ZIMPERIUM®
ADVANCED MOBILE SECURITY

Les 5 meilleures pratiques en matière de protection des clés cryptographiques

Les clés cryptographiques constituent un élément de base de la cybersécurité moderne. Elles ont pour but de chiffrer les données en toute sécurité et de garantir la sécurité des réseaux lors d'une communication client-serveur. Malheureusement, cela en fait une cible parfaite pour les pirates informatiques. Une seule clé compromise est capable de donner accès à une mine de données personnelles et d'adresses IP précieuses, et de permettre d'autres actions malveillantes comme l'accès à un système ou la signature de certificats numériques non autorisés. Malgré l'importance de la protection des clés cryptographiques, de nombreux développeurs de solutions logicielles ne lui donnent malheureusement pas la priorité.

Les récentes attaques contre les clés cryptographiques démontrent l'étendue et les retombées du problème :

- Le vol des clés de cryptage du plus grand fabricant de cartes SIM au monde, qui produit annuellement plus de deux milliards de cartes SIM. Cet accès permettrait, par hypothèse, aux pirates de décrypter les communications des appareils mobiles et des modems qui sont censés être sécurisés.

- Les attaques par canal auxiliaire qui utilisent les signaux « fuyants » des appareils pour voler des clés cryptographiques, notamment un appareil créé par des chercheurs et qui pouvait lire des fréquences électromagnétiques tout en étant dissimulé dans du pain pita.

- Une banque sud-africaine a stocké sa clé de chiffrement principale en clair dans un centre de données, cette clé a ensuite été volée par des employés qui l'ont utilisée pour commettre une fraude. Cette banque a finalement été contrainte de changer 12 millions de cartes bancaires.

- Le piratage en masse de l'hôtel Marriott, qui a provoqué le vol d'un demi-milliard de données de clients, n'aurait pas été tellement destructeur si les pirates n'avaient pas réussi à voler les clés cryptographiques,qui étaient stockées sur le même serveur que les données cryptées des clients.

La majorité de ces attaques auraient pu être atténuées si des stratégies de base de protection des clés cryptographiques ont été implémentées. Comment les équipes de développement peuvent-elles donc assurer la sécurité des clés ? Voici un aperçu des cinq bonnes pratiques à mettre en place.

Les meilleures pratiques en matière de protection des clés cryptographiques

1. Ne jamais coder en dur les clés dans votre logiciel
Cela peut paraître évident, mais cela se produit plusieurs fois, même chez les fournisseurs de solutions de cybersécurité. L'utilisation d'une clé cryptographique codée en dur augmente nettement le risque de récupération des données cryptées. Ce type de vulnérabilité est notablement connu pour sa difficulté de correction, puisqu'il requiert une mise à jour du logiciel pour y remédier. À titre d'exemple, il a fallu 18 mpois au fournisseur de cybersécurité précité pour supprimer l'ensemble de clés de cryptage codées en dur de tous ses logiciels.
De plus, les bonnes pratiques de codage sécurisé exigent que les variables contenant des clés cryptographiques soient écrasées après chaque utilisation. Ces mesures permettent d'éviter toute sorte de compromission en cas d'accès ultérieur à cet emplacement de mémoire par un code non fiable.

2. Limiter les clés à un usage unique et bien spécifique
Chaque clé doit être utilisée pour une seule et unique application et dans un seul but : chiffrement, authentification, enveloppement de clés, génération de nombres aléatoires ou encore signature numérique. Les clés doivent être générées avec le niveau de sécurité approprié pour l'usage auquel elles sont destinées - les utiliser pour un autre processus risque de ne pas fournir le niveau de sécurité requis. Réutiliser une clé risque également d'entraîner des dommages accrus en cas de compromission de la clé.

Il importe de prêter une attention particulière aux clés de cryptage, également appelées clés de chiffrement (KEK). Il s'agit de clés utilisées pour protéger d'autres clés cryptographiques. Les KEK doivent toujours être d'une force égale ou supérieure à celle de la clé cryptographique qu'elles enveloppent, elles ne doivent surtout pas être utilisées à d'autres fins, comme le cryptage de données ou de communications.

3. Dans la mesure du possible, utilisez une sécurité renforcée par matériel
Un module matériel de sécurité (HSM) permet de garantir une protection accrue des clés cryptographiques et peut être obligatoire dans certains cas d'utilisation, comme la sécurisation des clés racine dans les ICP (les infrastructures à clés publiques). Ce boîtier physique est capable d'exécuter des fonctions cryptographiques comme le cryptage, le décryptage et la génération de clés. L'utilisation d'un HSM élimine le besoin de stocker les clés d'un logiciel de façon sécurisée et empêche les pirates d'accéder aux données et aux clés dont ils ont besoin pour les décrypter en un seul endroit. Parmi les autres solutions matérielles, on trouve les modules de plateforme fiable (TPM) et les environnements d'exécution de confiance (TEE), qui fournissent des systèmes isolés sur le plan matériel pour effectuer des opérations cryptographiques.

