



Les piratages informatiques fréquents et leurs contre-attaques

Guide de protection des produits informatiques contre les 7 principales mesures de piratage

PRESENTATION GENERALE

Pour avoir la certitude d'être correctement payés pour l'utilisation de leurs applications, les distributeurs indépendants de logiciels doivent mettre en place un certain type de protection informatique. Une solution de protection informatique, quelle qu'elle soit, a pour objectif de limiter l'utilisation d'un logiciel de manière à respecter certaines dispositions spécifiques prévues dans la licence. Cela peut se faire à l'aide de jetons (également appelés « dongles »), de licences portant uniquement sur un logiciel ou d'un code interne.

Les solutions faisant appel à un matériel extérieur offrent actuellement la meilleure sécurité. Malheureusement, les pirates représentent une nuisance constante qui coûte des milliards de dollars de pertes de revenus aux distributeurs de logiciels du monde entier. Il est important de s'assurer que la solution matérielle que vous choisissez et votre mise en œuvre de cette dernière bloquent totalement les points habituels d'entrée des pirates. Ce livre blanc examine un large éventail des techniques de piratage les plus fréquentes et des meilleures contre-attaques dont vous disposez pour protéger votre application contre le piratage.

COMPARAISON ENTRE LES PIRATAGES GENERIQUES ET LES PIRATAGES SPECIFIQUES

Les piratages s'attaquant aux « dongles » de protection informatique appartiennent à l'un ou l'autre des types suivants : le premier est générique et le deuxième est spécifique. Lors d'un piratage générique, le « dongle » proprement dit est compromis. La mise en œuvre d'améliorations, quelle qu'en soit l'envergure, ne permet pas de contrer un piratage générique. Toutes les applications protégées par le « dongle » piraté sont en fait menacées. Les piratages spécifiques ne détruisent qu'une mise en œuvre spécifique du « dongle », et ce pour une application informatique bien précise. Ils ne posent aucun risque pour d'autres fournisseurs de logiciels employant le même « dongle ».

PERCEMENT DE TUNNELS SECURISES

Des jetons de protection informatique sont intégrés à des applications en faisant appel à une boîte à outils logiciels. Pour que le logiciel fonctionne, il faut rattacher le jeton à l'ordinateur ou au réseau de l'utilisateur. L'application protégée vérifie la présence de la clé pendant le fonctionnement pour s'assurer que l'utilisation du logiciel est autorisée et pour confirmer le respect de l'accord de licence.

Lors de la défense contre une attaque, il faut défendre la communication entre le jeton et l'application informatique car c'est potentiellement le point le plus vulnérable. Pour sécuriser cette communication, certains jetons matériels utilisent des algorithmes de cryptage pour créer un tunnel sécurisé et à l'épreuve du piratage, d'une extrémité à l'autre.

Pour créer un tunnel sécurisé de communication entre le jeton matériel et l'application, il faut tout d'abord remplacer les clés de cryptage. Cette procédure de remplacement des clés commence lorsque l'application produit une clé aléatoire AES (Advanced Encryption Standard) de cryptage. La production d'une nouvelle clé aléatoire lors de chaque session de communication renforce largement la sécurité. En particulier, il est important de ne pas utiliser de clé statique car cela augmente la vulnérabilité en cas d'attaque.

Ensuite, l'application enveloppe la clé AES en utilisant une clé publique ECC (Elliptic Curve Cryptography) de cryptographie à courbe elliptique. Ensuite, le lecteur transfère la clé AES enveloppée au jeton. Ce jeton, dès réception, déballe la clé AES en utilisant sa clé ECC privée, ce qui met fin à la procédure de changement de clé. La mémorisation de la clé ECC privée dans le jeton et

non pas dans l'application renforce en outre énormément la sécurité. Le piratage d'une application logicielle est relativement plus simple que le piratage du jeton car il tourne sur une plate-forme de matériel et de système d'exploitation bien comprise et pour laquelle existent des outils fournis par des tierces parties pour faciliter les programmes de débogage et de lutte contre l'ingénierie inverse. Il n'en va pas de même du logiciel qui tourne à l'intérieur du jeton. De ce fait, le débogage du logiciel du jeton pour trouver les clés n'est pas une entreprise facile, à moins que vous ne soyez le fabricant de ce jeton.

