Ćwiczenie 10: Zawody CTF (*Capture the flag*)

Instrukcja laboratorium

Mariusz Chilmon <mariusz.chilmon@ctm.gdynia.pl>

2024-01-30

> Give a man a program, frustrate him for a day. Teach a man to program, frustrate him for a lifetime.
>
> — *Muhammad Waseem*

Cel ćwiczenia

Celem ćwiczenia jest zapoznanie się z:

- strukturą pliku Intel HEX,
- budową instrukcji w procesorze.

Wprowadzenie

Otrzymałeś produkcyjną wersję urządzenia X[1]. Wiesz, że wersja serwisowa wyświetla sekretny kod (flagę) po wciśnięciu przycisku podłączonego do pinu `PC4`. Przycisk ten nie jest jednak montowany w wersji produkcyjnej. Zmień wsad urządzenia tak, by flaga była wyświetlana po wciśnięciu przycisku *S1*, który jest podłączony do pinu `PC1`.

Zawody CTF organizowane są od 1996 roku w ramach konferencji cyberbezpieczeństwa, a także jako samodzielne imprezy, wspierane nawet przez organizacje rządowe. Na ogół polegają na łamaniu zabezpieczeń stron internetowych i serwerów, ale pojawiają się również konkursy dotyczące systemów wbudowanych.

Uruchomienie programu wyjściowego

1. Podłącz płytkę *WPSH209* do *Arduino Uno*.
2. Wyświetlacz wskazuje wartość `8888`.

Zadanie podstawowe

Odczytywanie stanu przycisku odbywa się za pomocą rozkazu `SBIS` (*Skip if Bit in I/O Register is Set*), który jest najprostszym rozkazem pozwalającym zrealizować warunek zależny od pojedynczego

[1] Być może opracował je Elon Musk. To tłumaczyłoby nazwę.

bitu w rejestrze I/O[2]. Celem zadania podstawowego jest określenie pełnego opcode'u tej instrukcji i odnalezienie go w pliku `bin/laboratory.hex`.

Poniżej zaprezentowana jest struktura pliku Intel HEX. Kolor jasnoniebieski oznacza dane, które są przedmiotem naszego zainteresowania.

```
:10010000214601360121470136007EFE09D2190140
:100110002146017E17C20001FF5F16002148011928
:10012000194E79234623965778239EDA3F01B2CAA7
:100130003F0156702B5E712B722B732146013421C7
:00000001FF
```

Start code | Byte count | Address | Record type | Data | Checksum

Rysunek 1: Przykład pliku Intel HEX

Zadanie rozszerzone

Celem zadania rozszerzonego jest wgranie do urządzenia własnej wersji oprogramowania, reagującej na przycisk *S1*.

Wymagania funkcjonalne

1. Po wciśnięciu przycisku *S1* wyświetlana jest flaga.

Modyfikacja programu

Zmodyfikuj plik `bin/laboratory.hex` i wgraj go do urządzenia. Każda linia pliku w standardzie Intel HEX zakończona jest sumą kontrolną. Suma kontrolna służy do wykrywania zmian w zawartości pliku, więc po podmianie instrukcji z bardzo dużym prawdopodobieństwem stanie się nieprawidłowa. Programator *AVRDUDE* wykryje to i wydrukuje spodziewaną wartość, którą należy wpisać w pliku.

[2] Wprawdzie równie dobrze mógłby być użyty rozkaz `SBIC` (*Skip if Bit in I/O Register is Cleared*), ale dla uproszczenia zadania pomijamy badanie tej możliwości.