La nasa à découvert une faille de sécurité réseau qui pourrait affecter le engins spatiaux

Une nouvelle méthode d'attaque a été divulguée contre une technologie cruciale appelée ethernet à déclenchement temporel (TTE) utilisé dans les infrastructures critiques pour la sécurité, pouvant entraîner la défaillance des systèmes alimentant les engins spatiaux et les avions.

Doublé PCspooF par un groupe d'universitaires et de chercheurs Université du Michigan l'Université de Pennsylvanie et le Johnson Space Center de la NASA, le technique est conçu pour briser les garanties de sécurité de TTE et amener les appareils TTE à perdre la synchronisation pendant une seconde, un comportement qui peut même conduire à des manœuvres incontrôlées dans les missions de vol spatial et menacer la sécurité de l'équipage.

TTE est l'une des technologies de mise en réseau qui fait partie de ce qu'on appelle un réseau à criticité mixte dans lequel le trafic avec des exigences de synchronisation et de tolérance aux pannes différentes coexiste dans le même réseau physique. Cela signifie que les appareils critiques, qui, par exemple, permettent le contrôle du véhicule, et les appareils non critiques, qui sont utilisés pour la surveillance et la collecte de données, partagent le même réseau.

Un avantage évident de cette approche est le fait qu'il y a moins de poids et de puissance requis ainsi que des coûts de développement et de temps réduits résultant du fait de s'appuyer sur une seule technologie. Mais cela vient aussi avec ses propres inconvénients.

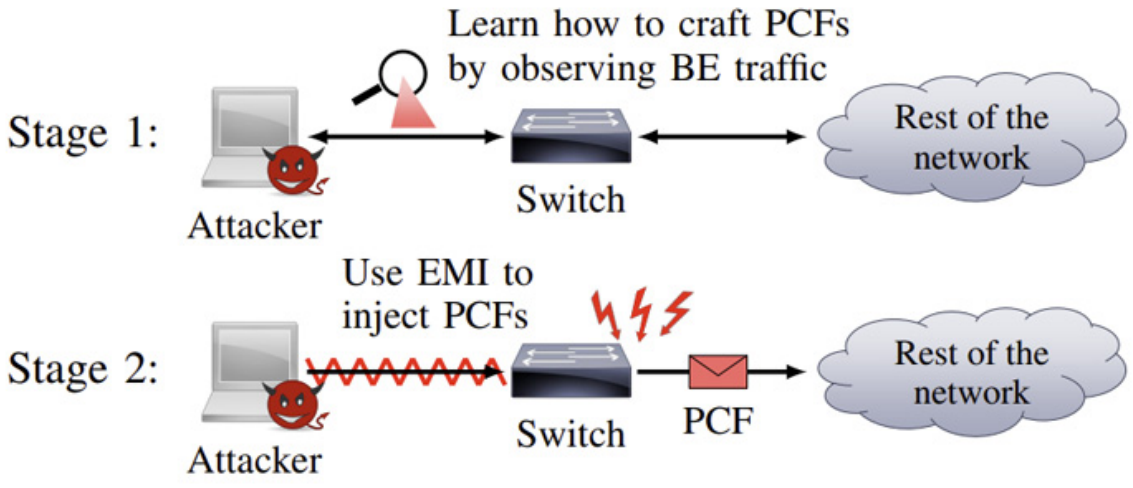


Fig. 3: High-level overview of PCSPOOF.

En plus de cela, alors que les appareils critiques du réseau sont soumis à une vérification approfondie, les homologues non critiques ne sont pas seulement des appareils commerciaux prêts à l'emploi (COTS), mais manquent également du même processus rigoureux, ce qui conduit à d'éventuelles voies d'approvisionnement. des compromis en

chaîne qui pourraient être militarisés pour activer l'attaque en intégrant un composant tiers malveillant dans le système.

C'est là qu'un réseau à criticité mixte aide à garantir que même si le périphérique COTS est malveillant, il ne peut pas interférer avec le trafic critique.

« Dans PCspooF, nous avons découvert un moyen pour un appareil malveillant non critique de briser cette garantie d'isolement dans un réseau TTE », a déclaré Baris Kasikci, professeur adjoint au département de génie électrique et d'informatique de l'Université du Michigan, à la publication.

Ceci, à son tour, est réalisé en utilisant le dispositif néfaste pour injecter des interférences électromagnétiques (EMI) dans un commutateur TTE via un câble Ethernet, incitant efficacement le commutateur à envoyer des messages de synchronisation d'apparence authentique (c'est-à-dire des trames de contrôle de protocole ou PCF) et obtenir acceptés par d'autres appareils TTE.

