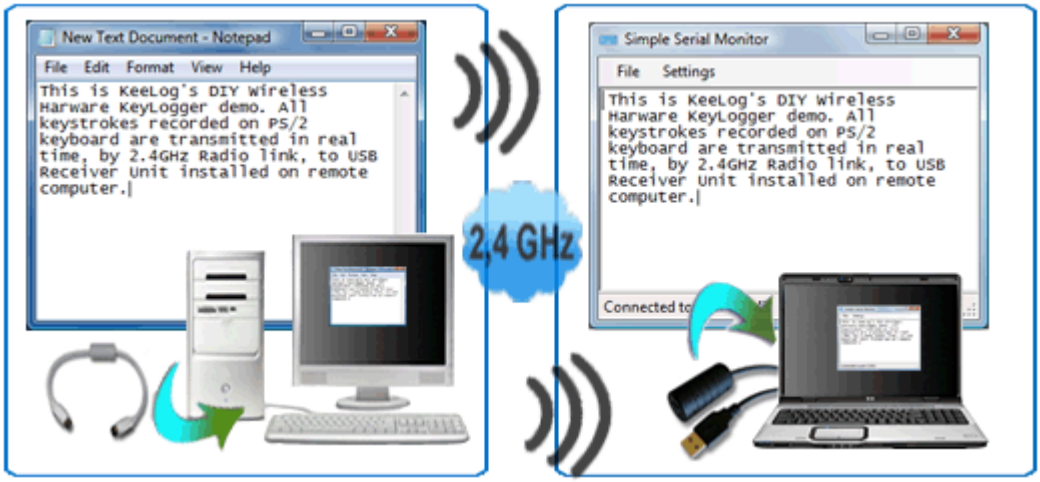
Keylogger wireless

Fai da te!



Introduzione **2**

Sottogruppi **4**

Montaggio **7**

Avviamento **11**

Download **15**

Firmware **16**

Introduzione

Conosci il concetto di hardware keylogger? L'hardware keylogger è la soluzione ideale per monitorare l'attività dell'utente di un computer con il rischio minimo di essere scoperto. Il hardware keylogger è un dispositivo elettronico al 100% non esige quindi l'acceso al sistema operativo, non lascia alcuna traccia e il software non è in grado di individuare questo dispositivo. Il concetto di hardware keylogger ha invece un inconveniente: per recuperare i dati intercettati è indispensabile un accesso fisico con un dispositivo. Ma questo problema è stato già risolto: Keylogger wireless.

KeeLog ha già pubblicato nel passato un progetto di hardware keylogger PS/2 tipo Open Source. Adesso facciamolo di nuovo con un progetto del Keylogger wireless, destinato al montaggio autonomo. Questo progetto può esser utilizzato sia per uso privato sia commerciale con le seguenti riserve:

1. Tutto il contenuto del sito internet è di proprietà intellettuale della ditta KeeLog e il suo utilizzo comporta l'accettazione delle seguenti condizioni e del Contratto dell'Utente generale.
2. Questo progetto del Keylogger wireless è stato pubblicato semplicemente "così com'è" con tutti i difetti e senza nessuna garanzia

Keylogger wireless non dovrebbe essere utilizzato per l'intercettazione illegale di dati altrui, specialmente nel caso di password, dati bancari, corrispondenza privata. Nella maggioranza dei paesi questo costituisce reato.

Keylogger wireless si compone di due parti principali: trasmettitore e ricevitore. La registrazione reale si fa nel trasmettitore e che è un hardware keylogger PS/2 con un modulo incorporato 2.4 GHz. I dati intercettati dalla tastiera non vengono archiviati nella memoria bensì trasmessi in tempo reale tramite collegamento radio. Il ricevitore dall'altra parte è un dispositivo wireless d'acquisizione con una interfaccia USB. Dal punto di vista del programma, i dati sono accessibili dalla porta virtuale COM che permette la loro visualizzazione da qualsiasi utente del terminale.

Keylogger wireless- schema a blocchi

Tutto il sistema funziona in tempo reale, per questo il testo digitato sul computer a distanza è visualizzato immediatamente nella parte del ricevitore. Il sistema ha un raggio massimo di funzionamento di circa 50 metri. Questo corrisponde ad un raggio d'efficienza di circa 20 metri attraverso 2-4 muri a seconda dal loro spessore.

Keylogger wireless - trasmettitore

Keylogger wireless - ricevitore

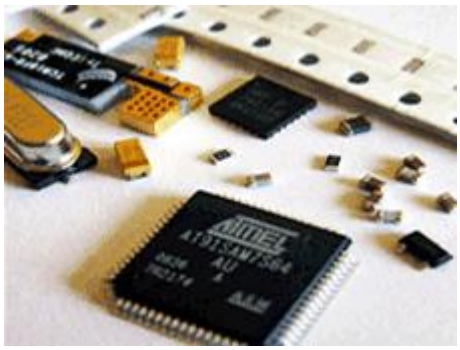
Sia il trasmettitore che il ricevitore si basano sullo stesso schema elettrico nel circuito stampato. Entrambi hanno le stesse dimensioni e sono destinati al montaggio su prolunghe corte PS/2 e USB. Si consiglia di utilizzare l'involucro per i filtri tipo EMC grazie a ciò tutto il dispositivo avrà l'aspetto di un adattatore o di una prolunga.

