무선망에서의 고속 인증 프로토콜 구현을 위한 구조 분석

정성혁, 김정태
목원대학교

Analyses of Hardware Architecture for High-speed authentication protocol in wireless communication

Sung-Hyuk Jung ,Jung-Tae Kim
Mokwon University
E-mail : jshcool@yahoo.co.kr

요 약

In this paper, we analyses of Architecture for High-speed authentication protocol in wireless communication. The rapid process in wireless communication systems, personal communications, and smartcard technologies has brought new opportunities and challenges to be met by engineers and researchers working on the security aspects of the new communication. In real world, we have restricted hardware environments with limited computational power and small memory, we meet more challenges. Then we analyes the need of consideration to implement the system.

Ⅰ. 서론

현대는 사람들의 편리를 위한 목적으로 전자 제품의 무궁한 발전을 이루었고 지금도 급속도로 발전을 이루고 있다. 또한 이에 따라서 나타나는 막대한 량의 정보도 나타나게 된다. 이러한 정보를 인터넷등과 같은 매체를 통해 공유하고 있는 실정이다. 따라서 이러한 매체를 통한 정보기기 사이 즉 컴퓨터끼리 또는 컴퓨터와 단말기 사이 등에서 정보 교환이 필요한 경우, 이를 원할하게 하기 위하여 정한 여러가지 통신 규칙과 방법에 대한 약속의 통신규약을 프로토콜이라 한다. 따라서 이러한 통신 규약을 미리 정하여 놓고 사용함으로써 상호간의 접속이나 전달방식, 통신 방식, 주고받을 자료의 형식, 오류검출방식, 코드 변환방식, 전송속도를 원활히 할 수 있는 것이다. 만약 이러한 규약이 없이 정보 통신을 하면, 개개의 정보 전달자 마다 다른 규약에 의한 통신을 하게 되므로 정보 소통의 마비를 야기 시키게 된다. 따라서 정보의 전송에 있어서 프로토콜이라는 규약의 집합 속에서 정보를 정확하고 효율적으로 전송하기 위해서는 송수신 개체간의 서로 정보의 전송 시점과 수신 시점을 맞추는 일을 수행하고 정보 흐름의 양을 조절하는 흐름 제어 방법도 사전에 약속하여 프로토콜 속에 포함해야 한다. 이때까지는 이러한 기본적인 프로토콜의 원리는 가지고 정보를 전달함에 있어서 크게 무리는 없이 사용을 하고 있다. 하지만 사회가 발전함에 따라, 또는 복잡해짐에 따라서 정보의 양은 기하 급수적으로 늘어나고 있다. 또한 개인적인 정보도 이와 같이 전송되고 있는 실정이다. 따라서 본 논문에서는 오늘날에 사용하고 있는 고속의 인증 하드웨어의 종류를 분석하고 이러한 하드웨어가 어떠한 특징을 가지고 사용하고 있는지를 알아보도록 하겠다.

Ⅱ. 프로토콜 설계를 위한 구조분석

2.1. 공개키 기반구조

PKI는 인터넷과 같이 안전이 보장되지 않은 공중망 사용자들이 신뢰할 수 있는 기관에서 부여된 한 쌍의 공개키와 개인키를 사용함으로써, 안전하고 은밀하게 데이터나 자금을 교환할

수 있게 해 준다. [1]

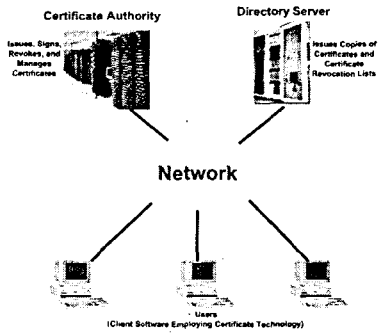

그림 1. PKI Infrastructure

이러한 PKI 방식은 인증기관에 의해 개개인의 공개키와 개인키를 수학적 공식에 의해 암호화 하고 이것을 제공해 준다.
다음에 이러한 방식에 대한 공개키와 개인키의 동작원리를 수학적으로 해석하고 있다.

