black hat®
ASIA 2023

MAY 11-12

BRIEFINGS

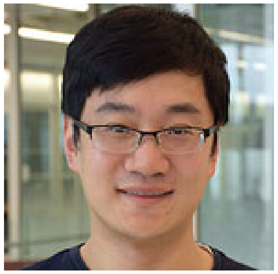
# Dilemma in IoT Access Control: Revealing Novel Attacks and Design Challenges in Mobile-as-a-Gateway IoT

**Speaker: Luyi Xing**

Indiana University Bloomington (USA)

Other contributors: Xin’an Zhou, Jiale Guan, Zhiyun Qian
From UC Riverside and Indiana University Bloomington

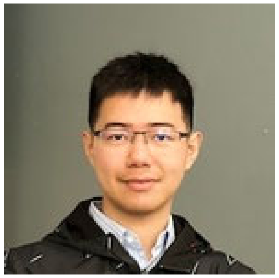
# Team/Contributors



Luyi Xing

Assistant Professor

Indiana University Bloomington



Xin’an Zhou

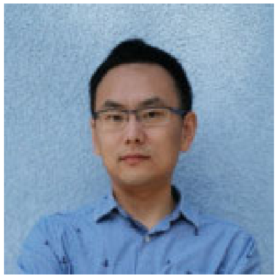
Ph.D. Student

UC Riverside

Jiale Guan

Ph.D. Student

Indiana University Bloomington



Zhiyun Qian

Professor

UC Riverside

# Our Black Hat talks of Internet of Things

**Black Hat’23 (Asia).** “Dilemma in IoT Access Control: Revealing Novel Attacks and Design Challenges in Mobile-as-a-Gateway IoT.”

**Black Hat’22 (Euro).** "IoT Manufacturers' New Nightmare: Design Flaws and Deployment Chaos in Cloud-based IoT Access Control Policies."

**Black Hat’22 (Asia).** "Codema Attack: Controlling Your Smart Home Through Dangling Management Channels."

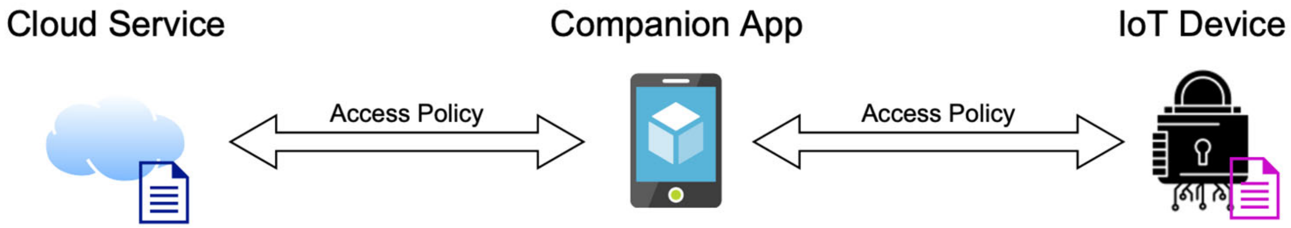
**Black Hat’21 (Asia).** "How I Can Unlock Your Smart Door: Security Pitfalls in Cross-Vendor IoT Access Control.”

**Black Hat’19 (Euro).** "Sneak into Your Room: Security Holes in the Integration and Management of Messaging Protocols on Commercial IoT Clouds.”

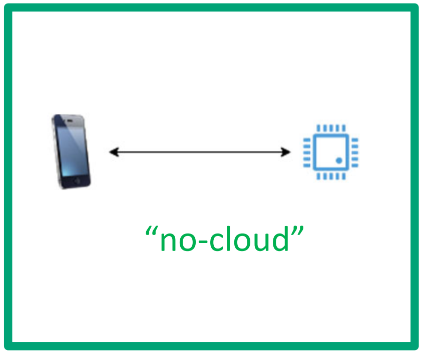
**BlackHat’16 (USA).** "Discovering and Exploiting Novel Security Vulnerabilities in Apple ZeroConf."

# What is Mobile-as-a-Gateway (MaaG) IoT?

1. MaaG IoT devices leverage mobile phones to as “Internet gateways” to communicate with the IoT cloud/server
2. MaaG IoT devices lack persistent Internet connectivity.

