Secure Bootstrapping for IoT devices

Mohit Sethi

Ericsson, Finland
Aalto University, Finland

Mohit Sethi

- Experienced Researcher – Ericsson Research
  - January 2012 – Present
- Postdoctoral Researcher – Aalto University
  - May 2017 – Present
- Visiting Researcher – Carnegie Mellon University
  - July 2016 – October 2016
- Doctor of Science (DSc.) Tech. – Aalto University
  - March 2014 – January 2017, Title: Security for Ubiquitous Internet-connected smart objects
- Master of Science (MSc.) 2010-2012: Security and Mobile Comp.
  - Royal Institute of Technology (KTH), Sweden 2010/2011
  - Aalto University, Finland 2011/2012

My Work

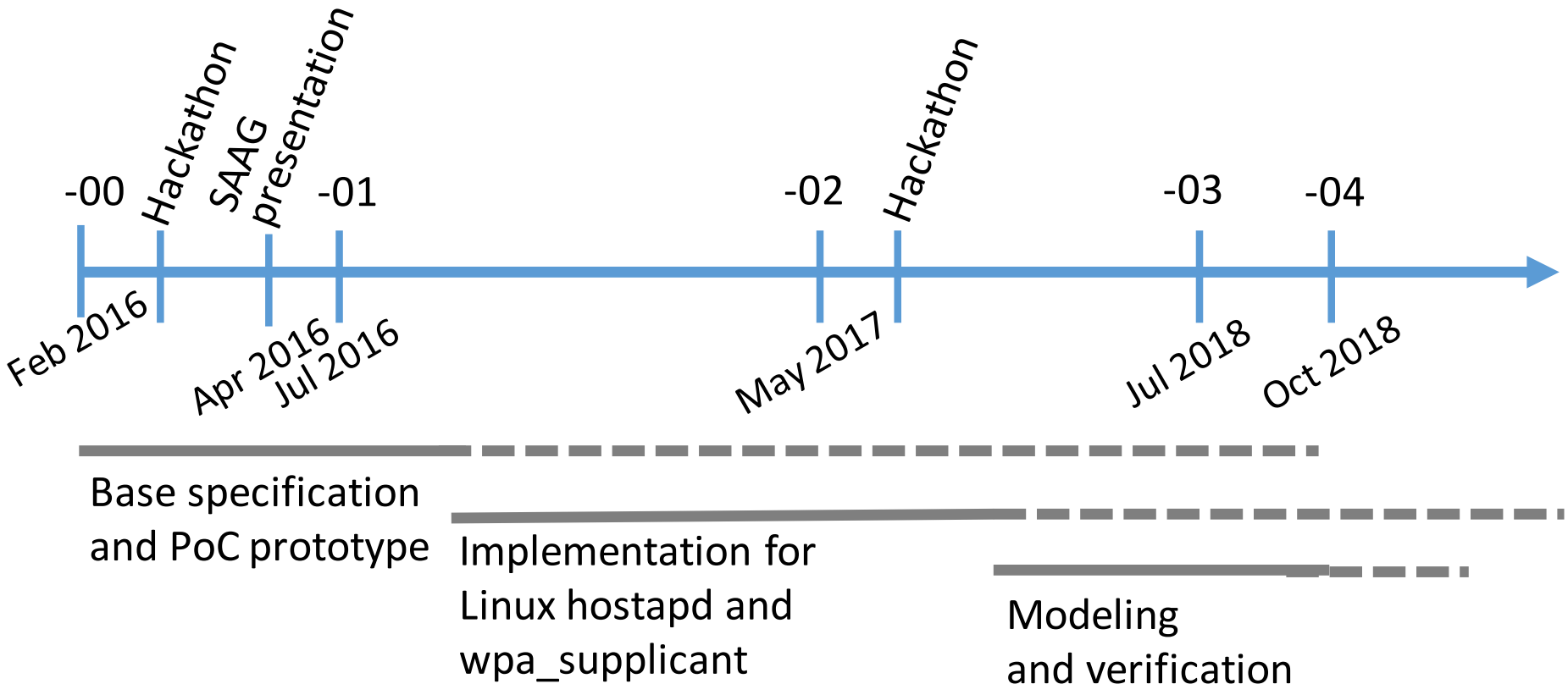
- Applied network security research
- Hands on coding: C/C++/Java/Python/Web
- Formal models
- Security standardization at IETF
  - Chair Light Weight-Implementation Guidance (LWIG)
  - Chair EAP Method Update (EMU)
- Best paper awards: ACM Ubicomp 2014, IEEE IoT 2015
- Patents and IPR: 50+ international patents

Why work on bootstrapping?

