Partie Théorique CC de SRIO

Réalisé par:
Yelli Coulibaly

RÉPONSES AUX QUESTIONS

1) *Debian est-il plus sécurisé que Windows?*

Debian est mieux sécurisé qu'un système Windows car c'est un système d'exploitation open source ce qui peut être plus sécurisé que les systèmes propriétaires comme Windows, il gère de façon restreints les droits d'accès, sa maintenance est plus facile, les virus n'affecte que le compte concerné, les utilisateurs ne sont pas les administrateurs et enfin il est beaucoup plus difficile de lancer des programmes en .exe que sur Windows.

2) *Quelle sont les deux principes de sécurité que vous jugez plus délicat*

Selon moi, les deux principes de sécurité les plus délicats à mettre en place sont la confidentialité et l'intégrité.
Les enregistrements collectées par les caméras étant conservés sur des serveurs distant en ligne

3) *Si vous devez résumer en un mot la raison pour laquelle les caméras de SRIOEYE sont vulnérables, quel mot utiliserez-vous ?*

En un mot la raison pour laquelle les caméras de SRIOEYE sont vulnérables est: **Interconnexion**

4) *Pour un équipement IOT comme une caméra connectée à faible puissance, quelles sont les conséquences sur les protocoles de sécurité ?*

Les équipements IOT à faible puissance ont généralement une faible puissance de calcul et une mémoire limitée, ce qui rend difficile la mise en place de certaines mesures de sécurité telles que les chiffrement bout à bout des données et l'authentification forte.
Ces limites auxquelles font face ces équipements ont bien sûr des conséquences sur les protocoles de sécurité telles que:

- une communication peu sécurisées au niveau des échanges de données car ces équipements utilisent des protocoles qui ne sont pas vraiment sécurisé ce qui offre une ouverture aux cyberattaques
- une faible gestion des droits d'accès car ces équipements peuvent ne pas avoir de système de gestion des droits d'accès solide, ce qui peut permettre à des utilisateurs non autorisés d'accéder à des données sensibles.
- Les mises à jour de certains logiciels ne sont pas faites régulièrement, ce qui les rend vulnérables et peut entraîner la non correction de certaines failles de sécurités.

5) *Quelle peut être l'avantage d'un protocole comme LORA pour SRIOEYE ?*

LoRa (Long Range) est un protocole de communication sans fil à longue portée qui est sécurisé et qui a une basse consommation en énergie. Il peut être utilisé dans des applications de réseau de capteurs, de suivi de véhicules, de surveillance de la qualité de l'air, de surveillance de l'environnement, etc.

L'entreprise SRIOEYE étant spécialisée dans la surveillance de grande surface, LoRa pourrait être avantageuse tout d'abord grâce à sa transmission de données à longue portées, sa faible consommation en énergie et est surtout sécurisé car il utilise un mécanisme de chiffrement de bout en bout pour protéger la transmission de données.

6) *Comment appelle-t-on cette stratégie façon d'extirper les informations sur une cible ?*

il s’agit de **l'ingénierie sociale**

7) *Sachant qu'on sait que l'algorithme RC4 est utilisé, quelle est la longueur de la clé utilisée par les caméras ?*

L'algorithme RC4 (ou Rivest Cipher 4) est un algorithme de chiffrement par flux.Dans notre cas ici, la longueur de la clé utilisée par les caméras est de 512 bits avec un vecteur d’initialisation de 24 bits et une clé de chiffrement de 488 bits.

8) La taille en MBytes que consommerons le stockage des clés

On a obtenu précédemment que les caméras utilisent une clé de 512 bits et si elles doivent en changer toutes les minutes, elles devront stocker 1440 clés par jour ce qui correspond à 64 octets en mémoire. Cela signifie que le stockage des clés consommera 1440 * 64 = 92 160 octets, ce qui correspond à environ **90 MBytes.**

9) *le nombre combinaisons pour une attaque de type force brute si on veut deviner la clé utilisée par les caméras*

La clé utilisée par les caméras etant de 512 bits et on suppose qu'elle est composée de caractères alphanumériques (lettres et chiffres), il y a 26 + 10 = 36 caractères possibles (26 lettres de l'alphabet et 10 chiffres). Cela signifie qu'il y a 36 ^ 512 combinaisons possibles.

10) *Avec un CPU cadencé à 2.8 GHz par seconde, pourrais-je réussir à obtenir la clé utilisée par une caméra en moins d'une minute ? Sinon, quelle puissance de calcul me faudrait-il ?*

11) *En hexadécimal, réaliser la conversion des chiffres ci-dessous (en expliquant votre cheminement) : **(1044), (481), (844), (24)***

Le principe est de convertir chaque nombre en binaire c’est-à-dire en base 2. Ensuite regrouper par groupes de 4 chiffres en partant de la droite vers la gauche

puis convertir chaque groupe en décimal si le denier groupe manque de chiffres (3 1 2) on y ajoute des 0.

- 1044 / 16 = 65 avec reste 4
  65 / 16 = 4 avec reste 1
  4 / 16 = 0 avec reste 4

On a donc 1044 = 414 en base hexadécimal

- 481 / 16 = 30 avec reste 1
  30 / 16 = 1 avec reste 14 (E)
  1 / 16 = 0 avec reste 1

On a donc 481 = 1E1 en hexadécimal

- 844 / 16 = 52 avec reste 12 (C)
  52 / 16 = 3 avec reste 4
  3 / 16 = 0 avec reste 3

On a donc 844 = 34C en hexadécimal

- 24/16= 1 avec reste 8
  1/16= 0 avec reste 1

On a donc 24 = 18 en hexadécimal

12) Quelles sont les techniques dans la littérature pour contrer le type de problème que présentaient les deux codes précédents.

Les deux codes précédents présentent un problème de Buffer Overflow. Il existe plusieurs façons de s'en protéger.
La première consiste à activer les canaries dans un système d'exploitation. Ils consiste en une page mémoire placées à la fin d'une zone de mémoire afin de détecter des débordements.
On peut également utiliser la technique Kernel Adress Space Layout Randomization (KASLR), qui consiste à changer régulièrement et aléatoirement l'emplacement des adresses du tas pour bloquer des attaques liées à l'ancien emplacement.
On peut aussi se préserver en limitant les zones de mémoire avec les droits d'exécution.