STUDENT SUMMER INTERNSHIP TECHNICAL REPORT

Authentication Protocol for Industrial Control Systems without Encryption

DOE-FIU SCIENCE & TECHNOLOGY WORKFORCE DEVELOPMENT PROGRAM

Date submitted:

September 14, 2018

Principal Investigators:

Ryan Cruz, DOE Fellow Student
Florida International University

Mr. Robert Barnett, Mentor
Savannah River National Laboratory

Florida International University Program Director:

Leonel Lagos Ph.D., PMP®

Submitted to:

U.S. Department of Energy
Office of Environmental Management
Under Cooperative Agreement # DE-EM0000598

FIU | Applied Research Center
FLORIDA INTERNATIONAL UNIVERSITY

ABSTRACT

Digital signatures added to industrial control systems as the proper authentication method is a top priority research effort being conducted at the Savannah River Site. The common protocol of Modbus was chosen to coincide with testing the added authentication. The implementation of a digital signature as the main authentication using TLS without encryption enabled will replace the standard encryption format. The proposed method for authentication was designed into the network using Raspberry Pis to run proxy servers to host the TLS protocol. These are just some of the requirements necessary to prevent malicious attacks to the infrastructure of industrial control systems.

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION

Industrial control systems (ICS) describe the different types of control systems and associated instrumentation which includes the devices, systems, networks, and controls used to operate and/or automate industrial processes. Depending on the industry, each ICS has different architectures and are built to electronically manage tasks efficiently. Historically, industrial plants have not included networking, and the addition of networking technologies over time have been done without consideration for security. As a result, many ICS devices currently have inadequate security features.

To address this general deficiency, many approaches are being developed to add security to the ICS environment. One practice that is becoming popular is deep packet inspection. This method takes advantage of the fact that many end devices in ICS have a very limited scope of possible commands; therefore, it is easy to inspect packets and verify that legitimate commands are traveling across the network. However, this still leaves open the possibility that devices can be abused with legitimate commands. This was the case with the recent Crashoverride malware (Lee, 2017). This method will also not protect against rogue devices added to a network by an insider threat that also issues legitimate but malicious commands. Therefore, a method of providing authentication between low-level devices and higher-level human machine interface (HMI) was devised. This method proposed using TLS without encrypting the data so that deep packet inspection is not hindered.

