김일성종합대학학보
(자연과학)
주체106(2017)년 제63권 제2호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 63 No. 2 JUCHE106(2017).

PKCS#11통표에서 외부열쇠반입때 열쇠검증의 한가지 방법

김진성, 리명철, 김종학

경애하는 최고령도자 **김정은**동지께서는 다음과 같이 말씀하시였다.

《과학기술부문에서 첨단돌파전을 힘있게 벌려야 하겠습니다.》(《조선로동당 제7차대회에서 한 중앙위원회사업총화보고》 단행본 39페지)

PKCS#11규약의 보안취약점들중 외부열쇠반입에 의한 취약점은 반출열쇠자료의 해쉬값을 리용하여 해결되고있으나 이것은 해쉬알고리듬들이 공개되여있기때문에 쉽게 해쉬값을 계산하여 공격할수 있는 가능성이 있다.[1]

론문에서는 암호화된 외부열쇠자료의 서명 및 검증을 리용하는 안전한 외부열쇠반입방법을 제안한다.

1. PKCS#11규약의 개념과 용어정의

PKCS(Public Key Cryptography Standards)는 공개열쇠암호화표준들의 집합이며 그중 PKCS#11은 응용프로그람과 암호학적장치(지능카드, USB열쇠통표 등)들사이의 대면부인 암호학적API(Application Programming Interface)에 대한 표준이다.[2]

PKCS#11의 취약점들을 리용한 여러가지 공격방법들이 알려지면서 이것들을 막기 위한 갱신된 판본들이 계속 나오고있다. 그중에서도 장치외부로부터 반입되는 열쇠와 관련되는 취약점들은 목적장치에서의 API호출권한을 획득하지 않고도 쉽게 공격할수 있는것으로 하여 많이 론의되고있다.[2]

론문에서는 외부열쇠반입에 의한 취약점들과 그것에 대한 해결방안들을 분석하고 검증된 열쇠들만을 반입할수 있는 한가지 방법을 제안한다.

서술을 위하여 다음의 용어들을 약속한다.

통표(Token): PKCS#11규약을 구현한 암호학적장치(PKCS#11통표라고도 함)

비공개열쇠(Pvk): 공개열쇠암호(비대칭열쇠암호)에서의 비공개열쇠

공개열쇠(Puk): 공개열쇠암호(비대칭열쇠암호)에서의 공개열쇠

비밀열쇠(Sek): 대칭열쇠암호에서의 열쇠

enc(·), dec(·): 암호화 및 복호화

열쇠반출함수: PKCS#11규약의 C_WrapKey함수

열쇠반입함수: PKCS#11규약의 C_UnwrapKey함수

T: 암호화된 외부열쇠(Wrapped Key)

KEK (Key Encrypting Key): 열쇠를 암호화하는 열쇠(Wrapping Key)

MK(Master Key): 기본열쇠(Master Key)

2. 외부열쇠반입에 의한 취약점들과 해결방법들

PKCS#11은 통표와 응용프로그람사이 또는 서로 다른 통표들사이에서 열쇠자료를 안전하게 주고받기 위하여 열쇠반출함수와 열쇠반입함수를 정의하고있다.

통표안의 열쇠들은 열쇠반출함수를 통하여 암호화된 상태로 송신자통표의 밖으로 반출되게 되며 열쇠반입함수를 통하여 수신자통표안에서 복호화되여 반입되게 된다.

공격자는 외부에 공개되는 암호화된 열쇠자료를 리용하여 복호화된 열쇠자료를 얻거나 통표안의 다른 열쇠들의 값을 알아내려고 한다.

이제 공격자의 몇가지 공격방법에 대하여 론의하자.

공격 1(비법열쇠생성 Key Conjuring) 비법열쇠생성은 통표안에 승인되지 않은 열쇠를 발생시키는 수법을 의미한다. 이것은 사용자가 우연발생한 자료 R를 리용하여 열쇠반입함수를 호출하는 방법으로 가능하다. 즉 $T_{random} = R$ 를 열쇠반입함수에 파라메터로 제공함으로써 $K_{random} = dec_{MK}(T_{random})$ 이라는 우연열쇠가 통표안에 생성되게 되는것이다.

