Livre blanc

Firmware signé, démarrage sécurisé et stockage TPM de clé dans les produits Axis

Novembre 2018

AXIS COMMUNICATIONS

Table des matières

Résumé

Ce document traite de trois menaces spécifiques que des attaquants externes malveillants pourraient tenter d'exploiter au sein d'un système. Ces menaces sont les suivantes : le sabotage de firmware, le sabotage du circuit de logistique et l'extraction de clés privées. Chacune de ces menaces est ici détaillée, accompagnée d'un exemple d'attaque type et il est expliqué comment Axis développe ses dernières fonctions de firmware signé, démarrage sécurisé et trusted platform module (TPM, ou coffres-forts numériques) afin de contrer ces menaces.

La fonction firmware signé est implémentée par le fournisseur de logiciels quand il signe l'image du firmware avec une clé privée. Lorsqu'un firmware est estampillé de cette signature, un composant avec cette fonction activée vérifiera le firmware avant d'autoriser son installation. Si le composant détecte que l'intégrité du firmware est corrompue, la mise à jour ou installation du firmware sera refusée. Le firmware signé Axis est basé sur la méthode conforme de chiffrement de clé publique RSA. La clé privée conservée dans les locaux d'Axis et sous haute surveillance tandis que la clé publique est embarquée sur les produits Axis.

Le démarrage sécurisé est un processus d'amorçage constitué d'une validation cryptographique de la chaîne software depuis la mémoire ROM. Comme elle s'appuie sur l'utilisation de firmware signé, la fonction démarrage sécurisé garantit qu'un composant ne pourra démarrer que si le firmware a été validé.

Un TPM est un élément qui délivre un panel de fonctions cryptographiques destinées à la protection d'information contre les accès non-autorisés. Les clés privées sont stockées dans le TPM et n'en sortent jamais, toutes les opérations cryptographiques qui nécessitent l'utilisation de la clé privée sont plutôt redirigées vers le TPM afin d'y être traitées. Cela assure que la partie secrète du certificat ne quitte jamais l'environnement sécurisé du TPM et reste protégée même en cas de violation de sécurité.

Le TPM utilisé dans les produits Axis sélectionnés est certifié de répondre aux critères FIPS 140-2.

1. Introduction

Au sein d'un système de vidéo protection en réseau, les composants les plus exposés sont les caméras. Souvent situées dans des zones éloignées et à hauts risques, elles sont constamment confrontées au risque d'être endommagées par des conditions météorologiques extrêmes, des tentatives de sabotage ou même des actes de vandalisme. Fort heureusement, il existe toute une gamme de caissons à l'épreuve des intempéries et du vandalisme, afin de protéger une installation de ces types de menaces. Lorsqu'il s'agit des risques d'attaques numériques, la cybersécurité consiste à protéger les données, les ressources et les infrastructures.

Ce document traite de trois menaces spécifiques que des attaquants externes malveillants pourraient tenter d'exploiter au sein d'un système. Ces menaces sont les suivantes : le sabotage de firmware, le sabotage du circuit de logistique et l'extraction de clés privées. Chacune de ces menaces est ici détaillée, accompagnée d'un exemple d'attaque type et il est expliqué comment Axis développe ses dernières fonctions de firmware signé, démarrage sécurisé et TPM afin de contrer ces menaces.

De nombreuses menaces sont liées à une mauvaise utilisation du système, accidentelle ou délibérée, par des individus qui possèdent une autorisation d'accès. Pour plus d'informations sur les mesures à prendre pour réduire les risques les plus courants, référez-vous au Axis Hardening Guide, disponible sur www.axis.com/about-axis/cybersecurity

2. Détection de sabotage du firmware

Quand plusieurs tentatives d'infiltration du système ont échoué, un angle d'attaque possible est d'inciter le propriétaire du système à installer des applications, des firmwares ou encore des modules de logiciels qui auraient été modifiés. Ces logiciels peuvent contenir du code malveillant créé dans un but précis. La recommandation habituelle est de ne jamais installer de logiciel provenant d'une source qui n'a pas toute votre confiance. Dans le contexte d'un système vidéo, il pourrait très bien y avoir un « intercepteur » qui aurait modifié un firmware et incité l'utilisateur final à l'installer. Ce n'est pas une tâche simple, l'attaquant doit être hautement qualifié et déterminé et il lui faut une connaissance générale du design des firmwares Axis et de leur fonctionnement opérationnel. Il est quand même possible que de tels profils existent si les enjeux derrière ces attaques ciblées sont d'importance stratégique. La contre-mesure habituelle est que le fournisseur de logiciels utilise un firmware signé.

