APT-Style Security Testbed and Ransomware File Detection in a Digital Substation

Seerin Ahmad, Bohyun Ahn, and Syed Alvee
Advisor: Dr. Taesic Kim
Department of Electrical Engineering and Computer Science
Texas A&M University-Kingsville

Abstract

Advanced Persistent Threat (APT) is a professional threat actor that uses continuous and sophisticated attack techniques to gain full system access to multiple industrial control system (ICS)/supervisory control and data acquisition (SCADA) devices. Previously, it has been observed that cyber-attacks by APT groups have been more and more increasing and threatening networked ICS including power infrastructures. This work first provides an APT-style security testbed and attack modeling method targeting the disruptive operation of a digital substation. Several real cyber-attacks, such as DoS, brute force, man-in-the-middle (MITM), and ransomware attacks, are emulated to validate the feasibility of the proposed security testbed. Besides, this work also investigates an artificial intelligence (AI)-based ransomware file detection method. The proposed ransomware file detection model is designed by a convolutional neural network (CNN) using 2-D grayscale image files converted from binary files. The experimental results show that the proposed method achieves 96.22% ransomware detection accuracy.

Terms and Definitions

- **Electrical Substation:** It is the interface between parts of the distribution grid and transmission systems where voltage is transformed from high to low or the reverse using transformers
- **Digital Substation:** It is a digitized substation where operation is managed between distributed intelligent electronic devices (IEDs) interconnected by communications networks
- **Advanced Persistent Threat (APT):** a professional stealthy threat actor who uses continuous and sophisticated attack techniques which have not been well mitigated by existing defense strategies
- **Ransomware**: The encryption of data or disruption of control in demand for a ransom.
- **Cyber Kill Chain (CKC) Model:** It is an attack modeling method that describing the chain of APT's actions in leveraging understanding of an adversary's tactics, techniques, and procedures.
- **Penetration Testing:** Emulating cyber-attacks on a target system.
- **Convolutional Neural Network (CNN):** It is a network architecture for deep learning which learns directly from data, eliminating the need for manual feature extraction.

Research Objectives

- Identifying the threats and vulnerabilities of a digital substation and potential attack APT-style models.
- Design of a cyber kill chain (CKC)-based ransomware attack modeling method.
- Penetration testing demonstration of a power transformer diagnosis system (PTDS) in a digital substation.
- Proposing a cybersecurity testbed.
- Investigates an artificial intelligence (AI)-based proactive ransomware file detection method.

Methodology

PTDS Security Threat Modeling

1. System Identification: Identifying 1) cyber-physical components such as hardware, firmware, communication, proxy, gateway, or cloud usage; 2) data modeling and data flow maps; and 3) current security mechanism of the system
2. Attack Vector: Specific path, method, or scenario that can be exploited to break into the PTDS in a digital substation.
   a) Attack Vector 1 through physical intrusion such as reverse engineering, USB attacks, supply chain, swapping, counterfeit, etc.
   b) Attack Vector 2 through manipulated substation devices and networks
   c) Attack Vector 3 through PTDS platforms and remote access via Internet.
3. Attack Modeling using MITRE ATT&CK for ICS method
4. Testbed: Real-time simulation of a substation in Simulink/OPAL-RT
5. Penetration Testing Demonstration
   a. xHydra/Ettercap/hping3 tools for initial access to the PTDS, and port scanning.
   b. IoT devices (e.g., Raspberry Pi) to represent an IED, SDU, and a PTDU.
   c. Kali-Linux OS (Raspberry Pi) to generate APT-style attacks.
   d. The ransomwares files consist of four different families: Cerber, TeslaCrypt, Locky and Darkside
6. Design & Training: Proposed CNN-based ransomware detection model is designed and trained in COLLAB (cloud computing platform by Google).
7. Experiment: The experiment is run on Raspberry Pi 4B and the program is written in Python 3.9.7 with Kera's and PyTorch as backend.

