안전한 전자서명을 위한 상호인증 메커니즘에 관한 연구

최상욱* · 채철주* · 이재광*

*한남대학교 컴퓨터공학과

A Study on The Mutually Authentication Mechanism for The Safe Electronic Signature.

Sang-Wook Choi* · Cheol-Joo Chae* · Jae-Kwang Lee*

*Dept of Computer Engineering, Hannam University

E-mail : [suchoi, cjchae, jklee]@netwk.hannam.ac.kr

요 약

무선 통신 기술이 발전함에 따라 모바일을 이용한 전자상거래가 활성화 되었다. 이러한 전자상거래의 안정성을 보장하기 위해서 WPKI가 개발되었지만 모바일 단말기의 기술적 제한 때문에 유선 통신에서와 같은 안전한 PKI 서비스를 보장받기 어렵다. 본 논문에서는 모바일 단말기의 제한적 특성을 고려해 안전하고 효과적인 전자금융 서비스를 위한 인증 시스템과 안전한 전자서명을 위한 암호화 알고리즘을 제안한다. 이는 WPKI에서 각 인증기관의 상호인증을 가능하게 하고 KCDSA 알고리즘과 SEED 알고리즘을 이용한 서명인증을 통해 안정성을 높였다.

ABSTRACT

As the wireless communication technology developed, the Electric Commerce using a mobile was activated. WPKI was developed in order to guarantee the stability of the Electric Commerce but it is difficult to be ensured for the safe PKI service which is the same at the wire communication in the technical because of restriction of the mobile terminal. In this paper, we propose the authentication system for the electronic financial service which is safe and is effective in consideration of the restrictive characteristic of the mobile terminal. Moreover, the encryption algorithm for the safe electronic signature is proposed. In WPKI, this makes the cross certification of each certificate authority possible. Moreover, a stability was enhanced through the signature authentication using KCDSA and SEED algorithm.

키워드

WPKI, KCDSA, CRL, OCSP, 상호인증

Ⅰ. 서 론

컴퓨터와 통신의 발전은 오프라인상의 전자상거래를 인터넷을 이용한 전자상거래로 발전시켜 왔다. 인터넷을 이용한 전자상거래 역시 무선 인터넷의 대중화와 맞물려 급속도로 반전하고 있는 가운데 현재는 모바일을 이용하는 전자상거래가 일반화 되었다. 이러한 전자상거래의 안정성을 보장하기 위해서 PKI를 기반으로 하는 WPKI가 개발 되었다. WPKI는 상대방의 공개키에 대한 유효성 검사를 위해 인증서를 사용하게 되며, 인증서는 검증된 공인 인증기관의 승인 하에 전자상거래에 이용된다. 또한 인증기관의 유효성 검사와 더불어 금융기관과의 전자서명을 통해서 안전한 뱅킹 데이터 전송을 완료하게 된다. 인증기관은 인증서의 유효성 여부 및 정지, 폐지 결정을 하기 위해서 위해서 CRL 및 OCSP를 활용하고 서명 인증을 위해서 RSA, DSA 알고리즘 등을 사용한

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

다. 그러나 모바일을 이용한 전자상거래는 모바일 폰의 특성상 유선 통신보다 성능의 제한이 따르고 상대적으로 저속의 통신을 제공하기 때문에 CRL이나 이를 개선하기 위해 등장한 확장 CRL 및 OCSP를 이용한 유효성 검증은 효율성이 떨어진다.

이에 따라서 본 논문에서는 에이전트 서버를 이용한 모바일 PKI 보안 시스템과 국내 표준 알고리즘인 KCDSA를 이용한 모바일 PKI 보안 시스템을 제안하는 바이다. 본 논문의 구성은 다음과 같다. 먼저 2장에서는 관련 연구와 더불어 CRL, OCSP를 이용한 기존 무선인증 시스템의 문제점과 서명인증 알고리즘을 분석하고 3장에서는 에이전트 서버를 이용한 대리 인증 시스템과 KCDSA와 SEED 알고리즘을 사용한 전자서명 시스템을 제안하며, 4장에서는 구현 시스템의 결과 분석, 마지막으로 5장에서는 앞으로의 나아갈 방향과 효율적인 활용 방안을 제시한다.

