국방전산통신망을 위한 국방인증체계(MPKI) 개선 방안에 관한 연구

한광택* · 이수연** · 박창섭***

요 약

국방 관련 암호 및 인증체계는 전장관리정보체계를 위한 키관리체계(KMI), 자원관리정보체계를 위한 국방인증체계(MPKI) 그리고 행정기관 연계 정보시스템을 위한 행정전자서명 인증체계(GPKI)로 구분한다. 본 논문에서는 국방인증체계(MPKI)에서 사용되고 있는 공개키기반구조(PKI)의 사용자 인증 관련 문제점과 보안 위협사항을 분석하고, 이를 보완하기 위한 속성기반 서명기법을 사용한 개선된 속성기반의 인증기법을 제시하고자 한다. 제안하는 기법에서는 서명에 포함되는 접근 구조를 Monotone Span Program(MSP)을 사용하였으며, 체계서버가 사용자 인증을 통해 서비스를 제공하게 하였다.

A Study of Improvement Schemes for MPKI of National Defense Digital Network

Kwang-taek Han* · Su-youn Lee** · Chang-seop Park***

ABSTRACT

Encryption and authentication system in National Defense is divided into three system; KMI, MPKI, and GPKI. In this paper, we report inherent problem and security threaten in MPKI and propose an attribute-based authentication scheme using attribute-based signature in order to improve user authentication. In our scheme, access structure is used by Monotone Span Program, and system server provides service after user authentication.

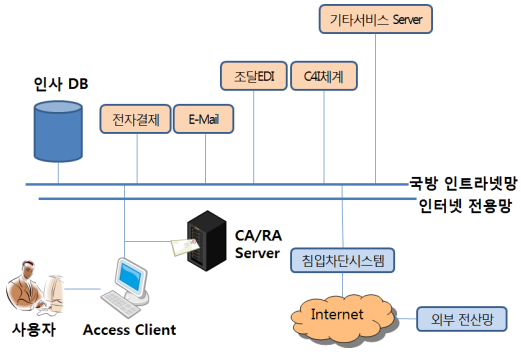
Key words : Military Public Key Infrastructure, Attribute-Based Signature, Monotone Span Program

접수일(2014년 10월 6일), 수정일(1차: 2014년 10월 13일), 게재확정일(2014년 10월 20일)

* 한국전자통신연구원 부설연구소(책임 저자)
** 백석문화대학교 인터넷정보학부(교신 저자)
*** 단국대학교 컴퓨터과학과

1. 서 론

현재 우리 군은 사무행정업무의 자동화, 문서관리 및 유통, 전자메일 사용을 통한 국방사무행정 효율성 향상을 위해 국방전산망을 구축하여 운영하고 있다[1]. 국방전산망은 군별·기관별 구분없이 전군을 지원하는 통합된 단일 네트워크로서 국방망 간선을 통한 인트라넷망과 ATM WAN을 통한 인터넷 전용선을 이용한 인터넷 전용망으로 구성되어 있다. 그 중 국방 인트라넷망은 [그림 1]과 같이 크게 전자결재시스템, E-mail 송수신, C4I시스템, 조달 EDI 등으로 나누어지며[2], 이들은 전군을 대상으로 전자결재, E-mail 송수신 등의 서비스를 제공하고 있다.



(그림 1) 국방전산망 구성도

군에서 운영하는 전산망에는 1급/2급 비밀, 대외비 등의 기밀문서도 취급함에 따라 TCSEC에서 강력한 보안이 보장되는 수준으로 평가하는 기준인 B2등급 이상의 보안수준을 만족해야 하며[2] 이에 따른 국방전산망에서의 보안 요구사항은 다음과 같은 항목이 있다.

- 인증: 사용자나 프로그램이 서로 통신할 때 상대방을 확인해야 한다.
- 부인방지: 누가, 무엇을, 언제, 어디서 했는지 알 수 있는 능력, 사용자들은 자신의 행위에 대해 책임을 질 수 있어야 한다.
- 무결성: 정보의 조작 및 변경여부를 확인할 수 있다.
- 접근 통제 및 시점 확인: 특정 자원에 대한 접근은 정해진 객체들에게만 허용된다. 또한 시점 확인은 타임스탬프를 적용하여 발신자를 구분한다.

