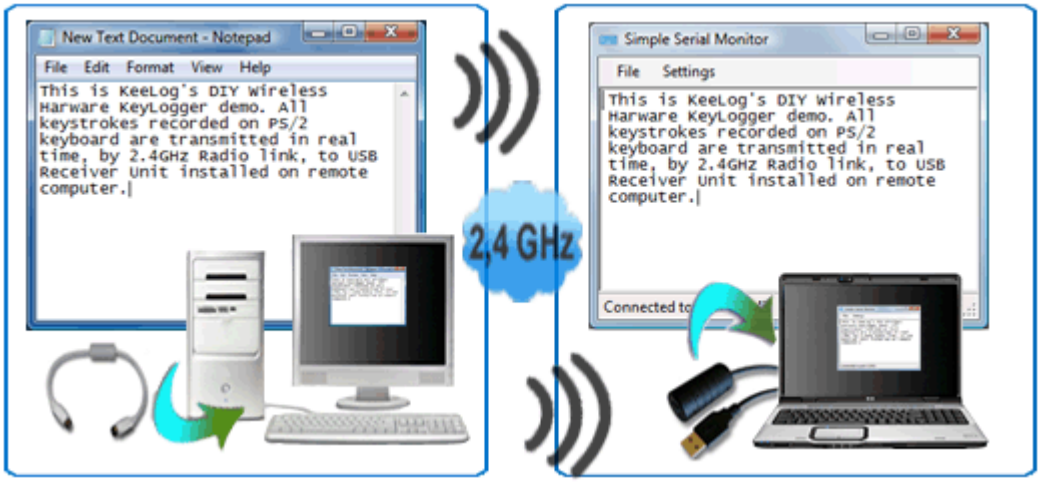
Keylogger sem fio

Faça Você Mesmo!



Introdução

Conhece o termo keylogger de hardware? Keylogger de Hardware é a solução ideal para monitorizar as actividades do utilizador do computador, sendo mínimo o risco de detecção. O Keylogger de Hardware é um dispositivo 100% electrónico e por isso não requer acesso ao sistema operativo, não deixa rastos e o software não é capaz de detectar este tipo de dispositivo. No entanto, o conceito de keylogger de hardware tem uma desvantagem: para recuperar os dados captados, é indispensável o acesso físico ao dispositivo. Entretanto, este problema já tem solução: Keylogger sem fio.

KeeLog já publicou um projecto de keylogger de hardware PS/2 tipo Open Source. Agora fazemos a mesma coisa com o projecto de Keylogger sem fio, destinado para a montagem individual. Este projecto pode ser usado tanto para os fins privados como os comerciais, com as restrições que se seguem:

1. Todos os materiais incluídos neste site da Internet são propriedade intelectual da empresa KeeLog e a utilização dos mesmos implica a aceitação das condições mencionadas a seguir e o Contrato de Licença do Utilizador.
2. Este projecto de Keylogger sem fio foi publicado "tal como é", com todos os defeitos e sem qualquer garantia.

O keylogger sem fio não deve ser utilizado para a captação ilegal dos dados alheios, sobretudo senhas, dados bancários, correspondência confidencial, etc. Em muitos países o referido é considerado infracção.

O keylogger sem fio é composto por duas partes principais: o transmissor e o receptor. O registo efectivo das teclas realiza-se no transmissor, que na verdade é um keylogger de hardware PS/2, com o módulo de rádio 2.4 GHz incorporado. Os dados captados do teclado não são arquivados na memória, mas sim transmitidos em tempo real através da conexão por rádio. O receptor, por outro lado, é um dispositivo de aquisição sem fio com interface USB. Todos os dados recebidos do transmissor são enviados para o computador através de USB. Do ponto de vista de software, estes dados estão disponíveis através da porta virtual COM, o que permite a sua visualização por qualquer cliente do terminal.

Keylogger sem fio - esquema de blocos

O sistema funciona em tempo real, por isso o texto que se está a escrever num computador remoto é visível imediatamente do lado do receptor. O alcance máximo do sistema é de 50 metros aproximadamente, o que corresponde ao alcance eficaz de aproximadamente 20 metros, atravessando 2-4 paredes, em função da sua espessura.

Keylogger sem fio - transmissor

Keylogger sem fio - receptor

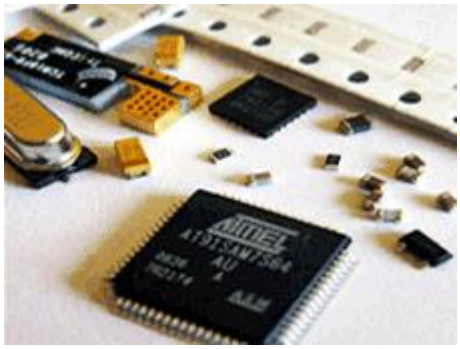
Tanto o transmissor, como receptor baseiam-se no mesmo diagrama de circuitos e circuito impresso. Ambos têm as mesmas dimensões e devem ser montados nas extensões curtas PS/2 e USB. É recomendável usar as caixas de filtros tipo EMC, para que o dispositivo seja parecido com um adaptador ou uma extensão.

