

Forum:[Hack Forums](#)

Thread: [Decompile MCU program](#)

gacakupaca - February 28, 2019, 1:10 pm

I have windows software which changing language to program another program on device via rs232 cable or usb. Device has microcontroller where that code is running as a program and have some gui on small lcd, nevermind. I assume that pc program just override existing program with new one, just with chosen language. That pc program is compiled with microsoft visual c++ 6 and no packer by informations from "detect it easy". Also i used to find some useful code with IDA pro but that's all about that pc software which just burn program to microcontroller...problem is that microcontroller file which i need to decompile. Goal is to translate to another language, even better if we can get and source code from that controller? If someone know or want to try is that possible? We can deal about price.

BTW it's legal job, because company, which is owner, doesn't exists anymore already more than 10 years.

kingofcomps - March 2, 2019, 1:04 am

Just want to clarify your case. So you have a device, it has an LCD panel with a GUI. You connect this device to your PC via USB, run the PC software, and the language on the LCD gets changed (translated) by the software. If this is the case, and if the device you are connecting is communicating through a COM port, you can use Realterm and make a man-in-the-middle attack using its "Spy" feature and see the communication between your PC and device. Find the custom protocol used there, replicate it yourself.

gacakupaca - March 2, 2019, 2:57 am

(Mar 2, 2019 02:04 AM)kingofcomps Wrote: [\[CITE\]](#) Just want to clarify your case. So you have a device, it has an LCD panel with a GUI. You connect this device to your PC via USB, run the PC software, and the language on the LCD gets changed (translated) by the software. If this is the case, and if the device you are connecting is communicating through a COM port, you can use Realterm and make a man-in-the-middle attack using its "Spy" feature and see the communication between your PC and device. Find the custom protocol used there, replicate it yourself.

Yes, that's how it works. I thought about that but i think program is override everything inside MCU, not just new translation over COM port. So if i use to sniff com communication i assume that i would see just bunch of hexadecimal codes which can represent anything?

kingofcomps - March 2, 2019, 3:13 am

(Mar 2, 2019 03:57 AM)gacakupaca Wrote: [\[CITE\]](#) Yes, that's how it works. I thought about that but i think program is override everything inside MCU, not just new translation over COM port. So if i use to sniff com communication i assume that i would see just bunch of hexadecimal codes which can represent anything?

Yes. But you need to guess the correct baud rate and stop bits. Not sure if it's possible in your situation but before all I'd open the case of the device, find the FTDI or whatever USB interface chip is placed near the usb/rs232 port on the device, trace the PCB routes to find RX/TX pins and look at them with an oscilloscope (or even better a logic analyzer) to find out the correct baud rate-stop bit configuration. After you find the correct UART configuration, use the Spy function on Realterm and sniff all the data. If you're lucky, the communication would be in plain text and you can easily find out the protocol created by the designer. If you aren't that lucky, all you'll see will be bunch of random hexadecimal numbers. In this case I'd save all the data (first few seconds for example) transferred as a .hex file, then without opening the PC software, send the saved .hex file back to the device

using the "Send File" feature. But you need to use some delay (can be anything, 1-2ms maybe) between every character because otherwise Realterm will send the file too fast.

It's not that easy to give the instructions here, there are many possibilities and you can try different approaches on different situations. What I wrote here are just basic stuff. If you're not into electronics and comm. protocols, you will probably need a professional support here.

fijasko - March 2, 2019, 5:41 am

upload the software, whole folder zipped to sendspace.com, I might take a look at it.

gacakupaca - March 2, 2019, 11:55 am

(Mar 2, 2019 06:41 AM)fijasko Wrote: [\[CITE\]](#) upload the software, whole folder zipped to , I might take a look at it.

That's it.

sendspace . com /file/819598

Inside MakeApp.exe you can select source folder which is "StarGas_F_Tecnotest_Croatia". I assume inside that folder is compiled code for renesas h8s MCU which is flashing to MCU then.

This may be useful [www . renesas . com](http://www.renesas.com)

[/in/en/products/software-tools/tools/simulator/hew-simulator-for-h8sx-h8s-h8-families.html#download](http://in/en/products/software-tools/tools/simulator/hew-simulator-for-h8sx-h8s-h8-families.html#downloads)s, there's programs for compiling programs for that type of MCU and as i saw when program is compiled i got "Motorola S-record" file, which is same file what i have inside that "StarGas_F_..." folder just with different extension .A20 (SW01131P.A20).

Also this [electronics . stackexchange . com /questions/424978/reverse-engineering-srec-firmware](http://electronics.stackexchange.com/questions/424978/reverse-engineering-srec-firmware)

I assume that .CRO files are about translation.

(Mar 2, 2019 04:13 AM)kingofcomps Wrote: [\[CITE\]](#) Yes. But you need to guess the correct baud rate and stop bits. Not sure if it's possible in your situation but before all I'd open the case of the device, find the FTDI or whatever USB interface chip is placed near the usb/rs232 port on the device, trace the PCB routes to find RX/TX pins and look at them with an oscilloscope (or even better a logic analyzer) to find out the correct baud rate-stop bit configuration. After you find the correct UART configuration, use the Spy function on Realterm and sniff all the data. If you're lucky, the communication would be in plain text and you can easily find out the protocol created by the designer. If you aren't that lucky, all you'll see will be bunch of random hexadecimal numbers. In this case I'd save all the data (first few seconds for example) transferred as a .hex file, then without opening the PC software, send the saved .hex file back to the device using the "Send File" feature. But you need to use some delay (can be anything, 1-2ms maybe) between every character because otherwise Realterm will send the file too fast.

It's not that easy to give the instructions here, there are many possibilities and you can try different approaches on different situations. What I wrote here are just basic stuff. If you're not into electronics and comm. protocols, you will probably need a professional support here.

I found bound rate and configuration already, i didn't try this yet but i am pretty sure there will be just bunch of hexadecimals because when i later inspect folders inside device, i see same files which i have on my disk (binary), u can also check for it [https: // sendspace . com/file/819598](https://sendspace.com/file/819598) that files are inside "StarGas_F_Tecnotest_Croatia" folder...i think it just somehow transport files to controller where MCU run that binary files. But i would try this, who knows how lucky am I. Thanks for your interest, every help means to me!

fijasko - March 2, 2019, 4:09 pm

yeah, reading from filelist.txt, I agree with you. *.cro file are for Croatian language. But decoding them has to go thru reversing the firmware.

gacakupaca - March 3, 2019, 3:30 am

(Mar 2, 2019 05:09 PM)fijasko Wrote: [\[CITE\]](#) yeah, reading from filelist.txt, I agree with you. *.cro file are for Croatian language. But decoding them has to go thru reversing the firmware.

Do you know to do it? I think firmware is inside MCU, not inside that files? I am not at that lvl with re engineering that's for sure, even if i understand...maybe i could read everything from controller but again i would need somehow to run that on pc to dump memory. If you could do something we can deal for price? Or maybe you know someone else who can help with this to recommend me?

But there's chance it override firmware every time because when device is connected it request to turn off device then do something and after that request to turn on to transfer files. In that case firmware could be in that folder, may be that A20 files i don't know.