Toutes les communications entre le lecteur et le « dongle » sont maintenant protégées en utilisant la clé de cryptage qui a été remplacée. La procédure de changement de clé est une forme de cryptographie à clé publique et donne lieu à la création de clés symétriques basées sur chaque session pour assurer la protection des communications. Le jeton et l'application communiquent par le biais d'un tunnel sécurisé en cryptant et décryptant toutes les communications en faisant appel à la clé AES. Lors de chaque session ultérieure de communication, une nouvelle clé AES sera utilisée.

L'algorithme AES a été adopté par le NIST (National Institute of Standards and Technology) en novembre 2001 et on estime que son piratage est improbable sur le plan mathématique. La cryptographie ECC à courbe elliptique est encore plus faible et on pense que son piratage est mathématiquement impossible.

PIRATAGE N°1 : ATTAQUE BRUTALE

Une attaque brutale essaye, de manière exhaustive, toutes les combinaisons sécuritaires jusqu'à ce que le secret ainsi attaché soit compromis. Les clés cryptographiques se trouvent au cœur même de la sécurité d'un « dongle ». Si une attaque brutale réussit, cela compromet les « dongles » mais uniquement ceux d'un fournisseur spécifique de logiciels. Il ne s'agit pas d'un piratage générique. En outre, l'utilisation de mots de passe courts avec certaines API peut accroître la faiblesse lors de cette attaque.

CONTRE-ATTAQUE

On peut éviter une attaque brutale lorsque le volume de données est suffisamment important pour rendre pratiquement impossible un décodage en employant toutes les combinaisons possibles. Pour protéger les algorithmes au cœur de la sécurité d'un « dongle », ce dernier doit comporter un noyau sécurisé de sécurité qui conservera en toute sécurité la clé cryptographique.

Par exemple, le noyau de sécurité d'un « dongle » peut être une clé AES 128 bits qui permet de crypter et protéger les algorithmes au cœur du « dongle ».

PIRATAGE N°2 : EMULATION D'APPAREIL

Cette émulation se produit lorsqu'un logiciel cherche à émuler le « dongle » sur le plan matériel. Tous les secrets du « dongle » comme, par exemple, les valeurs des clés cryptographiques, sont placés dans le logiciel émulateur. Ce logiciel assure l'émulation de l'appareil et se présente à l'application comme s'il était le « dongle » matériel. Connaissant les valeurs de la clé, le logiciel effectue les mêmes opérations que le jeton.

L'émulation d'appareil est un piratage générique du « dongle » et utilise la clé cryptographique, ce qui provoque une attaque brutale qui déverrouille et active l'utilisation de l'application logicielle.

CONTRE-ATTAQUE

L'émulation d'appareil peut être empêchée en sécurisant la zone mémoire du « dongle », ce qui fait qu'il est pratiquement impossible de compromettre le « dongle » en effectuant une attaque brutale.

L'un des moyens permettant de sécuriser la zone mémoire consiste à utiliser une clé AES 128 bits qu'il est difficile d'attaquer de manière brutale en employant la puissance informatique qui existe aujourd'hui.

PIRATAGE N°3 : ENREGISTREMENT/PLAYBACK

Lors d'une attaque du type enregistrement/playback, toutes les informations échangées entre l'application et le « dongle » sont enregistrées. Un intergiciel ou middleware (application logicielle) est alors créé par le pirate pour imiter les réponses fournies par le « dongle ».

A la suite d'une attaque du type Enregistrement/playback, l'application est compromise. Le fournisseur doit alors revoir la conception de la protection qu'il a mise en œuvre afin de lutter contre ce type d'attaque. Il ne s'agit pas d'un piratage générique mais cela affecte toutes les copies de l'application dans lesquelles existe une attaque de type Enregistrement/playback.

CONTRE-ATTAQUE

Les attaques du type Enregistrer/playback peuvent être évitées en procédant à un cryptage et une randomisation entre l'application et le « dongle ». L'utilisation d'une clé aléatoire 128 bits pour crypter les communications entre l'application et le « dongle » est un moyen efficace permettant d'éviter ce piratage.

