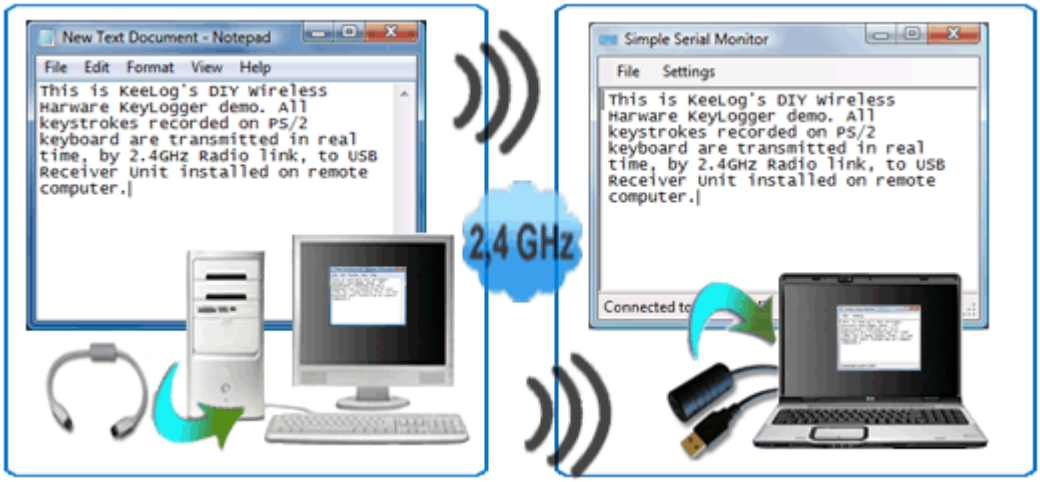
Bezprzewodowy Keylogger

Zrób to Sam!



Wprowadzenie

Czy znasz pojęcie keyloggera sprzętowego? Sprzętowy keylogger to idealne rozwiązanie służące monitorowaniu aktywności użytkownika komputera, przy znikomym ryzyku wykrycia. Keylogger sprzętowy jest urządzeniem w 100% elektronicznym, więc nie wymaga dostępu do systemu operacyjnego, nie zostawia żadnych śladów, zaś oprogramowanie nie jest w stanie tego typu urządzenia wykryć. Koncepcja keyloggera sprzętowego ma jednak jedną wadę: żeby odzyskać przechwycone dane, niezbędny jest fizyczny dostęp do urządzenia. Ten problem znalazł nareszcie rozwiązanie: Bezprzewodowy Keylogger.

KeeLog w przeszłości opublikował już jeden projekt keyloggera sprzętowego PS/2 typu Open Source. Teraz robimy to ponownie z projektem Bezprzewodowego Keyloggera, przeznaczonego to samodzielnego montażu. Ten projekt można wykorzystywać zarówno do celów prywatnych, jak i komercyjnych, z następującymi ograniczeniami:

1. Wszelkie materiały zamieszczone na tej stronie internetowej są własnością intelektualną firmy KeeLog i używanie ich oznacza akceptację poniższych warunków oraz ogólnej Umowy Użytkownika.
2. Ten projekt Bezprzewodowego Keyloggera opublikowany został "jak jest", ze wszystkimi wadami i bez żadnej gwarancji.

Bezprzewodowy Keylogger nie powinien być używany do bezprawnego przechwytywania cudzych danych, w szczególności haseł, danych bankowych, poufnej korespondencji itp. W większości krajów jest to naruszenie prawa.

Bezprzewodowy Keylogger składa się z dwóch głównych części: nadajnik oraz odbiornik. Rzeczywiste logowanie klawiszy odbywa się w nadajniku, który w istocie jest keyloggerem sprzętowym PS/2, z wbudowanym modułem radiowym 2.4 GHz. Przechwycone dane z klawiatury nie są archiwizowane w pamięci, lecz transmitowane w czasie rzeczywistym przez łącze radiowe. Odbiornik, z drugiej strony, jest bezprzewodowym urządzeniem akwizycyjnym z interfejsem USB. Wszystkie dane odebrane od nadajnika są wysyłane do komputera przez USB. Z programowego punktu widzenia, dane te są dostępne przez wirtualny port COM, co umożliwia ich wizualizację przez dowolny klient terminala.

Bezprzewodowy Keylogger - schemat blokowy

Cały system działa w czasie rzeczywistym, więc tekst pisany na zdalnym komputerze jest widoczny natychmiast po stronie odbiornika. System ma maksymalny zasięg około 50 metrów. To odpowiada skutecznemu zasięgowi około 20 metrów przez 2-4 ściany, w zależności od ich grubości.

Bezprzewodowy Keylogger - nadajnik

Bezprzewodowy Keylogger - odbiornik

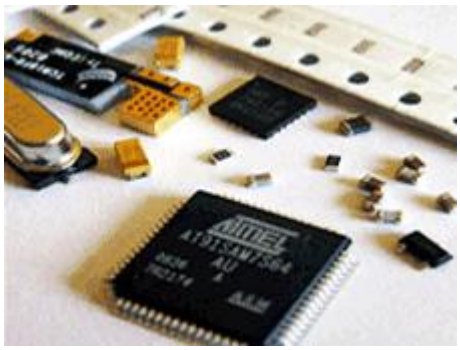
Zarówno nadajnik, jak i odbiornik są oparte na tym samym schemacie elektrycznym i obwodzie drukowanym. Oba mają te same gabaryty i są przeznaczone do zamocowania na krótkich przedłużaczach PS/2 i USB. Zaleca się użyć obudowy od filtrów typu EMC, co spowoduje, że całe urządzenie będzie przypominało adapter bądź przedłużacz.