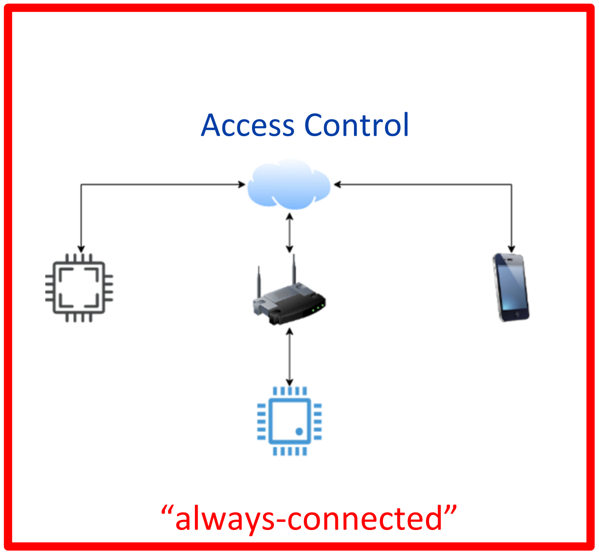


# Different Architectures of IoT



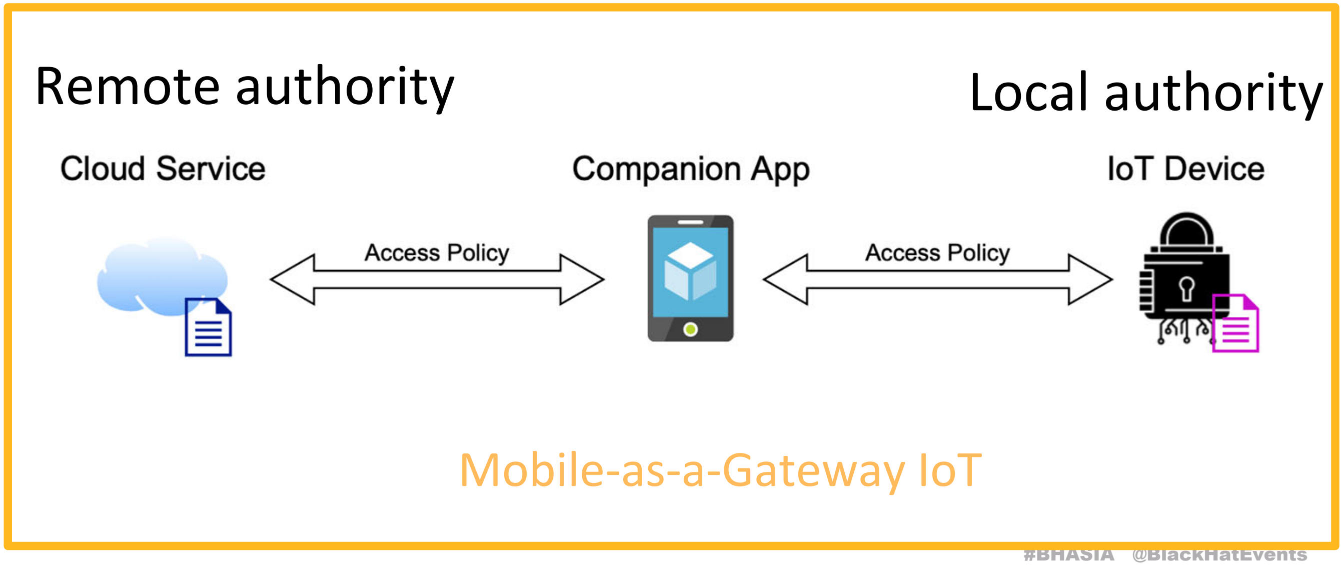
“no-cloud”

1. No cloud/server (“no-cloud”)
2. Cloud-centered: Always connected to the cloud (“always-connected”)
3. Mobile-as-a-Gateway IoT (“MaaG”)



Access Control

“always-connected”



