https://doi.org/10.33778/kcsa.2019.19.3.071

속성 기반 권한위임 관리 기법을 사용한 스마트 자동차 안전성 검토에 관한 연구★

김 진 묵*, 문 정 경**, 황 득 영***

요 약

스마트 자동차에 대한 수요가 급격하게 증가하고 있다. 3GPP와 5GAA와 같은 표준기구에서는 스마트 자동차를 위한 자율주행 자동차를 포함한 커넥티드 카, 자동차 네트워크 인프라에 대한 표준 통신 프로토콜을 제시하고 있다. 하지만 이와 같이, 스마트 자동차 네트워크 환경에는 기존의 유선 통신 네트워크 보다 더욱 위험할 것으로 예상되는 보안 위협 요소들이 존재한다. 대표적으로 스마트 자동차의 주변 장치들이 신분을 위장하여 차량에 대한 위치정보, 개인 정보 등을 탈취할 수 있을 뿐만 아니라, 스마트 자동차 주변의 인프라 요소들이 공모하여 주행중인 자동차를 위험한 상황에 빠뜨려 생명에 위협을 가할 수도 있을 것이다. 이를 해결하기 위해서, 본 논문에서는 속성 기반 권한 위임 관리 기법과 임계치 암호 알고리즘을 사용해 공모 공격으로부터 안전한 시스템을 제안하였다. 제안한 시스템은 앞서 예로 제시한 공모 공격으로부터 안전할 수 있음을 의미론적 안전 모델을 사용해서 증명하였다.

A Study of a Secure Smart Car System using Attribute-based Delegation Method

Jin-Mook Kim*, Jeong-Kyung Moon**, Deuk-Young Hwang***

ABSTRACT

The demand of smart cars is increasing rapidly. International stand organize such as 3GPP and 5GAA are proposing standard communication protocvols for connected-car, and automotive network infrastructure. But Smart car network have many security threats and more dangerous against the existed wire communication network. Typically, peripheral devices of a smart car may disguise their identity and steal location information and personal information about the vehicle. In addition, the infrastructure elements around smart cars can conspire and put driving cars in danger, threatening lives. This is a very serious security threat. Therefore, in order to solve these problems, we proposed a system that is secure from collusion and tampering attacks using attribute-based authorize delegation method and threshold encryption algorithms. We have demonstrated using a semantic safety model that the proposed system can be safe from collusion attack.

Key words : Smart car, Attribute-based authentication, Authority delegate manager, Attribute change key, Key share, Dynamic threshold cipher

접수일(2019년 6월 25일), 수정일(1차: 2019년 9월 19일)
게재확정일(2019년 9월 30일)

★ 본 논문은 2017년도 강원대학교 대학회계 학술연구조성비로 연구하였음(관리번호-620170062).

* 선문대학교 IT교육학부
** 가천대학교 소프트웨어중심대학
*** 강원대학교삼척캠퍼스 컴퓨터공학과(교신저자)

1. 서 론

만물 인터넷 시대가 다가오고 있다. 즉 사물과 사물이 스스로 통신을 하고, 이를 통해서 또 다른 사물을 제어할 수 있는 세상이 도래하는 실정이다. 그 중에서 스마트 자동차 분야의 발전은 가장 관심을 받고 있다. 자율 주행 뿐만 아니라 자동차 스스로 탑승자의 건강 상태 정보 등을 파악하여 주변의 병원으로 이동하거나 할 수 있는 세상이 되는 것도 그리 먼일은 아닐 것이다.

하지만 스마트 자동차 분야에서 사물인터넷 기술이 발전하면 할수록 보안 위협 요소들은 급증하고 있다. 예를 들어서, 스마트 자동차의 문을 열기 위한 비밀번호를 해킹할 수도 있고, 스마트 자동차 소유자만이 가져야 하는 권한을 불법으로 취득하여 스마트 자동차 자체를 강제로 이동시키거나 훔칠 수도 있다. 뿐만 아니라 스마트 자동차의 위치 정보를 불법으로 추적할 수도 있다. 그리고 스마트 자동차 자체의 하드웨어를 올바르게 동작하지 않도록 원격에서 공격할 수도 있다[1, 3, 4, 5].

본 논문에서는 스마트 자동차에 대한 위치 추적, 스마트 자동차 문을 원격에서 불법으로 잠금 해제, 스마트 자동차의 운행을 강제로 제어할 수 있는 기능에 대해 관심을 가지고 있다. 그 중에서도 스마트 자동차의 블랙박스에 불법으로 접근해서 보안 위협 공격을 할 수 없도록 하고자 한다. 이를 위해서 V2X 통신 환경에서 스마트 자동차에 접근을 위한 제어 방법으로 속성 기반 권한 위임 관리기법을 활용한 안전한 스마트 자동차 제어에 대해 연구하였다.