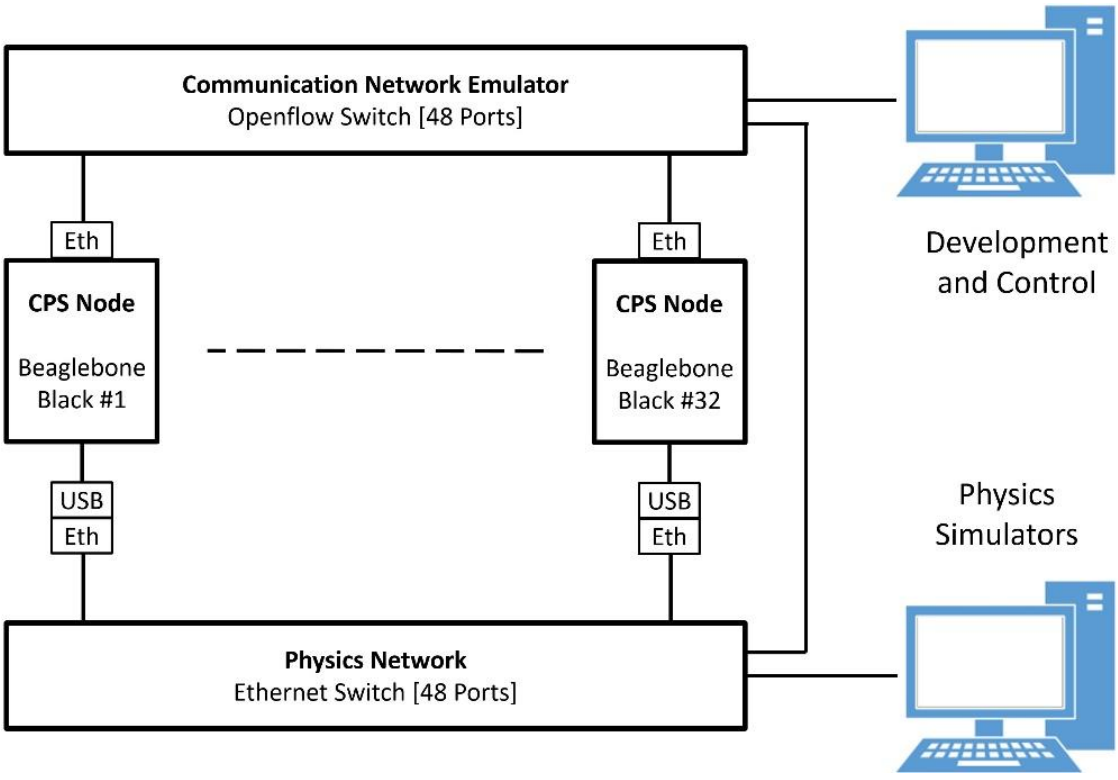

Figure 1. Cyber physical system hardware-in-the-loop testbed (Tang and Stouffer, n.d.).

In order to implement this scheme an authenticated connection is implemented using transport layer security (TLS) between two proxy servers between the end devices I/O and the HMIs. TLS has an obscure option that allows the obfuscation of the encryption to be disabled while still including digital signatures. This then allows for authenticated transmission of packets without obscuring the contents of the payload. The architecture in figure 2 was proposed as of the configuration for a cyber-physical test bed, which allows emulation of hardware components needed for data generation. Figure 1 shows the architecture of the cyber physical systems (CPS) security hardware-in-the-loop (HIL) testbed (Chidambaram Pappa, 2016). This is a general block diagram of the network envisioned for testing the proposed method. Within this network we would test the system to verify we can observe a difference between authenticated and unauthenticated traffic.

