Funkkeylogger

Machen Sie es selbst!

Einführung

Ist der Hardware Keylogger ein Begriff für Sie? Der Hardware Keylogger bildet die perfekte Lösung für die Überwachung der Benutzeraktivität bei einer geringen Aufspürungsgefahr. Der Hardware Keylogger stellt ein zu 100% elektronisches Gerät dar, er bedarf somit keinen Zugang zum Betriebssystem und hinterlässt keine Spuren, und die Software ist nicht imstande, ein solches Gerät aufzuspüren. Das Konzept des Hardware Keylogger hat jedoch einen Nachteil: Für die Wiedergabe der aufgezeichneten Daten ist der physische Zugang zum Gerät notwendig. Endlich wurde eine Lösung für das Problem gefunden: Der Funkkeylogger.

KeeLog hat bereits ein Projekt des Open Source PS/2 Hardware Keylogger veröffentlicht. Jetzt tun wir es wieder mit dem Projekt des Machen-Sie-es-selbst-Funkkeylogger. Das Projekt kann man sowohl für privaten Gebrauch als auch für Gewerbezwecke mit folgenden Einschränkungen verwenden:

1. Alle auf der Website publizierten Materialien bilden das geistige Eigentum der Firma KeeLog und die Verwendung deren ist mit der Annahme der anschließenden Bedingungen und des allgemeinen Benutzervertrages gleichbedeutend.
2. Das Projekt des Funkkeylogger wurde "as is" zur Verfügung gestellt, mit allen Fehlern und ohne jegliche Garantien.

Der Funkkeylogger darf nicht zur rechtswidrigen Aufzeichnung fremder Daten, insbesondere Passwörter, Bankdaten, vertraulicher Korrespondenz usw. benutzt werden. In den meisten Ländern gilt das als Rechtsverletzung.

Der Funkkeylogger besteht aus zwei Baugruppen: dem Sender und dem Empfänger. Das eigentliche Keylogging erfolgt im Sender, der ein PS/2-Hardware-Keylogger mit einem eingebauten Funkmodul 2,4 Ghz in Wirklichkeit ist. Aufgezeichnete Tastaturdaten werden nicht im Speicher archiviert, sondern in Real-Time über den Funkanschluss gesendet. Der Empfänger stellt dagegen eine Funkaquisitionseinheit mit USB-Schnittstelle dar. Alle vom Sender empfangenen Daten werden per USB in den Rechner gesendet. Vonseiten der Software sind diese Daten durch einen virtuellen COM-Port zugänglich, was ihre Visualisierung durch einen beliebigen Terminal-Client möglich macht.

Funkkeylogger - Blockschema

Das ganze System arbeitet in Real-Time, daher ist der am Remote-Computer geschriebene Text sofort auf der Seite des Empfängers zu sehen. Das System hat eine Maximalreichweite von 50 Metern. Dies entspricht einer effektiven Reichweite von ca. 20 Metern durch 2-4 Wände, je nach ihrer Dicke.

Funkkeylogger - Sender

Funkkeylogger - Empfänger

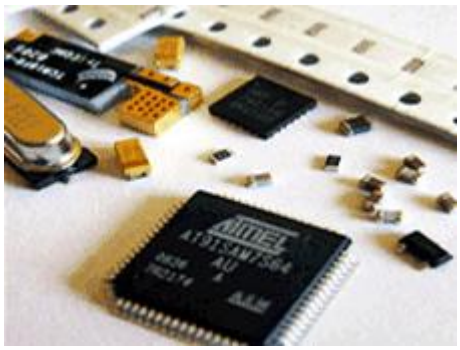
Sowohl der Sender als auch der Empfänger basieren auf dem gleichen elektrischen Schema und der gleichen Leiterplatte. Sie haben dieselben Abmessungen und sind für den Anschluss an PS/2- und USB-Verlängerungskabel bestimmt. Als Gehäuse wird das Gehäuse für EMC-Filter empfohlen, das das ganze Gerät einem Adapter oder Verlängerungskabel ähnlich macht.

Komponenten

Dieser Artikel beschreibt den ganzen Montageprozess des Funkkeylogger. Je nach Ihren Fähigkeiten können Sie wählen, ob Sie Ihren eigenen Funkkeylogger von null an zusammenbauen oder Komponenten bei uns bestellen. Wir können Ihnen ein Komponentenset mit vorprogrammierten Mikrocontrollern und Standardgehäusen (wie auf den Bildern) oder ein vollständig zusammengebautes und geprüftes Gerätekit liefern. Für mehr Details gehen Sie zum Kapitel Kits über.

Sollen Sie sich entschieden haben, Ihren eigenen Funkkeylogger zu bilden, müssen Sie Grunderfahrung in Elektronik und Löten, und am besten in der Technik der Oberflächenmontage (SMT) haben. Die einfachste Option ist die Bestellung eines Kits von Baugruppen bei uns und die eigenhändige Ausführung der Lötung, Verdrahtung und Endmontage. Dafür brauchen Sie einen Lötkolben mit Temperaturregelung und gute Lötfähigkeiten. Sollten Sie sich entschieden haben, die Leiterplatten selbstständig zu planen und auszuführen, so müssen Sie über viel Erfahrung auf dem Gebiet und entsprechende Ausrüstung dafür verfügen.

