무선 Ad Hoc 통신망 기반 유·무선 PKI 통합 모델에 관한 연구

김동욱[0] 남길현
국방대학교 전산정보학과
donoh@freechal.com, khnam@kndu.ac.kr

A Study on the End-to-End Certification PKI system based on the Wireless Ad Hoc Networking

Dong-Wook Kim[0] Kil-Hyun Nam
Dept. of Computer & Information Science, Korea National Defense University

요 약

인터넷과 개인휴대통신의 발달과 더불어 유·무선 인증서비스는 PKI를 기반으로 다양하게 구현되고 있다. 그러나 유·무선이 혼재된 형태의 통신망에서 Client간의 통신에 필요한 인증체계에 대한 연구는 초기단계이며 특히, Ad Hoc 통신망과 같이 가변적인 Topology를 형성하는 특수한 상황에서 지속적인 인증서비스를 제공할 수 있는 연구는 미미한 실정이다. 국가비상사태와 같은 긴급을 요하는 상황에서 신속히 구성되는 무선 Ad Hoc 통신망을 기반으로 한 인증체계를 구축하기 위하여 인증서 검증모델을 중심으로 유·무선PKI 통합모델을 제안한다.

1. 서 론

인터넷의 급성장에 따라 전자상거래(e-Commerce)에 대한 시장의 규모 또한 급격히 증가하고 있으며, 이러한 전자거래에 대한 안전성 및 거래당사자에 대한 신원확인을 보증할 수 있는 인증서비스는 PKI(Public Key Infrastructure) 인증체계의 형태로 자리를 잡아가고 있다.

정부도 국가 IT 산업의 한 축으로서 전자정부구현이라는 기치아래 전자서명법과 같은 선진 법 제도를 정비하여 전자거래에 대한 제도적 기반을 마련하기 위해 그 역할에 충실하고 있으며, G-PKI(Government-PKI) 구현을 통해 행정정보의 공유, 전자 민원서비스의 활성화를 추구하고 있다.

국방분야의 경우에도 21세기 정보화 군의 핵심적인 정보보호 체계로써 PKI 인증체계에 대한 필요성이 꾸준히 제기되어 왔으며, 근래 「국방전자정보 인증체계」로 구체화되고 있다. 그러나 국방정보체계의 다양한 운영환경과 전장이라는 특수한 상황을 충분히 고려한 인증체계 모델은 아직도 명확하게 그려지지 않고 있다.

특히 무선PKI에 대한 연구는 민간의 경우에도 최근에 이르러 제도적, 기술적 틀을 잡아가고 있으나 고정된 제어장치 없이 동적Host간에 무선 단대단 접속으로 Topology를 구성하는 Ad Hoc 통신망의 전형적인 형태인 국방무선환경은 상용 무선 PKI 체계를 그대로 적용하기에는 많은 제한사항이 따를 것으로 생각된다. 또한, 국방 통신환경이 평시-유선기반, 전시-무선기반과 같이 유·무선이 혼재된 형태로 운용될 경우 다양한 요구사항이 추가될 것이다.

그러므로 「국방전자정보 인증체계」는 기본적으로 전시와 같은 특수한 상황에서도 기동성 및 생존성을 확보할 수 있고, 유·무선의 구별없이 동일한 서비스를 중단없이 제공할 수 있는 다양한 정책적, 기술적 기반구조를 가져야 할 것이다.

본 논문에서는 국방통신 환경과 유사한 무선Ad Hoc 통신망에서의 유·무선PKI 통합모델 구축방안을 제안하고자 한다. 2장에서는 현재 활발히 표준화 및 상용화가 진행중인 무선PKI 정보보호 모델과 무선PKI 인증서 검증 권고사항인 OCSP(Online Certificate Status Protocol)에 대해 살펴보고 3장에서는 Ad Hoc 통신망을 간략히 설명하면서 4장에서 상황 변화시 유·무선의 운영환경의 제약을 극복하고 중단없는 인증서비스를 제공하기 위해 인증모델, 인증서 검증모델, 무선에서의 인증서 검증 프로토콜을 제안하면서 5장에서 결론을 맺는다.

