CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE
A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

Critical Security Vulnerabilities of Smart-Grid Power Meters

Author: Maximiliano Garcia (UTRGV)
Faculty Advisor: Dr. Sanjeev Kumar (UTRGV); Dr. David Nicol (CIRI, UIUC)

The University of Texas Rio Grande Valley

Homeland Security Challenge

Cyberattacks have become a common tool for adversaries to disrupt critical energy infrastructure. The entities behind cyberattacks more frequently aim to disrupt critical infrastructure affecting day-to-day life. Our team's challenge is the investigate and discover security vulnerabilities found in Smart Electric Meters, a critical component for the Smart Power Grid.

Background

Smart Grid is the name of an electrical power grid that utilizes devices that can communicate in more than one direction between the utility provider and the customers. A key device to a Smart Grid network is the Smart Electric Power Meter because of their Advanced Metering Infrastructure (AMI) capabilities. Research has shown that when these Smart Meters are faced with networking attacks, the data utility companies use to bill customers can show incorrect data that cause financial loss. This project focuses on security attacks that can compromise operation of Smart Grid and integrity of power data being reported to utility companies.

Approach / Methodology

A physical network using a switch, a router, and wireless access point was constructed to send data from the electric power meter to a monitoring station on that network as seen in Figure 1. Internet Control Message Protocol (ICMP) pings and Transmission Control Protocol (TCP) synchronization messages are used to attack the Smart Meters on the AMI network and investigate the adverse impact caused by these attacks, as reported in Figures 2-4.

