INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA

Institut National de Recherche en Informatique et en Automatique

Concours externe d'Ingénieur de Recherche
Ouvert au titre de l'année 2011

Concours n° TI2
«Responsable des partenariats et projets d'innovation»

Épreuve écrite d'admission du 16 juin 2011

Durée 3 heures
(Coefficient 3)

La notation prendra en compte la qualité des réponses, mais aussi, la présentation, le style et l'orthographe.

Veillez à respecter l'anonymat dans les réponses.
Ne pas omettre de noter votre numéro d'ordre sur les feuilles intercalaires.
Usage de la calculatrice non autorisé.

Concours Nancy

Question 1 (5 points)

Ecrivez un mémo pour votre directeur de centre synthétisant le paysage régional d'innovation (rôles et articulation des pôles de compétitivité, OSEO, etc.). Précisez notamment l'évolution à attendre dans le cadre de la mise en place des instruments du "Grand emprunt" (Programme Investissements d'Avenir: SATT, IRT, IEED, etc.). Donnez des éléments de positionnement de l'INRIA dans ce contexte et les implications pour sa politique de partenariats industriels et de transfert.

Question 2 (10 points) - Cas d'étude

Vous êtes chargé des partenariats et des projets d'innovation à l'INRIA. Un chercheur INRIA d'une équipe projet INRIA CPATOU vous a envoyé un courriel car il a été contacté par plusieurs industriels suite à une conférence scientifique où il a divulgué ses résultats de recherche. Il souhaite licencier son logiciel le plus rapidement possible à ses nouveaux contacts et vous presse de lui fournir un cadre contractuel. Dans son courriel, il vous indique un lien sur une page web qu'il a réalisée et dont le contenu est dans l'annexe jointe à votre sujet.
Vous lui proposez de le rencontrer et dans cette attente, vous allez préparer votre entretien.

Vous connaissez déjà en partie l'offre technologique de ce chercheur puisque quelques mois plus tôt vous l'avez rencontré dans le cadre d'une rencontre avec l'EPI CPATOU et tous ses membres et vous aviez identifié le logiciel mkCPAT. Avec le chercheur, seul auteur du code, vous aviez procédé facilement au dépôt à l'APP de ces codes et également établi le choix d'exploiter le logiciel en mode propriétaire. Plusieurs mois se sont donc écoulés et maintenant :

Le nouveau logiciel s'appelle TCA, son noyau est composé de mkCPAT. Le logiciel TCA est issu d'un travail dans le cadre d'une collaboration informelle avec le professeur WellDone d'une université européenne.

PKCS#11 est un standard RSA qui spécifie une API pour des opérations de cryptographie telles que l'encryption et la signature. Les attaques exploitent les vulnérabilités de l'interface de gestion des clés cryptographiques PKCS#11, le logiciel TCA permet de découvrir ces attaques. TCA utilise des méthodes formelles en contrant automatiquement un modèle de la fonctionnalité d'une pièce de matériel : il trouve une attaque dans le modèle et puis exécute l'attaque directement sur l'appareil.

Plusieurs contacts ont été établis avec le chercheur INRIA et des constructeurs de l'aéronautique et également des acteurs dans le secteur de la finance. En particulier, la banque Cdelaure souhaite tester ses smart-cards, et souhaite monter une réunion d'échange dans un mois. Une société aéronautique Cdanlair souhaite directement avoir une licence de ce logiciel.

(a) Vous vous attacherez en premier lieu à regarder l'état du code de TCA, le nouveau logiciel.
Quels sont les différents éléments et les étapes qui permettront de comprendre les liens entre TCA et mkCPAT ?

(b) En parallèle, vous regarderez les aspects éthiques relatifs aux applications de ce nouveau logiciel TCA :

- Le professeur WellDone souhaite utiliser ce logiciel auprès de ses étudiants. La question de la diffusion au monde académique se pose d'une manière générale. Vous essaierez de donner des solutions permettant de mettre à disposition un système de ce type pour l'enseignement,

avec un niveau de contrôle et de sécurité suffisant.