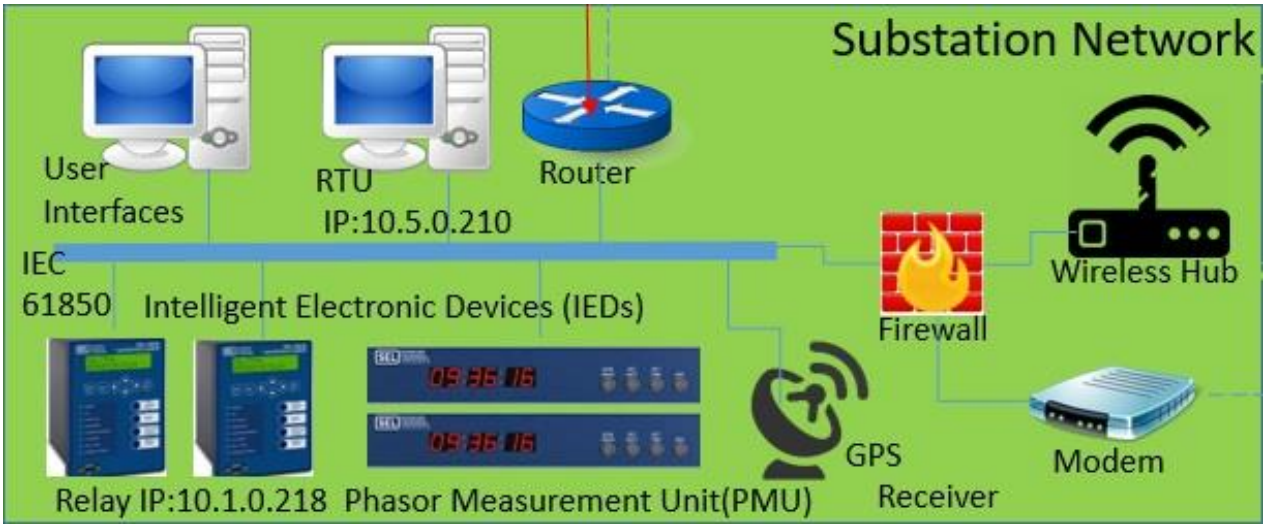

Figure 2. Example network for ICS of a normal internet connection sharing (ICS) network (Chidambaram Pappa, 2016). Deep packet inspection often is applied between the packets going between the relays and phase measurement units (PMUs), and the remote terminal units (RTUs). It is this line of communication that can be abused with legitimate commands telling the end devices to do inappropriate things.

2. EXECUTIVE SUMMARY

This research work has been supported by the DOE-FIU Science & Technology Workforce Initiative, an innovative program developed by the US Department of Energy's Environmental Management (DOE-EM) and Florida International University's Applied Research Center (FIU-ARC). During the summer of 2018, a DOE Fellow intern Ryan Cruz spent 10 weeks doing a summer internship at the Savannah River Site (SRS) located in Aiken, South Carolina, under the supervision and guidance of Mr. Robert Barnett from SRNL R&D Engineering. The intern's project was initiated on May 31, 2018 and continued through August 9, 2018 with the objective of developing an authentication protocol for industrial control systems without encryption.

3. Research Description

The setup includes a single serial cable connecting the serial ports on two devices, a Master and a Minion. Authentication will occur in the following methods:

- Data layer involving transport layer security/secure socket layer (TLS/SSL)
- Transmission control protocol/internet protocol (TCP/IP) route implementation
- Key exchange algorithm
- Raspberry Pi programming for hosting TLS/SSL

Modbus is the chosen ICS protocol. It is used to transmit signals from instrumentation and control devices back to a main controller or data gathering system. The overall network architecture begins with level 0 and level 1 devices (Weiss, 2018). Level 0 is the physical process. Level 1 is defined as a group of intelligent devices that operates and detects the physical process. Level 1 consists of field devices such as actuators, analyzers, process sensors, and related instrumentation that all operate on physical process due to their known standard of having the highest recognition of trust (Neitzel & Huba, 2014).

These two devices comprise of a sensor that will connect through a WAGO I/O device. WAGO is a vendor in the automation technology industry. They have a variety of input/output devices such as PFC100 and PFC200 controllers. WAGO devices are integrated with firewall protection against unauthorized access. The essential device that is necessary for the authentication to function efficiently with the industrial control systems protocol Modbus, is the Raspberry Pi. This device handles the authentication for the network traffic by implementation of a proxy server running the unique version of TLS. It will then verify if it can connect to the router such as going from one TLS device to another thus establishing a trusted link between two end points on the network.

The proposed network architecture of the Modbus protocol transmission was constructed as follows:

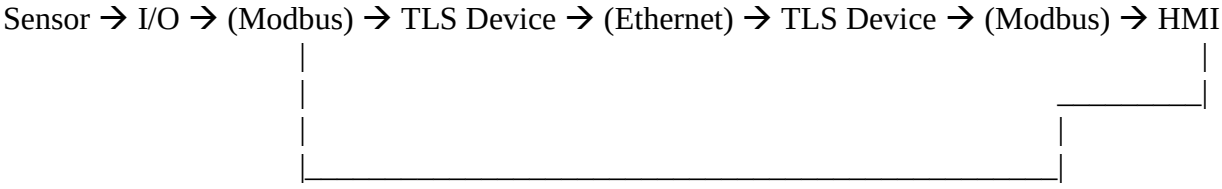

Figure 3. Initial design of the network architecture.

The infrastructure of the network begins with the sensor communicating its way to the WAGO input/output device via Modbus, which is by default an unauthenticated protocol. Data received from the sensors or the commands from the HMI will then be passed over by means of the Ethernet.

