무선 인터넷 환경에서의 PKI 기반 데이터 보호 시스템에 대한 연구

김영호* · 채철주* · 최상욱* · 이재광*

*한남대학교

A Study of Data Security System Based PKI on Wireless Internet Environment

Young-ho Kim* · Cheol-joo Chae* · Sang-wook Choi · Jae-kwang Lee*

*Hannam University

E-mail : {yhkim, cjchae, suchoi, jklee} @netwk.hannam.ac.kr

요 약

광대역 통합망의 유무선 통합 서비스가 진행되는 시점에서 유·무선 네트워크 기반에서 불법적으로 정보를 취득하려는 공격에 대응하고자 정보보호에 대한 이슈가 대두되고 있다. 이러한 정보보호 기술 중에서 PKI(Public Key Infrastructure) 암호 시스템의 사용자는 인증, 비밀성, 무결성, 부인방지, 접근통제 등의 다양한 보안서비스를 제공받게 된다. 무선 네트워크 환경에서 모바일 클라이언트와 서버는 신뢰성 있는 데이터 송수신을 위해 인증서 및 무선 인터넷 암호 모듈을 탑재하고, 인증서의 유효성 검사를 통한 인증 과정을 거친 후 데이터를 송·수신하게 된다. 본 논문에서는 무선 네트워크 환경에서의 PKI를 통한 인증 및 데이터 보호 시스템을 연구하였다.

ABSTRACT

Wire·wireless integrated service of BcN(Broadband convergence Network) is expanding. Information Security issue is highlighted for opposing attack of getting information illegally on wire·wireless network. The user of PKI(Public Key Infrastructure) cipher system among Information security technology receives various security services about authentication, confidentiality, integrity, non-repudiation and access control etc. A mobile client and server are loaded certificate and wireless internet cryptography module for trusted data send·receive. And data sends·receives to each other after certification process through validity check of certificate. Certificate and data security system is researched through PKI on wireless network environment and data security system in this paper.

키워드

무선네트워크, PKI, 인증, 데이터 보호

Ⅰ. 서 론

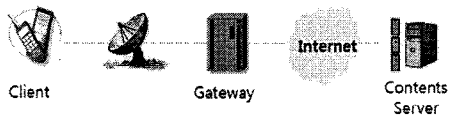
광대역 통합망(Broadband convergence Network :BcN)은 현재의 개별적인 망들이 갖고 있는 한계들을 극복하고 미래에 나타날 유·무선의 다양한 접속환경에서 고품질의 음성, 데이터 및 방송이 융합된 광대역 멀티미디어 서비스를 언제 어디서나 이용할 수 있도록 하는 차세대 통합 네트워크이다. 유·무선 네트워크 기반에서 불법적으로 정보를 취득하려는 공격에 대응하여 정보보호에 대한 이슈가 대두되고 있으며 BcN의 유무선 통합 네트워크기반 서비스를 안전하게 제공하기 위해 안전한 데이터 보호 시스템에 대한 연구가 필요한 실정이다.[1] 무선 인터넷 망은 유선 인터넷 망에 비교할 때 훨씬 제한적인 통신 환경을 가지며 전력 공급과 사용 대역, 이동성 등의 제한으로 인하여 낮은 대역폭과 낮은 연결 안정성 및 가능성, 높은 지연 특성을 가진다. 또한

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행 되었음(IITA-2008-C1090-0801-0027)

무선 인터넷을 위한 이동 단말기는 데스크 탑 컴퓨터에 비하여 CPU 성능의 제한과 낮은 메모리 용량, 사용전력 제한 등의 특성을 가진다. 이에 본 논문에서는 유선 인터넷 환경에 비해 상대적으로 안전에 취약한 무선 인터넷 환경에서의 PKI 기반 데이터 보호 시스템에 대한 연구를 수행하였다. 본 논문의 구성은 다음과 같다. 2장에서는 무선 인터넷의 구조와 WPKI를 소개하고, 3장에서는 안전한 데이터 전송을 위한 암호화 API를 소개하며 4장에서는 PKI 기반 데이터 보호 시스템을 기술하고 5장에서 본 논문을 결론짓도록 한다.