Subconjuntos

Este artigo descreve todo o processo de montagem do keylogger sem fio. Em função das suas capacidades, poderá decidir fazer o seu próprio keylogger sem fio do princípio, ou fazer a encomenda dos subconjuntos connosco. Nós podemos fornecer-lhe um kit de subconjuntos junto com os microcontroladores programados e as caixas típicas (veja as fotos), ou um kit de dispositivos completamente montado e verificado. Passe à secção kits, para conhecer mais detalhes.

Se você decidiu criar o seu próprio keylogger sem fio, deverá ter experiência básica na electrónica e na soldadura, de preferência na tecnologia de montagem superficial (SMT). A opção mais simples consiste em fazer a encomenda dum kit de subconjuntos connosco e fazer por si mesmo a soldadura, o sistema de cabos e a montagem final. Para isso deverá ter um ferro de soldar com regulação de temperatura e uma boa aptidão de soldar. Se você decidir desenhar e fazer os circuitos impressos por si mesmo, deverá ter grande experiência e equipamento adequado.

Na tabela a seguir encontrará uma lista de subconjuntos (BOM) indispensáveis para a execução de uma unidade de transmissor ou receptor. Uma extensão adicional PS/2 é requerida para o transmissor, e o cabo USB com conector tipo A é requerido para o receptor.



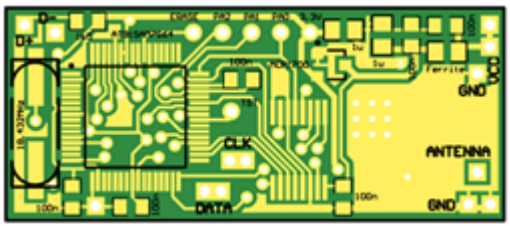
Kit de subconjuntos electrónicos

Cabos, caixa e circuitos impressos

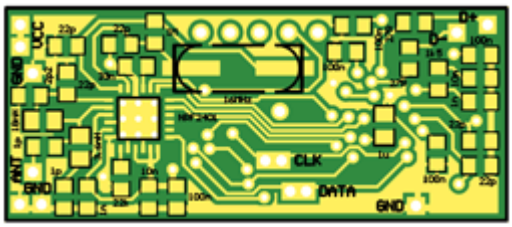
Designação	Descrição	Caixa	Quantia
U1	Microcontrolador AT91SAM7S64	TQFP64	1
U2	Transceiver nRF2401	QFN24	1
U3	Estabilizador MCP1700T-330	SOT-23	1
Q1	Oscilador de cristal 18.432 MHz	HC-49 SMD	1
Q2	Oscilador de cristal 16 MHz	HC-49 SMD	1
R1, R2	Resistência 1.5 kΩ	0805	2
R3, R4	Resistência 27 Ω	0805	2
R5	Resistência 1 MΩ	0805	1
R6	Resistência 22 kΩ	0805	1
C1, C27	Condensador 10 nF	0805	2
C2, C28	Condensador 1 nF	0805	2
C3, C4, C6, C7, C8	Condensador 22 pF	0805	5
C5	Condensador 33 nF	0805	1
C9	Condensador 2.2 pF	0805	1
C10, C11	Condensador 1 pF	0805	2
C12, C22, C23, C24, C25, C26, C32, C33, C34, C42, C43	Condensador 100 nF	0805	11
C21, C31, C41	Condensador 1 µF	0805	3
L1	Conta de ferrite	0805	1
L2	Indutor 3.6 nH	0805	1
L3	Indutor 18 nH	0805	1

Keylogger sem fio - lista de subconjuntos

Tanto o transmissor como receptor usam o mesmo circuito impresso e o mesmo kit de subconjuntos (só os cabos e firmware são diferentes). O microcontrolador Atmel AT91SAM7S64 e o transceiver de rádio nRF2401 são subconjuntos chave do circuito electrónico. Ambos requerem osciladores de cristal para o seu funcionamento correcto. Além do estabilizador MCP1700, todos os restantes subconjuntos são passivos (resistências, condensadores e alguns indutores). Um pedaço de arame é recomendado para servir de antena dipolo. O circuito impresso bilateral de duas camadas foi apresentado nas figuras que se seguem.

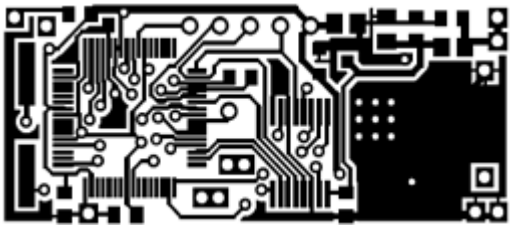


Distribuição do circuito impresso - página superior

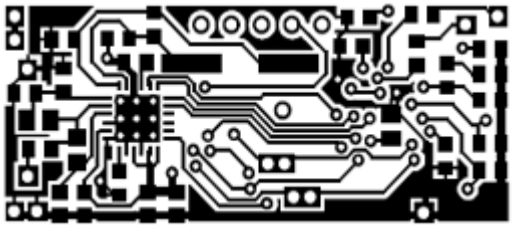


Distribuição do circuito impresso - página inferior

Se você tem experiência suficiente para fazer os circuitos impressos por si mesmo, poderá aproveitar um kit de máscaras em escala 1:1 disponíveis abaixo. O desenho de referência utiliza o laminado tipo FR4 de 1 mm de espessura.