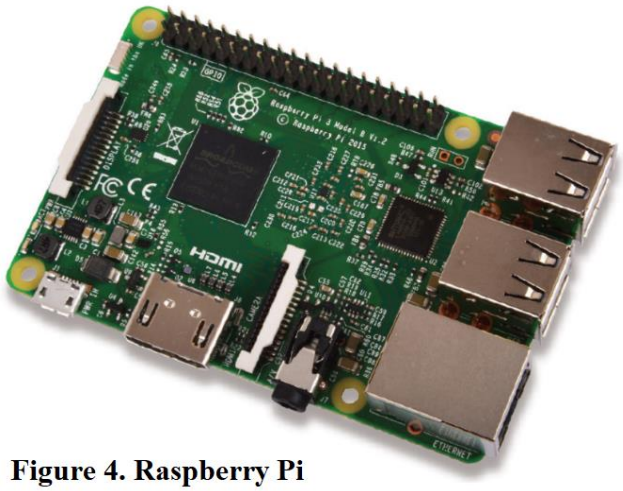

Figure 4. Raspberry Pi

A Raspberry Pi, as shown in Figure 4, cannot function without the installation of an operating system (OS) to the device. The highly recommended OS for the device is Raspbian because of the various features and utility software mechanisms that was included during its development. For setting up the Raspberry Pi, a guide was used for installing the OS to the Pi (Cawley, 2015). The guide included the following steps:

1. **Find an SD Card.** It must have a memory of at least 2 GB.

2. **Install the Raspbian OS on to the SD Card.** Be sure that there are no files in the card prior to installment.

3. **Use Win32DiskImager to write disk image.** Run it as an administrator prior to opening the software.

The importance of a proxy server is to store web site files and transmit data via the internet. In other words, they provide more control over what goes in and out of a network. A proxy server is very significant for the two Raspberry Pis to be able to communicate with one another. Figure 5 demonstrates the correlations of a proxy server between the transmissions of data from a PC at a workspace over the internet. The chosen proxy server is Squid due to its involvement of TLS with Nginx. It has an effectiveness towards being an SSL termination proxy. Certbot auto adds the necessary Nginx directives to set up the TLS certificate and redirect to HTTPS by default. By using the TestSSLServer tool, running the "TLS_RSA_WITH_NULL_SHA cipher suite" command is one way to protect authenticity and integrity without encryption.

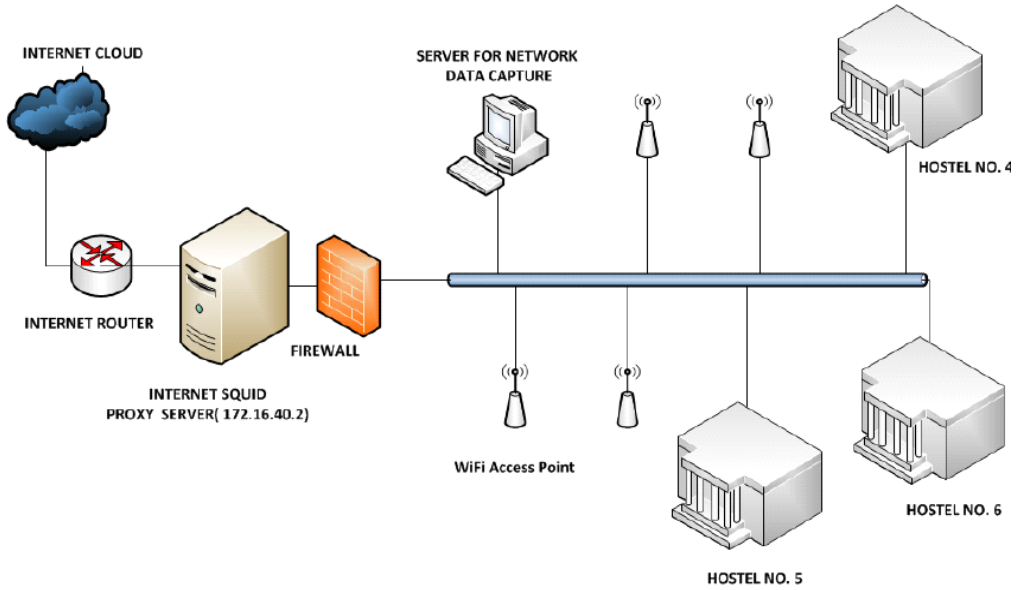

Figure 5. Visualization of a proxy server (Singh *et al.*, 2013).