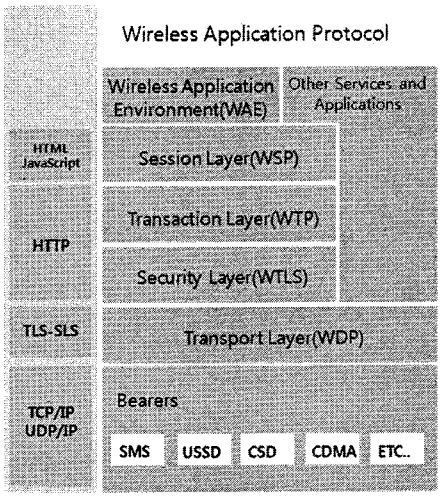
II. 무선 인터넷 구조와 WPKI

사용자가 무선단말기로 이동 중 무선망(Wireless Network)을 통해 인터넷 서비스에 엑세스하고 정보를 제공받을 수 있도록 하는 환경과 기술을 무선 인터넷이라 한다.



[그림 1] 무선 인터넷 구조

무선 인터넷의 구조는 [그림 1]에서와 같이 클라이언트, 서버, 그리고 게이트웨이가 있다. WAP의 핵심 요소인 게이트웨이의 역할은 유선 HTTP를 무선 프로토콜로 또는 그 반대로 변환하는 것이다. 무선 인터넷은 유선 인터넷에 이동통신의 이동성(Mobility)을 접목하기 위해 무선망과 연동이 필수적이다. 유무선 연동을 위해 제시되는 프로토콜 중 가장 대표적인 프로토콜은 WAP Forum의 WAP(Wireless Application Protocol) 방식이다. WAP Forum에서는 TCP/IP와 별도의 무선 환경에 적합한 프로토콜을 정의하는 작업을 진행 중인데 이 가운데 보안 프로토콜이 WTLS(Wireless Transport Layer Security)이다. WTLS는 인터넷에서 보안 메커니즘으로 잘 알려져 있는 SSL(Secure Socket Layer) 및 TLS(Transport Layer Security)를 기반으로 작성되었다. WTLS는 통신을 하는 두 응용 프로그램 사이에 안전한 채널을 형성해 통신 내용의 보안을 보장하는 방법이다. WTP와 WDP 사이에 수행되어 특정 응용프로그램에 종속되지 않고, WAP을 사용하는 모든 응용 프로그램들을 지원한다. WTLS는 기밀성, 사용자 인증, 메시지 무결성 등의 보안 서비스를 제공하며, 부인 봉쇄는 제공하지 않는다.[2][3]



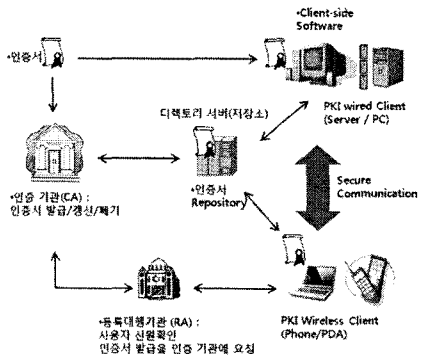
[그림 2] WAP Protocol

인터넷 상에서 전자거래 행위가 이루어지기 위해서는 비대면 특성을 보완하고 신뢰성을 보장하기 위한 거래 당사자 간 신분확인이 전제되어야 하며, 이는 인증, 무결성, 부인봉쇄 등의 서비스를 제공하는 전자서명 기술을 활용함으로서 해결이 가능하다. 전자서명 기술을 효과적으로 이용하기 위해서는 공개키 암호 방식이 필요하며, 공개키 암호 방식을 이용한 인증 방법을 구현하기 위한 기술적, 제도적 기반이 요구되는데 이를 공개키 기반구조(PKI : Public Key Infrastructure)라 한다.