Toutefois, les solutions basées sur les composantes matérielles peuvent être onéreuses, tant sur le plan de coût que d'espace physique. Elles sont également vulnérables aux attaques par canal auxiliaire qui mesurent les signaux non intentionnels transmis par les dispositifs physiques (comme la chaleur, le son ou le temps nécessaire pour effectuer une action).

4. Profitez de la cryptographie en boîte blanche pour combler les lacunes en matière de protection des clés.
Pour des applications et des données à forte valeur ajoutée, et lorsque la protection des clés par des composantes matérielles n'est pas possible ou est insuffisante, il faut penser à une protection logicielle des clés. Les applications ne peuvent pas être sûres que les appareils mobiles et de bureau sur lesquels elles s'exécutent disposent de la capacité matérielle requise pour effectuer des opérations cryptographiques en toute sécurité et assurer la protection des clés cryptographiques. C'est précisément le cas pour les applications Web, puisque les navigateurs n'arrivent pas à accéder au support de sécurité du matériel sous-jacent, même s'il est disponible. Dans ces cas, il est vivement recommandé d'utiliser la cryptographie en boîte blanche.

La cryptographie en boîte blanche a recours à une multitude de techniques de protection dans le but de créer un environnement d'exécution et de stockage sécurisé pour les fonctions cryptographiques dans les logiciels et les applications. zKeyBox, la solution de cryptographie en boîte blanche de Zimperium, parmi les meilleures de l'industrie, utilise une technologie brevetée pour protéger les principaux algorithmes de cryptographie (notamment DES, AES, RSA, SPECK, ECC, ECDSA, DH, ECDH et SHA) et ne dépend d'aucun mécanisme matériel fourni par les plates-formes (à titre d'exemple : Keystores, Secure Enclave, Trusted Execution Environment (TEE ou Environnement d'Exécution de Confiance) sur Android).

Les solutions logicielles de protection des clés sont beaucoup plus simples à implémenter par rapport à leurs équivalentes matérielles, car elles fournissent des fonctionnalités identiques sur tous les appareils. La situation devient encore plus critique quand on se trouve confronté à des applications réglementées qui doivent se conformer à des normes de sécurité très strictes. Une cryptographie puissante en boîte blanche a l'avantage supplémentaire de protéger les applications contre les vulnérabilités de l'exécution spéculative et d'autres attaques par canal auxiliaire.

5. Implémenter une gestion puissante de clés
La gestion des clés entraîne la création d'un bon nombre de politiques ayant pour objectif de garantir que les clés cryptographiques ne sont pas mises en péril par ignorance ou par manque de rigueur. Les politiques de gestion des clés efficaces sont axées sur :

- Cycle de vie des clés : Consiste à la gestion sécurisée de tous les aspects, depuis la création, la distribution et l'utilisation normale des clés jusqu'à leur substitution, leur expiration, leur archivage et leur destruction.

- Stockage et sauvegarde des clés : Comme mentionné plus haut, la protection des clés cryptographiques est tributaire d'un stockage sécurisé, comme un dispositif matériel de sécurité ou l'utilisation de la cryptographie en boîte blanche. Les clés stockées dans des dispositifs ou des bases de données hors ligne doivent être cryptées à l'aide de KEK avant un stockage ou une exportation. Les applications doivent inclure la possibilité de sauvegarder les clés de manière sécurisée, car il serait impossible de récupérer les données cryptées avec une clé cryptographique égarée.

- Protections et restrictions d'accès : L'accès aux clés cryptographiques pendant leur cycle de vie doit être rigoureusement contrôlé car les utilisateurs et le niveau d'accès sont identifiables. Une telle responsabilisation demeure indispensable pour garantir la sécurité des clés cryptographiques et réduire l'impact de toute éventuelle compromission.

Comment commencer

Heureusement, en ce qui concerne la sécurité des clés cryptographiques, il n'est pas nécessaire de repartir à la case zéro. Un certain nombre de normes et de protocoles recommandés, comme le NIST 800-57, fournissent des lignes directrices détaillées sur la meilleure façon de protéger les clés secrètes et sur les normes à respecter. L'outil de gestion des clés Cheat Sheet de l'OWASP est une excellente ressource en matière de la protection et de la gestion des clés cryptographiques pour les développeurs.

La protection des clés cryptographiques reste un maillon clé dans toute stratégie de cybersécurité. ZKeyBox de Zimperium est conçu pour garantir la sécurité des clés cryptographiques dans certaines des situations les plus vulnérables. Pour en savoir davantage sur le fonctionnement de la solution zKeyBox, leader sur le marché, prière de nous contacter pour échanger avec l'un de nos experts en sécurité.

ZIMPERIUM®

4055 Valley View Dallas, TX 75244
844.601.6760
info@zimperium.com