ECDSA인증모듈을사용한 웹카메라서버용영상처리시스템구현

*차 재 원, *박 덕 용, **김 영 철
*전남대학교 전자공학과, **전남대학교 전자 컴퓨터 정보통신 공학부
전화 : 062-530-0369 / 핸드폰 : 016-608-3857

Implementation of mutual Authentication Module using ECDSA for web-Camera system

*Jae-Won Cha, *Duck-yong Park, **Young-Chul Kim
*Dept of Electronics Engineering, Chonnam National University
**Dept of Electronics & Computer Engineering and RRC-HECS, Chonnam National University
E-mail : jwcha@neuron.chonnam.ac.kr

Abstract

In this paper, we propose a mutual Authentication module, using ECDSA(Elliptic Curve Digital Signature Algorithm) for web-Camera system. which. is based on three module. first is authentication module which is based on ECDSA algorithm. second is transfort module using stream socket. the last module is graphic module.

This paper describes cipher algorithm which can be used restrict condition for the same secret service with wire internet. we made a authentication module using based client and server system.

I. 서론

최근 인터넷 쇼핑몰과 같은 B2C 전자상거래가 활성화 되면서 정보 위조 및 유출에 대한 위협 뿐만 아니라 신분 위장에 의한 사기사건이 크게 문제 되고 있다. 따라서 거래 상대방에 대한 신원 확인 작업인 인증의 중요성이 커지고 있다. 이러한 인증 서비스에 이용되는 기술은 기존의 아이디와 패스워드를 이용한 방식, 일회용 패스워드(One Time Password)방식, X.509 공개키 인증서를 이용한 방식, SSO(Single sign on)등이 있다. 작년 전세계 정보기술업계의 침체에도 불구하고, 세계 보안시장 규모는 계속 증가하고 있으며 인증 암호화 시장은 2005년까지 연평균25%정도의 고성장이 예상되고 있다. 이는 정보보호 솔루션 중에서도 기반기술에 속하는 인증 암호화 특성상 타 정보보안에 비해 범용성 및 확장성이 탁월하기 때문이라 할 수 있다.

본 논문은 Ⅱ절에서 이산대수 문제에 기초한 타원곡선 암호 시스템의 배경에 대해 살펴보고 Ⅲ절에서 제한된 resource환경에서도 유선인터넷과 동등한 전자서명,인증 서비스를 제공할 수 있는 암호알고리즘 대해 기술하고 Ⅳ절에서 이를 인증보안 모듈로 웹 카메라 서버용 영상처리 시스템에 적용하고 마지막으로 Ⅴ절에서 결론 및 연구 및 응용분야에 대해서 기술하였다.

Ⅱ.타원곡선 암호 시스템의 배경

타원 곡선(Eliptic Curve)은 약 150년 전부터 광범위

※ 본 논문은 일부 "한국과학재단 지정 전남대학교 고품질 전기전자부품 및 시스템 연구센터(RRC)의 연구비 지원"과 "IDEC의 CAD툴 지원"에 의해 이루어졌음.

한 연구가 있어 왔고, 10여년전 비트당 안전도가 타 공개키 시스템보다 효율적이라는 것이 알려졌으며 최근 높은 속도의 구현이 가능하게 되었다.

타원곡선을 이용한 공개키 암호 시스템 즉, 유한체(finite fields)위에서 정의된 타원곡선 군에서는 이산대수 문제에 기초한 타원곡선 암호시스템(ECC, Eliptic Curve Cryptosystem)은 1985년 N.Koblitz와 V. Miller에 의해 처음 제안된 이후 활발히 연구되고 있다.

2.1 타원곡선 암호 시스템의 장점

타원곡선 암호시스템은 유한체의 곱셈군에 근거한 시스템으로써 다음의 장점을 가진다.

①군(Group)을 제공할 수 있는 다양한 타원곡선을 활용할 수 있다. 즉 다양한 암호시스템 설계가 용이하다.

②타원곡선, 암호시스템은 존재하는 다른 공개키 스킴과 같은 안전도를 제공하는 데에 더 작은 키 길이를 가지고 가능하다.(예, RSA 1024비트 키와 ECC 160 비트 키를 갖는 암호 시스템을 같은 안전도를 갖는다)

③타원곡선에서의 더하기 연산은 유한체에서의 연산을 포함하므로, H/W와 S/W로 구현하기가 용이하다. 더욱이 이 군에서의 이산대수 문제는 특히, 같은 크기의 유한체 k에서의 이산대수 문제보다 훨씬 어렵다고 알려져 있다.