2. 무선PKI 정보보호 모델

무선망은 일반적으로 유선망보다 물리적 보안 위협에 더 많이 노출되어 있으며 훨씬 낮은 대역폭을 가진다. 또한 무선망은 유선망보다 통신 에러율이 비교적 높을 뿐 아니라, 상용 무선망은 Cellular phone을 기본 단말기로 사용하기 때문에 CPU 및 memory의 사용이 극히 제한적일 수밖에 없다. 이런 이유로 유선PKI와는 구별되는 무선PKI 체계가 필요하며, WAP과 (M)ME로 대표되는 무선 프로토콜을 기반으로 정보보호 모델이 제공되고 있다.

2.1 WAP(Wireless Application Protocol) : WTLS

WAP의 정보보호는 유선의 SSL(Secure Socket Layer)에 대응하는 WTLS(Wireless TLS)에서 담당하고 있다. WTLS는 IETF의 TLS(Transport Layer Security)를 기반으로 무선환경에 적합하도록 개발된 보안 프로토콜이다.[1] TLS는 단말의 성능을 고려하여 여러 가지 관련 파라미터의 길이를 줄였으나 TLS를 기본으로 설계되었기 때문에 SSL과 큰 차이는 없으며, 데이터 무결성, 기밀성, 인증, DoS 보호 기능을 가지고 있다.

그러나 이동통신 단말기의 제약을 극복하고 귀중한 무선자원을 절약하도록 설계된 WAP은 HTTP, TCP 등 기존 인터넷 표준의 프로토콜을 사용하고 있지 않고 HTML과의 상호 교환성 및 화상 표시는 지원하고 있지 않기 때문에 WML로 변환하기 위한 Gateway가 반드시 필요하다. 이 때문에 WAP 서비스에는 시스템 구축에 필요한 비용이 증가하고, 서비스가 제한적이며 특히 데이터 변환시 Gateway상에서 암호화된 자료가 복호화 되는 문제점을 가지고 있다.

2.3. ME(Mobile Explorer) : SSL/TLS

마이크로소프트사에서 개발하여 현재 상용화된 ME v1.0은 보안프로토콜을 탑재하지 않고 있다. ME는 HTML 언어 전체를 사용하지 않고 일부만 사용하므로 일반 HTML 브라우저에서 지원되는 모든 것들이 지원되지는 않지만 기존의 컨텐츠를 사용할 수 있어 호환성이 뛰어나다. 내부적으로 기존의 HTTP 방식과 호환이 되도록 하고 있으며 HTML을 축약한 M-HTML을 사용하고 있다. 보안 매커니즘은 HTTP에 기반이므로 유선 인터넷에서 사용되고 있는 SSL/TLS 매커니즘의 수용이 가능하다.[2] 국내의 경우 무선 인터넷의 전자상거래 서비스를 위하여 SSL 3.0을 자체 개발하여 적용하였으며 국내 블록암호알고리즘인 SEED를 추가 구현하였다. 인증서는 X.509 v3를 사용하고 있으나 현재 ME의 SSL은 Server 인증만을 제공하고 있으며, 사용자 인증은 제공하고 있지 않다.[3]

2.4 온라인 인증서 상태확인 프로토콜 (OCSP : Online Certificate Status Protocol)

현재 표준화가 진행중인 국내 무선PKI에서는 인증서 상태정보를 확인하는 일반적인 방법인 CRL(Certificate Revocation List) 대신에 OCSP 서버의 사용을 권장하고 있다. OCSP는 인증서 검증을 필요로 하는 사용자가 CRL을 Download 받지 않고 실시간으로 인증서 상태를 확인할 수 있는 방법이다.[4] 그러나 CRL은 즉각적으로 인증서 상태를 반영하기가 힘들고, 대량의 CRL을 획득하고 처리하는 절차로 인해 네트워크에 부하를 가져오게 된다. 아울러 사용자는 고유의 CRL 데이터베이스 목록을 유지하여야 하기 때문에 사용자 단말기에도 부하를 동반하게 된다. 특히 일정 금액이상의 자금이체나 많은 양의 주식거래 경우 인증서의 상태를 실시간으로 조회할 수 있는 대안이 필요하게 되었다. [5]

OCSP는 요청, 응답, 응답메시지 검증의 3단계를 거치게 되며 각각의 단계에서 필요한 요구사항이나 에러 발생원인은 아래와 같다.

