The Journal of Natural Science,
Pai Chai University, Korea
Volume 8: 131~136, 1995

네트워크내의 다중센타를 위한 원격 암호 인증기법

조인준
배재대학교 전자계산학과

A Remote Password Authentication Scheme for Multiple Centers on Network

In-June Jo
Department of Computer Science, PaiChai University

본 논문에서는 개방형 분산 네트워크 접근에 적용할 수 있는 효율적인 원격 암호 인증기법을 제안하였다. 본 논문에서 제안한 인증기법은 네트워크 센터가 제공한 암호와, 네트워크 사용자를 위한 사용자 키 쌍이 주어진다. 센터가 제공한 암호는 센타 시스템이 생성하고, 사용자 키는 네트워크 사용자가 임의로 선택할 수 있다. 네트워크 사용자는 단일 슈퍼 스마트 카드를 사용하여, 개방형 분산 네트워크상의 다중센터를 접근한다. 네트워크 센터에서 생성된 암호들은 안전한 채널을 통해, 네트워크 사용자에게 전달되고, 자신의 슈퍼 스마트 카드에 기록된다.

In this paper, We propose an efficient remote password authentication scheme that enables network users to access an open distributed network. Our authentication scheme provides a pair of a center-supplied password and a user key for a network user. The center-supplied password is generated on the center, and the user key can be chosen by the network user. Each network user can access multiple centers through the open and distributed network by using single super smart card. The passwords generated by network centers are sent to the network users via secure channel, and put into their own supper smart card by themselves.

Key words : Authentication, Password, ElGamal, Chang, Liao, Signature, Smart card

Ⅰ. 서 론

현재까지 여러가지 중요한 디지탈 서명 기법들이 개발되어 왔다. ElGamal의 디지탈 서명 기법도 이들 중의 하나다.[2] ElGamal 서명 기법을 기반으로 한 원격 암호 인증기법은 Chang과 Liao가 제안하였다.[3] 이 원격 암호 인증기법은 몇 가지 문제점들을 가지고 있다. 하지만, 이는 k와 t에 대한 난수(Random Number)가 선형적 종속성(Linear Dependency)을 갖지 않게 하면, 보다 안전(Secure)할 수 있다. 본 논문에서는 상기의 2가지 기법을 기반으로 다중센타에 적용할 수 있는 새로운 기법을 제안한다.

본 논문의 내용은 2장에서 ElGamal의 서명 기법과 Chang과 Liao의 원격 암호기법을 분석하고, 3장에서 본 논문에서 제안한 기법을 설명한다. 그리고 4장은 결론으로 이루어져 있다.

Ⅱ. ElGamal와 Chang과 Liao기법 분석

1. ElGamal의 서명기법

ElGamal의 서명기법[2]을 분석하면 다음과 같다. m은 서명할 메세지, p는 자리수가 큰 솟수

(Large Prime Number), 그리고 α는 GF(p)의 원시근(Primitive Root), m의 조건은 $0 \leq m \leq P-1$ 이라고 하자. 이때 사용자의 기밀 키(Secret Key)를 x, 공용키(Public Key)를 y라 할 때, y는 다음식에 의해 얻어진다.

$$y \equiv \alpha^x \bmod P$$

모든 사용자는 α와 p를 근거로 공용 키 y를 사용하여, 메세지 m에 기밀 키 x를 적용, 서명을 검증한다. 따라서, 누구도 기밀 키 x를 알지 못하고는 서명을 위조할 수 없다. 이는 메세지 m에 대한 서명은 $0 \leq r, s \leq p-1$ 조건에서(r,s) 쌍이 되고 다음과 같은 식을 만족하게 된다.

$$\alpha^m \equiv y^r * r^s \bmod p \qquad (2.1)$$

ElGamal의 서명 기법은 다음 3단계로 이루어진다.

i) 난수 k를 선택한다. 여기에서 k는 $0 \leq k \leq p-1$, $\gcd(k, p-1) = 1$ 조건을 만족한다.

ii) $r \equiv \alpha^k \bmod p$ 계산한다.

iii) 식 (2.1)이 $\alpha^m \equiv \alpha^{xr}\ \alpha^{ks} \bmod p$로 대치시켜 (2.2)식을 얻는다.

$$m \equiv xr + ks \bmod(p-1) \qquad (2.2)$$

(2.2)식에서 쉽게 s 값을 구할 수 있다. 즉, 식 (2.2)는 $\gcd(k, p-1) = 1$를 만족하는 k를 선택, s의 값을 구한다.