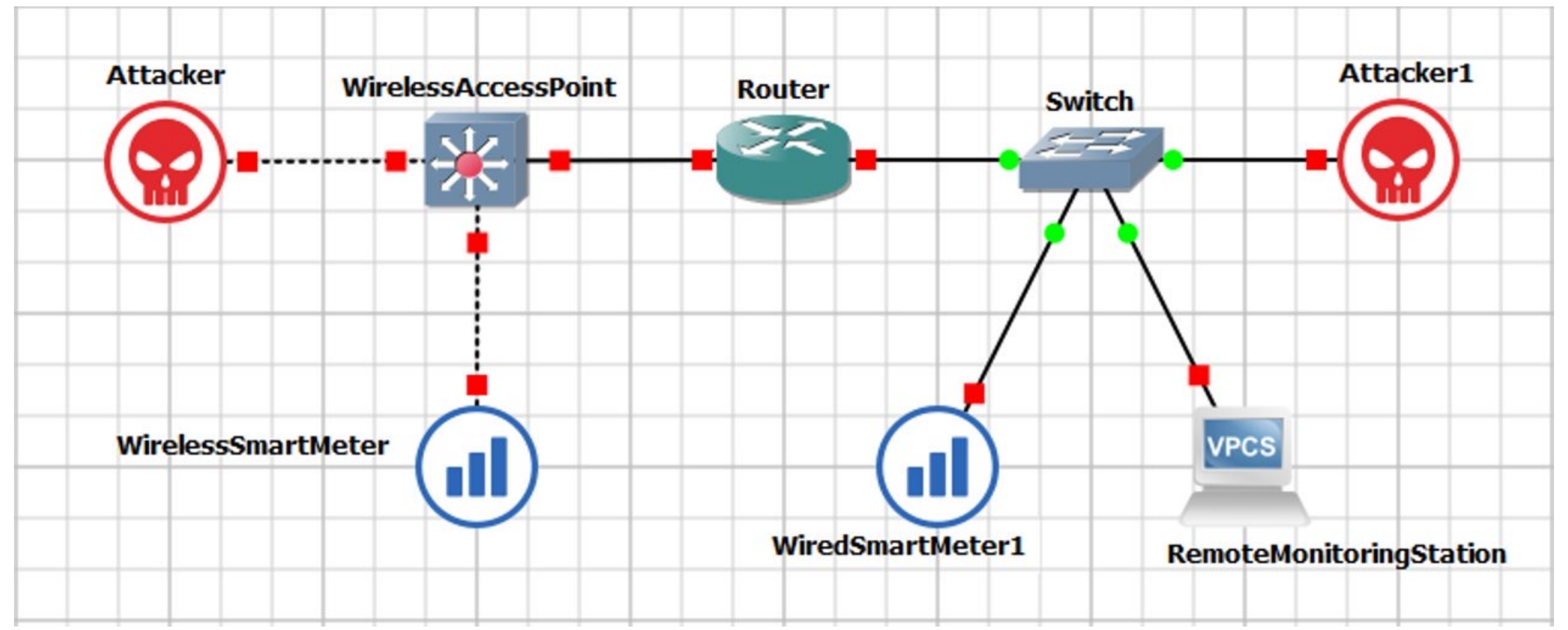


Figure 1. Network Topology

Outcomes / Results