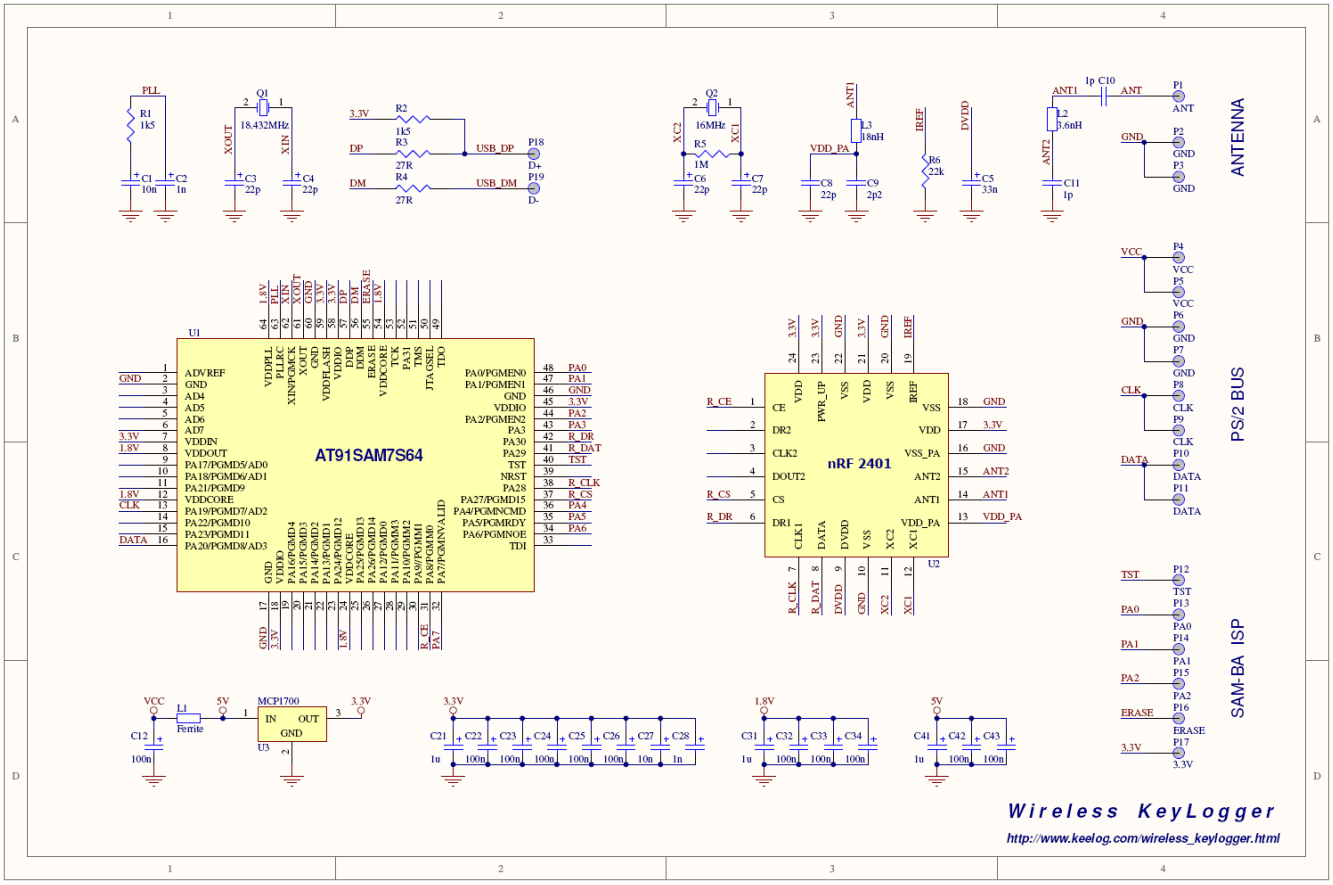
Máscara para o circuito impresso - página superior



Máscara para o circuito impresso - página inferior

Montagem

O circuito do keylogger sem fio é composto por dois elementos principais: microcontrolador AT91SAM7S64 e transceiver nRF2401. Os elementos passivos que os acompanham são, sobretudo, um oscilador e circuitos de alta frequência RF. Todo o circuito é alimentado através de 3.3V, gerados através de um estabilizador MCP1700 e filtrados através de um grupo de condensadores. A alimentação de entrada é tomada directamente do barramento PS/2 (transmissor), ou USB (receptor). Se já possui os circuitos impressos montados, passe à secção conjunto de cabos. Se optou pela montagem individual, as indicações e os diagramas de circuito que se seguem serão úteis para si.



Keylogger sem fio - diagramas de circuito

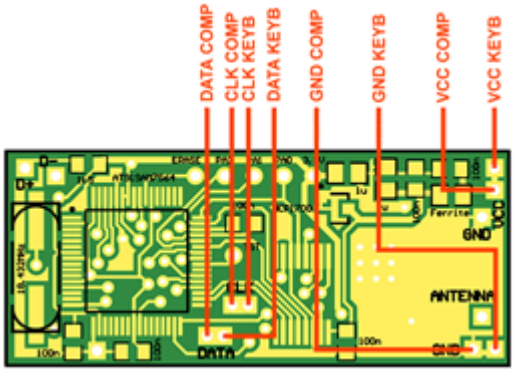
Para soldar, use um ferro de soldar com ponta fina (tipicamente inferior a 0.5 mm) e a pasta de soldar (por exemplo RMA7). Não deixe que os elementos sofram sobreaquecimento durante a soldadura. Comece a montagem a partir do transceiver nRF2401 devido ao tipo complicado da caixa. A seguir passe para o microcontrolador AT91SAM7S64 e estabilizador MCP1700. Lembre-se de que o pino número 1 na caixa deve corresponder ao primeiro pino no circuito impresso. Finalmente, solde todos os circuitos adicionais: os osciladores de cristal, resistências, condensadores e indutores. Deixe a antena para o final da operação. Poderá usar a antena específica para a banda ISM 2.4 GHz, ou faça uma simples antena dipolo de um quarto de onda, usando um pedaço de arame. O comprimento aconselhável é de 3,125 cm (1.23"). Os circuitos

