論文
7-4-1

RS_RCCS의 상호인증을 위한 프로토콜 설계
(Protocol Design for Mutual Authentication of RS_RCCS)

두창호Chang-Ho, Doo)[1]

요 약

본 연구는 중계형 서비스 기반 원격 컴퓨터 제어 시스템(RS_RCCS : Relay Sevice-based Remote Computing Control System)에서 참여자 사이에 패스워드를 이용한 인증센터가 필요 없이 독립적 인증을 제공할 수 있는 프로토콜을 제안하고 이를 설계하고자 한다. RS_RCCS 에서의 인증센터가 존재하지 않는 인증구조에서 구조적으로 원격 서비스 요청자들이 다수의 관리자와의 상호 인증 과정이 요구되며 이에 예상되는 패스워드 공격에 안전하게 보호될 수 있는 프로토콜이 필요로 한다. 이에 본 연구는 효율적인 RS_RCCS에 대한 인증 설정과 이에 대한 프로토콜을 연구하여 원격 제어 부분의 자원 관리의 유용성에 도움이 되고자 한다.

ABSTRACT

This study is to propose and design a protocol that offers independent authentication with no necessity of certification authority using password between participants in RS_RCCS(Relay Service-based Remote Computing Control System). In RS_RCCS without authentication center that remote service requesters have mutual authentication with many service managers, there needs for a protocol protected from password attacks. Hereupon, this study is to offer an efficient authentication setting and a protocol for RS_RCCS and helpful for the usefulness of resource management.

논문접수 : 2006. 7. 10.
심사완료 : 2006. 8. 5.

1) 정회원 : 동남보건대학 웹컨텐츠개발과 교수

※ 본 논문은 동남보건대학 교내연구비지원에 의하여 이루어짐.

1. 서론

최근 인터넷 사용자의 꾸준한 증가에 웹 서비스를 비즈니스 도구로 사용하고 있는 기업은 비즈니스 기업으로서는 빠른 서비스를 요구하는 고객의 요구에 부응하기 위해 웹 서비스를 이용한 원격 컴퓨터 제어 지원 서비스를 고려하고 있고 이에 관한 시장이 활성화 되고 있다. 그러나 이러한 기술은 먼저 다양한 통신 형태와 비즈니스 기업의 요구를 적절히 반영하지 못한 형태로 개발되고 있다.

본 논문은 비즈니스 기업 환경에서 고객의 가용성을 확보하기 위해 사용되는 중계형 서비스 기반 원격 컴퓨터 제어 시스템(RS_RCCS : Relay Sevice-based Remote Computing Control System) 서비스 운영[1]에서 신뢰성와 안전성을 높이기 위해 RC_RCCS에 패스워드 기반 독립적 상호인증 방법으로 프로토콜을 설계하여 비즈니스 기업 RS_RCCS 시스템의 인증 모델로서 유용성을 제공하고자 한다.

이에 중계형 원격 제어 시스템인 RS_RCCS에서 참여자 사이에 패스워드를 이용한 인증센터가 필요 없이 독립적 인증을 제공할 수 있는 프로토콜에 관한 연구들을 고찰하여, 일회용 패스워드 이용한 다수의 관리자를 인증, 부인방지기능, 원격제어 요청자와 다수 관리자 사이의 정보 유통시 안전성과 신뢰성을 확보하는 방법으로 강한 인증을 제공할 수 있는 SRP 프로토콜을 기반으로 하여 타원곡선 알고리즘의 이산대수 문제를 이용한 ECDSA 프로토콜을 접목하여 SRP_ECDSA 프로토콜을 설계와 이에 대한 안전성 분석 및 검증을 하려한다.

본 논문의 구성은 다음과 같다. 2장에서는 패스워드 기반 독립적 인증 프로토콜에 관련 연구와 3장에서는 SRP-ECDSA를 제안하고 4장에서는 제안된 프로토콜을 RS_RCCS 환경에서 적용하였을 경우 적용여부분석과 안전성을 분석하였다. 그리고 6장에서는 본 논문에 대한 결론을 내리고 향후연구에 대하여 기술한다.