Die anschließende Tabelle zeigt eine Liste von Baugruppen (Stückliste), die für die Anfertigung eines Senders bzw. Empfängers notwendig sind. Für den Sender ist ein zusätzliches PS/2-Verlängerungskabel und für den Empfänger - ein USB-Kabel mit einem Typ-A-Verbinder erforderlich.



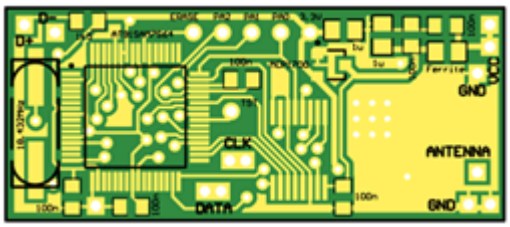
Set von Elektrokomponenten

Kabel, Gehäuse und Leiterplatten

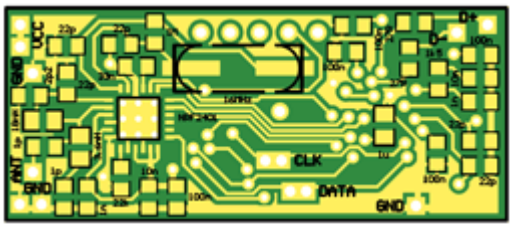
Kennzeichnung	Beschreibung	Gehäuse	Menge
U1	Mikrocontroller AT91SAM7S64	TQFP64	1
U2	Transceiver nRF2401	QFN24	1
U3	Spannungsregler MCP1700T-330	SOT-23	1
Q1	Quarz 18.432 MHz	HC-49 SMD	1
Q2	Quarz 16 MHz	HC-49 SMD	1
R1, R2	Widerstand 1.5 kΩ	0805	2
R3, R4	Widerstand 27 Ω	0805	2
R5	Widerstand 1 MΩ	0805	1
R6	Widerstand 22 kΩ	0805	1
C1, C27	Kondensator 10 nF	0805	2
C2, C28	Kondensator 1 nF	0805	2
C3, C4, C6, C7, C8	Kondensator 22 pF	0805	5
C5	Kondensator 33 nF	0805	1
C9	Kondensator 2.2 pF	0805	1
C10, C11	Kondensator 1 pF	0805	2
C12, C22, C23, C24, C25, C26, C32, C33, C34, C42, C43	Kondensator 100 nF	0805	11
C21, C31, C41	Kondensator 1 µF	0805	3
L1	Drosselspule	0805	1
L2	Spule 3.6 nH	0805	1
L3	Spule 18 nH	0805	1

Funkkeylogger - Stückliste

Sowohl der Sender als auch der Empfänger nutzen die gleiche Leiterplatte und das gleiche Komponentenset (sie haben nur unterschiedliche Kabel und Firmware). Der Atmel AT91SAM7S64 Mikrocontroller und Funktransceiver nRF2401 stellen die wichtigsten Komponenten dar. Für den richtigen Betrieb erfordern sie beide Quarzoszillatoren. Außer dem Spannungsregler MCP1700 sind alle anderen Baugruppen passiv (Widerstände, Kondensatoren und einige Spulen). Als eine Dipolantenne wird ein einfacher Draht empfohlen. Eine doppelseitige zweischichtige Leiterplatte wird auf den Bildern unten dargestellt.

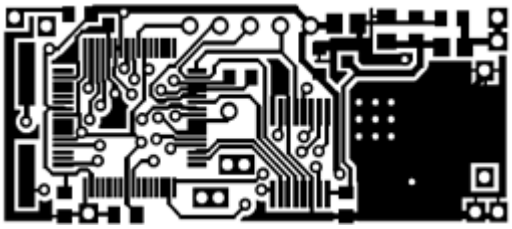


Leiterplatten-Layout - Oberseite

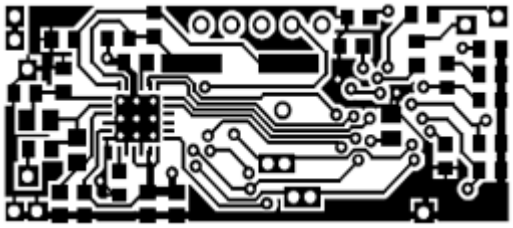


Leiterplatten-Layout - Unterseite

Wenn Sie genug Erfahrung haben, um selbstständig Leiterplatten auszuführen, können Sie das 1:1 Masken-Set verwenden, das unten erhältlich ist. Im Referenzprojekt wird die 1 mm dicke FR4-Glasfasermatte verwendet.