2. Chang과 Liao의 기법

상기의 ElGamal의 기법에 시간표식(Timestamp) 개념을 기초로 하여, Chang과 Liao는 원격 암호 인증기법을 제안하였다.[3] 이의 기법은 다음과 같이 3단계로 되어 있다.

가. 제 1단계 : 초기단계

암호 생성센터에서, 시스템 기밀 키 SK를 가진다고 합시다. 센터에서는 다음 방정식으로 공용 키 PK를 계산한다.

$$PK \equiv \alpha^{sk} \bmod p,$$

(P: Large Prime Number, α: Primitive root of GF(p))

이미 기록된 사용자의 경우, 사용자 U_i는 암호생성센타에 자신의 사용자 식별자(User-id) ID_i를 제공한다. 이때 암호생성 센터가 U_i에게 스마트 카드(Smart card) 제시를 요구한다. 스마트 카드는 빠른 지수, 덧셈 그리고 곱셈 연산들을 실행할 수 있는 일 방향 함수 f와 이의 알고리즘으로 구성된 난수생성기를 가지고 있다. 센터에서는 사용자 U_i에 대해, $0 \leq r_i, s_i \leq (p-1)$ 조건하에서 암호 $PW_i = (r_i, s_i)$를 선택한다. 이 암호를 사용자 U_i에게 안전한 채널(Secure Channel)을 통해서 보내게 된다. 즉, $\alpha^{ID_i} \equiv PK^{r_i} * r_i^{s_i} \bmod p$.

나. 제 2단계 : 로그-인(Log-in) 단계

이 단계에서 사용자 U_i는 스마트 카드를 터미널에 접착시키고, 터미널에 사용자 ID_i와 암호 PW_i를 입력한다. 이때, 스마트카드는 다음과 같이 실행된다. 첫째, 난수 t가 $1 < t < (p-1)$인 조건하에서 선택한다. 그리고 나서 다음 식을 계산한다.

$A = r_i^t \bmod p$

$B = t + s_i * f(A,T) \bmod(p-1)$

(T(TimeStamp): Current Login data & Time)

상기의 방정식 계산 후, 스마트 카드는 인증 메세지 $C = \{ID_i, r_i, A, B, T\}$를 센터 시스템에게 보낸다.

다. 제 3단계 : 인증 단계

시스템은 메세지 C를 근거로 하여 로그-인 요구를 검증한다. 첫째, 시스템은 메세지 C를 수신한 날짜와 시간을 나타내는 T를 기록한다. 그리고 나서 $\delta T = T' - T$를 계산한다. 이의 알고리즘은 다음과 같다.

If $\delta T \geq \Delta T$, ΔT: 전송 지연을 위한 적법한 시간 간격
then 로그-인 요구를 거절한다.
else $A' = r_i^B((PK^{-r_i} * \alpha^{ID_i})^{-1})^{f(A,T)} \bmod p$. 계산한다.
if $A = A'$
then 로그-인 요구를 허락한다.
else 로그-인 요구를 거절한다.

Ⅲ. 원격 암호 인증기법 제안

1. 배 경

Chang과 Liao의 기법은 ElGamal의 서명 기법

을 기반으로 한 비상호(Non Interactive) 암호 인증기법이다. 이를 다중 센타에 이용할 경우 발생되는 문제점은 다음과 같이 정리할 수 있다.

(1) 사용자가 로그-인 단계로 들어가면, 사용자는 자신의 사용자 ID_i와 암호 PW_i를 제시해야 한다. 이때, 사용자가 암호 PW_i를 기억하기가 어렵다. 왜냐하면, PWi는 (r_i, s_i) 쌍으로 이루어진 튜플이고, $0 \leq r_i, s_i < (p-1)$ 조건을 만족해야 하는데, 여기에서 p는 자리수가 큰 솟수이다. 만약 사용자가 이를 참조하기 위해서 몇몇 장소에 기록한다거나, 천천히 터미널에 입력한다면, 이들 암호의 누출 가능성 때문에 덜 안전하다. Chang과 Liao의 기법에서, 스마트 카드에 암호가 저장되도록 허용한다면, 자신의 암호에 대해 전혀 알 필요가 없지만, 스마트 카드를 도난 당했을 경우, 무자격자에 의한 사용을 막을 수가 없다.

