산업기술연구(강원대학교 산업기술연구소 논문집), 제22권 A호, 2002.
Journal of Industrial Technology, Kangwon Natl. Univ., Korea, No. 22 A, 2002.

PKI 방식의 차세대 이동통신 망에 적용 가능한 인증서 검증 절차 설계

Design of Validation Procedure for Certification for PKI Based Next Generation Mobile Networks

정 종 민* 이 구 연**
Jeong, Jong-Min Lee, Goo-Yeon

Abstract

When the wireless PKI is applied to 3G/4G mobile network which requires mutual authentication among all entities, the wired PKI procedure is not feasible for validating visited network's certifications because of the wireless environmental limitations. Also, if we depend on WAP based PKI, we cannot support confidence about certification validation since the information offered from visited network is not authenticated. Therefore, in this paper we consider various and unique characteristics of mobile environment for certification validation at 3G/4G mobile networks based on wireless PKI and then propose two certification validation procedures.

키워드 : 제 3세대/제 4세대 무선 통신, *인증서 검증, 무선 PKI*
Keywords: *3G/4G, Certification Validation, Wireless PKI*

1. 서론

인증, 무결성, 기밀성, 부인봉쇄, 접근 통제 등의 보안 기능을 일관성 있게 제공해 주는 보안 기술로서 PKI가 가장 일반적이며, 이동전화와 무선 인터넷의 급속한 성장에 따른 무선 환경에서 보안 기능도 무선 PKI가 궁극적인 대안으로 여겨지고 있는 실정이다. 특히 3G/4G 이동 통신 망의 VHE (virtual home environment) 서비스를 제공하기 위해서는 가입자의 프로파일이 방문 망에 필요하게 되는데, 이 경우 무선 PKI를 적용하여 망과 단말기 간, 그리고 망과 망 간의 상호 인증을 제공하여 상대의 신원을 확인할 수 있을뿐만 아니라, 전역 로밍 시에도 각 엔터티간의 인증과 암호화 키 교환을 통한 기밀성을 제공할 수 있다

하지만 이러한 PKI 기술이 무선 환경에 적용되기 위해서는 무선의 환경적인 제약과 단말기의 성능적인 한계를 고려하여 기존 유선 PKI의 요소와 동작 절차의 변경이 필요하게 된다. 여기에는 인증서 규격에 대한 정의, 인증서 보관 및 갱신/삭제에 대한 정의 그리고 인증서 검증 등에 관한 절차가 논의되어져야 할 것이다.

유선 PKI의 인증서 검증은 PKI의 구조에 따라 약간의 차이가 있긴 하지만 기본적으로는 인증서 체인의 각 인증서가 유효기간 및 여러 제약조건(정책제약, 이름제약 등)을 만족하고, 인증서 발급자 필드를 통하여 최종적으로 Root CA가 발급한 인증서 임을 확인하게 되면 인증서 검증이 완료되는데, PKI 기반의 3G/4G 무선 환경에서는 무선 단말기와 방문 망 간의 상호 인증을 위한 방문 망의

* 강원대학교 컴퓨터정보통신공학과, 박사과정
** 강원대학교 전기전자정보통신공학부 부교수, 공학박사

인증서 검증 시 무선 단말기와 CA 간의 직접적인 채널을 설정할 수 없어 인증되지 않은 방문 망을 경유해야하므로 방문 망에 의한 검증서 결과의 오류를 야기 할수도 있기 때문에 새로운 동작 절차가 요구되어 진다.

현재 WAP포럼에서 기존의 PKI의 표준을 가능한 재사용하면서 WAP 환경의 특정 요구사항을 지원하기 위한 목적으로 WAP PKI definition을 발표하였는데, WAP PKI 모델과 PKI 동작 등에 관하여 다루고 있다[1]. 하지만 앞서 언급한 인증서 검증 문제에 대해서는 무선 단말기가 trust CA 만의 정보를 미리 획득한 상태에서 상대방(서버 혹은 게이트웨이)이 전달해 주는 인증서 체인을 통해 인증서를 검증하는 SSL/TLS의 구조를 그대로 지니고 있어 몇 가지의 문제점이 존재한다. 즉 3G/4G 무선 통신의 전역 로밍 및 VHE 환경에서 인증서 검증 시 기존의 WAP based PKI는 다음과 같은 한계가 발생한다.