국방전산망은 이를 위한 보안 대책으로써 응용체계에서 송수신 되는 전자문서의 무결성, 기밀성 보장을 위해 암호장비를 사용하고 있고[3], 이와 더불어 국방 인트라넷 망에서는 ID/패스워드 노출 등의 내부자의 위협 및 해킹에 대비하여 국방인증체계(MPKI: Military Public Key Infrastructure)를 구축·운용하고 있다.

이러한 국방인증체계(MPKI)는 GPKI와 NPKI와 마찬가지로 인증서 기반의 사용자 인증만 수행하고, 현재 국방인증체계 내에서의 신원 확인은 사람이 직접 인사정보체계의 데이터베이스에 접근하여 확인하는 방식으로 이루어져 있으며 자동화된 연동 개념이 없는 상태로서, 전역, 면직 등 인사정보 내용의 변동이 발생해도 실시간으로 반영이 되지 않는 실정이다[3]. 이로 인해 효율성 측면에서나 안정성 측면에서도 문제가 있을 수 있으므로 이에 대한 연구가 필요하다.

이에 본 논문에서는 사용자가 다수의 국방 체계들이 제공하는 보안서비스를 받기 위해 사용자의 속성정보를 활용한 속성기반 서명기법을 통해 인증 후 서비스를 받게 함으로서, 앞서 제시한 효율성, 안정성 문제를 개선하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 국방 인트라넷망에서 ID/패스워드 노출 등의 내부자의 위협 및 해킹에 대비하여 구축 및 운용 중인 국방인증체계(MPKI)에 대해 알아보고, 3장에서는 본 논문에서 제시하고자 하는 속성 기반 인증에 대한 관련 기술로서 ID 기반 암호시스템(Identity Based Cryptosystem) 및 속성 기반 암호시스템(Attribute Based Cryptosystem)에 대해 살펴본다. 그리고 4장에서는 MPKI에서 개선 된 속성기반 인증 기법을 제안하고 5장에서는 보안 요구사항을 분석하였다. 마지막으로 6장은 결론으로 향후 연구방향을 제시하였다.

2. 국방인증체계(MPKI)

국방관련 인증체계는 전장관리정보체계를 위한 키

관리체계(KMI), 자원정보관리체계를 위한 국방인증체계(MPKI), 행정기관 연계 정보시스템을 위한 행정전자서명 인증체계(GPKI)로 구분한다[4]. 이중 국방인증체계는 국방정보보호체계에서 필수적으로 요구되는 기밀성, 무결성, 인증, 부인봉쇄, 가용성 등의 정보보호 기능을 통합적으로 지원하기 위한 공개키 기반의 정보보호 기반체계[5]로서, 국방 사용자 등을 대상으로 공개키 인증서를 발급, 관리하는데 공개키 인증서는 사용자 로그인과 같은 식별 및 인증 수단으로 제공한다.

현재 국방인증체계 내에서의 신원 인증은 사람이 직접 인사정보체계의 데이터베이스에 접근하여 확인하는 방식으로 이루어져 있으며 자동화된 연동 개념이 없는 상태이다. 전역, 면직 등 인사정보 내용의 변동이 발생해도 실시간으로 반영이 되지 않는 실정이다[1]. 이로 인해 효율성 측면에서나 안정성 측면에서도 문제가 있을 수 있으므로 이에 대한 연구가 필요하다. 또한 향후에는 군의 특성에 따라 각기 별도로 운용중인 네트워크들을 하나의 네트워크로 통합 예정인 바, 통합된 네트워크에서의 단일 인증체계를 통한 상호운용성 향상이 요구되고 있다. 이러한 단일 인증체계에서의 다양한 특성과 각기 다른 비도를 갖는 체계들에 대한 안전한 사용이 중요해짐에 따라, 이에 대한 권한 관리에 대한 연구도 필요하다.

