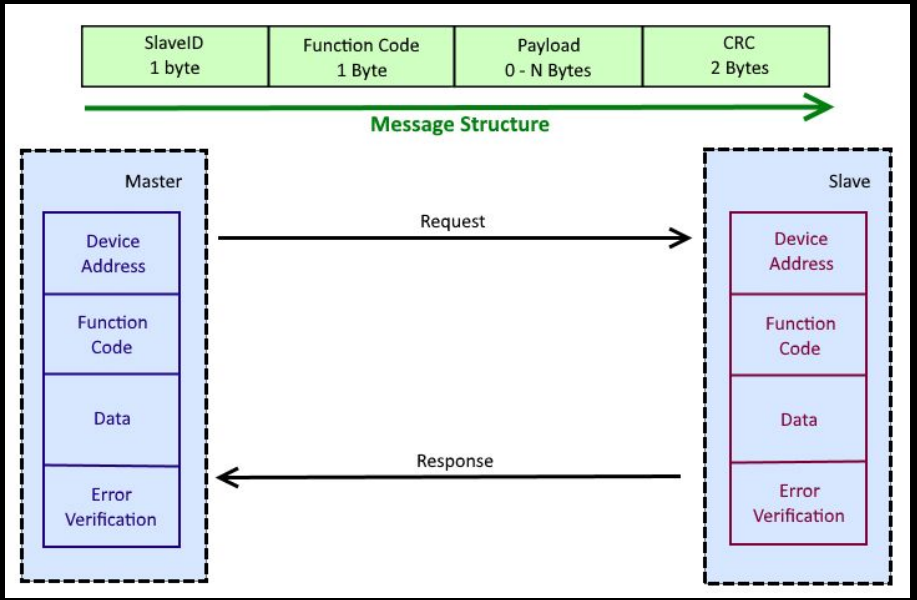
Modware: Secure Modbus Communication For Devices Without Complex Networking Stacks

Christopher Tremblay <cst1465@rit.edu>
Mohammad Eshan <me3031@rit.edu>

What is Modbus?

- Communication Protocol
- Connects Industrial Devices
- Master-Slave Architecture
- Developed in 1979



Why Secure Modbus?

- Developed in 1979
  - Security wasn't invented back then
- "Don't speak unless spoken to" protocol
- Susceptible to MITM, gratuitous server requests, etc
  - Ask me about my Capstone Project
- Some devices don't have complex networks stacks

What has already been done?

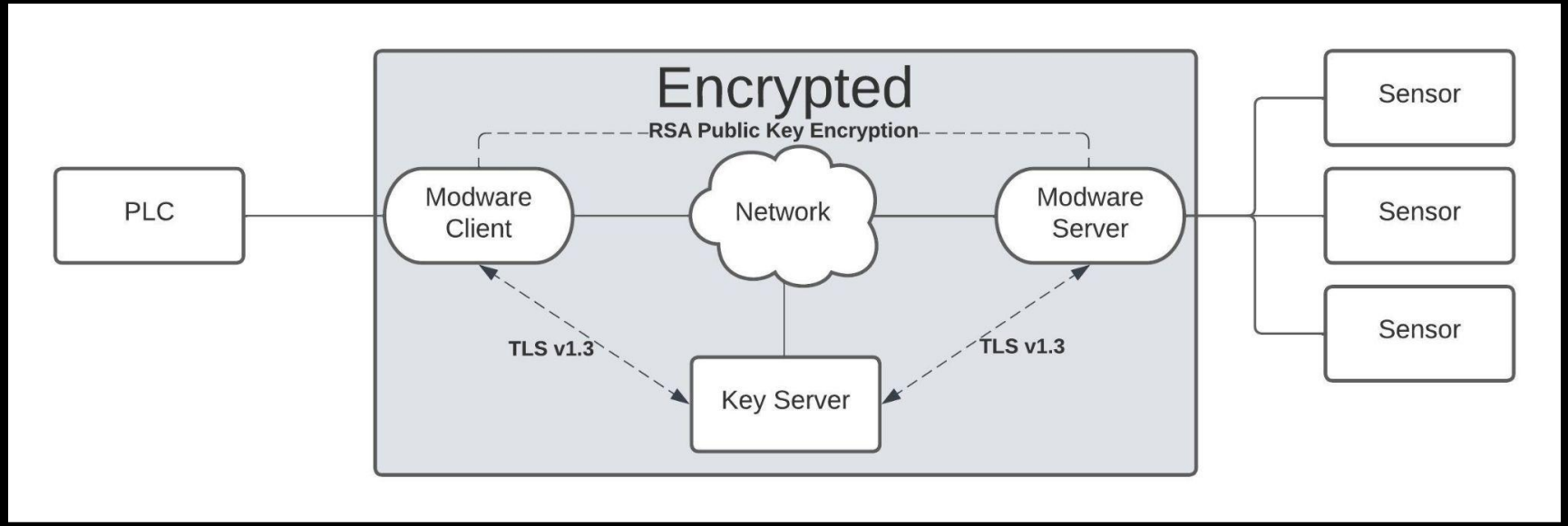
- Inherently Insecure
- Security Add-ons and Extensions
  - Modbus/TCP Security (IEC 62443)
  - Secure Authentication (RFC 6347)
- Encapsulation in Secure Protocols
  - VPNs, TLS, IPsec
- Network Segmentation and Firewalls