L'utilisation d'une clé statique ou d'une valeur codée en dur dans l'application affaiblit les attaques du type Enregistrer/playback. Si un « dongle » utilise des clés symétriques, lors du partage d'un secret, il faut en laisser une copie dans l'application. Lors du cryptage à l'intérieur de l'application, il faut y laisser la clé. Alors qu'avec le percement de tunnels sécurisés, la clé privée est conservée dans le jeton et la clé publique reste dans l'application.

Lorsque la clé publique est incorporée à l'application, la décompilation du code permettra au pirate de n'accéder qu'à une clé publique et non pas à une clé privée. La découverte d'une clé publique ne crée pas de vulnérabilité au niveau de la sécurité. Néanmoins, si un « dongle » utilise des clés symétriques statiques, la décompilation de l'application risque de révéler le secret des communications. Il s'agit d'un point potentiel d'entrée pour une infestation provoquée par un pirate car ce dernier peut comprendre toutes les communications.

PIRATAGE N°4 : VOL DE SECRETS

Il y a vol de secrets à la suite de l'obtention illégale d'un mot de passe, ce qui permet un accès non autorisé au « dongle ». Dès qu'un pirate a accédé au « dongle », il est en mesure de manipuler l'application en se servant de ce « dongle ».

CONTRE-ATTAQUE

Il ne faut jamais communiquer des mots de passe de « dongles » avant de les avoir cryptés. Il faut toujours crypter les données qui sont envoyées au « dongle ». En n'envoyant jamais des mots de passes et d'autres secrets « en clair », vous vous protégez de manière efficace contre ce type de pirate.

Néanmoins, même lorsque vous vous servez de canaux cryptés pour protéger des secrets, il est important de ne pas utiliser de clé statique. L'emploi d'une clé statique renforce la vulnérabilité des informations qui doivent être extraites de ces clés.

PIRATAGE N°5 : PARTAGE D'APPAREIL

L'expression partage d'appareils signifie que plusieurs ordinateurs personnels partagent un même « dongle » alors qu'ils n'ont pas reçu l'autorisation de le faire. Un « dongle » peut être utilisé par plusieurs machines sur un même réseau. Bien que l'application proprement dite ne soit pas mise en danger, le fournisseur de logiciels ne recevra pas les recettes prévues en cas d'utilisation de son application sur plusieurs copies. L'utilisation d'une clé statique de cryptage va renforcer la prédisposition à cette attaque.

Il existe deux scénarios potentiels qui permettent d'obtenir le partage de dispositifs.

1. Session VMWare : Systèmes virtuels multiples d'exploitation qui tournent sur plus d'une plate-forme matérielle. Le partage d'une licence dans cet environnement permet de faire tourner simultanément plusieurs applications lors de chaque session VMWare (au lieu d'une seule). Dans le cadre de ce scénario, chaque session VMWare utilise son propre lecteur pour communiquer avec le « dongle ».
2. Pivot central USB de partage : Un pivot central USB peut être rattaché à plusieurs ordinateurs pour partager un même dispositif USB. Dans un tel cas, chaque ordinateur relié à ce pivot central USB pense qu'il a un « dongle » personnel. Cela permet à plusieurs ordinateurs d'exploiter une application même lorsqu'une seule licence existe.

CONTRE-ATTAQUE

Les fournisseurs de logiciels doivent s'assurer que le nombre d'ordinateurs ou de lecteurs de périphériques qui ont accès au « dongle » ne dépasse pas le nombre payé par le client. Le percement de tunnels sécurisés permet de se protéger contre les tentatives d'accès au jeton par plusieurs dispositifs ou machines.

Chaque utilisation de l'application ouvre une unité d'exploitation de lecteur. Néanmoins, deux ou plusieurs utilisations du lecteur ne permettent pas de communiquer avec le « dongle » par l'entremise d'un tunnel sécurisé. Un lecteur de « dongle » intelligent permet de se protéger contre ces scénarios et n'applique que le nombre de licences qui ont le droit de fonctionner à partir du « dongle ». L'absence d'un lecteur risque d'augmenter votre vulnérabilité à cette attaque.

PIRATAGE N°6 : CLONAGE DE MATERIEL

Un clonage de matériel se produit lorsque des jetons de matériels qui autorisent l'application protégée font l'objet d'une duplication. Pour effectuer une duplication de la mémoire du matériel, le pirate achète tout d'abord des jetons auprès du même fournisseur de jetons dont se sert le distributeur individuel de logiciels. Ensuite, le pirate effectue un clonage des jetons en recopiant le contenu de la mémoire à partir du jeton d'origine.