3. 관련 연구

3.1 IBC(Identity Based Cryptosystem)

일반적으로 공개키 암호화를 이용한 메시지 전달이나 전자서명에서의 서명 검증절차 등에서 공개키에 대한 인증이 요구된다. 인증서 기반의 공개키 암호시스템에서는 이와 같은 문제를 신뢰된 인증기관으로부터 공개키 인증서를 발급함으로써 해결한다. 이와 같은 방법은 인증서에 대한 유지 및 관리 부담을 갖게 된다. 이는 군 환경에서 암호장비장애 및 인증모듈 에러시 신속대응이 제한된다. 이와 같은 문제를 해결하기 위해 제안된 기법이 ID기반 암호시스템 IBE이다.

3.1.1 IBE(Identity Based Encryption)[6]

- 설정(Setup): 설정 알고리즘은 보안 상수를 입력으로 하여 기관(Authority)의 마스터 비밀키($MSK: Master\,Secret\,Key$)와 공개 파라미터($PP: Public\,Parameter$)를 생성한다.
- 사용자 비밀키 생성(Key Generation): 기관의 집합 $S \subseteq \{1,2,....,n\}$에 대하여 접근 권한을 가지고 ID를 확인자로 사용하는 사용자는 다음과 같은 과정을 통해 비밀키를 발급 받는다.
  ① 기관 $a \in S$ 는 사용자의 확인자인 ID의 접근 권한을 확인한다.
  ② 기관은 ID에 대응하는 비밀키를 자신의 MSK를 이용하여 생성한다.
  ③ 기관은 사용자에게 비밀키를 안전하게 전송하고 사용자는 자신의 기관에서 받은 비밀키들을 안전하게 저장한다.
- 암호화(Encryption): ID에 대응하는 메시지 M에 대한 암호문을 생성하기 위해 기관의 집합 $S' \subseteq \{1,2,....,n\}$을 선택하고 각 S'에 포함된 기관들의 공개 파라미터를 이용하여 암호문을 생성한다.
- 복호화(Decryption): 암호문을 복호화하기 위해 사용자는 각 기관으로 받은 자신의 비밀키를 입력으로하여 다음과 같이 계산한다.
  ① $S' \subseteq S$ 을 만족하는지 확인한다.
  ② 암호문의 ID와 자신의 비밀키의 ID가 일치하면 암호문을 자신의 비밀키들로 복호화하여 메시지 M을 얻는다.

3.1.2 IBS(Identity Based Signature)

- 설정(Setup) : 사용자 비밀키 생성 (Key Generation)
- 서명(Sign): ID에 대응하는 메시지 M에 대한 서명을 생성하기 위해 기관으로부터 받은 자신의 서명키를 입력으로 한다. 기관의 집합 $S' \in S$을 선택하고 서명을 생성한다.
- 검증(Verify): ID, M 에 대응하고 기관의 집합 $S' \in S$ 포함된 서명을 S'에 포함된 기관에 대한 공개키와 사용자 공개키 ID와M을 입력으

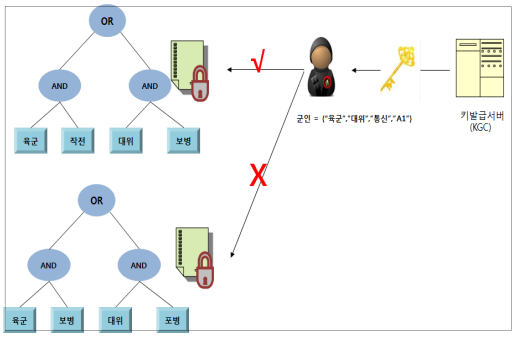
로 하여 서명을 검증한다.

3.2 ABC(Attribute Based Cryptosystem)

속성기반 암호기술은 ID기반 암호기술의 확장된 개념으로 Sahai와 Waters에 의해 처음 제안되었다. 이는 사용자의 속성 값을 암호 인자로 사용하여 속성에 대한 비밀키를 가지고 있는 사용자만이 암호화된 데이터를 복호화하는 기법이다. 즉, 사용자의 속성 정보의 집합과 속성의 접근 구조를 바탕으로 암·복화를 실시하는 방식이다. 여기서 접근 구조란 주어진 속성 집합에 대해 접근을 허가하는지 아닌지를 결정하는 방법이다. 접근 구조를 암호화 시에 지정하느냐 키 생성시에 지정하느냐에 따라 CP(Ciphertext Policy)-ABE, KP(Key Police)-ABE로 구분된다. 하지만 CP-ABE와 KP-ABE는 둘 다 다수의 속성에 대한 공개키와 개인키 쌍의 구조를 접근 트리(access tree)로 표현하였다. 이것이 CP/KP-ABE의 핵심이다[7].