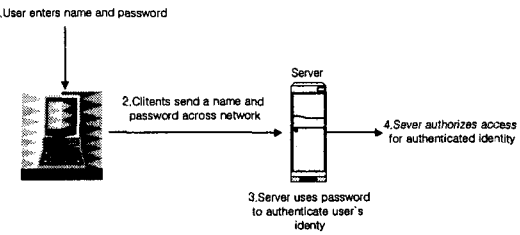
Ⅲ.인증 서비스 기술

분산 환경이 대량 보급되면서 컴퓨터 통신망에 접속된 단말기에서의 정당한 사용자를 확인하는 과정이 필수적인 요건으로 대두되고 있다. 중요한 정보나 자원을 보호하기 위해서는 컴퓨터 통신망에 불법 접속을 시도하는 것을 차단하는 방법이 필요하다. 이러한 정당한 사용자를 확인하는 과정을 사용자 인증이라고 한다.

또한 컴퓨터 통신망에서 전달되는 정보가 변경되지 않고 원하는 상대방에게 전달되고 있는지 확인하는 것 역시 중요한 일이다. 전달되는 정보의 변경은 송신자와 수신자 사이에 불신과 분쟁을 유발할 염려가 있어 송신자가 전송한 내용이 수신자에게 정보의 변경없이 전송되었는가를 상호 확인 할 수 있어야 한다. 이러한 과정을 메시지 인증이라 한다.

3.1 Password Based Authentication

[그림1]는 이름과 패스워드에 의해서 클라이언트가 인증하는 기초적인 단계를 보여주고 있다



【 그림 1 】 Password에 의한 인증 과정

[그림1]에서 다음 같은 단계를 보여주고 있다.

1) 서버로부터 요구되는 인증에 응답하기 위해서, 클라이언트는 사용자의 이름과 패스워드를 묻는 dialog box가 화면에 나타나게 된다. 사용자는 원하는 작업 세션을 사용하기 위해서 각각의 서버에 적용되는 이름과 패스워드를 입력해야 한다.

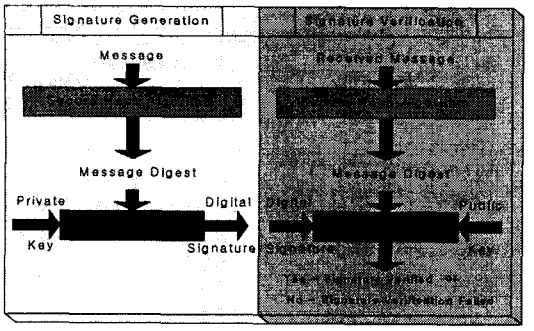
2) 클라이언트는 암호화하지 않거나 SSL에 연결하여 암호화해 네트웍을 통하여 이름과 패스워드를 보낸다.

3) 서버는 로컬 패스워드 데이터베이스에서 이름과 패스워드를 찾고 일치하면 사용자의 신원을 인증하는 증거로써 입력한 이름과 패스워드를 받아 들인다.

4) 서버는 신원이 확인된 사용자에게 사용자가 원하는 자원접근을 허가 할지를 결정하고 또한 클라이언트에게 자원 접근을 허가한다. 이러한 협정에 의해서 사용자들은 각각의 서버들에 대해서 새로운 패스워드를 입력해야 한다. 그리고 일반적으로 분리된 서버들의 관리자들은 각각의 사용자들에 대한 이름과 패스워드를 관리 해야만 한다

3.2. ECDSA를 이용한 인증 기술

ECDSA는 ANSI의 미 은행 연합(American Bankers Association)에 의해 X9.62로 표준화 되어 현재 널리 쓰이고 있는 전자 서명으로 기존의 미 연방 표준인 DSA(Digital Signature Algorithm) 전자서명을 타원곡선을 이용한 전자서명 알고리즘으로 변형한 것인데, 기존의 전자서명 알고리즘인 DSA, RSA와 함께 2000년 1월에 미국 전자서명 표준(DSS)에 포함되는 것으로 승인(FIPS PUB 186-2) 되었다.