- Many protocols and tools for security:
  - Transport Layer Security (TLS)
  - Datagram TLS (DTLS) for UDP oriented traffic
  - Internet Key Exchange Protocol version 2 (IKEv2)
  - X509 certificates
- Little appetite for:
  - New crypto: identity-based crypto, attribute-based encryption
  - New lightweight protocols that save x bytes, or is faster etc.
- Bootstrapping:
  - This IoT device is mine -> associate it with my user account
  - This IoT device is trusted -> allow it connect to the network

EAP-NOOB

draft-aura-eap-noob



What about this IoT?

INTRODUCING
amazon echo

Always ready, connected, and fast. **Just ask.**

amazon dash
BUTTON

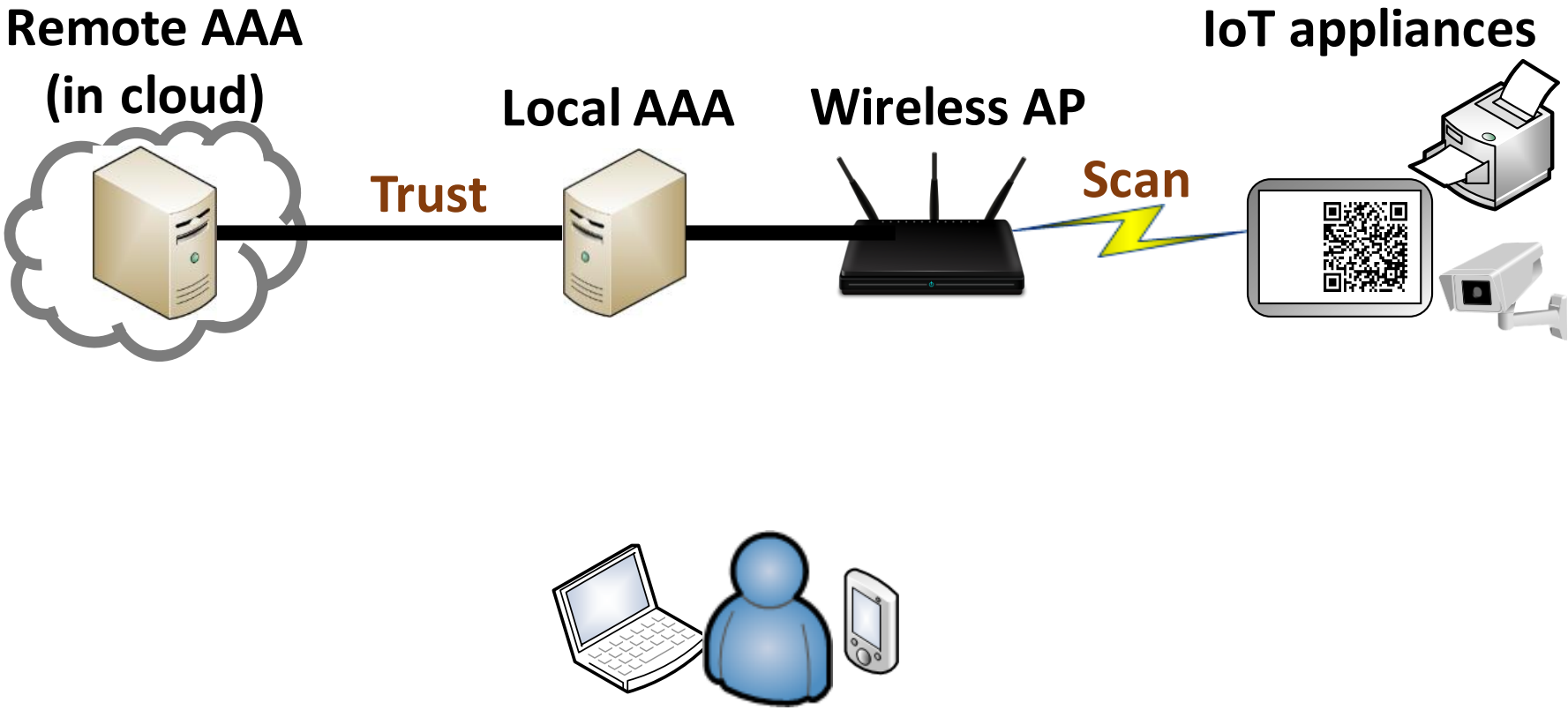
The Security problem - Challenges

- Non-expert users
  - A typical home user does not have a computer science degree
  - Even enterprise IT administrators are only marginally better
- Scalability
  - How do I manage 2,3,4 to 100s of devices
- Minimal User Interface
  - How do I configure an Amazon dash button
- Lifecycle
  - What do I do when my Internet-connected toaster is no longer supported
    - (Revolv smart hub: http://revolv.com/)