Podzespoły

Ten artykuł opisuje cały proces montażu Bezprzewodowego Keyloggera. W zależności od umiejętności, możesz zdecydować się stworzyć własny Bezprzewodowy Keylogger od podstaw, bądź zamówić podzespoły od nas. Możemy dostarczyć komplet podzespołów wraz z zaprogramowanymi mikrokontrolerami i standardowymi obudowami (widoczne na zdjęciach), lub w pełni zmontowany i przetestowany komplet urządzeń. Przejdź do sekcji zestawy, żeby uzyskać więcej szczegółów.

Jeśli zdecydowałeś się stworzyć swój własny Bezprzewodowy Keylogger, powinieneś mieć podstawowe doświadczenie w elektronice oraz lutowaniu, najlepiej w technologii montażu powierzchniowego (SMT). Najprostsza opcja to zamówienie kompletu podzespołów od nas, i wykonanie lutowania, okablowania oraz finalnego montażu samodzielnie. Wymaga to posiadanie lutownicy z regulacją temperatury oraz dosyć dobrych umiejętności w lutowaniu. Jeśli zdecydowałeś się zaprojektować i wykonać obwody drukowane samemu, będzie to wymagało dużego doświadczenia oraz odpowiedniego sprzętu.

Poniższa tabela przedstawia spis podzespołów (BOM), niezbędnych do wykonania jednej sztuki nadajnika, bądź odbiornika. Dodatkowy przedłużacz PS/2 jest wymagany dla nadajnika, oraz kabel USB z konektorem typu A jest wymagany dla odbiornika.



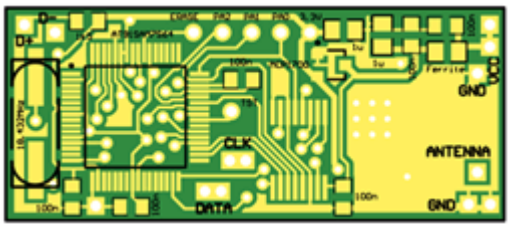
Zestaw podzespołów elektronicznych

Kable, obudowa oraz obwody drukowane

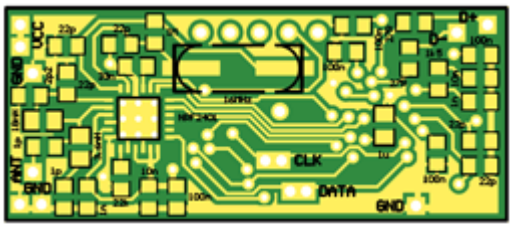
Oznaczenie	Opis	Obudowa	Ilość
U1	Mikrokontroler AT91SAM7S64	TQFP64	1
U2	Transceiver nRF2401	QFN24	1
U3	Stabilizator MCP1700T-330	SOT-23	☐
Q1	Kwarc 18.432 MHz	HC-49 SMD	1
Q2	Kwarc 16 MHz	HC-49 SMD	1
R1, R2	Rezystor 1.5 kΩ	0805	2
R3, R4	Rezystor 27 Ω	0805	2
R5	Rezystor 1 MΩ	0805	1
R6	Rezystor 22 kΩ	0805	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	Dławik	☐805	1
L2	Cewka 3.6 nH	0805	1
L3	Cewka 18 nH	0805	1

Bezprzewodowy Keylogger - spis podzespołów

Zarówno nadajnik, jak i odbiornik używają tego samego obwodu drukowanego i tego samego zestawu podzespołów (różnią się okablowaniem oraz firmware'em). Mikrokontroler Atmel AT91SAM7S64 oraz transceiver radiowy nRF2401 to kluczowe podzespoły obwodu elektronicznego. Oba wymagają oscylatorów kwarcowych do poprawnego działania. Poza stabilizatorem MCP1700, wszystkie pozostałe podzespoły są bierne (rezystory, kondensatory i kilka cewek). Zwykły kawałek druta jest polecany jako antena dipolowa. Dwustronny, dwuwarstwowy obwód drukowany jest pokazany na poniższych rysunkach.

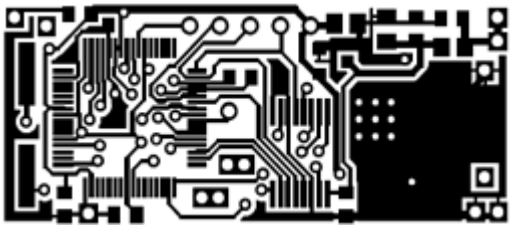


Rozkład obwodu drukowanego - strona górna

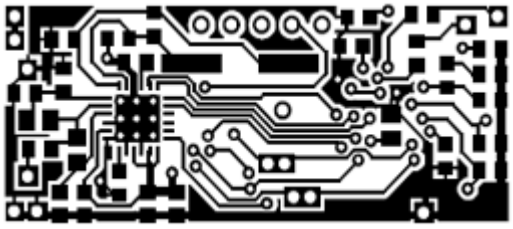


Rozkład obwodu drukowanego - strona dolna

Jeśli posiadasz wystarczające doświadczenie, żeby wykonać obwody drukowane samemu, możesz skorzystać z zestawu masek w skali 1:1 dostępnych poniżej. Projekt referencyjny używa laminatu typu FR4 o grubości 1 mm.