Why our solution?

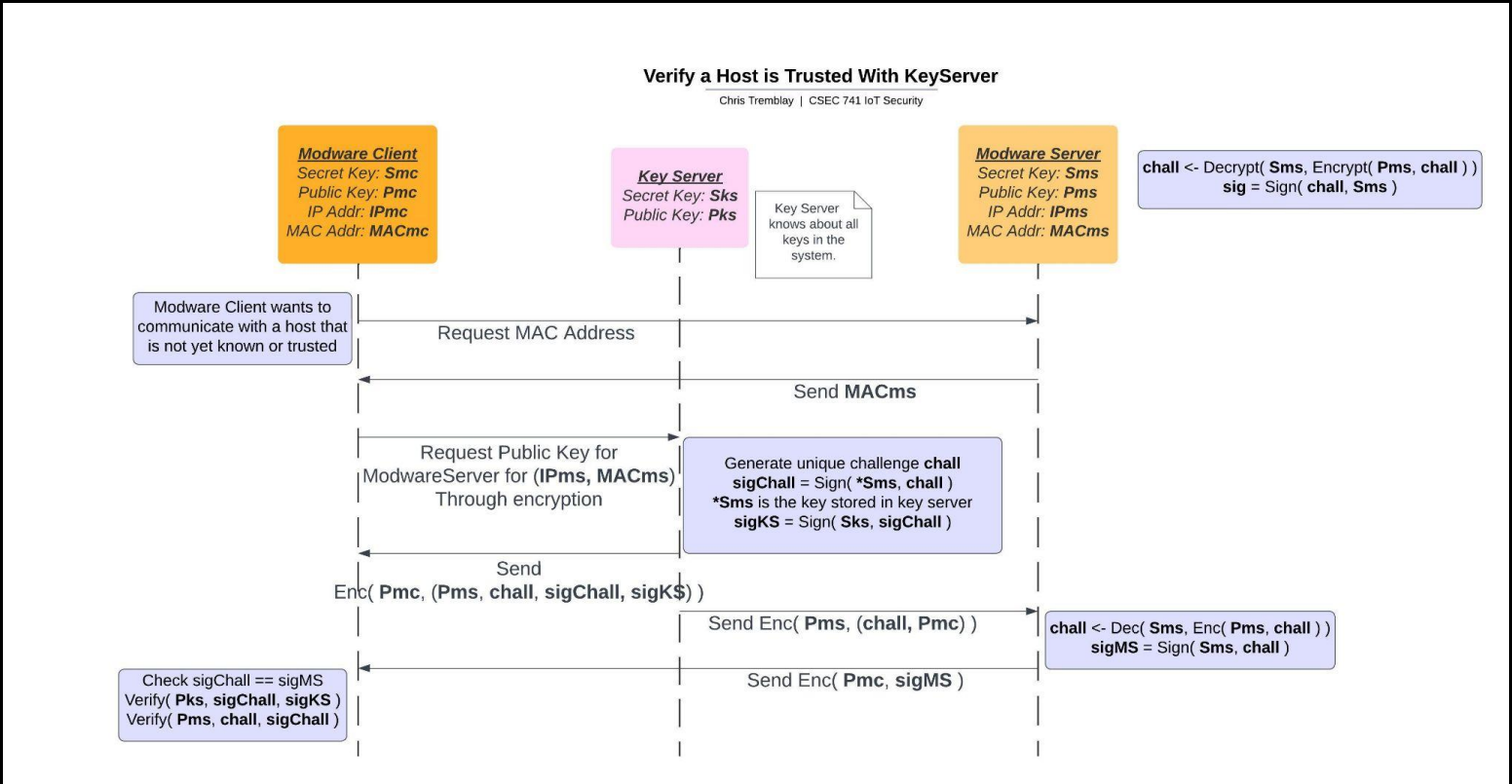
- Support for legacy hardware
- Minimal Integration with existing architecture
- Confidentiality, Integrity, and Non-Repudiation