impressos montados devem ser parecidos aos que foram apresentados nas fotos abaixo.

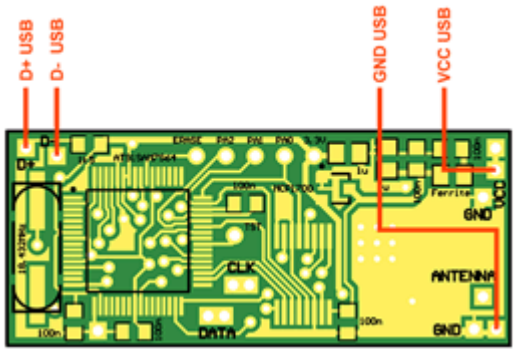
Circuito impresso montado - página superior com microcontrolador

Circuito impresso montado - página inferior com transceiver

Depois da montagem dos circuitos impressos é preciso fazer o conjunto de cabos. Além de firmware, é um aspecto em que o transmissor difere do receptor. O transmissor deve estar acoplado paralelamente com o barramento PS/2. O circuito impresso do transmissor possui pads que permitem soldar os cabos que vão tanto para o computador, como para o teclado. No entanto, o receptor deve ter uma ligação típica com a porta USB. As fotos abaixo demonstram como se devem fazer todas as ligações.



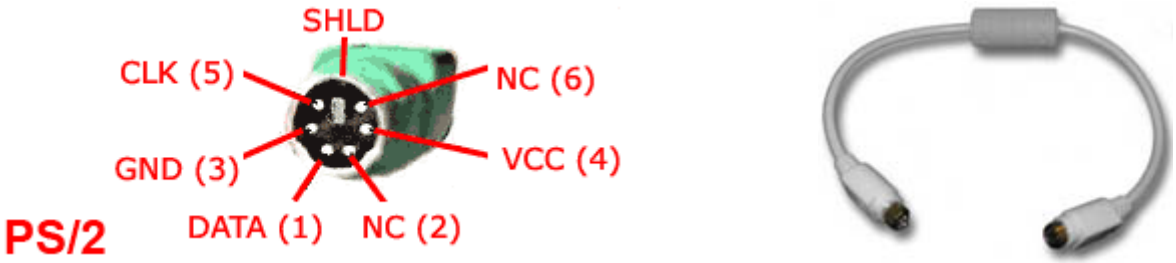
Esquema do conjunto de cabos PS/2 para o transmissor



Esquema do conjunto de cabos USB para o receptor

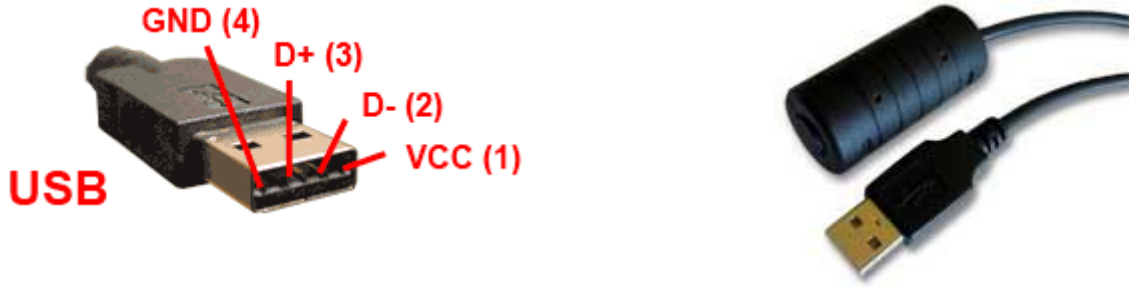
Use as extensões PS/2 e USB, corte-as e isole as linhas de sinal. Poderá ter certos problemas com a coordenação dos cabos com os sinais adequados. Certos cabos PS/2 e USB têm cores típicas, mas seria muito arriscado confiar nisso. A solução recomendável é utilizar um medidor de curto-circuitos ou ohmímetro para saber quais são os cabos que correspondem a cada uma das linhas de sinal. Os diagramas que se seguem deverão ser-lhe úteis.