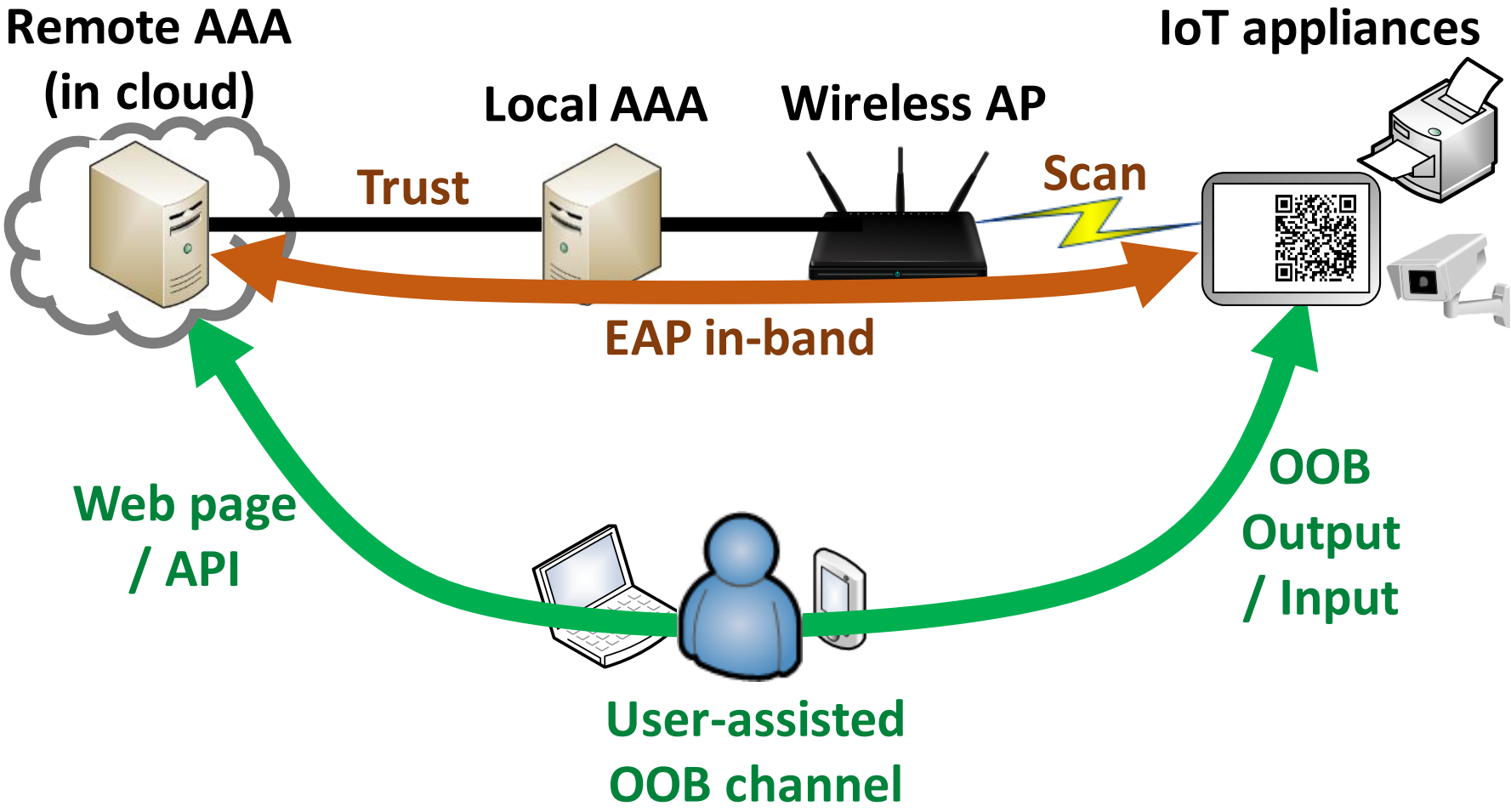
EAP-NOOB

- Cloud-connected IoT appliance
- New IoT appliance has no owner or domain, no credentials for cloud or Wi-Fi
- Need to:
  - connect the device to access network
  - register the device to AAA/cloud server
  - EAP-NOOB does both
- Security from a single user-assisted out-of-band message between peer device and AAA server

EAP-NOOB


Remote AAA
(in cloud)
Local AAA
Wireless AP
IoT appliances
Trust
Scan

EAP-NOOB


Remote AAA
(in cloud)
Local AAA
Wireless AP
IoT appliances
Trust
Scan
EAP in-band
Web page
/ API
OOB
Output
/ Input
User-assisted
OOB channel

EAP-NOOB protocol – high level view

- Protocol for new devices:
  1. Initial exchange in-band: ECDH over EAP
  2. Out-of-band step: one user-assisted message, in either direction
  3. Completion exchange in-band: authentication and key confirmation over EAP

- OOB step should not be not repeated. Reconnect exchange for rekeying, algorithm upgrade etc.

EAP-NOOB security details

- Authentication protocol details (with OOB from peer to server):
  - Initial ECDH without authentication
  - **OOB message** contains **secret N_{oob}** and **fingerprint H_{oob}**
  - **MAC with N_{oob} authenticates ECDH key in both directions**
  - Additionally, **H_{oob} authenticates ECDH key to AAA server**
  - Knowing N_{oob} authorizes the server and user to take control of the peer device

- OOB channel should protect both secrecy and integrity
