이동 동기화 데이터 전송에 필요한 인증 및 디지털서명에 관한 연구

이근호, 이송희, 김정범, 김태윤
고려대학교 컴퓨터학과
e-mail:{root1004, pine, qston, tykim}@netlab.korea.ac.kr

A Study on Authentication and Digital Signature Need of Mobile Synchronization Data Transfer

Keun-Ho Lee, Song-Hee Yi, Jeong-Beom Kim, Tai-Yun Kim
Dept of Computer Science & Engineering, Korea University

요약

이동 통신의 발전으로 인하여 이동 단말기를 통한 정보의 전송에 대한 연구가 활발히 진행되어 지고 있다. 이동 단말기마다 플랫폼 구조가 각각 다르고 사용하는 언어도 각각 다르다. 이러한 각각의 단말기를 하나의 데이터 구조로 동기화 할 수 있는 SyncML을 이용하여 데이터의 동기화 과정을 소개한다. 본 연구는 동기화처리에 이용되고 있는 SyncML의 인증과 디지털 서명 부분에 대해서 분석해 보고 이동 데이터의 전송에 무선 PKI의 구조를 적용하여 이동 데이터에 대한 인증과 디지털 서명을 적용하는 시스템을 설계하였다.

1. 서 론

국내외적으로 이동 통신산업은 급격한 발전을 이루고 있다. 무선 데이터 서비스는 별도의 PC(Personal computer), PDA(Personal Digital Assistant) 등을 이용하여 접속해야 하는 불편한 점이 있지만 파일 송수신과 같은 많은 데이터 처리에 유용하다. WAP은 별도의 PC없이 단말기 자체로 처리가 가능하다. 이를 위해서는 단말기보다 상대적으로 넓은 화면의 단말기와 더 성능이 우수한 처리속도 및 메모리가 필요하고 시스템에서는 별도의 망 구성요소가 요구되어진다. 무선 단말기와 유선 단말기간의 데이터 처리를 위해서 WAP 프로토콜을 이용하고 있다.

무선과 유선상의 데이터는 다른 플랫폼 구조로 되어있어 데이터의 상호 교환이 어렵다. 이러한 부분을 보완하여 유.무선 데이터 동기화 처리를 가능하게 하는 것이 SyncML이다. 본 연구에서는 SyncML의 인증과정에 대해서 살펴보고, 이동 동기화 데이터 전송시스템에 인증과 디지털 서명을 적용한 시스템을 설계하였다.

2. 관련연구

이동 통신에서 사용되어 지고 있는 데이터 전송 시스템에 대해서 살펴보고, 유선과 무선상의 데이터에 대한 인증과 디지털 서명에 대하여 살펴보도록 하겠다.

2.1 유선 데이터 처리

유선상의 데이터처리는 XML 기반으로 설계되어 진다. XML은 활용 대상이 단순한 전자문서에서부터 무선 인터넷 컨텐츠 언어, 통신, 비즈니스 프로세스 및 워크 플로우까지 너무나 많은 분야로 확산 되고 있다.

XML기반 구조를 살펴보면 MIME(Message Representation), Transfer Protocol(HTTP, FTP, SMTP), XML DTD, Schema, DOM, SAX, XSL, XSLT, EDMS, Registry & Repository, Application의 기반 구조를 가지고 있다. 메시지를 보내고 받기 위해 특별한 응용 프로그램을 구축하여 메시지를 주고 받으며, 각각의 응용 프로그램마다 나름대로의 메시지를 구성하는 고유방식을 사용하였다. 즉 서로간의 메시지의 규약이 다르면 메시지를 주고 받을 때 많은 어려움이 있다. 이러한 어려움은 OSI TP4를 이용하는 X.400과 TCP/IP를 이용하는 SMTP간의 메시지 교환을 들 수 있다. 그 둘간의 통신은 게이트웨이(Gateway)로 해