- 상호 인증이 완료되지 않은 상태에서 방문 망으로부터 받은 정보를 사용해야 함
- Trust CA 정보만으로 인증서 체인 내의 모든 인증서를 검증 할 수 없음
- 인증서 검증을 위한 무선 단말기와 CA간의 통신이 인증이 완료되지 않은 방문 망을 경유해야 함
- 무선 단말기의 성능 한계로 클라이언트가 인증서 검증의 주체가 될 수 없음

본 논문에서는 위에서 제기된 문제점을 해결하여 무선 PKI에서 동작할 수 있는 인증서 검증 모델과 이에 대한 절차를 제시하고 기존 동작과의 비교 분석을 한다.

2장에서는 유선 PKI와 WAP PKI에서 언급한 인증서 검증 절차에 대해서 살펴보고 3장에서 제안의 필요성을 언급하며 4장에서 무선 환경에 적합한 새로운 절차를 제시하고 5장에서 결론을 맺는다.

2. 배경 지식

유선 PKI와 WAP PKI에서의 인증서 검증 절차를 살펴보기 위해 SSL3.0/TLS1.0 인증서를 통한 상호 인증 절차의 인증서 검증과 WAP PKI의 인증서 검증 형태를 살펴본다.

2.1. SSL/TLS에서의 인증서 검증

SSL/TLS에서 서버 인증서를 검증하는 형태는, 핸드쉐이크 과정 중 서버에서 클라이언트로 전송하는 Certificate 메시지 내에 인증서와 함께 단순히 인증서 체인을 포함하여 전달하게 되는데, 서버의 공개키 인증서로 시작하여 인증기관의 루트 인증서로 종료하게 되며, 이를 수신한 클라이언트 측에서 서버 인증서의 신뢰 정도를 평가해야 하는 형태이다. 이를 위해 클라이언트는 인증서의 서명, 유효기간과 취소 상태를 검증해야 하는 책임이 있으며, 일반적으로 클라이언트는 trusted CA의 공개키를 획득함으로써 검증을 가능하게 할 수 있다. 현재의 netscape와 Microsoft의 경우 well-known CA의 공개키를 브라우저에 미리 저장하고 있음으로 가능하다. 즉 이 경우는 PKI의 여러 구조 중 (신뢰 목록 구조, 계층구조, 메쉬구조, 상호 인증 구조, 브릿지 구조[1] 등) 신뢰 목록 (trust list) 방식을 따르고 있다.[2]

즉 인증서 검증 주체에서 trust CA 공캐키를 미리 소유하고 있음을 가정하고 있으며, 사용자가 사용자의 목록에 없는 CA로부터 인증서를 가지고 있는 사용자와 통신하기 위해서는 사용자의 신뢰 목록에 새로운 CA를 추가해야 하며, 추가하기 전에 그 CA에 대한 신뢰 정도를 평가해야 한다. 또한 신뢰 목록이 증가할수록 최신 정보를 유지해야 한다.

2.2 WPKI에서의 인증서 검증

WAP PKI에서는 WAP1.2에서 정의된 보안 모델을 제공하기 위해 다음과 같은 모델로 분류하고 있다.

- WTLS Class2를 위한 CA 공개키 인증서 사용 구조
- WTLS Class3를 위한 클라이언트 공개키 인증서 사용 구조
- WMLScript sign text와 클라이언트 공개키 인증서 사용 결합 구조

향후의 WAP PKI모델은 응용 레벨에서의 종단간의 기밀성과 무결성을 위해 singed content 모델을 지원하기 위해 강화될 것이다[3].

WTLS의 Class 별로 서버의 인증서를 검증하기 위해 클라이언트가 소유해야 하는 정보는 Class 2인 경우 Root CA의 공개키를 지니고 있어야 하며, Class 3인 경우에는 Root CA의 공개키와 자신의 개인키를 포함하고 있어야 한다.