스마트 자동차의 탑승자가 위험한 상황에 빠진 경우를 가정해 보자. 주변의 경찰(신뢰할 수 있는 제 3의 위임자)이 차량 소유자의 권한을 위임 받아서 스마트 자동차를 멈추거나 혹은 잠긴 자동차 문을 열게 할 수는 있도록 하고자 한다.

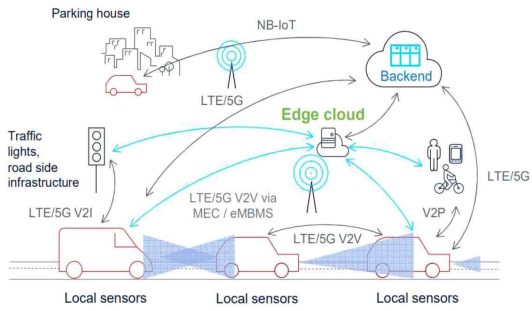
하지만 이를 악용해서 해커가 스마트 자동차에의 문을 불법으로 잠금 해제 하거나 달리고 있는 자동차의 엔진 출력을 강제로 높이거나 시동을 꺼버리는 것과 같은 위험한 행동을 막을 수 있도록 네트워크 환경을 제공해야만 한다.

본 논문의 구성은 다음과 같다. 2장은 관련 연구이다. 3장은 본 연구에서 속성 기반의 권한위임 관리 기법을 사용해서 스마트 자동차에 변조 공격 및 공모 공격이 불가능하도록 안전한 암호 통신 구조와 절차를 설명하였다. 4장은 제안한 시스템이 변조 공격 및 공모 공격에 안전하고, 기존의 속성기반 암호화만 하거나 속성기반 권한위임 가능한 암호 알고리즘과 비교하여 스마트 자동차가 보다 안전할 수 있음을 증명하였다. 마지막으로 5장은 결론을 기술하였다[9, 13].

2. 관련 연구

2.1 V2X(Vehicle to Everything) 통신환경

에지 컴퓨팅(Edge computing) 환경을 기반으로 도로에서 주행하고 있는 자동차와 다른 자동차들, 그리고 주변의 모든 인프라와 통신을 통한 차량 흐름의 제어가 가능하다. 특히, 미래의 차량은 주변의 모든 것들과 통신을 통해 신속하고, 안전하며, 편안한 운행환경을 유지할 수 있어야만 한다. 이처럼 스마트 교통망에서 자동차와 주변의 인프라 장치들의 상호 호환성을 담보하기 위해서 이동통신 표준기구인 3GPP에서는 이동통신망을 활용한 V2X 표준을 2016년에 제안하였다[2].



(그림 1) V2X(Vehicle to Everything) 환경

그리고 KT와 삼성전자, 현대자동차가 참여하고 있는 5GAA에서는 자율주행차를 위한 안전한 커넥티드-카 네트워크 환경을 제안하였다. (그림 1)은 3GPP가 제안한 스마트 교통망에서의 통신환경을 나타내고 있다.

만물 인터넷 환경에서 IEEE 802.11P를 기반으로 한 V2X에서는 스마트 자동차와 주변의 다른 자동차들, 주변 인프라들이 상호 능동적으로 통신을 하며, 자율 주행이 가능하도록 설계되었다. 이 프로토콜은 와이파이를 사용해서 스마트 자동차와 인프라 시설, 스마트 자동차와 주변의 다른 스마트 자동차들, 인프라 시설과 인프라 시설들끼리 주기적인 통신을 통해서 자율 주행 및 교통상황 제어가 가능하다.

하지만 위와 같은 V2X 통신 환경에서도 스마트 자동차 자체에 대한 신분 위조, 불법 원격 접속을 통한 공격, 주변의 자동차와 인프라들이 공모한 위 변조 공격에 대한 위험성이 여전히 다수가 존재한다.

2.2 속성기반 암호화(CP-ABE)와 속성기반 권한위임 가능 암호화(CP-ABTD)

앞서 밝힌 바와 같이, 본 논문에서는 스마트 자동차에 대한 신분 위조, 공모 공격과 같은 위협요소들을 방지하는 방법으로 속성기반 암호화와 속성기반 권한위임 기법을 사용할 수 있는 새로운 모델을 제안하고자 한다.