Sottogruppi

Questo articolo descrive tutto il processo del montaggio del Keylogger wireless. A seconda delle tue capacità, puoi decidere di creare il tuo Keylogger wireless personalizzato dall'inizio o ordinare da noi tutti i sottogruppi. Possiamo consegnare il kit di sottogruppi con i microcontrollori e gli involucri standard (visualizzati nella foto) o tutto il kit dei dispositivi pienamente controllato e comprovato. Vai alla sezione kit per ottenere altre informazioni.

Se hai deciso di creare il tuo Keylogger wireless personalizzato, dovresti avere un'esperienza di base in materia di elettronica e di saldatura nonché un'ottima esperienza in materia di tecnologia a montaggio superficiale (SMT). Un'opzione più semplice consiste nell'ordinare il kit dei sottogruppi da noi e di realizzare la saldatura, il cablaggio e il montaggio finale. Per questo devi possedere il saldatore col regolamento di temperatura e avere abbastanza buone capacità nella saldatura. Se hai deciso di progettare e realizzare i circuiti stampati da solo, devi avere grande esperienza e dei dispositivi adatti.

La seguente tabella presenta una distinta dei sottogruppi indispensabili alla realizzazione di un trasmettitore o di un ricevitore. La prolunga supplementare PS/2 è richiesta per il trasmettitore e un cavo USB con un connettore tipo A sono indispensabili per il ricevitore.



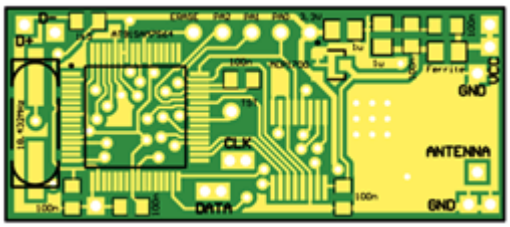
Kit dei sottogruppi elettronici

Cavi, involucro, circuiti stampati

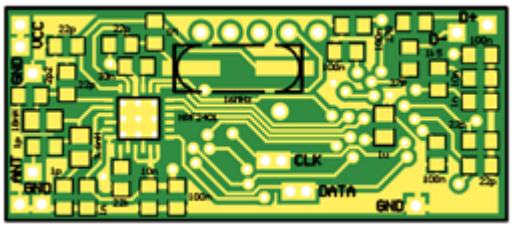
Codice	Descrizione	Involucro	Quantità
U1	Microcontrollore AT91SAM7S64	TQFP64	1
U2	Transceiver nRF2401	QFN24	1
U3	Stabilizzatore MCP1700T-330	SOT-23	1
Q1	Quarzo 18.432 MHz	HC-49 SMD	1
Q2	Quarzo 16 MHz	HC-49 SMD	1
R1, R2	Resistore 1.5 kΩ	0805	2
R3, R4	Resistore 27 Ω	0805	2
R5	Resistore 1 MΩ	0805	1
R6	Resistore 22 kΩ	0805	1
C1, C27	Condensatore 10 nF	0805	2
C2, C28	Condensatore 1 nF	0805	2
C3, C4, C6, C7, C8	Condensatore 22 pF	0805	5
C5	Condensatore 33 nF	0805	1
C9	Condensatore 2.2 pF	0805	1
C10, C11	Condensatore 1 pF	0805	2
C12, C22, C23, C24, C25, C26, C32, C33, C34, C42, C43	Condensatore 100 nF	0805	11
C21, C31, C41	Condensatore 1 µF	0805	3
L1	Bobina d'arresto	0805	1
L2	Bobina 3.6 nH	0805	1
L3	Bobina 18 nH	0805	1

Keylogger wireless - distinta dei sottogruppi

Sia il trasmettitore che il ricevitore usano lo stesso circuito stampato e lo stesso kit dei sottogruppi (c'è la differenza nel cablaggio e il firmware). Il microcontrollore Atmel AT91SAM7S64 e il transceiver radio nRF2401 sono i sottogruppi più importanti del circuito elettronico. Tutti e due per il funzionamento corretto richiedono oscillatori al quarzo. Ad eccezione dello stabilizzatore MCP1700 tutti gli altri sottogruppi sono di tipo passivo (resistori, condensatori e alcune bobine). Un semplice frammento di filo è utilizzato come antenna a dipolo. Il circuito stampato bilateralmente e a due strati è illustrato nelle immagini qui sotto.

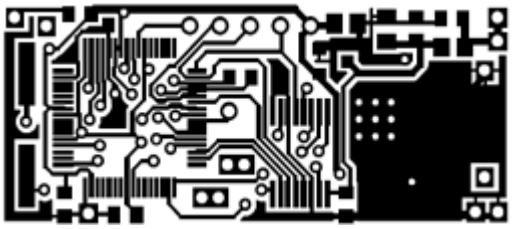


Disposizione del circuito stampato - parte di sopra

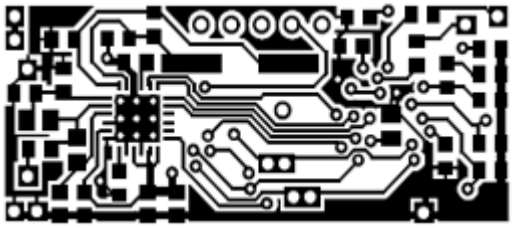


Disposizione del circuito stampato - parte di sotto

Se hai l'esperienza necessaria per realizzare da solo i circuiti stampati, puoi utilizzare il kit di maschere in scala 1:1 sotto disponibili. Il progetto di referenze utilizza il laminato tipo FR4 dallo spessore di 1 mm.