제1단계 : 요청(request)
- 메시지가 정상적으로 구성되었는지 여부
- Server 설정의 적절성
- Server가 요구하는 정보들의 포함 유무

제2단계 : 응답(response)
- 올바르지 않은 요청(MalformedRequest)
- 내부적 에러(InternalError)
- 이후 다시 시도(TryLater)
- 사용자 서명 요구(SigRequired)
- 사용자 인증 불가(Unauthorized)

제3단계 : 응답메시지 검증
- 요청 및 응답메시지의 인증서 식별자 확인
- 요청메시지의 서명의 유효성 판단
- 요청 및 응답메시지 Server의 동일성
- Server의 유효성
- 응답메시지에 표시된 시간(ThisUpdate)의 적절성
- 응답메시지에 표시된 변경시간(NextUpdate)의 적절성

OCSP는 사용자가 응답메시지를 확인하기 위해서 Server의 인증서를 확인하는 몇 가지 방법을 제안하고 있다.
- Server의 인증서를 Short-lived Certification으로 발행하거나 인증서를 자주 재발급한다.
- 인증기관은 Server 인증서 내에 검증방법을 명시할 수 있다. (CRL 분배점 등)
- 인증기관이 Server 인증서의 취소 여부를 확인하기 위한 특별한 방법을 제시하지 않는다. 이 경우, 사용자는 정책에 따라 Server 인증서의 상태를 확인할 것인지 결정해야 한다.

3. 무선 Ad Hoc 통신망

Ad Hoc 망은 중앙집중화된 관리나 표준화된 지원서비스의 도움 없이 임시망을 구성하는 무선 이동 호스트의 집합이다. 즉, 접속점이나 Server없이 주어진 영역안에서 여러 호스트들끼리 빠른 시간에 Self-organizing한 망이다. 이러한 망은 백본 호스트나 다른 이동 호스트로의 연결을 제공하기 위한 고정된 제어장치를 갖지 않으며, 각 이동 호스트가 라우터로 동작하여 이동 호스트로부터의 패킷을 다른 이동 호스트로 전달한다. 한 개 이상의 경로를 형성하는 이동 호스트가 다른 곳으로 이동함으로써 해당 경로를 무효화시키기 때문에 이러한 망에서의 통신 연결은 상당히 취약하다.

Ad Hoc 망은 그 특성상 임시 구성용 망이나 재해, 재난지역이나 전장 등의 기반시설이 갖추어져 있지 않은 환경에 적합한 것으로 연구되어 왔다. 따라서 주로 군사용이나 백업용 망으로서의 역할에 중점을 두어 연구가 진행되어 왔다. 대표적인 Ad Hoc 망 모델로서 미국의 DARPA에서 추진해온 GloMo(Global Mobile Information System) 프로그램은 이러한 역할로서의 Ad Hoc 망에 대한 개념을 잘 수용하고 있다. 최근 IETF의 MANet WG에서는 인터넷 프로토콜내에서 독자적으로 구성 가능한 이동망을 지원하는 라우팅과 인터페이스에 대한 표준화를 진행하고 있다. [6]

4. 유·무선PKI 통합모델

급박한 환경에서 가설된 무선 Ad Hoc 통신망에 필요한 무선PKI의 특징을 살펴보면 아래와 같다.
- 단말기의 성능에 대한 제약은 유선과 동일하므로 상대적으로 낮은 대역폭과 높은 에러율에 대한 고려가 요구된다.
- 무선체계에서는 메시지(명령)전파와 같은 단방향 전송시 Server(수신자) 인증보다 Client(송신자) 인증이 필요하다.
- 유·무선 통신체계가 혼재되어 있으며, 긴급을 요할시 주로 무선 Ad Hoc 통신망으로 운용된다.
- 가용성(생존성)이 보장되어야 한다.

이러한 무선PKI의 요구사항을 만족하면서 유선에도 적용할 수 있는 유·무선PKI 통합모델을 인증서 검증 메카니즘을 중심으로 제안한다.