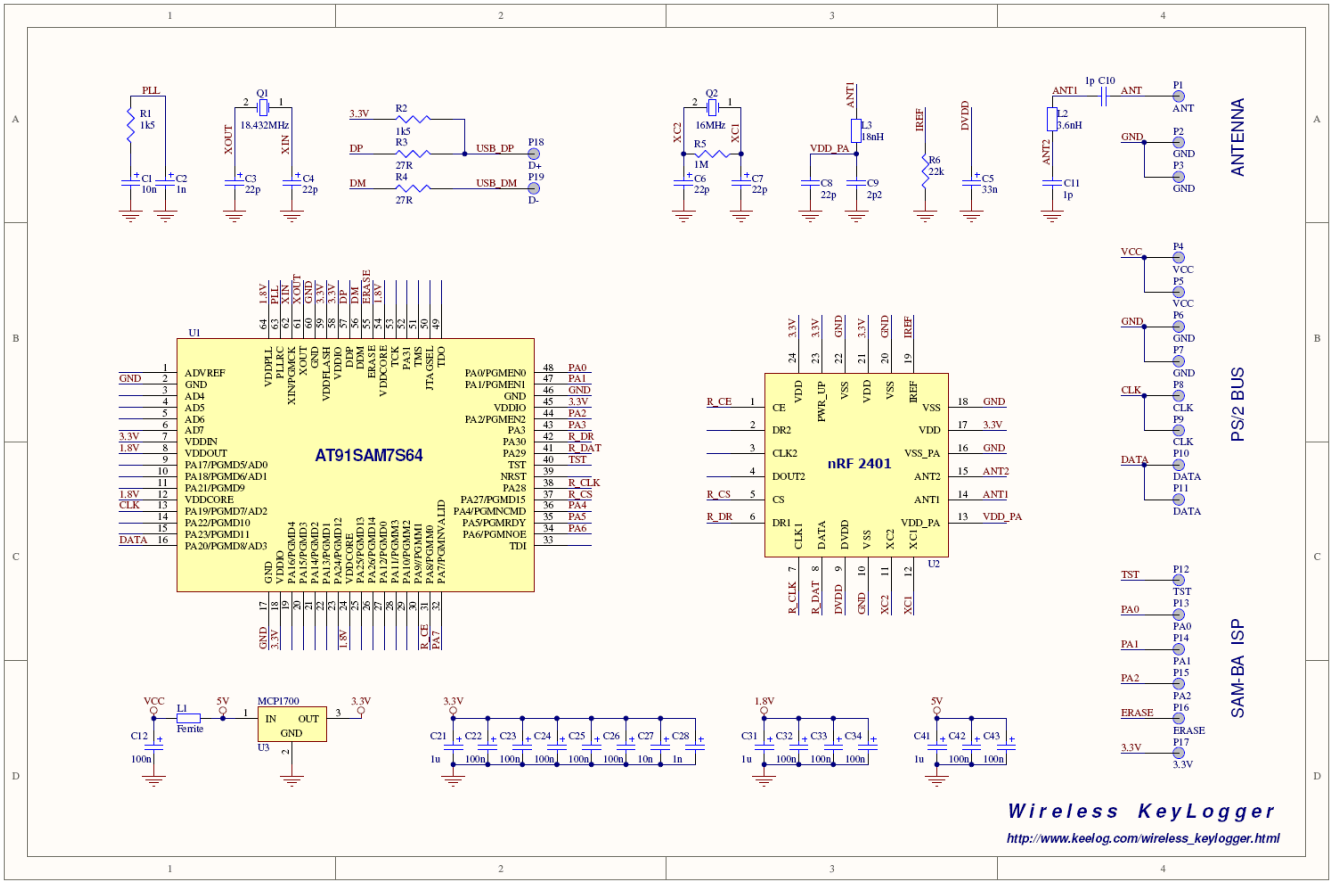
Leiterplattenmaske - Oberseite



Leiterplattenmaske - Unterseite

Montage

Der Stromkreis des Funkkeylogger besteht aus zwei Hauptbaugruppen: Mikrocontroller AT91SAM7S64 und Transceiver nRF2401. Die begleitenden passiven Baugruppen machen hauptsächlich der Oszillator und die RF-Schaltungen aus. Der ganze Kreis wird mit 3.3V betrieben, die durch den Regler MCP1700 generiert und durch einen Kondensatorensatz filtriert werden. Die Eingangsversorgung erfolgt direkt per PS/2-Bus (Sender) bzw. USB (Empfänger). Haben Sie die Leiterplatten bereits zusammengebaut, gehen Sie zum Kapitel Verdrahtung über. Wenn Sie sich für den selbstständigen Zusammenbau entschieden haben, können sich die anschließenden Hinweise und Schaltpläne als nützlich erweisen.



Funkkeylogger - Schaltplan

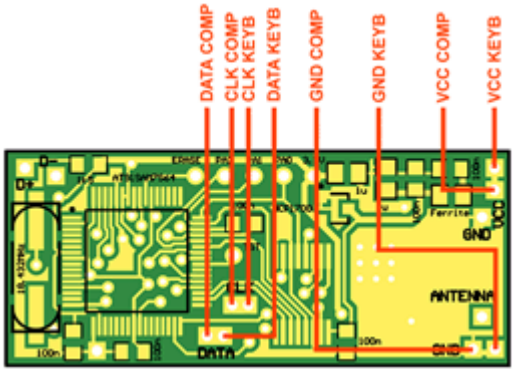
Für das Löten sind ein Lötkolben mit einer dünnen Spitze (typischerweise unter 0,5 mm) und eine Lötpaste (z.B. RMA7) zu verwenden. Lassen Sie nicht zu, dass sich die Baugruppen beim Löten überhitzen. Beginnen Sie den Zusammenbau mit dem Transceiver nRF2401, denn er hat das komplexeste Gehäuse. Dann gehen Sie zum Mikrocontroller AT91SAM7S64 und Spannungsregler MCP1700 über. Stellen Sie stets sicher, dass der Anschluss Nr. 1 am Gehäuse dem ersten Anschluss an der Leiterplatte entspricht. Schließlich löten Sie alle zusätzlichen Kreise an: Quarze, Widerstände, Kondensatoren und Spulen. Die Antenne lassen Sie für das Ende. Sie können eine dedizierte Antenne ISM 2.4 GHz verwenden oder eine einfache Viertelwellen-Dipolantenne aus einem Draht machen. Die optimale Länge beträgt 3,125 cm (1,23"). Zusammengebaute Leiterplatten sollen

ähnlich wie auf den Bildern unten aussehen.