(2) 암호 PW_i 만을 알고 있는 사용자가 적법한 인증에 의한 서명을 할 수 있기 때문에 다른 사용자가 스마트 카드를 사용할 수 있다. 무자격자가 공용 ID_B와 기밀 PW_B를 알고 있을 때, 그 사람은 사용자 B가 아닌 다른 사용자의 어떤 스마트 카드도 사용할 수 있다.

(3) 이 기법은 네트워크 내에서 단지 하나의 네트워크 센터에만 적용이 가능하기 때문에 네트워크 내의 다중센타 및 네트워크 사용자들 사이에 효율적인 인증을 제공할 수 없다. 만약 네트워크 사용자가 다른 네트워크 센터에서 관리하고 있는 서비스를 원한다면, 네트워크 사용자는 그 센터에서 발행한 추가적인 스마트 카드와 암호를 가져야만 한다.

본 논문에서 제안한 인증 기법은 상기의 문제를 해결하기 위해서 새롭게 설계하였다. 또한 제안된 기법은 단지 하나의 스마트 카드를 사용하여 다중 네트워크 센터를 대상으로 통합 서비스를 네트워크 사용자에게 제공하도록 하고 있다. 이를 위해서 제안된 기법은 다음과 같은 특성들을 갖는다.

(1) 네트워크 사용자 서비스는 네트워크내에 다중 센터들에 의해 제공된다.

(2) 센터에는 인증을 위해 어떤 검증 테이블(Verification Table)도 저장할 필요가 없다.

(3) 각 네트워크 사용자는 통합 서비스에 접근하기 위해서 자신의 단일 슈퍼 스마트 카드를 가진다.

(4) 각 네트워크 사용자는 센터가 제공한 키와 사용자 키를 쌍으로 가진다. 센터가 제공한 키는 Chang과 Liao 기법에서와 마찬가지로 암호 PW_i로 나타난다. 사용자 키는 인증 과정에서 권한을 가진 사용자가 자유롭게 변경할 수 있는 사용자 정의 키를 의미한다.

(5) 접근 요구는 센터가 제공한 키와 사용자 키를 사용하여 쉽게 검증될 수 있다. 센터가 제공한 키는 네트워크 사용자에 의해 효율적으로 접근 요구를 지원하기 위해, 스마트 카드에 저장된다. 하지만 사용자 키는 스마트 카드에 저장되지 않는다. 네트워크 사용자는 사용자 키를 자신이 선택했기 때문에 쉽게 자신의 키를 기억할 수 있다.

(6) 이 기법은 도난 당한 스마트 카드에 의해 네트워크 접근 공격을 막을 수 있다. 사용자 키를 가지고, 다른 스마트 카드를 이용하여, 센터가 제공한 키를 알고 있는 무자격 사용자를 차단함을 말한다.

(7) 이 기법은 바로전에 불법 취득한 접근 요구를 재현하는 공격을 막을 수 있다.

2. 용어 및 정의

제안 기법을 설명하기 위해서 다음과 같은 용어 및 정의를 한다.

- $\{\}$: 원소들의 연쇄적 결합(Concatenation of the Elements)
- m : 센터 수를 나타내는 작은 정수
- n : 네트워크 사용자 수를 나타내는 큰 정수
- C_m : m=1,2...,n인 네트워크상의 센터를 나타낸다.
- CID_m : 네트워크 센터 C_m의 식별자 (Identification)
- U_i : i=1,2...,n인 네트워크 사용자를 나타낸다.
- UID_i : 네트워크 사용자 U_i의 사용자 식별자 (Identification)
- SSC_i : 네트워크 사용자 U_i에게 제시한 슈퍼 스마트 카드를 나타낸다.
  상기의 SSC_i는 자신의 기억장치에 네트워크 사용자 자신의 암호 기록을 허용하고, 또한 네트워크 사용자가 이를 자유롭게 변경이 가능하도록 허용한다.
- f : SSC_i가 실행하는 단일 함수
- PK_m : 네트워크 센터 C_m의 공용 키
- SK_m : 네트워크 센터 C_m의 기밀 키

-UK_i : 네트워크 사용자의 사용자 키
UK_i는 네트워크 사용자 U_i가 선택할 수 있다. 즉 네트워크 사용자 U_i는 UK_i를 $1<UK_i<P-1$ 범위에서 자유롭게 선택할 수 있다.