PKI가 제공하는 서비스에는 인증, 무결성, 기밀성, 부인-방지, 접근 제어가 있다. 인증은 송신자 A가 메시지를 수신하였을 때 수신된 메시지가 실제 송신자 A로부터 보내진 메시지인가의 여부를 확인할 수 있어야 한다는 것이다. 무결성은 기밀성 서비스와 같이 메시지 스트림, 단일 메시지, 또는 메시지 특정 필드에 적용될 수 있다. 가장 유용한 접근 방법은 메시지 스트림 전체를 보호하는 것이다. 기밀성은 권한 없는 사용자에게 메시지가 노출되는 것을 막아 발신자가 원하는 수신자만이 메시지를 확인할 수 있도록 한다. 부인-방지는 송신자가 메시지를 수신자에게 전송한 후, 해당 메시지 전송사실을 부인할 수 없도록 해 수신자가 수신 메시지에 대해 아무런 의심 없이 받아들이도록 한다. 접근제어는 선택된 수신자만이 정보에 접근할 수 있도록 허용하는 것을 의미한다. 공개키·비밀키를 활용하여 접근 정보를 원하는 수신자에게만 데이터를 보냄으로서, 수신자로부터 온 접근 정보를 확인하여 허가된 사용자만을 선별하여 정보에 접근할 수 있도록 제어한다.

무선 PKI(Wireless Public Key Infrastructure: WPKI)에서는 유선 PKI의 구성요소를 그대로 이용하며, 무선 환경에 적합하도록 기능을 최소로

변화시켜 사용해야 한다. 무선 PKI를 구축하는 경우 클라이언트와 서버 간 대역폭, 클라이언트 컴퓨팅 능력, 제한된 메모리, 마지막으로 인증서 검증 메커니즘의 경량화 등을 고려해야 한다. 물론 단말기 사양이 급속히 발전하고 있으므로, 유선 PKI에서 요구하는 처리능력이나 메모리는 곧 극복되리라 예상되지만 현재의 단말기 사양에서 암호화 연산을 수행하는 데에는 여전히 많은 제한이 따른다. WPKI의 구조는 아래의 [그림3]에서 보듯 클라이언트, 등록대행기관(RA), 인증 기관(CA) 그리고 디렉토리 서버(repository)로 나뉜다. 인증기관은 인증서를 발급하고 인증서의 효력정지 및 폐지 기능의 역할을 하며, 등록기관은 인증기관과 사용자 사이에서 인증서 등록이나 신원을 확인한다. 디렉토리 서버는 인증서 혹은 CRL을 저장하는 역할을 한다. 먼저 클라이언트는 등록대행 기관에서 공개키 쌍을 생성하고, 이를 바탕으로 인증서를 생성한다.



[그림 3 | WPKI 구조

생성된 인증서는 클라이언트와 모바일 내지는 스마트 카드에 저장되고, 또한 디렉토리 서버에 저장된다. 클라이언트에게 암호화 통신을 원하는 사용자는, 디렉토리 서버로부터 클라이언트의 인증서를 확인하고 클라이언트의 공개키로 암호화 통신을 요청하게 된다. 또한 자신의 공개키가 노출되거나 유효기간이 만료되면, 이를 갱신하거나 폐기할 수 있는데, 이러한 요구를 위해서 인증서 관리 프로토콜(Certificate Message Protocol)을 이용하여 갱신, 수정, 폐기할 수 있다.

공개키 기반구조에서는 거래 당사자의 신분을 증명해주는 수단으로 인증서(Certificate)를 활용하고 있으며, 이를 관리하고 지원하기 위해서 IETF(The Internet Engineering Task Force)는 RFC 문서를 통해 표준으로 제정하고 있다.[4] 다시 말해 공개키 기반구조란 실체가 드러나지 않는 사이버 공간에서 공인된 인증기관이 사용자에게 법적 효력이 있는 인증서를 제공함으로써 비인가로부터 개인의 프라이버시 정보와 인터넷상에서 유통되는 전자거래 정보의 위·변조를 방지하기 위한 보안 인프라이다.

