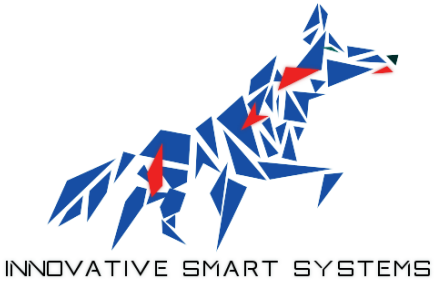
SECURITE IOT

DETECTION PAR BLUETOOTH DES APPAREILS MALVEILLANTS DANS LES STATIONS ESSENCES AUX ETATS-UNIS

https://www.usenix.org/conference/usenixsecurity19/presentation/bhaskar



INSA TOULOUSE

Marc Kassé

2020/2021

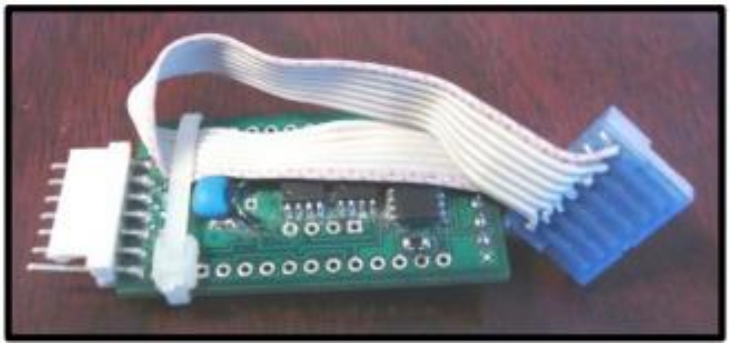
Table des matières

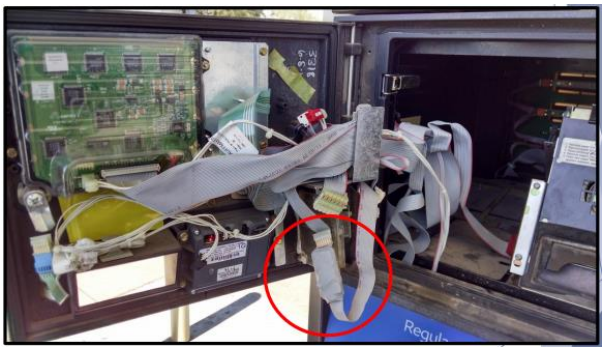
I. Contexte

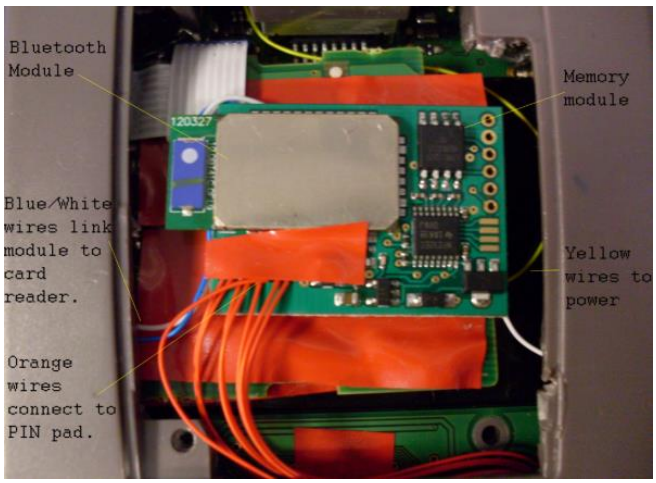
Aux Etats-Unis, le vol de données bancaires dans les stations essence est assez répandu. Les stations essence sont la cible principale. Cela s'explique par la faible sécurité sur les pompes essence. L'ouverture des pompes essence se fait grâce à une clé mécanique assez standard, laissant ainsi accès à toute personne malveillante. L'accès facile à l'électronique permet aux attaquants de fabriquer de simples dispositifs installés sur le lecteur de carte des pompes essences. En France, cette pratique commence à se faire connaitre.