결 될 수 있었는데 이러한 게이트웨이는 서로간의 통신을 위해 변환 작업을 수행하였다. 이러한 변환은 보기에는 쉬워 보이지만, 그렇게 간단하지만은 않은 작업이다. 이러한 변환 문제점들은 여러 가지가 있지만, 우선 근본적으로 다른 점은 인터넷 주소와 X.400의 주소체계가 완전히 다르다는데 있다. 또한 변환작업으로 인한 시스템의 부하도 무척 크다고 할 수 있다. 또한 메시지를 구성하는 봉투와 헤더에는 서로 다른 형식과 필드들로 구성되어 있기 때문에 한쪽에서만 존재하는 필드에 대해 처리하기가 곤란하다. 이러한 부분 문제점들은 극복하기 위한 가장 이상적인 방법은 서로 같은 메시징 방식을 채택하여 정보를 주고 받는 것이다.

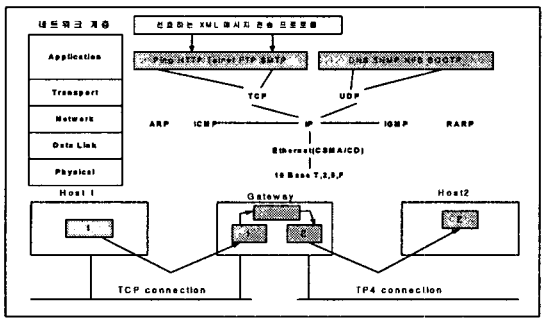

그림 1. XML 메시지 전송과 변환 과정

2.2 무선 데이터 처리

무선 인터넷은 WAP 포럼의 WAP(Wireless Application Protocol), Microsoft사의 ME(Mobile Explorer)와 Stringer, OPENWAVE사의 UP(Unwired Planet) Browser, NTT DoCoMo사의 i-mode 그리고, Qualcomm사의 단말기 플랫폼인 BREW(Binary Runtime Environment for Wireless)등 다양한 방법이 있다. 대부분의 무선 인터넷에서는 WAP 방식이 사용되어 지고 있다[3].

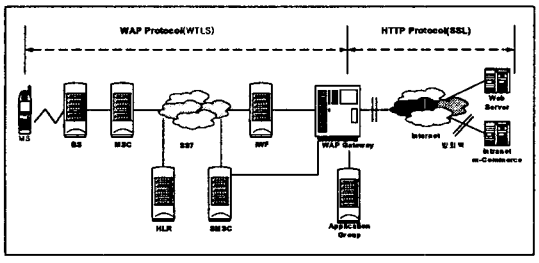

그림 2. WAP의 구조

2.3 WML 전자서명

WTLS에서는 기밀성, 무결성, 사용자 인증의 보안 서비스는 제공하지만 부인 봉쇄 기능은 제공하지 않는다. 부인봉쇄는 전송되는 데이터에 대해서 전자서명을 수행함으로써 제공이 가능한데, 전송되는 모든 데이터에 대해서 전자서명을 수행하는 것은 많은 연산을 필요로 하여 비효율적이기 때문이다. 따라서 부인 봉쇄 서비스는 애플리케이션 계층에서 제공하는 것이 일반적이다. 애플리케이션에서 부인봉쇄 서비스를 제공하기 위해서는 WAP에서는 WML 전자서명 매커니즘을 제공한다. WMLScript는 javaScript에 기반해서 설계된 WAP에서의 Script언어로수 그림 3과 같이 WMLScript Crypto Library에서 제공하는 Crypto.signText()라는 함수를 이용해서 WML 문서에 전자 서명하는 것이 가능하다. 이와 같은 경우 WML 문서 단위로 전자서명이 가능하기 때문에 사용자는 전자서명의 수행 때문에 발생하는 부담을 최소화 할 수 있다. 또한 WTLS와 WMLScript에 의한 전자서명을 함께 운용함으로써 기밀성, 무결성, 사용자 인증, 부인봉쇄 등 기본적인 정보보호 서비스를 모두 제공할 수 있다.

