Security Challenges for the Internet of Things

Tim Polk

Sean Turner

March 25, 2011

Mandatory to Implement Security

- Security solutions should be mandatory to implement, but optional to use
  - While initial deployments will surely turn security off, experience with WEP implies that attacks exploiting such configurations will follow closely
  - Including security support will allow early adopters to respond appropriately

Suitable Cryptographic Algorithms

- “Conventional” cryptographic algorithms assume significant resources (memory, CPU)
  - Some current algorithms seem plausible
    - AES-GCM provides auth & enc
    - ECC has smaller footprint than RSA, DSA, D-H
    - Wait and see for SHA-3
- If these algorithms are too demanding, new algorithms need to be developed
  - Critical that we require at least 112 bits security strength, since attacker is not resource constrained

Automated Key Management & Credentialing

- Automated key management is always harder than the cryptographic primitives
  - And the weak link is usually credentialing
- Pre-shared keys aren’t a realistic option
  - The sheer number of devices in the IoT demands automated key management
- Need to consider Usability
- May need to be innovative
  - Consider Leap-of-Faith, or pairing protocols, to efficiently introduce new devices

Meeting Privacy Expectations

- Build in privacy protection from the beginning
- Experiences with Smart Grid show that privacy concerns can seriously impede deployment
  - Exposing power consumption patterns for homes and businesses violates expectations of privacy
  - The IoT has the potential to expose our activities with greater precision

Summary

- Build security in, even if performance suffers when enabled
- Insist on 112+ bits of security in crypto algs
  - Build in crypt agility in case better algs emerge
- Automated Key Management is essential
  - Usable credential management is the challenge
- Respect privacy concerns
  - Essential to acceptance of IoT technology