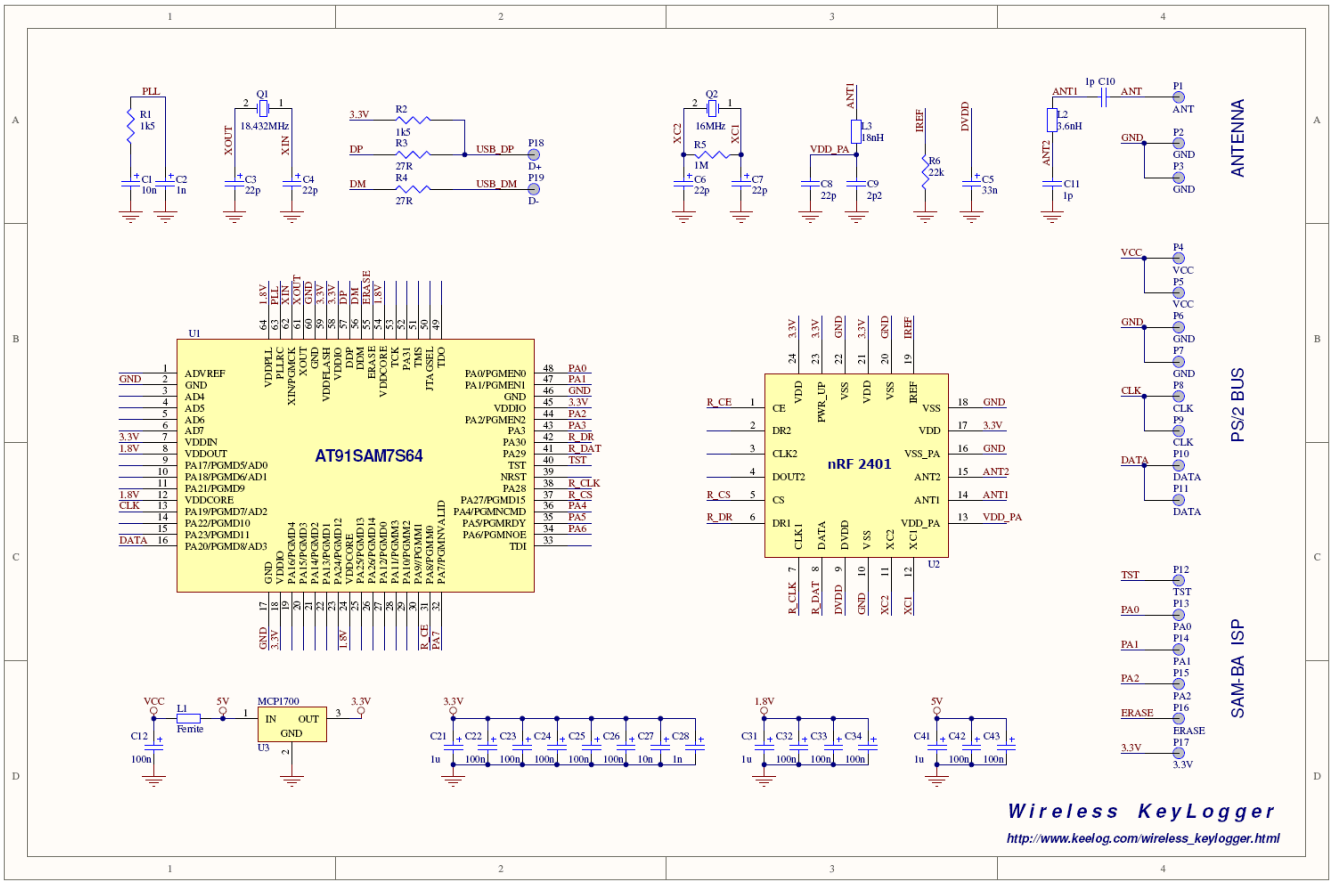
Maska obwodu drukowanego - strona górna



Maska obwodu drukowanego - strona dolna

Montaż

Obwód Bezprzewodowego Keyloggera jest złożony z dwóch głównych komponentów: mikrokontrolera AT91SAM7S64 oraz transceivera nRF2401. Towarzyszące im elementy pasywne to głównie oscylator oraz obwody wysokiej częstotliwości RF. Cały obwód jest zasilany przez 3.3V, generowane przez stabilizator MCP1700 i filtrowane przez zespół kondensatorów. Zasilanie wejściowe jest brane bezpośrednio z magistrali PS/2 (nadajnik), bądź USB (odbiornik). Jeśli już posiadasz zmontowane obwody drukowane, przejdź do sekcji okablowanie. Jeśli zdecydowałeś się na samodzielny montaż, poniższe wskazówki oraz schemat elektryczny okażą się przydatne.



