Keylogger Sans Fil

Faite-le vous-même !

Introduction

Connaissez-vous la notion de keylogger matériel ? Le keylogger matériel est une solution parfaite servant à surveiller les activités de l'utilisateur d'un ordinateur avec un très faible risque de détection. Le keylogger matériel est un appareil électronique à 100%, il ne nécessite donc pas d'accès à un système d'exploitation, ne laisse aucune trace et aucun logiciel ne peut détecter un appareil de ce type. Le principe de keylogger matériel a pourtant un défaut : afin de récupérer les données enregistrées, il faut avoir un accès physique au keylogger. Une solution de ce problème a enfin été trouvée : Keylogger Sans Fil.

KeeLog a déjà publié un projet accessible au public, celui d'un keylogger matériel PS/2 Open Source. Maintenant, nous faisons la même chose pour le projet du Keylogger Sans Fil à monter soi-même. Ce projet peut être utilisé aussi bien à des fins privées que commerciales sous les réserves suivantes :

1. Tous les matériaux présentés sur ce site Internet constituent la propriété intellectuelle de la société KeeLog et l'utilisation de ceux-ci implique l'acceptation des conditions ci-dessous ainsi que de l'Accord d'Utilisateur général.
2. Ce projet de Keylogger Sans Fil a été publié " en l'état ", avec tous les vices et sans aucune garantie.

Le Keylogger Sans Fil ne doit pas être utilisé afin d'intercepter d'une manière illégale les données d'autrui notamment les mots de passe, les coordonnées bancaires, la correspondance confidentielle etc. Cela constitue une violation de la loi dans la plupart des pays.

Le Keylogger Sans Fil se compose de deux pièces principales : d'un émetteur et d'un récepteur. La journalisation des frappes est faite par l'émetteur qui est en effet un keylogger matériel PS/2 avec un module Wifi 2.4 GHz incorporé. Les données captées ne sont pas stockées dans la mémoire, mais transmises en temps réel par les ondes radio. D'autre part, le récepteur est une unité d'acquisition sans fil avec une interface USB. Toutes les données issues de l'émetteur sont envoyées vers l'ordinateur via USB. Du point de vue du logiciel, ces données passent à travers un port COM virtuel ce qui permet d'utiliser n'importe quel client terminal pour les visualiser.

Keylogger Sans Fil - schéma-bloc

Tout le système fonctionne en temps réel, un texte écrit sur l'ordinateur à distance est donc tout de suite visible du côté du récepteur. Ce système a une portée maximale d'environ 50 mètres. Cela équivaut à une portée efficace d'environ 20 mètres à travers 2-4 parois selon leur épaisseur.

Keylogger Sans Fil - émetteur

Keylogger Sans Fil - récepteur

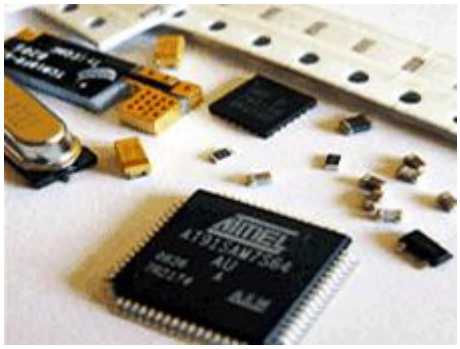
Aussi bien l'émetteur que le récepteur sont basés sur les mêmes schémas électriques et circuits imprimés. Les deux ont les mêmes dimensions et sont conçus pour être montés sur des câbles de rallonge PS/2 et USB. Il est recommandé d'utiliser des boîtiers de filtres de type EMC pour que l'appareil ressemble à un adaptateur ou un câble de rallonge standard.

Composants

Cet article décrit tout les processus d'assemblage du Keylogger Sans Fil. Selon vos capacités, vous pouvez vous décider à créer vous-même votre Keylogger Sans Fil à partir de zéro ou commander ses composants chez nous. Nous pouvons vous fournir un kit électronique avec des microcontrôleurs préprogrammés et des boîtiers standard (voir les photos) ou un kit d'appareils déjà assemblés et testés. Pour plus de détails, consultez la section kits.

Si vous vous êtes décidé à créer vous-même votre Keylogger Sans Fil, vous devez disposer d'une expérience de base dans le domaine de l'électronique et du brasage, de préférence, du montage en surface (TMS). L'option la plus courte consiste à commander les composants chez nous et à réaliser vous-même le brasage, le câblage et l'assemblage final. Vous devrez alors disposer d'un fer à souder avec réglage de température et savoir braser. Si vous vous êtes décidé à faire vous-même le projet et à réaliser des circuits imprimés, vous aurez besoin d'une solide expérience et d'un matériel approprié.

Dans le tableau ci-dessous vous trouverez la liste des composants (BOM) indispensables pour réaliser un émetteur ou un récepteur. Une rallonge PS/2 supplémentaire est nécessaire pour un émetteur tandis qu'un récepteur nécessite un câble USB avec connecteur A.



