열쇠속성을 고려한 PKCS#11표준의 형식적모형

김진성, 김종학

우리는 공개열쇠암호화표준의 한가지인 PKCS#11의 형식적모형에 대하여 연구하였다.

선행연구[1]에서는 항대수와 규칙기반서술언어로 PKCS#11에 대한 형식적모형을 처음으로 제기하였지만 PKCS#11의 안전성에 대한 결과는 주지 못하였다. 선행연구[2]에서는 FOLTL모형에 의해 PKCS#11이 안전한것으로 되기 위한 한가지 충분조건을 밝혔지만 관리자를 신뢰하는 조건에서만 안전하다는 문제가 있으며 선행연구[3]에서는 열쇠의 자료만을 고찰했기때문에 열쇠의 속성을 함께 반출하는 경우의 안전성은 론의할수 없다.

론문에서는 열쇠속성을 함께 반출하는 경우의 안전성도 고찰할수 있는 새로운 형식적모형을 제기하고 그것에 기초하여 PKCS#11의 안전성에 대하여 연구하였다.

1. 열쇠속성을 고려한 형식적모형

론문에서 견본(Template)은 선행연구[3]에서의 정의를 그대로 리용하며 값(Value)은 아래와 같은 문법으로 정의한다.

$$v ::= val \mid venc(v,\ v') \mid vdec(v,\ v') \mid v;T\ ,\ \ val \in \boldsymbol{V}\ ,\ \ T \in \boldsymbol{T}$$

여기서 T는 견본, $\boldsymbol{V}$는 원자 상수 및 새로운 값들의 모임, $v;T$는 열쇠자료와 속성자료를 결합한것을 의미한다.

열쇠속성을 고려하기 위하여 값과 견본의 쌍으로 이루어진 대상(Subject)의 개념을 새로 도입한다.

$$sub = (val,\ T)\ ,\ \ val \in \boldsymbol{V}\ ,\ \ T \in \boldsymbol{T}$$

sub를 원자값대상이라고 부르고 대상 s는 아래의 문법으로 정의한다.

$$s ::= sub \mid enc(s,\ s') \mid dec(s,\ s')$$

여기서 $enc(s,\ s') = (venc(v;T,\ v'),\ \phi)$, $dec(s,\ s') = \begin{cases} (v'',\ T''), & s = (venc(v'';T''),\ \phi) \\ (vdec(v,\ v'),\ \phi), & s \neq (venc(v'';T''),\ \phi) \end{cases}$ 이다.

우에서 정의한 대상을 리용하여 식과 기억, API함수, 공격자모형, API안전성을 선행연구[3]와 동일한 방법으로 정의할수 있다.

2. 형체계를 리용한 안전성해석

형에 기초한 안전성해석방법은 보안API들에서의 암호학적연산들에 대한 정보흐름속성을 분석하기 위하여 제안되였다.[3]

식과 명령들의 형을 결정하기 위하여 형결정환경 Γ를 다음과 같이 도입한다.

$$\Gamma : x \mapsto \tau\ (x\text{:변수},\ \tau\text{:형})$$

환경 Γ에서 식 e의 형이 τ로 된다는것을 $\Gamma \perp e : \tau$로 표시한다.

$\Gamma \perp e:\tau$는 다음의 규칙에 의하여 결정된다.

$$[var]\frac{\Gamma(x)=\tau}{\Gamma \perp x:\tau},\ [sub]\frac{\Gamma \perp e:\tau'\ \ \tau\le\tau'}{\Gamma \perp e:\tau}$$

$$[enc]\frac{\Gamma \perp x:\mathrm{Data}\ \ \Gamma \perp e:\mathrm{Un}}{\Gamma \perp \mathrm{enc}(e,\ x):\mathrm{Un}},\ [dec]\frac{\Gamma \perp x:\mathrm{Data}\ \ \Gamma \perp e:\mathrm{Un}}{\Gamma \perp \mathrm{dec}(e,\ x):\mathrm{Un}}$$

$$[wrap]\frac{\Gamma \perp x:\mathrm{Wrap}\ \ \Gamma \perp e:\mathrm{Any}}{\Gamma \perp \mathrm{enc}(e,\ x):\mathrm{Un}},\ [unwrap]\frac{\Gamma \perp x:\mathrm{Wrap}\ \ \Gamma \perp e:\mathrm{Un}}{\Gamma \perp \mathrm{dec}(e,\ x):\mathrm{Any}}$$

$$[enc-any]\frac{\Gamma \perp x:\mathrm{Any}\ \ \Gamma \perp e:\mathrm{Un}}{\Gamma \perp \mathrm{enc}(e,\ x):\mathrm{Un}},\ [dec-any]\frac{\Gamma \perp x:\mathrm{Any}\ \ \Gamma \perp e:\mathrm{Un}}{\Gamma \perp \mathrm{dec}(e,\ x):\mathrm{Any}}$$

다음으로 API의 형을 결정하자.