Remote authority

Local authority

Cloud Service

Companion App

IoT Device

Access Policy

Access Policy

Mobile-as-a-Gateway IoT

# Attacks and Results Overview

1. End-to-end attacks on ten popular MaaG IoT devices (mainly smart locks, also trackers).
2. Security-critical flaws in their access control

level

august

Yale

ULTRALOQ

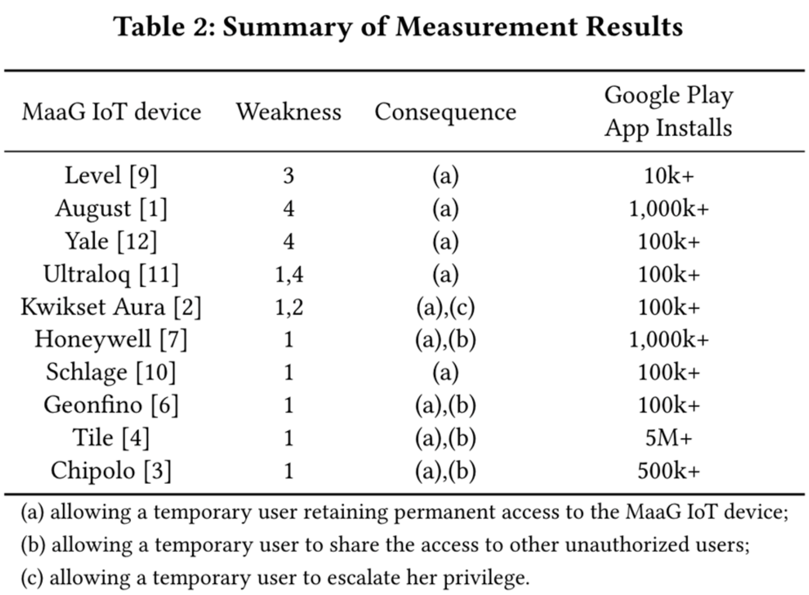


Table 2: Summary of Measurement Results

| MaaG IoT device | Weakness | Consequence | Google Play App Installs |
|---|---|---|---|
| Level [9] | 3 | (a) | 10k+ |
| August [1] | 4 | (a) | 1,000k+ |
| Yale [12] | 4 | (a) | 100k+ |
| Ultraloq [11] | 1,4 | (a) | 100k+ |
| Kwikset Aura [2] | 1,2 | (a),(c) | 100k+ |
| Honeywell [7] | 1 | (a),(b) | 1,000k+ |
| Schlage [10] | 1 | (a) | 100k+ |
| Geonfino [6] | 1 | (a),(b) | 100k+ |
| Tile [4] | 1 | (a),(b) | 5M+ |
| Chipolo [3] | 1 | (a),(b) | 500k+ |

(a) allowing a temporary user retaining permanent access to the MaaG IoT device;
(b) allowing a temporary user to share the access to other unauthorized users;
(c) allowing a temporary user to escalate her privilege.

Kwikset

Honeywell

SCHLAGE
Trust your home to Schlage.