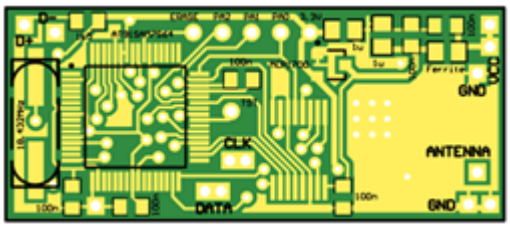
Kit électronique

Câbles, boîtier et circuits imprimés

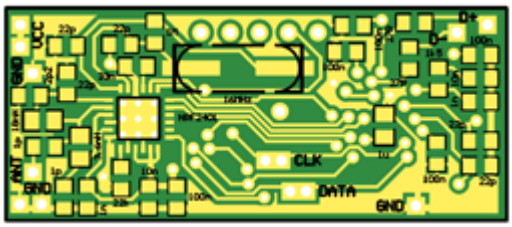
Indicateur	Description	Boîtier	Quantité
U1	Microcontrôleur AT91SAM7S64	TQFP64	1
U2	Émetteur-récepteur nRF2401	QFN24	1
U3	Régulateur de tension MCP1700T-330	SOT-23	1
Q1	Quartz 18.432 MHz	HC-49 SMD	1
Q2	Quartz 16 MHz	HC-49 SMD	1
R1, R2	Résistor 1.5 kΩ	0805	2
R3, R4	Résistor 27 Ω	0805	2
R5	Résistor 1 MΩ	0805	1
R6	Résistor 22 kΩ	0805	1
C1, C27	Condensateur 10 nF	0805	2
C2, C28	Condensateur 1 nF	0805	2
C3, C4, C6, C7, C8	Condensateur 22 pF	0805	5
C5	Condensateur 33 nF	0805	1
C9	Condensateur 2.2 pF	0805	1
C10, C11	Condensateur 1 pF	0805	2
C12, C22, C23, C24, C25, C26, C32, C33, C34, C42, C43	Condensateur 100 nF	0805	11
C21, C31, C41	Condensateur 1 µF	0805	3
L1	Bobine d'arrêt	0805	1
L2	Bobine d'induction 3.6 nH	0805	1
L3	Bobine d'induction 18 nH	0805	1

Keylogger Sans Fil - liste des composants

Aussi bien l'émetteur que le récepteur utilise le même circuit imprimé et le même kit électronique (les câblages et les micrologiciels sont différents). Un microcontrôleur Atmel AT91SAM7S64 et un émetteur-récepteur radio nRF2401 sont les composants clés. Les deux nécessitent des quartz pour bien fonctionner. Tous les composants (résistors, condensateurs et les bobines), sauf la bobine d'arrêt MCP1700, sont passifs. Un simple fil de métal est recommandé pour servir d'antenne dipôle. Sur les figures ci-dessous vous trouverez le circuit imprimé double face à deux couches.

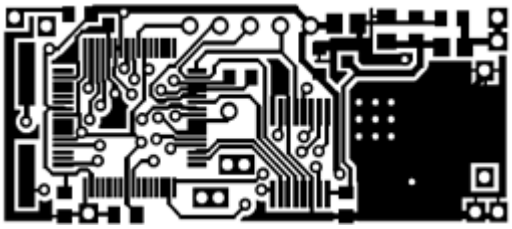


Vue du circuit imprimé / Topologie - face supérieure

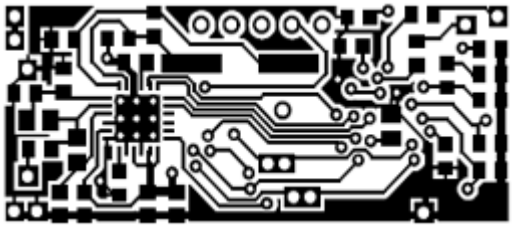


Vue du circuit imprimé / Topologie - face inférieure

Si vous disposez d'assez d'expérience pour réaliser vous-même les circuits imprimés, vous pouvez utiliser les masques à l'échelle de 1:1 disponibles ci-dessous. Le projet de référence utilise le FR4 de 1 mm d'épaisseur.