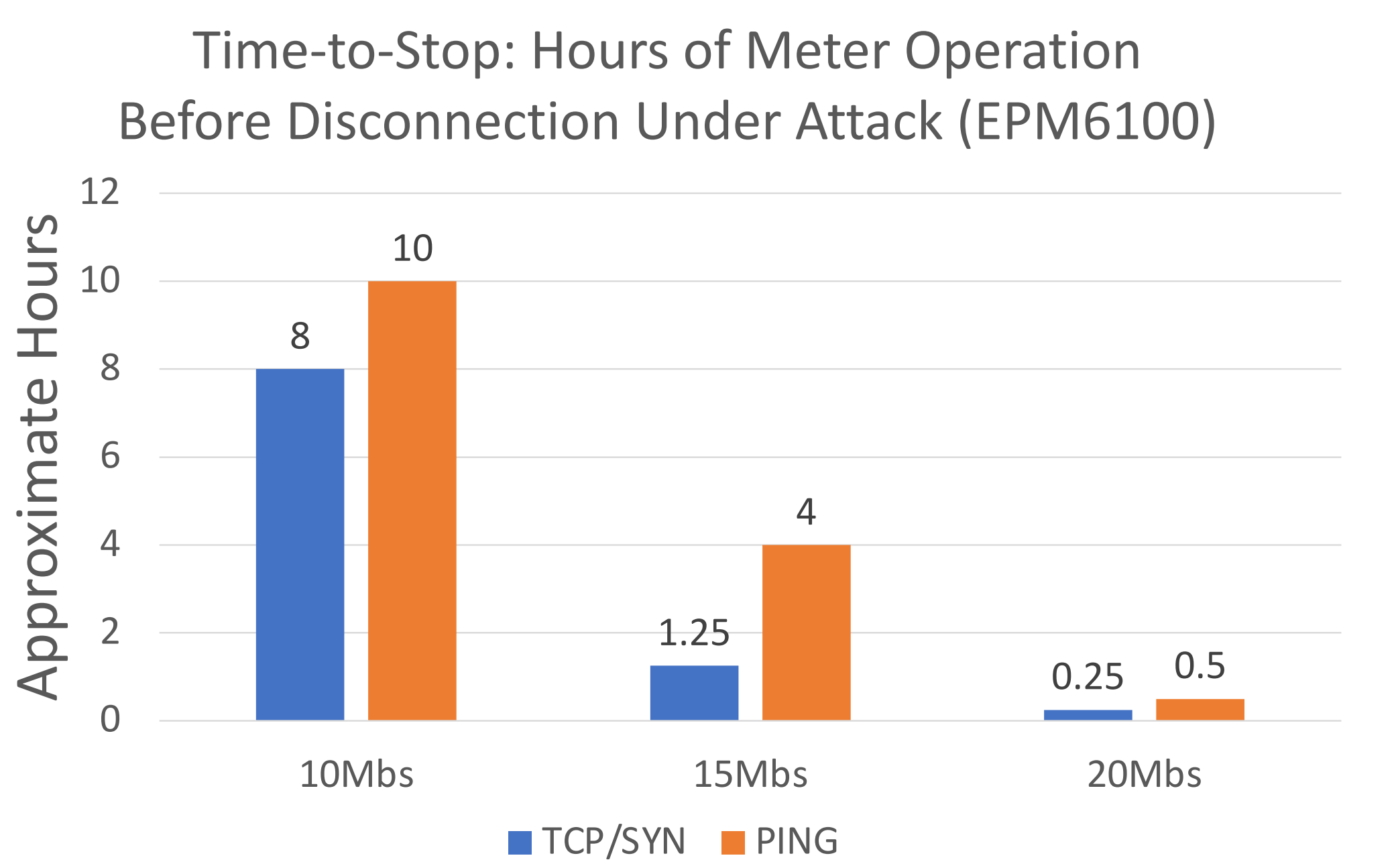


Figure 2. Hours of Operation before Connection Loss