  - Double protection: failure of one of these does not cause complete loss of security

Deploying EAP-NOOB

What is the cost?

- The EAP method implemented only in AAA/cloud server and peer devices
- No changes to the Authenticator (AP)
- No new code in access-network AAA server
- Access network admin chooses a AAA/cloud server and configures realm-to-server mapping for "@eap-noob.net"
- User must have accounts for accessing the organization's AAA/cloud server
- When OOB message is encoded as QR or NFC tag and scanned on smart phone, no phone app needed
- Home users would need WPA2-Enterprise and user accounts

Comparing it with other options:

- Configuring the peer offline with all it needs
  - Peer UI may have only output and no suitable input
- Simply transferring a secret key to/from the peer?
  - OOB channel may be vulnerable to spying. EAP-NOOB can work with only integrity
- Static QR code with hash of device public key
  - EAP-NOOB establishes two-way trust
  - EAP-NOOB assigns a network and owner to the device
- Reading and writing configuration data over NFC
  - EAP-NOOB only requires one OOB message in one direction
  - EAP-NOOB supports a variety of OOB channels incl. NFC
- Home networks with shared passphrase
  - Devices need to be managed and revoked individually; WPA-Enterprise is better

Summary:

- Join the discussion at emu@ietf.org
- Read, comment and ask questions
- Experimenting/Prototyping is always good