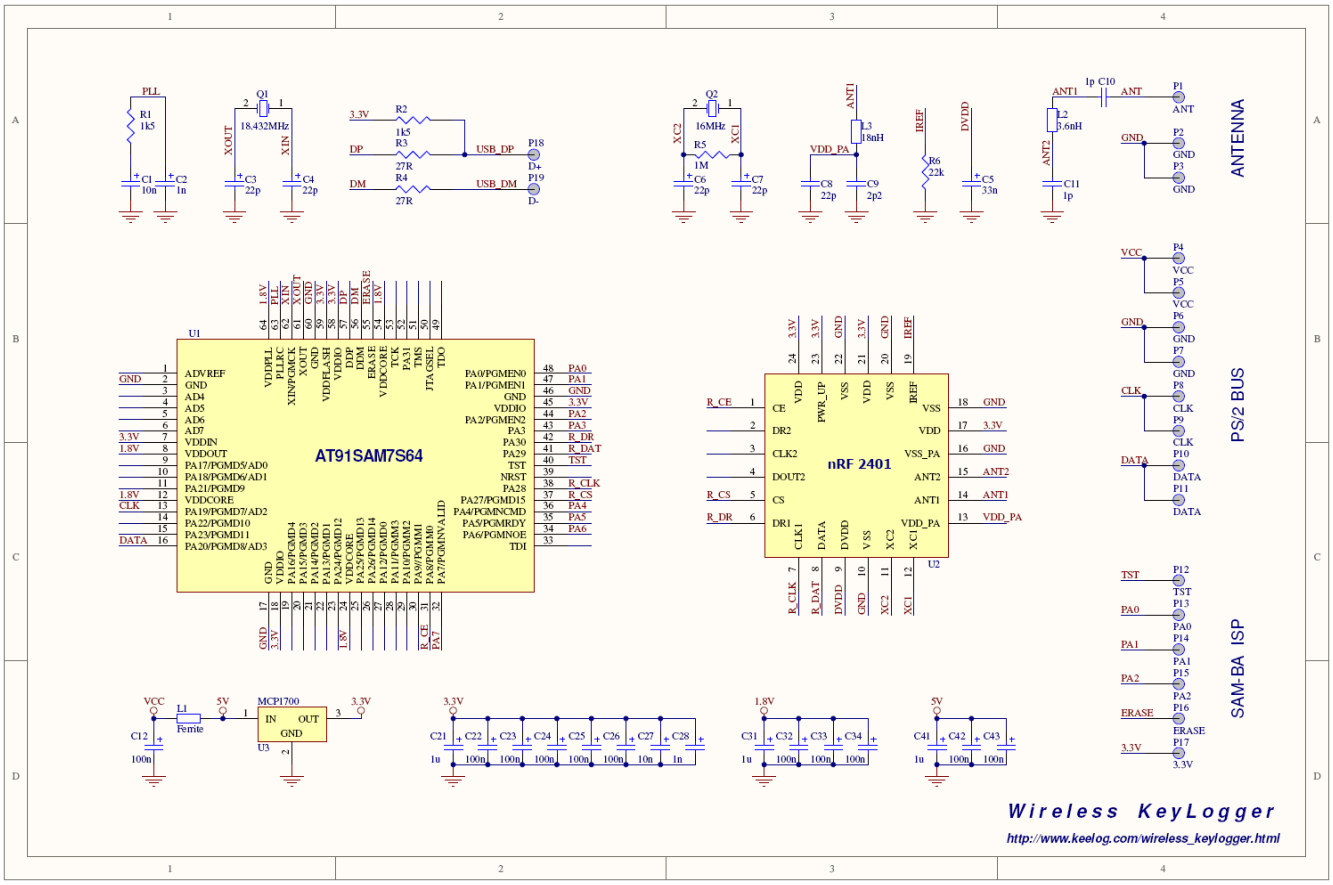
Masque du circuit imprimé - face supérieure



Masque du circuit imprimé - face inférieure

Montage

Le circuit du Keylogger Sans Fil contient deux composants principaux : un microcontrôleur AT91SAM7S64 et un émetteur-récepteur nRF2401. Les éléments passifs qui les accompagnent c'est avant tout un quartz et des circuits RF. Tout le circuit est alimenté par une tension de 3.3V générée par un régulateur de tension MCP1700 et filtrée par un ensemble de condensateurs. L'alimentation d'entrée provient directement du bus PS/2 (émetteur) ou USB (récepteur). Si vous disposez déjà des circuits imprimés assemblés, consultez la section câblage. Si vous vous êtes décidé à tout assembler vous-même, les indications et le schéma électrique ci-dessous peuvent vous être utiles.



Keylogger Sans Fil - schéma électrique

Pour braser, utilisez un fer à souder avec une panne fine (d'habitude de moins de 0.5 mm) et de la pâte à souder (par exemple RMA7). Faites attention à ne pas surchauffer les éléments pendant le brasage. Commencez l'assemblage par l'émetteur-récepteur nRF2401 dont le schéma est le plus compliqué. Passez ensuite au microcontrôleur AT91SAM7S64 et au régulateur de tension MCP1700. Faites attention que la broche numéro 1 corresponde à la première pastille du circuit imprimé. Enfin, brasez tous les circuits supplémentaires : quartz, résistors, condensateurs et bobines. L'antenne sera la dernière. Vous pouvez utiliser une antenne dédiée à ISM 2.4 GHz ou utiliser un morceau de fil de métal pour faire une simple antenne dipôle quart d'onde. La longueur optimale est de 3.125 cm (1.23"). Une fois assemblés, les circuits imprimés doivent ressembler à ceux figurant sur les photos ci-dessous.

Circuit imprimé assemblé - face supérieure avec microcontrôleur

Circuit imprimé assemblé - face inférieure avec émetteur-récepteur

Après avoir assemblé les circuits imprimés, il faut réaliser le câblage. Mis à part le micrologiciel, c'est le point qui fait la différence entre l'émetteur et le récepteur. L'émetteur et le bus PS/2 doivent être couplés en parallèle. Le circuit imprimé de l'émetteur est doté de pastilles qui permettent d'y braser des conducteurs menant aussi bien vers l'ordinateur que vers le clavier. Le récepteur doit par contre être normalement raccordé au port USB. Les photos ci-dessous montrent comment réaliser tous les raccordements.