- Le chercheur INRIA souhaite une couverture médiatique en lien avec la conférence scientifique de grande envergure qu'il va bientôt donner, où d'autres résultats seront dévoilés sur les attaques de son logiciel portant sur des composants du commerce.

(c) De cette première ébauche d'analyse, vous extrairez : les choix de licences pour TCA, en expliquant leurs avantages et leurs inconvénients. Vous commencerez à fournir des pistes possibles ou bien des pistes à éliminer en vous basant sur les éléments que vous avez pour le moment en votre possession.

(d) Vous rédigerez un texte court destiné à dresser une première ébauche de collaboration avec la banque Cdelaure et à aider à initialiser un premier contact avec eux. Dans cette ébauche vous essaierez de décrire en 3 phrases la collaboration et son objet, puis les connaissances antérieures qu'apporte votre chercheur et les résultats envisageables.

(e) Enfin, vous dresserez une liste de questions à poser au chercheur avec une trame d'entretien à suivre pour vous permettre de progresser dans l'accompagnement de ce chercheur et dans la mise en place de collaborations en classant les différentes pistes par ordre de priorité.

a) Question 3 (5 points)Un chercheur non INRIA, membre d'une équipe projet INRIA vient vous voir pour monter un projet européen en tant que partenaire.

- Quelles sont les implications en termes d'obligations et en termes de propriété intellectuelle ? L'INRIA peut-il être partenaire du projet et si oui, selon quelles conditions ?

b) Vous dresserez une liste de questions à poser au chercheur afin de vous permettre de l'accompagner dans la soumission de son dossier. Pouvez-vous décliner et commenter les différentes méthodes pour faire la promotion d'un résultat de recherche

c) Faites une synthèse en 10 lignes en anglais de votre réponse à la question a).

ANNEXE

TCA

TCA (Tool for Cryptoki ANalysis) is an automated tool which reverse-engineers a real PKCS#11 *token* to deduce its functionality, constructs a model of its API for the SATMC model checker, and then executes any attack trace found by the model checker directly on the token.

PKCS#11 specifies an API for performing cryptographic operations such as encryption and signature using cryptographic tokens. Sensitive cryptographic keys are stored inside the token and any cryptographic operation is performed by the token without revealing the key to the outside, insecure, world. In fact, compromising a key allows an attacker to clone the token and, more generally, to perform the same security-critical operations as the legitimate token user.

TCA is able to extract sensitive cryptographic keys from a variety of commercially available tamper resistant cryptographic security tokens, exploiting vulnerabilities in their RSA PKCS#11 based APIs.

Analysis results

We report here our ongoing results on real devices. All the vulnerabilities have been reported to manufacturers at least 5 months before publication. The following table summarizes the results.

IMPORTANT NOTE: Responses from manufacturers, when given, are linked from the device model.

	Device		Supported Functionality						Attacks found					
	Company	Model	sym	asym	cobj	chan	w	ws	a1	a2	a3	a4	a5	mc
USB	Aladdin	eToken PRO	X	X	X	X	X	X	X	X				a1
	Athena	ASEKey	X	X	X									
	Bull	Trustway RCI	X	X	X	X	X	X	X	X				a1
	Eutron	Crypto Id. ITSEC		X	X									
	Feitian	StorePass2000	X	X	X	X	X	X		X	X	X		a3
	Feitian	ePass2000	X	X	X	X	X	X		X	X	X		a3
	Feitian	ePass3003Auto	X	X	X	X	X	X		X	X	X		a3
	Gemalto	Smart Enterprise Guardian		X		X								
	MXI Security	Stealth MXP Bio	X	X		X								
	RSA	SecurID 800	X	X	X	X					X	X	X	a3
	SafeNet	iKey 2032	X	X	X		X							
	Sata	DKey	X	X	X	X	X	X	X	X	X	X	X	a3
Card	ACS	ACOS5	X	X	X	X								
	Athena	ASE Smartcard	X	X	X									
	Gemalto	Cyberflex V2	X	X	X		X	X		X				a2
	Gemalto	SafeSite Classic TPC IS V1		X		X								
	Gemalto	SafeSite Classic TPC IS V2	X	X	X	X	X	X	X		X	X	X	a3
	Siemens	CardOS V4.3 B	X	X	X		X					X		a4