3.2.1 CP-ABE

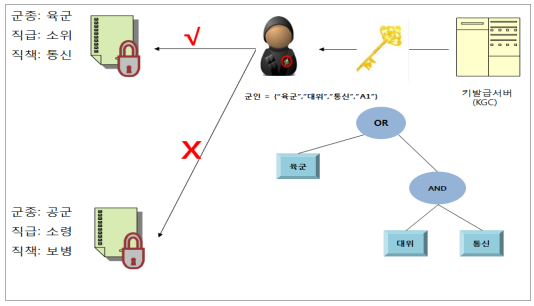
CP-ABE는 암호문 생성시 송신자가 접근 구조를 지정하여 수신자의 속성 집합을 바탕으로 복호화를 한다.



[그림 2] CP-ABE

■ KP-ABE

KP-ABE는 복호 가능한 속성 집합으로 송신자가 암호화하고 수신자의 키 생성 시 자신의 속성 집합에 근거하는 접근구조를 바탕으로 복호화한다.



[그림 3] KP-ABE

3.2.2 ABS(Attribute Based Signature)

속성 기반 서명 기법(ABS)은 2008년 H. Magi, M. Prabhakaran 그리고 M. Rosales에 의해 처음으로 소개되었다[8]. 서명자의 개인키에 속성 집합(Attribute Set)이 연관되고 서명에 접근 구조(Access Structure)가 연관되는 서명 기법이다. 속성 기반 서명 기법은 다음과 같은 알고리즘으로 정의된다.

(1) Setup(1^l): 설정 알고리즘은 입력으로 보안 파라미터 1^l 값을 받고 공개 파라미터 PP 값과 마스터 비밀키 MK 값을 출력한다.

(2) KeyGen(w, MK, PP) : 비밀키 생성 알고리즘은 속성 스트링 a_i 값으로 이루어진 속성 집합 $w = \{a_1, \ldots, a_l\}$, 마스터 비밀키 MK 그리고 공개 파라미터 PP 값을 받고 사용자의 비밀키 SK_w 값을 출력한다.

(3) Sign(M, AS, SK_w, PP) : 서명 알고리즘은 입력으로 메시지 M, 접근구조 AS, 사용자 비밀키 SK_w 그리고 공개 파라미터 PP 값을 받고 사용자의 속성 집합이 $w \in AS$ 조건을 만족하는 경우 서명 σ 값을 출력한다.

(4) Verify(σ, M, AS, PP) : 검증 알고리즘은 입력으로 서명 σ, 메시지 M, 접근구조 AS 그리고 공개 파라미터 PP 값을 받고 서명의 올바름 여부에 따라서 “accept” 또는 “reject” 값을 출력한다.

4. MPKI에서 속성기반 인증 개선 방안

군 직책 및 업무구조의 특수성과 국방전산통신망의 특성상 접근권한에 대한 구분이 명확하게 되어야 한다. 이것은 곧 사용자가 갖는 정보 즉, 직급, 직책, 업무형식 등에 따라 사용자 인증이 다르게 수행되며, 적절한 접근 권한이 적용되어야 한다는 것을 의미한다.

국방인증정책(CP)에 의거, MPKI는 <표 1>과 같이 많은 국방 체계들에 대해 각각 특성에 따라 사용자 인증, 보안메일 등의 보안 서비스를 선택적으로 제공하고 있다[4].