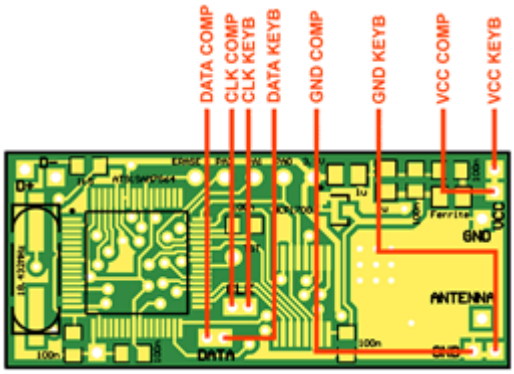


Schéma de câblage PS/2 de l'émetteur

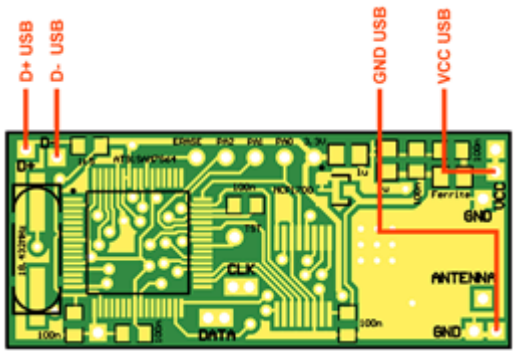
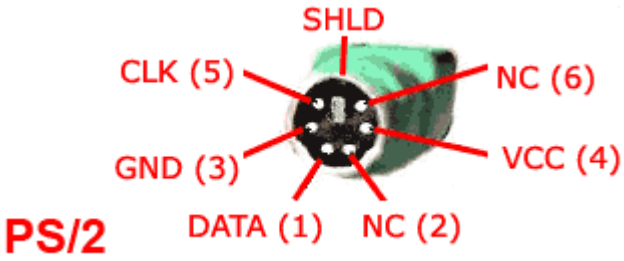


Schéma de câblage USB du récepteur

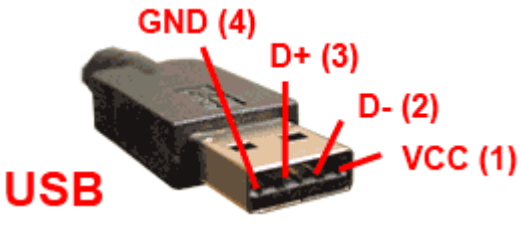
Utilisez des rallonges PS/2 et USB, coupez-les en deux et isolez les conducteurs de signal. Ce qui peut s'avérer compliqué c'est reconnaître quel conducteur correspond à quel signal. Certains câbles PS/2 et USB ont les couleurs standardisées, mais on ne peut pas s'y fier. Il est recommandé d'utiliser un capteur de courant ou un ohmmètre pour savoir quel conducteur correspond à quel ligne de signal. Les schémas ci-dessous peuvent vous être utiles.

Signal	Description	Connecteur PS/2	Commentaire
VCC	Alimentation +5V	4	doivent être raccordés au module
GND	Masse	3	
CLK	Horloge	5	
DATA	Données	1	
NC	Lignes non utilisées	2, 6	ne sont pas utilisés par le module, s'il y en a, laisser à l'état original
SHLD	Armature	-	



Connecteur PS/2 (émetteur)

Signal	Description	Connecteur USB	Commentaire
VCC	Alimentation +5V	1	doivent être raccordés au module
D-	Données	2	
D+	Données	3	
GND	Masse	4	
SHLD	Armature	-	ne sont pas utilisés par le module, s'il y en a, laisser à l'état original



Connecteur USB (récepteur)

Si les microcontrôleurs que vous utilisez n'ont pas encore été programmés, c'est le bon moment de les programmer in-situ (ISP : In-System Programming). Pour plus de détails, consultez la section micrologiciel. Après cette opération, les appareils assemblés doivent ressembler à ceux figurant sur les photos ci-dessous.

Émetteur avec câblage PS/2

Récepteur avec câblage USB

Avant de mettre le boîtier, nous vous recommandons de réaliser le dernier test. Utilisez un capteur de courant ou un ohmmètre pour mesurer la résistance entre l'alimentation (VCC) et la mise à la masse (GND) des connecteurs USB et PS/2. Un court circuit signifie qu'il faut vérifier tout le circuit sinon l'ordinateur risque d'être endommagé. Si tout va bien, fermez le boîtier avec de la colle ou de la résine. Voilà, c'est le moment de brancher votre appareil !

Mise en service

Après avoir assemblé la paire émetteur-récepteur, il est le temps de procéder au premier test. Il est recommandé d'utiliser un seul ordinateur pour tester les deux appareils. Pour commencer, mettez votre ordinateur hors tension et insérez l'émetteur entre le clavier PS/2 et le port PS/2.