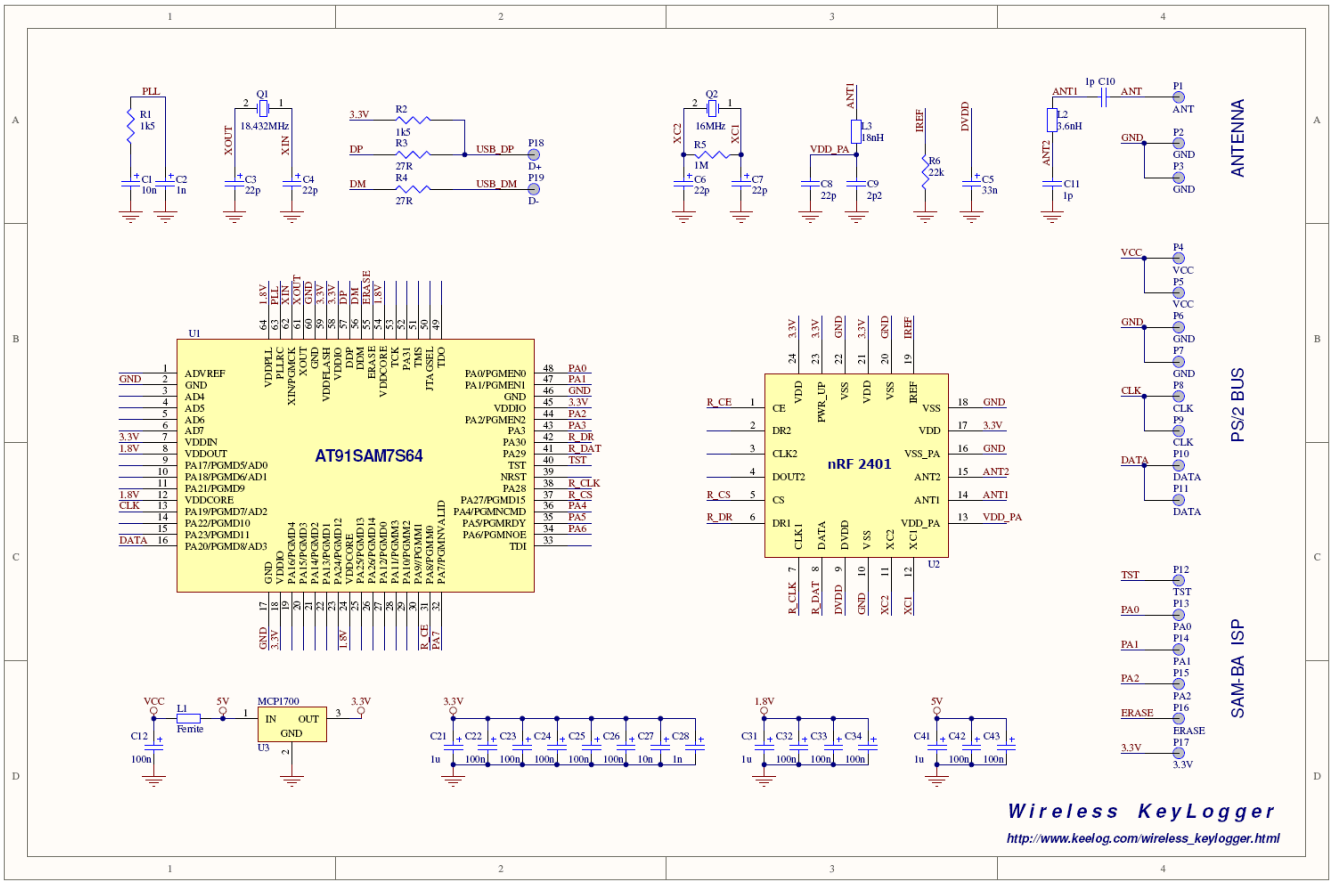
Maschera del circuito stampato - parte di sopra



Maschera del circuito stampato - parte di sotto

Montaggio

Il circuito di Keylogger wireless si compone di due elementi principali: microcontrollore AT91SAM7S64 e transceiver nRF2401. Altri elementi passivi sono l'oscillatore e i circuiti di alta frequenza RF. Tutto il circuito è alimentato da 3.3V, generati dal stabilizzatore MCP1700 e filtrati dal gruppo di condensatori. L'alimentazione iniziale è presa direttamente dalla linea principale PS/2 (trasmettitore), o quella USB (ricevitore). Se possiedi già i circuiti stampati assemblati, passa alla sezione cablaggio. Se hai deciso di realizzare il montaggio da solo, ti saranno utili tutti i consigli e lo schema elettrico presentati di sotto.



