Rapport partie théorique CC SRIO

Zoé Costan

Introduction

1 - Debian (distribution Linux) paraît plus sécurisé que Windows sur plusieurs points : premièrement, c'est un système d'exploitation open source, n'importe qui peut donc contribuer au projet et signaler tout problème de sécurité.Il propose également des mises à jour de sécurité fréquentes afin de corriger les failles de sécurité dès qu'elles ont été découvertes. De plus, tous les paquets logiciels sont vérifiés par les utilisateurs avant d'être inclus dans les dépôts officiels de la distribution. On s'assure donc qu'ils ne contiennent pas de logiciels espions ou de codes malveillants. L'accès est aussi limité aux fonctionnalités avancées du système : sous debian les utilisateurs ont un accès limité aux fonctionnalités avancées du système, ce qui peut réduire les risques de compromission du système.

2 - Les principes de sécurité les plus délicats dans le cas de SRIOEYE sont la confidentialité et la disponibilité. La confidentialité car SRIOEYE est une entreprise de maintenance de caméras de surveillance chez des particuliers et dans des lieux sensibles, donc on ne souhaite pas que des personnes extérieures non autorisées aient accès aux données des caméras. La disponibilité car pour que les caméras puissent effectuer correctement leur service qui est un service de surveillance en direct il faut qu'elles soient toujours disponibles.

3 - Le mot que j'utiliserai est le mot "interconnexion". Un équipement interconnecté est exposé à de nombreuses failles : envoi de données obtenues par le capteur et à travers les actionneurs, échange de données avec le cloud ou autres et traitement de données sensibles).

4 - Cela a des conséquences sur les protocoles de sécurité. Les caméras ont un faible stockage et une puissance de calcul limitée, cependant les protocoles de sécurité nécessitent beaucoup de ressources pour être utilisés, ils sont donc négligés dans ce cas.

5 - Lora permet de structurer un réseau étendu à basse consommation (LPWAN), intégrant des équipements terminaux à faible consommation électrique par l'intermédiaire de passerelles. Ce protocole s'adapte donc parfaitement aux équipements de surveillance tels que des caméras qui ne nécessitent pas énormément de ressources. De plus, il permet de transmettre des données sur de longues distances donc cela permet de couvrir de grandes zones. Au niveau de la sécurité, ce protocole utilise un chiffrement de bout en bout pour protéger les données transmises.

Obtention de secret d'architecture

1 - Cette stratégie s'appelle l'ingénierie sociale. C'est une pratique de manipulation psychologique pour parvenir à des fins d'escroquerie, donc d'obtenir des données, des accès ou encore du matériel en manipulant une cible dans le cadre de l'informatique.

Gestion de la base de données

1 - L'algorithme RC4 a un vecteur d'initialisation de 24 bits et la clé de chiffrement est de 488 bits. La longueur de la clé utilisée par les caméras est donc de 512 bits.

2 - Stocker des clés chaque minute revient à stocker 1440 clés par jour (1440 minutes par jour). La clé à une longueur de 512 bits, elle est donc stockée sur 64 octets. 64 x 1440 = 92 160 octets, soit environ 90 MBytes. Le stockage des clés consommera donc 90 MBytes environ.

3 - Le nombre de combinaisons est de 128^512.

4 - Il y a trop de combinaisons (128^512) donc il est impossible d'obtenir la clé en moins d'une minute et il faudrait certainement des années pour l'obtenir par la force brute.

5 -

- 1044 / 16 = 65, reste 4
- 65 / 16 = 4, reste 1
- 4 / 16 = 0, reste 4
  On a : 1044 = 414 en hexadécimal.

- 481 / 16 = 30, reste 1
- 30 / 16 = 1, reste 14 ou E
- 1 / 16 = 0, reste 1
  On a : 481 = 1E1 en hexadécimal

- 844 / 16 = 52, reste 12 ou C
- 52 / 16 = 3, reste 4
- 3 / 16 = 0, reste 3
  On a : 844 = 34C en hexadécimal

- 24/16= 1,reste 8
- 1/16= 0, reste 1
  On a : 24 = 18 en hexadécimal

6 - Réponse commune dans le rapport commun.

7 - Les différentes façons de se protéger d'un Buffer Overflow sont :

- L'activation de canaries dans un système d'exploitation. Les canaries sont des pages mémoires qui sont placées à la fin d'une zone de mémoire afin de détecter les débordements.
- La technique (K)ASLR ou le système va régulièrement changer l'emplacement des adresses de votre tas pour bloquer des attaques liées à l'ancien emplacement.
- Limiter les zones de mémoire avec les droits d'exécution.