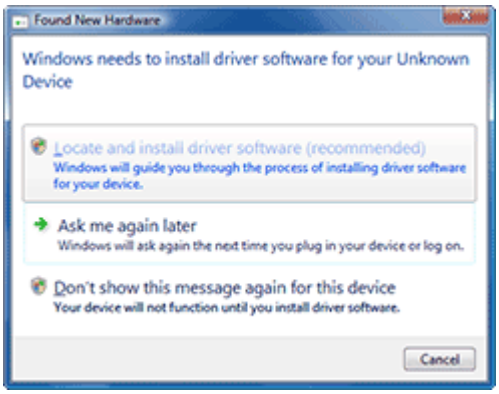
Branchez l'émetteur au port PS/2

Branchez le clavier PS/2 à l'émetteur

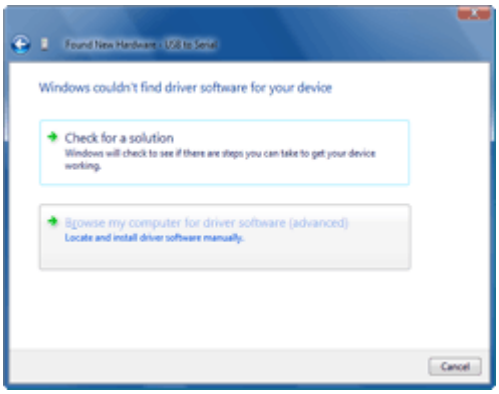
Après, démarrez l'ordinateur et assurez-vous que le clavier PS/2 fonctionne correctement (aucune influence du keylogger n'est perceptible). Ensuite, ce sera le temps de tester le récepteur. Avant, il faut télécharger le fichier du pilote KeeLog. Décompressez et sauvegardez les fichiers sur le disque dur local de l'ordinateur. Puis, branchez le récepteur à un port USB libre (il n'est pas nécessaire de mettre l'ordinateur hors tension). Assurez-vous que le récepteur est placé de manière à pouvoir recevoir la transmission radio de l'émetteur.

Branchez le récepteur à un port USB libre

Quand l'émetteur est branché pour la première fois, vous verrez la fenêtre de l'installateur du pilote. Plus exactement, le système utilisera les pilotes du port virtuel COM fournis avec la plupart des systèmes d'exploitation, comme Windows par exemple. Mais vous devrez sélectionner manuellement le fichier INF approprié. Quand le système vous demandera les pilotes, passez à la localisation des fichiers des pilotes. Les figures ci-dessous illustrent tout ce processus.

