# Secure IoT Bootstrapping: A Survey

draft-sarikaya-t2trg-sbootstrapping-00

Behcet Sarikaya, Yizhou Li,
Mohit Sethi, Robert Cragie

# Secure Bootstrapping

- What is bootstrapping and what is security bootstrapping?
  - Many definitions out there
- "it is the process by which a thing/device/smart object in an IoT network securely becomes operational at a given location and point of time."
- Secure bootstrapping vs. Secure authentication
- This definition is broad on purpose since the term IoT itself represents a very diverse spectrum of applications
  - pairing of phones over bluetooth to exchange files, and
  - securely connecting IEEE 802.15.4 sensors factory to the backend both require some form of secure bootstrapping

# Secure Bootstrapping

- Centralized/AAA/Managed
  - Extensible Authentication Protocol (EAP)
  - Generic Bootstrapping Architecture (GBA)
  - Open Mobile Alliance (OMA) Light-weight M2M:
    - Factory Bootstrap
    - Bootstrap from Smartcard
    - Client Initiated Bootstrap
    - Server Initiated Bootstrap
  - Kerberos

# Secure Bootstrapping

- P2P/Ad-hoc
  - Typically Diffie-Hellman exchange
  - MiTM prevented with OOB channel
  - Often for setting up ad-hoc associations
  - Example: Pairing phones
    - Key confirmation: A Diffie-Hellman key exchange occurs over the insecure network and the established key is authenticate with the help of the OOB channel.
    - Key derivation: Contextual information received over the OOB channel is used for shared key derivation.

# Secure Bootstrapping

- Miscellaneous
  - Components from both centralized and ad-hoc
  - [I-D.kumar-6lo-selective-bootstrap] presents a selective bootstrapping/commissioning method by introducing the concept of Commissioning Tool (CT)
  - Raw Public Key
  - Categorization is not always easy or clear

# Secure Bootstrapping

- Why?
  - Learn the assumptions
  - Design trade-offs
  - NOT produce a 100 page document
  - Hope to help developers choose what option suits when
  - End-of-life and re-bootstrapping is hard problem: https://www.iab.org/wp-content/IAB-uploads/2016/03/draft-farrell-iotsi-00.txt

Thank you