SAND2018-7549C

Introduction to Cryptography: Considerations for DER Systems

SAND #829970

PRESENTED BY
Christine Lai

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.

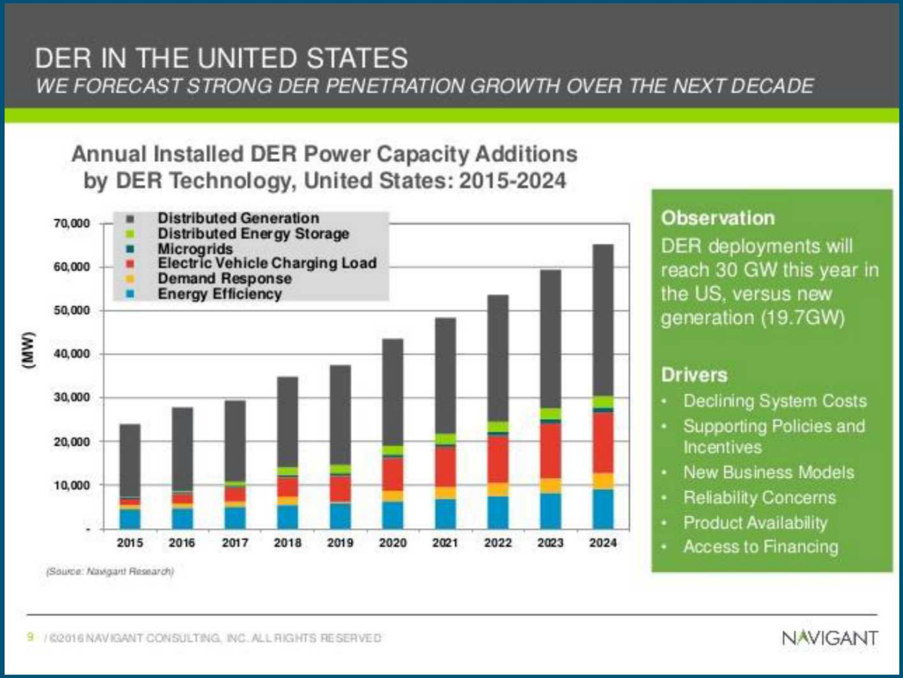
Introduction
Emerging Cybersecurity Concerns for DER

Penetration of DERs is increasing in the grid; this enables and motivates the addition of grid-support capabilities

- IEEE Std. 1547 mandates new interconnection and interoperability standards to achieve these capabilities and allow remote users to change behaviors of many devices

Recent cyber attacks exploit ICS protocols shared by DER and bulk power systems

- The IEC 61850 communications standard is specifically targeted by the CrashOverride framework used in malicious attacks on the Ukrainian grid*



*https://www.us-cert.gov/ncas/alerts/TA17-163A
Image credit: Navigant Consulting, INC., 2016

What is Cryptography?

Cryptography is used for securing communications in the presence of adversaries

- Historically, cryptography referred to encryption and decryption – the process of translating plaintext into ciphertext and vice versa

Modern crypto systems have many components:

- Encryption algorithms – symmetric and asymmetric
- Authentication protocol
- Identity management system
- Key exchange protocol
- Key management system
- Signing algorithm
- Public key infrastructure

All of these are needed to have strong cryptography!

Image credit: https://en.wikipedia.org/wiki/Scytale

Introduction to Cryptography: Algorithms and Protocols

Symmetric cryptographic algorithms

- Advanced Encryption Standard (AES), standardized in NIST FIPS 197
- Data Encryption Standard (DES, 3-DES), insecure but still used
- Many others for lightweight crypto, e.g., Blowfish, TEA (tiny encryption algorithm), etc. – but all have tradeoffs
- 128- or 256-bit keys are common for symmetric encryption

Asymmetric cryptographic algorithms, typically based on large prime factorization or discrete logarithms:

- Rivest–Shamir–Adleman (RSA), invented in 1978 and still used today
- Elliptic-Curve Cryptography (ECC), NIST FIPS 186-3, replacing RSA because smaller key sizes offer faster processing
- Longer keys are typically required for asymmetric algorithms (e.g. 1024- or 2048-bit for RSA, 256- or 384-bit for ECC)

Hash functions

- Secure Hash Algorithm (SHA-1, SHA-2, SHA-3), standardized in NIST FIPS 180
- Message Digest 5 (MD5), insecure but still used

Public-key cryptography

- Diffie–Hellman key exchange
- Public Key Infrastructure (PKI)

Introduction to Cryptography: Common Pitfalls

"We use 256-bit AES encryption"

- What is being encrypted?
- Offers no inherent security without proper key management, authorization, etc.

"The target area is only two meters wide. It's a small thermal exhaust port, right below the main port. The shaft leads directly to the reactor system."

- System designers are often poor judges for the vulnerabilities in their systems

Weaknesses in modern crypto systems:

- Encryption algorithms are designed to be safe against current computing capabilities – logical flaws are rarely exploited without advancements in computing
- Vulnerabilities are typically introduced through flaws in implementation
- Systems should be protected evenly and within reason against your threat

— Don't install steel doors on a straw hut but do install them on your bank vault

DER Security Standards
California Rule 21 Security Requirements

Use of security is mandatory for communications between utility servers and clients and is within the utilities' domain of responsibility:

- HTTP over TLSv1.2m
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 cipher suite with secp256r1 elliptic curve
- X.508v3 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

What are the implications?

- All components should be implemented to ensure system security
- Implied requirements: DER vendors must secure their private keys and install them on devices at time of manufacture