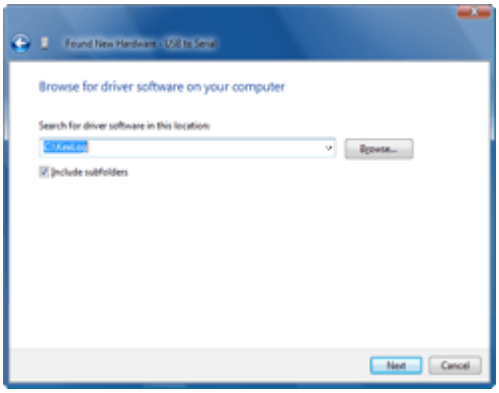


Sélectionnez la localisation et l'installation du logiciel



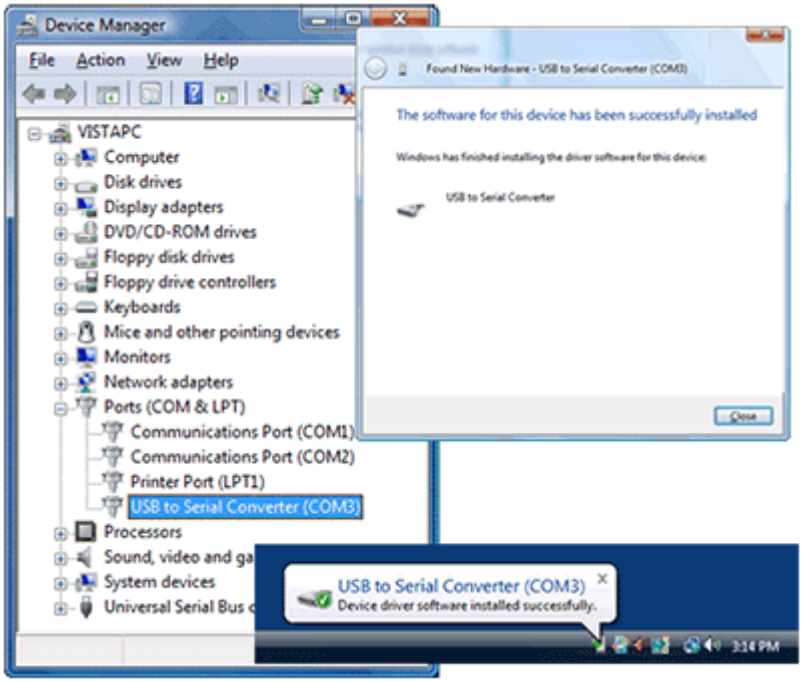
Sélectionnez la localisation du pilote

Sélectionnez pour indiquer l'option de localisation



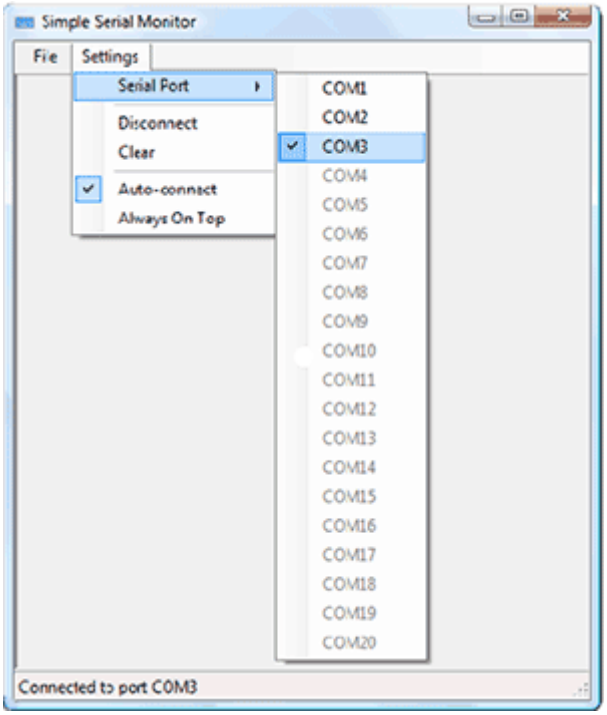
Indiquez la localisation des fichiers du pilote

Une fois le processus d'installation terminé, le récepteur doit être visible comme un convertisseur USB vers Série. Ouvrez le Gestionnaire de périphérique du système Windows pour voir quel port série a été attribué au récepteur.



Récepteur visible dans le Gestionnaire de périphérique

Pour commencer la réception des données envoyées par l'émetteur, on peut utiliser n'importe quel client terminal, comme par exemple Hyperterminal. Nous vous recommandons d'utiliser notre application gratuite Simple Serial Monitor qui est simple et facile à utiliser.



Simple Serial Monitor (client terminal gratuit, fourni par KeeLog)

Après avoir lancé Simple Serial Monitor (ou une application pareille), n'oubliez pas de sélectionner le port COM approprié. Si tout a été correctement fait, le récepteur commencera aussitôt à afficher les séquences des touches frappées sur le clavier PS/2.

Ordinateur distant avec émetteur PS/2 *Ordinateur local avec récepteur USB*

Le pas suivant consiste à réaliser le même test sur deux ordinateurs différents. Assurez-vous qu'ils se trouvent à une distance équivalente à la portée de transmission. Si un texte apparaît dans la fenêtre du terminal, votre Keylogger Sans Fil est prêt à sa première mission sérieuse. N'utilisez cet appareil que conformément à la loi !

Download

Micrologiciel pour le microcontrôleur permettant de programmer l'émetteur et le récepteur
http://www.keelog.com/files/WirelessKeyloggerFirmware.zip

Pilote permettant d'installer le récepteur comme un port virtuel COM
http://www.keelog.com/files/UsbToSerial.zip

Logiciel gratuit permettant d'afficher les séquences des frappes transmises par le port COM virtuel (équivalent de l'application Hyperterminal). Il requiert Microsoft .NET Framework.
http://www.keelog.com/files/SimpleSerialMonitor.zip

Logiciel permettant de programmer le micrologiciel à l'aide de SAM-BA
http://www.keelog.com/files/At91Isp.zip

Manuel de programmation du micrologiciel du microcontrôleur à l'aide d' un bootloader incorporé. Aucun autre logiciel de programmation supplémentaire n'est nécessaire.
http://www.keelog.com/files/SambaUserGuide.pdf

Liste des composants utilisés pour assembler le Keylogger Sans Fil (émetteur et récepteur)
http://www.keelog.com/files/WirelessKeyloggerBom.pdf

Schéma de câblage du Keylogger Sans Fil (émetteur et récepteur)
http://www.keelog.com/files/WirelessKeyloggerWiring.pdf

Schéma électrique du Keylogger Sans Fil (émetteur et récepteur)
http://www.keelog.com/files/WirelessKeyloggerSchColor.pdf

Face supérieure du circuit imprimé (émetteur et récepteur)
http://www.keelog.com/files/WirelessKeyloggerPcbTop.pdf

Face inférieure du circuit imprimé (émetteur et récepteur)
http://www.keelog.com/files/WirelessKeyloggerPcbBottom.pdf

Masque de la face supérieure du circuit imprimé (émetteur et récepteur), échelle 1:1
http://www.keelog.com/files/WirelessKeyloggerMaskTop.pdf

Masque de la face inférieure du circuit imprimé (émetteur et récepteur), échelle 1:1
http://www.keelog.com/files/WirelessKeyloggerMaskBottom.pdf

Micrologiciel

Lisez ce chapitre seulement si vous avez besoin de programmer vous-même le microcontrôleur AT91SAM7S64. Si vous avez acheté un kit chez nous, nous l'avons déjà fait à votre place.