2. 관련연구

2.1. SRP(Secure Remote Password)

강한 인증을 보장하는 패스워드 기반 인증 프로토콜들 중에서 SRP는 기존의 패스워드 기반 프로토콜이 갖는 대부분의 문제들을 어느 정도 해결한 프로토콜이라고 볼 수 있다.[7] 또한 패스워드 파일을 비대칭으로 저장해 파일 노출시 패스워드가 직접 노출되지 않는 특징을 가지고 있으며 상호 인증(mutual authentication)을 제공과 네트워크 상에서 어떠한 패스워드도 유출시키지 않는 영-지식(zero-knowledge)을 지향, 모든 수동적, 능동적 공격에도 견디는 새로운 클래스의 강한 인증 프로토콜이다.

2.1.1 SRP의 표기 및 시스템 설정

[SRP의 표기]

- n : 안전한 큰 소수 ($n = 2q + 1$, q 는 소수)
  모든 연산은 모듈로 n 상에서 이루어짐.
- g : 모듈로 n 상의 원시원소 , $g \in {}_nZ^*_p$
- pwd : 요청자의 패스워드
- s : 요청자의 $salt$ 값
- $Hash()$: 일방향 해시 함수
- x : 개인 키(private key)
- v : 패스워드 검증자
- a, b : 임의의 생성된(난수) 비밀키, 노출되지 않음
- A, B : 동의된 공개키
- u : 랜덤 은익 파라미터
- S : 세션키
- SK : 해싱된 세션키
- M : 증명값

여기서 $salt$ 값은 첫째, 사전 공격(dictionary attack)을 어렵게 하고, 둘째, 패스워드 파일이 보여 져도 패스워드를 복사가 불가능하도록 하고, 셋째, 사용자의 추가적인 문자 요구 없이 안전한 패스워드를 문자열을 증가시킬 수 있는 일종의 랜덤 스트링(random string)으

로, 일방향 함수로 계산하기 전에 패스워드와 연접(concatenation)한다. 본 논문에서는 *salt*로는 관리자 선택 시 제공받은 관리자 PIN 정보를 사용한다.

[시스템 설정]

n 이 큰 소수(large prime number)이라고 한 때,

$$q = 2*n+1, p = k*q+1$$

도 역시 소수가 된다.(k 는 짝수)

$g \in {}_N Z_p^*$ 는 order q의 원소라고 하고, 일 방향 검증자(one-way verifier-generator) v 는 다음과 같이 정의 할 수 있다.

$$v = (g^x) \bmod p$$

여기에서 지수 x 의 이산대수를 계산하는 것은 불가능하다고 가정한다. x 는 세션키 설정을 위해서 생성된 일회용 패스워드와 *salt* 한 해쉬함수의 값이다.

2.1.2 동작 과정

SRP은 DH 키 교환 방식에 기반으로 한 프로토콜로 두 참여자의 키 교환 설정단계에서 이산대수 문제를 이용하여 구성되었고, 두 참여자간의 상호인증은 해쉬함수를 이용하여 구성된다. 일방향 인증절차를 수행하기 위해 요청자와 관리자는 상호 연동하여 [그림 1]과 같이 프로토콜을 실행한다.

① 우선 관리자는 요청자의 웹 화면에서 관리자 선택 시 자신의 PIN 정보를 전달한다.

② 요청자가 *pwd*를 설정한다.(일회용 패스워드를 직접 입력)

③ *salt* 값 s 을 선택하고

$x = Hash(s, pwd)$, $v = g^x \bmod p$ 을 계산한다. 이때 관리자의 PIN 정보를 *salt* 값으로 사용한다.

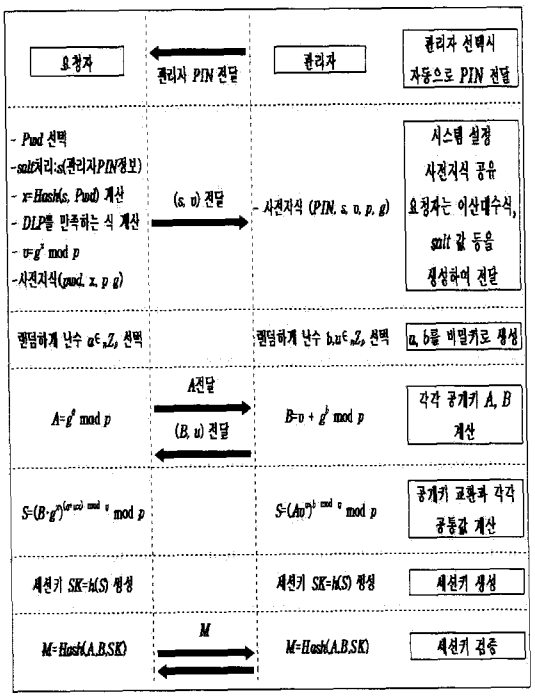
④ 요청자는 사전지식으로 *(pwd, q, p, g)*를 갖고, 관리자에게 *(s, v)*를 전달한다.