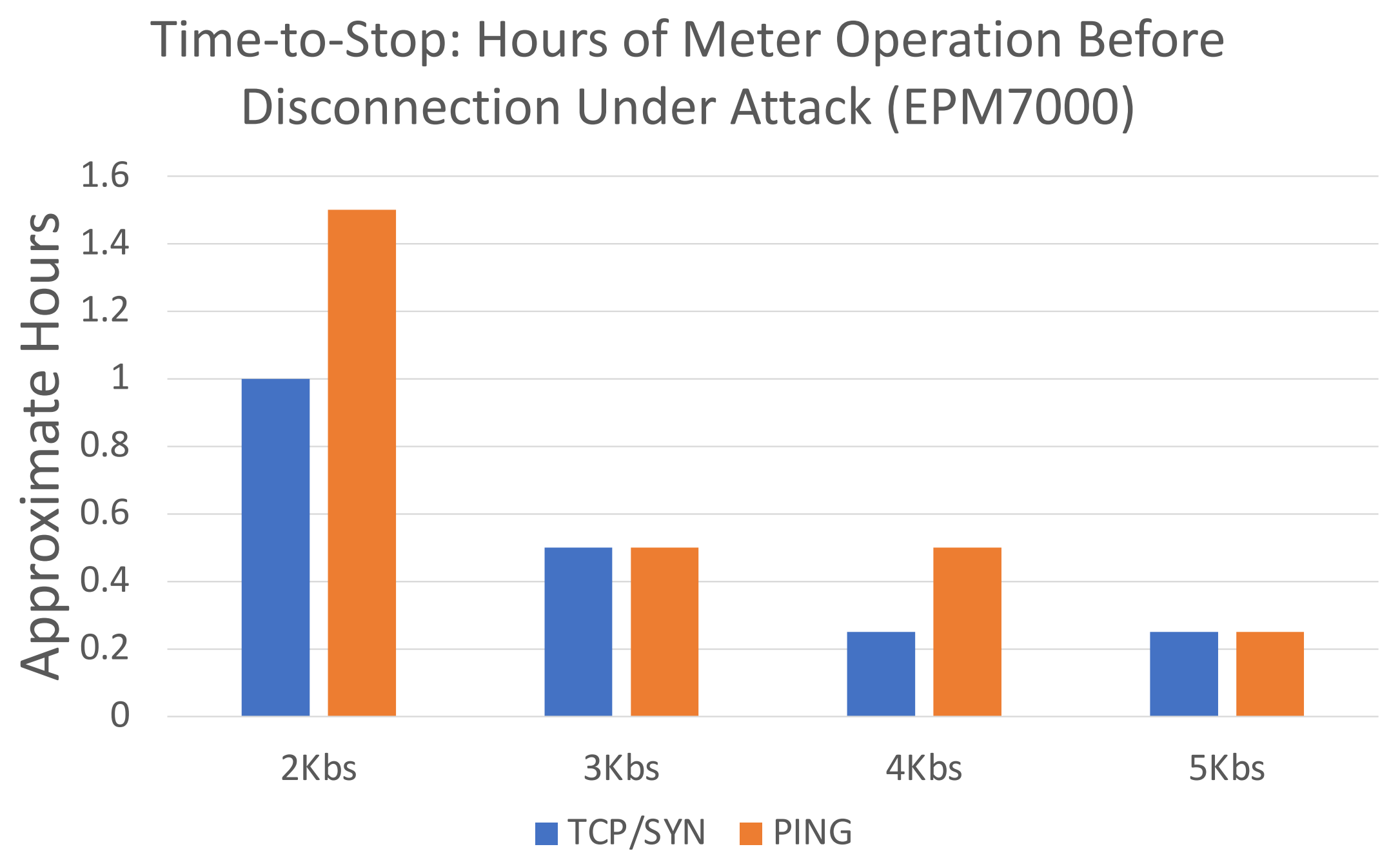


Figure 3. Hours Until Disconnect for EPM70000