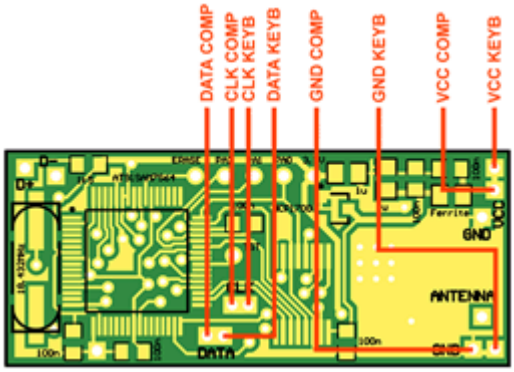
Keylogger wireless - schema elettrico

Per saldare utilizza il saldatore con una punta piccola (tipicamente sotto 0,5 mm) e della pasta per saldare (ad esempio RMA7). Fai attenzione a non riscaldare troppo gli elementi durante la saldature. Comincia il montaggio dal transceiver nRF2401 a causa del tipo complicato di involucro. Poi passa al microcontrollore AT91SAM7S64 e allo stabilizzatore MCP1700. Fai attenzione che il pin numero 1 sull'involucro corrisponda al primo pin sul circuito stampato. Alla fine salda tutti i circuiti supplementari: quarzi, resistori, condensatori e bobine. Il montaggio dell'antenna lascialo alla fine. Puoi utilizzare un'antenna apposita a ISM 2.4 GHz, o realizzare una semplice antenna a dipolo a quarto d'onda di un frammento di filo. La lunghezza ottimale è di 3.125 cm (1.23"). I circuiti stampati montati devono somigliare a quelli presentati sulle foto qui sotto.

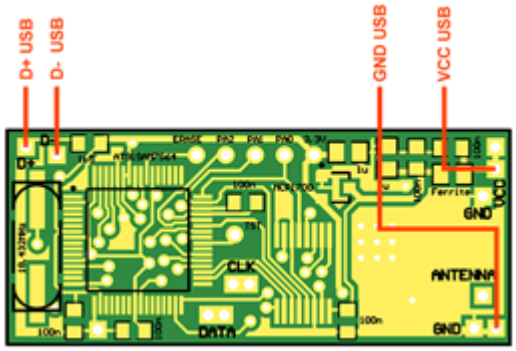
Il circuito stampato montato - parte di sopra con un microcontrollore

Il circuito stampato montato - parte di sotto con un transceiver

Dopo aver fatto il montaggio dei circuiti stampati si deve fare il cablaggio. Oltre al firmware è un punto dove il trasmettitore si distingue dal ricevitore. Il trasmettitore dovrebbe essere accoppiato in modo parallelo alla linea principale PS/2. Il circuito stampato del trasmettitore possiede i pad per saldare i cavi conducenti sia al computer, sia alla tastiera. Il ricevitore dovrebbe avere la connessione tipica alla porta USB. Le foto qui sotto mostrano come realizzare tutte le connessioni.



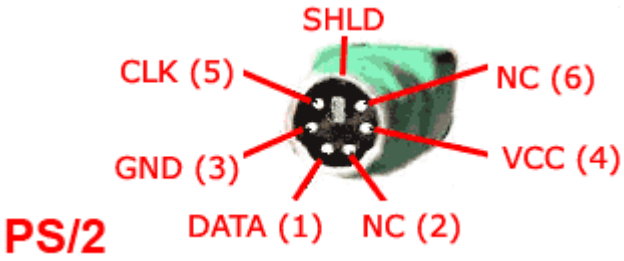
Schema del cablaggio PS/2 per il trasmettitore



Schema del cablaggio USB per il ricevitore

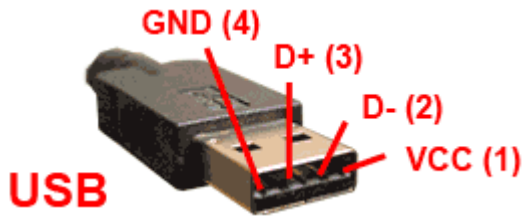
Utilizza le prolunghe PS/2 e USB, tagliale e isola le linee dei segnali. La cosa che può dare qualche problema è l'abbinamento dei cavi ai singoli segnali. Alcuni cavi PS/2 e USB sono di colori standard, ma è rischioso di darne la fiducia. Si consiglia di utilizzare il misuratore di cortocircuito, l'ohmmetro per sapere quale cavo corrisponde a quale linea dei segnali. Gli schemi sotto possono essere utili.

Segnale	Descrizione	Collegamento PS/2	Commento
VCC	Alimentazione +5V	4	Devono essere collegati al modulo
GND	Massa di alimentazione	3	
CLK	Orologio	5	
DATA	Dati	1	
NC	Linee non usate	2, 6	Non usate da modulo, se esistono, lasciare nello stato originale
SHLD	Schermo	-	



Collegamento PS/2 (trasmettitore)

Segnale	Descrizione	Collegamento USB	Commento
VCC	Alimentazione +5V	1	Devono essere collegati al modulo
D-	Dati	2	
D+	Dati	3	
GND	Massa di alimentazione	4	
SHLD	Schermo	-	Non usate da modulo, se esistono, lasciare nello stato originale



Collegamento USB (ricevitore)

Se i microcontrollori che utilizzi non sono stati programmati, è un buon momento per scaricare il firmware utilizzando la tecnologia ISP (In-System Programming). Leggi la sezione firmware per ottenere altre informazioni. Dopo aver realizzato questa fase, i dispositivi montati devono presentarsi come sulle foto qui sotto.