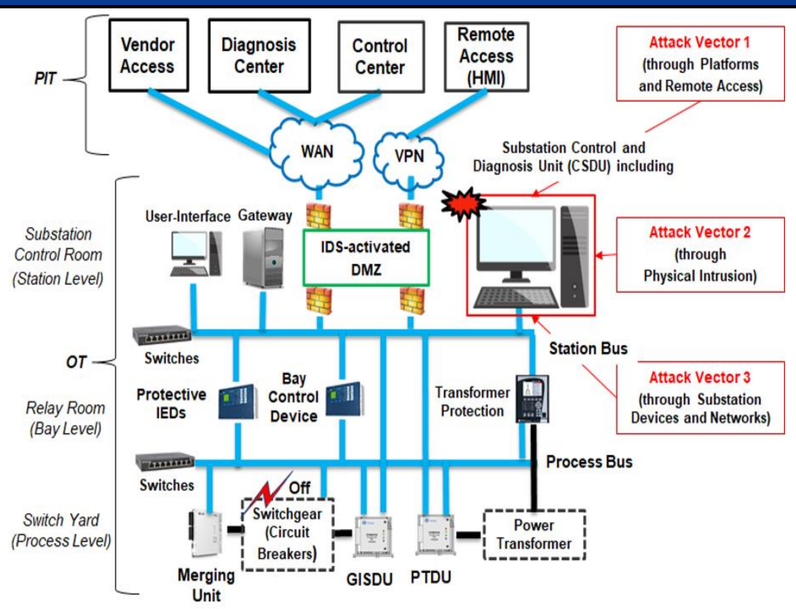


Fig. 1. An example of digital substation and attack vectors targeting PTDS (PTDU only or PTDU with a PTDS local server)

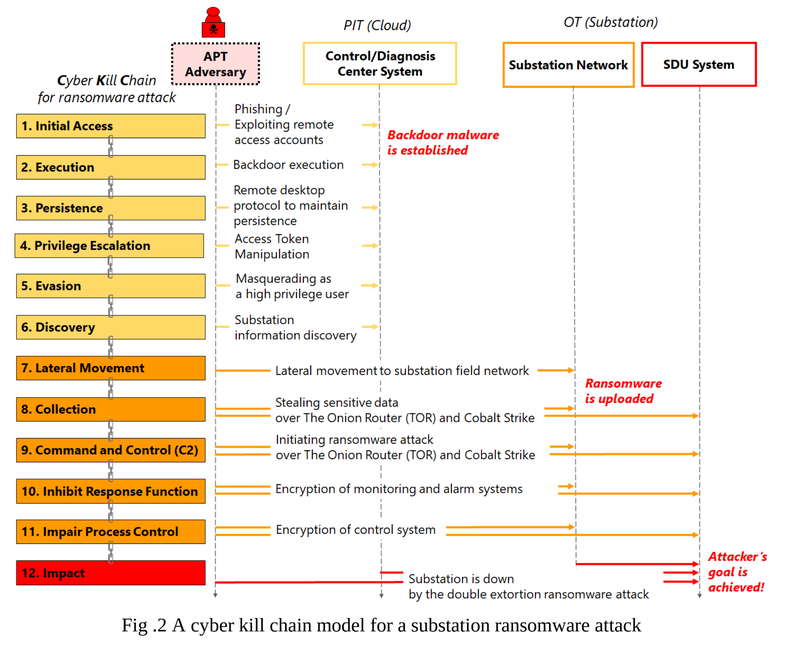


Fig .2 A cyber kill chain model for a substation ransomware attack

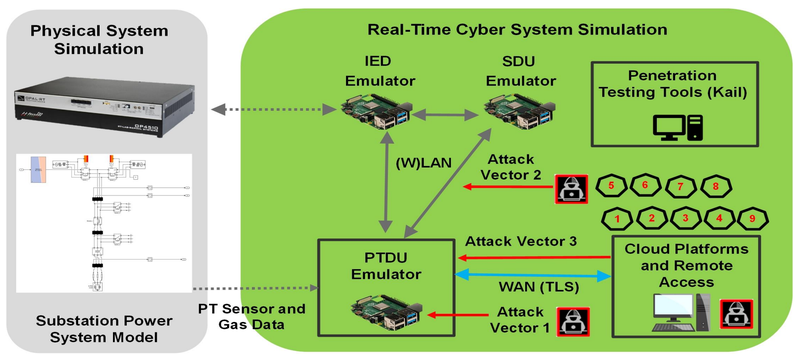


Fig .3 A diagram of the proposed real-time HIL cyber-attack testbed of a PTDS in a digital substation