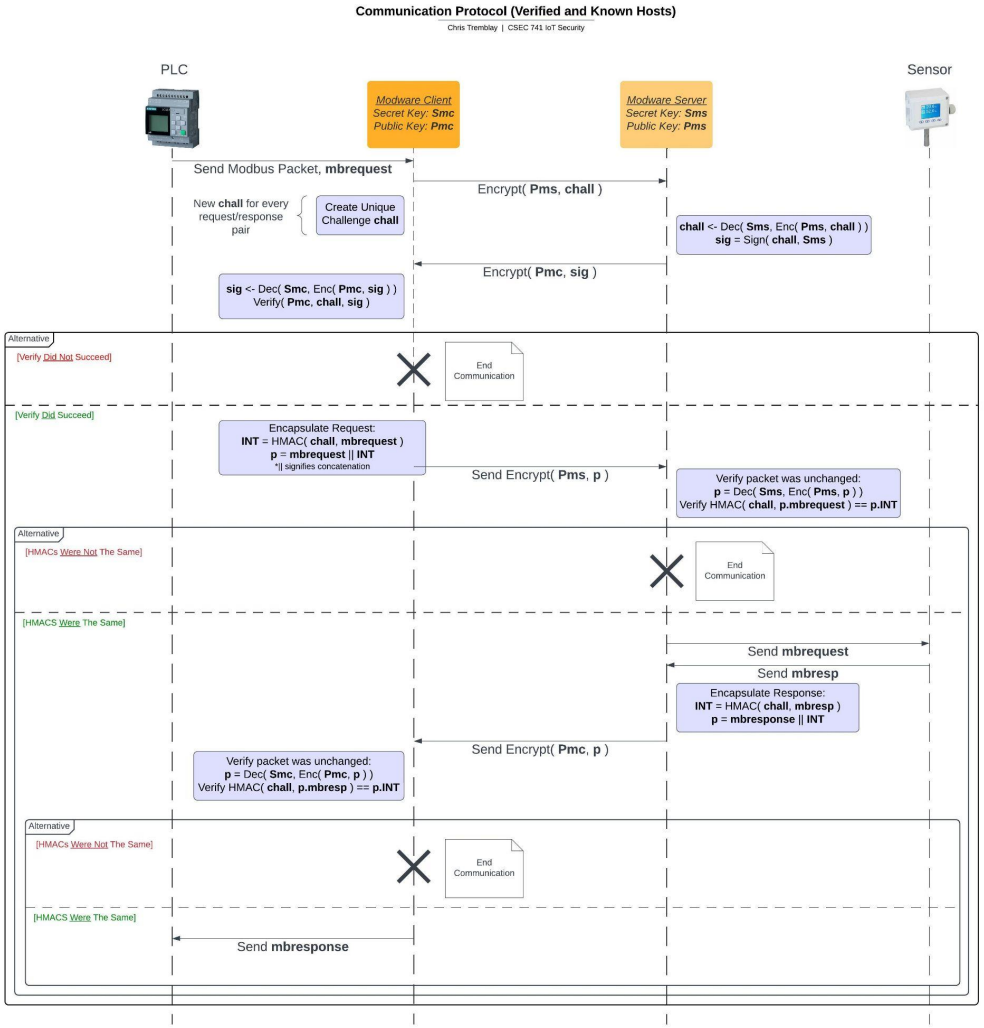
Basic Architecture

Middleware inline after client devices, and before