<표 1> 체계 서버 이름 및 제공 서비스

구 분	내 용
체계 서버	A체계, B체계, C체계
제공 서비스	사용자인증, 보안메일, 결재암호인증, 전자관인 등

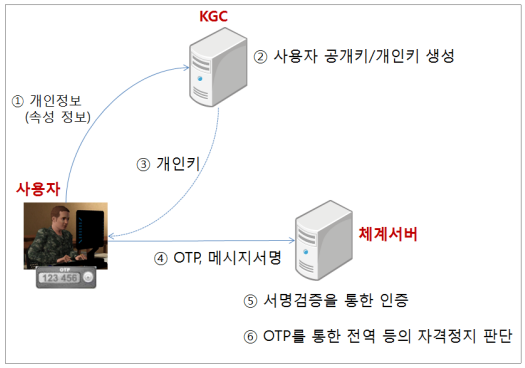
이러한 특성들과 제공되는 보안서비스는 <표 2>와 같이 각각의 속성정보로서 표현될 수 있으며, 이들을 활용하여 각각의 고유한 인증정보를 표현할 수 있다.

<표 2> 속성 정보

속성 종류	속성 내용
군종	육·해·공군 중 택일
소속	사단급 이상의 소속 부대
직책	보병·포병·기갑·공병·통신 등의 병과
직급	부사관 이상의 계급
인사 정보	전역, 면직 등의 인사 상태

개선 된 MPKI에서는 ABC를 사용하여 각 사용자는 자신의 식별자를 속성 집합으로 표현하며 키 생성기관이 속성집합에 대한 개인키를 생성하여 사용자에게 전달한다. 사용자는 속성 집합에 대한 개인키를 이용하여 메시지에 대한 서명을 수행하여 체계서버로부터 인증 및 서비스를 제공받을 수 있도록 설계되어져야한다.

[그림 4]는 본 논문에서 제안하고자 하는 MPKI에서 국방망 사용자에 대한 인증 및 서비스 제공 절차이다.



[그림 4] 제안 프로토콜

먼저, 국방망 사용자(U_i)는 자신을 식별할 수 있는 속성 정보($\AA = [u_1, u_2, ..., u_n]$)를 키 생성기관($KGC$)에 보내어 속성 집합에 대한 개인키를 발급받는다. 개인키를 통해 메시지를 서명하여 체계서버에 보내 인증을 수행하고 또한, $OTP(One\ Time\ Password)$ 값을 통해 인사정보를 확인하여 서비스 제공 유·무를 결정한다.

4.1 Monotone Span Program(MSP)

Karchmer와 Wigderson[9]에 의해 소개된 MSP는 논리 함수를 연산하기 위한 선형 대수 모델로써 소개되어졌다.

[정의] MSP는 행렬 $\widehat{M}(F, M, \epsilon, \rho)$ 으로 표현된다. 여기서 F는 필드이며 M 은 $F^{m \times d}$행렬이다. $\sigma : \{1,....,m\} \rightarrow \{1,....,n\}$으로 나타나고 $\epsilon = (1,0,....,0) \in F^d$로 target vector를 의미한다.

MSP는 $G \in \widehat{A} \Leftrightarrow \epsilon \in span(M_G)$이면 접근 구조(access structure)의 연산이 수행된다.

[예] $\widehat{M} = (F_{17}, M, \epsilon, \rho)$ 여기서

$$M = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \\ 1 & 4 & 16 \end{pmatrix}$$

$\rho(1) = \rho(2) = p_2$, $\rho(3) = p_1$, $\rho(4) = p_3$ 로 나타난다. $B = \{p_1, p_2\}$와 $T = \{p_3, p_4\}$집합을 고려해보자

$M_B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix}$ $M_T = \begin{pmatrix} 1 & 3 & 9 \\ 1 & 4 & 16 \end{pmatrix}$

$\epsilon \in span(M_B) : (3,14,1) M_B = \epsilon$이므로 $B \in \hat{A}$이고

$\epsilon \notin span(M_T)$이므로 $T \notin \hat{A}$ 이다.

ABC에서 어떠한 속성들의 집합으로 암·복호화 할 수 있는 개체를 유일하게 지정하기보다는 속성들의 집합을 만족하는 개체들이 복호화 할 수 있도록 할 수 있다. 따라서 이러한 접근 구조는 $AND(\wedge), OR(\vee)$ 등의 연산을 통해 비밀키 속성에 구성된다. 이와 같이 접근 구조는 논리 연산에 의해 이루어져야한다. 본 논문에서는 사용자가 체계서버에 메시지 서명 시 접근 구조(γ)로 MSP를 사용하므로 속성의 권한에 대한 접근 구조를 효율적으로 구성하였다.