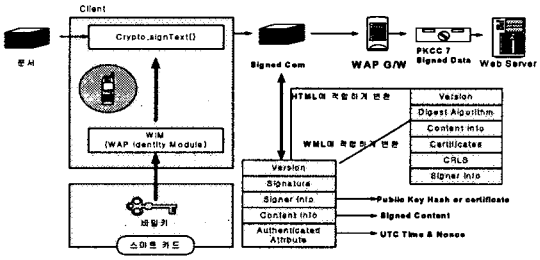

그림 3. WMLScript를 이용한 전자 서명

2.4 디지털 서명

전자화된 문서의 메시지 내용이 수정 및 변조되지 않았음을 보장하는 동시에 메시지 주체인 사용자들이 진정하다는 것을 제 3자가 확인 할 수 있게끔 하는 인증방식을 말한다. 전자화된 문서에 대한 서명의 종류는 크게 개인 신체의 고유성을 강조해서 지문, 성문(voice), 망막(retina)을 기준으로 파악하는 전자적 확인과 정보 보호 이론을 응용해 인증 하는 디지털 서명으로 구분한다. 디지털 서명의 종류는 상당히 많이 나와 있는데 미국에서 1991년에 표준 디지털 서명인 DSS(Digital Signature Standed)를 공포한 상태이며, 기술적으로 KCDSA(Korean Certificate Digital Signature Algorithm)를 검토하고 있는 중이다. 그 외에도 독일의 Schorr방식, Nyberg-Rueppel 방식 등이 있고, 공통키 암호 시스템을 이용한 Rabin, RSA, ElGamal 서명 방식, ID를 이용한 Fiat-Shamir방식과 Ohta방식, Knapsack문제를 이용한 Merkle-Hellman 방식등 상당수의 디지털 서명 방식이 나와 있는 상태이다[1].

2.5 SyncML 인증

SyncML은 데이터 동기화를 위한 프레임웍을 제공할 뿐 새로운 보안 스키마는 정의하지 않는다. 대신 신청에 의한 인증(challenge authentication), 인증(authentication), 권한부여(authorization)를 위한 프레임웍을 제공한다. 그래서 송신자는 다양한 보안 매커니즘을 추가해서 사용할 수 있다[2].

SyncML Representation프로토콜 스펙에서는 Chal 엘리멘트를 통해 인증을 요구한다. Cred엘리먼트를 통해 인증정보를 교환하도록 정의하고 있다. SyncML프로토콜 스펙에서는 인증 정보의 교환 과정을 위해 두가지방식을 정의하고 있다. 인증방식은 기본교환과 MD5 Digest Access 방식을 정의하고 있다. 인증정보의 표준은 Base64이다. 기본교환은 Base64 포맷으로 인코딩해 상대편으로 전송하는 일반적인 방식이다. MD5 Digest Access는 Chal엘리먼트의 NextNonce 필드에 인증정보를 담아 상대방에게 전송하고, 상대방은 다음 동기화 패키지를 보낼 때 Cred엘리먼트안의 수신한 Chal 엘리먼트의 NextNoce에 담겨진 정보를 Data에 담아 상대방에게 전송해야 한다. 기본 포맷으로 사용하는 Base64는 MIME에서 바이너리 데이터를 인코딩/디코딩하는데 사용하는 방법이다. 내부적으로 바이너리데이터를 ASCII문자열로 변형하는데, 변형방식은 원래 데이터에서 3바이트씩을 묶어 네 개의 6비티(24비트)단위로 바꾼다. 이렇게 바꾸면 원래 바이너리 데이터 크기보다 1/3정도 커진다. Base64의 체계는 RFC1521에 명시되어 있다[7].

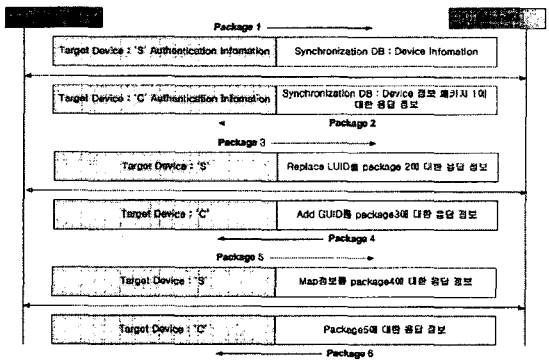

그림 4. SyncML 동기화 처리

3. 동기화 데이터의 인증 및 디지털서명 시스템 설계

3.1 동기화 데이터 인증

동기화 데이터 처리에 SyncML을 이용한다.