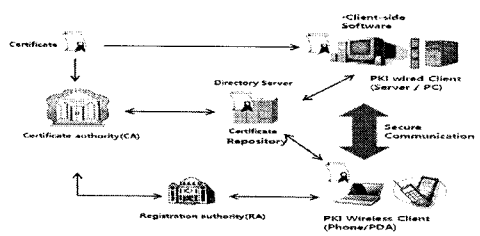
II. 관련 연구

2.1 PKI

인터넷의 개방적 구조는 인가되지 않은 사용자의 접근이 가능하다는 특징을 가지고 있으며 이것은 비인가자에 의한 불법이 자행될 수 있음을 의미한다. 전자상거래를 위해서는 당사자간의 신뢰성 보장과 상호 인증이 가능해야 하며, 이것은 인증, 부인봉쇄, 무결성 등의 서비스를 제공하는 전자서명 기술을 이용해 해결 가능하고 이러한 효과적인 전자서명 기술을 위해서는 RSA, DSA 등과 같은 전자서명 암호화 알고리즘이 필요하다. 공개키 암호화 방식을 이용한 인증을 구현하기 위해서는 기술적, 제도적 기반이 요구되는 공개키 기반구조(PKI : Public Key Infrastructure)를 사용해야 한다.[1]

2.2 WPKI

WPKI는 유선 PKI의 구성요소를 그대로 이용해 무선 단말기에 적용한다. 모바일 단말기의 특성을 고려해 클라이언트와 서버간의 대역폭, 클라이언트의 처리 속도, 제한된 메모리 및 인증서 검증 메커니즘의 경량화를 통해 무선 환경에 적합하도록 기능을 최소로 변화시켜 사용한다.



[그림-1] WPKI 구조

WPKI 구조는 다음 [그림-1]에서 볼 수 있드시 인증기관(CA), 등록대행기관(RA), 클라이언트, 디렉토리 서버(repository)로 구성된다. 인증기관은 인증서의 발급 및 인증서의 효력 정지 및 폐지 유무를 결정하는 역할을 하고, 등록기관은 사용자와 인증기관 사이에서 인증서의 신규 등록 및 신원 확인을 담당한다. 디렉토리 서버는 CRL 및 인증서의 저장 관리 역할을 담당하며, 클라이언트는 등록 대행 기관을 통해 공개키 쌍을 생성한다.[1][2]

2.3 CRL

인증기관에서는 인증서의 유효성을 검사하기 위한 방법 중 하나로 CRL를 사용한다. 조직 내외에서 사용자의 지위나 권한 변경, 암호키의 분실, 도난, 종업원의 퇴사 등의 이유로 인증서의 유효기간의 만기일이 도래하기 전에 인증서의 효력이 상실되어 폐지해야 하는 경우가 발행하는데 이런 급작스런 인증서 내용 변경 및 취소 정보를 취합한 것이 인증서폐지목록(CRL)이다.[3] CRL은 인증서의 유효성 목록을 갱신하는 시간이 정해져 있고, 목록 전체를 다운 받아야 한다. 이것은 인증서의 폐지 목록의 크기가 커질수록 다운 받는 양이 커지고 목록 갱신을 위한 시간이 증가하게 되며, 결과적으로 통신량의 증가로 인한 과도한 트래픽을 유발하게 된다. 따라서 CRL은 실시간 업데이트를 요구하는 금융 거래에는 적합하지 못하다.

2.4 OCSP

CRL 및 확장 CRL의 실시간 검증이 불가능하다는 문제점을 해결하기 위해 제안된 OCSP는 1999년 6월 RFC2560로 표준화되었고 99년부터 상업적으로 사용되기 시작하였다. OCSP는 먼저 Certificate Validation Module가 인증서 폐기 여부를 조회하기 위해 OCSP 클라이언트를 호출하고 OCSP 클라이언트는 HTTP로 PKI Portal을 통해서 OCSP Responder에 접속하여 인증서 폐기 상태 정보를 실시간 조회한다.[4]

실시간 취소 검증이 가능한 OCSP는 사용자가 CA와 직접 접촉하여 인증서의 유효성을 확인함으로써 시간 지연 문제를 해결했다. 그러나 OCSP 역시 CRL과 마찬가지로 하나의 인증서 저장 서버에 트래픽이 집중화됨으로써 병목 현상에 의한 서비스 지연 처리 문제가 발생하고 네트워크 상태에 따라 인증서 유효성 검사의 수행시간이 유동적인 문제를 야기 시킨다. 이처럼 서버의 과부하 현상을 막기 위해 D-OCSP를 설계함으로써 인증서 저장소의 트래픽 집중화를 최소화 할 수 있다.

2.5 KCDSA

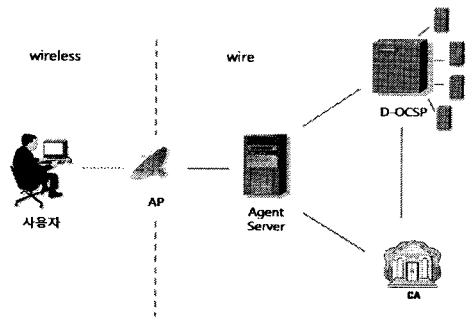
KCDSA(Korea Certification-based Digital Signature Algorithm)는 이산대수 문제의 어려움

에 기반을 둔 전자서명 알고리즘으로서, 한국통신정보보호학회의 주관 하에 국내의 암호학자들에 의해 1996년 개발되었으며, 지속적인 수정 및 보안 작업을 통해 한국전자통신연구원과 공동으로 TTA 단체에 제안되었다.[5] 그러나 KCDSA는 뱅킹 데이터 전송 시 암호화를 진행하지 않는다는 보안상의 문제점을 가지고 있다.

