Trideum Cyber-Physical Learning Model Security Assessment

Assessment by Chris Stickney

Last updated 4/25/2024

Cyber-Physical Learning Model by Wesley Cooke, Lauren Murach, Brycen Havens, and Chris Stickney

Executive Summary

Since our system will be offline the majority of the time, the primary vulnerabilities this system has are physical, only able to be taken advantage of by insiders and intruders. The primary vulnerabilities found in the building include two critical vulnerabilities in the RFID door which may allow illicit access to the restricted area it protects, and vulnerabilities in the temperature sensors, which can lead to improper measurements being sent to the controller. These HVAC vulnerabilities can lead to damage of expensive computational assets if the temperature gets too cold or warm. Lastly, the motion sensors in use can be circumvented if they are unable to detect thermal signatures moving, allowing intruders to not trigger alarms in the building after hours. These issues are the most troublesome issues found, and should be addressed immediately to improve site security and reduce risk.

Contents

Flipper Zero Can Bypass RFID Door Security

Threat Actor: Building Intruders and Insiders

Vulnerability: The Flipper Zero is a multi-purpose tool, with one of its capabilities being reading, saving, and emulating RFID and NFC tags. This means that a user with a Flipper Zero is capable of opening the RFID door without an RFID or NFC tag with access to the door, provided they are able to read the RFID or NFC tag with the appropriate permissions to open the door.

Mitigation: Implement more complex RFID and NFC systems, such as an RFID or NFC system that needs two RFID or NFC tags from the same card to gain access. It should also be noted that the process the Flipper Zero uses to read RFID and NFC cards takes several seconds, making successfully reading an RFID or NFC card more challenging for malicious actors. In addition, the Flipper Zero tends to cause errors in the RFID reader code, as occasionally the signal sent is not identical to the copied RFID or NFC tag.

Impact: Malicious actors can utilize this to bypass secure doors, gaining access to restricted areas. Any systems located in these restricted areas will be vulnerable to physical tampering.

PIR Motion Sensors Can Be Bypassed With Thermal Insulation

Threat Actor: Building Intruders and Insiders

Vulnerability: PIR motion sensors are unable to detect motion from objects with masked thermal signatures since PIR sensors rely upon thermal changes to trigger the sensor.

Mitigation: Other forms of motion detection may be used, such as Microwave motion sensors, which send a signal if a significant change is detected in the distance between the sensor and an object. Microwave sensors can be extremely sensitive however and can read data through walls at times. Other forms of motion sensors exist which have different upsides and downsides than PIR sensors and Microwave sensors.

Impact: Security alerts for people intruding on the building after hours can be prevented, giving malicious actors free access to the building (minus restricted areas), where they are free to do what they please.

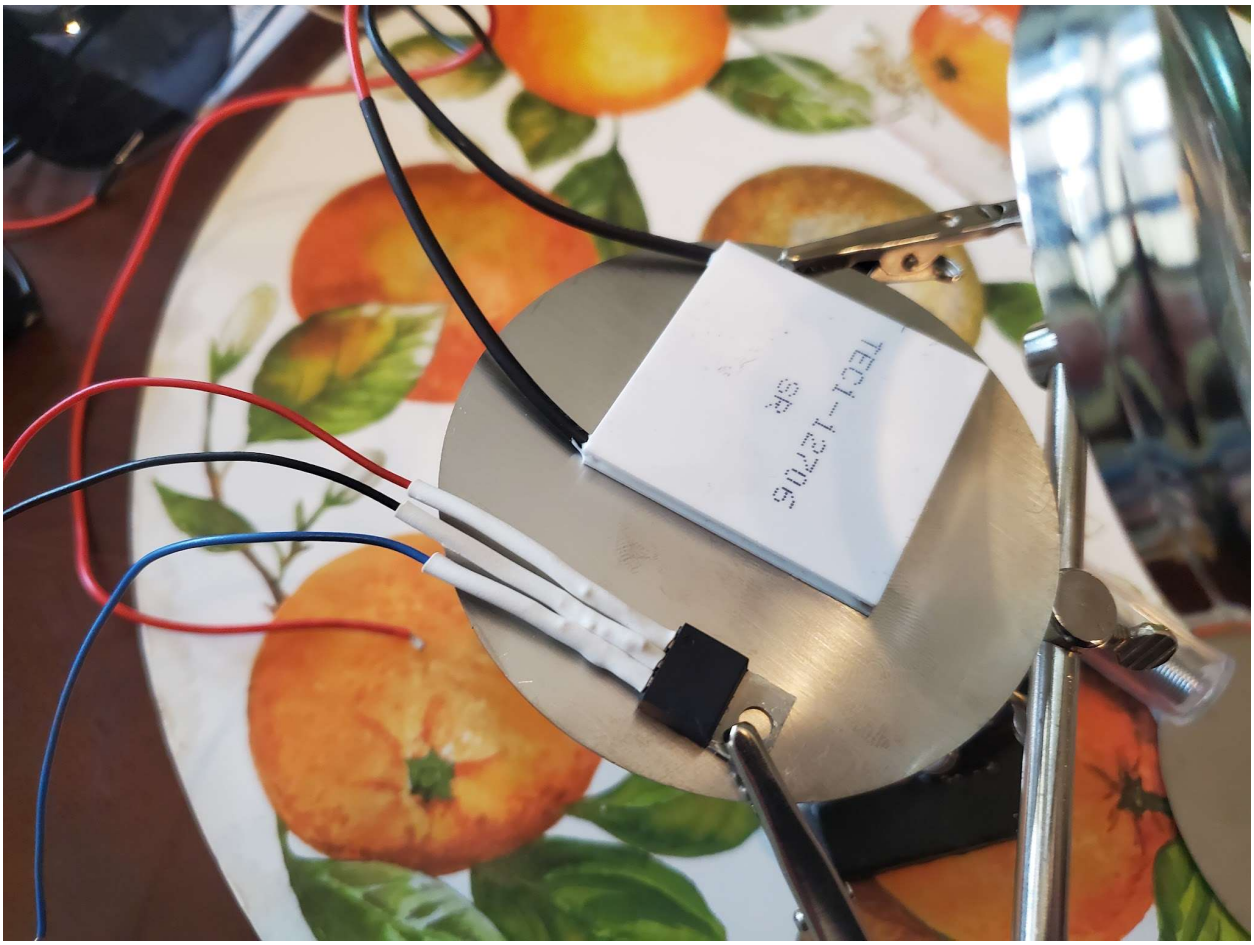
Temperature Sensors Are Vulnerable to Physical Manipulation

