

Atmel Studio 7
Easier to Use and More Powerful than Ever

Download Whitepaper



HACKADAY

[HOME](#)[BLOG](#)[HACKADAY.IO](#)[STORE](#)[HACKADAY PRIZE](#)[SUBMIT](#)[ABOUT](#)

November 21, 2015

MSP430-BASED CTF HARDWARE HACKING CHALLENGE

by: [Eric Evenchick](#)

6 Comments

f t g+

April 2, 2014



SEARCH

[SEARCH](#)

NEVER MISS A HACK



IF YOU MISSED IT

Hacking conferences often feature a Capture the Flag, or CTF event. Typically, this is a software hacking challenge that involves breaking into targets which have been set up for the event, and capturing them. It's good, legal, hacking fun.

However, some people are starting to build CTFs that involve hardware hacking as well. [Balda]'s [most recent hardware hacking challenge](#) was built for the [Insomni'hack 2014 CTF](#). It uses an MSP430 as the target device, and users are allowed to enter

commands to the device over UART via a [Bus Pirate](#). Pull off the exploit, and the wheel rotates to display a flag.

For the first challenge, contestants had to decompile the firmware and find an obfuscated password. The second challenge was a bit more complicated. The password check function used memcpy, which made it vulnerable to a buffer overflow attack. By overwriting the program counter, it was possible to take over control of the program and make the flag turn.

The risk of memcpy reminds us of this [set of posters](#). Only abstaining from memcpy can 100% protect you from overflows and memory disclosures!

Posted in [security hacks](#)

Tagged [buffer overflow](#), [ctf](#), [memcpy](#), [msp430](#), [reverse engineering](#)

← [Portable SMT Lab for Hacker On The Go](#)

[Boxing + Arduino + Geometry = Awesomeness](#) →



6 THOUGHTS ON “MSP430-BASED CTF HARDWARE HACKING CHALLENGE”

Dodo says:

April 2, 2014 at 12:00 pm

How can you avoid using memcpy? Sometimes you simply have to copy binary-memory. I tend to almost always use it with a fixed length though.

[Reply](#)

[Report comment](#)

Sergiusz Bazanski says:

April 2, 2014 at 12:20 pm

My writeup: <http://blog.dragonsector.pl/2014/03/insomnihack-ctf-2014-life-is-even.html>

[Reply](#)

[Report comment](#)

Chris C. says:

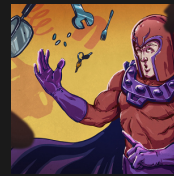
April 2, 2014 at 12:36 pm

[Eric], did you mean abstaining from strcpy? That matches the posters and makes



BUILDING A BETTER 3D PRINTED GUN

[45 Comments](#)



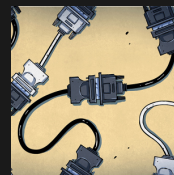
BACK TO BASICS: WHAT'S THE DEAL WITH MAGNETS?

[65 Comments](#)



THE STORY OF THE 2015 HACKADAY PRIZE

[9 Comments](#)



VIDEO STANDARDS ARE MORE THAN VIDEO SIGNALS

[68 Comments](#)



WATER-SAVING AGRICULTURAL SYSTEM WINS BEST PRODUCT

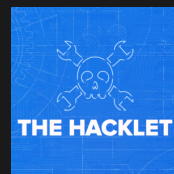
[26 Comments](#)

[More from this category](#)

CATEGORIES

Select Category

OUR COLUMNS



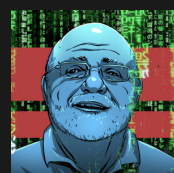
HACKLET 85: ALTERNATIVE AUDIO AMPLIFIERS

[1 Comment](#)



THE BEST CONFERENCE BADGE HACKING YOU'VE EVER SEEN

[22 Comments](#)



CODE CRAFT- EMBEDDING C++: HIDDEN ACTIVITIES?

[26 Comments](#)

more sense.