server devices



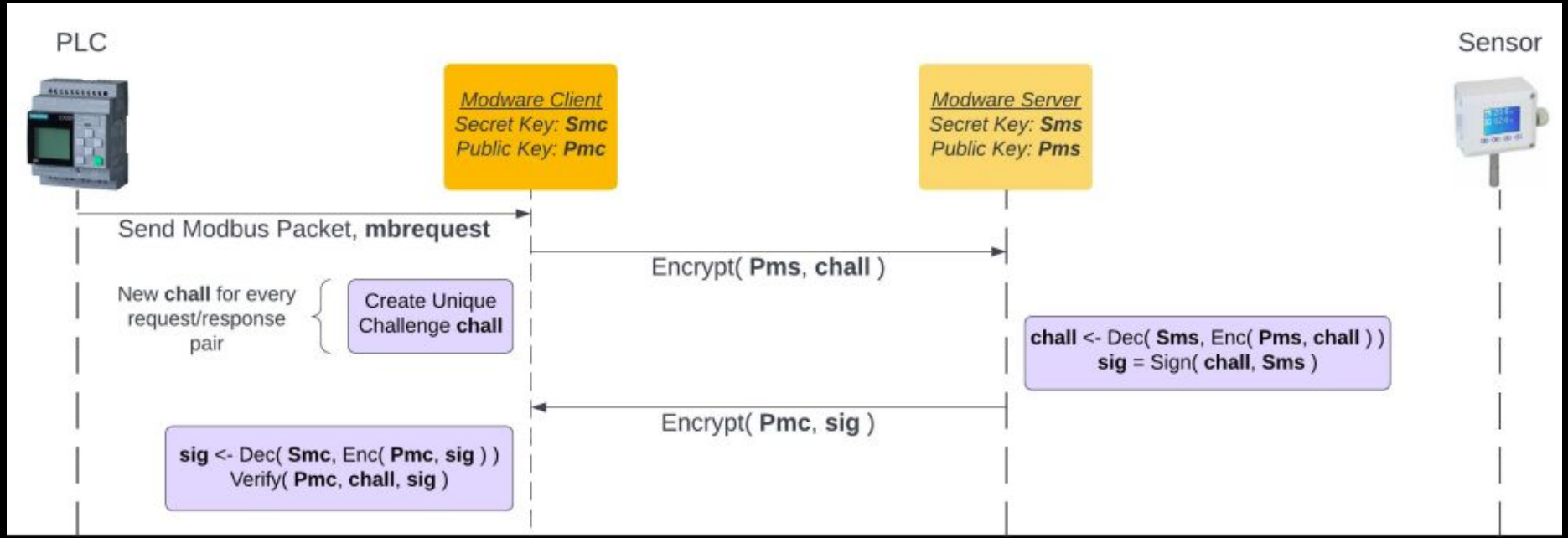
Verify Server Identity Before Communication



