Projet : Ingénierie des réseaux mobiles et IoT

1. Bluetooth5
2. Identifions les différentes attaques possibles :

Les attaques sont classés en deux catégories : les attaques passives qui sont des attaques ou un attaquant écoute simplement le trafic Bluetooth sans interagir avec les appareils Bluetooth et les attaques actives sont des attaques où un attaquant interagit avec les appareils Bluetooth pour obtenir des informations ou effectuer une action malveillante

* Attaque Bluesnarf : Les attaques Bluesnarf sont l'un des types de frappe Bluetooth les plus répandus. Le protocole OBject EXchange (OBEX) est utilisé pour importer la carte d'appel et d'autres éléments. Avec une requête GET OBEX, l'assaillant a accès à toutes les données de l'appareil de la cible si le logiciel chauffeur Bluetooth de la victime est installé par erreur. Cette solution ne nécessite généralement pas d'authentification, de sorte que toute personne peut l'utiliser.
* Attaque d'ingénierie sociale BlueBump :Cette attaque nécessite une certaine conception sociale. L'essentiel est de fournir une connexion sûre avec la victime. Ceci est faisable avec une carte de tâches virtuelle ou un transfert de documents. Si, après un transfert, la cible vous a ajouté à la liste des outils sur lesquels elle compte, l'agresseur lui demandera alors de supprimer le truc de connexion sans rompre la connexion. Ayant effectivement supprimé ce dernier, et n'étant pas non plus consciente que l'adversaire est toujours lié, la victime poursuit son entreprise habituelle. L'agresseur, quant à lui, demande une nouvelle clé en utilisant sa connexion existante. Par conséquent, l'appareil de l'agresseur réintègre la liste de confiance de la cible sans authentification, et l'agresseur peut accéder au gadget jusqu'à ce que la victime désactive cette clé.
* Attaque de BlueChop : c’est un phénomène qui menace la sécurité des réseaux informatiques et des données personnelles. Il s'agit d'une attaque par déni de service distribué (DDoS) qui vise à saturer les serveurs et à les rendre inaccessibles. Pour lutter contre cette menace, il existe plusieurs solutions possibles. Voici quelques exemples

## Attaque du chuchoteur de véhicule : Dans cette attaque, les assaillants utilisent des codes PIN qui arrive par défaut sur les radios Bluetooth des véhicules. Les appareils se connectent aux véhicules en reproduisant un téléphone. Après s'être connectés, ils peuvent diffuser des bruits provenant des systèmes de musique des véhicules et prêter attention au microphone. C'est peu fréquent mais peut tout à fait se produire, et à une distance surprenante.

1. Solutions pour chaque attaque

* Attaque par Bluesnarf : Pour se protéger contre Bluesnarfing, vous pouvez désactiver la fonction Bluetooth de votre téléphone lorsque vous ne l'utilisez pas. Vous pouvez également activer la fonction de visibilité limitée pour empêcher les appareils inconnus de se connecter à votre téléphone. Enfin, vous pouvez utiliser des applications de sécurité pour détecter et prévenir les attaques de piratage.
* Attaque d'ingénierie sociale BlueBump :

- Sensibiliser les employés aux risques de l'ingénierie sociale et aux signes d'une tentative d'attaque. Par exemple, se méfier des appels, des e-mails ou des messages non sollicités demandant des informations personnelles, des mots de passe ou des codes d'accès.

- Renforcer les politiques de sécurité de l'information et les procédures d'authentification. Par exemple, utiliser des mots de passe forts, changer régulièrement de mot de passe, ne pas partager son mot de passe avec personne, vérifier l'identité de son interlocuteur avant de divulguer des informations confidentielles.

- Mettre en place des systèmes de détection et de prévention des intrusions. Par exemple, surveiller les activités suspectes sur le réseau, bloquer les adresses IP ou les domaines malveillants, signaler les incidents de sécurité aux responsables.

* Attaque de BlueChop :

- Utiliser un pare-feu ou un système de détection d'intrusion (IDS) pour filtrer le trafic entrant et bloquer les requêtes suspectes ou malveillantes.

- Recourir à un service de protection DDoS qui offre une capacité de bande passante supérieure à celle de l'attaquant et qui peut rediriger le trafic vers des serveurs de secours.

- Renforcer la sécurité des appareils connectés au réseau, notamment en mettant à jour les logiciels, en utilisant des mots de passe forts et en évitant les liens ou les pièces jointes douteux.