⑥ 관리자는 난수 b, $u \in {}_N Z_q$을 생성하여 자신의 임시 공개키를 계산해 *(B, u)*를 요청자에게 전송한다.

⑦ 요청자와 관리자는 각각 지니고 있는 값을 이용해 공통 지수값 S를 계산한다.

그리고 $SK=Hash(S)$를 계산하여 상호 동의된 세션키를 설정한다.

⑧ 요청자는 관리자에게 정확한 S 을 지니고 있음을 증명하는 M 을 구 성해 전달하면 요청자가 검증을 통해 확인한다.

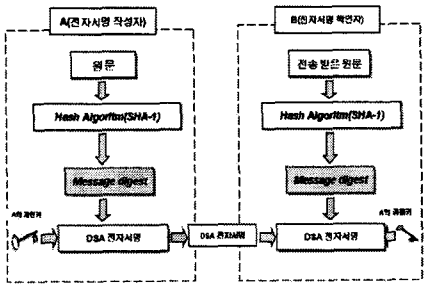


[그림 1] SRP 프로토콜 수행 절차

2.1 전자서명을 위한 ECDSA 적용

본 논문에서 제안하려는 프로토콜에 암호화된 전자서명을 기능을 사용하여 원격제어 요청자의 부인방지를 제공하려한다. 전자서명의 대표적인 프로토콜로 DSA(Digital Signature Standard)가 있는데 이 프로토콜의 응용 프로토콜인 타원곡선 이산대수에 기반을 둔 ECDSA(Elliptic Curve DSA)를 전자서명에 사용하려 한다. DSA는 원문에 대한 인증과 완전성을 위한 전자서명 생성 목적으로 사용

되는데 안전성은 이산대수 문제에 기반 한다. DSA 표준에서 전자서명 작성시 원문 다이제스트는 해쉬 알고리즘 SHA-1을 사용한다.[6] 다음 [그림 2]는 원문을 해쉬 알고리즘 SHA-1로 다이제스트해서 보내면 상대측에서는 전송받은 원문을 해쉬 알고리즘(SHA-1)으로 메시지 다이제스트하여 A의 공통키로 풀면 A가 보낸 문서인지를 확인할 수 있고 부인방지를 제공할 수 있다.



[그림 2] DSA 프로토콜의 개념

ECDSA 프로토콜은 DSA를 타원곡선 알고리즘으로 옮긴 것으로 ECDSA와 DSA의 중요 차이점은 r의 생성에 있다. DSA는 r을 임의의 $g^k \bmod p$ 를 선택/계산한 후, $\bmod q$ 를 계산하여 얻는다. 그러나 ECDSA에서 r은 임의의 점 kP 의 x 좌표를 $\bmod n$ 하여 얻는다. ECDSA가 160비트 q와 1024비트 p 을 가진 DSA와 비슷한 안전도를 갖기 위해서는 매개변수 n이 약 160비트이면 된다. 이 경우 DSA와 ECDSA는 같은 서명길이(320비트)를 갖는다. 즉 기존 DSA 알고리즘 보다 ECDSA를 사용하는 것이 키 bit 당 암호화 정도가 강하다. 이 프로토콜 구성은 키 생성단계와 서명생성단계, 서명검증단계로 나눌 수 있다.[6]

[ECDSA 키 생성]

요청자가 키를 생성한다고 가정하자.

① 유한체 Z_p 에서 정의된 타원곡선 E를 선택한다. 타원곡선 군 $E(Z_p)$는 큰 소수 n에 의해 나누어져야 한다.