4.1. 인증 레벨

인증레벨은 WTLS에서 정의한 anonymous, Server Authentication only, Client-Server Authentication에 Client Authentication only를 추가하였다. 이것은 앞서 무선 Ad Hoc 통신망의 특징에서 설명한 것처럼 메시지 전파와 같이 단방향 전송에 따른 Client(송신자) 인증만이 필요한 경우 기존의 Client-Server Authentication에서 불필요한 Server(수신자) 인증을 제거함으로써 네트워크의 부하를 줄여 낮은 대역폭과 높은 에러율에 대한 제한사항을 부분적으로 극복할 수 있다.

또한 통신망 연결에 필요한 보안프로토콜은 다양한 통신체계에 공통적으로 운용할 수 있는 SSL/TLS를 준용함으로써 유·무선간 보안채널의 단대단(End-to-End) 보안을 보장한다.

4.2. 인증서 검증 모델

CA Directory Server의 CRL에 대한 접근은 OCSP Server를 포함한 각종 Server 및 기타 가용한 Client로 제한하여야 하며, 이를 고려한 정책적인 결정이 필요하다. 필요시 Directory Server를 RA등에 분산 설치하여 운용 할 수 있으나 OCSP

Server를 운용하는 체계에서는 별로 효율적이지는 못할 수 있다.

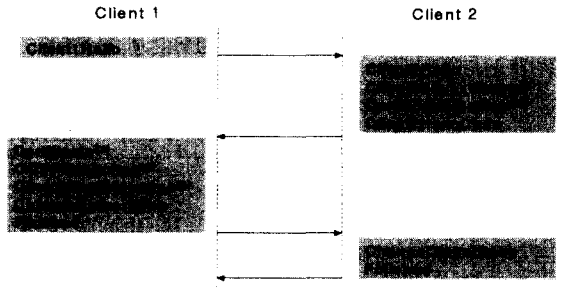
OCSP 응답메시지에는 인증서를 발행한 인증기관의 비밀키나 OCSP Server의 비밀키로 전자서명이 되어있기 때문에 위조가 불가능할 뿐 아니라, 수신측에서 즉시 확인할 수 있는 장점을 가지고 있다. 물론 CA가 발행한 인증서도 CA의 비밀키로 서명되어 있기 때문에 인증서에 대한 최소한의 신뢰성은 보장해 줄 수 있으나, Client 인증서의 변경주기가 대부분 1년 정도의 유효기간을 가지고 있기 때문에 전시 또는 유사시와 같은 급변하는 운용환경에 적용하기 어려울 것으로 판단된다.

본 논문에서는 메시지를 보내는 쪽에서 자신의 인증서에 대한 OCSP 응답메시지를 포함하여 송신하는 방법을 Short-lived OCSP로 명명한다. OCSP response Spec의 Single Response는 Update 시간을 기록하게 하였으며, 정책결정을 통해 이 시간을 기준으로 일정시간 동안 인증서가 유효한 것으로 판단하고, 필요시 수신측에서 CRL이나 OCSP 서버를 통해 인증서 검증을 실시한다. 이것은 CA가 전체 Client에 Short-lived Certification을 발행하는 것과 동일한 효과를 가질 수 있으며, 동일한 메시지의 동일한 인증서를 수신하는 n개의 수신측 Client들이 각각 CRL을 download하거나 OCSP Server에 접근해야하는 번거로움을 없앨 수 있으므로 네트워크의 부하도 줄일 수 있다. 아울러, 긴급한 상황에서 무선 Ad Hoc 통신망의 특성상 topology의 변화 등으로 인해 CRL이나 OCSP Server에 대한 접근이 불가능할 경우 망복구에 필요한 일정시간 동안에도 운용이 가능하다.

이러한 Short-lived OCSP Certification을 적용하기 위한 제한사항으로는 동일한 OCSP Server의 사용이 보장되지 않을 경우 OCSP Server의 키 쌍을 CA에서 동일하게 생산하여 분배함으로써 국방PKI와 같은 특수한 환경에서 정책적으로 서명용과 암호화용 메커니즘을 분리할 경우 암호화용 공개키 인증서에 대한 Short-lived OCSP Certification의 적용은 별도의 Handshaking 과정을 통해 제한적으로 이용이 가능할 것이다.

4.3 인증서 검증 프로토콜

Short-lived OCSP Certification 검증 프로토콜은 SSL Handshaking 프로토콜을 최적화하여 사용하며 <그림 1>과 같이 간략하게 표현하였다. Client1, 2는 특정 메시지에 대한 송신측과 수신측이다.