1). 서로 같지않은 p, q를 정함
2). 공개키 n=pq
3). $\phi = (p-1)(q-1)$
4). $1< s < \phi$ 를 만족하는 공개키 s 생성
5). $d = s^{-1} \pmod{\phi}$ $(sd \equiv 1 \pmod{\phi})$ 다음공식을 이용하여 비밀키 d를 생성

공개키 암호화 시스템의 효율성에대하여 말할 때 다음의 세가지 중요한 요소가 있다.
1) Computational overtheads : 공개키와 개인키의 transformation을 수행하는데 얼마나 많은 계산이 필요한가.
2) Key size : 키 쌍과 시스템 파라메터를 저장하기 위하여 얼마나 많은 bits가 필요한가.
3) Bandwidth : 암호화된 메시지나 서명이 transfer되기 위하여 얼마나 많은 bit가 통신되어져야 하는가.[2]
따라서 이러한 세가지의 요건이 작용이 얼마나 잘 되어 지느냐에 따라서 암호화 시스템의 효율을 극대화 할 수 있다.

2.2 타원곡선 암호

다음의 프로토콜 방식은 타원곡성암호로써 약칭은 ECC이다. 타원곡선이라고 불리는 수식에 의해서 정의되는 특수한 가산법을 가지고 암호화 복호화를 하는 암호화 방식이다.[3] 이 방식은 짧은 키 사이즈로 높은 안전성이 확보되고, 또한 서명할 때의 계산을 고속으로 할 수 있는 것이 특징이다. 현재의 스마트 카드(IC 카드) 등의 정보처리능력이 그다지 높지 않은 기기에서 이용하기에 적합한 암호화 방식이다. 타원곡선 암호 시스템은 이산대수에서 사용하는 유한체의 곱셈군을 타원곡선군으로 대치한 암호시스템이다.

타원곡선 암호 시스템은 특징을 열거했지만 이러한 연산에서도 가장 효율적인 방법을 찾아 타원곡선 암호 시스템을 구현해야 할 것이다. 따라서 타원곡선이 가지고 있는 특성을 얼마나 잘 이용하느냐에 따라서 효율적인 시스템이 되는 것이다. 또한 타원곡선 시스템에서는 시스템 구성을 위해다음과 같은 단계들이 요구된다.

a. 기본 유한체의 선택
b. 선택된 유한체의 원소의 표현방법 선택
c. 유한체상에서의 연산의 구현
d. 선택된 유한체상에서 정의된 안전하고 효율적인 타원곡선의 선택
e. 타원곡선상의 연산의 구현

III. 암호 시스템의 동작 흐름

3.1 시스템 초기화 과정

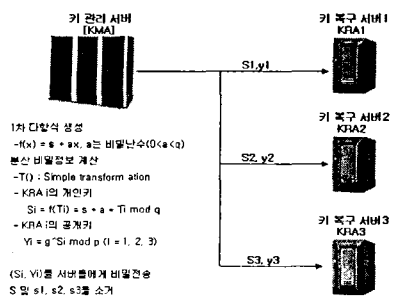

그림 2. 시스템 초기화 과정

위의 그림은 시스템 초기화 과정을 그림으로 나

타낸 것으로 사용자는 서버에 등록을 한 후, 관리 서버로부터 공개정보(p,q,g,y)를 전송받아 시스템에 저장한다. 또한 암호화용 패스워드를 생성한다. 키 관리 서버는 KMA 암호용 인증서 및 서명용 인증서를 발급 받고, (s, y)를 생성한 후, 비밀 분산 방식을 통해 각 서버에게 복구키를 안전하게 분배한다.[]

