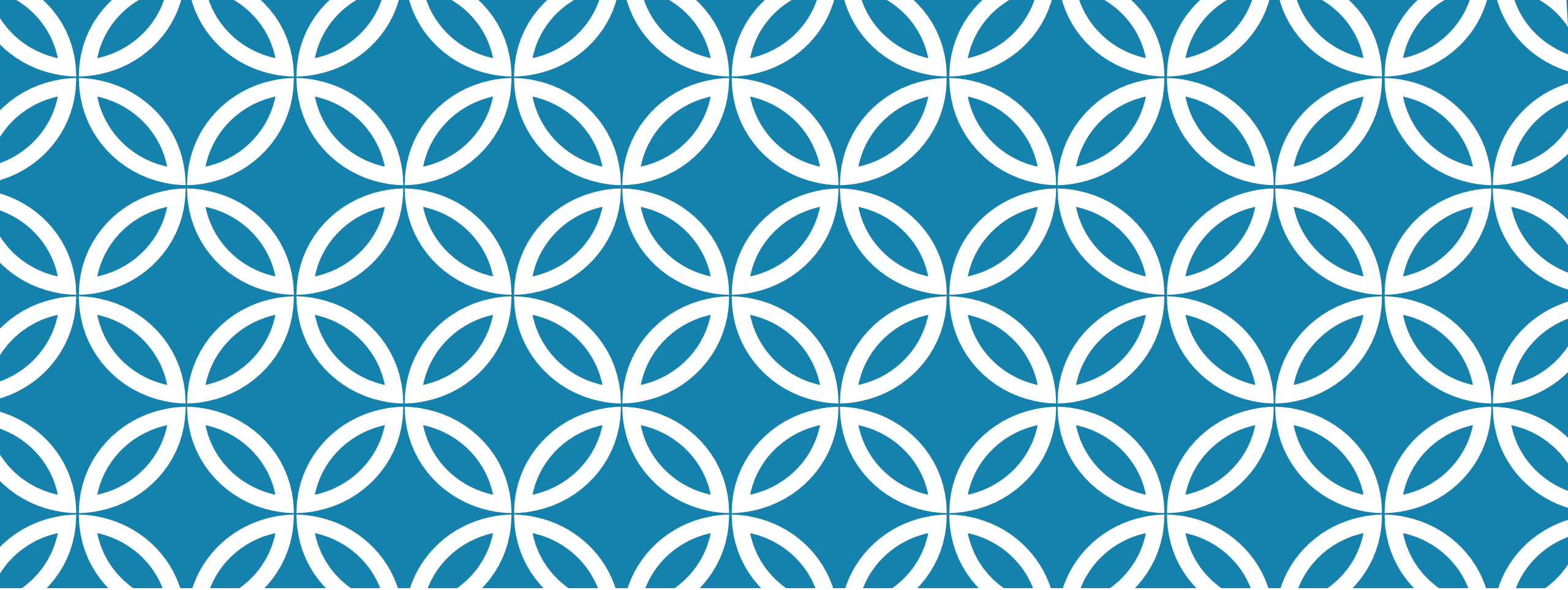


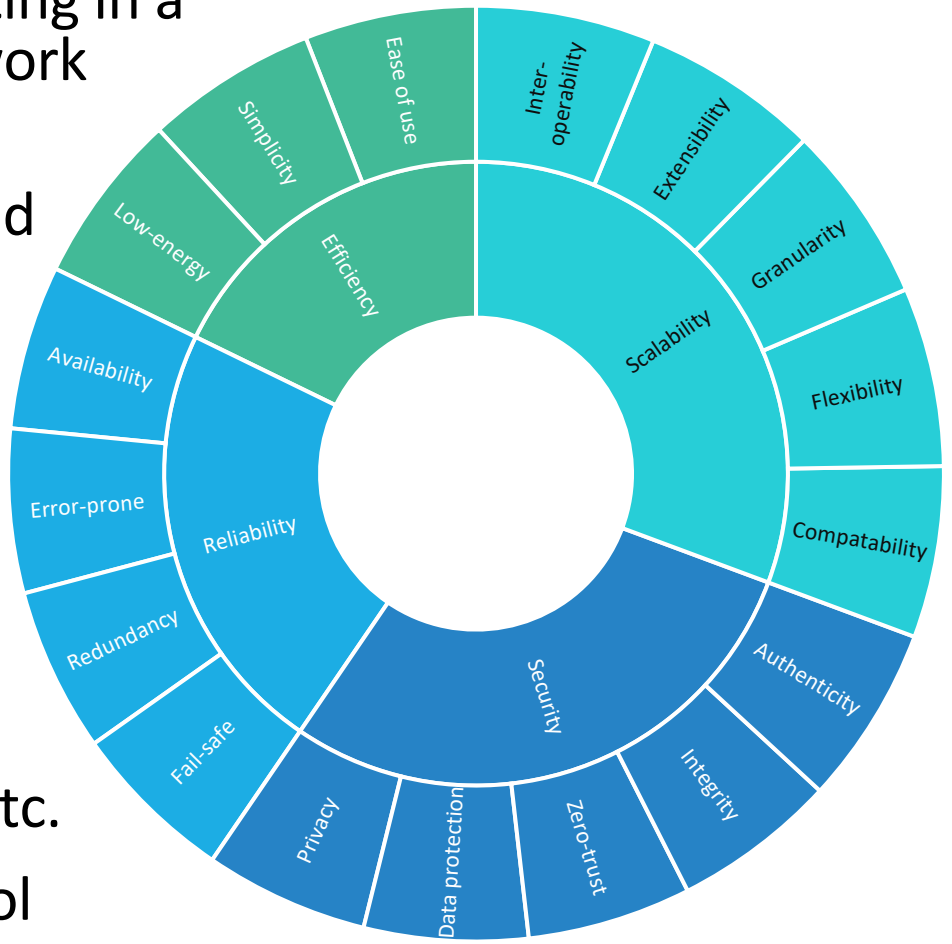
THE NEED FOR NEW AUTHENTICATION METHODS FOR IOT