WAP PKI에서는 CA가 발급한 공개키 인증서를 검증하기 위한 정보를 지칭하는 'trust CA information'을 언급하고 있는데, 여기에는 공개키와 이름 그리고 기타 필요한 정보를 포함하고 있다. 이 CA 정보는 안전한 형태로 클라이언트에게 분배되어야 하며(shoud be), 클라이언트는 CA정보가 WAP PKI 스펙에서 정의하고 있는 hashing이

나 singing등의 방식으로 신뢰된다면 이 정보를 받아들이게 되는데, CA information이 신뢰되었다 하더라도, 클라이언트는 새로운 CA의 정보를 수용하였음을 알릴 수 도 있다.

Trust CA information은 self-signed X.509 공개키 인증서 혹은 self-signed WTLS 인증서의 형태로 표현될 수 있다.[4]

이와 같이 WAP PKI에서도 서버/게이트웨이의 인증서 검증의 주체가 유선 PKI와 동일하게 클라이언트로서 미리 검증에 필요한 정보를 지니고 있거나 통신 중에 분배 받으며, 또한 인증서 체인 구성에 있어서도 서버/게이트웨이의 정보에 의존적이게 된다.

3. 제안의 필요성

앞 절에서 유선 PKI 적용 프로토콜로 대변될 수 있는 SSL/TLS와 WAP PKI를 살펴본 결과 이를 3G/4G 무선 환경으로 적용시키기에는 여러 가지의 변형 요구사항이 발생된다. WAP PKI의 경우 무선 환경을 위한 구조로 제안된 것이지만 인증서 검증을 포함한 PKI의 구조가 유선 PKI의 형태를 유사하게 따르고 있음을 알 수 있다. 이는 현재 무선 응용이 확대되고 있지만, 아직은 초기 단계의 망 구조를 이루고 있어 유선의 PKI 구조가 어느 정도 수용되고 있음을 나타내고 있지만, 향후 VHE 및 전역 로밍의 3G/4G 서비스가 일반화 될 경우에는 이에 대한 적용이 불가능 할 것이다 3G/4G 환경을 고려할 경우 기존 형태의 PKI 및 WAP PKI 구조가 갖는 문제점을 좀더 구체적으로 살펴보면 다음과 같이 정리할 수 있을 것이다.

[문제 1] 서버 인증서 검증을 위해 검증되지 않은 단계에서 서버가 전송해 준 인증서 체인을 사용해야 하는 문제

[문제 2] 서버 인증서 검증이 성능이 제한된 무선 단말기를 의존해야 하는 문제

[문제 3] PKI 구조가 '신뢰 목록'을 따를 경우 무선 단말기에 보관해야 하는 정보의 양이 증가되는 문제

[문제 4] 3G/4G 망의 무선 PKI 구조가 '신뢰 목록' 형태를 따르지 않을 경우 다른 구조 적용에 따른 인증서 검증 절차 제안 요구

[문제 5] 인증서 체인이 다수의 인증서로 구성될 경우 Root CA 공개키만으로 검증 불가

[문제 6] 서버 인증서를 검증하기 위해 무선 단말기는 검증에 필요한 정보를 보관하고 있어야 하는 문제

[문제 7] 인증서 검증을 위한 무선 단말기와 CA 등 간의 통신이 요구되는 문제

이상과 같이 기존 PKI의 방식을 3G/4G의 무선 환경으로 적용시킬 경우 망과 무선 단말기의 성능 문제가 발생될 수 있으며, 인증서 검증 및 PKI 구조의 안정성에 위배되는 문제가 발생될 수 있다.

다음 절에서는 이러한 유선 PKI와 WAP PKI의 제한 점을 극복할 수 있는 무선 환경에서의 인증서 검증 절차를 묘사한다.

4. 제안 구조

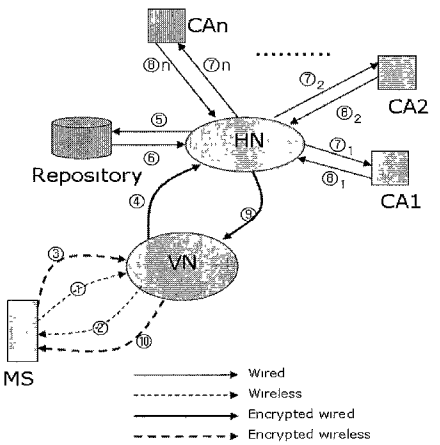
본 논문에서는 3G/4G의 차세대 무선 환경에 적용 가능한 인증서 검증 구조를 2가지 형태로 구분하여 정의한다. 첫째는 인증서 검증의 주 기능을 홈 망에 두어 가입자는 미리 알고 있는 홈 망과 무선 단말기 간의 암호 세션을 통해 인증서 검증 요구 및 결과를 획득하게 되며, 두 번째는 방문 망 근처에 있는 DS (delegation server)[5][6]를 이용하여 인증서 패스 및 검증을 위임한 후 이에 대한 결과를 전달받는 구조이다.