4.2 제안 기법 설명

본 논문에서는 사용하는 용어들을 <표 3>에서 정의하였다.

(1) 새로운 사용자 U_i가 키 생성 서버(KGC)에 등록하기 위해서는 자신에 대한 속성(군종, 소속, 직책 등)에 따라 속성 집합 $Å = [u_1, u_2, ..., u_n]$를 KGC 에게 전송한다.

(2) KGC는 U_i가 입력한 속성에 따라 공개파라미터(PK)와 마스터키(MK)를 생성하며 그 과정은 다음과 같다.

<표 3> 용어 정의

용어	정의
KGC	키 생성 서버
U_i	사용자
MK	마스터 키
PK	공개 파라미터
SK_A	사용자 속성 개인키
p	임의의 큰 소수
$t_{\max}$	monotone span program 넓이
$h(\bullet) : \{0,1\}^* \rightarrow \{0,1\}^n$	일방향 해쉬 함수
$Å = [u_1, u_2, ..., u_n]$	사용자 U_i에 대한 모든 속성 집합

① Setup(1^k): 설정 알고리즘은 먼저 소수 p를 윗수로 가지는 bilinear 그룹 G_1, G_2와 G_T를 선택한다. 여기서 $e : G_1 \times G_2 \rightarrow G_T$ 이다. 이 때 소수 p는 랜덤 소수로 k 비트 길이를 가진다. 알고리즘은 그룹 생성원 $g \in G_1$와 $\prod_{i=0}^{t_{\max}} h_i \in G_2$를 랜덤하게 선택한다. 충돌회피를 위해 $H : \{0,1\}^* \rightarrow Z_p^*$를 선택한다. 그리고 랜덤하게 $a_0, a, b, c \in Z_p^*$를 선택하고 $C = g^c$; $A_0 = h_0^{a_0}$; $A_j = h_j^a$와 $B_j = h_j^b (\forall j \in [t_{\max}])$ 을 계산한다. 시스템 전체의 공개파라미터 PK와 마스터 키 MK는 다음과 같이 설정한다.

- $PK = (A_0, ..., A_{t_{\max}}, B_1, ..., B_{t_{\max}}, C)$

$MK = (a_0, a, b)$

② 키 생성(MK, Å) : KGC의 마스터 키 MK를 이용하여 속성 집합 $Å = [u_1, u_2, ..., u_n]$에 대한 개인키 SK_A를 생성하기 위해서는 다음 과정을 수행한다. 랜덤 값 $K_t \in G$ 를 선택한 후

$K_0 = K_t^{1/a_0}$; $K_u = K_t^{1/(a+bu)}$ $(\forall u \in Å)$

$SK_A = (K_t, K_0, \{K_u | u \in Å\})$

(3) KGC는 U_i에게 SK_A 를 안전하게 전송하고 U_i는 KGC에게 받은 자신의 개인키 $SK_A = (K_t, K_0, \{K_u | u \in Å\})$를 안전하게 저장한다.

(4) U_i 는 자신이 가진 다양한 속성 중에서 체계서버에서 서비스를 제공받기 위해 메시지를 서명하고 OTP 값과 함께 보낸다.

① 서명(PK, SK_A, m, γ): 서명 알고리즘은 입력

으로 메시지 m, 접근구조 γ, 개인키 SK_A를 사용한다. 이때 사용자의 속성 집합이 $Å \in \gamma$ 조건 즉, $\gamma(Å)=1$을 만족하는 경우 서명 σ 값을 출력한다. 서명 생성과정은 다음과 같다.

▪ 먼저, 접근구조 γ 를 적합한 MSP $M \in (Z_p)^{l \times n}$으로 변환시킨다. 또한, 속성집합 $Å$에 적합한 벡터 $\vec{v}$ 와 $\mu = H(m \| \gamma)$를 계산한다.