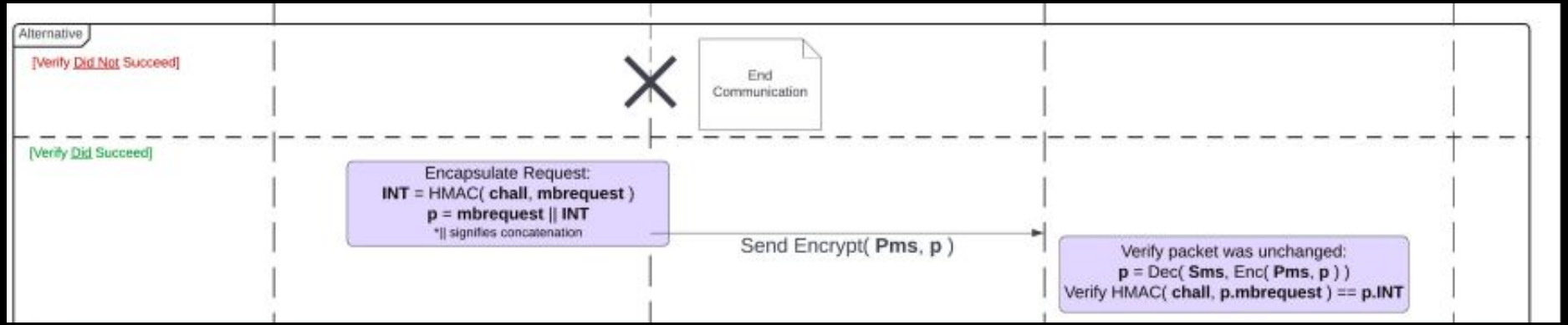


Communication Between Verified Hosts

Send Server a Challenge For Liveliness

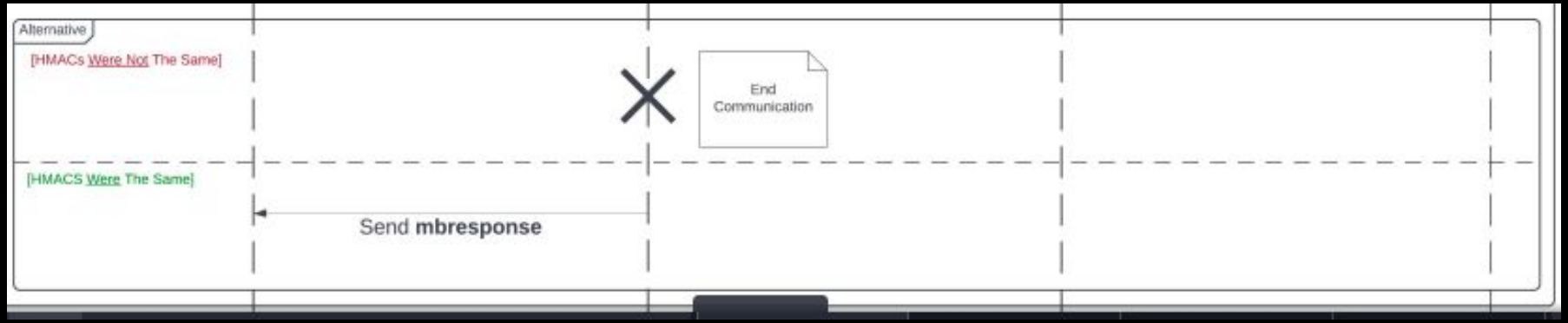


If Server Passes Challenge, Then Send Packet



De-Encapsulate Request → Encapsulate Response

De-Encapsulate Response



References

- What is Modbus and How does it work
- Research and Implementation of Modbus TCP Security Enhancement Protocol
- ISA/IEC 62443 and RFC 6347
- I. Modbus Organization, “Mb-tcp-security-v21 2018-07-24.pdf,” Jul 2018.
- W. Jingran, L. Mingzhe, X. Aidong, H. Bo, H. Xiaojia, and Z. Xiufang, “Research and implementation of secure industrial communication protocols,” in 2020 IEEE International Conference on Artificial Intelligence and Information Systems (ICAIIS), p. 314–317, Mar 2020.
- T. Martins and S. V. G. Oliveira, “Enhanced modbus/tcp security protocol: Authentication and authorization functions supported,” Sensors, vol. 22, p. 8024, Oct 2022.
- I. N. Fovino, A. Carcano, M. Masera, and A. Trombetta, “Design and implementation of a secure modbus protocol,” in Critical Infrastructure Protection III (C. Palmer and S. Shenoi, eds.), IFIP Advances in Information and Communication Technology, (Berlin, Heidelberg), p. 83–96, Springer, 2009dis

Thank you!