Reply

Report comment

fede.tft says:

April 2, 2014 at 1:36 pm

I think this article misinterprets the goal of <http://natashenka.ca/posters> which IMHO is to warn against C functions that write into a string (or an array) without explicitly passing the size of the memory buffer together with the pointer, because that creates too many ways for the buffer to be overflowed. For example, the site says `strcpy()` is safe. Now, `memcpy()` is safe in this respect, while `strcpy()` is not.

Reply

Report comment

HackJack says:

April 2, 2014 at 2:30 pm

You will be amazed how many people still think `strcpy()` is the same as `memcpy()`. Just ask my coworkers...

Reply

Report comment

Rollyn01 says:

April 2, 2014 at 8:47 pm

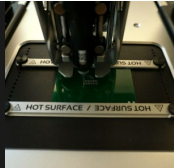
I'll admit, that second link made me laugh. However, wouldn't this still be considered software hacking? You are still using some form of code to access the program counter.

Reply

Report comment


Leave a Reply

Enter your comment here...



REVIEW: VOLTERRA V-ONE PCB PRINTER

61 Comments



ON SEMICONDUCTOR ACQUIRES FAIRCHILD

23 Comments

More from this category

RECENT COMMENTS

- Keith on [Garbage can CNC Machine Build](#)
- bl on [Physical Fitness for the Truly Lazy](#)
- Valentin Angelovski on [FleaFPGA + Arduino Uno = FleaFPGAUno](#)
- hackedomg on [Building A Better 3D Printed Gun](#)
- hackedomg on [Building A Better 3D Printed Gun](#)
- RÖB on [FleaFPGA + Arduino Uno = FleaFPGAUno](#)
- jack laidlaw on [FleaFPGA + Arduino Uno = FleaFPGAUno](#)
- Al Williams on [Physical Fitness for the Truly Lazy](#)
- tekkieneet on [FleaFPGA + Arduino Uno = FleaFPGAUno](#)
- CJ on [Building A Better 3D Printed Gun](#)

NOW ON HACKADAY.IO

Andrey gave a skull to PowerBlade.

roy.arnabendu.77 has updated their profile.

Raj has updated their profile.

Mark Dalton has updated their profile.

Mark Dalton has added a stack page.

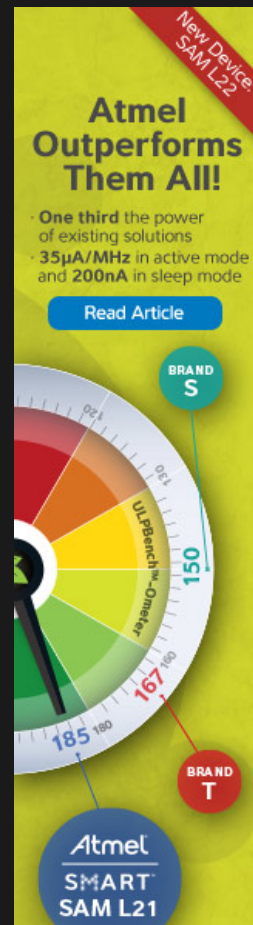
aangelicabolanos has updated their profile.

K.C. Lee has updated instructions for the project titled Charleplex Xmas Tree without uC.

JRodrigo has followed a list.

rizwanah.bb has updated their profile.

Aleksandar Bradic has added a new log for Hackaday Omnibus 2015.



[HOME](#)
[BLOG](#)
[HACKADAY.IO](#)
[STORE](#)
[HACKADAY PRIZE](#)
[VIDEO](#)
[SUBMIT A TIP](#)
[ABOUT](#)
[CONTACT US](#)

NEVER MISS A HACK



SUBSCRIBE TO NEWSLETTER

SUBSCRIBE

Copyright © 2015 | Hackaday, Hack A Day, and the Skull and Wrenches Logo are Trademarks of Hackaday.com
Powered by [WordPress.com](#) VIP