DS는 DPV (delegation path verification) 프로토콜을 사용하여 검증 정책이라 불리는 일련의 룰에 따라 특성 시간 T를 기준으로 하나의 인증서를 검증하는 시스템이다.[5]

원칙적으로는 무선 PKI를 통해 상호 인증, 즉 무선 단말기와 방문 망 그리고 방문 망과 홈 망이 상대를 인증하게 되는데, 유선으로 연결되어 있는 방문 망과 홈 망사이의 상호 인증은 기존의 PKI 방식의 절차와 유사할 수 있기 때문에, 본 논문에서는 무선 구간, 특히 서론에서 언급한 문제로 인해 무선 단말기에서 방문 망의 인증서를 검증하기 위해 새로운 절차를 정의해야 하는 사항에 초점을 맞춰 진행된다.

3.1 제안 구조 1 : 홈 망을 의존한 형태의 VN인증서 검증

다음 [그림 1]은 홈 망을 의존하여 터널링 방식을 통한 방문 망의 인증서를 검증하는 구조를 묘사하고 있다. 무선 단말기를 MS, 홈 망을 HN, 방문 망을 VN, 키 K로 암호화 된 메시지 M을 {M}K, 재전송 탐지를 위한 타임 스탬프를 TS로 표기할 경우 수행 절차는 다음과 같다.



〔그림1〕 제안 1의 VN인증서 검증 절차

· 인증서 요청 단계

M1. MS는 VN에게 VN의 인증서를 요청
MS -> VN : MS, VN, ReqCertVN, TS1

M2. VN은 VN의 인증서 URL을 MS에 전송
VN -> MS : VN, MS, URLCertVN, TS2

· 인증서 검증 요구 단계

M3. MS는 M2의 VN인증서를 MS와 HN의 비밀키로 암호화 후 인증서 검증 요청 메시지를 포함하여 VN으로 전송
MS -> VN : {MS, VN, HN, URLCertVN, TS3}$K_{MS/HN}$, MS, VN, HN, ReqCetVerify

M4. VN은 수신한 M3을 HN으로 포워딩
VN -> HN : {MS, VN, HN, URLCertVN, TS3}$K_{MS/HN}$, MS, VN, HN. ReqCertVerify

· 인증서 획득 및 검증 단계

여기서 HN이 인증서를 획득하고 실제 검증하는 과정은 유선 PKI 구조와 동일 하므로 유선 PKI 프로토콜을 사용하게 된다.

M5. HN는 M4를 복호화 후 VN의 인증서 URL 정보를 통해 VN인증서 탐색

M6. VN의 인증서 획득

M71~ M7n, M81~ M8n. : HN은 VN의 인증서를 통해 인증서 패스를 구성하며, trust CA까지 검색하며 인증서를 검증

M9. HN은 인증서 검증 결과(Token)를 MS와 HN의 비밀키로 암호화 인증서 검증 결과 메시지를 포함하여 VN에 전송
HN -> VN : {Token}$K_{MS/HN}$, VN, MS, HN
Token = ResultCertVerify, HN, MS, TS4

M10. VN은 M9를 MS에 포워딩
VN -> MS : {Token}$K_{MS/HN}$, VN

M10을 수신한 무선 단말기는 이를 통해 최종적으로 VN의 인증서를 신뢰하여 사용하게 된다.

3.2 제안 구조 II : DS를 이용한 VN인증서 검증

두 번째로 고려할 수 있는 구조는 위임 서버를 이용하는 것이다. 이 경우 무선 단말기의 현재 위치에 상관없이 방문 망 근처에 있는 위임 서버를 사용하여 홈 망의 직접적인 의존 없이 방문 망의 인증서를 검증할 수 있다. 하지만 이 경우 무선 단말기와 DS 간의 메시지를 암호화시키는데 사용되는 키 분배가 선행되어야 한다. 다음 [그림 2]는 이에 대한 절차를 나타낸 것이다.