CONTRE-ATTAQUE

Les distributeurs de logiciels doivent s'assurer qu'ils sont protégés contre le clonage en faisant en sorte que la mémoire du jeton soit cryptée. Une solution possible consiste à crypter la mémoire en faisant appel à une clé AES 128 bits à jeton unique. Ce processus doit faire automatiquement partie de la protection assurée par votre « dongle ». Il faut éviter de ne pas crypter les données de l'utilisateur dans la mémoire du jeton.

PIRATAGE N°7 : FALSIFICATION DE LA DATE ET DE L'HEURE

La falsification de la date et de l'heure consiste à faire défiler à l'envers l'horloge du système pour tricher dans le cadre d'une licence basée sur la durée. En utilisant une telle technique, il serait possible d'utiliser à l'infini une version d'évaluation destinée à une utilisation de durée limitée.

CONTRE-ATTAQUE

Une méthode de sécurisation de ces périodes à l'essai consiste tout simplement à offrir des versions limitées ou estropiées du logiciel. Néanmoins, si vous souhaitez créer des licences de durée limitée, afin d'offrir des abonnements à des logiciels ou de proposer des versions complètes d'évaluation limitées en matière de durée, la falsification de la date et de l'heure présente un risque qu'il faut évaluer afin de lutter contre lui.

Une méthode permettant de créer des licences sécurisées de durée limitée consiste à intégrer une horloge en temps réel dans une clé matérielle. Le pirate potentiel devra alors chercher à s'infiltrer dans la clé pour en modifier l'horloge, ce qui entraînera la destruction complète de la clé. Malheureusement, les clés équipées d'horloges en temps réel sont plus coûteuses et ont également besoin d'une batterie interne qui finira par être complètement à plat.

Heureusement, il y a des méthodes simples et intelligentes qui permettent de lutter contre la falsification de la date et de l'heure sans augmentation de coûts. Si un jeton matériel est équipé d'une fonction qui lui permet de vérifier et mémoriser l'heure actuelle du système, les développeurs peuvent se servir de cette information pour éviter toute falsification de la date et de l'heure. Si le jeton détecte des changements notables dans l'heure du système, l'application peut être programmée pour se désactiver ou pour fonctionner dans un mode restreint. Cette solution va vous permettre d'offrir des options de licences basées sur la durée ainsi que des évaluations sécurisées et limitées dans le temps. Le vol résultant d'une utilisation illimitée dans le temps « d'une évaluation gratuite mais limitée en durée » est ainsi empêchée, sans encourir les frais supplémentaires d'horloges en temps réel et sans les inconvénients posés par de telles horloges.

CONCLUSION

Outre la sélection de la technologie à « dongle » la plus sécurisée sur le marché, une mise en œuvre sécurisée est vitale. Pour prendre connaissance des meilleures pratiques et de consignes spécifiques ayant pour but de sécuriser la licenciation pour votre logiciel, quelle que soit votre technologie de mise en œuvre de ces licences, consultez le livre blanc de SafeNet et séminaire sur le Web « Un guide du développeur pour la protection des logiciels : Application de techniques de codage des modems pour sécuriser les logiciels » (Applying Modern Coding Techniques to Securing Software Assets).

A propos de SafeNet, Inc.

SafeNet est un des leaders mondiaux en matière de sécurité des données. Fondée il y a plus de 20 ans, la société assure une sécurité totale en utilisant ses technologies de cryptage pour protéger les communications, les droits de propriété intellectuelle et les identités numériques, et elle offre toute la gamme des produits, notamment systèmes logiciels, systèmes matériels et puces (circuits intégrés). UBS, Nokia, Fujitsu, Hitachi, Bank of America, Adobe, Cisco Systems, Microsoft, Samsung, Texas Instruments, les Départements américains de la Défense et de la Sécurité intérieure, le U.S. Internal Revenue Service (service de collecte des impôts américains) et bien d'autres clients font confiance à SafeNet pour garantir la sécurité de leurs données. En 2007, SafeNet a été rachetée par Vector Capital.

Pour de plus amples informations sur les solutions proposées par SafeNet pour la protection de logiciels et l'octroi de licences de logiciels, veuillez visiter www.safenet-inc.com/sentinel.