환경 Γ와 방책 $\boldsymbol{T}$에서 명령 c가 형완정성을 가진다는것을 $\Gamma \perp_{\boldsymbol{T}} \mathrm{c}$로 표시하며 다음의 규칙에 의하여 판단한다.

$$[\mathrm{API}]\frac{\forall a\in \mathrm{A}\ \ \Gamma \perp_{\boldsymbol{T}} \mathrm{a}}{\Gamma \perp_{\boldsymbol{T}} \mathrm{A}},\ [assign]\frac{\Gamma(x)=\tau\ \ \Gamma \perp e:\tau}{\Gamma \perp_{\boldsymbol{T}} x:=e}$$

$$[seq]\frac{\Gamma \perp_{\boldsymbol{T}} \mathrm{c}_1\ \ \Gamma \perp_{\boldsymbol{T}} \mathrm{c}_2}{\Gamma \perp_{\boldsymbol{T}} \mathrm{c}_1;\mathrm{c}_2},\ [getobj]\frac{\Gamma(x)=\mathrm{Any}\ \ \Gamma \perp y:\mathrm{Un}}{\Gamma \perp_{\boldsymbol{T}} x:=\mathrm{getobj}(y)}$$

$$[checktmp]\frac{\Gamma(x)=\mathrm{LUB}(T,\ \boldsymbol{T})\ \ \Gamma \perp y:\mathrm{Un}}{\Gamma \perp_{\boldsymbol{T}} x:=\mathrm{checkTemplate}(y,\ T)},\ [genkey]\frac{\Gamma(x)=\mathrm{Un}\ \ T\in\boldsymbol{T}}{\Gamma \perp_{\boldsymbol{T}} x:=\mathrm{genkey}(T)}$$

$$[impkey]\frac{\Gamma(x)=\mathrm{Un}\ \ \Gamma \perp y:\tau\ \ \mathrm{Attr}(y)=T\ \ \perp T:\tau}{\Gamma \perp_{\boldsymbol{T}} x:=\mathrm{importkey}(y)}$$

$$[return]\frac{\Gamma \perp e:\mathrm{Un}}{\Gamma \perp_{\boldsymbol{T}} return},\ [function]\frac{\Gamma \perp x_1:\mathrm{Un}\ \cdots \Gamma \perp x_k:\mathrm{Un}\ \ \Gamma \perp_{\boldsymbol{T}} \mathrm{c}}{\Gamma \perp_{\boldsymbol{T}} \lambda x_1,\ \cdots,\ x_k \mathrm{c}}$$

$\mathrm{LUB}(T,\ \boldsymbol{T})$는 $T\subseteq T'$인 견본 T'들에 대한 모든 형들의 최소웃경계를 나타낸다. 즉

$$\mathrm{LUB}(T,\ \boldsymbol{T})=\bigcup\{\tau' \mid \exists T'\in\boldsymbol{T},\ T\subseteq T'\wedge \perp T':\tau'\}$$

넘기기 $\theta:sub\mapsto\rho$가 주어졌다고 하자. 여기서 sub는 원자값대상, ρ는 형이다.

θ에 의하여 대상이 형식완정성을 가진다는것은 식의 형결정규칙과 동일한 규칙들로 판단한다.

보조정리 1 $\theta \perp_{\boldsymbol{T}} \mathrm{H}$이고 S는 원자값대상들의 모임이며 $sub\in S\Rightarrow\theta(sub)=\mathrm{Un}$이라고 할 때 $s\in \mathrm{K}(S)\Rightarrow\theta \perp s:\mathrm{Un}$이다.

보조정리 2 $\Gamma \perp e:\tau$, $e\downarrow^{\mathrm{M}} s$라고 하면 $\Gamma,\ \theta \perp_{\boldsymbol{T}} \mathrm{M}\Rightarrow\theta \perp s:\tau$이다.

이 보조정리들은 공격자지식 $\mathrm{K}(S)$와 식 e의 구조에 관한 귀납법으로 증명할수 있다.

다음의 정리는 형완정성을 가지는 API함수는 실행시에 형완정성을 보존하며 기억과 손잡이지도는 형식완정성을 그대로 보존한다는것을 보여준다.

정리 1 $\Gamma,\ \theta \perp_{\boldsymbol{T}} \mathrm{M},\ \mathrm{H}$이고 $\Gamma \perp_{\boldsymbol{T}} \mathrm{c}$라고 할 때 $\langle \mathrm{M},\ \mathrm{H},\ \mathrm{c}\rangle \to \langle \mathrm{M}',\ \mathrm{H}',\ \mathrm{c}'\rangle$이면 다음의 결과들이 성립된다.