▪ 랜덤 값 $r_0 \in Z_p^*$ 와 $\prod_{i=1}^{l} r_i \in Z_p$을 선택하고

$Y = K_t^{r_0}$; $S_i = (K_{u_i}^{v_i})^{r_0} \bullet (Cg^{\mu})^{r_i} (\forall i \in [l])$;

$W = K_0^{r_0}$; $P_j = \prod_{i=1}^{l} (A_j B_j^{u_i})^{M_{ij}} \bullet {}^{r_i} (\forall j \in [n])$;

서명 값 $\sigma = (Y, W, S_1, ..., S_l, P_1, ..., P_n)$을 보낸다.

(5) 체계서버는 U_i가 서명해서 보낸 서명 값 σ을 검증한다.

② 검증(σ, PK, m, γ)

▪ 검증 알고리즘은 입력으로 서명 σ, 메시지 m 그리고 접근 구조 γ 값을 받는다. 먼저, 접근구조 γ를 적합한 MSP $M \in (Z_p)^{l \times n}$으로 변환시킨다.

▪ 만약 $Y=1$ 즉, 랜덤 값 $K_t=1$이거나 $r_0=0$이면 reject이고 그렇지 않으면 다음 두 수식이 성립하는지 체크한다.

$$e(W, A_0) = e(Y, h_0)$$

$$\prod_{i=1}^{l} e(S_i, (A_j B_j^{u_i})^{M_{ij}}) = \begin{cases} e(Y, h_1) e(Cg^{\mu}, P_1), & j=1 \\ e(Cg^{\mu}, P_j), & j > 1 \end{cases}$$

위의 두 수식이 성립하는 경우 "accept" 출력하고 그렇지 않은 경우 "reject" 출력한다.

(6) OTP 값을 통해 사용자의 인사정보를 확인하여 서비스 제공 유・무를 결정한다.

5. 보안 요구 분석

지금까지 속성기반 서명을 통해 MPKI 개선 된 속성기반 인증방식을 알아보았다. 본 장에서는 MPKI 환경에 필요한 보안 위협을 분석한다.

- 인증: 키 생성 시 사용자의 속성 집합 $Å = [u_1, u_2, ..., u_n]$에 대해 랜덤 값 KGC의 마스터 키 MK로 SK_A가 생성되어 서명이 되었고 체계서버는 공개파라미터 PK를 통해 서명이 확인되므로 사용자가 인증되어진다.
- 부인방지: 사용자는 메시지 m을 접근구조 γ과 해쉬한 값 $\mu = H(m \| \gamma)$ 을 사용하므로 부인 할 수 없다.
- 무결성: 공격자가 서명 σ을 위조하여 $\grave{\rho}$로 보낼 경우 검증단계에서 정의 된 두 가지 수식이 성립되지 못하므로 위조가 불가능하다.
- 접근 통제 및 시점 확인: OTP 값에 동기 값(timestamp)이 들어가 있으므로 사용자의 인사정보(전역, 면직 등)를 확인하여 해당 정보에 접근 여부 및 시점 확인을 할 수 있다.

위에서 살펴본 결과 본 논문에서 제시하고자 하는 속성기반 서명 기법을 통한 국방인증체계(MPKI) 인증기법의 개선점을 정리해보면 다음과 같다.

첫째, 기존의 MPKI에서는 공개키기반구조(PKI)를 사용하므로 인증서기반의 사용자 인증만을 수행하고 있다. 그러므로 공개키에 대한 인증서 유지 및 관리에 부담이 따르고 있다. 즉, 인증서 유효기간이 만료되어 갱신이 필요한 경우 인증서 갱신과 폐기목록(CRL) 관리가 필요하다. 따라서 본 논문에서 제시한 속성기반기법(ABC)은 인증서 관리가 필요 없고 PKI를 구축하지 않아도 되는 장점을 가지고 있다.

둘째, MPKI에서 사용자 인증은 사람이 직접 인사정보체계의 데이터베이스에 접근하여 확인하는 방식으로 이루어져 자동화된 연동 개념이 없는 상태로 전역, 면직 등 인사정보의 실시간 반영이 되지 않는 실정이다. 따라서 본 논문에서 제시한 속성기반서명 기법(ABS)을 사용한 인증기법은 사용자의 속성(군종, 소속, 직책, 직급, 인사정보)을 통해 체계서버에 접근하여 인증 후 서비스 유・무가 결정되므로 인사

정보를 실시간으로 반영할 수 있다.