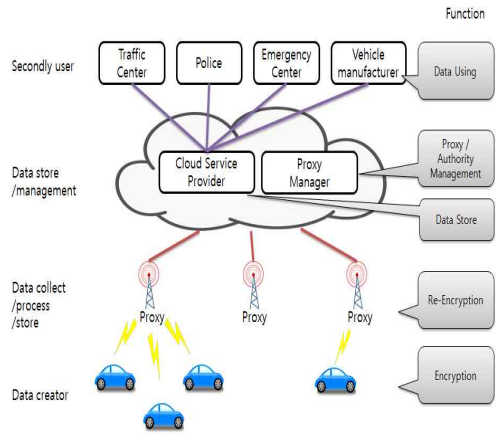
이를 위해서, 속성기반 암호화[4]에서 사용자 비밀키는 속성집합과 관련되며 암호문은 속성 접근구조와 관련이 있다. 암호문 내의 특정 복호화 정책에 대해서 사용자의 비밀키 속성집합이 만족해야만 암호문이 복호화된다. 속성기반 암호화 방식은 권한 철회와 권한 위임(Delegation)에 대해 다루지 않고 있다.

속성기반 철회 가능한 암호화[5]는 속성기반 프록시 암호화의 확장된 형태로서, 유연한 속성 위임과 동시에 속성 철회 기능을 수행할 수 있다. 이 알고리즘은 3가지 특징을 갖는다. 첫째, 속성집합과 관련된 비밀키를 가지는 권한 위임자는 피-위임자에게 자신의 권한을 위임할 수 있다. 둘째, 권한 위임자는 피-위임자에게 자신의 권한을 재-위임할 수 있도록 결정할 수 있다. 셋째, 위임했던 권한을 철회하는 권한 철회가 가능하다.

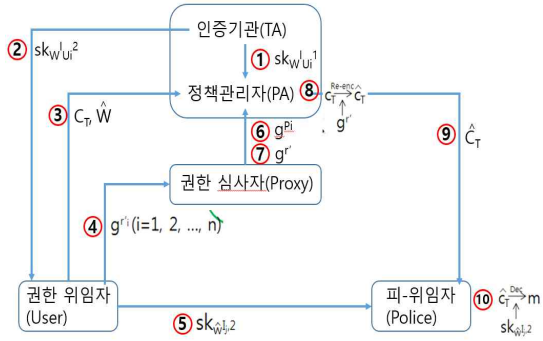
3. 제안시스템

3.1 제안시스템

(그림 2) 본 논문에서 제안하고자 하는 스마트 자동차 네트워크 모델을 나타내었다.



(그림 2) 제안시스템 네트워크 모델



(그림 3) 제안시스템 구성과 동작절차

(그림 3)은 제안시스템의 구조와 동작절차에 대해서 간략히 나타내었다. 제안시스템은 스마트 자동차에서 생성된 데이터들을 V2X에서 주변 인프라를 통해 수신받는다. 이때, 전송되는 데이터 중에서 개인정보와 같은 민감한 데이터는 기밀성 보장을 위해 암호화한다. 하지만 스마트 교통망 환경에서 스마트 인프라는 충분한 계산 및 암.복호화 자원을 보유하지 못한다는 제약사항을 갖는다.

제안시스템은 권한 위임자(User), 피-위임자(Police), 인증기관(TA: Trusted Authority), 정책 관리자(PA: Policy Administrator), 권한 심사자(Proxy)들로 구성된다. 제안시스템은 CP-ABTD를 기반으로 권한 위임자가 자신의 권한을 임의로 피-위임자에게 권한을 위임할 수 있고, 철회할 수 있도록 설계하였다.

3.2 제안시스템 동작 절차

(그림 3)에 나타낸 바와 같이 총 10단계의 동작절차를 갖도록 구성하였다. 첫 번째단계는 인증기관이 Setup을 수행하는 단계이다. 인증기관은 권한위임을 지원하기 위해서 보안 파라메터 k를 생성한다. 그리고 두 번째 단계인 KeyGen 과정을 수행하여 정책관리자, 권한위임자에게 전달한다(①, ②단계 수행). 인증기관과 정책관리자는 제3의 신뢰기관으로 하나의 행정기구로 구성할 수 있다.

권한 위임자는 전달받은 보안 파라미터와 세션키를 사용해서 정책 관리자에게 암호화를 위한 암호화 설정 값을 전달한다(③단계 수행). 그리고 네 번째로 권한 심사자(프록시)에게 랜덤값을 생성해서 전달한다(④단계 수행). 그리고 피-위임자에게 세션키를 사용해서 설정한 값을 전달한다(⑤단계 수행).

권한 심사자는 전달받은 랜덤값과 이를 기반으로 자신이 생성한 임시값을 생성해서 정책 관리자에게 확인 과정을 거친다(⑥. ⑦단계 수행).

정책 관리자는 프록시로부터 전달받은 랜덤값과 권한 위임자를 인증한 정보를 사용해서 전달한 암호화 데이터를 생성(⑧단계 수행)하고, 암호화된 데이터를 피-위임자에게 전송한다(⑨단계 수행).