II. Skimmers

Un « skimmer » est un dispositif électronique installé sur des machines de paiement afin de compromettre les données bancaires. La majorité des « skimmers » sont conçus simplement et sont très abordables. Ils sont constitués d'un module Bluetooth et d'une mémoire. Ils sont raccordés au lecteur de carte et au clavier, ainsi qu'à une source de tension.







III. Problématique

Le problème étant connu aux Etats-Unis, une institution se charge de faire des contrôles réguliers afin de repérer ces dispositifs installés. Certaines inspections lors d'opérations de maintenance peuvent permettre également de les identifier. Néanmoins, il est vraiment difficile de les repérer car les dispositifs sont parfaitement intégrés dans le système. Le dispositif est relié au lecteur de carte par une bande magnétique par laquelle sont transférées les données non cryptées de la carte.

Chaque inspection prend environ 30 min alors que les attaquants installent leurs dispositifs en une dizaine de secondes. Le coût pour lutter contre ces fraudes peut devenir faramineux. Cette fraude à la carte bancaire est lucrative pour celui qui installe plusieurs de ces dispositifs. En moyenne, 500$ sont soutiré par carte bancaire. L'attaquant retire l'argent tout de suite après avoir subtilisé les données ou le revend ces mêmes données sur le Dark Web.

Afin de récupérer les données des cartes, les attaquants utilisent différentes méthodes telles que la transmission Bluetooth ou SMS ou la récupération physique. Le Bluetooth est le plus souvent utilisé d'après les données recueillies par la Law Enforcement aux Etats-Unis. L'attaquant se trouve généralement dans un petit périmètre lui permettant de récupérer les données.

IV. Solution

La solution apportée par cet article est une application Bluetana permettant de scanner les appareils Bluetooth et récolter les données envoyées sur une base de données qui est ensuite exploitée. Les données recueillies à chaque scan sont le *type d'appareil, l'adresse MAC et le nom de l'appareil.*

Cette application possède un algorithme permettant d'identifier les dispositifs malveillants et basé sur une liste d'adresses MAC fournie par le Law Enforcement. Cette liste est constituée de 23 adresses provenant des informations remontées lors des inspections faites par le Law Enforcement. Une code couleur permet d'identifier rapidement les appareils suspects. La couleur orange est attribuée aux appareils ayant un même nom d'appareil que sur la liste. La couleur rouge est attribuée aux appareils ayant un type, une adresse et un nom identiques à ceux d'un appareil identifié sur la liste.

V. Avantages de la solution

Des applications existent déjà pour détecter ces appareils malveillants. Cette application Bluetana applique un filtre beaucoup plus précis. En effet, en se basant sur 3 critères différents, le filtre est plus cohérent et permet de limiter les erreurs.

Là où les autres applications ne permettaient pas de repérer que des adresses MAC standards données par IEEE, Bluetana le permet.

L'application permet une mise à jour à distance pour faire évoluer les critères au fur et à fur des données récoltées.

Bluetana permet de réaliser un scan sans se connecter aux appareils détectés volontairement pour ne pas compromettre la continuité de cette étude.

VI. Expérimentation

La durée de l'expérimentation s'étale sur 19 mois. Pendant cette période, 1185 stations ont été passées au crible avec au total 491 stations différentes.

La période de scan s'est étalée de 30 secondes à 5 minutes. Une analyse a permis de démontrer que 80% des dispositifs étaient repérés dans la minute.

La distance qui a été appliquée est de 45m à proximité des stations d'essence.

Le RSSI est récupéré à chaque scan et permet ainsi de réaliser une cartographie des appareils repérés afin d'identifier avec plus grande certitude les dispositifs installés dans les pompes essence.

L'application permet de détecter des dispositifs utilisant un module Bluetooth RN ou HC, modules les plus répandues.