Dirk v. Hugo, Behcet Sarikaya

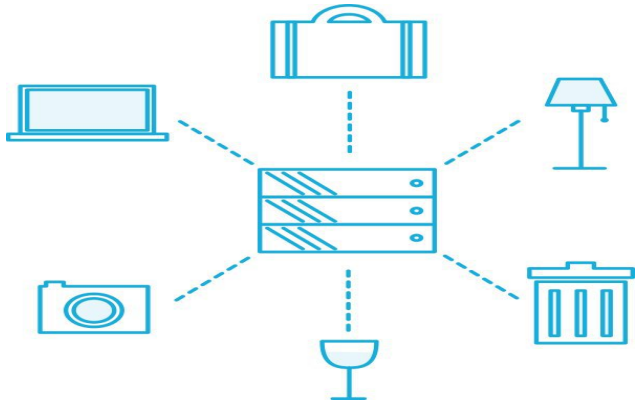
IETF 114 July 2022

Next Generation Type of Communication

- Characterized by diverse applications connecting in a heterogeneous environment in terms of network technologies and devices
- ultra massive (um)IoT may become chance and challenge - basic requirements in dimensions/assessment criteria:
  - Efficiency
  - Reliability
  - Scalability
  - Security
    - Opening risk of DDoS attacks etc.
    - Strong access admission control



Authentication for NG connected things



- Authentication of high-end (platinum) vs. simple cheap (iron) devices: elaborated/refined ‘5G-like’ vs. affordable and convenient
- Authentication models based on human intervention (like 802.1X) not fitting for low-cost IoT in this type of next-gen communication era
- Hardware based authentication via sensing of video/audio or shape/gestures from a device or touch of a person uses out-of-band (OOB) channel

Source: https://www.3gpp.org/ and https://www.ietf.org/topics/iot/

Security Challenges for “dumb” IoT devices

“zero trust security model” (ZTSM) and 2- or multi-factor authentication (2FA/MFA)

- User and device are separated and not physically connected.
- Unique identity for user applying to all own/personalized devices is given.
- Authentication has to work mutually.
- Simple (“dumb”) devices characterized by:
  - No pre-established relation with intended server or user,
  - No pre-provisioned device identifier or authentication credentials,
  - Input or output interface may be capable of only one-directional OOB communication.
  - …