이 수법은 통표사용자의 열쇠발생방책(실례로 암호화알고리듬이나 열쇠길이에 대한 제한)을 무시할수 있으며 또한 대량의 열쇠들을 발생하여 병렬열쇠탐색에 리용할수 있다는데 위험성이 있다.[1]

공격 2(열쇠묶음 Key Binding) 2중길이열쇠 $K = \langle K_1, K_2 \rangle$ 의 외부반출때 K_1, K_2 가 각각 독립적으로 암호화되는 경우(실례로 ECB방식의 암호화) K_1, K_2 를 각각 개별적인 열쇠로 통표안에 넣을수 있다.

$$T = enc(K) = enc_{KEK}(\langle K_1, K_2 \rangle) = \langle enc_{KEK}(K_1), enc_{KEK}(K_2) \rangle = \langle T_1, T_2 \rangle$$
$$dec_{KEK}(T_1) = dec_{KEK}(enc_{KEK}(K_1)) = K_1 \quad (T_1 \text{에 대한 열쇠반입함수호출})$$
$$dec_{KEK}(T_2) = dec_{KEK}(enc_{KEK}(K_2)) = K_2 \quad (T_2 \text{에 대한 열쇠반입함수호출})$$

결과적으로는 절반길이의 암호화열쇠에 대한 탐색공격만으로도 전체 암호화열쇠를 알수 있게 된다.[2]

공격 3(트로이동봉열쇠 Trojan Wrapped Key) 통표안에 비공개열쇠 $\langle d, n \rangle$ 이 있고 공격자가 공개열쇠 $\langle e, n \rangle$ 을 알고있다고 하자.

이때 공격자는 자신이 알고있는 임의의 열쇠 K 를 통표안에 넣을수 있다. 즉 알려진 공개열쇠를 리용하여 $T = K^e \bmod n$ 을 계산한 후 T 를 열쇠반입함수의 파라메터로 제공함으로써 $T^d \bmod n = (K^e)^d = K$ 가 새로운 암호화열쇠로 통표안에 생성되게 한다. 공격자는 K 를 KEK 로 리용하여 다른 암호화열쇠들을 암호화된 형태로 반출한 후 복호화하여 열쇠값을 알아낼수 있게 된다.

우의 3가지 공격방법들은 모두 외부로의 반출 또는 반입때 암호화된 열쇠자료에 대한 검증을 할수 있는 기능이 없는데로부터 발생하는것들이다.

이에 대한 대책방법으로서 암호화된 열쇠자료에 대한 해쉬값을 리용하는 방법이 제안되였지만 이 방법도 해쉬알고리듬이 공개되여있고 해쉬값계산이 어렵지 않은 조건에서 직접 해쉬값을 계산하여 공격하는것은 막을수 없다.

3. 서명자료에 의한 외부반입열쇠검증방법과 그 안전성

론문에서는 해쉬값대신 서명자료를 리용하여 암호화된 열쇠자료를 검증하는 방법을 제안한다. 이 방법은 신뢰할수 있는 증명기관으로부터 통표별로 통표증명서를 발급받아 통표안에 보관하고 암호화된 열쇠자료의 서명에 리용함으로써 외부열쇠자료가 신뢰할수 있는 통표로부터 반출된것이며 외부열쇠자료가 변조되지 않았음을 확인할수 있도록 해준다.

제안하는 알고리듬은 다음과 같다.

1) 통표증명서 발급단계

① 통표별로 통표의 PKCS#11암호생성함수를 리용하여 공개열쇠암호쌍 (Pvk, Puk)을 생성한다.

② 생성된 공개열쇠 Puk 를 신뢰할수 있는 증명기관에 제출하여 통표증명서 C 를 발급받는다.

③ 통표안에 발급받은 통표증명서 C 와 증명기관의 증명서 C_{Root} 를 함께 보관한다.

