SAND2019-2180C

Cryptography Considerations for Distributed Energy Resource Systems

PRESENTED BY

Christine Lai*

Patricia Cordeiro*, Adarsh Hasandka†, Nicholas Jacobs*, Shamina Hossain-McKenzie*, Deepu Jose*, Danish Saleem†, Maurice Martin†

*Sandia National Laboratories, †National Renewable Energy Laboratory

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Summary

- DER Security Considerations
- Review of DER Cryptography
- Case Study 1: Hardware Design Considerations
- Case Study 2: Performance Testing
- Takeaways and Conclusions

DER Security Trends

DER systems represent a growing portion of generation

- Devices are being built with grid-support functions and network communications capabilities
- IEEE 1547 mandates new interconnection and interoperability standards which include support for remote access

Emergence of malware frameworks targeting ICS

- Triton
- BlackEnergy/GreyEnergy
- CrashOverride/Industroyer

DER Security Challenges

Challenges to be addressed:

- Compatibility
  - Embedded hardware
  - Protocols: DNP3, Modbus, etc.
- Performance impacts
- PKI still under development

Review of Symmetric Encryption

Symmetric Ciphers:

- Advanced Encryption Standard (AES)
- Salsa/ChaCha20

Block Cipher Modes:

- Electronic codebook (ECB)
- Cipher block chaining (CBC)
- Counter mode (CTR)
- Counter with cipher block chaining message authentication code (CCM)
- Galois/counter mode (GCM)

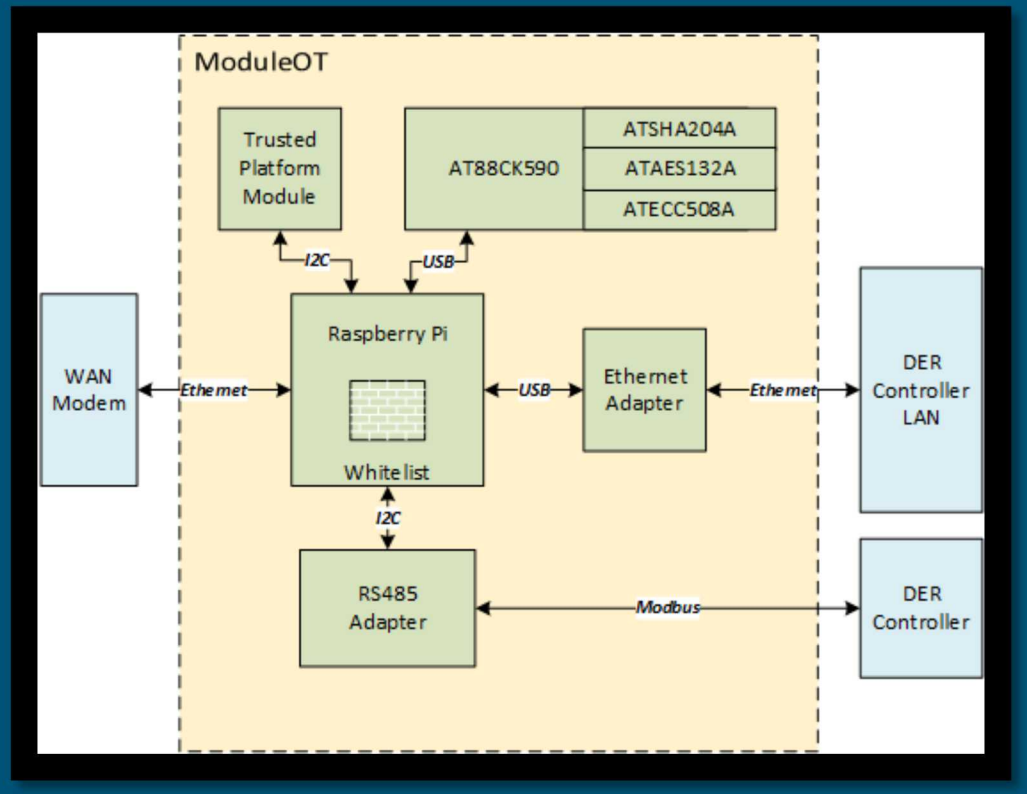
Current Standards for DER Cryptography

IEEE 2030.5 / CA Rule 21

Cryptographic guidelines on track to become standard for DER

- HTTP over TLSv1.2m
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 cipher suite with secp256r1 elliptic curve
- X.509v3 device certificate that chains to the Root-CA
  - SHA256 certificate hash
  - 160-bit Long-Form Device Identifier (LFDI)
  - 11-digit decimal plus 1-digit checksum Short-Form Device Identifier (SFDI)
- PKI authentication
- LFDI for authorization
- Server ACL