Sinal	Descrição	Conector PS/2	Comentário
VCC	Alimentação +5V	4	devem estar ligados ao módulo
GND	Massa de alimentação	3	
CLK	Clock	5	
DATA	Dados	1	
NC	Líneas no utilizadas	2, 6	não utilizadas pelo módulo; se houver, deixar no seu estado original
SHLD	Ecrã	-	



Conector PS/2 (transmissor)

Sinal	Descripción	Conector USB	Comentário
VCC	Alimentação +5V	1	devem estar ligados ao módulo
D-	Dados	2	
D+	Dados	3	
GND	Massa de alimentação	4	
SHLD	Ecrã	-	não utilizadas pelo módulo; se houver, deixar no seu estado original



Conector USB (receptor)

Caso os microcontroladores que você usa ainda não estejam programados, é um bom momento para descarregar firmware utilizando a tecnologia ISP (In-System Programming). Leia a secção firmware para conhecer mais detalhes. Depois de tomar este passo, os dispositivos montados deverão ser assim como os nas fotos abaixo.

Transmissor com o conjunto de cabos PS/2

Receptor com o conjunto de cabos USB

Antes de colocar a caixa, recomendamos que se faça a última prova. Use um medidor de curto-circuitos ou ohmímetro para medir a resistência entre a alimentação (VCC) e a massa (GND), tanto na conexão USB como PS/2. O curto-circuito significará que é preciso examinar todo o sistema. Caso contrário poderá avariar o computador. Se tudo correr bem, feche a caixa usando cola. Agora já pode fazer a primeira ligação.

Arranque

Uma vez montado o sistema transmissor-receptor, será preciso fazer a primeira prova. É recomendável que se use só um computador para examinar ambos dispositivos. Para começar, desligue o computador e ligue o transmissor entre o teclado PS/2 e a porta PS/2.

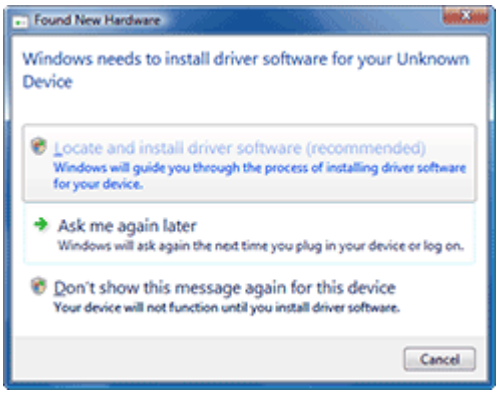
Ligue o transmissor à porta PS/2

Ligue o teclado PS/2 ao transmissor

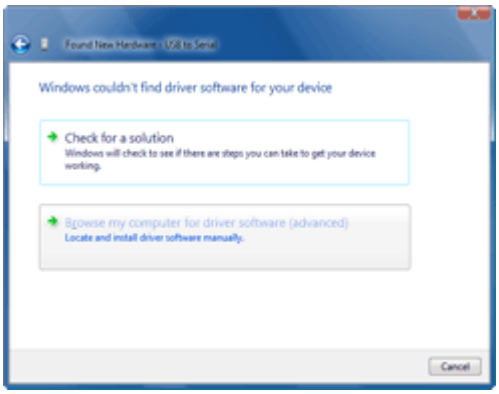
Quando já o fizer, ligue o computador e assegure-se de que o teclado PS/2 funciona correctamente (não deverá observar qualquer tipo de influências do lado do keylogger). A seguir, faça a prova do receptor. Antes, é preciso descarregar o ficheiro do driver KeeLog. Descompacte e guarde os ficheiros no disco local do computador. A seguir, ligue o receptor à porta USB livre (não é requerido desligar o computador antes de que o faça). Assegure-se, de que a posição do receptor permitirá realizar a transmissão rádio desde o transmissor.

Ligue o receptor à porta USB livre

Quando o transmissor for ligado pela primeira vez, aparecerá a janela de instalação do driver. Precisamente, serão utilizados os drivers da porta virtual COM fornecidos junto com a maioria dos sistemas operativos, por exemplo Windows. No entanto, o ficheiro de descrição INF adequado deverá ser seleccionado manualmente. Quando o sistema perguntar sobre o driver, passe àquela rota em que foram guardados os ficheiros dos drivers. As imagens a seguir ilustram todo o processo.