② 위수 n인 점 $P \in E(Z_p)$을 선택한다.

③ 구간 $[2, n-2]$에서 통계적으로 유일하고 예측 불가능한 정수 d 을 선택한다.

④ 타원곡선식 $Q = dP$을 계산한다.

⑤ 이때 요청자의 공개키는 (E, P, n, Q)가 되고, 비밀키는 d 된다.

[ECDSA 서명생성]

메시지 m에 요청자가 서명한다고 가정하자.

① 구간 $[1, n-1]$에서 통계적으로 유일하고 예측 불가능한 정수 k을 선택한다.

② $kP = (x_1, y_1)$과 $r = x_1 \bmod n$을 계산한다(x_1은 정수로 간주).

③ $r = 0$이면, ①단계로 되돌아간다.

④ $k^{-1} \bmod n$을 계산한다.

⑤ $s = k^{-1}\{h(m) + dr\} \bmod n$을 계산한다.(h : SHA-1)

⑥ $s = 0$이면, ①단계로 되돌아간다.

⑦ 메시지 m에 대한 서명은 (r, s)이다.

[ECDSA 서명 검증]

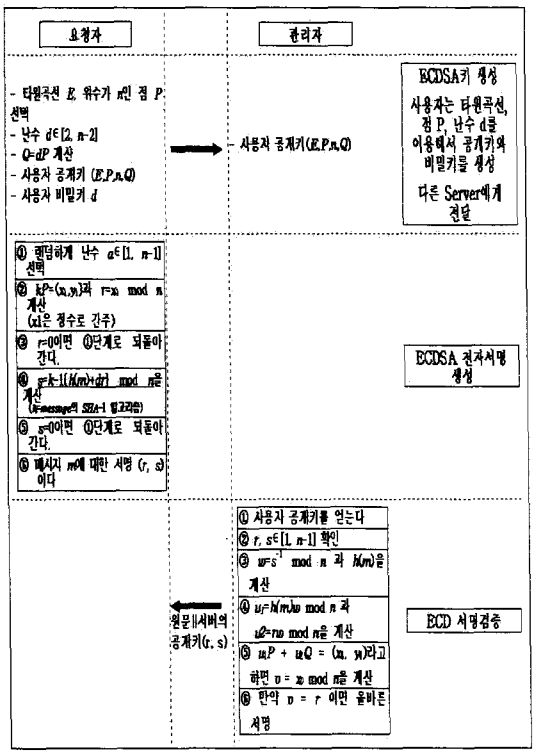
관리자는 요청자의 서명 (r, s)을 검증한다고 가정하자.

① 요청자의 인증된 공개키 (E, P, n, Q)을 얻는다.

② r과 s가 구간 $[1, n-1]$에 있는지 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 타원곡선 이산대수식
$u_1P + u_2Q = (x_0, y_0)$와
$v = x_0 \bmod n$을 계산한다.
⑥ $v = r$ 이면 올바른 서명인지 확인이 된다.



[그림 3] ECDSA 프로토콜 수행 절차

3. SRP_ECDSA 프로토콜

본 논문에서의 최종적 제안 프로토콜은 기존의 패스워드 프로토콜이 클라이언트와 서버 사이에 인증기관을 통하여 인증하던 방식과 달리 클라이언트와 서버가 독립적으로 키 교환 및 인증을 하는 패스워드 기반 프로토콜에서 안전성과 효율성이 입증된 DH 키 교환 방식에 기반을 둔 SRP 프로토콜을 사용하고, SRP 프로토콜에 부가하여 안전성과 사용자 부인방지를 해결하기 위한 ECDSA의 서명기법을 적용, SRP_ECDSA을 제안하였다.

SRP는 기본적으로 키 교환 설정 단계가 이산대수 문제에 근거하므로 타원곡선 프로토콜 방식인 ECDSA도 같은 타원곡선 이산대수 문제를 이용하므로 SRP 프로토콜에 적용이 가능하다. 제안한 프로토콜은 안전성 향상 및 프로토콜의 간략화를 위해 일방향 최적화된 SRP에 ECDSA를 적용하였다.

