M2M 통신을 위한 X.509 인증서 구조 경량화

오상학*, 김형식**
*성균관대학교 소프트웨어플랫폼학과
**성균관대학교 전자전기컴퓨터공학과
osh920807@gmail.com, hyoung@skku.edu

Lightweight X.509 Certificate Format for M2M Communication

Sanghak Oh*, Hyoungshick Kim*
*Dept of Platform Software, Sungkyunkwan University
*Dept of Computer Science and Engineering, Sungkyunkwan University

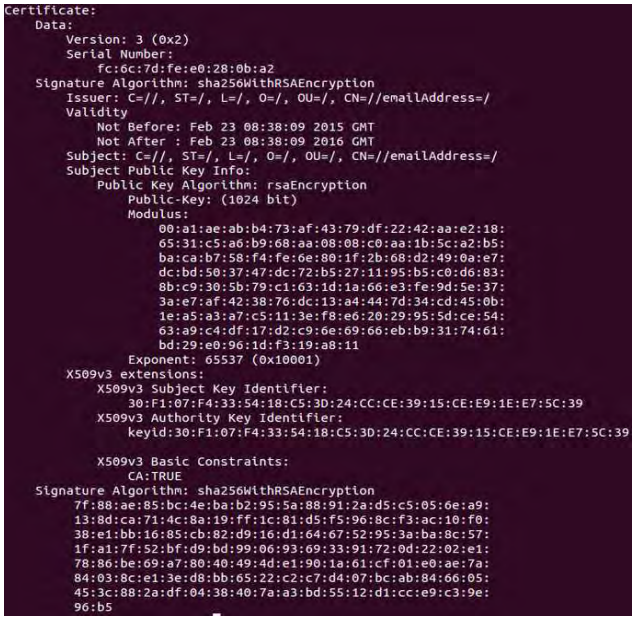
요 약

공개 키 기반(PKI)에서 사용되는 표준 인증서인 X.509 인증서 내 정보들은 사람이 읽기 좋은 형태로 이루어져 있지만 기계와 기계 사이의 통신에서는 필요하지 않은 부분이 존재한다. 이 부분은 M2M 통신에서 사용되지 않을 뿐 아니라 통신의 효율성 또한 감소시킨다. 따라서 본 논문에서는 X.509 인증서를 경량화 시킨 새로운 구조를 제시함으로써 M2M 통신에서의 효율성을 높이고자 한다.

1. 서론

X.509 인증서는 공개 키 기반(PKI)의 표준 인증서로써 공개키와 개인키와 같은 비대칭 키를 인증하는 용도로 사용되고 있다. 최근에는 SCADA 네트워크(System Control and Data Acquisition network)에서도 X.509가 공개키 인증서로 사용되고 있다. 하지만 SCADA의 경우 산업 제어 시스템으로써 관리자가 단순히 제어 시스템을 통해 관리하고 통신의 대부분이 기계와 기계 사이의 통신으로 이루어져 있다. 기계와 기계 사이의 통신에서는 인증서를 이용하여 단순히 암호화 된 공개키 내용과 전자 서명 내용을 비교해 비대칭 키의 무결성을 확인한다. 이러한 특징을 가진 SCADA 네트워크에서 사용하는 X.509 인증서 version 3의 구조에는 필요 이상의 많은 정보들이 포함되어 있다. M2M 통신에서의 불필요한 필드들에 대해 그림 1의 X.509 인증서 version 3 예시를 통해 소개하겠다.

그림 1의 예시에서 볼 수 있듯이 인증서의 내용 중 텍스트 형태로 인코딩 된 정보들이 존재한다. 예를 들어 서명 암호화 알고리즘과 공개키 암호화 알고리즘 필드 속 각각의 알고리즘의 이름이 텍스트 형태로 인코딩 되어 있다. 발행인 이름과 공개키 소유자 필드 또한 발행인과 공개키 소유자의 정보들이 텍스트 인코딩 된 채 저장되어 있다. 이러한 텍스트 형태의 정보들은 사람이 읽고 이해하기 편리하게 만든 형태일 뿐 단순히 받은 정보에 대한 연산을 하는 기계들 사이의 통신에서는 사용되지 않는다. 그리고 X.509 인증서 구조 중 발행인에 대한 상세한 정보를 쓰는 부분과 같이 M2M 통신에서 불필요한 부분이나 같은 내용의 데이터를 좀 더 축소시키는 방향으로 개선할 부분이 존재한다.