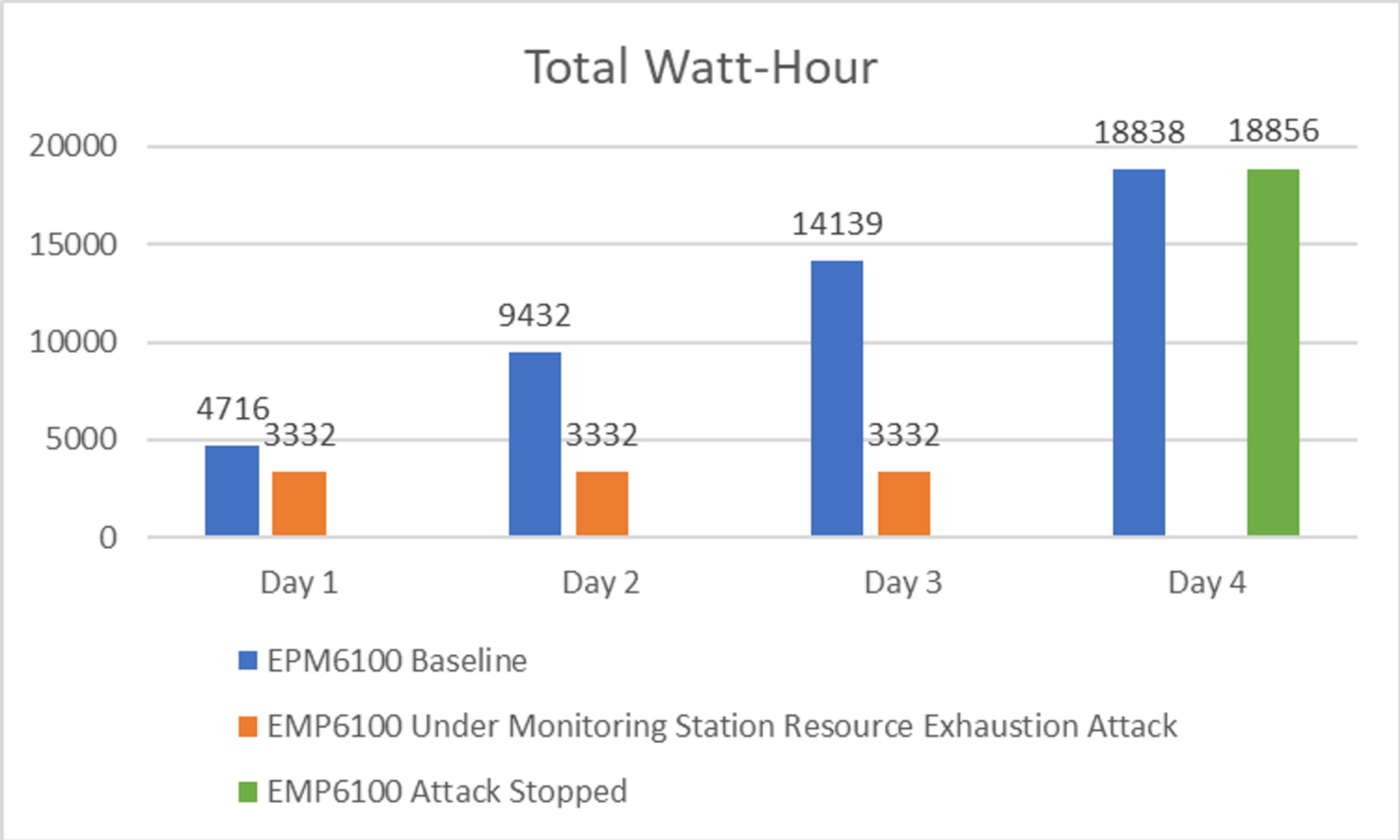
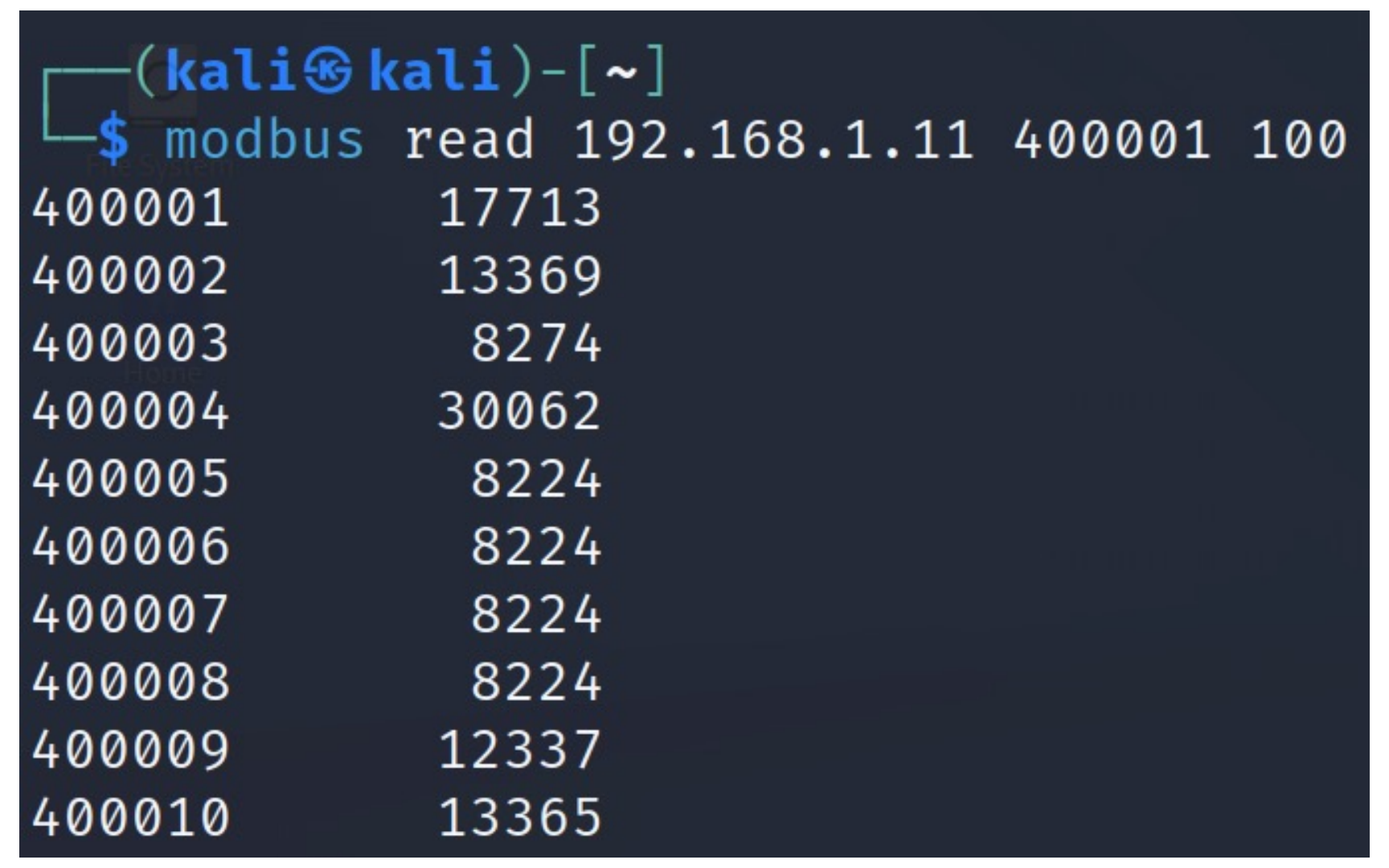