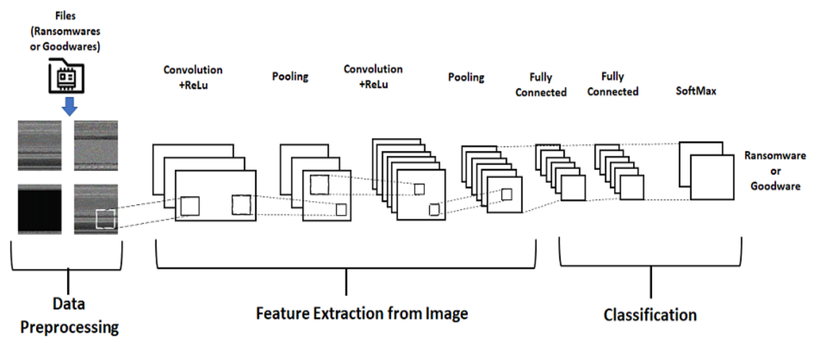


Fig .4 Proposed CNN-based ransomware detection method

Results

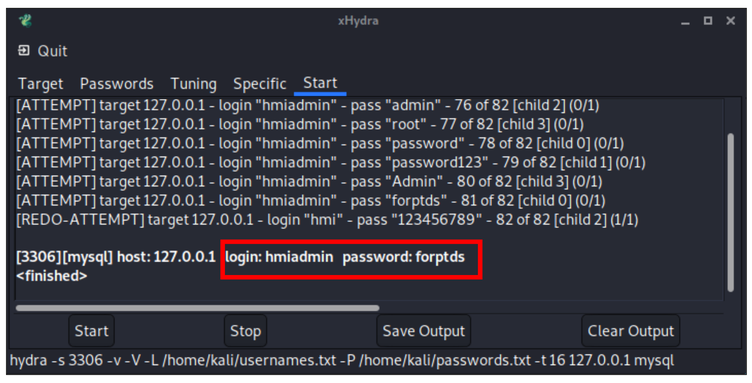


Fig .5(a) brute force attack to obtain log-in information of HMI

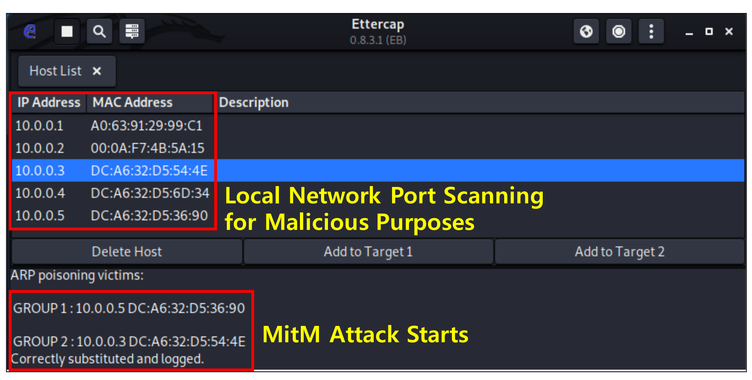


Fig .5(b) local network port scanning and MitM attack

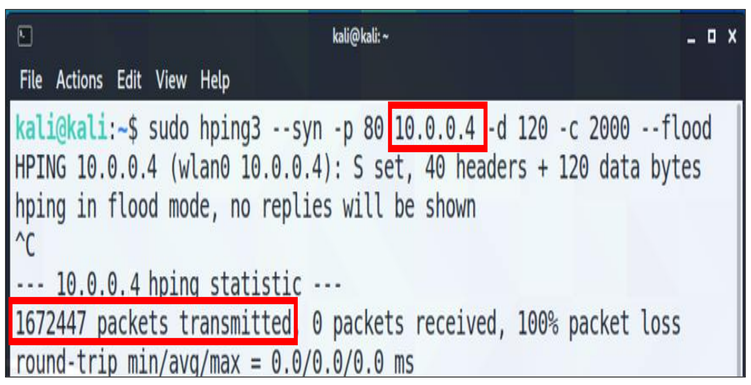


Fig .5(c) DoS attack sending numerous packets to PTDU

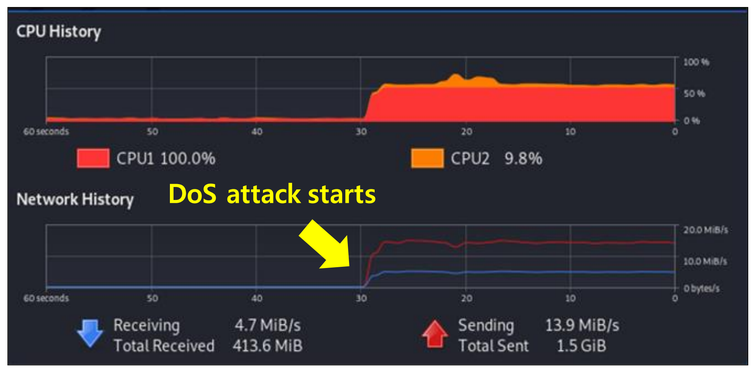
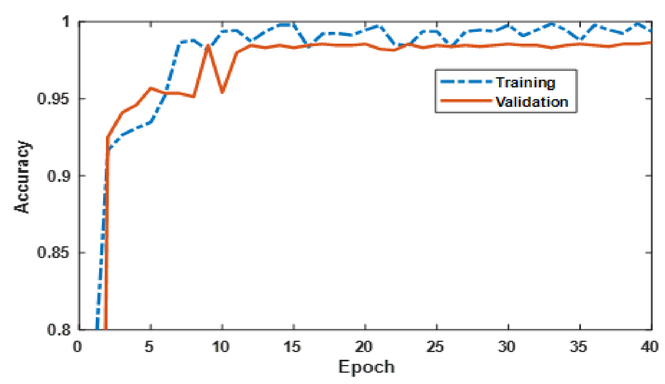
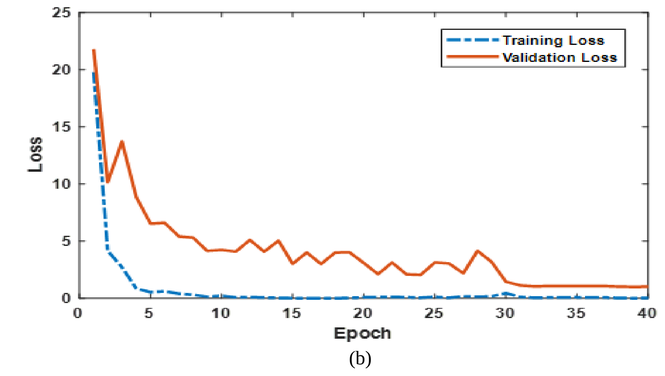


Fig .5(d) DoS attack impact on the PTDS resources



(a)



(b)

Fig. 6. Training and Validation results of the CNN model: (a) accuracy and (b) loss

Results Continued

TABLE I
THE COMPARISON OF RANSOMWARE DETECTION ALGORITHMS

Method	Feature Extraction	Datasets (ransomware/goodware)	Accuracy
Proposed	Images from raw files	672/845	96.22
Zhang et al. [16]	Opcodes from raw files using a disassembler	1787/100	91.43

Conclusion

- This work explores the APT-style cyber-attack modeling and proposes a real-time penetration testing testbed for online PTDS in Digital Substation.
- The proposed attack modeling and testbed can leverage security built-in PTDS that provides defenses for secure utilization of cyber-physical power transformers in modem power infrastructures.
- It explored potential attack surface of ransomware attacks in a digital substation and provided a CKC-based ransomware attack model.
- Moreover, this work has investigated and demonstrated an AI-based proactive ransomware file detection methods.

Future Work

- Upgrading the digital substation and network co-simulation model.
- Combining more attack vectors, models, and penetration testing tools in the testbed.
- Developing a comprehensive intrusion detection algorithm to be implemented in a security gateway in a digital substation.
- Investigating variants of malware attacks and defense methods.
- Developing a security-built substation devices such as PTDS, IEDs.

Acknowledgement

This work was funded by the Department of Energy (DOE, DE-EE0009026) and the Korea Electrotechnology Research Institute (KERI). Any opinions, findings or recommendations expressed in this poster were created by authors and not reviewed by nor necessarily reflect the views of DOE and KERI.

Selected References

S. Ahmad, et al., "Advanced persistent threat (APT)-style attack modeling and testbed for power transformer diagnosis system in a substation," in *Proc. 2022 IEEE PES ISGT-North America*, New Orleans, LA, April 24-28, 2022, pp. 1-5.