3.1 SRP_ECDSA 표기 및 키 설정 단계

3.1.1 SRP_ECDSA의 표기

프로토콜에 사용되는 표기방법은 2절의 SRP 프로토콜 표기 방법에 다음 사항을 더하여 표기한다.

- E : Z_p에서 정의된 타원곡선
- h() : 일방향 해쉬함수
- g : 곱셈군(multiplicative group)
  Z_p^*의 생성자 (generator),
  p의 원시근
- P, Q : 타원곡선상의 임의의 두 점

3.1.2 키 설정 단계

먼저 SRP 프로토콜과 같이 관리자의 PIN을 이용한 사전공격에 대비한 *salt* 처리와 강한 소수(p, q) 을 정의한다.

본 논문에서는 타원곡선 E을 단순화하기 위해 $K = F_p = Z_p$(p : 소수, p 개의 원소를 갖는 유한체)로, 타원곡선 E 는 $y^2 = x^3 + ax + b\,(a, b \in Z_p)$, $4a^3 + 27b^2 \neq 0$ in Z_p 와 무한원점 (o)을 말하기로 하자.

- n : 160비트 이상의 크기를 갖는 소수
- 타원곡선 $E(Z_p)$:

$y^2 = x^3 + ax + b\,(a,\ b \in Z_p)$의 방정식을 만족하는 Z_p상의 점들과 무한 점으로 이루어진 집합을 의미한다.

① 위수 n을 갖는 Z_p에서 정의된 타원곡선 $E(Z_p)$을 선택한다.

② 위수가 n인 $P \in E(Z_p)$을 선택한다.

③ 안전한 일방향 해쉬함수 h 을 선택한다.

④ 요청자가 **pwd**를 설정한다.

⑤ ***salt*** 값 s를 선택하고 $x = h(s, pwd)$을 계산하고 점 $Q = xP$을 계산한다.(SRP과 같이 관리자 PIN을 *salt* 값 처리)

⑥ 요청자는 사전지식으로 *(E, P, Q, pwd, q, p)*를 갖고, 관리자에게 *(E, P, n, Q, s)*를 전달한다.

3.2 키 상호 인증 프로토콜

① 구간 $[1, n-1]$에서 난수 a을 선택하고, $A = aP = (x_1, y_1)$을 관리자에게 전송한다.

② 난수 $b,\ u \in [1, n-1]$을 선택한다.

③ 요청자와 관리자는 각각 공통 값 S를 계산한다.

④ $i = a^{-1}(h(s) + xr)$을 계산한다. 그리하여 서명 쌍은 *(A, i)* 가 되고, 관리자에게 i 값을 전달한다.

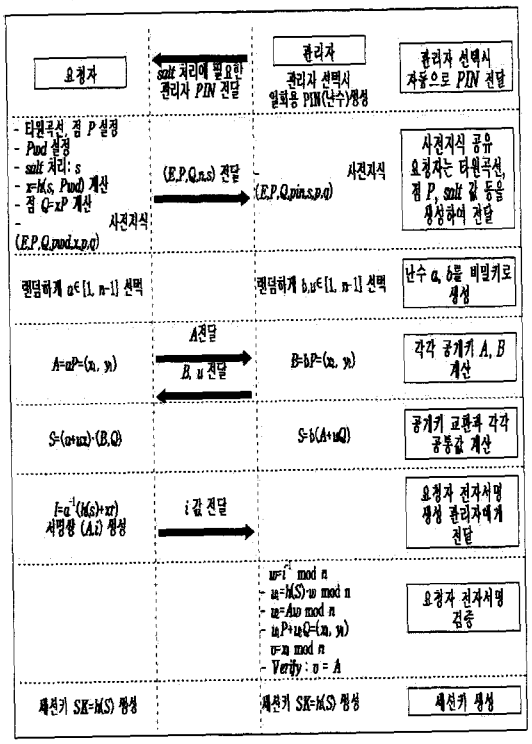
⑤ 관리자는 $w = i^{-1} \bmod n$을 계산하고, $u_1 = h(s)w \bmod n,\quad u_2 = Aw \bmod n$을 계산한다.

⑥ $u_1P + u_2Q = (x_0, y_0),\ v = x_0 \bmod n$을 계산하여 $v = A$이면 올바른 서명이다.