Figure 4. Data Loss in Ongoing Attack on the Monitoring Station



```
┌──(kali㉿kali)-[~]
└─$ modbus read 192.168.1.11 400001 100
400001      17713
400002      13369
400003       8274
400004      30062
400005       8224
400006       8224
400007       8224
400008       8224
400009      12337
400010      13365
```

Figure 5. Register Access Without Authentication

Attack	Type	Effect	Severity
Ping	Resource Exhaustion	Availability	Disturbs Operations
TCP/SYN	Resource Exhaustion	Availability	Disturbs Operations
Modbus Protocol	Protocol Exploit	Integrity	Data Alteration
Wi-Fi De-authentication	Protocol Exploit	Availability	Disturbs Operations

Table 1. Possible Vulnerabilities and their Severity

Impact

- Common security attacks can disrupt Smart Electric Meters and their operation
  - Attacks are found to stop the operation of Smart Electric Meters completely
  - Power data integrity can be affected
  - Meter data can be accessed without authentication by attackers

Conclusions

Our investigation shows that Smart Electric meters can be overwhelmed even by low bandwidth attacks. Our investigation shows that the Smart Electric Meters were compromised by denial-of-service attacks and protocol exploits. Internal software configuration on the meters of protocols used to communicate also poses a major risk if improperly configured. While the de-authentication attack targets wireless access points and devices on them; the good-faith nature of the Modbus protocol allows anyone on the network to possibly read and write to memory on the meters without authentication.

The significance of this work is that it has helped us discover serious security vulnerabilities in critical energy infrastructure. Furthermore, our study has provided us basis for further investigation and analysis related to security vulnerabilities in modern Electric Smart Grid infrastructure.

References

- S. Kumar, H. Kumar and G. R. Gunnam, "Security Integrity of Data Collection from Smart Electric Meter under a Cyber Attack," *2019 2nd International Conference on Data Intelligence and Security (ICDIS)*, 2019, pp. 9-13, doi: 10.1109/ICDIS.2019.00009.
- Eia.gov. 2022. *Frequently Asked Questions (FAQs) - U.S. Energy Information Administration (EIA)*. [online] Available at: https://www.eia.gov/tools/faqs/faq.php?id=97&t=3
- Adamiak, M., 2022. *IEC 61850 Communication Networks and Systems In Substations: An Overview for Users*. [online] Gegridsolutions.com. Available at: https://www.gegridsolutions.com/multilin/journals/issues/spring09/iec61850.pdf

Acknowledgements

This research was performed under an appointment to the U.S. Department of Homeland Security (DHS) Science & Technology (S&T) Directorate Office of University Programs Summer Research Team Program for Minority Serving Institutions, administered by the Oak Ridge Institute for Science and Education (ORISE) through an interagency agreement between the U.S. Department of Energy (DOE) and DHS. ORISE is managed by ORAU under DOE contract number DE-SC0014664. All opinions expressed in this paper are the author's and do not necessarily reflect the policies and views of DHS, DOE or ORAU/ORISE.

ILLINOIS