-$PW_{m,i}$: 네트워크 사용자 Ui에게 센터 C_m에서 생성한 암호를 나타낸다.
$PW_{m,i}$는 Chang과 Liao의 기법에서 센터 C_m에서 생성된 암호 $r_{m,i}$와 $s_{m,i}$의 쌍을 기본으로 하여, $(r_{m,i}, s_{m,i})$의 튜플로 나타난다.
사용자 키 UK_i는 센터 혹은 사용자에 의해 만들어 질 수 있다.
하지만, $r_{m,i}$와 $s_{m,i}$ 쌍은 네트워크 사용자에 의해 변경될 수 없다.

-EUK_i : SSC_i의 함수 f에 의해 사용자 키 UK_i의 암호화(Encryption) 결과를 나타낸다.
EUK_i는 U_i의 슈퍼 스마트 카드 SSC_i에 저장되어 진다.

-$K_{m,i}$: ElGamal 기법을 근거로 $r_{m,i}$와 $S_{m,i}$쌍을 만들기 위해서, 네트워크 사용자 U_i에 대해 센터 C_m에서 생성한 난수를 말한다. 여기에서 C_m은 두명의 다른 사용자를 기록하기 위해 $K_{m,i}$를 똑같이 두번 사용하지 않는다고 가정한다.

-$SSCPW_i$ $[CID_m]$: 네트워크 사용자 U_i에 대해서 네트워크 센터 C_m이 생성한 $(r_{m,i}, s_{m,i})$쌍의 유지를 표시한다. 이는 네트워크 사용자 U_i의 슈퍼 스마트 카드 SSC_i 메모리에 저장된다.

-$IM_{m,i}$: 초기에 슈퍼스마트 카드를 설치(Set-up)하기 위해서 제공된 메세지이다.
센터 C_m은 네트워크 사용자에 대해 이 메세지를 생성한다.
$IM_{m,i}$는 $\{CID_{m,i}, UK_i\}$로 나타난다.
이 메세지는 안전한 채널을 통해서 네트워크 사용자 U_i에게 보내진다.

-T : 현재의 날자와 시간으로 구성된 시간 표식(Timestamp)

-ΔT : 전송지연에 대한 적법한 시간 간격

-$LT_{m,i}$: 네트워크 사용자 U_i측에서 만든 로그-인 메세지이다.
이는 $LM_{m,i} = \{UID_i, r_{m,i}, A, B, T\}$로 정의된다. 여기에서 T는 시간표식 값이고, A와 B는 $r_{m,}$, $s_{m,}$, T 값을 사용해서 슈퍼 스마트 카드 SSC_i가 계산한다.
이 메세지가 사용자 인증을 위해 센터 C_m에 보내진다.

3. 제안 기법

제안 기법은 상기의 특성을 지원하기 위해서 3단계로 구성된다. 이 기법의 제 1단계는 사용자 키를 제외하고는 Chang과 Liao의 기법과 같이 초기화 단계이다. 제 2단계는 사용자가 슈퍼 스마트 카드 소지 자격을 가졌는지를 검증하는 사용자 검증 단계이다. 사용자 키가 이 단계에서 슈퍼 스마트 카드에 입력된다. 이 단계가 성공적으로 완료되면, 슈퍼 스마트 카드는 다음 단계를 실행할 수 있다. 기타의 경우는 스마트 카드가 사용자를 거절하고, 진행을 멈춘다. 제 3단계는 사용자 인증 단계이다. 이 단계에서 네트워크 사용자의 슈퍼 스마트 카드는 암호와 사용자 키를 사용하여 서명하게 되고, 특정 네트워크 센터에 사용자 인증 메세지를 보낸다. 이를 가지고 네트워크 센터에서는 사용자의 접근자격을 검증한다. 네트워크 사용자가 성공적으로 네트워크 센터로 부터 인증되면, 네트워크 사용자는 통합 네트워크 서비스를 접근할 수 있다. 기타의 경우는 사용자 접근 요구를 거절한다.

