SCHOOL OF INFOCOMM

Penetration Testing on a Secure Smart Home Metering System

Project Overview

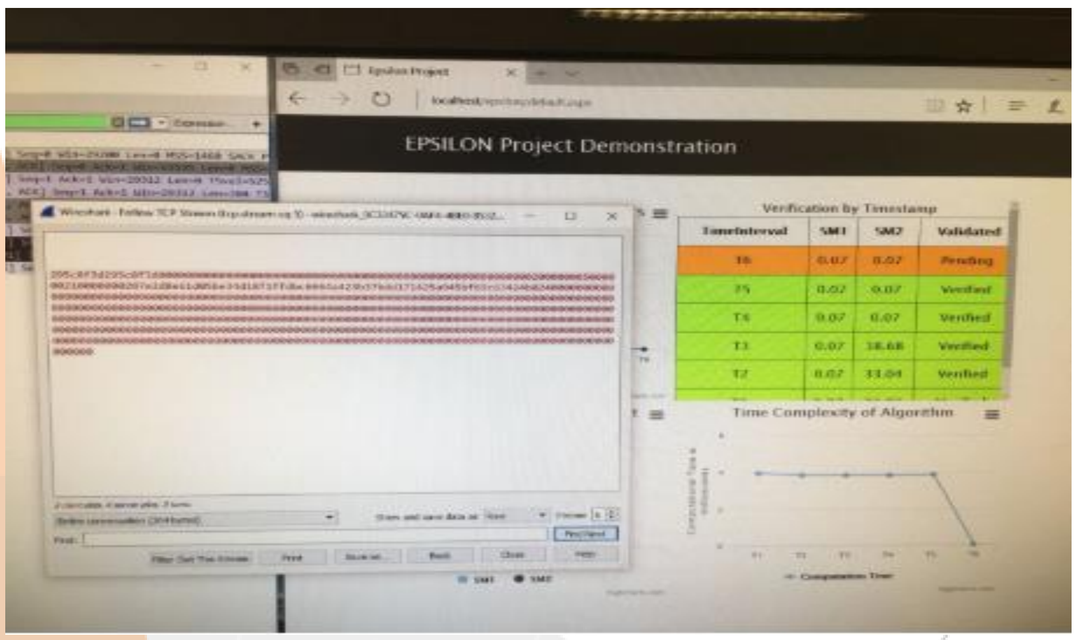
Problem: Conduct penetration testing on the Secure IoT Smart Home Metering System. Derive solutions to harden the system.

Requirements: Understanding the setup of the Advanced Metering Infrastructure (AMI) and the Wireless Smart Utility Network (Wi-SUN). This project also requires the use of penetration testing methodologies and techniques to conduct various network attacks on the smart home metering system.

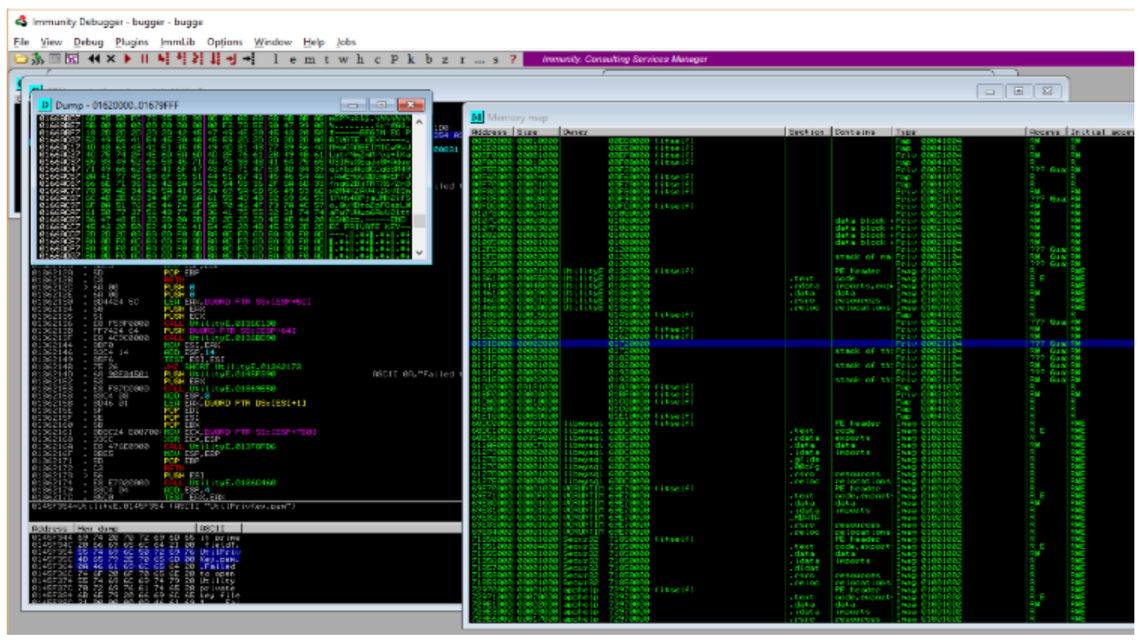
Solution: A security assessment on the prototype setup along with working exploits and recommendations on ways to harden the smart home metering system. The security assessment report consists of project findings, such as working exploits and the proof of concepts that can be used against the current smart home metering system.