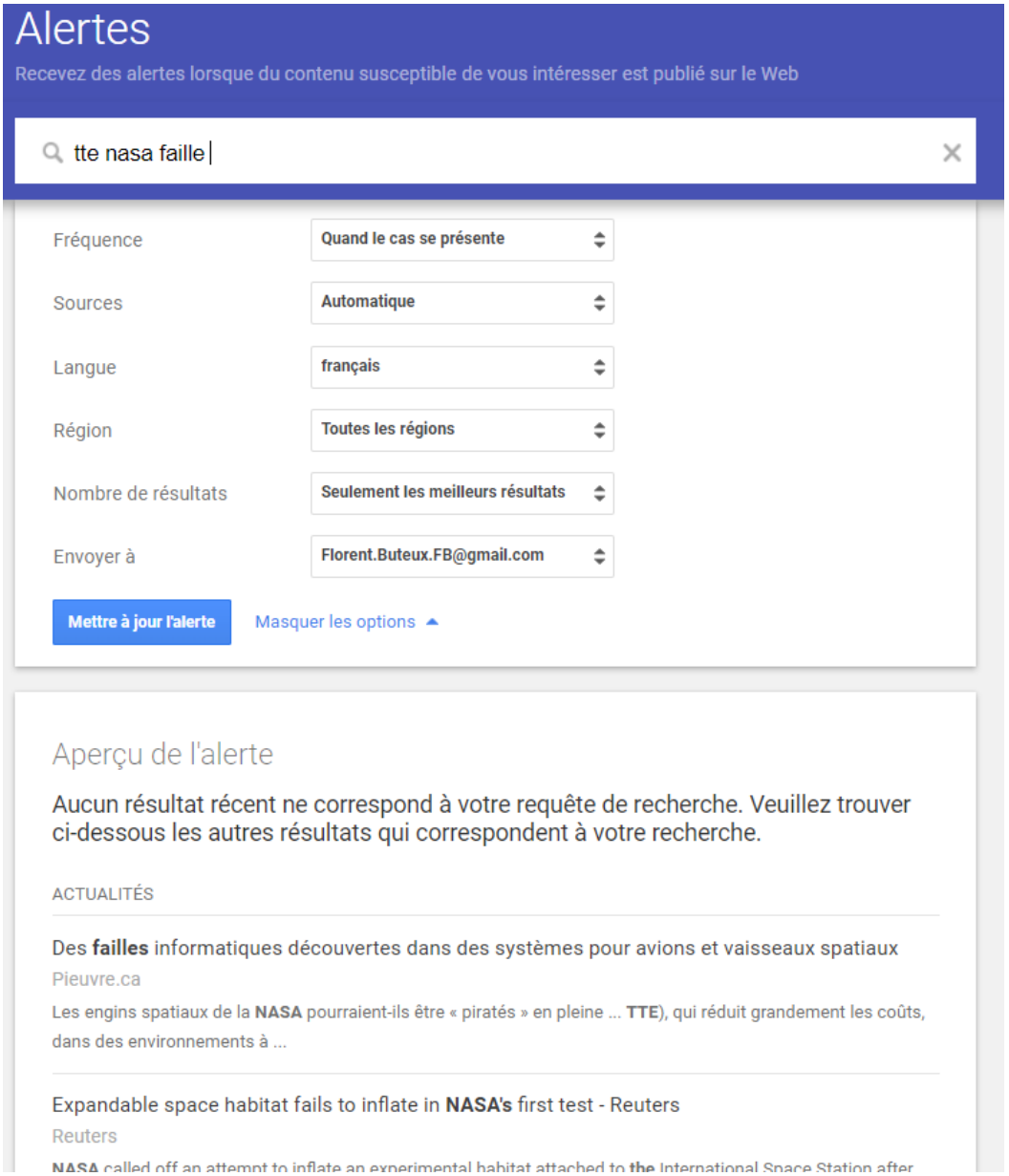
Un tel circuit de génération de « bruit électrique » peut occuper aussi peu que 2,5 cm × 2,5 cm sur une carte de circuit imprimé monocouche, ne nécessitant qu'une puissance minimale et qui peut être dissimulé dans un dispositif au mieux et intégré dans un système TTE sans lever des drapeaux rouges.

Comme mesures d'atténuation, l'étude recommande d'utiliser des optocoupleurs ou des parasurtenseurs pour bloquer les interférences électromagnétiques, de vérifier les adresses MAC source pour s'assurer qu'elles sont authentiques, de masquer les champs PCF clés, d'utiliser un protocole d'authentification de couche de liaison comme IEEE 802.1AE, d'augmenter le nombre de synchronisation maîtres et en désactivant les transitions d'état dangereuses.

Les résultats montrent que l'utilisation de matériel commun dans un système conçu pour fournir des garanties d'isolation strictes peut parfois vaincre ces mêmes protections, ont souligné les chercheurs, ajoutant que les systèmes logiciels à criticité mixte doivent être examinés méticuleusement de la même manière pour s'assurer que les mécanismes d'isolation sont infaillible.

« Les protocoles TTE sont très matures et bien contrôlés, et bon nombre des parties les plus importantes sont formellement prouvées », a déclaré Kasikci.

« D'une certaine manière, c'est ce qui rend notre attaque intéressante – que nous avons pu comprendre comment violer certaines garanties du protocole malgré sa maturité. Mais pour ce faire, nous avons dû sortir des sentiers battus et trouver comment faire le le matériel se comporte d'une manière à laquelle le protocole ne s'attend pas. »



sources :
https://actualnewsmagazine.com/la-nasa-a-decouvert-une-faille-de-securite-reseau-qui-pourrait-affecter-les-engins-spatiaux/
https://teknomers.com/fr/pcspoof-une-nouvelle-vulnerabilite-affecte-la-technologie-de-mise-en-reseau-utilisee-par-les-engins-spatiaux-et-les-aeronefs/