Case Study 1: Cryptographic Hardware Design



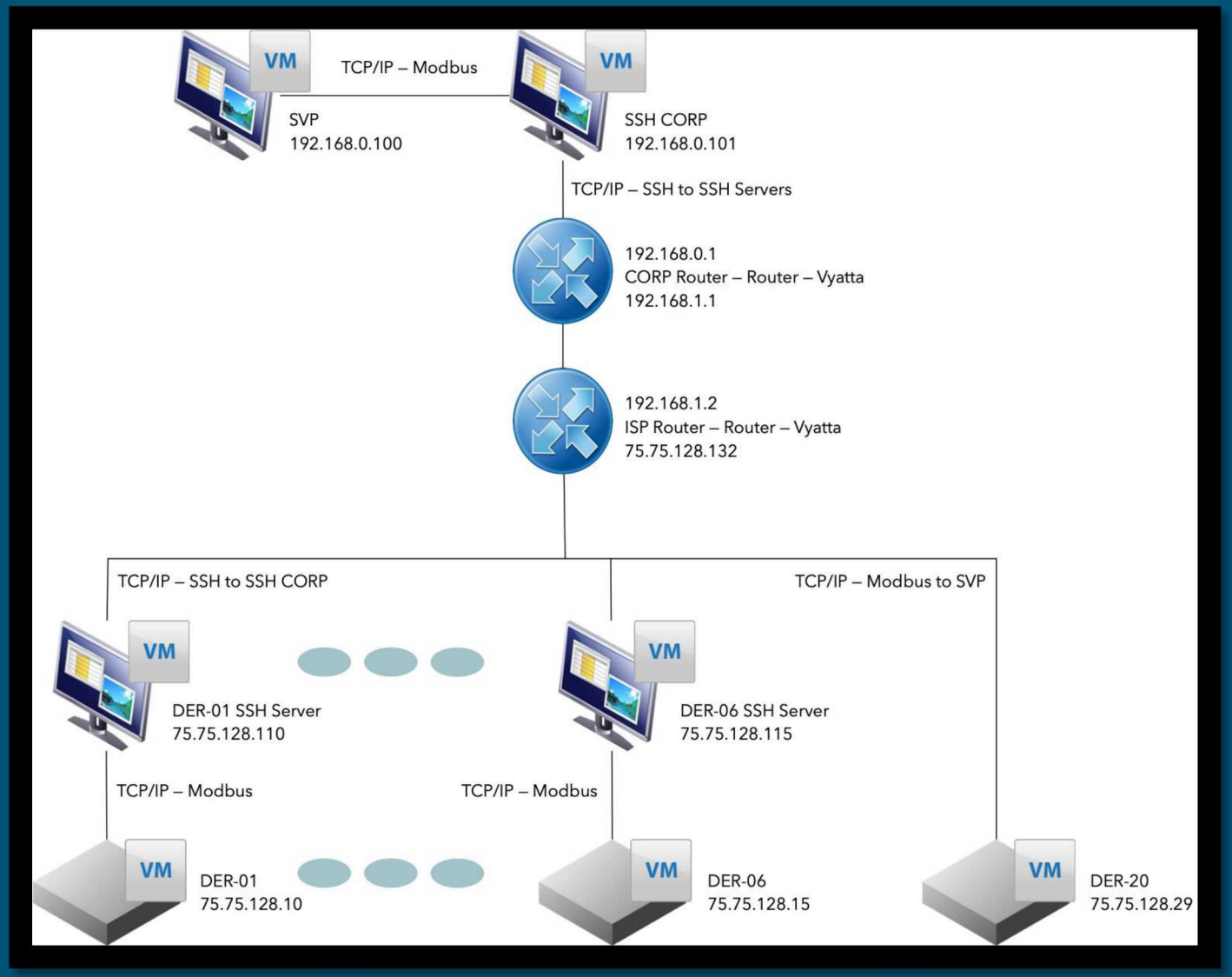
Security Principles:

- Defense in Depth
- Least Privilege
  - Modularity
  - Resource Management
  - Access Control
- Anti-Tamper
  - Dedicated hardware
  - Immutability

Case Study 2: Encryption Performance Testing

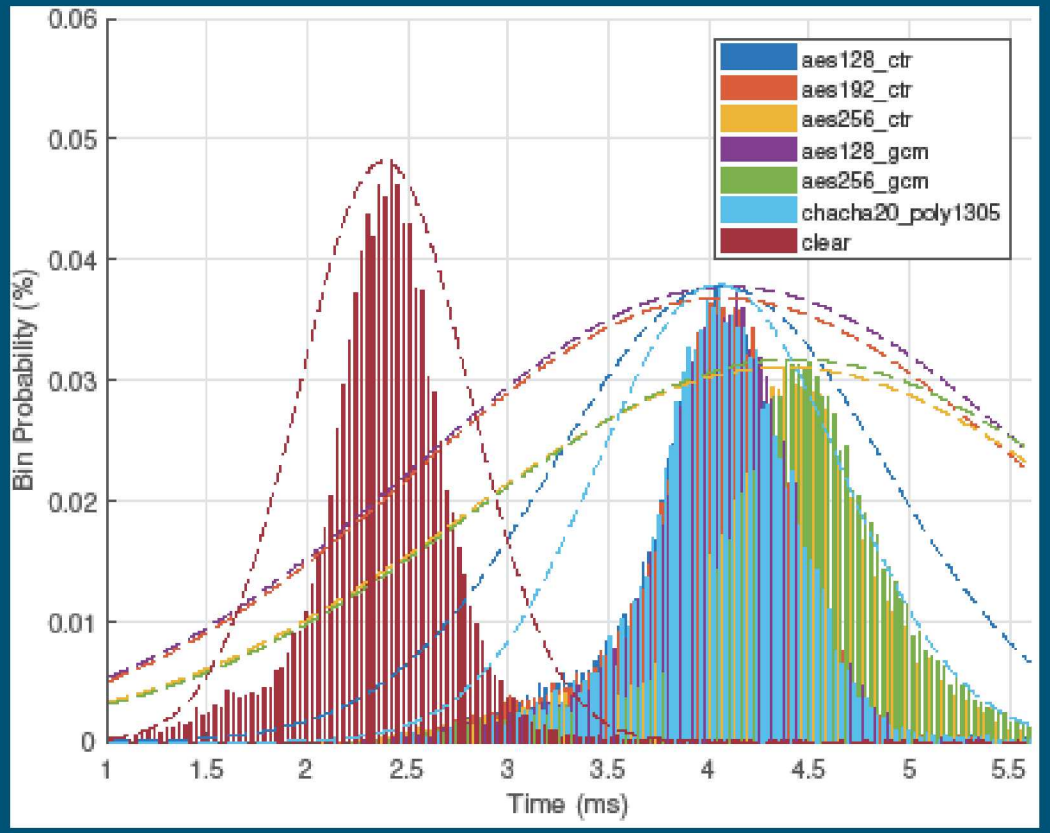
Emulation Topology:

- 20 distributed inverters
  - 6 ciphers tested with SSH encryption tunnels
  - unencrypted baseline
- HMI/controller on utility network



Case Study 2: Encryption Performance Testing

Case	Mean Latency (ms)	Jitter (ms)
AES128-CTR	4.0526	0.4086
AES192-CTR	4.0662	0.4127
AES256-CTR	4.3728	0.5278
AES128-GCM	4.1056	0.4255
AES256-GCM	4.4290	0.5333
ChaCha20-Poly1305	4.0496	0.3852
Unencrypted	2.3834	0.3358



Takeaways and Conclusions

Encryption will need to be implemented in DER systems to meet security requirements

Cryptographic hardware design needs to meet specific challenges for DER

Performance testing shows that encryption is feasible for inverter communications

- However, latency may become a limiting factor if encryption is applied to other devices or if DERs take up more grid-support functions