tile by Life360

chipolo

# Security Design Flaws (Logic Faults)

Category 1: Flaws in MaaG **Access Model Translation**

Category 2: Flaws in MaaG **Policy Synchronization**

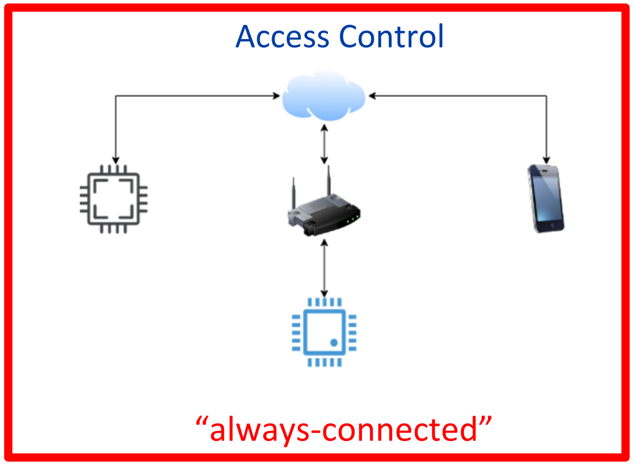
# Practical Threat Model

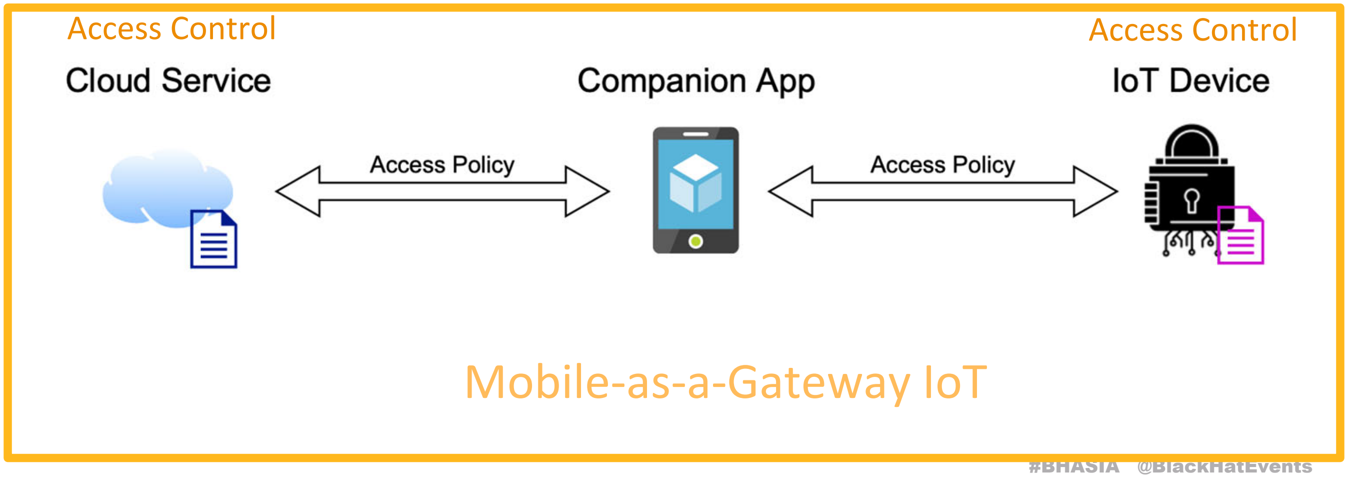
1. IoT cloud infrastructure and systems are benign
   - Cloud, network infrastructure, and the IoT devices (hardware/firmware)
2. Owners/administrators may temporarily share access (guests/employees)
3. Low-privileged users may be malicious
   - Aims to escalate privileges, or retain access after revocation
4. “App” in this talk refers to the IoT vendor’s mobile app

# Security Challenges of MaaG IoT

MaaT IoT significantly complicates access control

- Access control span the cloud and device
- Different access control semantics/models
- Each (cloud/device) as an autonomous authority (to make same access decisions)