⑦ 요청자와 관리자는 세션키 $SK = h(S)$을 생성한다.

이 프로토콜 구성을 요약해서 설명하자면 첫 번째, 준비단계에서 관리자 선택시 자동으로 관리자 정보인 PIN이 전달된다. 두 번째, 사전지식을 공유하기 위해서 요청자는 타원곡선 점 P, *salt* 등을 생성하여 관리자에게 전달한다. 실행단계에서는 요청자와 관리자 모두 난수 a, b를 개인키로 생성한다. 이때 관리자 측에서는 난수 u를 더 생성하는데 u의 목적은 랜덤 은닉 파라미터로, 공개적으로 노출되어 b 의 개인키를 은닉할 목적이다. 다음 단계에서는 요청자와 관리자는 각각의 공개키 A, B를 타원곡선 이산대수 문제 식에 의해 계산하여 공개키 A, B를 상대측에 전달하고 각각 공통 값을 계산한다. 다음 요청자의 전자서명을 생성, 관리자에게 전달하고 요청자의 전자서명이 검증되면 각각의 세션키를 설정할 수 있다.

다음 [그림 4]는 제안된 SRP_ECDSA 프로토콜이다.



[그림 4] SRP_ECDSA 프로토콜 절차

4. 프로토콜의 분석

4.1 프로토콜 특징

본 논문에서 제안된 SRP_ECDSA 프로토콜은 비즈니스 기업에서 RCC 서비스를 제공하기 위한 패스워드 이용한 인증 프로토콜이다. 다수의 요청자와 다수의 관리자가 접속을 원하는 RS_RCCS 환경에서 데이터베이스에서 제공하는 웹 페이지 리스트를 선택하여야 하는 요청자의 입장에서는 1 : N 의 관계이다. 이때 관리자 선택 시 관리자는 클라이언트에서 PIN 정보를 제공하여 요청자에게 보내고 요청자는 일회용 패스워드를 *salt* 처리하여 키 교환 알고리즘에 의해 시스템 설정을 위한 정보를 관리자에게 전달한다. 이때 SRP_ECDSA 프로토콜이 키 교환을 위한 패스워드가 비대칭적으로 전달되는 구조이고 상호 서로 다른 정보을 지니게 되고 관리자는 전달받은 정보로 세션키를 생성하고 요청자도 관리자 정보를 이용 세션키를 생성하여 세션키와 같음을 검증하여 인증기관이 필요 없이 선택된 관리자와 세션 생성을 위한 세션키를 생성하는 구조이다. 또한 관리자도 요청자가 전자서명을 붙인 정보를 수신 받음으로 이를 해독하면 요청자의 부인방지가 되어 RCC 참여자 상호간에 인증이 확실하여 진다.

SRP기반이므로 SRP가 가지는 기술적 실용적 장점이 비교적 구현하기 쉬운 지수 승, 덧셈, 곱셈, 해싱으로 이루어져 있고, 매우 간단한 프로토콜로 되어 있기 때문에 DH 키 교환 프로토콜만큼 빠르고 지연시간을 줄이기 위해 병렬연산 같은 최적화 기법을 이 프로토콜에 적용할 수도 있다. 또한 SRP는 간단한 연산의 집합이므로, 구성된 기능들을 수행하는 코드를 찾기 쉽고, 그것을 어떤 클라이언트 응용과도 통합이 가능하다. 이런 이유는 다른 기존의 키 교환 프로토콜과 인증 프로토콜들로부터 부분적 요소를 도입하여 이를 변형하여 정제하였기 때문이다.

ECDSA의 타원곡선 알고리즘은 최근 RSA 방식에 적은 연산량으로 제한된 환경에서 전자서명과 암호기술로 최적의 대안으로 휴대폰, PDA에도 적용되는 프로토콜로 사용되어 입증되고 있다. SRP_ECDSA는 SRP에 ECDSA를 적용하여 상호 인증인 가능하며, 세션키를 독립적으로 교환하며 키 교환에 의해 생성된 세션키에 대해서도 서명을 통해 인증하게 되고 통신회수도 4회로서 강한 인증을 제공한다.

