From: Matthew Luallen

To: Behnam Ghaffari
Date: February 05, 2020

Subject: 0118-EX-ST-2020

Message:

We are requesting permission to allow participants at the ICS Sandbox during the RSA Conference to experiment with wireless replay attacks and defenses.

We have designed an example to demonstrate a wireless replay attack. The model uses 433 MHz and consumer grade technologies. We associate the impact and defense with industrial technologies. CYBATI will allow participants to perform the wireless transmission during the RSA Conference at the Moscone Center in San Francisco during the requested week. If this laboratory exercise is successful we may request formal FCC approval beyond temporary.

CYBATI personnel have captured wireless traffic from a consumer grade temperature and humidity sensor as well as data from a consumer grade wireless relay. CYBATI uses publicly available software on Github using a Raspberry PI version 3 to capture select wireless traffic of sensor data and actuator control. The experiment participants will use the same software to transmit the captured data. The tool is configured with the appropriate frequency to capture using a software defined radio and then is subsequently configured to transmit the captured data using GPIO 4 (Header Clock pin) located on the Raspberry PI. The pin is connected to a 6.7" breadboard wire serving as the antenna. The pin itself uses 16ma for the transmission. The intent is demonstrate 1) the ease of capturing replay-able wireless transmission and 2) the ability to transition a CPU clock in to a intentional radiator.

The intent of the exercise is to demonstrate the need to protect wireless transmissions through supply chain, authentication, integrity and confidentiality controls.