Soft	Eracom	HSM simulator	X	X		X	X	X	X	X	X		a1
	IBM	opencryptoki 2.3.1	X	X	X	X	X	X	X	X	X		a1

Below, we give more details on the supported functionalities:

- Columns '**sym**' and '**asym**' respectively indicate whether or not symmetric and asymmetric key cryptography are supported. (Gemalto SafeSite Classic TPC IS V1 should implement both symmetric and asymmetric cryptography according to its specification, but the one we tested could not generate and use symmetric keys. This may be a hardware issue with the specific token we possess.)
- Column '**cobj**' refers to the possibility of inserting external, unencrypted, keys on the device via C_CreateObject PKCS#11 function. This is allowed by almost all of the analysed tokens. Although this command does not directly violate a security property, allowing known keys onto a device is generally a dangerous thing: an attacker might import an untrusted wrapping key from outside and ask the device to wrap a sensitive internal key with it.
- The next column, '**chan**', refers to the possibility of changing key attributes through C_SetAttributeValue. This functionality can easily be abused if not limited in some way. For example, it is clear (and stated in the standard) that it should never be possible to make a sensitive key nonsensitive.
- The following two columns, '**w**' and '**ws**', respectively indicate whether the token permits wrapping of nonsensitive and sensitive keys. It is discouraging to observe that every device providing 'ws', i.e., the wrapping of sensitive keys, is also vulnerable to attack. All the other devices avoid attacks at the price of removing such functionality.

The reported attacks are as follows:

- Attack **a1** is a wrap/decrypt attack. The attacker exploits a key k2 with attributes wrap and decrypt and uses it to attack a sensitive key k1 . More precisely (& is used to note an handle to a key):

  Wrap(&k1,&k2) → senc(k1,k2)
  SDecrypt(senc(k1,k2), &k2) → k1

  As we have discussed above, the possibility of inserting new keys in the token (column 'cobj') might simplify further the attack. It is sufficient to add a known wrapping key k2 and use it to wrap the sensitive key k1. The attacker can then decrypt the wrapped k1, since he knows the wrapping key k2 . SATMC discovered this variant of the attack on vulnerable tokens. We note that despite its apparent simplicity, this attack has not appeared before in the PKCS#11 security literature.

- Attack **a2** is a variant of the previous ones in which the wrapping key is a public key and the decryption key is the corresponding private key;
- Attack **a3** is a clear flaw in the PKCS#11 implementation. It is explicitly required that the value of sensitive keys should never be communicated outside the token. In practice, when the token is asked for the value of a sensitive key, it should return some "value is sensitive" error code. Instead, we found that some of the analysed devices just return the plain key value, ignoring this basic policy;
- Attack **a4** is similar to a3: PKCS#11 requires that keys declared to be unextractable should not be readable, even if they are nonsensitive. If they are in fact readable, this is another violation of PKCS#11 security policy;
- Attack **a5** refers to the possibility of changing sensitive and unextractable keys respectively into nonsensitive and extractable ones.

All the acronyms are summarized below:

Acronym Description

Supported functionality	sym	symmetric-key cryptography
	asym	asymmetric-key cryptography
	cobj	inserting new keys via C_CreateObject
	chan	changing key attributes
	w	wrapping keys
	ws	wrapping sensitive keys
Attacks	a1	wrap/decrypt attack based on symmetric keys
	a2	wrap/decrypt attack based on asymmetric keys
	a3	sensitive keys are directly readable
	a4	unextractable keys are directly readable (forbidden by the standard)
	a5	sensitive/unextractable keys can be changed into nonsensitive/extractable
	mc	first attack found by TCA

Model files

the models of the above token, as extracted by TCA, are available here. Models are written in the TCA model metalanguage syntax.