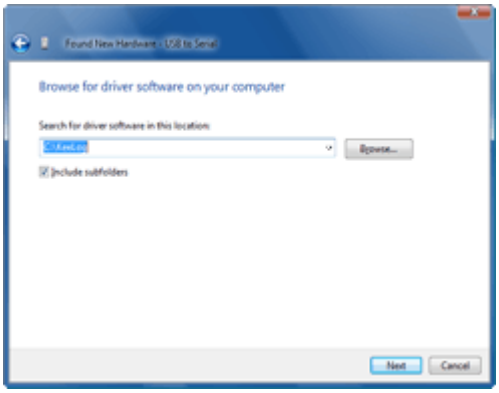


Escolha a localização e instalação de software



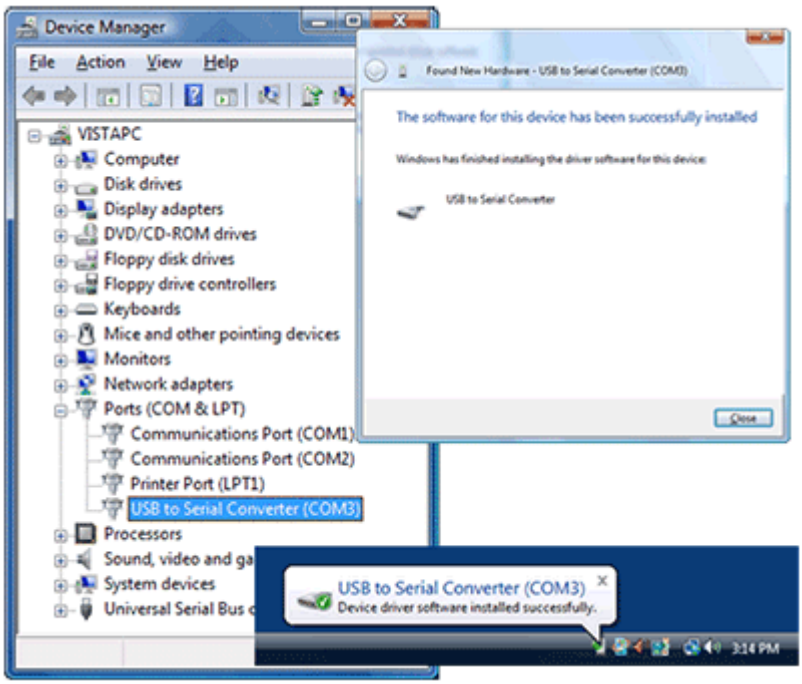
Escolha a localização do driver

Escolha para mostrar a opção de localização



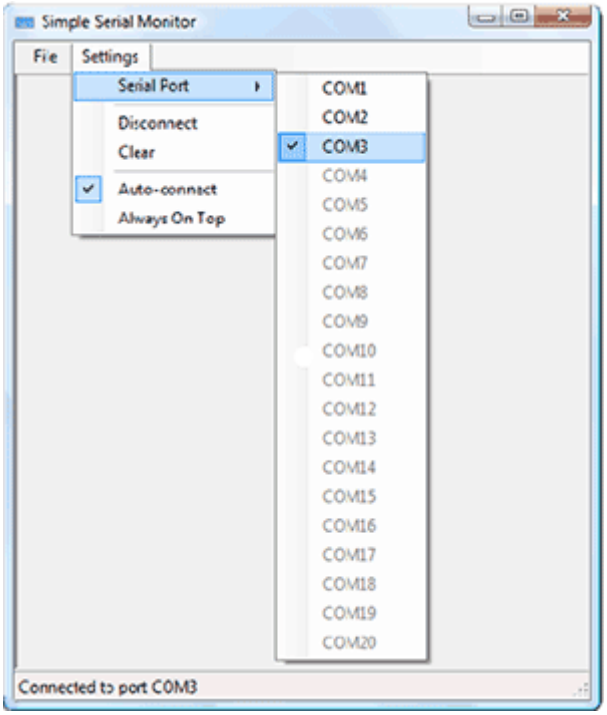
Indique a localização dos ficheiros do driver

Se o processo de instalação terminar com êxito, o receptor deverá ser visível como o conversor de USB para porta serial. Abra o Gestor de Dispositivos no sistema Windows para verificar qual é a porta serial que foi atribuída ao receptor.



Receptor visível no Gestor de Dispositivos

Para começar a receber os dados de teclado do transmissor, pode-se usar qualquer cliente de terminal, por exemplo Hyperterminal. Recomendamos o uso da nossa aplicação gratuita Simple Serial Monitor devido à comodidade e simplicidade do seu uso.



Simple Serial Monitor (cliente de terminal gratuito fornecido por KeeLog)

Uma vez posto em funcionamento o Simple Serial Monitor (ou uma aplicação alternativa), lembre-se de escolher a porta COM adequada. Se tudo correr bem, o receptor começará a visualizar imediatamente todos os toques nas teclas do teclado PS/2.

Computador remoto com transmissores PS/2 *Computador local com receptor USB*

O passo a seguir seria o teste da mesma coisa em dois computadores diferentes. Assegure-se de que estão dentro do alcance da transmissão. Se o texto aparece na janela do terminal, o seu keylogger sem fio está pronto para iniciar a sua primeira missão. Lembre-se de usar este dispositivo conforme à lei!

Download

Firmware para o microcontrolador que permite programar o transmissor e receptor
http://www.keelog.com/files/WirelessKeyloggerFirmware.zip

Driver que permite a instalação do receptor como a porta virtual COM
http://www.keelog.com/files/UsbToSerial.zip

Software gratuito que permite a recepção dos dados captados através da porta virtual COM (homólogo da aplicação Hyperterminal). Requer plataformas Microsoft .NET Framework.
http://www.keelog.com/files/SimpleSerialMonitor.zip

Software que permite programar firmware utilizando SAM-BA
http://www.keelog.com/files/At91Isp.zip

Uma guia que ensina como programar firmware para o microcontrolador através do bootloader incorporado, sem usar um programador adicional
http://www.keelog.com/files/SambaUserGuide.pdf

Lista de subconjuntos usados para montar o keylogger sem fio (transmissor e receptor)
http://www.keelog.com/files/WirelessKeyloggerBom.pdf

Esquema do conjunto de cabos para o keylogger sem fio (transmissor e receptor)
http://www.keelog.com/files/WirelessKeyloggerWiring.pdf

Diagramas de circuito do Keylogger sem fio (transmissor e receptor)
http://www.keelog.com/files/WirelessKeyloggerSchColor.pdf

Página superior do circuito impresso (transmissor e receptor)
http://www.keelog.com/files/WirelessKeyloggerPcbTop.pdf

Página inferior do circuito impresso (transmissor e receptor)
http://www.keelog.com/files/WirelessKeyloggerPcbBottom.pdf

