Challenges of Using Cryptography in IoT

Lily Chen, NIST

February 6, 2018

Discussion Topics

- Can “lightweight cryptography” solve all IoT security problems?
- How to manage cryptographic keys in a network which tethers heterogeneous “things”?

Security Challenges for Internet of Things

- IoT connects massive heterogenous devices together from very constrained sensors to powerful servers
- Security challenges are due to the following factors
  - Some devices have limited capacity and constrained environment for some device – lightweight cryptography is needed
  - Some devices are physically vulnerable and have a short lifetime – authentication and identification can be problems
  - Asymmetric two ends, powerful and constrained, for a communication channel – key establishment using IKE or TLS can be a challenge

Lightweight Cryptography* - General

- Cryptography that aims to provide crypto solutions for constrained environments
- Lightweight cryptography does not mean weak crypto
- Security properties may be different than those desired for general use, but must be sufficient for the target application
- Lightweight crypto may
  - be less robust against sophisticated cryptanalysis
  - Vulnerable to dictionary attacks
  - be less misuse resistant
  - have fewer features

* Here we focus on symmetric key algorithms for lightweight cryptography

Lightweight Cryptography* – Design Ideas and Implications

- Design Strategies
  - Many iterations of simple rounds, simple operations (e.g., XORs, rotation, 4x4 Sboxes, bit permutations)
  - Smaller block/key sizes, smaller security margins by design
  - Simpler key schedules
- Implications
  - Less robust against sophisticated cryptanalysis with lower data complexity
  - Vulnerable to dictionary attacks
  - Enable attacks using related key, weak key, known key or even choose key
- Counter measures
  - Change key more frequently
  - Use good random number generator to generate keys
  - Even lightweight, do not use shorter than 128 bits

* Here we focus on symmetric key algorithms for lightweight cryptography

Lightweight Cryptography - Standards

- ISO/IEC SC 27 has developed a series of lightweight cryptography standards in 20192 series, including block cipher, stream cipher, hash function, message authentication code and asymmetric key cryptography schemes
- NIST Lightweight Cryptography Project
  - Engage with industry and academic on lightweight crypto
    - Two workshops in 2015 and 2016
  - Publish NISTIR 8114 in March 2017
    - Overview lightweight crypto
    - Design consideration and profiles
  - Release Profile white paper April 2017
    - Prole I Authenticated Encryption with associated data (AEAD) and hashing for constrained software and hardware environments
    - Prole II AEAD for constrained hardware environments
  - Planning to release draft call for proposals in 2018 – Industry involvement is very critical

Security of Using Lightweight Cryptography in IoT

- IoT consists of not only resource constrained devices, e.g. sensors, but also powerful processing platform which transforms groups of raw data into intermediate, aggregated data
  - Use lightweight cryptography to protect the interface only when constrained devices are involved
  - Obtain good estimation on data rate to set a limit for how long a key can be used
- The attackers to the IoT may not be constrained
  - Use randomly generated “full length” key to be secure against exhaustive search attack
  - Change keys frequently to limit the available data, e.g. plaintext and ciphertext pairs, useful for cryptanalysis
- The attacking objective may not be to obtain confidential information from an individual device but a collective of data from massive devices
  - Strong protection on data processing platform is critical and deserves ‘heavy duty” treatment

Key Management for Heterogeneous "Things"

- For an individual "thing", when considering cryptography usage to protect platform and interface, consider
  - Whether it can run a complex key exchange protocol, like IKE and TLS
  - Whether it can execute "over-the-air" provision and how secure the mechanism is
  - Whether it has a user interface for manual configuration of keys and how to share, protect, and update the key
- For a communication channel between "two things", consider algorithm agility, check whether they can securely
  - Negotiate algorithms to prevent downgrade attack
  - Update keys to barrier cryptanalysis
- For short-life device, when key update is not possible, the data to be protected in the lifetime shall not exceed the limit for a given key
  - Otherwise the data can be compromised
- For very low-end "things", if it is infeasible to use cryptography at all,
  - Block massive attacks, like DDoS, and limit the leakage
  - Focus on reliability of the statistics results of massive data

Lessons Learned – WEP to DUHK

- **Wired Equivalent Privacy** (**WEP**) has been included in the textbook for security in communications as an example how security can be failed
- WEP was failed for many reasons, one of them is not able to facilitate key update
  - With the same key and 24 bits of IV, it will take 5 seconds for IV collision to happen
  - WEP does not provide message authentication
  - The challenge response authentication reveals the key stream
  - As a result, a 104-bit WEB key can be recovered in 60 seconds
- **Don't Use Hard-coded Keys (DUHK)** is a strong message sent through an attack
  - Use a weak random number generator specified in X9.17 which is broken in 1997
  - The attacker reverse-engineers a firmware image and extracts the hard-coded key
  - The key is the only source to generate “random” private keys
  - By discovering status, the traffic from any VPN using FortiOS 4.3.0 to FortiOS 4.3.18 can be decrypted

Take-home messages

- Lightweight cryptography cannot solve all the security problems in IoT
- Use lightweight cryptography only when constrained devices are involved
- Any weakness in key management can lead to catastrophic failures
- The key point for IoT is to prevent damages from spreading when attacks happen

Questions and Discussions

References

1. McKay, K. et. al. NIST Internal Report (NISTIR) "*Report on Lightweight Cryptography*" March 2017
2. Voas J. NIST Special Publication 800-183 "*Network of Things*" July 2016