④ 통표증명서발급은 통표의 배포전에 한번만 진행하면 충분하다.

2) 외부열쇠 반출 및 반입

① 송신자는 K 의 암호문 T 와 함께 T 를 통표의 비공개열쇠 Pvk 로 서명한 자료, 통표증명서를 보낸다.

열쇠반출함수는 $K \rightarrow \langle T,\ S,\ C_s \rangle$ 이다. 여기서 $S = sign(T,\ Pvk)$, C_s: 송신통표증명서.

② 수신자는 서명자료와 통표증명서의 검증에 성공한 경우에만 열쇠를 반입한다.

열쇠반입함수 C_s 에 포함된 Puk 로 T 의 서명 S 를 검증하고 수신자통표에 보관된 C_{Root} 를 리용하여 C_s 의 유효성을 검증한다.

③ 검증에 성공한 경우 암호화된 열쇠 T 는 정당한 통표로부터 반출된 열쇠임을 확신할수 있다.

우의 알고리듬에서 공격자가 C, C_{Root} 를 교체하려고 시도할수 있기때문에 이 증명서들은 PKCS#11 API로는 접근할수 없도록 하여야 하며 통표를 배포하기 전에 전용의 프로그람을 리용하여 통표안에 넣어주어야 한다. 만일 통표증명서를 갱신하는 경우에는 통표안의 다른 열쇠자료들은 모두 자동적으로 초기화되도록 하는것이 안전하다. 그것은 공격자가 전용의 프로그람을 악용하여 C, C_{Root} 를 자신이 만든 증명서들로 교체하고 통표안의 열쇠자료들을 얻어내는것을 방지하기 위해서이다.

통표증명서의 검증때 증명서의 유효사용기간도 검사하여야 하며 통표증명서는 유효기간내에 다시 발급받아야 한다.

공격자가 우의 알고리듬을 구현한 통표에 대해서 변조된 열쇠자료를 통표안에 넣는것은 원리적으로 불가능하다. 그것은 열쇠자료의 서명에 리용된 비공개열쇠 Pvk 는 하드웨어적으로 통표안에서 생성되여 통표밖으로는 나올수 없고 통표안에서만 리용되기때문이며 또한 서명확인에 리용되는 C, C_{Root} 도 우와 같은 리유로 하여 교체가 불가능하기때문이다.

변조된 열쇠자료를 통표안에 넣는것이 불가능해진 결과 공격 1, 2, 3을 효과적으로 막을수 있게 된다. 그것은 공격 1, 3에서는 공격자가 열쇠암호문을 만들어도 그것을 서명

할수 없기때문에 알고리듬의 2) ②의 열쇠자료서명검증에서 실패하게 되기때문이다.

만일 공격자의 증명서로 서명하는 경우에는 알고리듬의 2) ②의 증명서확인에서 실패하게 된다.

공격 2는 열쇠암호문을 변조하여 통표안에 넣는것이기때문에 알고리듬의 2) ②의 열쇠자료서명검증에 실패하며 열쇠반입에서도 실패하게 된다. 즉 론문에서 제안한 이 방법은 해쉬값에 의하여 반출열쇠자료의 변조여부만을 검사하던 선행방법에 비해 변조여부와 함께 반출통표에 대한 반출자확인까지 가능하게 하는 방법으로서 통표증명서를 교체하지 않고는 비법적으로 열쇠자료들을 얻을수 없게 한다.

참 고 문 헌

[1] M. Bond et al.; Computer, **34**, **10**, 67, 2001.

[2] R. Focardi et al.; LNCS, **35**, 6858, 2011.

주체105(2016)년 10월 5일 원고접수

A Method of Checking Key for Importing the External Key in PKCS#11 Token

Kim Jin Song, Ri Myong Chol and *Kim Jong Hak*

We studied a new method for importing the wrapped key, which is able to check if the wrapped key has been changed and identified the exporting token by signing and verification of wrapped key.

Key words: wrapped key, sign, verification