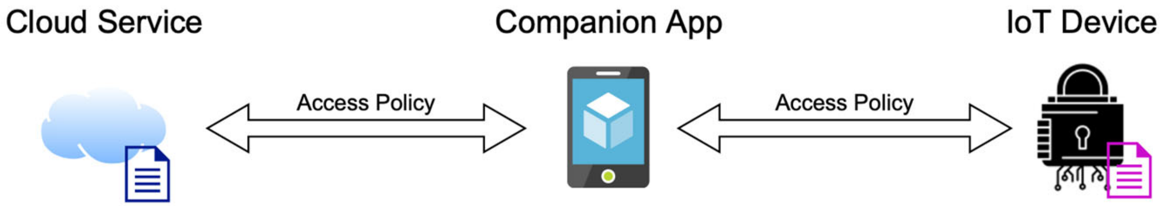




# Expectation for MaaG Access Control

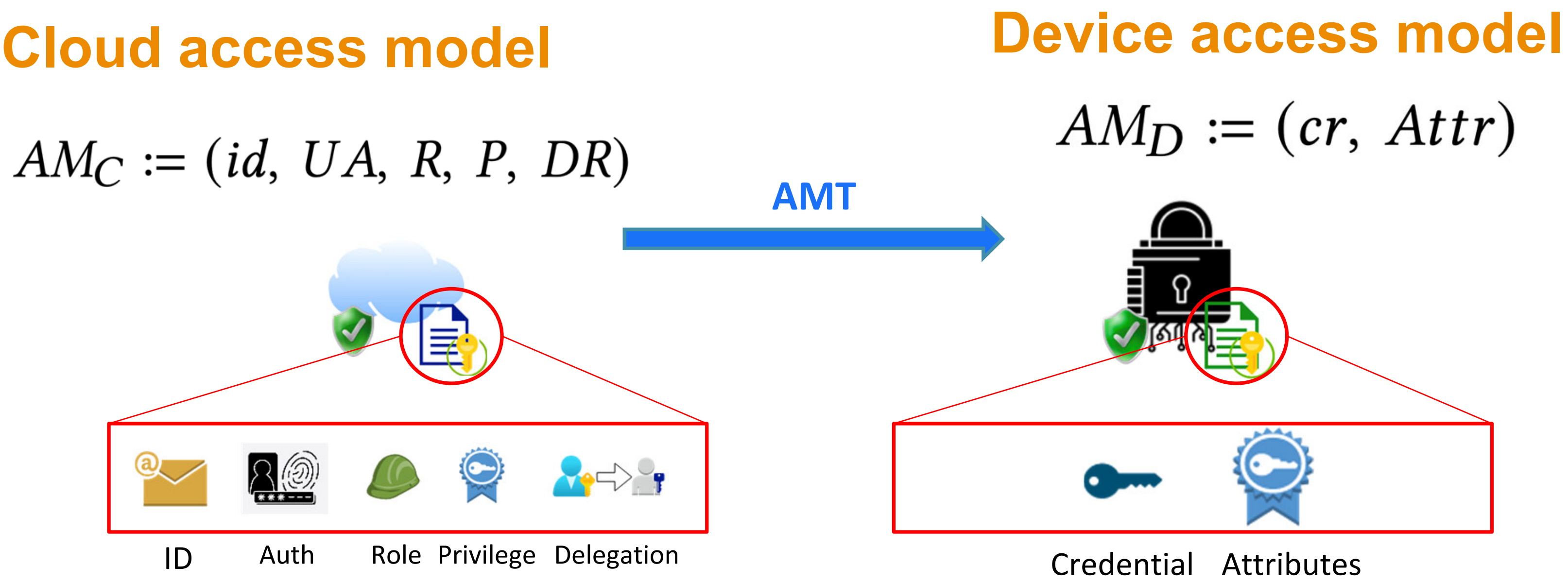
## Access Model Translation

1. The cloud as the authority to issue/manage policies
   - increasingly complicated policies
2. The device often enforces the policies (received from cloud)
   - translated to simpler on-device policies