III. 제안 시스템 설계

3.1 제안 시스템의 구성

본 논문에서 모바일폰의 제약사항을 고려한 PKI 기반 무선랜 보안시스템을 제안한다. 무선랜 보안시스템의 전체 구성은 [그림-2]와 같다. 최초 모바일 인증자는 인증자가 속한 AP를 이용해 AS(agent server)에 접속하게 되고 AS는 인증자의 요구에 따라 OCSP 서버를 이용한 실시간 인증서 유효성 검사를 한다. OCSP는 부하가 집중되는 것을 방지하기 위해 분산 D-OCSP로 설계되며 에이전트 서버는 타 인증기관에서 발행한 인증서의 유효성 여부 및 폐지 유무를 검증하기 위해 다른 그룹의 에이전트 서버와 상호인증 단계를 거친다.



[그림-2] 대리인 서버 시스템 구성

3.2 전자서명 알고리즘 구현

안전한 데이터 전송을 위해 국내 표준 서명 알고리즘인 KCDSA를 사용한다. 그러나 KCDSA는 뱅킹 데이터 전송 시 암호화 하지 않는다는 문제점을 가지고 있기 때문에 이를 해결하기 위해서 SEED 암호화 알고리즘을 사용한다. SEED 알고리즘은 한국정보보호진흥원에서 개발한 128 bit 대칭 알고리즘으로써 국내 표준 암호 알고리즘이다. KCDSA 서명 알고리즘을 이용한 전자서명은 다음과 같은 서명 생성 과정과 서명 검증 과정으로 나뉜다.

3.2.1 서명 생성 과정

Step 1. 도메인 변수와 공개 검증키의 검증과정을 거친다.

Step 2. 난수 값 K를 랜덤하게 선택후 증거 값 $W = G^K \bmod P$를 계산한다.

Step 3. 증거값을 이용해 서명을 첫 번째 값 R =h(W)를 계산한다.

Step 4. Z = Y mod 2을 계산해서, 해쉬코드 H = h(Z || M)을 계산한다.

Step 5. 중간 값 E =(R ⊕ H) mod Q를 계산하고 서명의 두 번째 값 S = X(K - E) mod Q를 계산한다.

Step 6. 비트열 R과 정수 S의쌍, ∑= {R, S}를 서명으로 출력한다.

3.2.2 서명 검증 과정

Step 1. 서명자의 인증서를 확인 후, 서명검증에 필요한 도메인 변수와 공개 검증키를 추출한다.

Step 2. 수신한 서명 ∑'= {R', S'}에 대해 R' 해시 함수의 출력 길이와 같은지 확인한다.

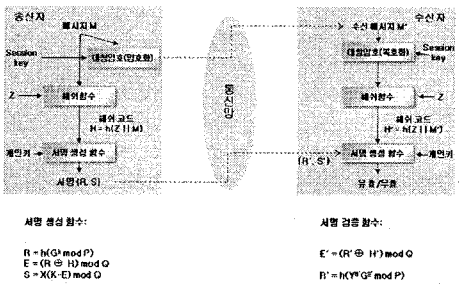
Step 3. 중간 값 E' =(R' ⊕ H') mod Q를 계산한다.

Step 4. 서명자의 공개 검증키 Y를 이용하여 증거 값 $W' = Y^{s}G^{e'} \bmod P$를 계산한다.

Step 5. h(W') = R' 이 성립하는지 확인한다.

3.3 데이터 암호화

KCDSA를 이용한 전자서명 방법의 문제점을 보안하기 위해서 SEED 알고리즘을 사용하여 뱅킹 데이터를 암호화 한다. [그림-3]은 서명 인증 및 검증 과정에서 대칭키 알고리즘을 이용한 이중 메시지 암호화 과정을 보여준다.



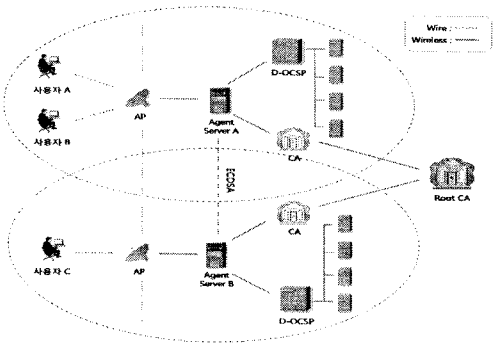
[그림-3] 서명 인증 및 검증 과정

이처럼 모바일 뱅킹 데이터를 암호화함으로써 메시지 전송 간에 발생할 수 있는 데이터 위조, 변조 및 가로채기 공격에 대응 가능하다.