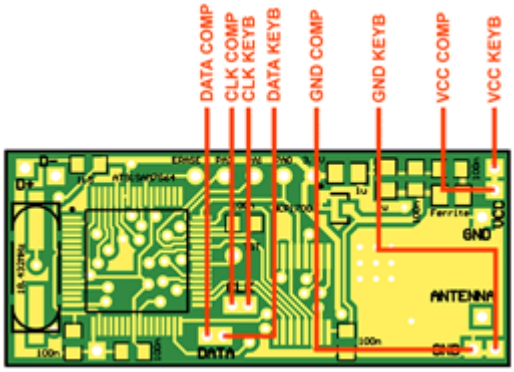
Bezprzewodowy Keylogger - schemat elektryczny

Do lutowania użyj lutownicy z cienkim grotem (typowo poniżej 0.5 mm) oraz pasty lutowniczej (przykładowo RMA7). Pilnuj, żeby nie przegrzać elementów podczas lutowania. Rozpocznij montaż od transceivera nRF2401 ze względu na skomplikowany typ obudowy. Następnie przejdź do mikrokontrolera AT91SAM7S64 oraz stabilizatora MCP1700. Pilnuj, żeby pin numer 1 na obudowie zgadzał się z pierwszym pinem na obwodzie drukowanym. Na końcu przylutuj wszystkie obwody dodatkowe: kwarce, rezystory, kondensatory i cewki. Zostaw antenę na sam koniec. Możesz użyć dedykowanej anteny na pasmo ISM 2.4 GHz, lub wykonać prostą ćwierć-falową antenę dipolową z kawałka drutu. Optymalna długość to 3.125 cm (1.23"). Zmontowane obwody drukowane powinny wyglądać podobnie do tych na poniższych zdjęciach.

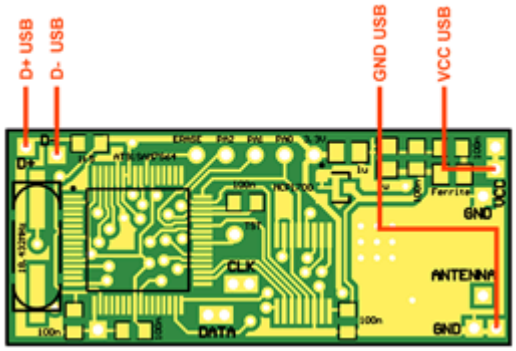
Zmontowany obwód drukowany - strona górna z mikrokontrolerem

Zmontowana obwód drukowany - strona dolna z transceiverem

Po montażu obwodów drukowanych należy wykonać okablowanie. Oprócz firmware'u, jest to punkt w którym nadajnik różni się od odbiornika. Nadajnik powinien być sprzęgnięty równolegle z magistralą PS/2. Obwód drukowany nadajnika posiada pady umożliwiające przylutowanie kabli prowadzących zarówno do komputera, jak i klawiatury. Odbiornik natomiast powinien mieć standardowe podłączenie do portu USB. Zdjęcia poniżej pokazują jak wykonać wszystkie połączenia.



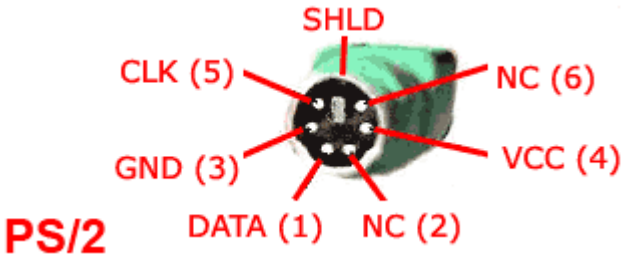
Schemat okablowania PS/2 dla nadajnika



Schemat okablowania USB dla odbiornika

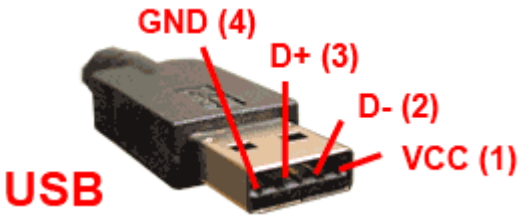
Użyj przedłużaczy PS/2 i USB, przetnij je, i odizoluj linie sygnałowe. Rzecz, która może przysporzyć pewnych kłopotów, to przyporządkowanie kabli do poszczególnych sygnałów. Niektóre kable PS/2 i USB posiadają zestandaryzowane kolory, jednak ufanie temu jest bardzo ryzykowne. Zalecanym rozwiązaniem jest użycie miernika zwarć, lub omomierza, żeby dowiedzieć się, który kabel odpowiada której linii sygnałowej. Poniższe schematy powinny być przy tym przydatne.

Sygnał	Opis	Złącze PS/2	Komentarz
VCC	Zasilanie +5V	4	muszą zostać podłączone do modułu
GND	Masa zasilania	3	
CLK	Clock	5	
DATA	Dane	1	
NC	Nieużywane linie	2, 6	nie używane przez moduł, jeśli występują, zostawić w oryginalnym stanie
SHLD	Ekran	-	



Złącze PS/2 (nadajnik)

Sygnał	Opis	Złącze USB	Komentarz
VCC	Zasilanie +5V	1	muszą zostać podłączone do modułu
D-	Dane	2	
D+	Dane	3	
GND	Masa zasilania	4	
SHLD	Ekran	-	nie używane przez moduł, jeśli występują, zostawić w oryginalnym stanie



Złącze USB (odbiornik)

Jeśli mikrokontrolery których używasz nie zostały jeszcze zaprogramowane, teraz jest dobry moment na załadowanie firmware'u używając technologii ISP (In-System Programming). Przeczytaj sekcję firmware żeby uzyskać więcej szczegółów. Po wykonaniu tego kroku, zmontowane urządzenia powinny wyglądać jak te na poniższych zdjęciach.

