Calypso Networks Association

Communiqué Officiel

12 Mars 2018

Principes de sécurité HCE dans un environnement Calypso

Garant de la sécurité et de l'intégrité des systèmes utilisant la technologie Calypso, CNA a publié la version finale de la *Spécification d'une application HCE Calypso* fondée sur plusieurs prérequis:

1. **Être compatible avec le jeu de commandes Calypso 3.1.**
2. **Être acceptée sur les systèmes billettiques existants sans entraîner d'évolutions majeures sur les équipements déjà opérationnels.**
3. **Garantir le maintien du niveau de sécurité des systèmes Calypso déjà déployés.**
4. **Garantir un niveau de sécurité raisonnable au regard de l'état de l'art Calypso.**

En complément de cette spécification, CNA a édité un guide d'implémentation, *Calypso HCE Guidelines*, qui décrit l'écosystème HCE Calypso et prescrit les contremesures sécuritaires à implémenter. Ce guide s'appuie sur les recommandations d'une étude de sécurité commandée par l'AFIMB, l'Agence Française pour l'Information Multimodale et la Billettique, et réalisée par un expert indépendant de l'Institut Mines-Télécom.

Contrairement à un composant sécurisé, type carte à puce, carte SIM ou eSE, conçu pour protéger des données sur une longue durée, une application HCE d'un téléphone mobile est hébergée dans environnement purement logiciel et ne peut donc assurer leur protection que sur une période limitée. Elle présente des vulnérabilités intrinsèques qui nécessitent d'adopter des contremesures sécuritaires au niveau du système central.

Ainsi, les Calypso HCE Guidelines définissent les exigences de sécurité suivantes:

- Les applications HCE Calypso doivent utiliser une plage spécifique de numéros de séries sur 8 octets. 6 octets sont réservés pour l'identification unique de l'application, et 2 octets pour une date de validité, l'ensemble des 8 octets étant utilisé pour les opérations cryptographiques, notamment la diversification de la clé de débit.

- Une fois la date de validité du numéro de série, et donc de la clé de débit, dépassée, ces éléments doivent être renouvelés via le serveur HCE. La durée de validité maximale du numéro de série d'une application HCE est fixée à 3 jours.
- Les données sensibles telles que les contrats de transport doivent être signées en incluant le numéro de série à 8 octets dans la signature, afin de lier la validité de ces données à celle du numéro de série. Un contrat de longue durée doit donc être signé autant de fois que nécessaire pour rester valide.

Pour se prévaloir de la marque Calypso, tout déploiement de solution HCE doit respecter l'ensemble des prescriptions de ces deux documents, en particulier les contremesures sécuritaires décrites ci-dessus.

Par ailleurs, au niveau des terminaux billettiques, le logiciel de traitement d'une application Calypso HCE doit, en particulier:

- Implémenter la version 3.1 des spécifications Calypso.
- Reconnaître un numéro de série Calypso spécifique HCE et savoir interpréter sa date de validité pour refuser les applications HCE avec un numéro de série périmé.
- Embarquer des SAMs avec des clés TDES et la fonction de signature (avec les clés de signature associées)
- Vérifier la validité de la signature des données de contrats transport.

Télécharger la **Spécification d'une application HCE Calypso**

Télécharger les **Calypso HCE Guidelines, révision 1.0 ***

** Documentation réservée aux membres CNA*

Philippe Vappereau
Président Calypso Networks Association