CIPHER TECH SOLUTIONS

CIPHER TECH SOLUTIONS, INC.
1945 OLD GALLOWS ROAD, SUITE 620
VIENNA, VA 22182
WWW.CIPHERTECHSOLUTIONS.COM
PHONE: 888-948-8324
FAX: 845-230-6632

Applicants,

Cipher Tech uses various technical challenges to assess the skills and aptitude of potential hires seeking Embedded Reverse Engineering positions within our company.

For this challenge, you are tasked with analyzing an STM32F429I-DISC1 development board that has been programmed with unknown functionality. In lieu of a physical board, you are being provided with the archive **Embedded_RE_Challenge_2022.zip**, which contains several files that you will need for your analysis:

- **flash.bin** – The firmware image used to program the device. It was obtained by using STM32CubeProgrammer to read data starting from address 0x08000000.
- **device_powered_on.jpg** – A photo of the device taken when it was first powered on.
- **Hardware_References** – A directory containing various hardware datasheets and reference manuals that you will likely find helpful for your analysis.

Analyze the firmware within **flash.bin** using any tools of your choice to answer the questions that follow. Only the first question must be answered correctly to pass the challenge, but you are encouraged to answer as many of the remaining bonus questions as you can.

1. What is the password needed to unlock the device?
2. What interface or communication protocol is used to enter the password? Explain how you arrived at your answer and provide as many associated configuration parameters as you can.
3. Besides entering the correct password, what other conditions, if any, must be satisfied to unlock the device?
4. What vulnerabilities exist in the device's firmware? How might you go about exploiting them?

Your submission should consist of a writeup of your answers and any other files you created as part of your work, such as scripts, IDA Pro databases, and/or Ghidra workspaces.

We look forward to reviewing your response!

-Cipher Tech Technical Recruiting