· 인증서 요청 단계

M1. MS는 VN에게 인증서 요청 및 신뢰 DS 목록 요청
MS -> VN : MS, VN, ReqCertVN, ReqDSList, HN, TS1

M2. VN은 HN에게 신뢰 DS 목록 요청 메시지를 포워딩
VN -> HN : VN, HN, MS, ReqDSList, TS2

M3. HN은 암호화된 DS 신뢰 목록을 VN에 전송
HN -> VN : HN, VN, MS, TS3, {HN, ResDSList, SessionKey, TS4}$K_{MS/HN}$

SessionKey는 MS와 DS간의 채널 암호화를 위해 사용되는 것으로, HN이 전달해주는 SessionKey를 그대로 사용할 수도 있으며, 이 정보를 통해 새로운 키를 생성 할 수도 있다.

M4. VN은 HN으로 수신한 암호화된 DS 신뢰 목록과 자신의 인증서 URL을 MS에 전송
VN->MS : VN, MS, {HN, ResDSList, SessionKey, TS4}$K_{MS/HN}$, URLCertVN

· 인증서 검증 요구 단계

M5. MS는 DS를 선택 후 VN에게 인증서 검증

요청

MS->VN : {MS, DS, VNCertURL, TS5}$K_{MS/DS}$, VN, DS, MS

M6. VN은 M5의 DS의 위치로 인증서 검증 요청 메시지 포워딩

VN->DS : {MS, DS, VNCertURL, TS5}$K_{MS/DS}$, VN, MS

· 인증서 획득 및 검증 단계

M7. ~ M8 인증서 탐색 및 획득

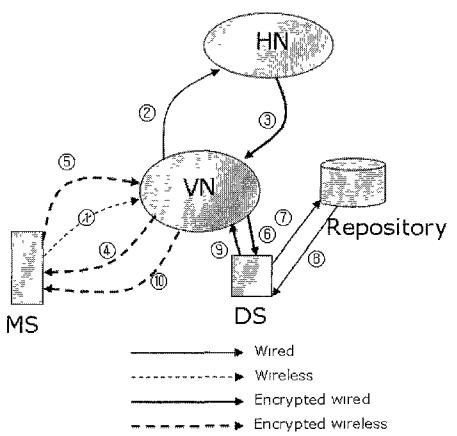
M9. DS에서 VN인증서 검증 후 결과를 DS와 MS의 비밀키로 암호화 후 전송

DS -> VN : {Token}$K_{MS/DS}$, VN, MS, DS

Token = ResultCertVerify, DS, MS, TS6

M10 VN은 메시지 9를 MS에 포워딩

VN -> MS : {Token}$K_{MS/DS}$, VN,



〔그림2〕 제안 2의 VN인증서 검증 절차

3.3 제안 구조 분석

제안하는 구조 I/II를 살펴보면 앞서 제기한 문제를 다음과 같이 해결하고 있음을 알 수 있다.

· VN의 인증서 검증을 위해 VN이 제공하는 정보를 사용하지 않고, HN과 DS가 인증서 체인 구성 및 Root CA의 공개키 등의 필요한 정보를 직접 획득하여 VN 인증서 검증 : [문제 1,3] 해결

· 인증서 검증 주체가 무선 단말기에 비해 성능이 우수한 HN/DS를 사용 : [문제 2,6] 해결

· 인증서 검증을 위해 무선 단말기와의 직접적인 통신 없이 HN/DS를 통해 수행 후 이에 대한 결과 정보만 획득 : [문제 7] 해결

이와 같이 공통된 특성과 더불어 각 방식을 비교하면, 제안 I의 경우, 인증서 검증 주체가 홈 망으로, 홈 망은 방문 망과 무선 단말기 간의 상호 인증 절차와 더불어 인증서 검증 역할을 수행하므로, 인증서 패스가 상대적으로 길거나 잦은 검증을 수행할 경우 부하가 생긴 수 있다. 또한 무선 단말기와의 거리에 따른 성능 차이가 유동적일 수도 있다

이에 비해 제안 II의 경우 방문 망과 거리적으로 근접하게 위치한 DS를 사용할 수 있으므로 제안 I의 단점이 해결 될 수 있다. 하지만 DS라는 새로운 엔티티의 추가에 따른 역할 정의 및 DS와 무선 단말기 간의 프로토콜 정의가 필요하게 되는데, 이 경우에도 인증 되지 않은 방문 망을 경유하여 통신이 이루어지므로 반드시 안전한 키 교환 혹은 생성 절차를 통해 기밀성을 유지해야 한다.