3.4 상호인증 및 데이터 전송

무선 단말기는 앞서 기술한 바와 같이 유선에 비해 상대적으로 성능이 낮으며 저용량의 메모리를 가지고 있기 때문에 인증 처리 과정이 느리다. 이는 에이전트 서버를 이용한 대리 인증 과정을 통해 해결할 수 있다. 에이전트 서버는 모바일 사용자를 대신해 인증서를 발급 받는다. 대리 인증

서를 발급받은 에이전트 서버는 다른 CA에서 발급된 인증서를 보유하고 있는 또 다른 에이전트 서버와 상호 인증을 위해 EAP를 사용한다. [그림-4]는 다른 CA에서 발급 받은 대리 인증서를 이용한 상호인증 기반 데이터 통신 과정을 보여 준다.



[그림-4] CA간의 상호 인증 설계

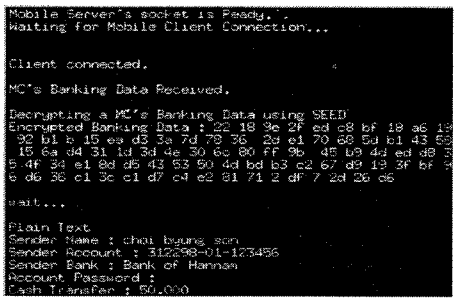
대리 인증서를 이용한 모바일 사용자와 다른 CA에서 인증서를 발급 받은 사용자B의 상호 인증 과정은 다음과 같은 인증 단계를 거친다.

1. IEEE 802.11x에 의해 모바일 사용자A는 에이전트 서버에게 접속 요청 후 에이전트 서버 A는 접속 허용 여부를 결정
2. 에이전트 서버 A는 인증된 사용자의 인증서를 호출하고 이를 통해 통신하고자 하는 모바일 사용자 B의 에이전트 서버 B에게 데이터 전송을 위한 통신 요청.
3. 에이전트 서버 B는 서버 A와 EAP를 이용한 상호인증.
4. 유효성 검증을 마친 에이전트 서버B는 데이터 전송을 허용.
5. 에이전트 서버 A와 서버 B는 데이터 전송을 위해 ECC기반 암호화 알고리즘을 사용.
6. 데이터 전송을 받은 서버 B는 모바일 사용자 B에게 데이터를 전달.
7. 데이터 전송 후 완료 메시지 전달하고 상호인증 연결 종료.

IV. 시스템 구현 결과

3장에서 설계된 암호화 알고리즘의 구현 결과이다.

[그림-5]는 모바일 서버가 에이전트 서버로부터 암호화된 모바일 뱅킹 정보를 전송받은 후, 복호화 과정을 보여준다.



[그림-5] 뱅킹 데이터의 복호화

이처럼 본 논문에서 제안한 시스템은 KCDSA 알고리즘에 SEED 알고리즘을 적용함으로써 보다 보안성이 강화된 전자서명이 가능해졌다.

V. 결 론

본 논문에서는 모바일 단말기의 제한적 특성을 고려해 대리인 서버를 이용한 효율적인 모바일 인증 및 상호인증 메커니즘을 설계하고 뱅킹 데이터의 암호화를 통해 보다 안전한 전자서명이 가능하도록 설계하였다. 인증서의 유효성 검증을 위해 에이전트 서버는 D-OCSP를 사용하여 트래픽의 분산화와 더불어 모바일 단말기의 하드웨어적 한계를 극복함과 동시에 KCDSA와 SEED 알고리즘의 접목으로 보다 안전한 데이터 암호화가 가능해졌다. 이를 통해 모바일 단말기를 이용한 전자상거래 및 모바일 단말기간의 데이터 전송에 있어 안전함을 보장할 수 있고 새로운 소형 단말장치에 적용 가능할 것이다. 또한 모바일 통합인증 시스템에 적용함으로써 보다 효율적인 상호인증 및 전자상거래가 가능해질 것이다.

참고문헌

[1] Wiress Application Protocol Wireless Identity Module Specification, WAP Forum, Feb. 2000.
[2] WAP Forum, Wireless Application Protocol Wireless Transport Layer Security Specification Version18-FEB -2000, Feb. 2000.
[3] 채송화, "CRL 분배 및 온라인 인증서 상태 확인 비교", 전자서명 인증관리 센터, 한국정보보호진흥원, 1999.
[4] M.Myers et al, "Draft, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol", version 2, IETF, 2002
[5] Moonseog Seo and Kwangjo Kim, "Blind Signature Schermes based on KCDSA and EC-KCDSA", CISC'99, Vol.9, No.1, pp.141-150, 1999. 11.6.