Mobile-as-a-Gateway IoT

# Access Model Translation



Cloud access model

$$AM_C := (id,\ UA,\ R,\ P,\ DR)$$

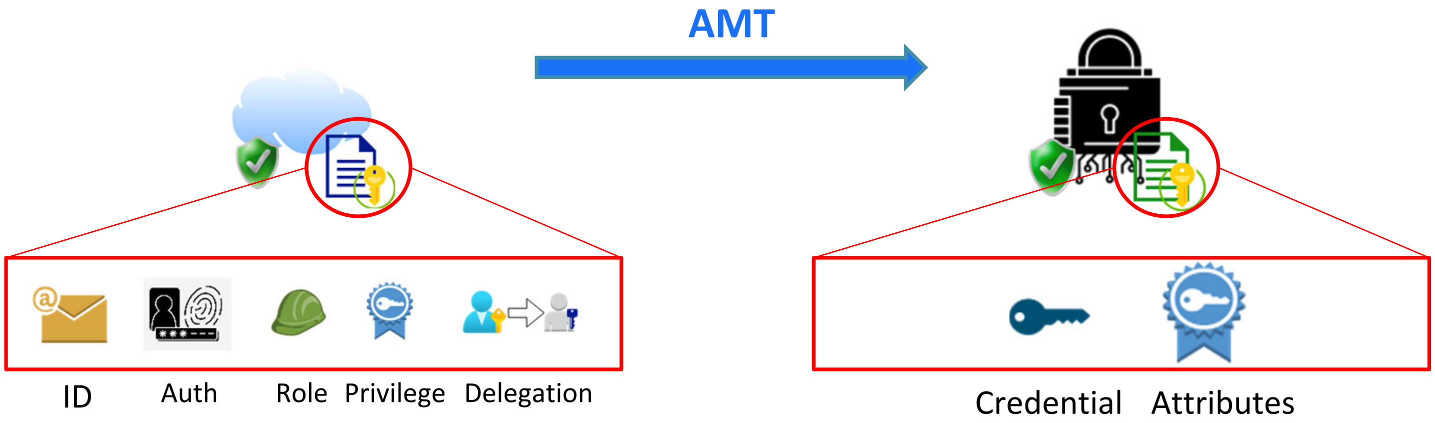
AMT

Device access model

$$AM_D := (cr,\ Attr)$$

# Flaws in Access Model Translation

1. IoT devices have lighter-weight access model than the cloud
2. Commensurate, sufficient semantics when the complex cloud-side access model is translated to the device-side (AMT)

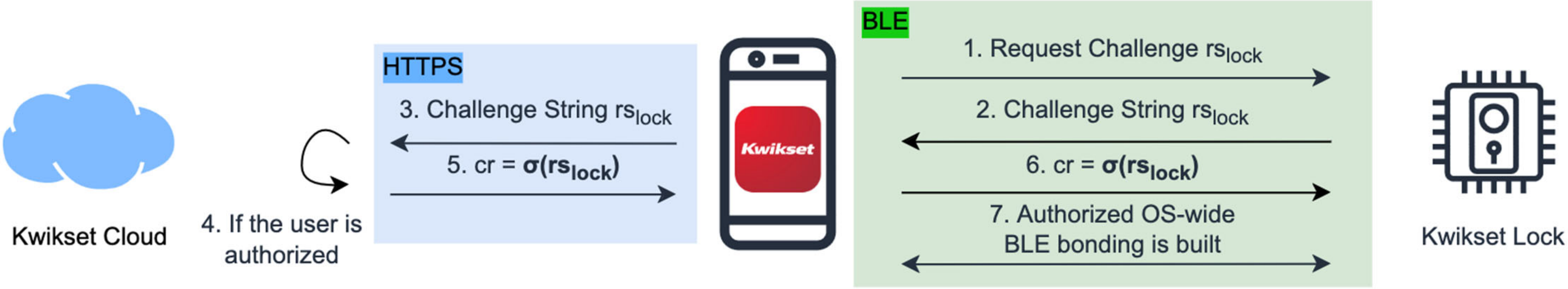


# Example (with flaw): Kwikset smart lock's AMT

**Cloud access model** $\xrightarrow{\text{AMT}}$ **Device access model**

$$AM_C := (id,\ UA,\ R,\ P,\ DR)$$

$$AM_D := (cr,\ Attr)$$


Kwikset Cloud
4. If the user is authorized
HTTPS
3. Challenge String $rs_{lock}$
5. $cr = \sigma(rs_{lock})$
Kwikset
BLE
1. Request Challenge $rs_{lock}$
2. Challenge String $rs_{lock}$
6. $cr = \sigma(rs_{lock})$
7. Authorized OS-wide BLE bonding is built
Kwikset Lock

Kwikset lock is assured for the user legitimacy (cloud-signed cr)

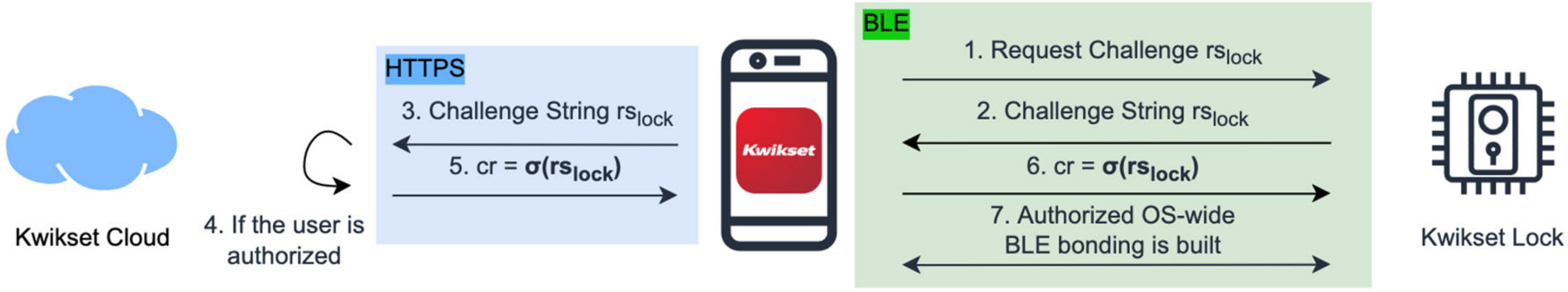
# Flaw/Attack 1: Lost Identities in AMT

$$AM_C := (id,\ UA,\ R,\ P,\ DR) \xrightarrow{\text{AMT}}$$

$AM_D$ (lock-side policy):