Les microcontrôleurs contemporains comme AT91SAM7S64 se caractérisent par une petite taille et un haut degré d'intégration. Il est donc difficile de trouver un programmateur traditionnel adapté. C'est la raison pour laquelle la Programmation in-situ (ISP - In-System Programming) se développe rapidement depuis quelques années. ISP permet d'assembler d'abord un circuit entier et de programmer ensuite son micrologiciel, souvent à l'aide d'outils très simples. Le microcontrôleur AT91SAM7S64 implémente une solution ISP très pratique basée sur un module USB. Elle s'appelle SAM-BA (SAM Boot Assistant) et ne requiert qu'un câble USB et quelques cavaliers simples. Pour lancer SAM-BA sur le Keylogger Sans Fil, téléchargez d'abord le logiciel AT91 ISP. Ensuite procédez de façon décrite ci-dessous pour charger le micrologiciel dans les modules émetteur et récepteur.

Etape 1 : Concerne uniquement l'émetteur. Préparez un câble USB avec un connecteur de type A mâle d'un côté et des câbles sans isolation de l'autre. Brasez les lignes USB : VCC, GND, D+ et D- aux pastilles correspondantes du circuit imprimé. Cette étape est déjà accomplie dans le cas du récepteur, il a son propre connecteur USB.

Etape 2 : Préparez quelques morceaux de fil de métal courts pour court-circuiter les broches SAM-BA : TST, ERASE, PA2, PA1, PA0, 3.3V. Brasez un bout de chaque fil à la pastille SAM-BA sur les deux platines. Sinon, vous pouvez préparer des cavaliers spéciaux comme sur les figures ci-dessous.

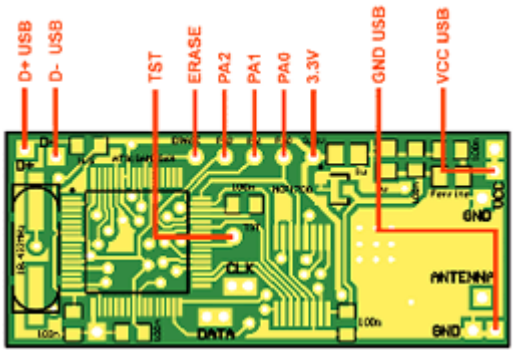


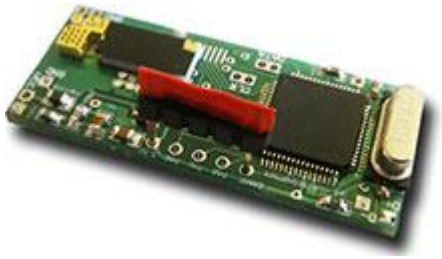
Schéma de câblage SAM-BA

Etape 3 : Installez le progiciel AT91 ISP.

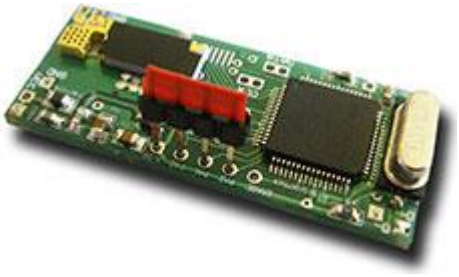
Etape 4 : Branchez l'appareil à un port USB libre. Le message Périphérique non reconnu est normale à cette étape.

Etape 5 : Court-circuitez un instant le connecteur ERASE avec 3.3V. Cela effacera la mémoire flash du microcontrôleur.

Le câble USB et les cavaliers du bootloader SAM-BA



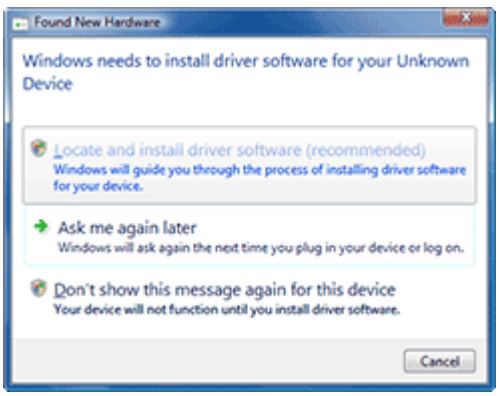
Effaçage de la mémoire (ERASE court-circuité avec 3.3V)



Activation du bootloader (PA0, PA1, PA2 et TST court-circuité avec 3.3V)

