Joseph King
Medical Device VIP

Paper Review Checklist

1.

Methods for Extracting Firmware from OT Devices for Vulnerability Research

01/11/2022

Nozomi Networks Labs

Website: https://www.nozominetworks.com/blog/methods-for-extracting-firmware-from-ot-devices-for-vulnerability-research

2.

This research article talks about the SPI protocol and the ways in which it can be used to extract information from a targeted device. In general, this can be done by using an SPI bus interface that is used to extrapolate data from a targeted device that also uses the SPI protocol. The article talks about how to wire the extrapolating process, and the article also gives an example from a passed device they have done. They explain the challenges and obstacles that they have faced which gives us an idea on what to look out for when we interface with our own targeted device doing this approach.

Overall, I would say articles can be helpful to beginners who are starting to get into the embedded system environment. However, there isn't enough information to give to a reader with intermediate (and higher) experience. I say this because it doesn't go in depth in certain areas that I think would be beneficial to someone who would want to recreate this project if they wanted to learn. For example, it talks about the Bus Interface, but it doesn't go into detail about the one they're using. If they go into more detail if give the reader more confidence that the bus bar that they are using is a good one, they can use or have more confidence in general to ensure they are taking the right steps to interact with the targeted device.

3.

I would suggest that they include more information about how they interact with their targeted device so that it helps the reader understand how to do it in a proper way.

I would feel confident using this paper as a reference because even though it lacks some detail it still provides the reader with a crucial understanding of the method being used. It gives us an idea of another method that we can use, and we can research further in that direction to learn more about it.