Rapport de Projet de fin d'études

Patcher l'IoT par intrusion

Soutenance de mi-projet

Alexis Dorian
Département IMA

21 décembre 2017

Table des matières

Introduction

Dans le cadre de mon projet de fin d’étude de cinquième année en Informatique, Micro- électronique, Automatique, j'ai été amené à travailler sur patcher les Iot par intrusion

L'objectif est de lister les différentes failles de sécuriser d'un objet connecter et de voir il elle sont utilisable pour patcher l'objet en question ou dans le cas que le patch n'est pas possible de faire remonter l'information

Ce projet se découpe en une première phase qui consiste a faire un état de l'art approfondit des failles appliquer au Iot pour énumérer le maximum de failles et de trouver les similitude entre elle

dans une seconde phase il s'agira d'appliquer les technique et failles découverte pendant l'etat de l'art a des objet connecter puis essayer de corriger les failles grâce a l'intrusion

IOT

Définition

l’IEEE définit l’IoT comme un « réseau d’éléments chacun muni de capteurs qui sont connectés à Internet »

L’IoT-GSI définit également un objet connecté comme un équipement possédant les sept attributs suivants :

• Capteurs

• Connectivité à Internet

• Processeurs

• Efficacité énergétique

• Coût optimisé

• Fiabilité

• Sécurité

Dans le cadre de mon projet je l'intéresse seulement a l’attribut de la sécurité mais cette attributs peux affecter les autres attributs en altérant la fonctionnement globale

Repartissions des Objet connecter

Les objet connecter sont répartie dans tout les aspect de notre vie actuel donc voici une liste de certain de leurs domaine d'application

Systèmes industriels :

- Armement : drones , chars , avions de chasse
- Automatisation : centrales nucléaire et électrique
- Maintenance prédictive

Transports

- Navires connectée
- Voiture autonomes

Santé

- Dispositifs médicaux dans les hôpitaux : lits, scanners , appareils de radiologie
- Télémédecine
- Implants

Domotique

- Équipement internet
- Surveillance : baby phone
- Sécurité : serrures alarmes
- Capteurs

Services publics

- Transports public intelligents
- Bâtiments connectés

État de l'art

Logiciel couramment utiliser

De type contrôle a distance

ASPXSpy : Peut effectuer l'exécution de commandes à distance, télécharger / télécharger des fichiers, interagir avec des bases de données SQL, interroger des clés de registre, effectuer des analyses de ports

Gh0st RAT Backdoor avec un client graphique et un serveur

Poison Ivy Backdoor avec des capacités d'accès à distance complètes sur un système compromis. A un interface graphique.

Xdoor Backdoor avec fonction d'enregistrement des touches, capture audio / vidéo, transferts de fichiers, proxy HTTP, récupération d'informations système, injection de DLL et exécution de commandes

De type augmentation des privilège

Cachedump Obtient les mot de passe qui sont mises en cache dans le registre Windows

GetHashes Obtient les mot de passe

Gsecdump Obtient les mot de passe

Hookmsgina Obtient les mot de passe

on arrive assez facilement a dresser une liste de telle logiciel il sont présenter sur plusieurs blogs/article comment étant utiliser pour vérifier la sécurité du matériel mais il sont facilement détournable de leurs rôles premiers qui est de vérifier la sécurité du matériel

Attaque possible

Remplacement du firmware : attque la plus simple il suffit d'un accès au périphérique une fois l'attaque effectuer l'accès peut être complet

Attaque de l'homme du milieu :attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis.

Attaque par déni de service : attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser.

Attaque Sinkhole : attaque qui a pour but d'attirer tout le trafic réseaux vers un réseaux informatique compromis qui a pour conséquence d'augmenter la consommation réseaux , ce qui augmente la consommation énergétique des périphériques et réduit la durée de vie du réseau

Attaque Sybil :attaque qui consiste a manipuler une ou plusieurs identités à un instant donnée ont et susceptible d'altérer les données produits par les nœuds et d'atteindre à la confidentialité des données échangées par les utilisateurs Le but de l'attaque est de corrompre la table de routage et réduire l'efficacité des mécanisme de tolérance au fautes

Attaque Wormhole : attaque qui consiste a enregistre les paquets en un point, et les rejouer à un autre

Exploiter une faille de l'objet : attaque au contraire des autre attaque qui vise particulièrement une type d'objet ou un modèle spécifique pour exploiter soit une faille lier au logiciel dans l'objet ou soit soit dans les protocole utiliser

dans le cadre du projet je me concentre sur les attaque pas exploitation de faille

Objet viser

Comme vu dans la partie Repartissions des Objet connecter il y a des objet connecter dans tout les domaine donc je vais lister 2 objet dans chaque catégorie pour montrer que tout catégorie sont affecter

Systèmes industriels :

- Gps navire de guerre
- Fusil connecté

Transports

- Jeep Cherokee
- Tesla Model S

Santé

- Brosse à dents
- Pacemaker

Domotique

- Lix Wi-Fi de Philippe
- Cayla poupée connectée

Services publics

- Transport San Francisco
-

Autre :

- Svakom Siime Eye

Protection possible

Modifier les configuration par défaut de l'objet : la protection la plus simple mais l'une des plus efficace reste de changer la configuration par défaut de l'objet pour éviter de garder les mots de passe et identifiant par défaut

Mettre a jour l'objet : il faut maintenir si il et possible l'objet le plus possible a jour sur des version ou il n'y pas de grosse failles de sécurité connus

Vérifier son entourage : l'objet a protéger n'évolue pas tout seul il peux être entourer d'un ou plusieurs autre périphérique qui eux sont compromis et qui peuvent essayer de corrompre l'objet en lui envoyant des fausse information

Conclusion

Pour le moment le projet avance petit à petit le fait de ne faire que des recherche ne me donne pas une réelle impression d'avance car même si des découverte de nouvelle technique / faille de sécurité et très intéressant mais sans pourvoir réellement pouvoir les appliquer rend l'interer moindre