마지막으로 피-위임자는 정책관리자가 권한 위임자를 대신해서 암호화해 송신한 데이터를 사전에 발급받아 둔 피-위임자를 인증할 수 있는 랜덤값을 세션키로 사용하여 복호화할 수 있다. 세부 동작과정을 8단계(Setup, KeyGen, Encrypt, Delegate, Reconstruct, m-Delegate, m-Decrypt, Decrypt)로 간소화하여 아래와 같이 나타내었다.

① Setup( ) : 보안 파라메터 k를 입력받아서 생성자 g, 소수 위수 p인 를 생성한다. bilinear map은 $e: G_0 \times G_0 \quad G_1$이고 시스템 속성 집합 $\Omega = a_1, a_2, \ldots a_n$)($n$은 정수)이며 $a_j \in \Omega$는 임의의 요소 $t_j \in Z_p^*$를 선택한다. $y = \hat{e}(g,g)^{\alpha}$ ($\alpha \in Z_p^*$, $T_j = g^t \quad 1 \quad j \quad n$)), 공개키 $pk = \hat{e}, g, y, T_j(1 \quad j \quad n)\big)$, 마스터키 $mk = \big(\alpha, t_j(1 \quad j \quad n)\big)$가 생성된다.

② KeyGen(mk, w, I_u) : 속성 집합 w와 위임자의 식별자 I_u로 비밀키를 생성한다.

(a) 비밀키의 베이스 콤포넌트를 계산 : $d_0 = g^{\alpha - u_{id}}$ ($u_{id} \in {}_R Z_p^*$)를 계산.

(b) 비밀키의 속성 콤포넌트를 계산 : 속성 $a_j \in w$, $u_j \in {}_R Z_p$를 선택하고 $d_{j,1} = g^{u_j t_j^{-1}}$와 $d_{j,2} = g^{u_{id} - u_j) t_j^{-1}}$를 계산.

첫 번째 비밀키 share $sk_{wI_w,1} = \quad a_j \in w : d_{j,1}\big)$를 PA에게 전송하고, 다음으로 두 번째 비밀키 share $sk_{w_{I_w},2} = \big(d_0, \quad a_j \in w : d_{j,2}\big)$를 위임자에

게 전송한다.

③ Encrypt($,\tau, pk)(m\in$) : $s\in Z_p^*$를 임의로 선택하고 암호문 $c_0 = g^s$, $c_1 = m\cdot y^s = m\cdot e(g,g)^{\alpha s}$를 계산한다. 접근구조 τ를 구성하는 데 root node를 s로 한다. (AND)게이트일 경우 leaf attribute를 $s_i\in Z_p^*$로 선택하고 마지막 속성값을 $s_n = s - \Sigma_{i=1}^{n-1} s_i$로 선택한다. (OR)게이트일 경우 leaf attribute를 root node의 값으로 한다. leaf attribute는 $a_{j,i}\in\tau,\ c_{j,i} = T_j^s$ 로 계산한다. 위임자의 암호문 $c_\tau = \tau, c_0, c_1, \quad a_{j,i}\in\tau : c_{j,i})$를 만들어낸다.

④ Delegate($sk_{wI_w,2}, w, I_j$) : $r'\in_R Z_p$를 선택하고 $f\ 0) = r'$인 $k-1$차 임의의 다항식을 생성한다.

$$f(x) = r' + f_1 x + f_2 x^2 + \ldots + f_{k-1} x^{k-1}$$

Proxys의 각 식별자 $ID_i(1 \quad i \quad n)$를 이용하여 $f\ ID_i) = p_i$를 계산하고 $g^{p_i} = E$를 계산한다.

$a_j\in\hat{w}$로 $g^{t_j r'} = g^{r_j''}$을 설정한다. 속성 변환키 $sk_{w\ \ w} = g^{r'}$을 설정하고 $a_j\in\hat{w}$로 $d_{j,2}$을 계산한다.

$$\widehat{d_{j,2}} = g^{u_{id} - u_j) t_j^{-1} - r'} = g^{(u_{id} - u_j) t_j^{-1} - r_j'' t_j^{-1}}$$

$$= g^{u_{id} - u_j) t_j^{-1}} \ (u_j = u_j + r_j'')$$

비밀키 share $sk_{\hat{w}I_{j'},2} = d_0, \quad a_j\in\hat{w}: \widehat{d_{j,2}})$는 피위임자에게, 속성 집합 $\hat{w}$를 PA에게 전송하고 n만큼의 속성 변환키 share g^{p_i}를 Proxys에게 전송한다.