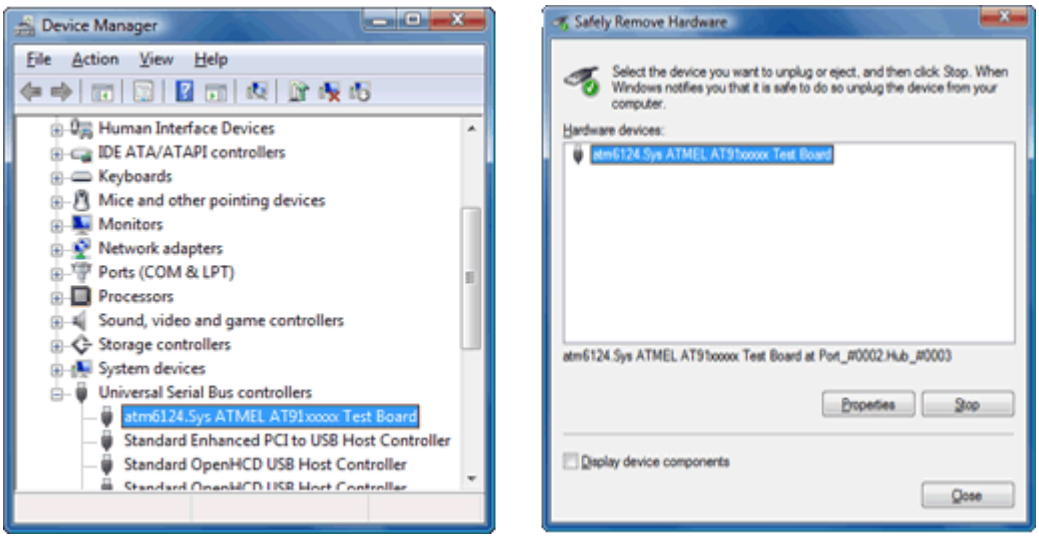
Etape 6 : Débranchez l'appareil du port USB. Assurez-vous que la broche ERASE n'est plus connectée au 3.3V. Ensuite, court-circuitez l'ensemble des broches PA0, PA1, PA2 et TST avec 3.3V. Rebranchez l'appareil au port USB (Périphérique non reconnu peut réapparaître). Laissez l'appareil branché pendant environ 10 secondes, et puis débranchez-le. Cette opération devrait activer le bootloader interne SAM-BA.

Etape 7 : Enlevez tous les cavaliers ou connecteurs et branchez l'appareil au port USB. Le message Nouveau matériel détecté devrait apparaître. Suivez une procédure d'installation standard et laissez le système trouver tous les pilotes.



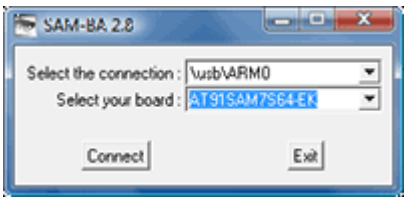
Boîte de dialogue Nouveau matériel détecté

Etape 8 : Lancez le Gestionnaire de périphérique pour vous assurer que le bootloader SAM-BA a été activé.



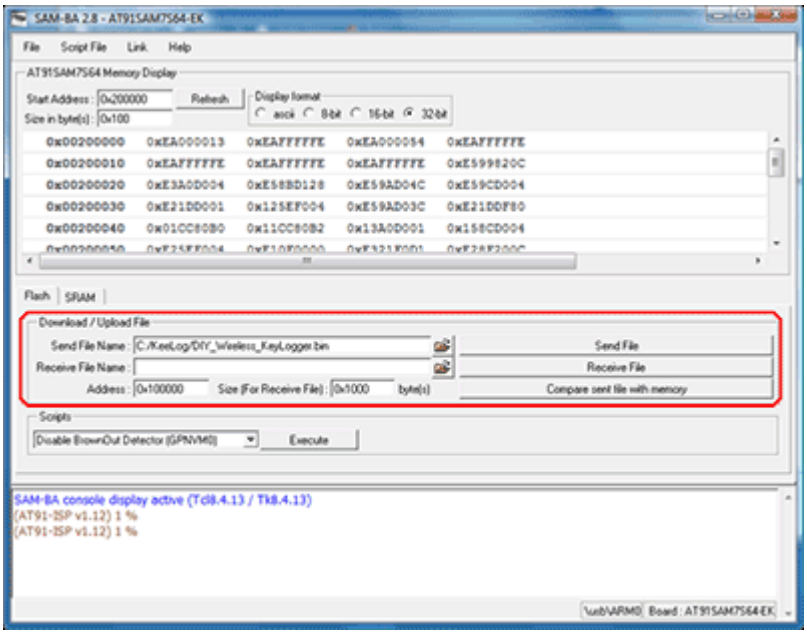
Gestionnaire de périphérique avec appareil Atmel AT91

Etape 9 : Lancez l'application SAM-BA du progiciel AT91 ISP et sélectionnez la plateforme microcontrôleur de destination AT91SAM7S64-EK.



Sélection de la plateforme microcontrôleur

Etape 10 : Après avoir établi la connexion avec la plateforme, ouvrez l'onglet Flash, sélectionnez un micrologiciel approprié pour l'émetteur/récepteur et cliquez sur Send File. Quand le logiciel demandera la permission de verrouiller et déverrouiller certaines régions de la mémoire, il faut sélectionner Yes. Si cette étape est terminée avec succès, le micrologiciel a été correctement chargé dans la mémoire flash du microcontrôleur.



Application SAM-BA

N'oubliez pas de répéter la procédure SAM-BA aussi bien pour l'émetteur que pour le récepteur. Une fois les procédures terminées, les deux appareils seront prêts à l'emploi.