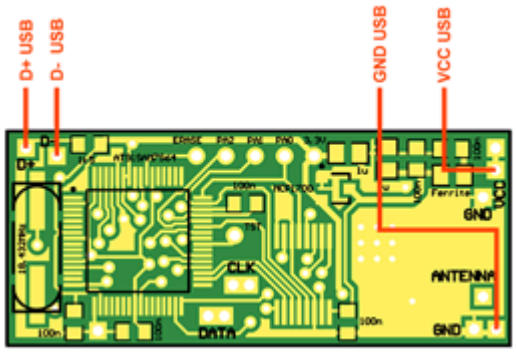
Zusammengebaute Leiterplatte - Oberseite mit Mikrocontroller

Zusammengebaute Leiterplatte - Unterseite mit Transceiver

Nach der Montage der Leiterplatten ist die Verdrahtung vorzunehmen. Es ist neben der Firmware der einzige Unterschied zwischen dem Sender und dem Empfänger. Der Sender soll parallel mit dem PS/2-Bus gekoppelt sein. Die Leiterplatte des Senders weist Pads auf, die das Anlöten von Verbindungen ermöglichen, die sowohl zum Rechner als auch zur Tastatur führen. Der Empfänger soll dagegen eine Standardverbindung zu einem USB-Port haben. Die Bilder unten zeigen, wie die Verbindungen auszuführen sind.



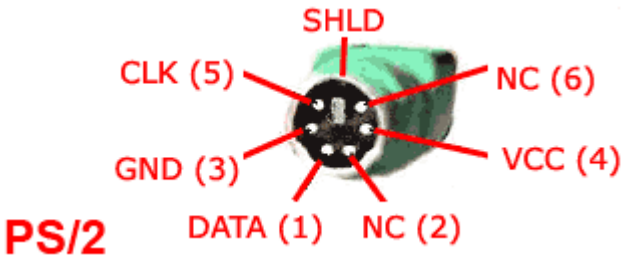
Schema der PS/2-Verdrahtung für den Sender



Schema der USB-Verdrahtung für den Empfänger

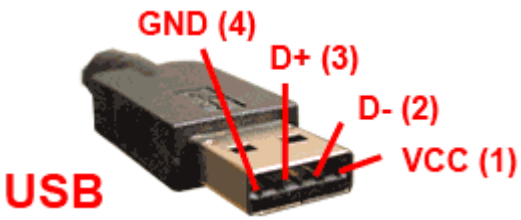
Benutzen Sie PS/2- und USB-Verlängerungskabel, schneiden Sie sie durch und isolieren Sie die Signalleitungen. Was einige Probleme bereiten kann, ist die Zuordnung der Drähte zu den einzelnen Signalen. Manche PS/2- und USB-Kabel weisen standardisierte Farben auf, das Vertrauen darin kann jedoch sehr riskant sein. Die empfohlene Lösung ist die Verwendung eines Kurzschlussmessgerätes bzw. Ohmmeters für die Identifizierung, welcher Draht welcher Signalleitung entspricht. Die Diagramme unten können dabei hilfreich sein.

Signal	Beschreibung	PS/2-Anschluss	Kommentar
VCC	+5V Stromversorgung	4	müssen an das Modul angeschlossen werden
GND	Stromversorgungsmasse	3	
CLK	Taktgeber	5	
DATA	Daten	1	
NC	Unbenutzte Leitungen	2, 6	durch das Modul nicht benutzt, falls sie vorhanden sind, im Originalzustand lassen
SHLD	Abschirmung	-	



PS/2-Anschluss (Sendereinheit)

Signal	Beschreibung	USB-Anschluss	Kommentar
VCC	+5V Stromversorgung	1	müssen an das Modul angeschlossen werden
D-	Daten	2	
D+	Daten	3	
GND	Stromversorgungsmasse	4	
SHLD	Abschirmung	-	durch das Modul nicht benutzt, falls sie vorhanden sind, im Originalzustand lassen



USB-Anschluss (Empfängereinheit)

Sind die Mikrocontroller, die Sie verwenden, noch nicht programmiert, so ist es nun der beste Augenblick für das Hochladen der Firmware unter Verwendung der ISP-Technologie (In-System Programming). Für mehr Details gehen Sie zum Kapitel Firmware über. Nachdem das gemacht worden ist, sollen die Leiterplatten so wie auf den Bildern unten aussehen.

Sender mit der PS/2-Verdrahtung

Empfänger mit der USB-Verdrahtung

Bevor das Gehäuse aufgesetzt wird, empfehlen wir, den letzten Test durchzuführen. Verwenden Sie das Kurzschlussmessgerät oder den Ohmmeter, um den Widerstand zwischen der Stromversorgung (VCC) und Erdung (GND) sowohl auf dem USB- als auch auf dem PS/2-Verbinder zu messen. Ein Kurzschluss bedeutet, dass der ganze Kreis geprüft werden soll, sonst kann es zur Beschädigung Ihres Rechners kommen. Wenn alles in Ordnung ist, schließen Sie die Gehäuse mithilfe eines Klebers - und nun geht's los.

Inbetriebnahme

Nach dem Zusammenbau des Paares Sender-Empfänger kommt die Zeit für den ersten Test. Wir empfehlen, nur einen Rechner für die Überprüfung der beiden Geräte zu verwenden. Zuerst schalten Sie den Computer aus und schließen Sie den Sender zwischen die PS/2-Tastatur und den PS/2-Port an.