⑤ Reconstruct($g^{p_i}(1 \quad i \quad n)$) : 속성 변환키 share g^{p_i}를 받은 임계치 k개 이상의 Proxys는 각각 k_i를 계산한다.

$$k_i = \underset{\substack{i\in \\ i\in Q_k}}{\overset{-ID_j}{\underset{j}{ID_i - ID_j}}}$$

(Q_k : k개 이상의 Proxys)

$E^{k_i} = g^{p_i})^{k_i}$를 계산한다.

k개 이상의 Proxys는 E^{k_i}를 계산하여 $sk_{w\ \ \hat{w}} = g^{r'}$를 복원한다.

$$\prod_{i\in Q_k} E^{k_i} = g^{i\in\ \ (p_i\cdot k_i)} = g^{\sum_{i\in Q_k} p_i (\prod_{i\in Q_k} \overset{ID_j}{ID_i - ID_j})} = g^{r'}$$

⑥ m−Delegate($sk_{wI_w,1}, \hat{w}, sk_{w\ \ \hat{w}}$) : 속성 위임 리스트(Attribute Delegation List)를 체크하고 속성 위임대상이라면 $a_j\in\hat{w}$로 $sk_{\hat{w}I_{j'}1}$을 계산한다. 속성 위임 리스트에 확인되지 않으면 계산은 진행되지 않는다.

$$\widehat{d_{j,1}} = g^{u_j t_j^{-1} + r'} = g^{\hat{u_j} t_j^{-1}}$$

⑦ m−Decrypt($c_\tau, sk_{\hat{w}I_{j'}1}, I_j$) : 속성 철회 리스트(Attribute Revocation List)를 체크하고 속성 철회대상이 아니라면 $\hat{c_\tau}$를 계산한다. 철회대상이라면 계산이 진행되지 않는다.

$$c_{j,i} = \prod_{a_j\in\hat{w}} \hat{e}\ T_j^{s_i}, g^{\hat{u_j} t_j^{-1}}) = \hat{e}(g,g)^{\Sigma_{a_j\in w} \hat{u_j} s_i}$$

$$\hat{c_\tau} = \left(\hat{\tau}, c_0, c_1, \quad a_{j,i}\in\hat{\tau} : \widehat{c_{j,i}}\right)$$

⑧ Decrypt($\hat{c_\tau}, sk_{\hat{w}I_{j'}2}$) :

(a) 모든 속성 $a_j\in\hat{w}$로 계산:

$$c_\tau'' = \prod_{a_j\in\hat{w}} \hat{e}\left(T_j^{s_i}, g^{(u_{id} - \hat{u_j}) t_j^{-1}}\right)$$

$$= \prod_{a_j\in\hat{w}} \hat{e}\ g^{t_j s_i}, g^{(u_{id} - \hat{u_j}) t_j^{-1}})$$

$$= \hat{e}(g,g)^{\Sigma_{a_j\in\hat{w}} (u_{id} - \hat{u_j}) s_i}$$

(b) 계산:

$$\hat{e}(c_0, d_0)\cdot\widehat{c_{j,i}}\cdot c_\tau''$$

$$= \hat{e}\ g^s, g^{\alpha - u_{id}})\cdot\hat{e}(g,g)^{\Sigma_{a_j\in\hat{w}} \hat{u_j} s_i}\cdot\hat{e}(g,g)^{\Sigma_{a_j\in\hat{w}} (u_{id} - \hat{u_j}) s_i}$$

$$= \hat{e}\left(g^s, g^{\alpha - u_{id}}\right)\cdot\hat{e}(g,g)^{u_{id} s} = \hat{e}\left(g^s, g^\alpha\right)$$

(c) m의 반환

$$= \begin{matrix} c_1 \\ e\ g\ , g^{\alpha}) \end{matrix} = \begin{matrix} m \cdot \hat{e}(g,g)^{\alpha s} \\ \hat{e}(g^{s}, g^{\alpha}) \end{matrix}$$

4. 비교 및 검토

4.1 기존 시스템과 제안시스템 비교

기존의 공개키 기반 암호화 방법이나 ID기반 암호화 기법과 비교해서 속성기반 암호화 방법은 악의적인 공모 공격으로부터 안전하다는 장점을 갖는다. 하지만 속성기반 권한 위임 가능한 암호화방법과 비교할 때, 사용자 속성의 위임과 철회 기능을 다룰 수 없다.

속성기반 권한위임이 가능한 암호화 알고리즘은 기존의 속성기반 암호화 알고리즘과 비교하여 속성을 위임하거나 철회하는 기능을 제공할 수 있다. 하지만 현실적으로 명확한 모델을 제시하지 못하고 있다. 또한, 속성 변환키의 소실이나 변조에 대해 안전하지 않기 때문에 악의적인 외부공격자의 속성 변환키 변조 공격이 가능하다는 약점을 갖는다.