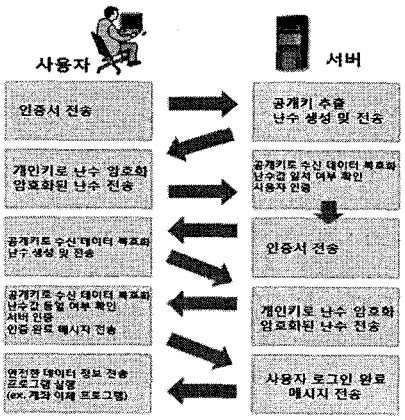
인터넷 상에서 송수신되는 전자문서의 송수신자 확인 및 송수신 내용을 확인해주는 서비스를 인증 서비스라 부르며 공개키 암호 기술을 사용한다. 공개키 시스템에서는 두 종류의 키를 필요로 하는데, 하나는 송신자가 전자 서명을 생성할 때 사용하는 개인키(private key)이고, 다른 하나는 수신자가 송신자의 전자서명을 검증할 때 사용하는 공개키(public key)이다. 개인키는 인감도장과 마찬가지로 개인이 안전하게 보관하는 키 정보인 반면, 공개키는 네트워크상의 누구나 접근할 수 있도록 공개해 놓는 키 정보이다. 이 키 쌍의 합치 여부를 통하여 송수신 메시지의 위·변조를 확인하는 서비스를 제공한다.[5][6]

III. 암호화 API

대칭키 암호화 알고리즘은 송신측과 수신측이 동일한 키를 사용하며, 대칭 암호화는 또한 개인키(Private Key) 또는 비밀 키(Secret Key) 암호화라 한다. 대칭 암호를 사용하는 것은 적절치 않을 수 있는데 키를 비밀스럽게 유지해야 하기 때문이다. 또한, 사용자의 수취인도 키를 비밀스럽게 유지하고 있다는 것을 믿어야 한다. 블록 암호화 알고리즘은 입력되는 메시지를 일정한 길이의 블록 단위로 암호화하는 방법으로, DES를 비롯한 대부분 대칭키 암호화 알고리즘은 블록 암호화 알고리즘 방법을 사용한다. 스트림 암호화 알고리즘은 이진 평문과 키에 대하여 이진 수열을 배타적 논리합(exclusive-OR)이라는 비트 단위의 이진 연산으로 결합하여 암호문을 생성한다. 대칭 암호화의 단점은 공개키 암호화라고도 불리는 비대칭 암호화에 의해 해결될 수 있다. 이 암호화는 자유롭게 공개된 공개키와 비밀스럽게 유지되어야만 하는 개인키의 쌍으로 생성된다. 공개키는 공개되며 어떤 사람도 개인키 없이는 사용자의 프라이버시를 침해하거나 흉내 낼 수 없다. 공개키를 이용하여 암호화 된 데이터는 개인키를 이용하여 복호화 된다. 해쉬 함수는 입력으로 다양한 크기의 메시지를 받고 출력으로 고정된 크기의 해쉬 코드인 메시지 다이제스트를 만든다. 해쉬 코드는 에러 탐색 기능을 제공한다. 일반적으로 사용하는 해쉬 함수들은 단방향 해쉬 함수를 말하며, 다른 메시지가 같은 메시지 다이제스트를 가질 확률은 매우 적다.

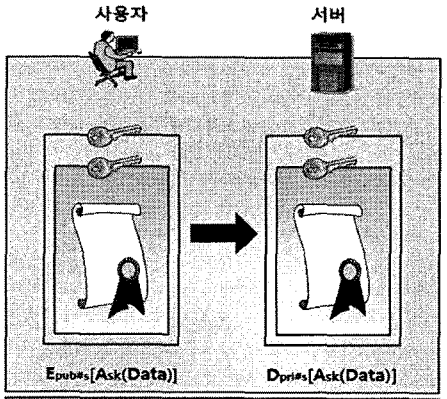
IV. PKI 기반 데이터 보호 시스템

2장에서 언급된 PKI 시스템은 개발된 암호 API와 CA 및 관련 응용 프로그램을 사용해 안전한 데이터 정보 전송을 제공한다.