- $(BLE\_phone\_name, BLE\_binding\_key)$
- ~~$cr$~~

AMT lost identities, and cannot even map in-device policies back to user identifies.



Kwikset Cloud

4. If the user is authorized

HTTPS

3. Challenge String $rs_{lock}$

5. cr = $\sigma(rs_{lock})$

BLE

1. Request Challenge $rs_{lock}$

2. Challenge String $rs_{lock}$

6. cr = $\sigma(rs_{lock})$

7. Authorized OS-wide BLE bonding is built

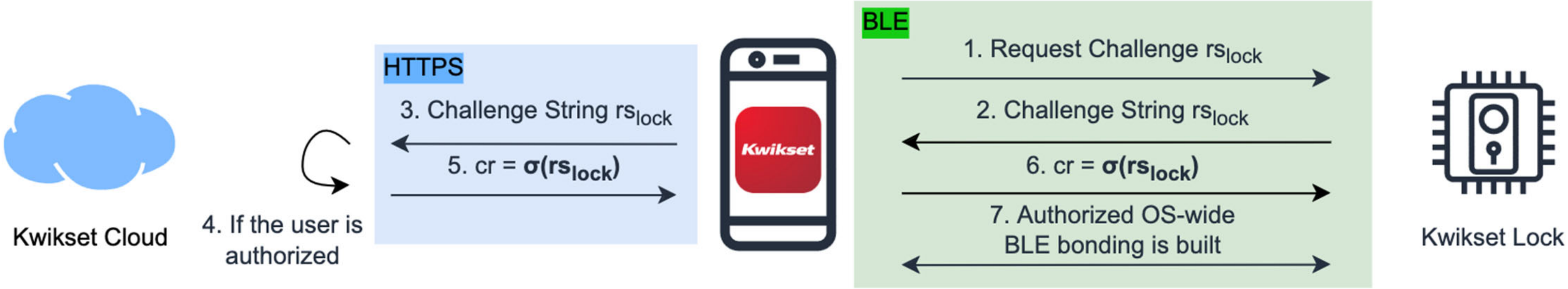
Kwikset Lock

# Flaw/Attack 2: Lost roles, permissions, and lifecycle control in AMT

$$AM_C := (id,\ UA,\ R,\ P,\ DR) \xrightarrow{\text{AMT}} AM_D := (BLE\_binding,\ Attr)$$

Kwikset lock assured for the user legitimacy (cloud-signed cr)

- Locks do not differentiate users for permissions/roles
- Only app GUI control options different
- Attack: Low-privilege users send high-privileged commands to locks


Kwikset Cloud
4. If the user is authorized
HTTPS
3. Challenge String $rs_{lock}$
5. cr = $\sigma(rs_{lock})$
Kwikset
BLE
1. Request Challenge $rs_{lock}$
2. Challenge String $rs_{lock}$
6. cr = $\sigma(rs_{lock})$
7. Authorized OS-wide BLE bonding is built
Kwikset Lock