가. 제 1단계 : 초기화 단계

(1) 각 네트워크센타 C_m에서의 초기화 단계

각 네트워크 센터 C_m은 초기에 시스템 공용키 PK_m과 시스템 기밀 키 SK_m를 다음 방정식에 의해 생성한다.

$$PK_m \equiv \alpha_m^{SKm} \bmod p,$$
P_m : Large prime number,
α_m : Primitive root of $GF(P_m)$ (3.1)

(2) 네트워크 센터에 사용자 등록을 위한 초기화 단계

사용자 U_i가 특정 네트워크 센터가 관리하는 네트워크 서비스에 접근하고자 할 때, 사용자 U_i는 네트워크센타 C_m에게 자신의 UID_i를 제시한다. 그리고 나서 네트워크 센터 C_m은 네트워크 사용자 U_i에게 슈퍼 스마트 카드 SSC_i를 발행한다. 만약 네트워크 사용자 U_i가 다른 네트워크 센터에 이미 등록되어 슈퍼 스마트 카드를 가지고 있다면, 네트워크 센터 C_m은 네트워크 사용자 U_i에게 슈퍼 스마트 카드를 발행하지 않는다.

슈퍼 스마트 카드는 빠르게 지수, 덧셈, 곱셈 연산을 할 수 있도록 구성되고, 이들을 이용하여 함수 f와 이의 알고리즘으로 이루어진 난수 발생기를 가지고 있다. 여기에서 각 네트워크 사용자는 다중 네트워크 센터를 접근하기 위해서, 단지 하나의 슈퍼 스마트 카드만을 갖는다. 이 단계에서, 네트워크 센터 C_m이 네트워크 U_i에 대해, 사용자 키 UK_i와 암호 $PWm,i = (r_{m,i}, s_{mi})$를 생성해 낸다. 사용자 U_i의 등록을 위해서, 네트워크 센터는 다음 방적식이 가지는 암호 $PW_{m,i}$를 만들어 낸다.

$$\alpha_m^{UIDi} \equiv PK_m^{Sm,i} \mod P_m \quad (3.2)$$

센터는 사용자 U_i에 대해 $PW_{m,i}$를 생성하기 위해서 다음과 같은 절차에 따른다. 이때 방정식 (3.2)가 만족되어야 한다.

i) $gcd(K_{m,i}, P_m - 1) = 1$인 0과 P_m-1사이에서 무자귀로 $K_{m,i}$를 선택한다. $K_{m,i}$는 결코 다른 사용자에 의해 중복 사용되지 않는다.

ii) $r_{m,i} = \alpha m^{km,i} \mod P_m$을 계산 (3.3)

iii) 다음 식을 만족하는 $s_{m,i}$를 계산

$$UID_i \equiv SK_m r_{m,i} + S_{m,i} \mod(P_m - 1) \quad (3.4)$$

네트워크 센타 C_m은 네트워크 사용자 U_i의 UK_i를 $1 < UK_i < P-1$ 조건하에서 무자귀로 생성한다. 또한 네트워크 센터는 다음과 같은 메세지를 생성하여 이를 안전한 채널을 통해서 네트워크 사용자 U_i에게 전송한다.