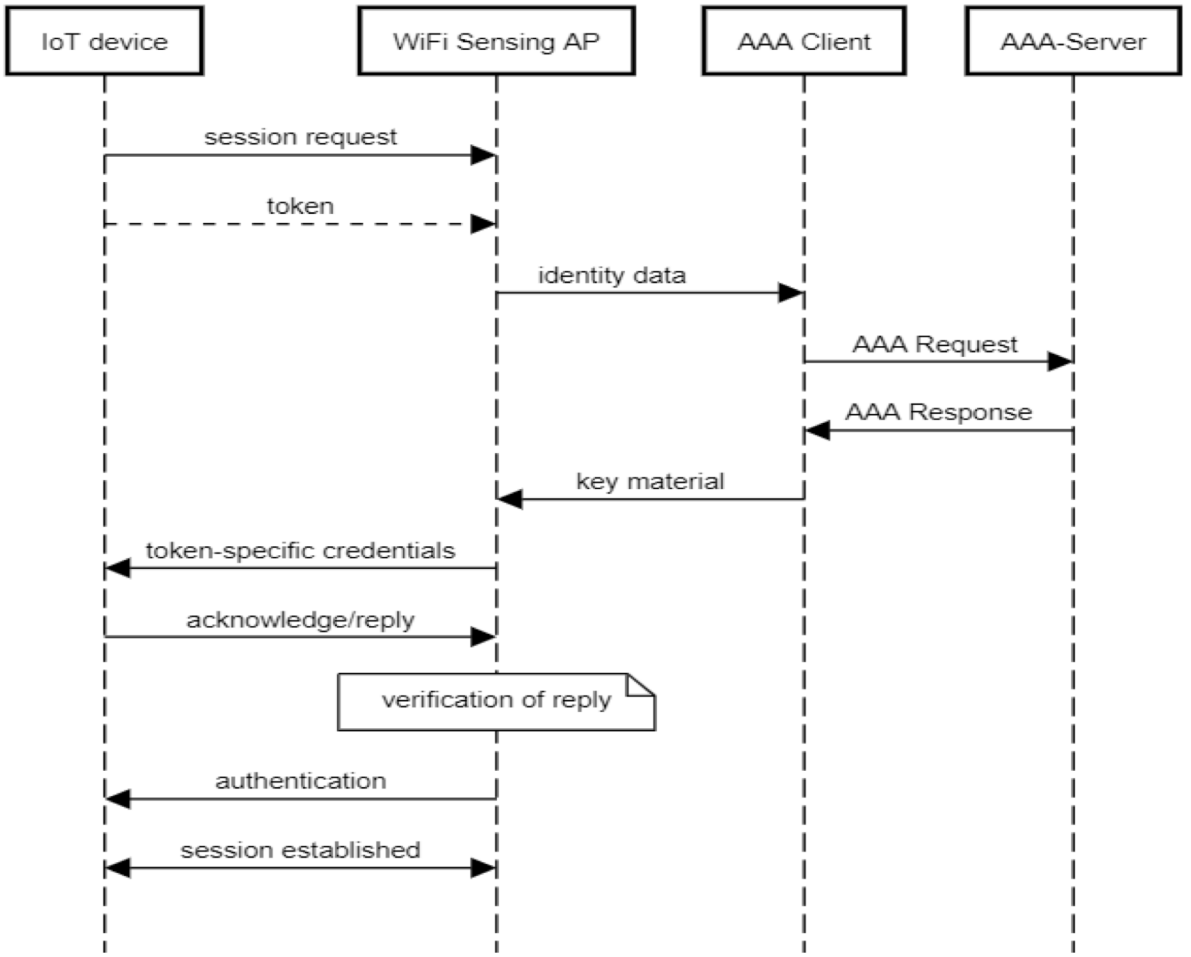
Hardware based admission model

- E.g., for including new devices into a home/personal network:
  - Optical /LED detection
  - Acoustic (speaker/microphone) signal
  - Via another device as smartphone (gyro, geographic data, …)
  - Haptic, …
- All those requiring 2nd interface (main channel and OOB channel) – sensing via same radio tx/rx antenna signal analysis may simplify devices!
- IEEE 802.11bf sensing project provides proper framework for hardware based authentication of Wi-Fi enabled devices
- 3GPP is expected to have a similar project for 5G/6G RAN

Proposed 2FA message exchange

draft-hsothers-iotsens-ps open issues:

- Detailed parameter specification in MSC
- Token regarding pre-defined type of access to device to be generalized (w/o LOS)
- Standard IoT device ID in terms of (geospatial) (re-)naming
- Extension of AP to (L2) mesh / multicast communication
- Possible extension to RFC9140 on Nimble out-of-band (NOOB) authentication for EAP



Key Technologies needed

- Sensing
  - Wi-Fi signals for gesture and motion detection
  - 5G/6G signal can also be used as the two are similar technologies
- AI or Neural Network Models
- make sensing resilient to spoofing and adverse channel conditions, i.e., presence of noise and interference from other technologies
- New work needed OOB channels other than LED light, geo spatial naming for IoT devices, etc.
- With these IoT will be potentially the driving force of 6G?

Next Steps

- Presented our draft “The Need for New Authentication Methods for Internet of Things” discussing the problem statement and potential IETF work:
  - https://www.ietf.org/archive/id/draft-hsothers-iotsens-ps-02.txt
- Improved it much since Rev-00
- Solicit review and comments by WG
- Aiming at WG adoption