The diagram in Figure 6 displays the final setup of the network architecture for authenticating the industrial control system. Previously, it consisted of a supervisory control and data acquisition (SCADA) connecting to a programmable logic controller (PLC). As seen here, the flow of the new architecture begins with the sensor going to the I/O system and, between the two devices. Modbus is used as the communication protocol. The process after that involves two Raspberry PIs which are providing the authenticated connection. The first Raspberry Pi, along with the sensor and I/O, acts as the sender. It will then send data through the TLS plus TCP/IP routing to the other Raspberry Pi, acting as the receiver. Once that process is done the flow then goes to the SCADA up until the human machine interface. The involvement of transport layer security/secure sockets layer all will occur in the TCP/IP layer.

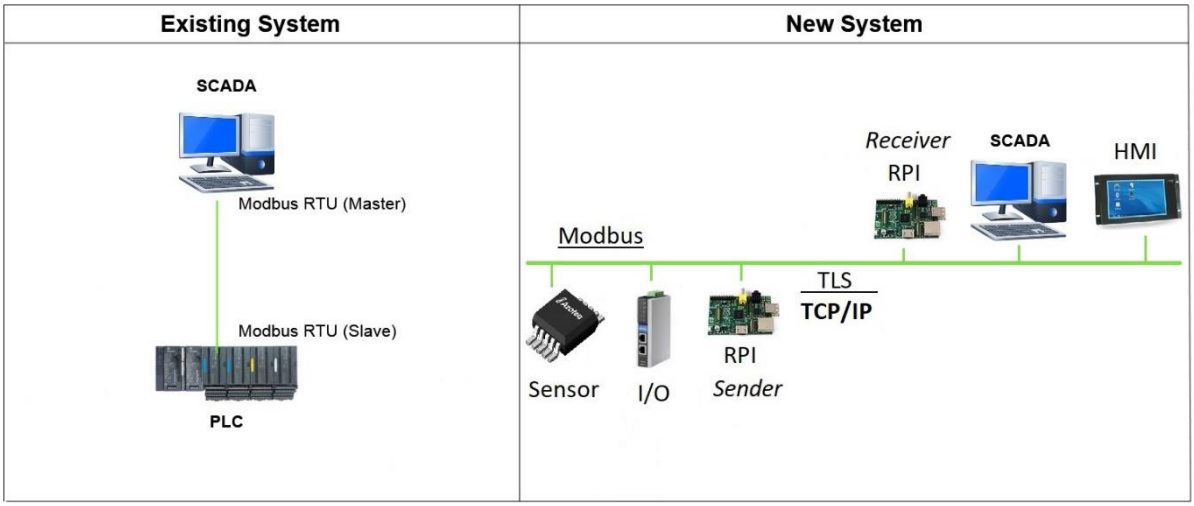

Figure 6. Network architecture for ICS.

In the following diagram, an act of a man-in-the-middle attack takes place. This is a type of malicious attack commonly seen against vulnerable systems. Industrial control systems tend to be susceptible to these types of attacks, causing them to be easy targets.