SRP_ECDSA는 요청자의 서명을 이용함으로써 요청자의 부인 방지를 제공하고, 인증에 사용되는 키 쌍 *(A, i)*은 두 통신자 사이의 키 교환(요청자와 관리자)에 의해 생성된다. [그림 4]를 이용해 설명하면, A 와 i 값은 사용자에 의해 생성되는 서명값으로 사용자가 자신의 비밀키 $x = h(s, pwd)$ 을 이용해 서명값을 생성하고, 서버는 사용자의 공개키 (E,P,Q,n,s)를 이용해 서명을 검증하여 인증하게 됨으로 생성한 세션키 S에 대한 사용자의 부인을 방지할 수 있다. 그리고 사용자의 인증에 사용되는 키 쌍은 매 세션마다 새롭게 생성되는 값이며, 세션키도 매 세션마다 생성이 된다.

네트워크 상에서의 통신 회수는 네트워크 자원의 효율성과 네트워크상의 지연(delay) 등을 고려할 때 적을수록 장점을 갖는다. 그러나 통신회수가 줄어도 보안의 안전도는 변함이 없어야 한다. 일반적으로 3개의 메시지를 사용한 전송이 강한 인증을 위한 최소라고 하는데, SRP_ECDSA는 4번의 패스를 사용하고 있으나 안전도에 확실한 검증을 마친 프로토콜이다.

4.2 프로토콜의 안전성 분석

4.2.1 사전공격(dictionary attack) 차단

사전공격은 공격자가 사용자의 패스워드를 추측하여 실제 메시지에서 드러나는 값에 대입하여 결과를 비교해 실제 패스워드를 찾는 방법이다. SRP_ECDSA에서는 요청자가 자신의 메시지를 전송하고 관리자로부터 받는 메시지 첫 번째 메시지와 상관없는 값을 받게 됨으로 추측한 패스워드로부터 생성한 결과값을 비교할 수 없다. 또한 요청자의 일회용 패스워드에 *salt* 값을 추가하여 일방향 해쉬함수에 적용했으므로 사전 공격에 더 강력하다.

4.2.2 재전송 공격(replay attack) 차단

공격자가 요청자의 메시지를 재전송하여 이미 정상적인 사용자에 의해 생성된 이전키(old session key)를 다시 생성하는 공격이다. 이 공격 방법은 요청자와 관리자간에 임의의 난수 값 *a*와 *b*가 매 세션마다 새롭게 생성됨으로 공격이 불가능하다.

4.2.3 완전 전향적 안전성(Perfect Forward Secrecy :PFS) 제공

현재의 세션키 정보가 알려져도 이전키를 알 수 없는 안전성을 말하는 것으로, PFS를 제공하기 위해서는 요청자와 관리자간에 주고받는 메시지 내용이 이전키 생성을 위한 정보와 관련이 없어야 한다. 이를 위해서는 생성되는 세션키 값이 임의의 값이 생성되어야 하며 메시지에서 임의의 값도 암호화되어 전달되어야 한다. SRP_ECDSA 에서는 생성되는 세션키 값이 임의의 난수 값 *a, b*로 생성되고 전달되는 메시지도 타원곡선 이산대수 문제의 암호화 방법으로 전달되어 PFS를 제공한다.

4.2.4 이전키(denning-Sacco) 공격

이전키를 안다고 할 때 패스워드를 알아내는 공격 방법으로 SRP_ECDSA 는 매 세션마다 요청자와 관리자가 임의의 값 a, b 을 생성됨으로서 a, b 값은 타원곡선 이산대수 문제로 분리할 수 없으므로 패스워드가 알려져도 이전의 세션키를 알 수가 없다.

4.2.5 가로채기 공격(MIMA: Man-In-Middle-Attack)

가로채기 공격은 공격자가 요청자와 관리자 사이에서 존재하여 요청자와 관리자의 메시지를 가로채어 요청자와 공격자, 공격자와 관리자 간에 각각의 세션키를 생성하는 공격하는 방법이다. SRP_ECDSA는 인증 정보인 패스워드가 사용되고 있으므로 공격이 불가능하다.

4.2.6 노출공격(impersonation attack)

관리자의 패스워드 파일이 노출되었을 경우 공격으로, SRP_ECDSA에서는 패스워드 파일은 패스워드 자체가 일회용이며 패스워드가 직접 저장되지 않고 검증하여 세션키 생성만 하므로 이 공격은 고려되지 않는다.