그러므로, 본 논문에서는 CP-ABTD의 권한위임 기법을 기반으로 변조 공격과 공모 공격에 대해서 안전한 시스템을 제안하였다. 제안시스템은 권한위임과 철회를 위해서 권한 심사자를 통해서 정당한 접근 여부를 판별할 수 있다. 여기서, 피-위임자의 접근에 대한 정당성 판별의 의미는 동적 임계치 암호로 분할된 속성 변환키의 share를 부여받은 각 권한 심사자가 피-위임자의 신원을 파악 후 접근을 승인할 때 임계치 만큼의 share를 이용해서 원래의 속성 변환키를 생성한다.

암호화된 데이터를 열람하기 위해서 피-위임자에게 암호화된 데이터를 열람할 수 있는 권한을 위임하기 위해서 동적 임계치 암호기술을 추가로 적용하였다. 이를 통해서 권한 위임 기술만으로는 해결할 수 없는 변조 공격에 대한 문제를 해결할 수 있다.

<표 1> 제안시스템 비교

	CP-ABE	CP-ABTD	제안 방식
속성철회	×	○	○
권한위임	×	×	○
공모공격	○	○	○
변조공격	×	×	△

(○ : 우수, △ : 보통, × : 미흡)

4.2 안전성 검토

(1) 공모 공격에 대한 안전성

속성기반 권한 위임 암호화에서 마스터키를 안전하게 저장하는 TA는 전적으로 신뢰(fully trusted)하는 기관이다. Proxys(행정심사위원회)는 어느 정도 신뢰(semi-trusted)할 수 있는 기관이다. 즉, 피위임자의 비밀키 share를 만들고 재암호문을 생성하여 사용자들에게 정직하게 배부해야 한다. 하지만 평문에 대한 어떠한 정보도 알 수 없어야 한다는 점에서 신뢰할 수 없다.

여기서 공격자와 사용자(challenger)간의 보안성 게임(security game)을 통해서 속성 기반 권한위임 암호화 기법이 의미론적 안전성(semantic security)을 가짐을 알 수 있다. 의미론적 안전성이란 공격자가 암호문과 공개키를 사용해서 주어진 암호문을 만들 때 평문에 대한 어떠한 정보도 습득할 수 없음을 의미한다.

보안성 게임은 아래와 같은 요구사항을 갖는다.

- 사용자들간의 공모 공격을 방지할 수 있어야 한다. 즉, 2명 이상의 사용자가 그들의 복호권한을 확장하기 위해서 각자의 속성집합을 조합할 수 없어야 한다.

- 권한 심사자와 사용자의 공모 공격을 방지할 수 있어야 한다. 접근 정책에 만족하는 비밀키를 가지고 있지 않은 사용자와 권한 심사자가 악의적으로 협력해서 암호문을 복호화할 수 없어야

만 한다.

- 위임된 비밀키(위임자가 피-위임자를 위해 생성한 비밀키)가 안전성을 위험하게 하면 안된다. 위임된 비밀키를 이용한 인증기관의 마스터키 도출 등 위임된 비밀키에 의해서 안전성이 저해되면 안 된다.

속성기반 암호화 방식의 가장 중요한 보안 특징은 공모 공격에 대한 안전성이다. 공모 공격이란 둘이상의 사용자들이 그들의 복호 권한을 확장하기 위해서 그들의 속성집합을 조합한 것이다.

예를 들면 접근구조 $= a \quad a_2)$로 구성된 암호문이 있다. 사용자 A의 비밀키는 속성집합 $w \;=\; a_1, a_3)$로 구성되어 있고 사용자 B의 비밀키는 속성집합 $w_B = (a_2, a_4)$로 구성되어 있다. 공모 공격이란 사용자 A와 사용자 B의 비밀키를 조합하므로서 $w_A \quad w_B = (a_1, a_2, a_3, a_4)$와 관련된 비밀키를 생성하여 접근구조 $\tau = (a_1 \quad a_2)$로 구성된 암호문을 열람하는 것이다.

본 제안방식은 속성기반 권한 위임 암호화 기법이 공모공격에 대한 안전성을 기반으로 하고 있다. 속성기반 권한위임 암호화 기법은 속성집합과 관련된 비밀키를 조합하는 공모 공격에 대해 안전하다. 그 이유는 Keygen 알고리즘에서 각 사용자의 고유 식별자 u_{id}가 임의의 난수로 생성되어 비밀키에 내재되어 있기 때문이다(e.g 사용자의 비밀키 share $sk_{wI,2} = (d_0, \quad a_j \in w : d_{j,2})$, $(d_0 = g^{\alpha - u_{id}},\ d_{j,2} = g^{\ u_{id} - u_j) t_j^{-1}})$).

