RSA 2020 : qui veut les clés du Wi-Fi ?

Quel point commun entre un iPhone XR, un Raspberry Pi 3 et une enceinte Amazon Echo 2e génération ?

Tous trois embarquent une puce Wi-Fi touchée par une faille de sécurité.

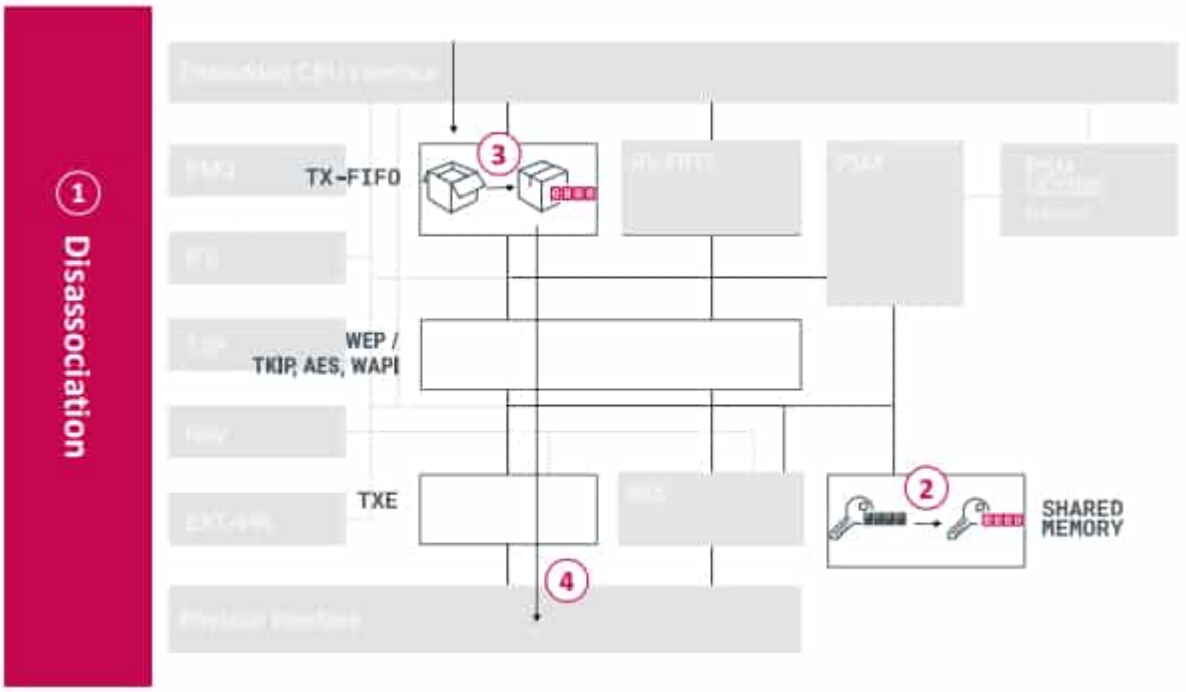
ESET a découvert cette vulnérabilité (CVE-2019-15126) qu'il a baptisée Kr00k et sur laquelle il est revenu dans le cadre de la conférence RSA 2020.

Les puces en question émanent de Broadcom et de Cypress Semiconductor. Elles sont commercialisées essentiellement sous la marque FullMAC WLAN.

ESET a concentré ses recherches sur le protocole WPA2 avec chiffrement AES-CCMP, standard sur les réseaux Wi-Fi modernes.

Chiffrement « zéro »

Le problème observé se manifeste au moment de la dissociation (lorsqu'un terminal se déconnecte d'un point d'accès).