(그림 1) X.509 인증서 예시

본 연구는 M2M 통신에서 전달하는 인증서 구조를 경량화 하여 새로운 구조의 X.509 인증서를 제안하였다. 본 연구에서 제안한 X.509 인증서 구조는 향후에 M2M 통신에서 사용하면 보다 더 빠른 통신을 하는데 도움이 될 것이

* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2015-H8501-15-1008)
본 논문은 미래창조과학부가 지원하는 2014년도 정보통신·방송(ICT)연구개발 사업[2014044072003, SDN 기술을 이용한 사이버 검역 시스템 개발]의 연구결과로 수행되었음.

다.

2. 기존의 X.509 인증서 구조(Version 3)

X.509 인증서 version 3의 구조는 다음과 같다.

<표 1> X.509 인증서 version 3 구조

버전 (Version)
일련번호 (Certificate Serial Number)
서명 알고리즘 (Signature Algorithm)
발행인 이름 (Issuer Name)
유효기간 (Validity)
공개키 소유자 (Subject Name)
공개키 (Subject Public Key Information)
발행인 고유번호 (Issuer Unique Identifier)
공개키 소유자 고유번호 (Subject Unique Identifier)
확장 필드 (Extension)
서명

- 버전 (Version) : X.509 인증서 버전으로써 버전에 따라 인증서의 구조가 달라진다. 현재 version 3이 표준으로 사용되고 있다.
- 일련번호 (Certificate Serial Number) : 인증서 고유의 일련번호를 나타낸다.
- 서명 알고리즘 (Signature Algorithm) : 서명을 하는데 사용된 알고리즘의 이름을 나타낸다.
- 발행인 이름 (Issuer Name) : 인증서를 발행한 기관의 이름이 입력된다.
- 유효기간 (Validity) : 인증서가 유효한 기간을 나타내고 있으며 유효 시작 시각부터 유효 만료 시각이 입력된다.
- 공개키 소유자 (Subject Name) : 공개키를 전달하는 주체의 이름이 들어간다.
- 공개키 (Subject Public Key Information) : 공개키의 내용이 암호화 알고리즘을 통해 입력되며 공개키 암호화 알고리즘의 이름 또한 입력된다.
- 발행인 고유번호 (Issuer Unique Identifier) : X.509 인증서 version 2에서 추가된 필드로써 인증서를 발행한 기관의 고유번호가 입력된다.
- 공개키 소유자 고유번호 (Subject Unique Identifier) : X.509 인증서 version 2에서 추가된 필드로써 공개키를 전달하는 주체인 공개키 소유자의 고유번호가 입력된다.
- 확장 필드 (Extension) : X.509 인증서 version 3에서 추가된 필드로써 공개키의 사용법, 인증서 정책, 발행인 관련 정보, 발행인/소유자의 다른 이름, 제한점 등이 입력된다.
- 서명 : 전달될 공개키에 대한 서명의 내용이 서명 알고리즘을 통해 암호화되어 입력된다.

3. 새로운 X.509 인증서 구조

본 연구에서 제안하는 새로운 X.509 인증서 구조는 다음과 같다.

<표 2> 새로운 X.509 인증서 구조

버전 (Version)
일련번호 (Certificate serial Number)
서명 알고리즘의 대표번호 (Key Number of Signature Algorithm)
유효기간 (Validity)
공개키 (Subject Public Key Information)
서명
발행인 고유번호 (Issuer Unique Identifier)
공개키 소유자 고유번호 (Subject Unique Identifier)

현재 X.509 인증서 version 3에 사용되는 서명 알고리즘은 텍스트 형태로 인코딩 되어 있으며 알고리즘의 종류가 한정적이다. 따라서 알고리즘의 이름과 알고리즘에 대표번호를 붙여 테이블로 만들어 관리하고 실제로 통신이 이루어질 때 사용되는 인증서에는 서명 알고리즘의 대표 번호를 입력해 데이터 공간을 줄일 수 있다. 공개키 필드에 들어가는 공개키 암호화 알고리즘 또한 동일한 방식으로 암호화 알고리즘과 대표번호를 테이블로 정리해 인증서에는 공개키 암호화 알고리즘의 대표번호만 입력하도록 한다. 이러한 구조로 알고리즘 이름에 대한 필드를 변경하였을 때 그림 1의 인증서를 예로 들면 공개키 알고리즘의 필드는 13 비트에서 1비트로 12비트를 줄일 수 있고 서명 알고리즘의 필드는 23비트에서 1비트로 22비트를 줄일 수 있다.