① $\mathrm{c}'\ne\varepsilon\Rightarrow\Gamma \perp_{\boldsymbol{T}} \mathrm{c}'$

② $\exists\theta'\supseteq\theta\,\Gamma,\ \theta' \perp_{\boldsymbol{T}} \mathrm{M}',\ \mathrm{H}'$

다음의 정리는 형완정성을 가지는 API는 안전하다는것을 보여준다.

정리 2 $\Gamma \perp_{\boldsymbol{T}} \mathrm{A}$이면 API A는 안전하다.

증명 먼저 $\langle \mathrm{H}_0,\ S_0\rangle \to^{*}_{\mathrm{A}} \langle \mathrm{H},\ S\rangle$일 때

$$\exists\theta,\ \theta \perp_{\boldsymbol{T}} \mathrm{H},\ \forall s \in S,\ \theta \perp s : \mathrm{Un} \tag{1}$$

임을 증명한다. 이것은 보조정리들과 변환의 길이에 관한 귀납법으로 증명할수 있다.

다음 API안전성에 대한 정의인 식 (1)이 성립된다는것을 증명하자.

$sub \notin \mathrm{K}(S)$, $sub : \mathrm{H}$ 에서 기밀대상이므로 $\widetilde{\theta} = \theta[sub \mapsto \mathrm{Data}]$ 로 정의하면 $\widetilde{\theta}$ 에 대해서도 식 (1)이 그대로 성립된다.

변환 $\langle \mathrm{H},\ S\rangle \to^{*}_{\mathrm{A}} \langle \mathrm{H}',\ S'\rangle$ 에 대하여 식 (1)의 증명과 같은 론의를 적용하면

$$\exists\theta' \supseteq \widetilde{\theta},\ \theta' \perp_{\mathrm{T}} \mathrm{H}',\ \forall s \in S',\ \theta' \perp s : \mathrm{Un} \tag{2}$$

$\theta'(sub) = \widetilde{\theta}(sub) = \mathrm{Data}$ 이므로 $\theta' \not\perp sub : \mathrm{Un}$ 이고 보조정리 1로부터 $sub \notin \mathrm{K}(S')$ 이므로 API안전성에 대한 정의인 식 (2)도 성립된다.

H 에서 신뢰할수 있는 대상인 sub 가 가질수 있는 형은 Wrap, TData, Seed뿐이다.

따라서 $\theta \perp sub : \mathrm{Un}$ 과 보조정리 1로부터 $sub \notin \mathrm{K}(S)$ 이고 $A \in T \Rightarrow S \in T$ 이므로 $sub \notin \mathrm{K}(S')$ 이다. 따라서 $sub \notin \mathrm{K}(S) \bigcup \mathrm{K}(S')$ 이다.(증명끝)

3. PKCS#11의 안전성고찰

우에서 정의한 형식적모형에 기초하여 PKCS#11의 안전성에 대하여 고찰하자.

보안방책 $\boldsymbol{T}$ 가 아래의 조건을 만족시킨다고 하자.

$$T \in \boldsymbol{T},\ \{W\} \in T \Rightarrow T = \{A,\ S,\ W,\ U\},\ \{D\} \in T \Rightarrow T = \{S,\ E,\ D\}$$

이 조건을 만족시키는 $\boldsymbol{T}$ 에서의 형결정환경 Γ 를 $\Gamma(Data) = \mathrm{Un}$, $\Gamma(h\_key) = \mathrm{Un}$ 로 정의하면 C_Encrypt, C_Decrypt, C_WrapKey, C_UnwrapKey함수들이 형완정성을 가진다는것을 알수 있다. 이 4개 함수가 모두 형완정성을 가지므로 API의 형결정규칙 [API]에 의해 이 함수들로 이루어진 API는 형완정성을 가지며 정리 2로부터 API는 안전하다.

참 고 문 헌

[1] S. Delaune et al.; In Proceedings of the 21st IEEE Computer Security Foundations Symposium, IEEE Computer Society Press, 331～344, 2008.

[2] S. B. Fröschle et al.; Lecture Notes in Computer Science, Springer, 34～78, 2011.

[3] M. Centenaro et al.; Type-Based Analysis of PKCS#11 Key Management, DAIS, 122～156, 2012.

주체106(2017)년 12월 5일 원고접수

A Formal Model for PKCS#11 Standard Considering Key Attributes

Kim Jin Song, Kim Jong Hak

We suggested a new formal model which takes account of key attributes for PKCS#11 standard, which could consider a security even in case of exporting key attributes with key values and showed a sufficient condition for security of PKCS#11.

Key words: PKCS#11, key attribute