즉, 인증기관이 임의의 난수로 결정한 u_{id}를 각 사용자가 알 수 없으므로 공모 공격을 위해서 비밀키를 조합시킬 수 없다. 그러므로 제안시스템은 사용자들 사이의 비밀키를 조합하는 공모 공격으로부터 안전하다.

그리고 권한심사자와 사용자 사이의 공모 공격으로부터도 안전하다. 예를 들어, 사용자 B는 악의적인 권한심사자와 공모하여 사용자 A의 암호문을 자신의 암호문으로 변환하고자 한다고 가정할 때, 암호문을 변환하기 위해서 사용자 A가 사용자 B에게 접근권한을 위임하는 속성 변환키 $g^{r'}(r' \in_{R \ p})$를 생성해야 한다. 속성 변환키가 생성되지 않으면 재-암호화가 이루어지지 않는다. 그러므로 제안시스템은 권한심사자와 사용자 사이의 공모 공격에 대해서도 안전하다.

(2) 속성 변환키 share에 대한 변조 공격

속성 변환키 share에 대한 변조 공격이란 속성 변환키 share g^{p_i} 1 i $n)$가 소실 또는 변조를 통해서 원래의 속성 변환키 $g^{r'}$는 재조합할 수 없게 하는 공격을 말한다. 속성기반 권한위임 암호화 기법은 속성 변환키가 유일하므로 r'가 소실되거나 유출되거나 변조된다면 재-암호화를 수행할 수 없다. 이에 비해 제안시스템은 동적 임계치 암호로 속성 변환키 $g^{r'}$를 속성 변환키 share $g^{p_i}(1 \quad i \quad n)$로 분할하여 재-조합시 k개만큼 share가 모여야만 속성 변환키 $g^{r'}$가 구성할 수 있다. 예를 들어 $g^{p_i}(1 \quad i \quad n)$에 대해서 $n = 5,\ k = 3$이라고 할 때 g^{p_1}, g^{p_2}, g^{p_3}, g^{p_4}, g^{p_5} 중 3개의 share만 있어도 $g^{r'}$를 도출할 수 있다. 즉, k개의 share만 안전하다면 속성 변환키를 복원할 수 있다는 점에서 안전하다고 볼 수 있다.

5. 결 론

만물인터넷 시대에는 너무나 많은 센서와 주변의 장치들이 스스로 통신을 수행할 수 있는 환경이 될 것이다. 그 중에서 스마트 자동차 네트워크(V2X) 환경이 앞으로 인공지능 기술을 기반으로 자율주행 자동차와 관련해서 급속히 발전할 것으로 예상된다. 하지만 스마트 자동차의 편리함을 가질 수 있는 것과 달리, 스마트 자동차의 비밀번호를 해킹하거나 위치를 추적하거나, 스마트 자동

차 주인의 신분을 위장하여 악의적으로 사용하고자 하는 보안위협요소들도 너무나 많이 발견되고 있다. 이러한 보안위협요소들이 발생될 수 있는 문제를 해결하기 위해서 본 논문에서는 에지 컴퓨팅 환경에서 프록시(권한심사자 역할을 수행하는)에서 속성기반 권한위임 암호화 기법과 임계치 암호 기술을 혼용한 안전한 스마트 자동차 접근제어 시스템을 제안하였다.

제안시스템은 스마트 자동차의 정보 유출을 고려하여 암호화된 데이터를 전송할 수 있다. 그리고 신뢰할 수 있는 권한 심사자와 정책관리자, 인증기관으로 구성된 시스템에서 피-위임자(경찰)는 특정 차량에 대한 정보를 재-암호화해서 전달 받은 후, 이를 복호화하여 운전자(사용자, 정보 생성자)를 대신해서 자동차를 열거나, 멈추거나 하는 것이 가능하도록 하고자 하였다.

본 논문에서는 속성기반 권한위임 기법과 임계치 암호화 기술을 사용하여 에지 컴퓨팅 환경을 기반으로 한 스마트 자동차 네트워크(V2X)에서 악의적인 사용자의 공모 공격에 대한 안전성을 가질수 있음을 보였다. 그리고 속성 변환키 share에 대한 변조 공격에 대한 안전성을 보였다. 하지만 본 연구를 수행하면서 알게 된 새로운 점은 제안 시스템에서 속성 철회가 발생할 때마다 재-암호화키를 생성해야 하는 문제로 인해 계산상의 부하가 걸리는 단점이 있다는 점이다.

향후 IEEE 802.11P 기반의 와이파이 환경에서 좀 더 다양한 시뮬레이션을 수행하여 위에서 새롭게 발견된 단점을 보완할 방법을 찾고자 시도하고자 한다.