Nadajnik z okablowaniem PS/2

Odbiornik z okablowaniem USB

Przed założeniem obudowy, zalecamy wykonanie ostatniego testu. Użyj miernika zwarć lub omomierza żeby zmierzyć rezystancję pomiędzy zasilaniem (VCC) a masą (GND) zarówno na złączu USB, jak i PS/2. Zwarcie oznacza, że należy sprawdzić cały układ, w przeciwnym wypadku może to doprowadzić do uszkodzenia komputera. Jeśli wszystko jest w porządku, zamknij obudowę używając kleju i czas na pierwsze podłączenie.

Uruchomienie

Po zmontowaniu układu nadajnik-odbiornik, czas wykonać pierwszy test. Zalecane jest użycie tylko jednego komputera do przetestowania obu urządzeń. Na początku wyłącz komputer i podłącz nadajnik pomiędzy klawiaturę PS/2 a port PS/2.

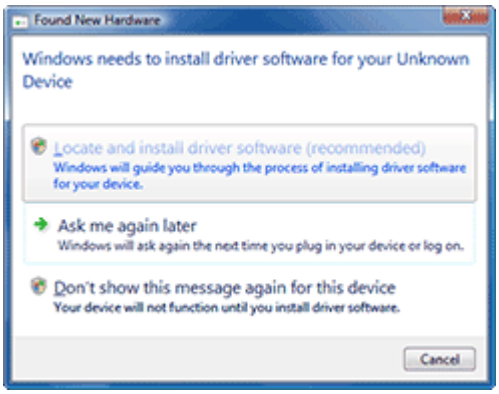
Podłącz nadajnik do portu PS/2

Podłącz klawiaturę PS/2 do nadajnika

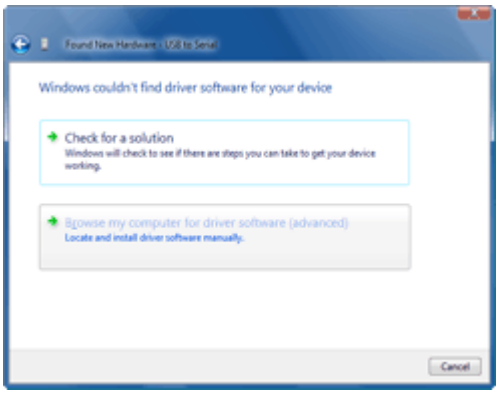
Po tym, włącz komputer i upewnij się, że klawiatura PS/2 działa poprawnie (nie powinien być widoczny żaden wpływ keyloggera). Następnie czas na test odbiornika. Przed tym należy ściągnąć plik sterownika KeeLog. Rozpakuj i zachowaj pliki na dysku lokalnym komputera. Następnie, podłącz odbiornik do wolnego portu USB (nie jest wymagane wyłączenie komputera przed tym). Upewnij się, że pozycja odbiornika umożliwia odbiór transmisji radiowej od nadajnika.

Podłącz odbiornik do wolnego portu USB

Gdy nadajnik jest podłączony pierwszy raz, pojawi się okno instalacji sterownika. Dokładnie rzecz biorąc, użyte zostaną sterowniki wirtualnego portu COM dostarczane z większością systemów operacyjnych, jak Windows. Jednak odpowiedni plik opisu INF musi zostać wybrany ręcznie. Gdy system zapyta o sterowniki, przejdź do ścieżki w której zostały zachowane pliki sterowników. Poniższe obrazki ilustrują cały proces.