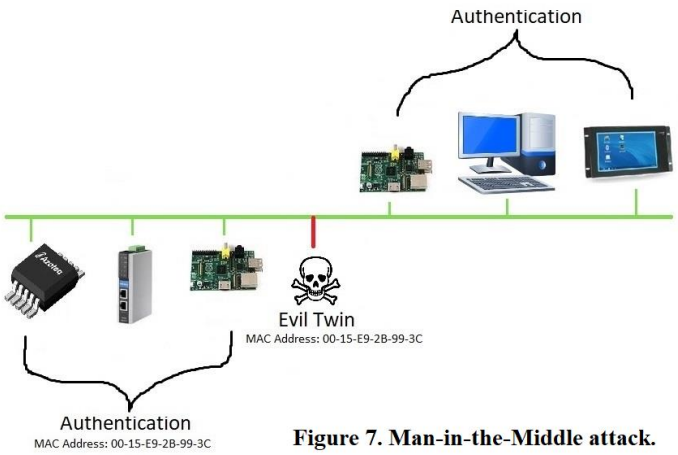

Figure 7. Man-in-the-Middle attack.

To test if the authentication method provides data protection, an evil twin would be introduced to the network on the same bus as the raspberry pis. An evil twin device is a device on a network that shares the same MAC or IP address as another device that is providing malicious data or connections to devices trying to communicate with the good twin. Figure 7 shows the evil twin added on the same bus as the raspberry pis. The good devices are behind the pi providing authentication. In this arrangement the good device sits behind the authenticated route, and the evil twin is outside of it, but still topographically equivalent. This configuration will allow us to verify that the evil twin can be ignored from passing malicious data upstream.

4. RESULTS AND ANALYSIS

Typically, the device identity is assumed but not verified. For verifying device identity, a digital signature architecture with TLS was constructed. Figure 8 represents the requirements necessary for a digital signature. A novel adaptation of this is to use only the digital signature that is provided and not the encryption capability. This allowed ICS traffic to flow unobscured while still providing verification for the integrity of the data. Verification of this process will involve adding additional I/O level network devices with spoofed IP addresses and detecting the authenticated versus unauthenticated traffic.

The time provided for this project allowed for the construction of the basic network needed to test this configuration, but not full testing of the authentication method.

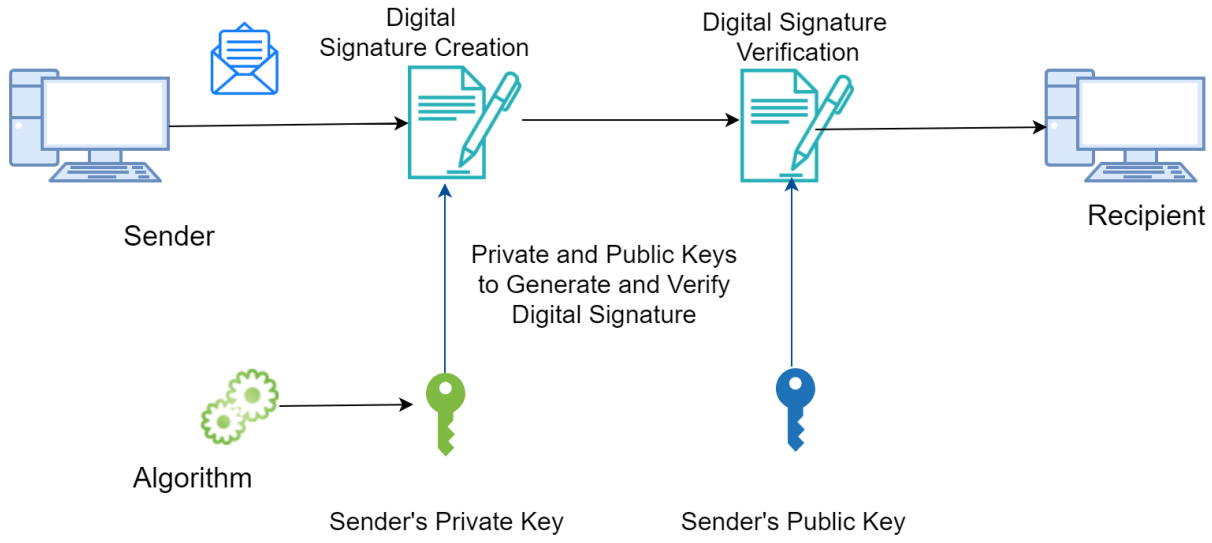

Figure 8. Digital signatures ("Electronic-signatures-vs-digital-signatures", 2017).