- Base64 인증

패키지 1은 클라이언트가 송신자의 인증 정보를 가지는 Cred커맨드 없이 서버에 접근하려 한다. 패키지 1은 인증 정보가 없기 때문에 서버와 곧바로 동기화 처리를 할 수 없다.

인증정보가 없는 메시지를 받았기 때문에 서버는 인증을 위해서 다시 패키지 2에서 Chal을 보낸다. 이때 서버는 Chal 태그의 메타 정보로 타입 syncmlauth-basic과 포맷 b64를 설정하여 Chal을 전송한다. 클라이언트는 반드시 메타 타입이 syncml:auth-basic인 Cred와 인코드된 데이터를 패키지 1로 재전송해서 다시 인증 과정을 확인한다.

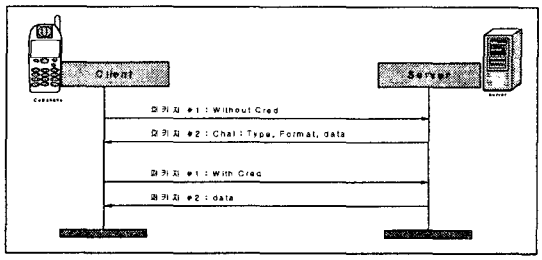

그림 5. 인증 신청이 있는 Base64

- MD5인증

패키지 1은 클라이언트가 송신자의 인증 정보를 갖는 Cred 없이 서버에 접근한다.

패키지 1은 인증 정보가 없기 때문에 서버와 즉시 동기화를 할 수가 없다.

인증정보가 없는 메시지를 받았기 때문에 서버는 인증을 위한 시도를 위해 패키지 2에서 Chal 명령어를 전송하여 인증정보가 빠졌음을 알린다. 클라이언트는 반드시 타입 태그에 syncml:auth-md5를 표기하고 데이터에는 MD5로 인코드된 데이터를 Cred를 갖는 패키지 1을 재전송 한다. 서버는 Cred를 받아들이고 세션을 인증하게 된다. 이때 서버는 Basic과는 다르게 Nextnonce값을 보내기 위해서 Chal 명령어를 포함한 Status 명령어를 보낸다.

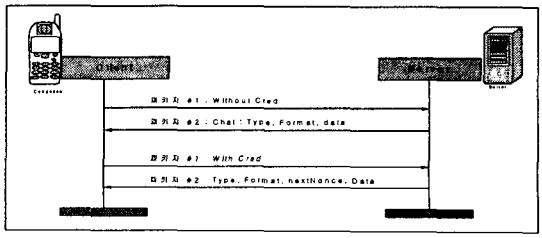

그림 6. 인증 신청이 있는 MD5 인증

3.2 이동 동기화 데이터의 인증 및 디지털 서명 시스템

동기화를 처리할 수 있는 SycnML 서버의 플랫폼 구조를 분석하였다. SyncML은 Sync Engine에서 인증과정이 일어난다. SyncEngine의 Authentication Handler에서는 인증 타입의 개수와 관계없이 세가지 함수에서 모든 부분에 대한 인증을 처리하게 된다.

세가지 함수는 Basic과 MD5에 대해서 구현되어 있다. SyncEngine을 이용하여 동기화 데이터를 인증처리하고, 인증처리된 데이터는 Chal element를 이용하여 인증 신청을 받아서 데이터를 인증한다. 그림 7의 시스템에서는 SyncML의 인증처리부분을 이용하여 인증기관에 인증서를 발급 받는다. 인증기관은 유선 인증기관과 모바일 인증기관을 따로 두어 각 인증서의 발급과 관리를 담당하도록 한다. 인증기관의 모델은 무선PKI를 기반으로 하였다. 무선 단말기에서 데이터의 동기화를 처리한후 인증서 URL, 인증서를 PKI Portal에 의뢰하므로서 이동 단말기를 인증해 준다. 인증 처리시에 디지털 서명을 하여 사용자의 신원을 확인한다.