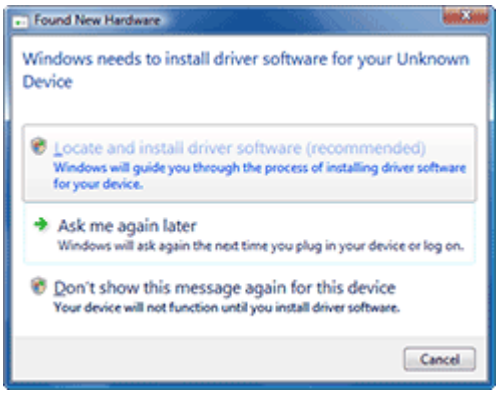
Schließen Sie den Sender an den PS/2-Port an

Schließen Sie die PS/2-Tastatur an den Sender an

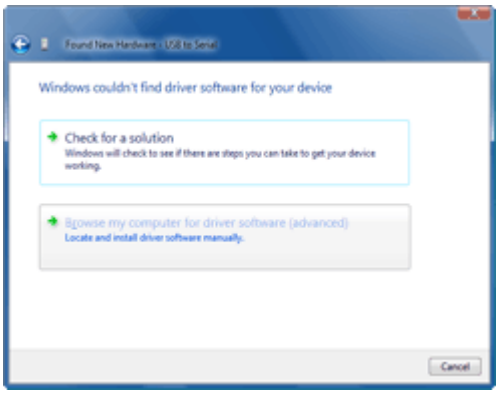
Dann schalten Sie den Rechner ein und stellen Sie sicher, dass die PS/2-Tastatur richtig funktioniert (es soll keinerlei Einfluss des Keylogger feststellbar sein). Nun kommt die Zeit für den Empfängertest. Laden Sie zuerst die Datei des KeeLog Treibers runter. Entpacken Sie die Dateien und speichern Sie sie auf der lokalen Festplatte Ihres Rechners. Dann schließen Sie den Empfänger an einen freien USB-Port an (der Rechner muss nicht ausgeschaltet werden). Stellen Sie sicher, dass die Stellung des Empfängers den Empfang des Funksignals des Senders ermöglicht.

Schließen Sie den Empfänger an einen freien USB-Port an

Beim ersten Anschließen des Senders wird das Installationsdialogfenster des Treibers angezeigt. Genau gesagt, werden hier Treiber des virtuellen COM-Port verwendet, die mit den meisten Betriebssystemen wie Windows geliefert werden. Die entsprechende INF-Datei muss jedoch manuell gewählt werden. Fragt das Betriebssystem nach Treibern, so wechseln Sie zum Speicherort, wo die Treiberdateien gespeichert worden sind. Die Bilder unten veranschaulichen den ganzen Vorgang.

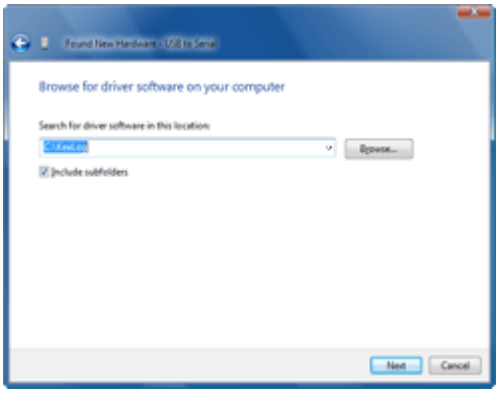


Wählen Sie, um den Speicherort des Treibers zu finden und den Treiber zu installieren



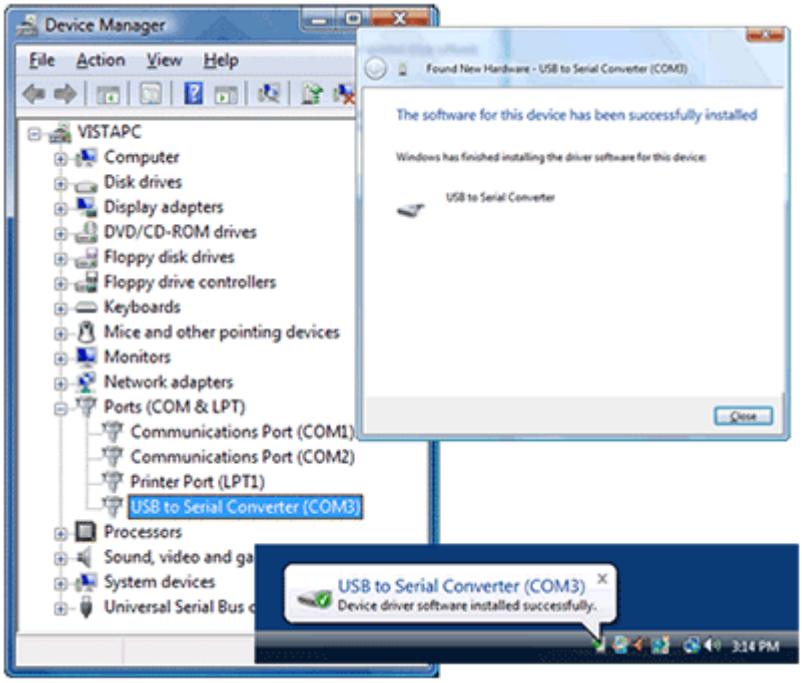
Wählen Sie, um den Speicherort des Treibers zu suchen