Trasmettitore con il cablaggio PS/2

Ricevitore con il cablaggio USB

Prima di istallare l'involucro, si consiglia di realizzare un'ultima prova. Utilizza il misuratore del cortocircuito o l'ohmmetro per misurare la resistenza tra l'alimentazione (VCC) e la massa (GND) sia sul collegamento USB che sul collegamento PS/2. Un cortocircuito significa che si deve verificare tutto il sistema per non deteriorare il computer. Se tutto va bene, chiudi gli involucri utilizzando la colla e inizia il primo avviamento.

Avviamento

Dopo aver montato il sistema trasmettitore-ricevitore, è l'ora di fare la prima prova. Si consiglia di utilizzare un computer per realizzare la prova di tutti e due dispositivi. All'inizio spegni il computer e collega il trasmettitore tra la tastiera PS/2 e la porta PS/2.

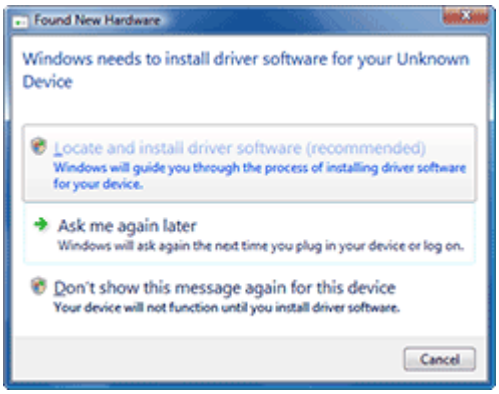
Connetti il trasmettitore alla porta PS/2

Connetti la tastiera PS/2 al trasmettitore

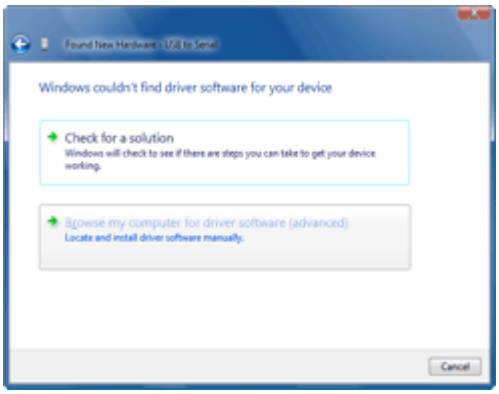
Dopo accendi il computer e assicurati che la tastiera PS/2 funzioni correttamente (non si deve osservare nessun influenza del keylogger). Poi fa' la prova del ricevitore. Prima si deve scaricare il file del combinatore KeeLog. Scarica e conserva i file sul disco locale del computer. Poi connetti il ricevitore a qualsiasi porta USB (non è richiesto spegnere il computer). Assicurati che la posizione del ricevitore permetta di ricevere la trasmissione radio dal trasmettitore.

Connetti il ricevitore alla porta USB libera

Quando il ricevitore viene connesso per la prima volta si presenterà la finestra dell'installazione del driver e più precisamente saranno utilizzati i driver della porta virtuale COM, consegnati insieme alla maggioranza dei sistemi operativi come Windows. Tuttavia il file adatto della descrizione INF deve essere scelto in un modo manuale. Quando il sistema ti chiederà il driver, devi passare a pathname, dove sono stati registrati i driver. Le immagini di sotto presentano tutto il processo.