2.1 Signature de firmware

La fonction firmware signé est implémentée par le fournisseur de logiciels quand il signe l'image du firmware avec une clé privée. Lorsqu'un firmware est estampillé de cette signature, un composant avec cette fonction activée vérifiera le firmware avant d'autoriser son installation. Si le composant détecte que l'intégrité du firmware est corrompue, la mise à jour ou installation du firmware sera refusée.
Le processus de signature du firmware (voir schéma 1) est initialisé par la génération d'une valeur cryptographique. La valeur obtenue est ensuite signée de la clé privée appartenant à une paire clé privée/clé publique avant que la signature ne soit attachée à l'image du firmware.

Schéma 1. Le processus de signature de firmware.

Avant une mise-à-jour du firmware, la nouvelle version doit être vérifiée. Afin d'assurer que le nouveau firmware n'a pas été modifié, on utilise la clé publique (qui est intégrée au composant Axis) pour confirmer que la valeur cryptée a bel et bien été signée de la clé privée. En calculant également la valeur cryptée du firmware et en la comparant à la valeur confirmée de la signature, l'intégrité du firmware peut être vérifiée. (voir schéma 2).

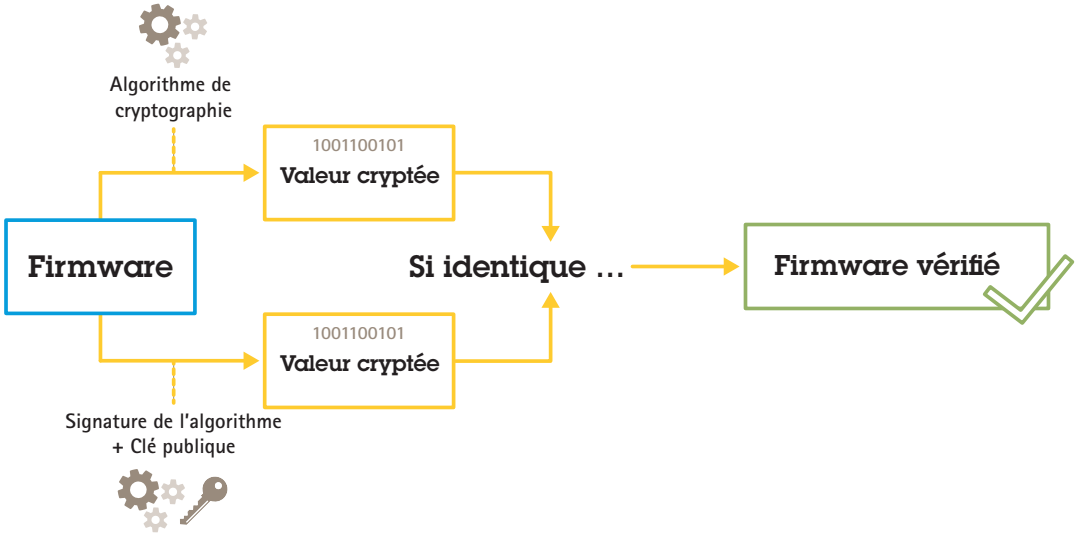

Schéma 2. Le processus de vérification de signed firmware.

2.2 Firmware signé chez Axis

Le firmware signé Axis est basé sur la méthode conforme de chiffrement de clé publique RSA. La clé privée est conservée dans les locaux d'Axis et sous haute surveillance tandis que la clé publique est embarquée sur les produits Axis. L'intégrité de toute l'image du firmware est assurée par une signature du contenu de l'image. Une signature première vérifie un nombre de signatures secondaires pendant que l'image est décompilée.