Wählen Sie, um die Suchoptionen anzuzeigen



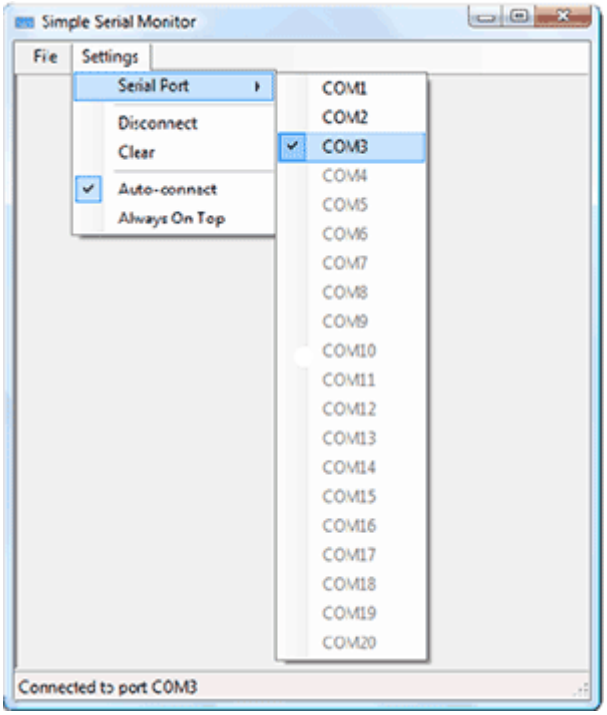
Wechseln Sie zum Speicherort des Treibers

Ist die Installation erfolgreich abgeschlossen, so soll der Empfänger als ein USB-to-serial-Konverter zu sehen sein. Starten Sie den Geräte-Manager im Windows, um zu prüfen, welcher virtuelle Port dem Empfänger zugeordnet worden ist.



Empfänger im Geräte-Manager sichtbar

Um die Aufzeichnung von Tastenanschlagdaten zu beginnen, kann man einen beliebigen Terminal-Client, wie zum Beispiel Hyperterminal verwenden. Wir empfehlen die Verwendung unserer kostenlosen Software Simple Serial Monitor, die bequem und einfach im Gebrauch ist.



Simple Serial Monitor (kostenloser Terminal-Client von KeeLog)

Nach Starten von Simple Serial Monitor (oder einer alternativen Anwendung) denken Sie an die Wahl eines entsprechenden COM-Ports. Ist alles erfolgreich abgelaufen, zeigt der Empfänger sofort alle Tastenanschläge der PS/2-Tastatur an.

Remote-Computer mit PS/2-Sender *Lokaler Computer mit USB-Empfänger*

Der nächste Schritt ist die Überprüfung desselben auf zwei verschiedenen Rechnern. Stellen Sie sicher, dass sie sich in der Übertragungsreichweite befinden. Wenn Sie Text im Terminalfenster sehen, so ist Ihr Funkkeylogger zu seiner ersten wirklichen Mission bereit. Verwenden Sie dieses Gerät nur für rechtmäßige Zwecke!

Herunterladen

Mikrocontroller-Firmware für das Programmieren des Senders und des Empfängers
http://www.keelog.com/files/WirelessKeyloggerFirmware.zip

Treiber, der den Empfänger als virtuellen COM-Port installieren lässt
http://www.keelog.com/files/UsbToSerial.zip

Kostenlose Software, die den Empfang aufgezeichneter Daten über einen virtuellen COM-Port erlaubt (Äquivalent zur Hyperterminal-Anwendung). Sie erfordert das Microsoft .NET Framework.
http://www.keelog.com/files/SimpleSerialMonitor.zip

Software, die das Programmieren der Firmware unter Verwendung von SAM-BA ermöglicht
http://www.keelog.com/files/At91Isp.zip

Das Handbuch enthält Informationen über das Programmieren der Firmware für den Mikrocontroller über einen eingebauten Boot-Loader ohne Verwendung eines zusätzlichen Programmers
http://www.keelog.com/files/SambaUserGuide.pdf

Liste von Baugruppen, die beim Zusammenbau des Funkkeylogger (Sender und Empfänger) verwendet wurden
http://www.keelog.com/files/WirelessKeyloggerBom.pdf

Verdrahtungsschema des Funkkeylogger (Sender und Empfänger)
http://www.keelog.com/files/WirelessKeyloggerWiring.pdf

Schaltplan des Funkkeylogger (Sender und Empfänger)
http://www.keelog.com/files/WirelessKeyloggerSchColor.pdf

Oberseite der Leiterplatte (Sender und Empfänger)
http://www.keelog.com/files/WirelessKeyloggerPcbTop.pdf

Unterseite der Leiterplatte (Sender und Empfänger)
http://www.keelog.com/files/WirelessKeyloggerPcbBottom.pdf

Maske für die Oberseite der Leiterplatte (Sender und Empfänger), Skalierung 1:1
http://www.keelog.com/files/WirelessKeyloggerMaskTop.pdf

Maske für die Unterseite der Leiterplatte (Sender und Empfänger), Skalierung 1:1
http://www.keelog.com/files/WirelessKeyloggerMaskBottom.pdf

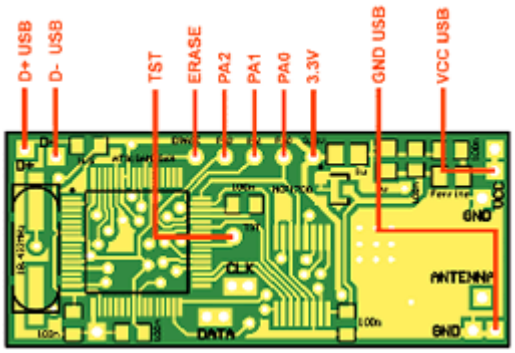
Firmware

Lesen die das Kapitel nur dann, wenn Sie den Mikrocontroller AT91SAM7S64 selbstständig programmieren wollen. Haben Sie ein Kit bei uns gekauft, so haben wir das bereits für Sie getan.