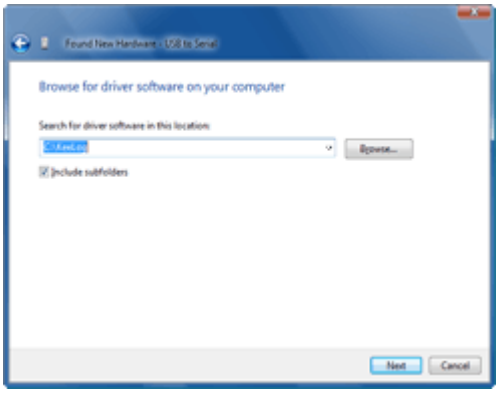


Scegli la localizzazione e l'installazione del software



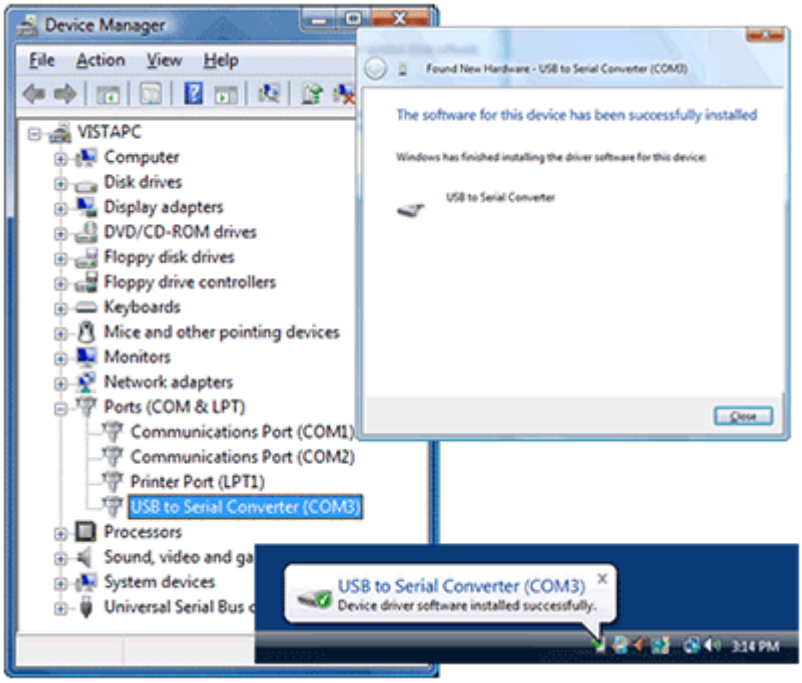
Scegli la localizzazione del driver

Scegli di presentare l'opzione della localizzazione



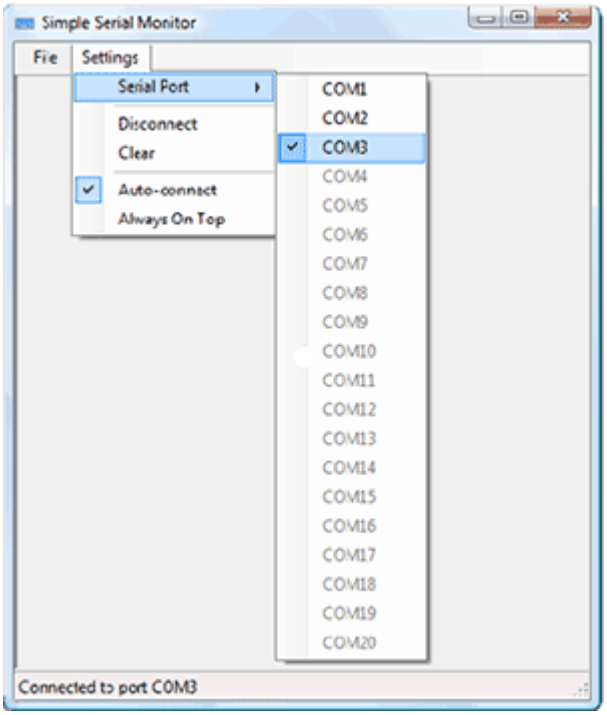
Indica la localizzazione di file dei driver

Quando il processo dell'installazione sarà terminato con successo, il ricevitore sarà visualizzato come il convertitore USB alla porta in serie. Apri la Gestione periferiche nel sistema Windows per verificare quale porta in serie è stata assegnata al ricevitore.



Il ricevitore visualizzato in Gestione periferiche

Per poter intercettare i dati dalla tastiera dal trasmettitore si può utilizzare qualsiasi cliente del terminale come ad esempio Hyperterminal. Si consiglia di utilizzare la nostra applicazione gratuita Simple Serial Monitor vista la sua comodità e la semplicità d'uso.



Simple Serial Monitor (utente del terminale gratuito consegnato dalla KeeLog)

Dopo l'avviamento del Simple Serial Monitor (oppure di una applicazione alternativa) ricordati che devi scegliere una porta COM adatta. Se tutto è stato realizzato con successo, il ricevitore comincia immediatamente a visualizzare il flusso dei pulsanti digitati sulla tastiera PS/2.

Computer a distanza con il trasmettitore PS/2 *Computer locale con il ricevitore USB*

Un passo seguente sarebbe la prova dello stesso su due computer differenti. Assicurati che sono alla portata della trasmissione. Se il testo si presenta nella finestra del terminale, il tuo Keylogger wireless è pronto alla sua prima missione reale. Ricordati che si deve utilizzare il dispositivo conformemente alla legge!

Download

Firmware per il microcontrollore che permette di programmare il trasmettitore e il ricevitore.
http://www.keelog.com/files/WirelessKeyloggerFirmware.zip

Driver per l'installazione del ricevitore quale la porta virtuale COM
http://www.keelog.com/files/UsbToSerial.zip

Il software gratuito per il ricevimento dei dati tramite la porta virtuale COM (equivalente dell'applicazione Hyperterminal). Esige della piattaforma Microsoft .NET Framework.
http://www.keelog.com/files/SimpleSerialMonitor.zip

Il software che rende possibile di programmare del firmware utilizzando SAM-BA
http://www.keelog.com/files/At91Isp.zip

Il manuale dell'utente come programmare il firmware al microcontrollore mediante il bootloader incorporato senza l'utilizzo del programmatore addizionale.
http://www.keelog.com/files/SambaUserGuide.pdf

Distinta base dei sottogruppi utilizzati durante il montaggio del Keylogger wireless (trasmettitore e ricevitore)
http://www.keelog.com/files/WirelessKeyloggerBom.pdf

Schema del cablaggio per Keylogger wireless (trasmettitore e ricevitore)
http://www.keelog.com/files/WirelessKeyloggerWiring.pdf

Schema elettrico del Keylogger wireless (trasmettitore e ricevitore)
http://www.keelog.com/files/WirelessKeyloggerSchColor.pdf

Parte di sopra del circuito stampato (trasmettitore e ricevitore)
http://www.keelog.com/files/WirelessKeyloggerPcbTop.pdf

Parte di sotto del circuito stampato (trasmettitore e ricevitore)
http://www.keelog.com/files/WirelessKeyloggerPcbBottom.pdf

La maschera per la parte di sopra del circuito stampato (trasmettitore e ricevitore) in scala 1:1
http://www.keelog.com/files/WirelessKeyloggerMaskTop.pdf