3. Prévention de sabotage sur le circuit de logistique

La signature de firmware protège un composant des installations de firmwares dangereux au fil de toutes les mises-à-jour. Que se passerait-il si le produit était modifié par un intercepteur durant son transfert du fournisseur au client final ? Un attaquant qui a un accès direct au produit pendant le transport pourrait effectuer une attaque comme par exemple compromettre la partition de démarrage en passant outre la vérification de l'intégrité du firmware, afin d'en installer un modifié et malveillant avant que le composant ne soit déployé.

3.1 Démarrage sécurisé

Le démarrage sécurisé est un processus d'amorçage constitué d'une validation cryptographique de la chaîne software depuis la mémoire ROM. Comme elle s'appuie sur l'utilisation de firmware signé, la fonction démarrage sécurisé garantit qu'un composant ne pourra démarrer que si le firmware a été validé.

Le processus d'amorçage (voir schéma 3) est initialisé par la ROM de démarrage qui valide le l'unité de chargement démarrage. La fonction de démarrage sécurisé vérifie alors, en temps réel, les signatures embarquées de chaque segment du firmware chargé depuis la mémoire flash. La mémoire de démarrage ROM fait office de racine de confiance et le processus d'amorçage continue tant que chaque signature est vérifiée. Chaque segment de la chaine authentifie le suivant jusqu'à fournir un noyau Linux et un système racine vérifiés.

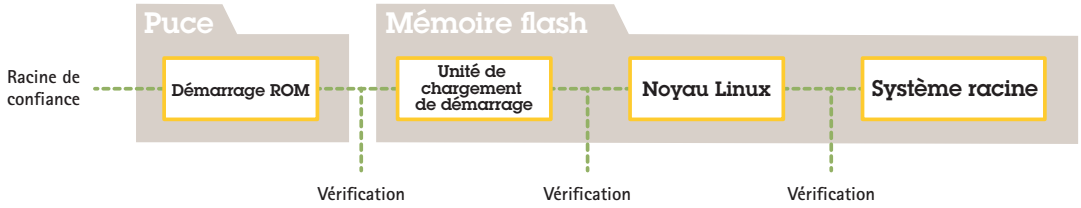

Schéma 3. Le processus de démarrage sécurisé.

3.2 Démarrage sécurisé Axis

Il est capital pour de nombreux produits que leur fonctionnalité basique soit à l'épreuve de toute modification. Quand d'autres mécanismes de sécurité reposent sur le logiciel de base, le démarrage sécurisé constitue le premier rempart au détournement de ces mécanismes.

Pour un produit équipé du démarrage sécurisé, le firmware installé sur la mémoire flash est protégé des modifications. L'image prédéfinie est protégée tandis que la configuration reste sans défense. Le démarrage sécurisé garantit qu'aucun malware ne se trouve dans la caméra après un retour aux paramètres d'usine.

3.3 Démarrage sécurisé et certificats de Custom Firmware

Si la fonction de démarrage sécurisé contribue à rendre le produit plus sûr, il réduit sa capacité d'adaptation, ce qui complique l'installation sur produit de firmwares temporaires comme les firmwares tests ou encore ceux qui ont été faits sur mesure par Axis. Cependant, Axis a implémenté un mécanisme qui autorise les composants individuels à accepter ce type de firmwares hors-production. C'est un firmware signé autrement, avec l'accord du propriétaire et celui d'Axis, ce qui donne un certificat de Custom Firmware. Lorsqu'il est installé sur les composants autorisés, le certificat permet d'utiliser un firmware sur-mesure qui ne fonctionne que sur le composant autorisé, en se référant à son numéro de série et à sa puce ID. Les certificats Custom Firmware ne peuvent être créés que par Axis puisque c'est Axis qui détient la clé nécessaire pour les signer.

