RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ M'HAMED BOUGARA – BOUMERDES

FACULTÉ DES SCIENCES

THÈSE DE DOCTORAT

Présentée par :

Mesbah Abdelhak

Filière : Informatique

Option : Informatique

Rétro-conception d'application Java Card

Devant le Jury :

M.BADACHE	Nadjib	Prof-USTHB	Président
M. MEZGHICHE	Mohamed	Prof-UMBB	Encadreur
M. LANET	Jean-Louis	Prof-INRIA	Co-Encadreur
M.HAMADOUCHE	M'hamed	Prof-UMBB	Examinateur
M.RIAHLA	Mohamed Amine	MCA-UMBB	Examinateur
M.HAMMAL	Youcef	MCA-USTHB	Examinateur
M.BOUFFARD	Guillaume	ING-CHER-ANSSI	Invité

Année Universitaire : 2017/2018

RÉSUMÉ

Les objets de sécurité comme des Secure Element (SE) procèdent du paradigme `"Secure-by-Design"`. Ils sont protégés par des mécanismes matériels et offrent probablement le plus haut niveau de sécurité. Néanmoins ces objets peuvent être étudiés afin de déceler s'ils ne possèdent pas des vulnérabilités pouvant mettre en danger les secrets qu'ils possèdent. Ces objets sont implémentés dans les passeports électroniques, les cartes bancaires ou bien les terminaux de télécommunication. S'assurer de l'intégrité et de la confidentialité des données sensibles est donc vital.

Dans cette thèse nous montrons comment il est possible de réaliser une analyse complète d'un tel objet en développant une méthodologie basée sur l'observation d'expérience et la rétro-ingénierie des données et du code. Nous avons été amené à développer de nombreux outils afin de faciliter ces étapes. En particulier, après une phase de caractérisation des objets, nous sommes capables de tracer le graphe des objets atteignables. Nous avons aussi développé un moteur d'inférence de type permettant de calculer un chemin menant entre deux états du système pouvant représenter une séquence d'instructions valides. L'exploitation de cette analyse a permis de déchiffrer les clés cryptographiques stockées pourtant chiffrées dans le SE. Nous avons aussi pu faire revenir le système dans un état normalement inaccessible, autorisant l'exécution de méthodes privilégiées. Enfin nous avons proposé la possibilité de rendre permanente une attaque en faute initialement transiante.

L'analyse du contenu de ce SE nous a permis de proposer des contremesures pouvant bloquer une telle rétro-ingénierie. Les contrôles d'intégrité sur des éléments clés du système d'exploitation, une bonne vérification du typage des paramètres et l'offuscation du code nous semblent des techniques abordables et nécessaires pour éviter cette attaque.

Ce travail a mis en évidence que, bien que développé avec des ingénieurs reconnus dans leur domaine, des implémentations très sécurisées des algorithmes cryptographiques ne protègent pas d'une attaque par une personne motivée. La sécurité par l'obscurité ne fait que retarder le succès de l'attaque mais ne peut jamais se substituer à une conception rigoureuse et auditée d'un logiciel dédié à un objet de sécurité.

Mots clés : Élément sécurisé, Rétro-ingénierie des données, Java Card, Attaque logicielle, Découverte de vulnérabilités

ABSTRACT

Secure elements store and manipulate assets in a secure way. They are protected by hardware mechanisms and probably offer the highest level of security. Nevertheless, these objects can be studied to detect if they do not have vulnerabilities that could endanger the secrets they possess. These objects are implemented in e-passports, identity, bank cards or telecommunication terminals. Ensuring the integrity and confidentiality of sensitive data is therefore crucial.

In this thesis we show how it is possible to perform a complete analysis of such an object by developing a methodology based on the observation's experience and the reverse engineering of data and code. We have developed many tools to facilitate these steps. In particular, after a characterization phase of the objects, we are able to draw the graph of the reachable objects. We have also developed a type inference tool that calculates a leading path between two system states that can represent a valid instruction sequence. The exploitation of this analysis made it possible to decipher the cryptographic keys stored but encrypted in the operating system. We are also able to return the system to a normally inaccessible state, allowing the execution of privileged methods. Finally we propose the possibility of making fault permanent attack which is initially transient.

This work has highlighted that although developed with engineers recognized in their field, very secure implementations of cryptographic algorithms, do not protect an attack by a motivated person. Security by obscurity only delays the success of the attack, but it can never replace a rigorous and audited design of software dedicated to a security object.

Keywords : Secure element, Data reverse engineering, Java Card, Software Attack, Vulnerability discovery

ملخص

تُطور عناصر الأمان على حسب نموذج التصميم بالأمان. هذه العناصر محمية بواسطة آليات مادية وربما توفر أعلى مستوى من الأمان. ومع ذلك، يمكن دراسة هذه العناصر للكشف عما إذا كانت لا تعاني من نقاط ضعف قد تعرض للخطر الأسرار التي تمتلكها. يتم استعمال هذه العناصر في جوازات السفر الالكترونية، أو البطاقات المصرفية أو محطات الاتصالات السلكية واللاسلكية. لذلك فإن ضمان سلامة البيانات الحساسة وسريتها يعد أمر حيوي.

في هذه الرسالة، نوضح كيف يمكن إجراء تحليل كامل لمثل هذه العناصر من خلال تطوير منهجية مبنية على ملاحظة الخبرة والهندسة العكسية للبيانات و الاوامر. لقد قمنا بتطوير العديد من الأدوات لتسهيل هذه الخطوات. على وجه الخصوص، بعد مرحلة توصيف الكائنات، يمكننا تمثيل هذه الكائنات برسم بياني للكائنات القابلة للوصول. لقد طورنا أيضا محركا للاستدلال من النوع الذي يحسب مسارا عكسيا بين حالتين لتمثيل تسلسل تعليمات صالحة. يمكننا استغلال هذا التحليل في فك رموز مفاتيح التشفير المخزنة بطريقة مشفرة في نظام التشغيل. كما تمكنا من إعادة النظام إلى حالة يتعذر الوصول إليها عادة، مما يسمح لنا تجاوز الصلاحيات. وأخيراً اقترحنا إمكانية جعل هجوم دائم على غرار انه كان مفعول الهجوم عابراً.

سمح لنا تحليل محتوى هذا العنصر الآمن باقتراح تدابير مضادة يمكن أن تعوق مثل هذه الهندسة العكسية. التحقق من نزاهة العناصر الأساسية لنظام التشغيل، و تشويش شفرة واجهة برمجة التطبيقات تبدو لنا أساليب معقولة و ضرورية لتجنب هذا الهجوم.

سمح لنا تحليل محتوى هذا العنصر الآمن باقتراح تدابير مضادة يمكن أن تعوق مثل هذه الهندسة العكسية. التحقق من نزاهة العناصر الأساسية لنظام التشغيل، و تشويش شفرة واجهة برمجة التطبيقات تبدو لنا أساليب معقولة و ضرورية لتجنب هذا الهجوم.

الكلمات الرئيسية : عناصر الامان، الهندسة العكسية للمعلومات، جافا كارد، هجوم البرمجيات، اكتشاف الضعف

TABLE DES MATIÈRES