Threat Actor: Building Intruders and Insiders

Vulnerability: TC74 temperature sensor is a contact-based temperature sensor, meaning very hot or very cold objects may be applied to the sensor to manipulate readings and interrupt HVAC operations.

Mitigation: Change the TC74 sensors out to a non-contact-based temperature, which operates by reading infrared radiation of the surroundings. These can be interrupted by objects that cloak thermal signatures being placed around the sensor, like an acrylic dome covering the sensor. The best solution for both of these vulnerabilities is to place the temperature sensors in concealed, out of reach locations to prevent tampering.

Impact: HVAC controls being manipulated can lead to uncomfortable working environments, or in more extreme cases, damaged computer systems if the temperature becomes much too hot or too cold. In this case, this can cause large financial loss of assets.



This image shows a similar contact based temperature sensor on a hot plate. A similar setup could be used to manipulate the TC74 into running the HVAC too much. The opposite could also occur if a cold object was attached to the TC74.

System Stability Could Be Crippled By Online Attacks Which Ruin System Performance

Threat Actor: Malicious Outsiders and Insiders

Vulnerability: The control software's operation could be interrupted by applications with high performance draw, which could be activated by outside users to interrupt the system.

Mitigation: Critical cyber physical systems which can remain offline should remain offline to prevent connections. The Raspberry Pi should be placed within a secure location to better protect against unauthorized manipulation. Alternatively, if the system must be connected to the internet, ensure proper security practices are in place and for added security against attacks, implement an IDPS that can cut off connections. As a final line of protection, implementing revised code that can improve the average Lyapunov stability of the system while under external stress should be considered. This should not be an issue, as the system only needs to momentarily touch the internet to set the system time.

Impact: If systems have inadequate safeguards against online attacks such as DDoS attacks or False Data Injection attacks, the system's performance and behavior could be altered, leading to the system running behind or breaking entirely, needed to be restarted.

Reed Switches May Be Manipulated With Strong Enough Magnets

Threat Actor: Insiders and Building Intruders

Vulnerability: Reed switches can be easily activated if not properly concealed or if too sensitive. Magnets can be affixed to extra surfaces to make systems malfunction.

Mitigation: Getting reed switches with less sensitivity may work, but a better solution to ensure the operation of the elevators is not interrupted is to make sure applying magnets in locations that may disrupt the elevator is very challenging. Hall sensors would also have issues since they also rely upon magnetic fields.

Impact: Strong enough magnets placed within or around the elevator cabin could interfere with the reed sensors, sending faulty signals to the controller which may result in the elevator stopping in the wrong spots.

Physical Access to Wires May Allow Replay Attacks

Threat Actor: Insiders and Building Intruders

Vulnerability: If attackers are able to identify which wires are used for SPI or I2C, they could mimic signals sent by sensors, such as the temperature sensor or RFID card reader. This can lead to system malfunctions due to the system receiving erroneous data from malicious devices. It should also be noted that the motion detection system also faces this issue, as an external device could send a constant high or low signal to manipulate the program into thinking there is motion when there isn't or there isn't motion when there is.

Mitigation: The best way to mitigate this threat is to ensure that all wiring is protected from tampering. Exposed wiring can be disconnected from their sensors and connected to a malicious device which sends false information. New log alerts could be made which record when unreasonable values are detected for the RFID reader or temperature sensors.

```
#include <SPI.h>
void setup() {
  Wire.begin(0x48);
  Wire.onRequest(sendReading);
}

void loop() {
  delay(100);

}

void sendReading() {
  Wire.write(0x1D);
}
```

This simple program is able to send a false temperature reading of 29°C, which equals around 84°F. It should be noted that this program is run on an Arduino which uses 3.3V logic like a Raspberry Pi. The erroneous value being sent will force the HVAC system into cooling the floor with the TC74 with address 0x48. This code could be altered to send a constant value below the activation threshold to prevent the HVAC from turning on.

Impact: HVAC controls being manipulated can lead to uncomfortable working environments, or in more extreme cases, damaged computer systems if the temperature becomes much too hot or too cold. In this case, this can cause large financial loss of assets. A similar attack using more advanced techniques may also be performed on the RFID door, where information could be captured and retransmitted by a third party device, allowing the door to open without an RFID device being used. This allows illicit access to restricted areas that are supposed to be protected by these doors, which can lead to restricted system tampering.