Máscara para a página superior do circuito impresso (transmissor e receptor), em escala 1:1
http://www.keelog.com/files/WirelessKeyloggerMaskTop.pdf

Máscara para a página inferior do circuito impresso (transmissor e receptor), em escala 1:1
http://www.keelog.com/files/WirelessKeyloggerMaskBottom.pdf

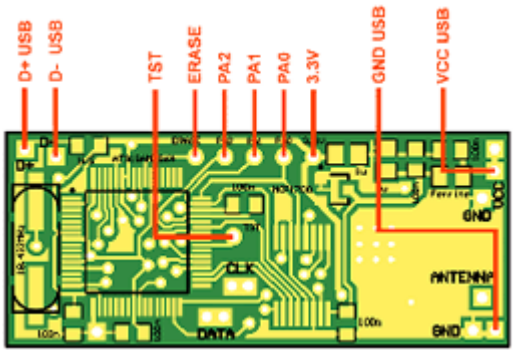
Firmware

Leia este capítulo só se precisa de programar o microcontrolador AT91SAM7S64 por si mesmo. Se comprou o nosso kit, nós já tomámos este passo por si.

Os microcontroladores modernos, tais como Atmel AT91SAM7S64 têm as caixas superlotadas, o que faz difícil encontrar um programador tradicional que possa trabalhar com um determinado tipo de microcontrolador. Por este motivo a programação no sistema ISP (In-System Programming) desenvolve-se rapidamente nos últimos anos. ISP permite, primeiro, a montagem do circuito inteiro, e a seguir a programação de firmware, utilizando as ferramentas muito simples em várias ocasiões. O microcontrolador AT91SAM7S64 possui a solução ISP muito cómoda, com base no módulo USB incorporado. Chama-se SAM-BA (SAM Boot Assistant) e requer só um cabo USB e algumas ligações em ponte simples. Para pôr em funcionamento SAM-BA no keylogger sem fio, descarregue primeiro o software AT91 ISP. A seguir, tome os seguintes passos para descarregar firmware no módulo de receptor e transmissor.

Passo 1: Só se refere ao transmissor. Prepare o cabo USB com o conector tipo A dum lado e com cabos não isolados do outro lado. Solde as linhas USB: VCC, GND, D+, e D- nos pontos adequados no circuito impresso. Este passo é dispensável no caso do receptor que já tenha o conector USB preparado.

Passo 2: Preparar alguns pedaços curtos de arame para juntar os pinos SAM-BA: TST, ERASE, PA2, PA1, PA0, 3.3V. Solde um extremo de cada arame no ponto de soldadura adequado SAM-BA em ambas placas. Alternativamente, poderá preparar ligações em ponte especiais, assim como foi demonstrado nas imagens que se seguem.



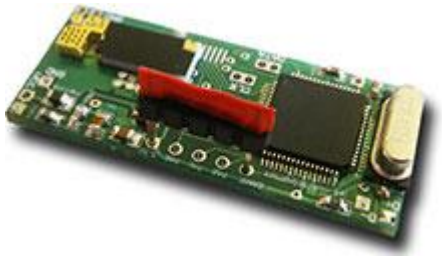
Esquema do conjunto de cabos SAM-BA

Passo 3: Instale o pacote de software AT91 ISP.

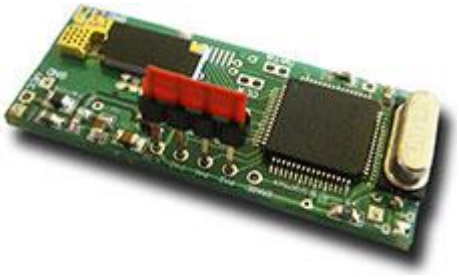
Passo 4: Ligue o dispositivo à porta USB livre. O comunicado Dispositivo não reconhecido é normal nesta etapa.

Passo 5: Ponha em curto-circuito o conector ERASE e 3.3V por um momento. Desta forma apagará a memória flash do microcontrolador.

O cabo USB e as ligações em ponte para o bootloader SAM-BA



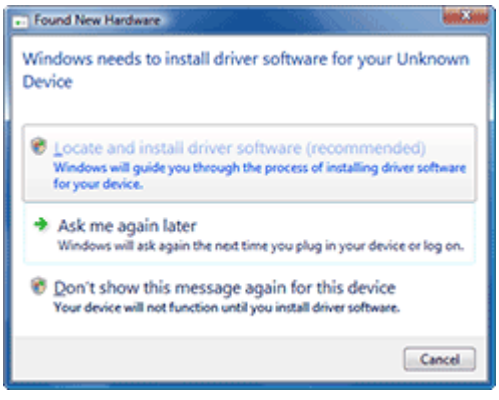
Apagamento da memória (ERASE posto em curto-circuito com 3.3V)



Activação do bootloader (PA0, PA1, PA2 e TST postos em curto-circuito com 3.3V)

