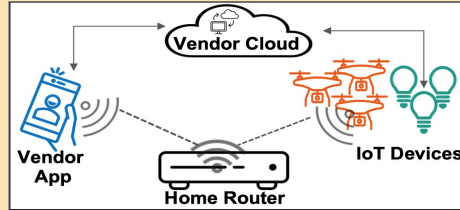# Unveiling IoT Devices Provisioning Processes

Rostand A. K. Fezeu, Timothy J. Salo, Amy Zhang, Zhi-Li Zhang

1. Today's Smart Home IoT Devices (Challenges)

- **Cloud-Centric** i.e., *Opaque, closed "Device-to-cloud"*
- **Forced** to used **vendor**-provided **mobile apps**
- Limited **security policies** & data to cloud **filtering**
- Manual, **one-device-at-a-time** provisioning process


2. Our Goals (Two Fold)

1. Gain a deeper understanding of IoT devices provisioning processes; device-to-cloud communication protocols; & security & privacy implications.
2. Explore the feasibility of developing an *open, edge-centric* gateway to simplify management & control and automate IoT device provisioning.

3. Typical IoT Device Provisioning Process
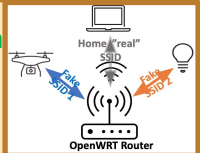
IoT Dissect I
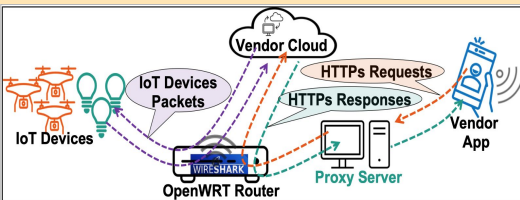
IoT Dissect II
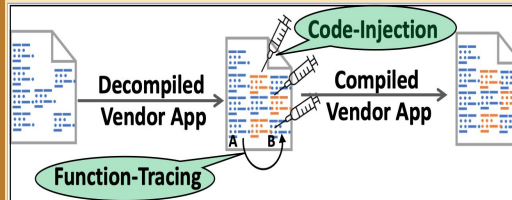
5. Breaking the opaque, device-to-cloud
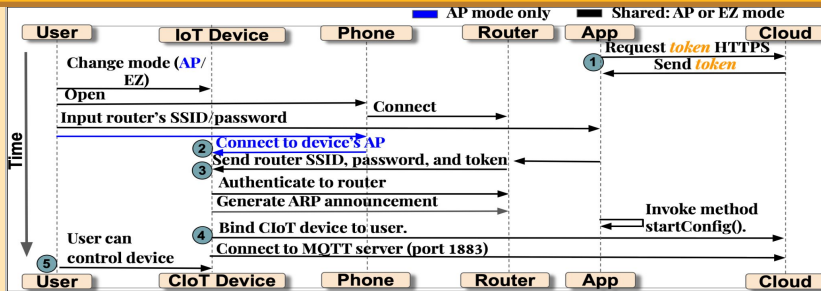
Exp. 1) IoT Devices & Tokens

➜ **Arbitrary Length or random** *tokens*

➢ **Expiring** *tokens,* **prevents replay attacks**

Exp. 2) Isolating Device-Cloud Communication

➢ **Device isolation is feasible**

4. Preliminary Observations

6. Conclusions

1. **Uncover** the **mechanism** for **provisioning** IoT devices.
2. **Reveal** potential **vulnerabilities** & **privacy** issues.
3. *Open, edge-centric* platform is **feasible**.

Future Works

1. Build a platform independent of vendor clouds and apps
2. Enforce security policies and data filtering.
3. Provisioning will be automated, simplified, and the user will have 100 % control of home network.