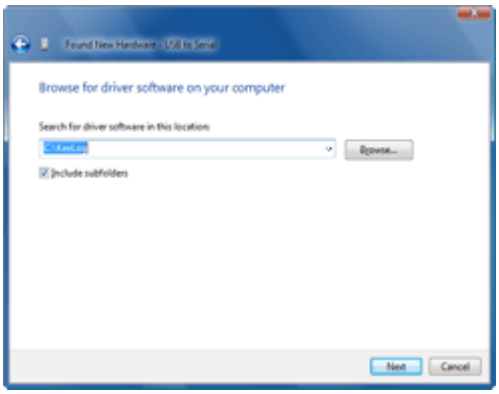


Wybierz lokalizację i instalację oprogramowania



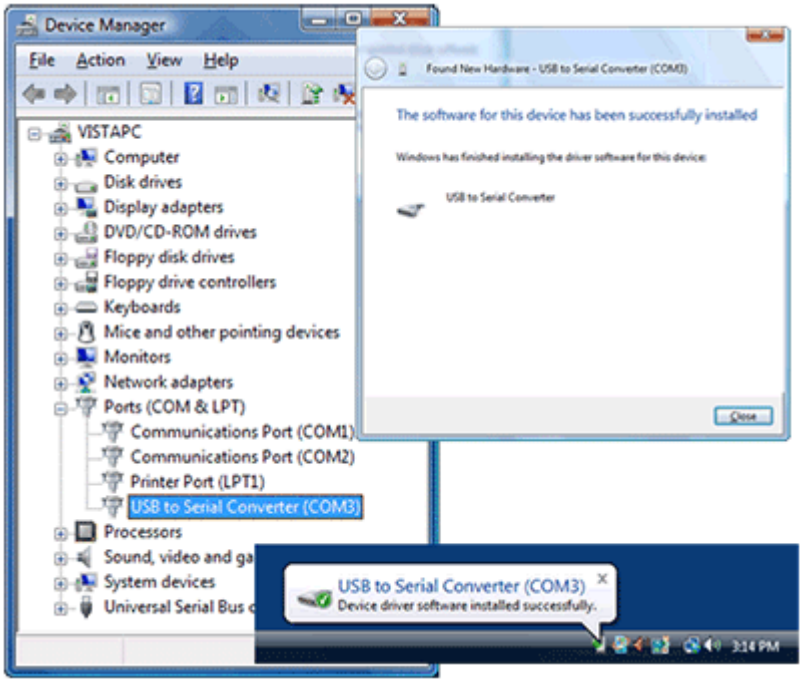
Wybierz lokalizację sterownika

Wybierz żeby pokazać opcję lokalizacji



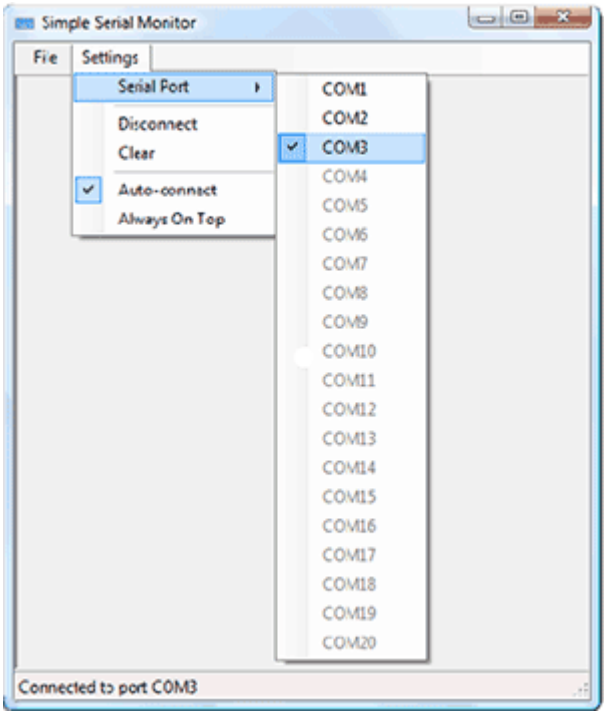
Wskaż położenie plików sterownika

Gdy proces instalacji zakończy się sukcesem, odbiornik powinien być widoczny jako konwerter USB na port szeregowy. Otwórz Menadżer Urządzeń w systemie Windows, żeby sprawdzić który port szeregowy został przypisany do odbiornika.



Odbiornik widoczny w Menadżerze Urządzeń

Żeby zacząć odbierać dane klawiatury od nadajnika, można użyć dowolnego klienta terminalu, jak na przykład Hyperterminal. Zalecamy użycie naszej darmowej aplikacji Simple Serial Monitor ze względu na jej wygodę i prostotę użycia.



Simple Serial Monitor (darmowy klient terminala dostarczony przez KeeLog)

Po uruchomieniu Simple Serial Monitor (lub alternatywnej aplikacji), pamiętaj żeby wybrać odpowiedni port COM. Jeśli wszystko przebiegło pomyślnie, odbiornik zacznie natychmiast wyświetlać strumień klawiszy naciśniętych na klawiaturze PS/2.

Komputer zdalny z nadajnikiem PS/2 *Komputer lokalny z odbiornikiem USB*

Następnym krokiem byłoby przetestowanie tego samego na dwóch różnych komputerach. Upewnij się, że są w zasięgu transmisji. Jeśli tekst pojawia się w oknie terminala, Twój Bezprzewodowy Keylogger jest gotowy na swoją pierwszą rzeczywistą misję. Pamiętaj żeby używać tego urządzenia zgodnie z prawem!

Download

Firmware dla mikrokontrolera umożliwiający zaprogramowanie nadajnika i odbiornika
http://www.keelog.com/files/WirelessKeyloggerFirmware.zip

Sterownik umożliwiający instalację odbiornika jako wirtualny port COM
http://www.keelog.com/files/UsbToSerial.zip

Darmowe oprogramowanie umożliwiające odbiór przechwyconych danych przez wirtualny port COM (odpowiednik aplikacji Hyperterminal). Wymaga platformy Microsoft .NET Framework.
http://www.keelog.com/files/SimpleSerialMonitor.zip

Oprogramowanie umożliwiające zaprogramowanie firmware'u używając SAM-BA
http://www.keelog.com/files/At91Isp.zip

Przewodnik jak zaprogramować firmware do mikrokontrolera przez wbudowany bootloader, bez użycia dodatkowego programatora
http://www.keelog.com/files/SambaUserGuide.pdf

Spis podzespołów użytych dla montażu Bezprzewodowego Keyloggera (nadajnik i odbiornik)
http://www.keelog.com/files/WirelessKeyloggerBom.pdf

Schemat okablowania dla Bezprzewodowego Keyloggera (nadajnik i odbiornik)
http://www.keelog.com/files/WirelessKeyloggerWiring.pdf

Schemat elektryczny Bezprzewodowego Keyloggera (nadajnik i odbiornik)
http://www.keelog.com/files/WirelessKeyloggerSchColor.pdf

Strona górna obwodu drukowanego (nadajnik i odbiornik)
http://www.keelog.com/files/WirelessKeyloggerPcbTop.pdf

Strona dolna obwodu drukowanego (nadajnik i odbiornik)
http://www.keelog.com/files/WirelessKeyloggerPcbBottom.pdf

Maska dla strony górnej obwodu drukowanego (nadajnik i odbiornik), skalowana 1:1
http://www.keelog.com/files/WirelessKeyloggerMaskTop.pdf

