Création d’un keylogger

# Initialisation du projet

Un keylogger est un intermédiaire USB que nous allons brancher entre un clavier et un ordinateur. Le but est de récupérer les touches qu’un utilisateur va appuyer sans que cela ne soit détecté par le système.

Avant d’initier le projet, nous devons rappeler que la création et la possession d’un keylogger n’est pas interdit, ce qui est juridiquement illégale, c’est l’utilisation de ce système dans des circonstance autres que sur des appareils que nous possédons. Ce document permet de suivre les étapes que nous avons réalisés pour faire un keylogger, mais en aucun cas ce projet ne doit être détourné à des fin nuisible ou illégale.

Maintenant que nous avons fait un peu de prévention, nous pouvons commencer les explications du projet. Comme nous l’avons mentionné précédemment, l’objectif est de pouvoir construire un intermédiaire entre un clavier et un ordinateur. Pour cela, nous avons commencé nos recherches sur les câblages USB pour pouvoir faire un intermédiaire. Le câblage de l’intermédiaire doit être réalisé de cette manière.

Une image contenant capture d’écran, ligne, diagramme, conception

Description générée automatiquement

Nous avons sur les pins à l’extrémité la masse et l’alimentation en 5 volt. Puis les connecteurs au centre sont utilisés pour transmettre les données. Nous avons les données transmis en polarité positive à le second qui a une polarité négative. Les données sont transmises en série.

# Première version du keylogger

Avec le schéma de la partie précédente, nous avons commencé le montage électrique pour pouvoir réaliser l’intermédiaire. Nous disposions d’un connecteur USB-A mâle et femelle.

Une image contenant intérieur

Description générée automatiquement

Nous avons ensuite soudé des câbles en respectant les couleurs que nous avions définie sur le schéma pour que les connecteurs puissent continuer à transmettre les données. Nous avons utilisé une planche qui permet de connecter des éléments sans soudure pour connecter les deux connecteurs entres eux.

Une image contenant fils électriques, Appareils électroniques, Ingénierie électronique, câble

Description générée automatiquement

A cette étape, nous pouvons vérifier que les connecteurs sons bien branché en connectant un clavier à un ordinateur (un vieil ordinateur pour ne pas causer de problème sur nos machine) pour être sûr que le clavier continue à fonctionner ce qui nous permettras de continuer.

En branchant le clavier à un ordinateur avec cet intermédiaire, nous avons vérifié que le clavier fonctionnait. Ensuite nous avons ajouter une carte Arduino qui récupère les fils D+ et D- sur des broches digitales. Nous avons essayé de comprendre ce qu’il se passais dans la transmission et nous nous sommes rendu compte qu’il aurait fallu implémenter le protocole USB dans l’Arduino pour pouvoir réaliser ce projet. Par manque de temps, nous avons changé notre fusil d’épaule. La seconde partie de ce rapport indique la méthode utiliser pour ne pas à avoir à implémenter le protocole USB.

# Seconde version du keylogger

Pour cette seconde version du keylogger, nous disposons d’une carte Arduino Leonardo, un ESP32 DEVKIT V1. L’objectif est de récupérer les touches appuyer du clavier avec l’ESP32 pour les transmettre à la carte Leonardo, ainsi qu’à distance en wifi. Le schéma de l’installation est représenté ci-dessous.

Une image contenant capture d’écran, conception

Description générée automatiquement

Sur cette représentation, nous avons en rouge le keylogger, et en gris les éléments matériels de la cible. Le choix d’utiliser un Arduino Leonardo est pour le fait que nous pouvons virtualiser un clavier avec celle-ci. L’ESP32 possédé déjà un module Wifi, et le port série peut être utilisé pour recevoir des touches d’un clavier.