【그림 2】 전자 서명 알고리즘

3.3 ECDSA 암복호화 알고리즘

ECDSA는 DSA를 타원곡선으로 변형시킨 것이다. ECDSA와 DSA의 중요한 차이점은 r의 생성에 있다. DSA는 r을 임의의 $g^k \bmod p$를 선택/계산한 후, mod q를 계산하여 얻는다. 그러나 ECDSA에서 r은 임의의 점 kP의 x 좌표를 mod n 하여 얻는다. ECDSA가 약 160비트 q와 1024비트 p를 가진 DSA와 비슷한 안전도를 갖기 위해서는 매개변수 n이 약 160비트이면 된다. 이 경우 DSA와 ECDSA는 같은 서명길이(320비트)를 갖는다.

[ECDSA 키생성] Alice가 키를 생성한다고 가정하자.
① Z_p에서 정의된 타원곡선 E를 선택한다. $\#E(Z_p)$는 큰 소수 n에 의해 나누어져야 한다.
② 위수 n인 점 $P \in E(Z_p)$를 선택한다.
③ 구간 [2, n-2]에서 통계적으로 유일하고 예측불가능한 정수 d를 선택한다.
④ Q = dP를 계산한다.
⑤ Alice의 공개키는 (E,P,n,Q)이고 비밀키는 d이다.

[ECDSA 서명생성] 메시지 m에 Alice가 서명한다고 가정하자.
① 구간 [2, n-2]에서 통계적으로 유일하고 예측불가능한 정수 k를 선택한다.
② $kP=(x_1,y_1)$과 $r=x_1 \bmod n$을 계산한다.(x_1은 정수로 간주)
③ r=0이면 ①단계로 되돌아간다.
④ $k^{-1} \bmod n$을 계산한다
⑤ $s=k^{-1}\{h(m) + dr\} \bmod n$을 계산한다.(h:SHA-1)
⑥ s=0이면 ①단계로 되돌아간다.
⑦ 메시지 m에 대한 서명은 (r , s)이다.

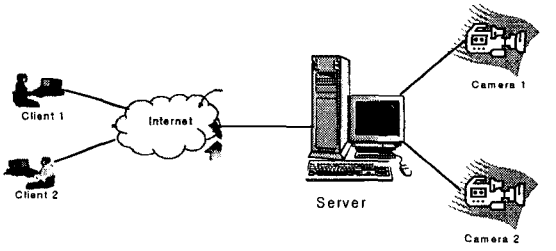
서명(sign)	검증(verification)
$k \leftarrow \{1,\ldots,n-1\}$	$e \leftarrow SHA1(m)$
$(x_1,y_1) \leftarrow kG$	$a \leftarrow s^{-1}e \bmod n$
$r \leftarrow x_1 \bmod n$	$b \leftarrow s^{-1}r \bmod n$
$e \leftarrow SHA1(m)$	$(x_2,y_2) \leftarrow aG + bQ$
$s \leftarrow k^{-1}(e+dr) \bmod n$	$t \leftarrow x_2 \bmod n$
서명:(r,s)	r=t인지 검증

【표 1】 ECDSA의 서명 및 검증

[ECDSA 서명생성] Bob이 Alice의 서명(r , s)을 검증한다고 가정하자.
① Alice의 인증된 공개키 (E,P,n,Q)을 얻는다.
② r과 s가 구간[1,n-1]에 있는 지 확인한다.
③ $w=s^{-1} \bmod n$과 h(m)을 계산한다.
④ $u_1=h(m)w \bmod n$과 $u_2=rw \bmod n$을 계산한다.
⑤ $u_1P+u_2Q = (X_0,Y_0)$와 $v=X_0 \bmod n$을 계산한다.
⑥ v=r를 확인한다.

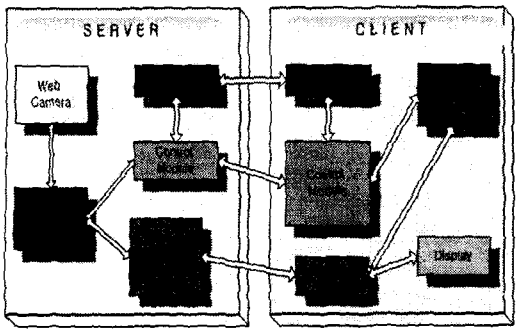
Ⅳ. 웹 카메라 서버용 영상처리 시스템

본 장에서는 앞서 설명한 ECDSA암호 알고리즘을 인증모듈로 구현 하였으며 이를 웹카메라 서버용 영상처리 시스템에 적용하도록 하겠다. 웹카메라 서버용 영상처리 시스템은 두 대의 PC에서 서버 및 클라이언트로 구성되었으며 stream 소켓방식을 이용하여 이상없이 동작함을 확인하였다. 그림 에 전체 시스템 구성도를 나타내었다.