3.2. 키위탁 과정

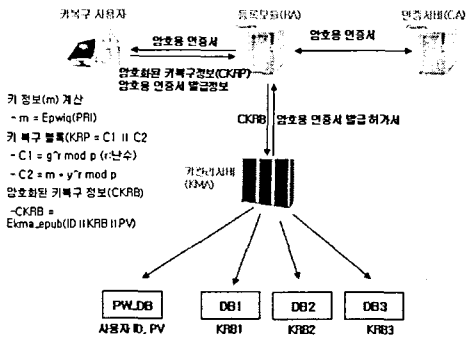

그림 3. 키 위탁 과정

먼저 사용자는 자신의 개인키, 공개키(PRI, PUB)를 생성하고 키 복구 블록을 암호화한 후 암호용 인증서 발급 정보와 같이 등록 서버에 전송한다. 이것을 받은 등록서버는 키 관리 서버에게 전송한 후, 응답을 기다린다. 키 관리 서버는 키 복구 정보를 그림 아래의 블록과 같이 분산 저장 후, 암호용 인증서 발급 허가서를 등록 서버에게 전송한다. 인증서버는 이것을 확인 후 암호용 인증서 발급 처리 및 인증서를 등록 서버에게 전송하고, 사용자는 이것을 받아 암호화된 개인키로 저장한다.[]

3.3. 키 복구 과정

사용자는 사용자 ID와 패스워드를 이용하여 암호키 복구 요청 메시지를 전송한다. 이를 키관리 서버는 사용자 인증을 한 후 요청 메시지를 처리하기 위해 블록을 재구성한다. 재구성한 블록은 블라인드 디코딩 기법을 이용하여 계산한 값을 전송한다.

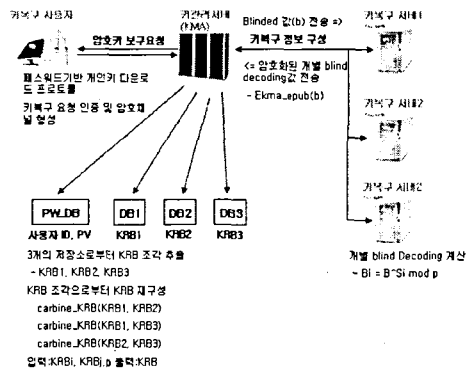

그림 4. 키 복구 과정

이를 키복구 서버는 개인키를 이용하여 계산한 각 키 복구 정보를 키 관리 서버로 전송하고, 전송된 값을 암호화된 개별 블라인드 디코딩 값을 이용하여 사용자의 키 정보(m)을 복구한다. 이를 사용자는 패스워드 기반 개인키 다운로드 프로토콜을 이용하여 키 관리서버로부터 기 정보를 안정하게 전송받게 되는 것이다. [8]

IV. 결론

서론에서 이야기 한바와 같이 우리의 일상생활에서는 무수히 많은 정보가 고유되고 전송되는 과정을 거치고 있다. 또한 이러한 정보에는 개인의 고유의 정보나 보안상의 정보도 같이 이동하고 있는 실정이다. 따라서 본문에 설명된 것과 같은 고속의 인증 프로토콜을 통해 내가 아닌 타인으로 부터 개인 정보 등을 보호하는 규약이 필요하게 된 것이다. 이러한 규약이 없이 무분별하게 사용함에 따라서 당사자가 아닌 제 삼자가 그 사람의 개인정보를 인터넷에 공개하거나 개인의 신상을 악용하는 일이 벌어질 수 있는 것이다. 따라서, 이러한 인증 프로토콜이 필요한 것이다.

현재의 인증 프로토콜도 모두 보완상 완벽하다고는 할 수 없다. 하지만 이러한 인증 프로토콜의 특성에 따라서 잘 활용하고 우리 사회에 적용시킨다면 보다 효율적으로 이용할 수 있을 것이다. 또한 그 시대의 상황에 맞게 인증 프로

토콜을 발전시킨다면 미래의 원활한 정보의 전송을 할 수 있을 것이다.

참고문헌

[1] 김동근, " 컴퓨터 용어사전", 2000.
[2] http://ks.hmall.com/top/detail?eid=06MoA
[3] http://omniknow.com/common/wiki.php?in=simple&term=RSA
[4] http://www.hill.com/archive/pub/papers/papers.asp?yr=2004&mn=01
[5] 웹 초심자를 위한 암호 기술의 활용
[6] http://www.kisa.or.kr/K_trend/KisaNews/200105/focus.html
[7] 암호용 키 및 인증서의 안전한 관리 발급을 위한 암호키 관리 기술