셋째, 현재 속성 기반 암호기법이 소개된 이후 암호문에 접근 권한 구조를 지정하는 암호문-정책 속성 기반 암호 기법이 제안되어지고 있다. 또한, 암호기법과 달리 속성 기반 시스템에 적용이 가능한 서명 기법에 대한 연구는 아직 미진한 상태이며 최근에 몇 가지 연구 결과가 나오고 있다. 따라서 본 논문에서 제시한 속성기반서명기법에서 객체의 권한 또는 속성들로 구성된 접근 구조를 *MSP*을 사용하므로써 연산 측면에서 효율적이라 할 수 있다.

또한, 보안 요구 분석을 통해 속성기반서명기법을 사용한 인증 기법이 MPKI 환경에서 안전하다는 장점을 가지고 있다.

6. 결 론

본 논문에서는 국방인증체계(MPKI)에서 사용되고 있는 공개키기반구조(PKI)의 사용자 인증 관련 문제점을 살펴보았다. 이를 해결하기 위해 속성기반 암호기술에서 사용되고 있는 기법 중 속성기반 서명을 사용하여 개선된 인증 메커니즘을 제시하였고 보안요구사항도 분석하였다. 향후에는 다양한 접근 정책을 적용한 메커니즘에 대해 연구할 계획이다.

참고문헌

[1] 손상일, “NCW 환경에 부합한 국방 KMI 구축방안 연구”, 수원대학교 박사학위논문, pp.9-14, 2012

[2] 윤희승, “국방망에서의 AC 및 PMI 모델에 관한 연구”, 연세대학교, 석사학위논문, pp.21, 2002

[3] 박춘석, 정연식, 송홍엽, "국방 인트라넷 전자서명 인증시스템 구축 프레임워크," 2000 한국 통신정보보호학회 종합학술발표회 논문집, 연세대학교, pp.3-4, 2000

[4] 이원만, “전장관리체계(C4I)에서의 암호 및 인증방법 개선방안에 관한 연구”, 고려대학교 석사학위논문, pp3, 2000

[5] 최인수, “NCW를 대비한 국방인증체계 종합발전방향 연구”, 한국국방연구원 보고서, pp.93-103, 2008

[6] A.Shamir, “Identity-based cryptosystem and signature schemes,” Advance in Cryptology - Crytpo 1984, LNCE 196, pp 47-53

[7] L. Cheung and C. Newport, “Provably secure ciphertext policy ABE”, Proc, ACM Conference on Computer and Communication Security(CCS), pp. 456-465, 2007

[8] Piyi Yang and Tanveer A.Zia etc, "Efficient and expressive fully secure attribute-based signature in the standard model", Security Research Institute Conferences, pp.252-261, 2011

[9] M.Karchmer and A.Wigderson, "On Span Programs", Structure in Complexity Theory Conference ,pp.102-111, 1993

[자 자 소 개]

한 광 택 (Kwang-taek Han)

1998년 고려대학교 전자계산학과 (이학사)
2001년 고려대학교 전자계산학과 대학원 석사(이학석사)
2006년 고려대학교 정보보호대학원 수료
2000년 4월 ~ 현재 한국전자통신 연구원 부설연구소 선임연구원

이 수 연 (Su-youn Lee)

1990년 단국대학교 전자계산학과 (이학사)
1993년 단국대학교 전산통계학과 대학원 석사(이학석사)
2003년 성균관대학교 전기전자 및 컴퓨터공학부 대학원 박사 (공학박사)
1997년 3월 ~ 현재 백석문화대학교 인터넷정보학부 교수

박 창 섭 (Chang-seop Park)

1983년 연세대학교 경제학사
1983년 한국IBM 근무
1990년 미국 Lehigh Univ. 컴퓨터과학 박사
1990년 3월 ~ 현재 단국대학교 컴퓨터과학과 교수