Technologies: Windows, Linux, MySQL, Raspbian, Wi-SUN, AMI.

Outcome: Team discovered three critical security vulnerabilities that need to be fixed urgently. These vulnerabilities are falsifying data, MDMS private key leakage and hash replay attack through packet manipulation. They permit the attacker to submit fraudulent utility readings to the backend MDMS.

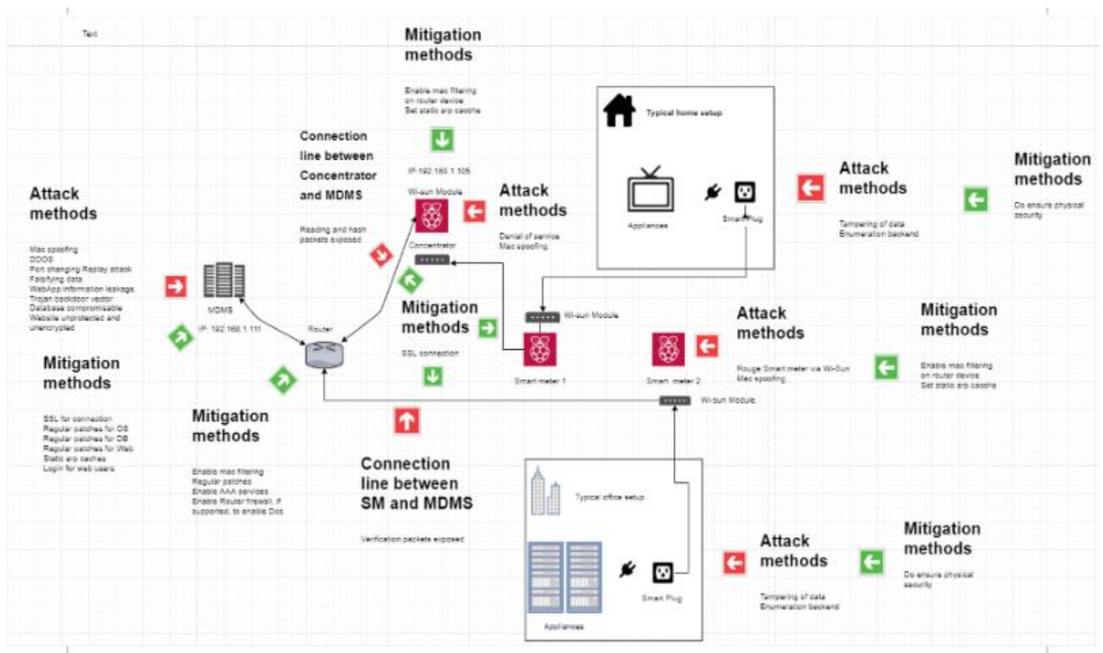


False data is getting verified by the system



Extracting out the private key

Team Members
Johnny Pan, Ryan Yu, Yee Loon
Mr David Leong (supervisor)



Attack Diagram

REPUBLIC POLYTECHNIC
DISCOVER. TRANSFORM. ACHIEVE