<표 3> 서명 알고리즘 관리 테이블 예시

Signature Algorithm	Key number
RSA	0
KCDSA	1
DSA	2
EC-DSA	3
EC-KCDSA	4
others	5

기존의 유효기간 필드는 인증서의 유효 시작 시각과 인증서의 유효 만료 시각이 입력되었다. 하지만 새로운 X.509 인증서 구조에서는 인증서의 유효 시작 시각은 그대로 두고 인증서의 유효 만료 시각을 대신 유효 기간으로 입력함으로써 데이터 공간을 줄일 수 있다. 이 경우 또한 그림 1의 인증서 정보를 예로 들었을 때 기존의 인증서 유효 만료 시각 정보 24 비트에서 유효기간을 어떻게 정하느냐에 따라 달라지겠지만 1년을 초단위로 나타내었을 때 8 비트로 16비트를 줄일 수 있다.

X.509 인증서 version 3에서는 발행인 이름, 공개키 소유자 필드를 만들어 발행인과 공개키 소유자에 대한 정보를 입력하였다. 하지만 이 정보는 실제로 M2M 통신을 할 때는 사용되지 않고 사람이 확인하는 내용이다. 따라서 발행인 이름과 공개키 소유자 필드를 제거하고 X.509 인증서 version 3에 있는 발행인 고유번호와 공개키 소유자

고유번호로 대체하여 인증서의 데이터 구조를 줄일 수 있다. 그리고 만약 인증하는 과정에서 문제가 생겨 발행인과 공개키 소유자에 대한 정보가 필요한 경우, 발행인과 공개키 소유자 고유번호를 이용해 데이터베이스에 저장된 발행인과 공개키 소유자에 대한 정보를 가져오도록 한다.

나머지 버전, 일련번호, 공개키의 암호화된 내용, 서명의 암호화된 내용은 수정할 수 있는 사항이 아니라 그대로 사용한다.

4. 결론

현재 표준 인증서로 널리 사용되고 있는 X.509 인증서 version 3의 구조에는 M2M 통신에서 사용되지 않는 필드들이 존재하였고 데이터의 공간을 줄일 수 있는 필드 또한 존재하였다. 따라서 본 연구에서는 기존의 X.509 인증서 version 3보다 경량화 된 새로운 X.509 인증서 구조를 제시하였다. 제안된 X.509 인증서의 구조는 M2M 통신의 데이터 전송 시간을 줄이고 효율성을 더 증진시킬 것이다. 앞으로의 연구는 새로운 X.509 인증서 구조를 실제 Secure Socket Layer(SSL) 환경의 통신에 적용시키는 방향으로 연구를 진행하려 하고 있다. 먼저 OpenSSL 모듈을 이용하여 서버와 클라이언트 간 공개키와 인증서를 주고 받으며 메시지에 대한 인증을 하는 통신을 먼저 구현을 한다. 그리고 OpenSSL에서 제공하는 모듈 중 공개키와 인증서를 발급하는 부분과 검증하는 부분을 본 논문에서 제안한 새로운 구조의 인증서에 맞게 수정한다. 마지막으로 같은 환경에서 기존의 X.509 version 3 구조의 인증서를 사용한 통신과 새로운 구조의 X.509 인증서 구조를 사용한 통신의 네트워크 지연시간(delay time)을 비교함으로써 새로운 인증서 구조의 사용으로 인한 데이터 전달 시간 감소와 효율성 증가를 증명해낼 것이다.

참고문헌

[1] 최태영, “OpenSSL을 이용한 컴퓨터 시스템 보안”2nd Ed. 카오스북

[2] John Viega, Matt Messier, Pravir Chandra "Network Security with OpenSSL", O'Reilly Media