$$IM_{m,i} = \{CID_m, PW_{m,i}, UK_i\}$$

(3) 네트워크 사용자 초기화 단계

네트워크 사용자 U_i가 제공한 메세지 $IM_{m,i}$를 수신했을 때, 네트워크 사용자 U_i는 사용자 키 UK_i와 암호 $PW_{m,i}$를 얻게 된다. 이때 네트워크 사용자 U_i는 네트워크 센터에서 송신한 UK_i를 사용할 수 있고 혹은 자유롭게 다른 사용자가 선택할 수도 있다. 네트워크 사용자 초기화 단계에서는 2가지 경우가 발생할 수 있다. 슈퍼 스마트 카드가 최초로 네트워크 사용자 U_i에게 발행되면, 네트워크 사용자 U_i는 센터가 제공하는 암호 PW_i를 슈퍼 스마트 카드 SSC_i에 넣기 전에 사용자 키 UK_i를 기록한다. 이렇게 넣어진 사용자 키는 슈퍼 스마트 카드 함수 f에 의해 암호화되어 SSC_i에 저장된다. 사용자 키 저장이 성공된 후에 네트워크 사용자 U_i는 슈퍼 스마트 카드 SSC_i의 $SSCPW_i[CID_m]$에 $(r_{m,i}, s_{m,i})$ 쌍으로 이루어진 암호 $PW_{m,i}$를 기록한다. 만약, 네트워크 사용자 U_i가 이미 스마트 카드 SSC_i를 가지고 있다면, 네트워크 사용자 U_i는 그들의 사용자 식별을 검증하기 위하여, 사용자 키 UK_i를 슈퍼 스마트 카드에 표현한다. 그때, 슈퍼 스마트 카드가 그의 함수 f를 사용하여, 사용자 키 UK_i를 암호화 한다. 만약 암호화 된 사용자 키가 암호화 형태에 있어서 이전에 저장된 사용자 키와 동일하면, 네트워크 사용자 U_i는 슈퍼 스마트 카드 SSC_i의 적법한 소유자로 인정한다. 그리고 나서, 네트워크 사용자 U_i는 슈퍼 스마트 카드 SSC_i로 암호를 입력한다. 만약 이 암호가 슈퍼 스마트 카드 SSC_i에서 정당한 사용자 키로 표현되지 않으면, 슈퍼 스마트 카드는 더 이상 접근할 수 없게 된다. 따라서 이 기법은 침입자에 의해, 암호의 수정을 방지한다. 이 단계는 다음과 같은 절차로 나타낼 수 있다.

if 슈퍼 스마트 카드 SSC_i를 네트워크 사용자 U_i에게 처음 발행한다.

then 슈퍼 스마트 카드에 사용자 키 UK_i를 기록한다.
슈퍼 스마트 카드 함수 $EUK_i = f(UK_i)$를 사용하여 사용자 키 UK_i를 암호화한다.
슈퍼 스마트 카드 SSC_i에 EUK_i를 저장한다.
슈퍼 스마트 카드 SSC_i의 $SSCPW_i[CID_m]$에 암호 PWm,i와 네트워크 센터 식별자 CID_m을 기록한다.

else 슈퍼 스마트 카드 SSC_i에 사용자 키 UK_i를 기록한다.
슈퍼스마트카드 함수 $f(UK_i)$에 의해, 사용자 키 UK_i를 암호화 한다.

if 산출된 $f(UK_i)$ = 정장된 EUK_i

then 슈퍼 스마트 카드 SSC_i의 $SSCPW_i[CID_m]$에 센터 식별자 CID_m과 암호 $PW_{m,i}$를 기록한다.

else 진행을 중단하고 멈춘다.

나. 제 2 단계 : 로그-인 단계

이 단계에서 네트워크 사용자 U_i는 터미널에 슈퍼 스마트 카드를 접착시켜, 터미널에 암호 $PW_{m,i}$가가 아닌, 사용자 식별자 UID_i와 사용자 키 UK_i를 제출한다. 이는 Chang과 Liao의 로그-인 단계를 수정한 것이다. 네트워크 사용자 U_i의 슈퍼 스마트 카드 SSC_i는 자신이 가지고 있는

함수 f에 의해, 넣어진 사용자 키 UK_i를 암호화 한다. 만약 사용자 키가 타당하면, 슈퍼 스마트 카드 SSC_i는 다음의 ii), iii), iv)를 차례로 실행한다.

i) 사용자 식별자 UID_i를 입력한다.
사용자 키 UK_i를 입력하고, $f(UK_i)$ 함수에 의해 UK_i를 암호화 한다.
if 산출된 $f(UK_i)$ = 저장된 EUK_i
then 다음 단계인 ii)를 실행한다.
else 진행을 거절하고 멈춘다.

ii) $1<t<p-1$ 조건을 만족하는 난수 t를 선택한다.