참고문헌

[1] Maruyama Hiroshi, "Edge-Heavy Data and architecture in the big data era, Journal of Information Processing and Management, 2013, 56.5:269-275

[2] 한상기, 윤대균, 김태진, 이민석, 클라우드 이슈레포트(엣지 컴퓨팅과 인공지능) Vol.4, 한국정보화진흥원, April 2019.

[3] P. Robinson, H. Vogt and W. Wagealla, "Privacy, Security, and Trust Within the Context of Pervasive Computing," Springer-Verlag, ISBN 0387234616, 2005.

[4] J. Bethencourt, A. Sahai and B, Waters, "Ciphertext-Policy Attribute-Based Encryption," Proceedings of the 2007 IEEE Symposium on Security and Privacy, pp.321-334, 2007.

[5] L. Ibraimi, M. Petkovic, S. Nikova1, P. Hartel and W. Jonker, "Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes," 2009 University of Twente, Centre for Telematics and Information Technology, Internal Report, 2009.

[6] M. Jakobsson, "On Quorum Controlled Asymmetric Proxy Re-encryption," Lecture notes in computer science; Vol. 1560, Springer-Verlag, pp.112-121, 1999.

[7] HONG, Kirak, et al. Mobile fog: A programming model for large-scale applications on the internet of things. In: Proceedings of the second ACM SIGCOMM workshop on Mobile cloud computing. ACM, 2013. p. 15-20.

[8] BLAZE, Matt; BLEUMER, Gerrit; STRAUSS, Martin. Divertible protocols and atomic proxy cryptography. In: Advances in Cryptology—EUROCRYPT'98. Springer Berlin Heidelberg, 1998. p. 127-144.

[9] MAMBO, Masahiro; OKAMOTO, Eiji. Proxy cryptosystems: Delegation of the power to decrypt ciphertexts. IEICE transactions on fundamentals of electronics, Communications and computer sciences, 1997, 80.1: 54-63.

[10] ROY, Sandip; BOSE, Rajesh; SARDDAR, Debabrata. A Fog-Based DSS Model for Driving Rule Violation Monitoring Framework

on the Internet of Things. International Journal of Advanced Science and Technology, 2015, 82: 23-32.

[11] You-Jin Song, Jin-Mook Kim, Characterization of privacy based on context sensitivity and user preference for multimedia context-aware on IoT, Multimedia Tools and Applications, https://doi.org/10.1007/s11042-018-6103-5, 2018.

[12] Hyung-Jong Cha, Ho-Kyung Yang, Jin-Mook Kim, You-Jin Song, A Study on Data Processing for Application of Vehicular CPS in Fog Computing Environment, Advanced Science Letters, Vol. 23, No. 10, pp. 10379-10383, 2017.

[13] 김진묵, 문정경, 황득영, 스마트 자동차 네트워크의 보안 취약점 분석 및 해결방안 마련, 융합보안논문지 제18권 제3호, pp.69-76, 2018.09.

〔저자소개〕

김 진 묵 (Jin-Mook Kim)
1998년 2월 : 배재대학교 전자계산학과(이학사)
2000년 2월 : 배재대학교 컴퓨터공학과(공학석사)
2006년 2월 : 광운대학교 컴퓨터과학과(공학박사)
2006년 9월 ~ 2008년 2월 : 선문대학교 컴퓨터공학과 연구교수
2008년 3월 ~ 현재 : 선문대학교 IT교육학부 부교수

관심분야 : 정보보호, 네트워크 보안, 사용자 인증, 빅-데이터 분석, 인공지능, 스마트 자동차
E-Mail : calf0425@sunmoon.ac.kr

문 정 경(Jeong-Kyung Moon)
1993년 2월 : 배재대학교 원예학과(학사)
2006년 2월 : 단국대학교 인터넷정보학과(공학석사)
2013년 2월 : 공주대학교 컴퓨터공학과(공학박사)
2012년 3월 ~ 2월 : 선문대학교 IT교육학부 계약교수
2018년 3월 ~ 현재 : 가천대학교 소프트웨어중심대학 초빙교수

관심분야 : 에지 컴퓨팅, 정보보안, 빅데이터 분석, 인공지능, 스마트 자동차
E-mail : jkmoon@gachon.ac.kr

황 득 영 (Deuk-Young Hwang)
1988년 2월 : 광운대학교 전자계산학과(이학사)
1990년 2월 : 광운대학교 전자계산학과(공학석사)
1999년 2월 : 광운대학교 전자계산학과 (공학박사)
1990년 3월 ~ 1994년 2월 : 전주 기전대학교 전자계산학과 조교수
1994년 3월 ~ 현재 : 강원대학교 삼척캠퍼스 컴퓨터공학과 교수

관심분야 : 프로그래밍 언어, 컴파일러, 정보보안, 빅-데이터 분석, 소프트웨어 공학
E-mail : dyhwang@kangwon.ac.kr