Moderne Mikrocontroller wie Atmel AT91SAM7S64 haben dicht gepackte Gehäuse, was Schwierigkeiten bei der Suche einer herkömmlichen Programmiersoftware bereitet, die den jeweiligen Mikrocontroller unterstützen würde. Daher entwickelt sich die ISP-Programmierung (In-System Programming) in den letzten Jahren so schnell. Die ISP macht es möglich, die Leiterplatte zuerst einzubauen und dann die Firmware oft mit Hilfe von sehr einfachen Werkzeugen zu programmieren. Der Mikrocontroller AT91SAM7S64 beinhaltet eine sehr praktische ISP-Lösung, die auf einem eingebauten USB-Modul basiert. Es wird SAM-BA (SAM Boot Assistant) genannt und erfordert nur ein USB-Kabel und einige einfache Steckbrücken. Um SAM-BA auf dem Funkkeylogger zu starten, müssen Sie zuerst die Software AT91 ISP herunterladen. Dann folgen Sie den folgenden Schritten, um die Firmware auf das Empfänger- und Sendermodul zu laden.

Schritt 1: Betrifft nur den Sender. USB-Kabel mit dem Typ-A-Stecker auf der einen Seite und isolierten Drähten auf der anderen Seite vorbereiten. Die USB-Leitungen: VCC, GND, D+, und D- an entsprechende Pads der Leiterplatte anlöten. Dieser Schritt ist für den Empfänger nicht nötig, denn er weist die USB-Verbindung bereits auf.

Schritt 2: Einige kurze Drähte vorbereiten, um die SAM-BA-Anschlüsse: TST, ERASE, PA2, PA1, PA0, 3.3V kurzzuschließen. Ein Ende des jeweiligen Drahts an den entsprechenden SAM-BA-Pad der beiden Platten anlöten. Alternativ können Sie spezielle Steckbrücken vorbereiten, wie auf den Bildern unten gezeigt wurde.



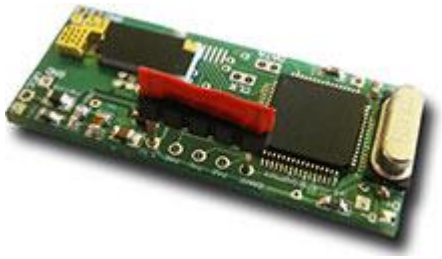
SAM-BA-Verdrahtungsschema

Schritt 3: Das Software-Paket AT91 ISP installieren.

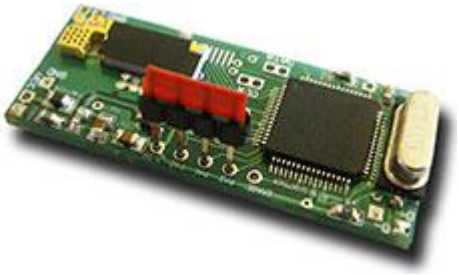
Schritt 4: Das Gerät an einen freien USB-Port anschließen. Die Meldung Gerät wurde nicht erkannt ist in dieser Phase normal.

Schritt 5: Den ERASE-Anschluss mit dem 3,3V-Anschluss für eine kurze Zeit kurzschließen. Dadurch wird der Flash-Speicher des Mikrocontrollers gelöscht.

USB-Kabel und Steckbrücken für SAM-BA-Boot-Loader



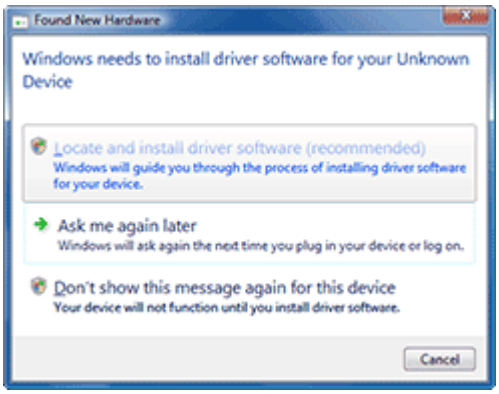
Löschen des Speichers (ERASE mit 3,3V kurzgeschlossen)



Aktivierung des Boot-Loaders (PA0, PA1, PA2 und TST mit 3.3V kurzgeschlossen)