난수 t는 (3.5)를 만족하고, 서로 다른 A를 계산하기 위해 이중으로 사용되어서는 안된다.

iii) 다음을 계산한다.

$$A = r_{m,i}\ t * r_{m,i}\ UK_i \bmod p \qquad (3.5)$$

$$B = (t+UK_i)+s_{m,i} * f(A,T) \bmod p-1 \qquad (3.6)$$

iv) 로그-인 메세지 $LM_{i,m}$ = {UID_i, $r_{m,i}$, A,B,T} 를 센터로 전송한다.

다. 제 3 단계 : 인증 단계

네트워크 사용자 U_i로 부터 보내 온 로그-인 메세지 $LM_{i,m}$ = {UID_i, $r_{m,i}$, A, B, T}를 받은 후에, 센터 C_m은 이를 근거로 하여, 로그-인 요구를 검증한다. 첫째, 시스템이 로그-인 메세지를 수신한 날자와 시간을 나타내는 T'를 기록한다. 그리고 나서 $\delta T = T'-T$를 계산한다. 만약 δT가 전송지연에 대한 적법한 시간 간격 ΔT보다 작다면, 센터 C_m은 아래의 방정식(3.7)을 계산한다. 기타의 경우는 네트워크 사용자 U_i의 로그-인 요구를 거절한다. 만약 방정식(3.7)의 결과인 A1이 제 2 단계의 방정식(3.5)에서 네트워크 사용자 U_i에 의해 생성된 로그-인 메세지 $LM_{i,m}$으로 부터 주어진 A와 같다면, 사용자 U_i는 성공적으로 인증된다. 이 단계의 알고리즘은 다음과 같다.

if $\delta T \le \Delta T$,
T' : Received date & Time, $\delta T = T'-T$
then 사용자 로그-인 거절
else $A1' = r^{B}_{m,i}((PK_m - R_{m,i} * \alpha_m^{UIDi})^{-1})^{f(A,T)} \bmod P$ (3.5)
If A1=A1'
then 사용자 U_i의 인증이 성공됨
else 사용자 인증 실패

Ⅳ. 결 론

본 논문에서는 ElGamal의 디지탈 서명 기법과 이를 기반으로 한 Chang과 Liao의 원격 암호 기법을 분석하였다. ElGamal의 서명 기법은 유한 영역에서 이산 log 계산에 어려움이 있다. 참고 자료[3]에서 Chang과 Liao의 기법의 보안도 또한 이러한 어려움을 설명하고 있다. Chang과 Liao의 기법은 k와 t에 의한 난수를 생성하는데 몇 가지 문제점이 있다. 하지만 Chang과 Liao의 기법에서 이러한 문제점을 제거하면, 원격 로그-인 환경에 적용이 가능하다. 본 논문에서 제안한 기법은 상기의 2기법을 근간으로 하여, 효율적으로 네트워크상의 다중 센터와 상호 작용할 수 있는 원격 인증기능을 한다. 새롭게 제안된 시스템은 k와 t에 의한 난수 생성기를 개선했기 때문에 Chang과 Liao의 기법보다 더 안전(Secure)하다.

감사의 말씀

본 논문은 95년도 배재대학교 교내학술연구비 지원에 의하여 수행된 연구의 일부로 이에 감사를 드립니다.

참 고 문 헌

1. R.E. Lennon, S.M. Matyas and C.H. Meyer, "Cryptographic authentication of time-invarient quantities", IEEE Transactions on Communications, Vol. COM-29, No.6,pp. 773-777, Jun, 1985.
2. T.ElGamal, "A public key cryptosystem and a signature schemse based on discrete logarrithms", IEEE Transactions on Information Theory, vol. IT-31, No.4, pp.469-472, Jul. 1985.
3. C.C. Chang and W.Y. Liao, "A Remote Password Authentication Scheme based upon ElGamal's Signature Scheme", Computer and Security, Vol, 13,No.2, pp.137-144, Apr. 1994.
4. Jerome Svigals, "Smartcards-A Security Assessment", Computer and Security, Vol.13, No.2, pp.107-114, Apr. 1994.