[그림 4] 인증서를 이용한 로그인 절차

[그림 4]는 PKI 기반 인증서를 이용한 로그인 과정을 도식화 한 것이다. 로그인 과정이 성공하면, 안전한 데이터 정보 전송 서비스를 제공하는 데이터 보호 시스템을 사용할 수 있다. 데이터 보호 시스템은 사용자가 입력한 중요한 정보를 인증서와 암호 라이브러리를 사용하여 안전하게 서버로 전송한다. 여기서 서버는 기존의 CA 서버에서 인터넷 뱅킹을 담당하는 뱅킹 서버라 가정할 수 있다. 기존의 로그인 과정에서 이용한 인증서 정보를 바탕으로 송신자가 작성한 데이터를 암호화하여 전송한다. 암호화된 데이터를 수신한 서버는 자신의 개인키와 세션키를 이용하여 데이터를 복호화하게 된다. 따라서 중간에 악의적인 해커에 의한 데이터 유출 및 변경 또는 삭제로부터 데이터를 안전하게 보호하며, 데이터에 대한 인증, 기밀성 및 무결성 등을 제공한다.



[그림 5] 세션키와 공개키를 이용한 안전한 데이터 전송 절차

[그림 5]는 데이터 보호 시스템의 동작 과정을 도식화 한 것이다. 사용자 A는 데이터를 안전하게 서버에게 보내기 위해 서로 합의하에 생성한 세션키로 데이터를 암호화하고, 서버의 공개키로 다시 한 번 암호화하여 서버에게 전송하고, 서버에서는 이중 암호화된 데이터를 수신한 다음 자신의 개인키로 복호화하고, 그 결과 값을 다시 한 번 세션키로 복호화해서 평문의 데이터 값을 받게 된다.

V. 결 론

PKI 기반의 인증 시스템은 현재 인터넷 망에서 두 개체의 상호 인증을 위해 널리 사용되는 사용자 인증 시스템이다. 본 연구는 무선 PKI 기반의 인증 시스템을 기반으로 하여 각각의 인증서 교환을 통해 상대의 신원을 확인한 후 자신의 비밀키와 상대의 공개키를 통한 이중 암호화를 수행하여 데이터에 대한 인증, 기밀성, 무결성 등을 제공하는 데이터 보호 시스템을 제안한다.

PKI 기반 데이터 보호 시스템은 무선 인터넷 환경의 무선 단말기 상에서의 전자 상거래나 인터넷 뱅킹과 같은 중요 데이터의 안전한 전송이 필요한 서비스 혹은 개인 정보의 전송이 요구되는 시스템 상에 적절한 보안 서비스를 제공하며 유용하게 적용될 수 있다고 생각되며, 가치 있는 데이터의 안전한 보호에 도움을 줄 것이다.

참고문헌

[1] 박진우, 김영부, 박경준, "IT839 기반기술 BcN의 배경과 발전", 정보통신연구진흥원 기술정책 정보단2005. 8

[2] WAP Forum, Wireless Application Protocol Wireless Transport Layer Security Specification Version18-FEB -2000", Feb. 2000

[3] Wireless Application Protocol Wireless Identity Module Specification, WAP Forum, Feb. 2000

[4] 최용락, 소우영, 이재광, 이임영, "컴퓨터 통신 보안", 그린출판사, 2001

[5] 류종호, 염흥렬, "인증서 관리 프로토콜(CMP)의 최근 동향", 정보보호학회지, 제 10권 제 4호, 2002. 12

[6] 김지연, "PKI 구성 객체의 상호연동을 위한 명세서 분석", 한국정보보호진흥원, 1998. 7