WAP의 방식에서는 WTLS를 유선에서는 SSL방식을 이용하여 데이터를 안전하게 전송할 수 있다.

동기화 처리를 위한 SyncML 서버의 플랫폼 구조를 이용하여 이동 데이터의 인증 및 전자서명을 생성하여 중요한 데이터를 전송하도록 설계하였다.

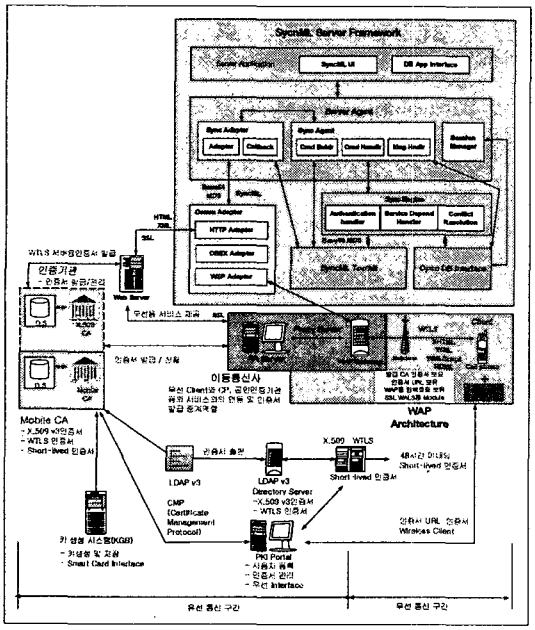

그림 7. 인증 및 디지털 서명에 관한 시스템

4. 결론 및 향후과제

본 논문에서는 이동 통신에서 사용하는 동기화 데이터 처리에 대한 구조를 이해하고, 동기화 데이터 처리시 발생할 수 있는 보안 문제점에 대하여 살펴보았다. 이동 통신과 유선간의 데이터 동기화 처리시 발생할 수 있는 보안 문제를 해결하기 위하여 SyncML의 인증 부분을 이용하여 전자서명 표준을 지원하는 시스템을 설계하였다. 향후 본 시스템에 대한 인증 및 전자 서명의 안정성 검증을 통한 프로토콜을 설계하도록 한다. 본 시스템의 설계 부분을 전자상거래에서 요구하는 안전성을 충족하기 위한 응용시스템에 대한 연구 및 개발을 해 나갈 예정이다.

참 고 문 헌

[1] 이만영, 김지홍, 류재철, 송유진, 염홍열, 이임영, "전자상거래 보안 기술", 생능출판사, 1999

[2] 김창회, 류수희, 최훈, "SyncM 인증(Authentication) 기능 구현", 정보과학회 가을 학술발표 논문집, Vol. 28. No. 4, 2001, page : 754-756

[3] "동기화 표준 SyncML의 표준화 동향", ITFIND, 주간 기술 동향, 통권 1031호, 2002.01.30, ETRI IT 정보센터

[4] SyncML, http://www.syncml.org

[5] 하인숙, 조재혁, 양지현, "데이터 동기화의 표준 SyncML기초 다지기, 마이크로 소프트웨어, 2001.5월, page:330-340

[6] 김세영외 5명, " XML 전자서명 시스템의 설계 및 구현", 정보처리학회 추계 학술발표논문집 제 8권, 제 2호 page:891-894

[7] 하인숙, 조재혁, 양지현, "SyncML 레퍼런스 툴킷 그 내부를 보자", 마이크로 소프트웨어, page:324-336, 2001. 7

[8] WAP specifications.
http://www.wapforum.org/what/technical.htm

[9] S.Saba, M. Jamtagaard, J. Villasenor, "Bringing the Wireless Internet to Mobile Devices", Journal of the Computer 2001, page : 54-58, June, 2001

[10] 박남제, 송유진, "모바일 서비스 플랫폼 기반의 무선 전자상거래 보안 기술", 정보보호학회지, 제 11권, 제 4호, 2001.8, page : 9-28