【그림 3】 웹 카메라 시스템의 구성도

웹 카메라 서버용 영상처리 시스템은 그림 에 보는 것과 같이 서버와 클라이언트 부분으로 나뉘며 크게 세부분으로 분류된다.



【그림 4】 웹 카메라 서버용
영상처리 시스템 구성도

① 인증 모듈 : 인증은 크게 사용자인증과 데이터인증 부분으로 나뉘는데 타원곡선 암호시스템을 적용한 전자서명 방식인 ECDSA를 사용였다.. 이 방식은 기존 RSA를 사용한 방식보다 훨씬 안정되고 효과적이며 스마트카드, PDA등 이동매체를 이용한 전자상거래 서비스를 위해 필요한 방식이다.

② 전송 모듈 : 전송모듈은 네트워크 상에서 데이터를 전송하고 받기위해 사용하는 부분으로 Stream Socket과 Datagram Socket으로 나뉜다. Stream Socket 연결방법은 서버가 실행되면서 클라이언트를 기다리고 이때 클라이언트가 자신의 주소를 서버프로그램에게 주면 서버는 이 ID를 받고 클라이언트 컴퓨터에 접근하는 길을 설정한다. 이렇게 서버와 클라이언트가 온라인을 이루게 되어 통신이 시작되는 것이고 Datagram Socket은 한 컴퓨터가 어떤 데이터를 담아서 특정 컴퓨터 주소 IP로 데이터를 날리는 것이다. Datagram방식은 서버가 많은 곳에서 유리한 방식이고 stream 방식은 Data의 정확성을 요구할 때 사용하는 방식이다. 본 논문에서는 Stream Socket방식을 구현하였다.

③ 영상출력 모듈 : 웹 카메라 영상을 모니터 화면에 뿌려주는 역할로 멀티미디어 어플리케이션 제작에 쓰이는 MicroSoft社에서 출시된 DirectX SDK(Software Development Kit)를 사용하여 제작하였다.

V.결론

본 논문은 현재 많은 이슈가 되고 있으며, 정보화 신용사회에서 가장 시급히 그리고 중대하게 다루어야 하는 정보보안을위한 하나의 모듈화하여 멀티미디어 시스템에 적용함으로써 실용성과 보편성을 증대하기 위한 대안을 제공하고자 한다.

본인이 구현한 전자서명 인증방식의 영상처리 시스템은 기존의 열쇠,출입증 ID,Password방식에서 보안이 강화된 사용자 인증이 필요한 모든 분야에 활용이 가능하고 방송국/인터넷 방송을 위한 동영상 서비스, 휴대용 TV전화, 멀티미디어 교육 시스템, 멀티미디어 영상관등 여러 시스템에 응용 및 확장 가능하다.

참 고 문 헌

[1] FIPS PUB 186-2, "DIGITAL SIGNATURE STANDARD," 2000. 01.

[2] 박영호 외 ,"ECDSA를 적용한 ID기반의 사용자 인증 및 키 교환 프로토콜", 정보보호학회논문지, 2002. 02.

[3] 이명옥 외 "웹캠:새로운 인덱스 검색 알고리듬을 이용한 웹기반 원격 녹화 보안 시스템", 정보처리학회논문지C 제9-권 제 1호, 2002. 02.

[4] 김진환 "사용자 인증 보안을 위한 온라인 서명 검증 시스템", 정보보호학회지,2002. 04.

[5] 심규복 외 "H.235. 프로토콜에 의한 영상회의의 인증과 암호화 구현", 정보처리학회논문지C 제9-권 제 3호, 2002. 06.

[6] 한국정보보호센터, "전자서명 인증관리센터 운영 보고서", 2000. 12

[7] 김진환, "보안을 위한 온라인 서명검증시스템에 관한 연구" 성심외국어대학 산학연구, 제 18권 제 2호 1998. 10