5. 결론

본 연구결과로서 RS_RCCS에서 통신 세션을 확립하기 위한 객체간의 인증 프로토콜들 중 요청자와 다수 관리자 사이의 인증 문제를 해결할 수 있는 독립적 인증 프로토콜인 SRP_ECDSA를 제안하였다.

일반적으로 클라이언트와 서버 사이에 별도의 인증기관을 통하여 인증하는 방식이 가장 안전하다고 평가되지만 일시적 서비스를 받기 위해 인증서 발급을 하는 문제가 있다.

제안된 프로토콜은 요청자와 관리자가 독립적으로 키 교환 및 인증이 가능하다. 이 프로토콜은 패스워드 기반을 둔 SRP 프로토콜에 인증의 강도를 높이고 요청자의 부인방지를 제공하기 위해 전자서명이 가능한 ECDSA 프로토콜을 적용한 형태이다.

이 프로토콜의 특징은 RS_RCCS에서 발생할 수 있는 요청자와 관리자 사이의 1 : N 관

계에서 별도의 인증기관 없이 세션키 교환을 위해 패스워드를 인자로 갖는 함수를 이용 검증자 기반(verifier-based) 프로토콜로 독립 인증을 가능하다.. 또한 요청자가 관리자를 선택할 때 PIN 정보를 이용하여 패스워드를 *salt* 처리하고, 요청자의 전자서명으로 검증자가 상호 세션키를 생성하여 안전성을 보장하는 특징을 가진다. 이 세션키는 매 세션마다 새롭게 생성되고 타원곡선 이산대수 문제에 기반한 암호 알고리즘을 이용함으로써 사전공격, 재 전송 공격, 완전 전향적 안전성, 이전키 공격, 가로채기, 노출공격 등에 안전성을 지닌다.

RS_RCCS 시스템은 기업의 고객 기술지원 부서에서 고객 시스템의 가용성 확보 지원을 위해 원격제어를 필요로 하는 고객들에게 콜센터와 접목하여 다양한 네트워크 환경에서 자동화된 접속이 가능한 환경에서 SRP_ECDSA 프로토콜은 원격지원 과정에서 신뢰와 안정성을 제공하기 위한 인증 모델로서 가치를 제공할 수 있다.

참고문헌

[1] 두창호, "중계형 원격 컴퓨팅 제어 시스템을 위한 인증 프로토콜", 경기대학교 대학원, 2004.2

[2] 박호상, 정수환, "패스워드 기반의 상호 인증 및 키 교환 프로토콜", 한국정보보호학회, 2002. 10.

[3] 김지영, 정영숙, 정태충, "패스워드 기반의 독립적 인증 및 키 교환 프로토콜", 통신정보합동학술대회, 제3권, 2003. 6

[4] 박호상, 정수환, "패스워드 기반의 상호 인증 및 키 교환 프로토콜", 한국정보보호학회, 2002. 10

[5] 손기욱, 서인석, 원동호, "패스워드 기반 키 분배 프로토콜 표준화 동향", 정보보호학회지 논문지, 제12권, 제4호, 2002. 8.

[6] ANSI X9.62, The elliptic curve digital signature algorithm(ECDSA), draft standard, 1997.

[7] T. Wu, "The Secure Remote Password Protocol," Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium, San Diego, pp.97~111, March 1998.

[8] D. Dolev and A. C. Yao, "On the Security of Public Key Protocols", IEEE Trans. on Information Theory, Vol.29, No.2, Mar., 1983, pp 198~208.

[9] D. Jablon, "Extended Password Key Exchange Protocols Immune to Dictionary Attacks," Proceedings of the Sixth Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises(WET-ICE '97), IEEE Computer Society, Cambridge, MA, pp.248~255, June 18-20, 1997.

두 창 호

1988년 경기대학교 수학과 졸업(이학사)
1996년 경희대학교 산업정보대학원 전자계산학과 (공학석사)
2004년-경기대학교 대학원 전자계산학과(이학박사)
1997년- 현재 동남보건대학 웹컨텐츠개발과 부교수
관심분야 : 시스템 프로그래밍 분산처리, 운영체제