powersecurity

Доверие в новом мире IoT

Корабельников Николай

Вопросы безопасности

- С одной стороны - бурное развитие Internet of Things. С другой – это не что-то принципиально новое.
- Вопросы безопасности:
  - Защита трафика
  - Аутентификация устройств
  - Аутентификация пользователей
  - Защита firmware

Защита сети

- «Умные вещи» бывают разными. Это могут быть как полнофункциональные, так и сенсоры с ограниченным энергетическим и производительным ресурсом.

HTTP => CoAP

TLS/TCP => DTLS/UDP

IP => 6LoWPAN

Ассиметричная криптография

- Шифрование трафика
- Односторонняя и взаимная аутентификация
- Firmware Code Signing

Public Key Infrastructure

- Управление жизненным циклом сертификатов
- HSM
- Simple Certificate Enrollment Protocol (SCEP)
- Elliptic Curve Cryptography (ECC):

  224ECDSA⇔2048RSA
- OCSP

Аутентификация

- X.509
- Ассиметричные ключи без сертификатов
- Симметричные ключи
- OAuth2

powersecurity

Спасибо за внимание!

Корабельников Николай

korabelnikov@powersecurity.ru