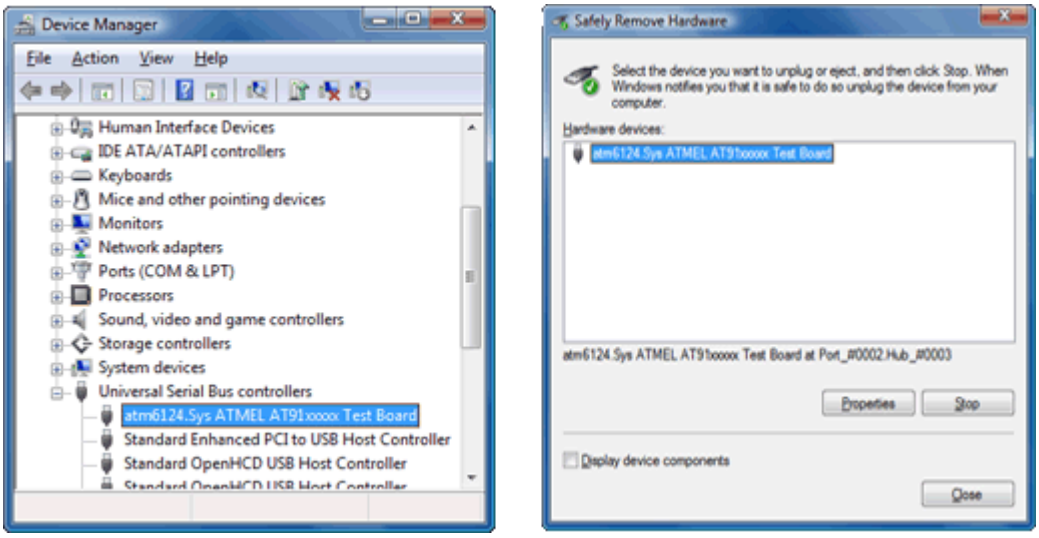
Schritt 6: Das Gerät vom USB-Port trennen. Sicherstellen, dass der ERASE-Anschluss nicht mehr an 3,3V angeschlossen ist. Dann den Satz von Anschlüssen PA0, PA1, PA2 und TST mit dem 3.3V kurzschließen. Das Gerät wieder an den USB-Port anschließen (Die Meldung Gerät wurde nicht erkannt kann wieder erscheinen). Das Gerät ca. 10 Sekunden angeschlossen lassen und dann vom USB-Port trennen. Die Operation soll den SAM-BA-Boot-Loader aktivieren.

Schritt 7: Alle Steckbrücken und Kurzschlüsse entfernen und das Gerät an den USB-Port anschließen. Es soll die Meldung Neue Hardware gefunden erscheinen. Das Standardverfahren durchführen und das Betriebssystem den Treiber selbstständig finden lassen.



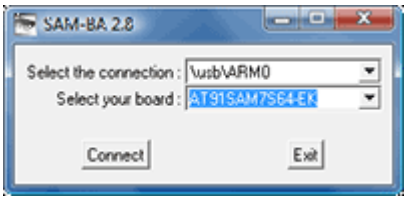
Dialogfenster Neue Hardware gefunden

Schritt 8: Den Geräte-Manager starten und sicherstellen, dass der SAM-BA-Boot-Loader aktiviert wurde.



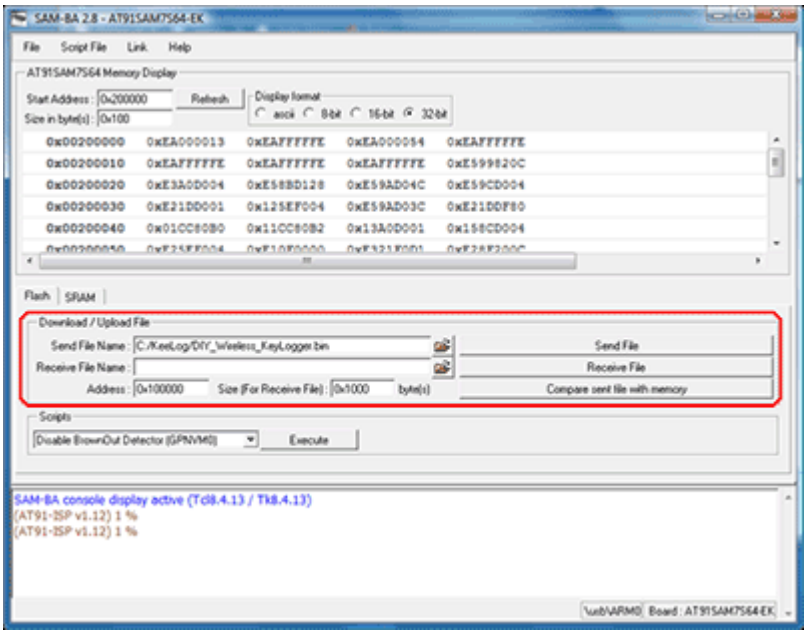
Geräte-Manager mit dem Atmel AT 91 Gerät

Schritt 9: Die Anwendung SAM-BA aus dem Softwarepaket AT91 ISP starten und das Ziel-Mikrocontroller-Board AT91SAM7S64-EK wählen.



Wahl des Mikrocontroller-Board

Schritt 10: Nach der Verbindung mit dem Board zum Tab Flash wechseln, entsprechende Firmware für den Sender/Empfänger wählen und auf Send File klicken. Yes wählen, wenn die Anwendung fragt, ob die einschlägigen Flash-Regionen freigegeben und gesperrt werden sollen. Wurde dieser Schritt erfolgreich abgeschlossen, so bedeutet es, dass die Firmware in den Flash-Speicher des Mikrocontrollers richtig geladen worden ist.



SAM-BA-Anwendung

Beachten Sie, dass das SAM-BA-Verfahren sowohl für den Sender als auch für den Empfänger ausgeführt werden muss. Nach der Ausführung der oben genannten Maßnahmen sind die beiden Geräte betriebsbereit.