* Attaque du chuchoteur de véhicule :

- Utiliser des dispositifs de protection anti-piratage, comme des brouilleurs de signal, des alarmes ou des verrous électroniques, qui empêchent les hackers d'accéder aux données ou aux commandes du véhicule.

- Mettre à jour régulièrement le logiciel du véhicule, en vérifiant sa provenance et sa fiabilité, pour éviter les failles de sécurité ou les virus qui pourraient être exploités par les pirates.

- Sensibiliser les conducteurs aux risques et aux bonnes pratiques en matière de cybersécurité, comme ne pas laisser son véhicule sans surveillance, ne pas connecter des appareils inconnus au système du véhicule, ou signaler toute anomalie ou tentative de piratage aux autorités compétentes.

1. **Zigbee**
2. Identifions les différentes attaques possibles :

- L'attaque par brouillage : elle consiste à émettre un signal radio de forte puissance sur la même fréquence que Zigbee, afin de perturber la communication entre les nœuds du réseau. Cette attaque peut rendre le réseau inopérant ou réduire sa performance.

- L'attaque par interception : elle consiste à capter les trames Zigbee échangées sur le réseau, afin d'en extraire des informations sensibles, comme les clés de chiffrement, les identifiants des nœuds ou les données applicatives. Cette attaque peut permettre à un attaquant de déchiffrer le trafic Zigbee ou de se faire passer pour un nœud légitime.

- L'attaque par injection : elle consiste à envoyer des trames Zigbee falsifiées sur le réseau, afin de modifier le comportement des nœuds ou de transmettre des ordres malveillants. Cette attaque peut permettre à un attaquant de prendre le contrôle du réseau ou d'induire des actions nuisibles, comme l'ouverture d'une porte ou le déclenchement d'une alarme.

1. Solutions contre ces attaques

- Utiliser un chiffrement fort : il s'agit de rendre le signal incompréhensible pour un tiers qui n'a pas la clé de déchiffrement. Cela permet de se protéger contre l'interception et l'injection, mais pas contre le brouillage.

- Utiliser un codage correcteur d'erreurs : il s'agit d'ajouter des bits redondants au signal, afin de pouvoir détecter et corriger les erreurs dues au bruit ou à l'injection. Cela permet de se protéger contre l'injection, mais pas contre l'interception ou le brouillage.

- Utiliser un saut de fréquence : il s'agit de changer aléatoirement la fréquence du signal à intervalles réguliers, afin de rendre difficile le suivi et le brouillage du signal. Cela permet de se protéger contre le brouillage, mais pas contre l'interception ou l'injection.

1. **UDP**

# Attaques possibles du protocole UDP et les solutions à chaque attaque

Le protocole UDP (User Datagram Protocol) est un protocole de communication qui permet d'envoyer des données sans établir de connexion préalable ni vérifier l'arrivée des paquets. Il est utilisé pour les transmissions sensibles au facteur temps, comme la lecture de vidéos ou les recherches DNS. Cependant, il présente aussi des vulnérabilités qui peuvent être exploitées par des attaquants.

## Attaque par réflexion

Une attaque par réflexion consiste à usurper l'adresse IP d'une victime et à envoyer des paquets UDP à des systèmes tiers, qui vont répondre à la victime en pensant qu'elle a initié la communication. Cela peut générer un trafic important qui va saturer la bande passante ou les ressources de la victime, provoquant un déni de service.

### Solution

Pour se protéger contre ce type d'attaque, il faut filtrer les paquets UDP entrants dont l'adresse source ne correspond pas à un système autorisé ou attendu. Il faut aussi limiter le nombre de paquets UDP sortants vers des systèmes tiers, notamment ceux qui offrent une amplification du trafic (comme memcached).

## Attaque par écoute

Une attaque par écoute consiste à intercepter les paquets UDP échangés entre deux systèmes, en se plaçant sur le chemin du réseau ou en modifiant le routage des datagrammes. Cela permet à l'attaquant d'accéder aux données transmises en clair, voire de les modifier ou de les injecter.

### Solution

Pour se protéger contre ce type d'attaque, il faut chiffrer les données envoyées par UDP, en utilisant par exemple le protocole DTLS (Datagram Transport Layer Security) ou le protocole IPsec (Internet Protocol Security). Il faut aussi authentifier les systèmes communicants, en utilisant par exemple des certificats numériques ou des clés partagées.