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 amenés 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