Maska dla strony dolnej obwodu drukowanego (nadajnik i odbiornik), skalowana 1:1
http://www.keelog.com/files/WirelessKeyloggerMaskBottom.pdf

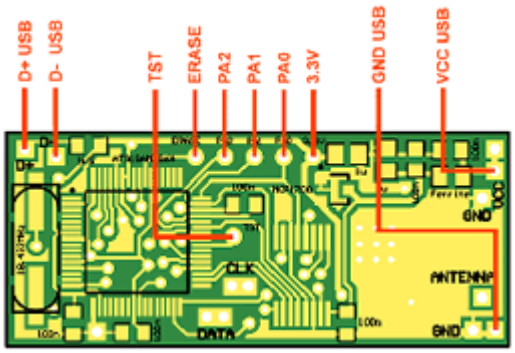
Firmware

Przeczytaj ten rozdział tylko jeśli potrzebujesz zaprogramować mikrokontroler AT91SAM7S64 samodzielnie. Jeśli zakupiłeś zestaw od nas, wykonaliśmy już ten krok za Ciebie.

Współczesne mikrokontrolery, jak Atmel AT91SAM7S64 mają gęsto upakowane obudowy, co sprawia trudności przy znalezieniu tradycyjnego programatora obsługujący dany typ mikrokontrolera. Z tego względu programowanie w układzie ISP (In-System Programming) rozwija się bardzo szybko w ostatnich latach. ISP umożliwia wpierw montaż całego obwodu, a następnie zaprogramowanie firmware'u, często używając bardzo prostych narzędzi. Mikrokontroler AT91SAM7S64 posiada bardzo wygodne rozwiązanie ISP, w oparciu o wbudowany moduł USB. Nosi nazwę SAM-BA (SAM Boot Assistant), i wymaga wyłącznie kabla USB oraz kilku prostych zworek. Żeby uruchomić SAM-BA na Bezprzewodowym Keyloggerze, ściągnij najpierw oprogramowanie AT91 ISP. Następnie, przejdź poniższe kroki żeby załadować firmware na moduł odbiornika i nadajnika.

Krok 1: Dotyczy wyłącznie nadajnika. Przygotuj kabel USB ze złączem typu A po jednej stronie, i odizolowanymi kablami po drugiej stronie. Przylutuj linie USB: VCC, GND, D+, oraz D- do odpowiednich punktów na obwodzie drukowanym. Ten krok jest zbędny dla odbiornika, ponieważ ma on już przygotowane złącze USB.

Krok 2: Przygotuj kilka krótkich drutów żeby zwierać piny SAM-BA: TST, ERASE, PA2, PA1, PA0, 3.3V. Przylutuj jeden koniec każdego z drutów do odpowiedniego punktu lutowniczego SAM-BA na obu płytkach. Alternatywnie, możesz przygotować specjalne zworki, jak pokazano na poniższych rysunkach.



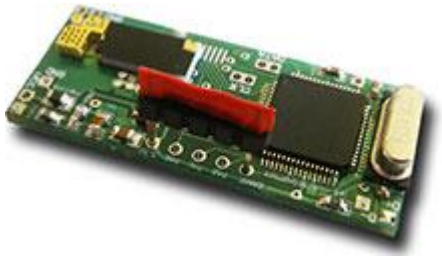
Schemat okablowania SAM-BA

Krok 3: Zainstaluj pakiet oprogramowania AT91 ISP.

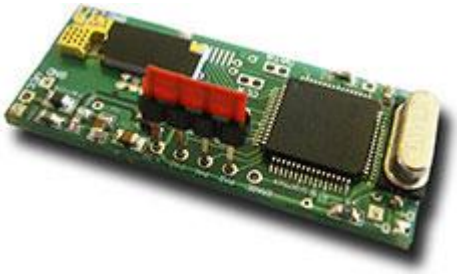
Krok 4: Podłącz urządzenie do wolnego portu USB. Komunikat Nierozpoznane urządzenie jest na tym etapie normalny.

Krok 5: Zewrzyj złącze ERASE do 3.3V na krótki moment. Spowoduje to wykasowanie pamięci flash mikrokontrolera.

Kabel USB i zworki dla bootloadera SAM-BA



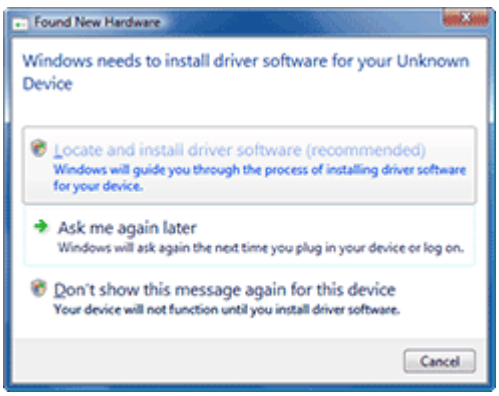
Kasowanie pamięci (ERASE zwarty do 3.3V)



Aktywacja bootloadera (PA0, PA1, PA2 i TST zwarte do 3.3V)