<그림 1> Short-lived OCSP Certification 검증 프로토콜

(1) Client2KeyExchange :
Session Key 암호화를 위한 Server의 공개키 전송
(2) CertificateRequest : Client1의 인증서를 요구
(3) Certificate : Client1 X.509 인증서를 전송
(4) OCSPResponse : Client1 OCSP 응답메시지를 전송
(5) Client1KeyExchange : Client1의 공개키 전송

5. 결 론

현재 공인인증기관은 유선통신망을 대상으로 인증서비스를 제공하고 있다. 현재 표준안이 마련된 무선PKI 체계가 기존의 유선PKI 체계와 어떠한 형태로 상호인증체계가 마련될지 불투명한 상태지만 정부PKI의 경우에는 유선PKI로 한정될 것으로 판단된다. 그러나 국방부분의 경우에도 이러한 상용기술 및 표준안을 여과 없이 도입할 경우 유선과 무선환경이 혼재되어 있는 통신체계로 인해 이원화되어야 할 것이다. 그러나 본 논문에서 제시하고 있는 유·무선 PKI 통합모델은 이러한 제약을 넘어 일원화된 인증서비스를 제공하고자 하였다.

Client Certification Only를 통해 필요한 수준의 적절한 인증서비스를 제공할 수 있으며, 그에 따른 네트워크 부하의 감소 등을 기대할 수 있다. 또한, CRL 및 OCSP Server를 통한 검증뿐만 아니라 Short-lived OCSP Certification을 통해 인증서 검증방법을 최적화함으로써 수신메시지의 수준과 통신망 상태에 따라 사용자가 판단할 수 있도록 하였다.

신속히 무선 Ad Hoc 통신망을 기반으로 전개되는 긴급한 상황에서 요구되는 인증서비스는 생존성이 우선한다. 본 논문에서 제안하는 유·무선PKI 통합모델은 CRL을 운용하는 일반적인 형태의 인증체계나, 잦은 topology의 변경이 불가피한 특수한 상황에서도 지속적인 인증서비스를 제공할 수 있는 장점이 있다. 또한 SSL/TLS 보안프로토콜을 적용함으로써 OCSP가 갖는 취약한 DoS(Denial of Serveice)공격에 보다 안전하며, SSL 프로토콜이 뛰어난 보안성을 최대한 활용하면서 통신망의 부하를 최소화하였다.

앞으로 인증서 및 인증서 효력정지 및 폐지목록(CRL), OCSP에 대한 명확한 Spec을 설계하면서 국제/국내 표준을 최대한 수용하되 확장영역의 사용을 최소화하여 Compact한 모델이 되어야 할 것이다. 또한 인증서 등을 저장하고 암호화 작업을 수행할 Hardware Token[7]에 대한 연구는 경제성과 보안성이라는 두 가지 관점에서 접근하여 최적의 솔루션을 도출하여야 한다. 국방 인증체계와 같이 특수한 형태의 운영환경에서는 상용 유·무선PKI와 같은 독자적인 체계로 설계될 수가 없으며, 유선PKI 인증체계를 기반으로 최적화하여 무선구간 종단 Client간에도 지속적인 인증서비스가 제공될 수 있도록 구현되어야 할 것이다.

이러한 인증서 검증모델은 국방통신운용환경과 같은 전형적인 Ad Hoc 통신망 외에도 다양한 멀티캐스팅 환경에서의 인증서 기반 그룹키 관리기술 등에도 응용이 가능할 것으로 판단된다.

참 고 문 헌

[1] Martin Christinat, WTLS-The Security Layer in the WAP Stack, Colloquium on Information Security, 2000
[2] Stephan Thomas, SSL and TLS Essential, Willy, 2000
[3] 이용, "무선 PKI 인증기술," 제6회 정보보호 심포지움, 2001, pp564-566
[4] RFC: 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
[5] 박종욱, "전자서명 인증관리 실무," 제6회 정보보호 심포지움, 2001, pp76-84
[6] 김동완, 이성식, "이동 Ad Hoc망 기술 개요," Telecommunication Review, 제10권 1호, 2000, pp158-160
[7] FIPS140-1, Security requirements for cryptographic modules, 1994