5. CONCLUSION

Industrial control systems are designed to constantly meet safety and regulatory requirements. Cybersecurity for ICSs not only consist of securing the OT networks but also the analyzers, instrumentation, and controllers. Each of them communicate by serial-based protocols before being converted to Ethernet communications. ICS security is different from ordinary IT security. ICS security aims to maintain integrity of production processes and component availability. The validation of critical information is a priority and any decrease in production equates to a financial loss.

The Raspbian operating system was able to install successfully into the Raspberry Pi. The final phase for this experiment required the Raspberry Pis to function properly, have proxy servers on the Raspberry Pis, and configurations for the proxy servers. Once configured, a router was added to connect the Pis to the network, allow for verification, and direct network traffic. After the traffic was sent, communicating between the two Raspberry Pis, the architecture for the network was finalized. This portion of the project was not completed this summer due to time constrains.

This experiment conducted during the internship at Savannah River National Laboratory had a primary goal of building the test setup of the network, which was completed. This should allow for scaling to a larger network size after the initial proof of concept. One concern with this scheme is a certificate deployment has a large-scale key management. Network size will thus increase the key management task for security. This configuration may still be vulnerable to man in the middle attacks. A man-in-the-middle (MiM) attack is a malicious user or device that disguises itself between two parties communicating with one another where it causes alteration and unauthorized access to information passing between the two parties. The weakness of the method proposed here is that a MiM could still occur since the signature for the PIs are being sent in clear text. Further research should be performed to explore the use of this method to defeat man-in-the-middle attacks.

6. REFERENCES

Chidambaram Pappa, Aswin, "Moving target defense for securing smart grid communications: Architectural design, implementation and evaluation" (2016). *Graduate Theses and Dissertations.* 15681. https://lib.dr.iastate.edu/etd/15681

Cawley, C. (2015, January 21). *How To Install An Operating System To Your Raspberry Pi.* Retrieved September 7, 2018, from https://www.makeuseof.com/tag/install-operating-system-raspberry-pi/

Electronic-signatures-vs-digital-signatures. (2017, July 12). Retrieved September 21, 2018, from https://www.esigngenie.com/blog/electronic-signatures-vs-digital-signatures/

Lee, R. M. (2017, June 12). *CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations.* Retrieved September 21, 2018, from https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

Neitzel, L., & Huba, B. (2014, May/June). *Top ten differences between ICS and IT cybersecurity.* Retrieved September 6, 2018, from https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/2014/may-jun/features/cover-story-top-ten-differences-between-ics-and-it-cybersecurity/

Singh, R., Kumar, H., & Singla, R. (2013). *Sampling Based Approaches to Handle Imbalances in Network Traffic Dataset for Machine Learning Techniques*(Vol. 3). doi:10.5121/csit.2013.3704

Tang, C., & Stouffer, K. (n.d.). *Evaluating the Effects of Cyber-Attacks on Cyber Physical Systems using a Hardware-in-the-Loop Simulation Testbed*. Retrieved July 27, 2018, from https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=923409

Using a proxy server. (n.d.). Retrieved September 7, 2018, from https://www.raspberrypi.org/documentation/configuration/use-a-proxy.md

Weiss, J. (2017). *Hacking Level 0,1 devices can be more significant than Stuxnet.* Retrieved September 6, 2018, from http://iiot-world.com/cybersecurity/hacking-level-01-devices-can-be-more-significant-than-stuxnet/

Weiss, J. (2018, February 13). *The Gap in ICS Cyber Security - Cyber Security of Level 1 Field Devices.* Retrieved September 6, 2018, from https://sigasec.com/the-gap-in-ics-cyber-security-cyber-security-of-level-1-field-devices/