L'analyse des résultats à partir de la base de données a permis de montrer qu'une bonne proportion de dispositifs malveillants sont n'ont aucun type défini :*Uncategorized* (100% des dispositifs malveillants).

L'adresse MAC est souvent celle des constructeurs par défaut qui inscrivent la date dans les 4 premiers octets de l'adresse (YY :YY :MM :DD). Il est donc simple de repérer les dispositifs possédant un module RN ou HC.

Le nom des dispositifs malveillants est en grande majorité celui par défaut. Néanmoins, cela est à relativiser car l'application n'a pas relevé les noms des appareils dans tous les cas car le nom de l'appareil est envoyé dans un deuxième paquet de données après le paquet de données envoyé pour le scan. Par conséquent, ce paquet a pu se perdre parfois.

Ces différents filtres ont permis ainsi d'identifier les appareils suspects et malveillants.

VII. Résultats

Sur une période d'un peu plus d'an an, il été possible de détecter autant d'appareils malveillants que ne l'a fait le Law Enforcement sur trois ans : environ 1.5% des appareils scannés étaient des appareils malveillants. Cela prouve que l'application est efficace.

64 dispositifs ont été détectés par l'application. 22 des dispositifs malveillants repérés ont été retirés de l'étude car ceux-ci réapparaissaient régulièrement au cours des différentes visites. Vu que les appareils malveillants étaient régulièrement retirés alors ces 22 dispositifs devaient être des appareils sains utilisant le Bluetooth.

42 dispositifs malveillants ont été démontés sur la période dont 36 ont été détectés par Bluetana soit un taux de succès de 86%. Ce chiffre s'explique certainement par le fait que les moyens pour récupérer les informations sont différents : récupération physique ou transmission par SMS. Une autre possibilité est que les dispositifs n'étaient pas sous tension.

Le taux d'erreur de l'application est de 5.9%. En effet, certains dispositifs ont été identifiés comme malveillants alors qu'ils ne l'étaient pas. Ce taux s'explique par le fait que nous sommes entourés d'équipements qui utilisent des modules RN ou HC avec un nom par défaut (RNBT-xxxx ou HC-05). Heureusement le RSSI permet de lever les doutes sur les erreurs.

VIII. Analyse

Bien que les résultats soient assez satisfaisants, des limites à cette études peuvent être pointées :

- La solution ne détecte que les appareils utilisant le Bluetooth. L'utilisation du BLE est beaucoup plus massive et il est donc plus compliqué d'identifier des intrus parmi un nombre aussi importants d'appareils qui possèdent aussi certainement des caractéristiques similaires à celles des dispositifs malveillants. La solution serait d'utiliser la valeur du RSSI comme localiser précisément les dispositifs dans cette jungle d'appareils.

- Deuxio, pour réaliser le scan via l'application, il faut que les appareils soient en mode discoverable. Un attaquant pourrait très bien enlever ce mode. Néanmoins, il semblerait que les attaquants utilisent des mules pour récupérer les données par conséquent ce mode ne serait pas avantageux pour eux. Il est tout de même possible de découvrir des appareils non découvrables moyennant des composants plus chers et ça prendrait beaucoup de temps. En effet, un appareil même non découvrable répond aux requêtes qui lui sont adressées à son adresse BD_ADDR. Le temps est long car la taille des BD_ADDR est assez grande.

- Troisièmement, comme vu précédemment, changer les caractéristiques des appareils pourrait permettre aux attaquants de se fondre dans la masse. Même s'il n'y pas d'intérêt pour l'attaquant à le faire, Bluetana peut mettre à jour ses filtres à distance à posteriori, après analyse des donnés. En effet, ce n'est pas si simple de changer l'adresse MAC et cela demande de la programmation que tous les attaquants ne peuvent pas réaliser.

- Enfin, de nouveaux dispositifs commencent à arriver avec des modes de transmission par wifi ou SMS ce qui rend le traçage beaucoup plus compliqué. On pourrait utiliser un SDR pour détecter un réseau GSM et tracer des messages.