인 CVLI 의 전자서명을 추가함으로써 구성된다.

추가적으로 CVL 에 대한 설명과, 발급시리얼번호, 정책 정보 등이 포함될 수 있다.

3. 결론

외부 네트워크와 단절된 내부 인트라넷 시스템에서 PKI 시스템을 사용하고자 할 경우에는 인트라넷 내부에 별도의 PKI 시스템을 구축해야만 한다. 하지만 본 논문에서 제안하는 인증서유효목록 검증 시스템에 따르면 기 구축된 PKI 시스템에서 발급된 인증서의 유효성 검증을 인트라넷 내부에서 지원할 수 있다. 이미 구축되어 운영되고 있는 PKI 시스템의 자원을 그대로 활용할 수 있으며 내부 정책에 따라 특정 인증서의 사용을 제한할 수 있는 장점이 있다.

하지만, 시스템의 규모가 중소형 이상일 경우 유효한 인증서의 수가 너무 많아지기 때문에 효율성이 떨어질 수 있다.

본 논문에서 제안하는 인증서유효목록 검증 시스템은 특수한 목적을 가진 중소형 인트라넷 시스템을 구축하고 내부 사용자에 대한 인증을 기 구축된 PKI 시스템의 자원을 그대로 사용하고자 하는 경우 대안이 될 수 있을 것이다.

참고문헌

[1] 정연호,최원석,권태경,이광수.[국내 PKI 구축 현황 및 기술], {정보보호학회지}.제 17 권 제 6 호. 한국정보보호학회, 2007.12.

[2] 정은희,김학춘,이병관.[Local CA 를 이용한 최적화된 PKI 설계],{한국인터넷정보학회 학술발표대회 논문집}.제 7 권 제 1 호. 한국인터넷정보학회, 2006

[3] 최인환 ,채병수 ,차홍준.[인증서 유효성 검증시 CRL 과 OCSP 방식의 문제점 제안],{기초과학연구}. 제 17 권.강원대학교 기초과학연구소,2006

[4] Carlisle Adams and Steve Lloyd, Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition, 2002.

[5] IETF RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", 1999.

[6] IETF RFC 2510, "Internet Public Key Infrastructure Certificate Management Protocol", Mar. 1999.

[7] IETF RFC 2527, "Internet Public Key Infrastructure Certificate Policy and Certification Practies Freamework", Mar. 1999.

[8] IETF RFC 2560, "X.59 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP", Jun. 1999.

[9] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile, RFC3280,2002