La maschera per la parte di sotto del circuito stampato (trasmettitore e ricevitore) in scala 1:1
http://www.keelog.com/files/WirelessKeyloggerMaskBottom.pdf

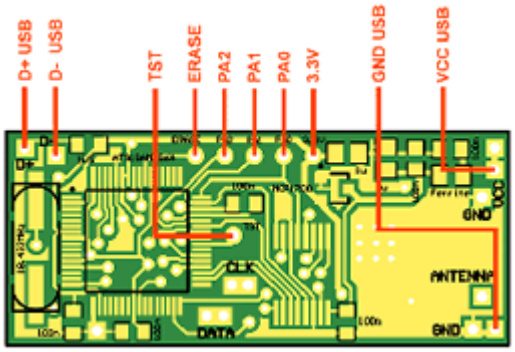
Firmware

Leggere questo capitolo se hai bisogno di programmare il microcontrollore AT91SAM7S64 da solo. Se hai comprato il kit da noi, abbiamo già fatto questo passo per te.

I microcontrollori contemporanei come Atmel AT91SAM7S64 hanno involucri con pacchetti troppo densi, cosa che rende difficile trovare il programmatore tradizionale che potrebbe servire un dato tipo di microcontrollore. Per questi motivi il software nel sistema ISP (In-System Programming) si sta sviluppando rapidamente negli ultimi anni. ISP permette di montare prima tutto il circuito, e poi di programmare il firmware, utilizzando strumenti molto semplici. Il microcontrollore AT91SAM7S64 possiede una soluzione confortabile ISP, in base al modulo incorporato USB. Si chiama SAM-BA (SAM Boot Assistant), e richiedo solo il cavo USB e alcuni semplici jumper. Prima di avviare di SAM-BA sul Keylogger wireless, devi scaricare il software AT91 ISP. Poi effettua i seguenti passi per scaricare il firmware sul modulo del ricevitore e del trasmettitore.

Passi 1: Riguarda solo il trasmettitore. Prepara il cavo USB con il collegamento tipo A da una parte e i cavi isolati dall'altra parte. Salda le linee USB: VCC, GND, D+, e D- ai punti particolari sul circuito stampato. Questo passo non è obbligatorio per il ricevitore perché esso ha già preparato il collegamento USB.

Passo 2: Prepara qualche filo corto per controcircuitare i pin -BA: TST, ERASE, PA2, PA1, PA0, 3.3V. Salda un'estremità di ogni filo al punto concreto di saldatura SAM-BA su entrambe piastrelle. In alternativa puoi preparare i jumper speciali, come è stato dimostrato sulle immagini sotto.



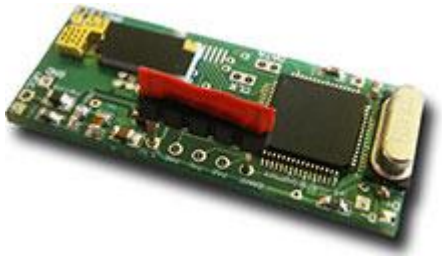
Schema del cablaggio SAM-BA

Passo 3: Installa il pacchetto software AT91 ISP.

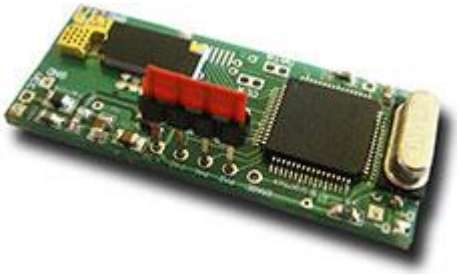
Passo 4: Connetti il dispositivo alla porta USB libera. Un messaggio Dispositivo non riconosciuto a questa fase è normale.

Passo 5: Controcircuita il collegamento ERASE a 3.3V per un breve momento. Questo provocherà la cancellazione della memoria flash del microcontrollore.

Il cavo USB e i jumper per il bootloader SAM-BA



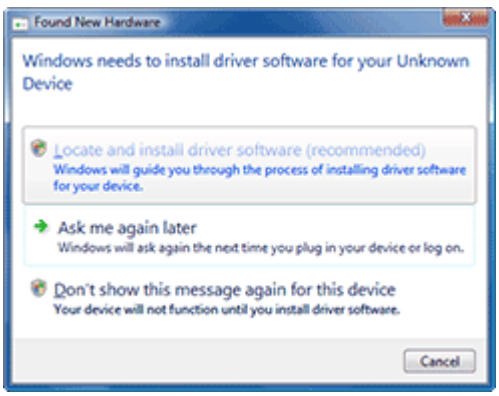
Cancellazione della memoria (ERASE controcircuitato a 3.3V)



Attivazione del bootloader (PA0, PA1, PA2 e TST controcircuitati a 3.3V)