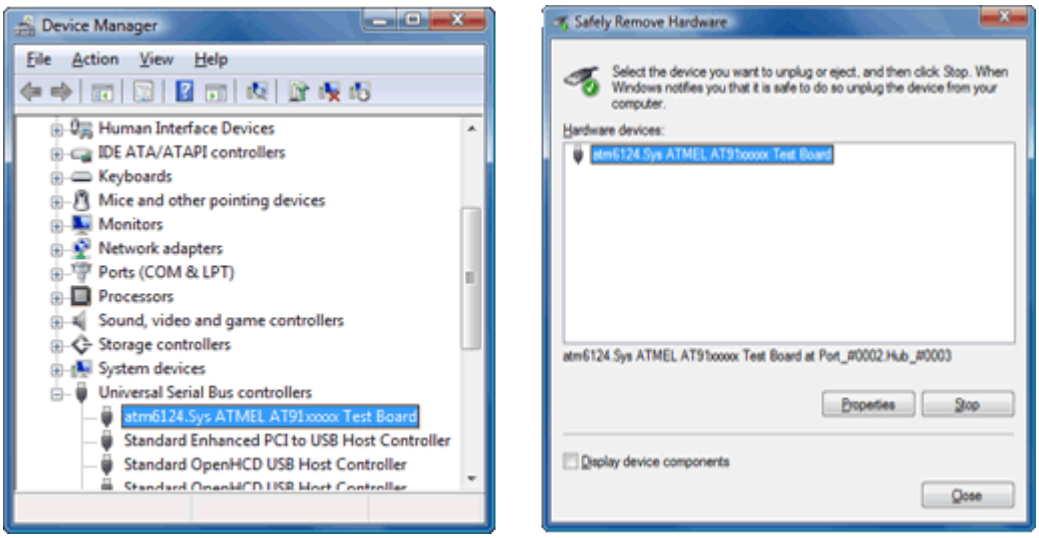
Passo 6: Desligue o dispositivo da porta USB. Assegure-se de que o conector ERASE já não esta ligado a 3.3V. A seguir, ponha em curto-circuito o conjunto de conectores PA0, PA1, PA2 e TST com 3.3V. Ligue de novo o dispositivo à porta USB (Dispositivo não reconhecido pode aparecer outra vez). Deixe o dispositivo ligado durante cerca de 10 segundos, e a seguir desligue-o da porta USB. Esta operação deveria ter activado o bootloader interno SAM-BA.

Passo 7: Eliminar todas as ligações em ponte ou conectores e ligar o dispositivo à porta USB. O comunicado Novo hardware encontrado deve aparecer. Proceda ao procedimento padrão de instalação e deixe que o sistema encontre os drivers por si mesmo.



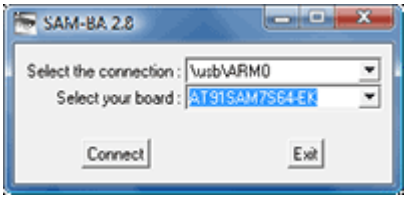
Diálogo Novo hardware encontrado

Passo 8: Abra o Gestor de Dispositivos para assegurar-se de que o bootloader SAM-BA foi activado.



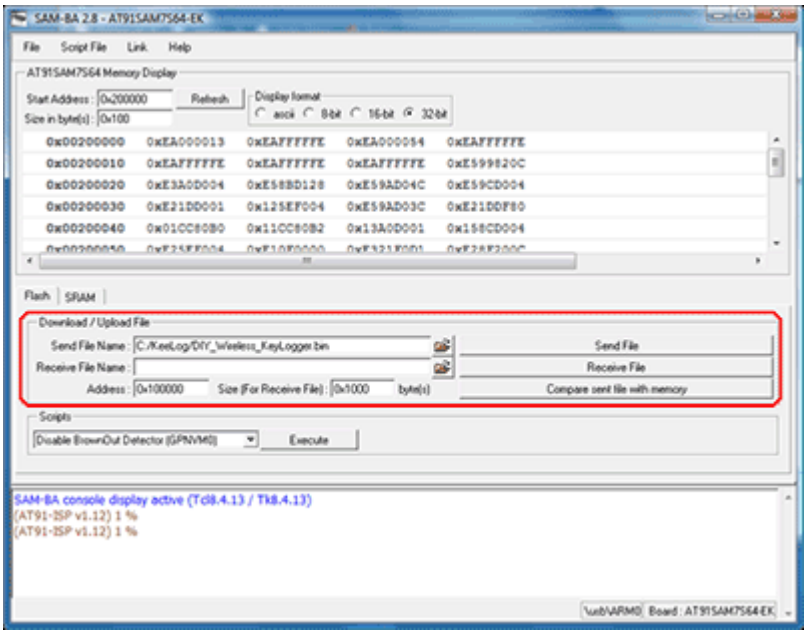
Gestor de Dispositivos com o dispositivo Atmel AT91

Passo 9: Arranque a aplicação SAM-BA do pacote de software AT91 ISP e escolha a plataforma de hardware alvo AT91SAM7S64-EK.



Escolha da plataforma de hardware

Passo 10: Uma vez ligada a plataforma de hardware, passe para o marcador Flash, escolha o adequado firmware para o transmissor/receptor, e a seguir clique Send File. Quando a aplicação perguntar se deve desbloquear e bloquear as regiões pertinentes da memória flash, é preciso escolher Yes. Se este passo foi dado com êxito, o firmware foi correctamente descarregado na memória flash do microcontrolador.



Aplicação SAM-BA

Lembre-se de repetir o procedimento SAM-BA tanto para o transmissor, como para o receptor. Depois de terminar, ambos dispositivos estarão prontos a funcionar.