4. Sécurité des clés privées

Les produits Axis sont compatibles avec les chiffrements HTTPS (cryptage réseau) et 802.1X (Network Access Control) qui utilisent tous les deux le TLS (Transport Layer Security). Le certificat numérique du TLS utilise une paire clé publique/clé privée. La clé privée est embarquée dans le produit tandis que la clé publique est incluse dans le certificat. Notez que si ni HTTPS, ni 802.1X ne sont utilisés, il n'y a pas de clé à protéger.

Un attaquant pourrait tenter d'extraire la clé privée et le certificat du produit pour ensuite les installer sur son ordinateur. Quand il s'agit d'HTTPS, la clé privée pourrait être utilisée afin d'espionner les échanges cryptés entre la caméra et le VMS via le réseau. Ou bien, en cas d'usurpation du réseau, l'ordinateur de l'attaquant pourrait se faire passer pour une vraie caméra et ainsi accéder au VMS. Quand il s'agit de 802.1X, l'attaquant pourrait utiliser la clé privée pour obtenir un accès à un réseau, même protégé, en se faisant passer pour une caméra.

Les certificats et les clés privées sont généralement stockés dans les fichiers de la caméra, protégés par la police d'accès au compte et utilisés dans l'environnement informatique habituel. Cela suffit la plupart du temps puisqu'un compte n'est pas facilement compromis. Notez que les certificats peuvent être annuler en cas de soupçon de danger, rendant la clé privée inutilisable.

Les utilisateurs qui possèdent un système critique peuvent être soumis à un risque accru d'individus déterminés et compétents qui tentent de s'introduire dans la caméra afin d'en extraire la clé privée. Un TPM stocke la clé de telle façon qu'il devient presque impossible de l'extraire, même si le produit est compromis.

4.1 Stockage de clé sécurisé avec un TPM (trusted platform module)

Un TPM est un composant qui fournit un panel de fonctions cryptographiques destinées à la protection d'information contre les accès non-autorisés. Les clés privées sont stockées dans le TPM et n'en sortent jamais, toutes les opérations cryptographiques qui nécessitent l'utilisation de la clé privée sont plutôt redirigées vers le TPM afin d'y être traitées. Cela assure que la partie secrète du certificat ne quitte jamais l'environnement sécurisé du TPM et reste protégée même en cas de violation de sécurité.

4.2 Certification FIPS 140-2

Suivant les produits et les cas de figure, l'utilisation d'un TPM pour protéger les informations peut être imposée par la réglementation, en plus de l'obligation de répondre aux critères FIPS 140-02. FIPS (Federal Information Processing Standard) 140-02 est un indice de normes de sécurité pour les modules cryptographiques. Aux Etats-Unis ces normes sont décrétées par NIST (National Institute of Standards and Technology).

Passer un test certifié NIST en laboratoire offre la garantit que le système et la cryptographie du module sont implémentées correctement. Pour faire simple, la certification nécessite une description, une précision et une vérification des modules cryptographiques, des algorithmes et des modes opératoires approuvés et enfin des tests de démarrage.

Pour plus d'information sur les critères de certification FIPS 140-02, se rendre sur le site web de NIST : https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards

4.2.1 TPM certifié dans les produits Axis

Le TPM utilisé dans certains des produits Axis est certifié conforme aux critères FIPS 140-02. Plus précisément, il possède une certification de Sécurité Niveau 2, ce qui signifie que le TPM est également conforme pour, entre autres, effectuer une authentification des opérateurs basée sur leur identité et gérer les preuves de sabotage.

73416/FR/R1/1907

À propos d'Axis Communications

En concevant des solutions réseau qui améliorent la sécurité et permettent le développement de nouvelles façons de travailler, Axis contribue à un monde plus sûr et plus clairvoyant. Leader de la vidéo sur IP, Axis propose des produits et services axés sur la vidéosurveillance, l'analyse vidéo, le contrôle d'accès et les systèmes audio. L'entreprise emploie plus de 3000 personnes dans plus de 50 pays et collabore avec des partenaires du monde entier pour fournir des solutions clients adaptées. Axis a été fondée en 1984, son siège est situé à Lund en Suède.

Pour en savoir plus, visitez notre site web www.axis.com

AXIS COMMUNICATIONS