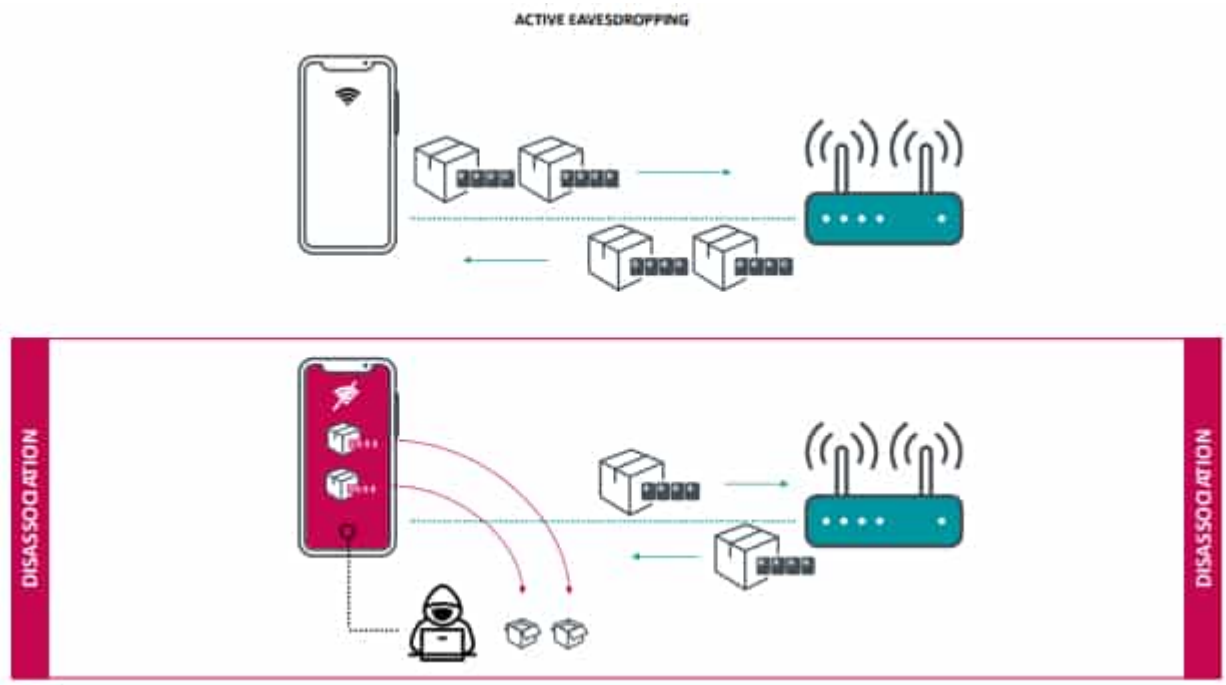


Cette opération entraîne la mise à zéro de la clé de session négociée lors de l'association.

Le souci : sur les appareils vulnérables*, les données non transmises avant la dissociation finissent par l'être… avec pour seule protection cette clé « vide ». Il n'y a plus qu'à récupérer et à déchiffrer les données (quelques kilo-octets à chaque fois).

Le mécanisme est d'autant plus simple à activer qu'on peut envoyer des instructions de dissociation sans avoir besoin de s'authentifier.

Il est, en outre, possible d'intercepter des données sans être connecté au Wi-Fi concerné, en exploitant un contrôleur d'interface réseau en mode moniteur.



Les attaques fondées sur cette faille ne sont réellement effectives que si les données ne sont pas chiffrées au préalable. Or, elles le sont généralement au niveau de la couche de transport (TLS).

Cerberus s'en prend à l'authentification forte

Autre menace signalée en marge de la conférence RSA : le renforcement des capacités de Cerberus.

Le cheval de Troie bancaire, découvert à la mi-2019, est désormais capable de mettre à mal l'authentification forte. Plus précisément, d'intercepter les codes à usage unique que génère l'application mobile Google Authenticator.

** Sur la liste des appareils vulnérables figurent aussi des smartphones Google Nexus, Samsung Galaxy et Xiaomi Redmi. Côté routeurs, ESET mentionne un modèle Asus (RT-N12) et trois modèles Huawei (B612S-25d, EchoLife HG8245H, E5577Cs-321).*

Photo d'illustration © Shutter_M – Shutterstock.com