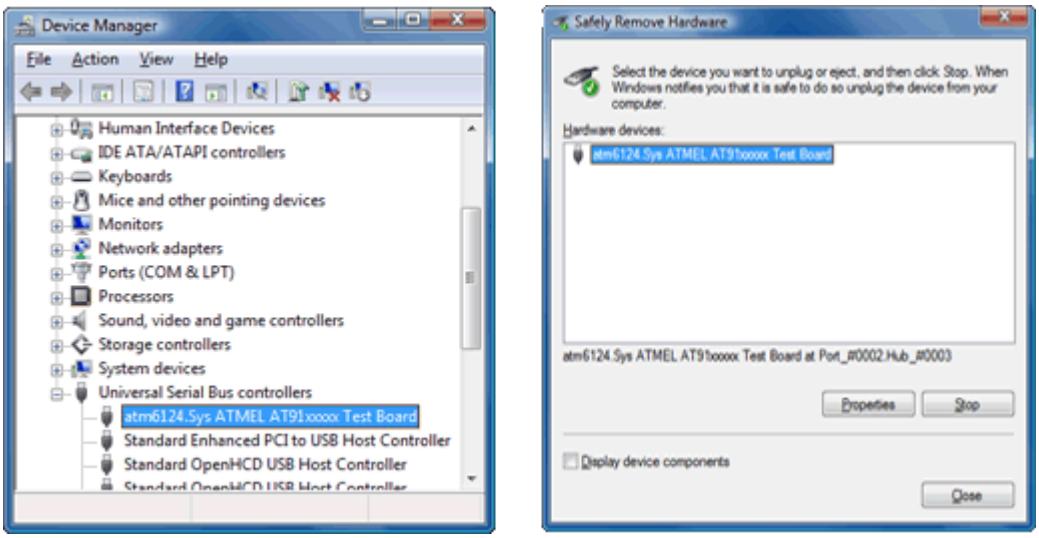
Passo 6: Sconnetti il dispositivo dalla porta USB. Assicurati che il collegamento ERASE non sia già stato connesso a 3.3V. Poi controcircuita PA0, PA1, PA2 i TST a 3.3V. Connetti di nuovo il dispositivo alla porta USB. (Dispositivo non riconosciuto può presentarsi di nuovo). Lascia il dispositivo connesso per circa 10 secondi e poi disconnettilo dalla porta USB. Questa operazione dovrebbe attivare il bootloader interno SAM-BA.

Passo 7: Elimina tutti i jumper o tutti i collegamenti e connetti il dispositivo alla porta USB. Si dovrebbe visualizzare un messaggio Trovato nuovo hardware Fa' la procedura tipica dell'installazione e lascia trovare al sistema i driver da solo.



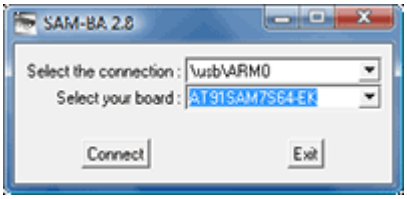
Dialogo Trovato nuovo hardware

Passo 8: Apri la Gestione periferiche per assicurarti che il bootloader SAM-BA è stato attivato.



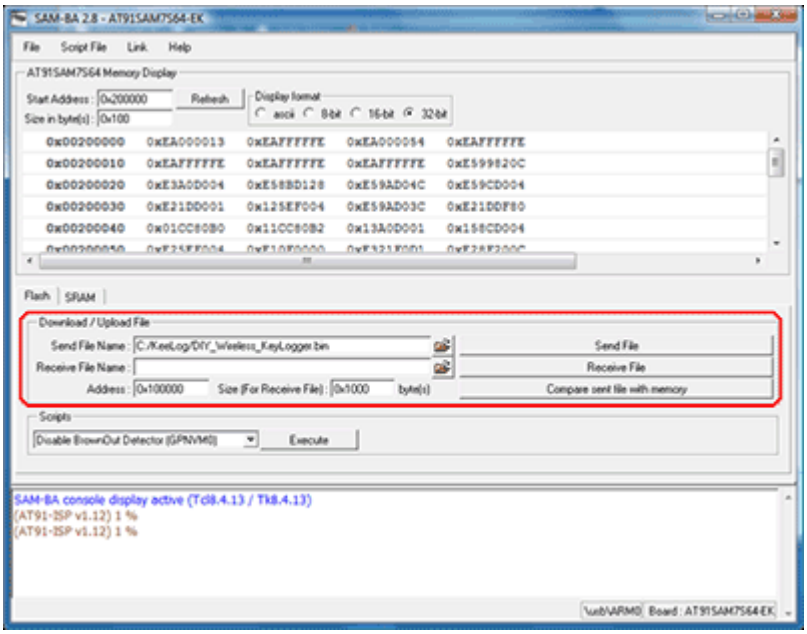
Gestione periferiche con il dispositivo Atmel AT91

Passo 9: Fa' l'avviamento dell'applicazione SAM-BA dal pacchetto del software AT91 ISP e scelga la piattaforma finale del hardware AT91SAM7S64-EK.



Scelta della piattaforma del hardware

Passo 10: Dopo aver effettuato la connessione alla piattaforma del hardware, passa a Flash e scelga un firmware per il trasmettitore/ricevitore e clicca Send File. Quando l'applicazione chiederà se sbloccare o bloccare le opportune regioni della memoria flash, si deve scegliere Yes. Se questo passo è stato realizzato con successo, questo significa che il firmware è stato correttamente scaricato alla memoria flash del microcontrollore.



Applicazione SAM-BA

Ricordati che devi ripetere tutta la procedura SAM-BA sia per il trasmettitore che per il ricevitore. Dopo aver terminato, i dispositivi sono pronti all'uso.