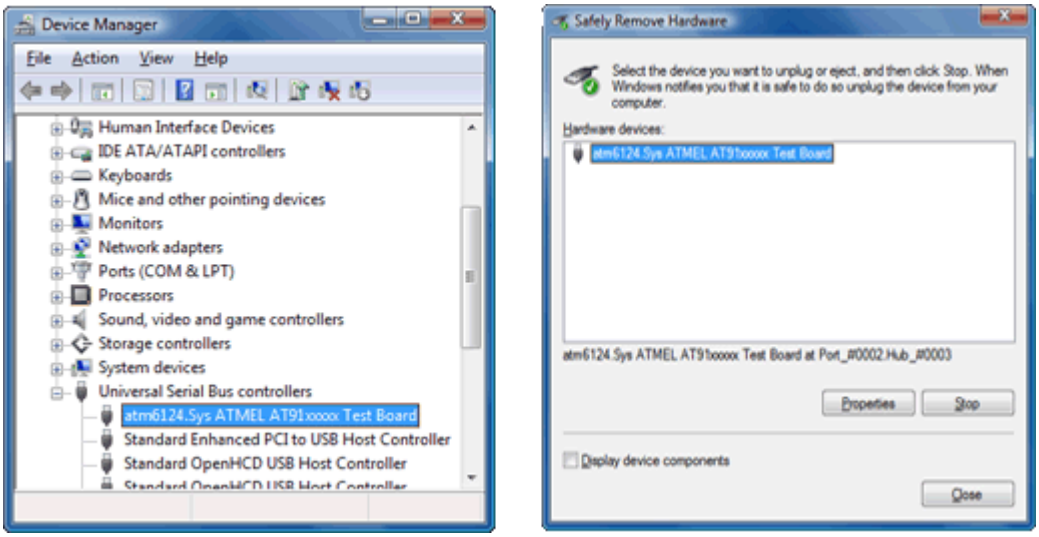
Krok 6: Odłącz urządzenie od portu USB. Upewnij się, że złącze ERASE nie jest już podłączone do 3.3V. Następnie, zewrzyj zestaw złącz PA0, PA1, PA2 i TST do 3.3V. Podłącz ponownie urządzenie do portu USB (Nierozpoznane urządzenie może się znowu pojawić). Zostaw urządzenie podłączone przez około 10 sekund, a następnie odłącz je od portu USB. Ta operacja powinna była aktywować wewnętrzny bootloader SAM-BA.

Krok 7: Usuń wszystkie zworki lub złącza i podłącz urządzenie do portu USB. Komunikat Znaleziono nowy sprzęt powinien się pojawić. Przeprowadź standardową procedurę instalacji i pozwól systemowi znaleźć sterowniki samodzielnie.



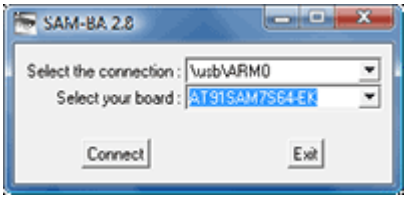
Dialog Znaleziono nowy sprzęt

Krok 8: Otwórz Menadżer Urządzeń żeby się upewnić, że bootloader SAM-BA został aktywowany.



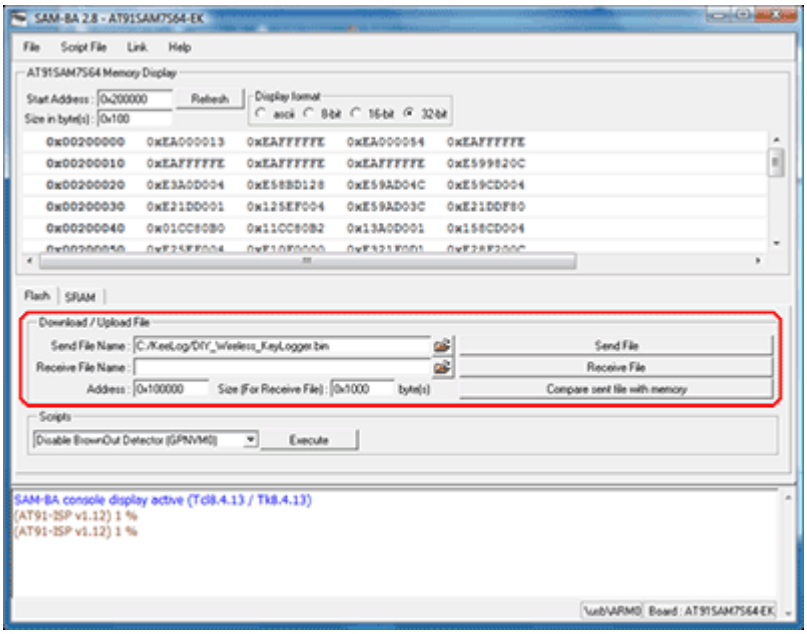
Menadżer Urządzeń z urządzeniem Atmel AT91

Krok 9: Uruchom aplikację SAM-BA z pakietu oprogramowania AT91 ISP i wybierz docelową platformę sprzętową AT91SAM7S64-EK.



Wybór platformy sprzętowej

Krok 10: Po podłączeniu do platformy sprzętowej, przełącz na zakładkę Flash, wybierz odpowiedni firmware dla nadajnika/odbiornika, a następnie kliknij Send File. Kiedy aplikacja zapyta czy odblokować i zablokować odpowiednie rejony pamięci flash, należy wybrać Yes. Jeśli ten krok przebiegł pomyślnie, oznacza to, że firmware został poprawnie załadowany do pamięci flash mikrokontrolera.



Aplikacja SAM-BA

Pamiętaj, żeby powtórzyć procedurę SAM-BA zarówno dla nadajnika, jak i odbiornika. Po zakończeniu, oba urządzenia są gotowe do działania.