다음 [표 1]는 SSL/TLS에서의 유선 PKI 동작과 WAP based PKI 그리고 제안하는 구조에 대해 몇 가지의 항목에 따른 비교를 나타낸 것이다.

항목	유선 PKI	WPKI	제안 1	제안 2
검증 주체	클라이언트/ DS	무선 클라이언트	HN	DS
클라이언트 소유 정보	인증서	Trust Info, 인증서 URL	인증서 URL	인증서 URL
인증서 패스 구성 주체	클라이언트/ DS/서버	서버/ 게이트웨이	HN	DS
서버 정보 의존 여부	독립적/ 의존적	의존적	독립적	독립적

〔표 1〕 기존 방식과 제안 구조 비교

유선 PKI와 WAP PKI는 클라이언트가 주체가 되어 미리 획득한 Root CA의 정보를 보관하여 이를 통해 직접 검증하는 것에 반해 제안하는 구조 I/II는 무선 환경의 단말기 성능 제약을 고려하여 망이나 기타 새로운 검증 엔티티로 그 역할이 이동되는 형태로 설계하였으며, 인증서 패스 구성 및 인증서 체인을 방문 망의 정보에 독립적으로 획득하여 검증을 수행하므로 신뢰성을 제공할 수 있게 된다. 또한 무선 단말기는 인증서 검증을 위해 과다한 정보를 포함하지 않게 됨을 알 수 있다.

Ⅳ. 결론

본 논문에서는 무선 환경, 특히 VHE 서비스를 위해 가입자 프로파일 등을 방문 망에게 전달해야 하는 3G/4G 이동 통신 망에서 PKI 기반 보안 서비스를 제공하기 위한 선행 절차로, 인증서 검증에 관한 절차를 제안하였다. 3G/4G 망에서의 인증서 검증은 환경적인 제약으로 인해 유선 PKI에서와 같이 클라이언트가 주체가 되어 인증서를 검증 할 수 없으며, 또한 WAP based PKI와 같이 서버 혹은 게이트웨이로부터 인증서 패스를 전달받아 클라이언트가 미리 소유하고 있는 trust CA의 정보를 통해 검증하는 경우, 인증되지 않은 방문 망의 정보를 신뢰할 수 없게 된다.

이러한 문제점을 해결하기 위해 본 논문에서는 인증서의 검증 주체를 클라이언트가 신뢰할 수 있는 홈 망이나 새로운 엔티티로 변경하며, 인증되지 않은 방문 망의 정보에 독립적인 형태로 방문 망의 인증서를 검증할 수 있는 구조를 제안하였다.

감사의 글

본 논문은 정보통신부에서 주관하는 2001년도 대학기초연구 지원사업에 의하여 수행되었음

참 고 문 헌

[1] Russ Housley, Tim Polk, "Planing for PKI : Best Practices Guide for Deploying Public key Infrastructure", Wiley Computer Publishing, 2001

[2] Stephen Thomas "SSL and TLS Essentials" Wiley Computer Publishing, 2000

[3] "WAP Public Key Infrastructure Definition", Ver 24, Apr, 2001

[4] "WAP Wireless Transport Layer Security Specification", Ver 18, Feb, 2000

[5] Denis Pinkas, "Delegated Path Validation and Delegated Path Discovery Protocols", July, 2001

[6] Micahel Myers, "Delegated Path Validation" Aug, 2000

[7] "3rd Generation Partnership Project : The Virtual Home Environment (3G TS22.121 Ver 3.1.0)", 3GPP Technical Spec. 1999

[8] "3rd Generation Partnership Project : General Report on the Design, Specification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms", 3GPP Technical Spec. 2000

[9] M. Torabi, "A Shift in the Mobile Network Service Provisioning Paradigm", Bell Lab Tech. Journal, 2000