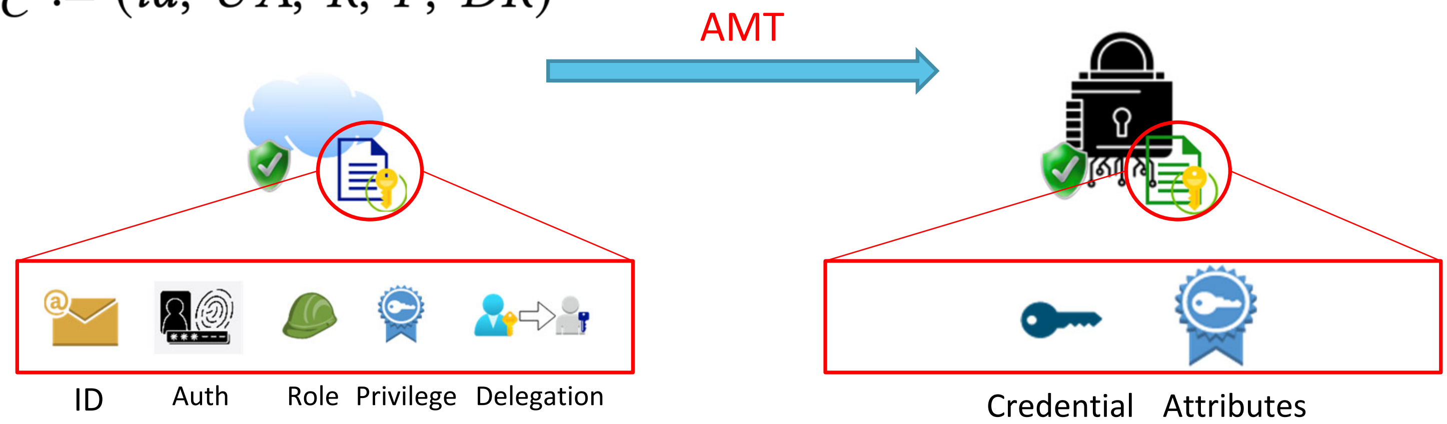
# Flaw/Attack 3: Un-Synced offline keypad passcode

Kwikset lock: device maintains certain policies not intended to be shared with the cloud

Asymmetric policies: cloud  vs. device

$$AM_D := Attr(\text{offline keypad passcode}, \dots)$$

$$AM_C := (id,\ UA,\ R,\ P,\ DR)$$



# Security Design Flaws (Logic Faults)

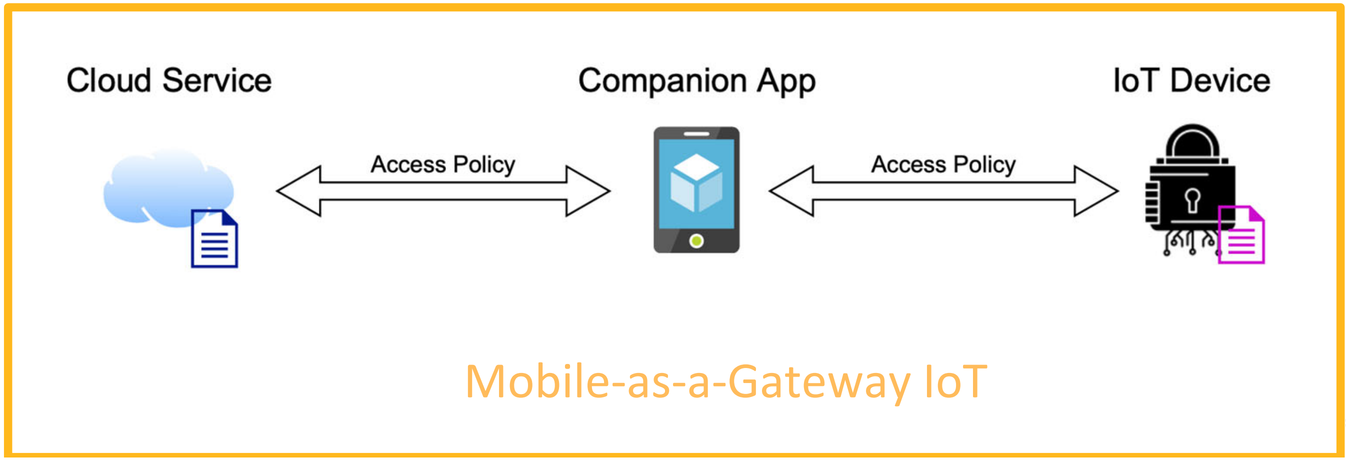
Category 1: Flaws in MaaG **Access Model Translation**

Category 2: Flaws in MaaG **Policy Synchronization**

# Security Challenges of MaaG IoT (cont.)

Lack consistency models for access policies (cloud and IoT devices)

- Policy sync must route through the untrusted mobile phone
- Essentially featured with network partition and weak consistency
- “Eventual consistency” model?

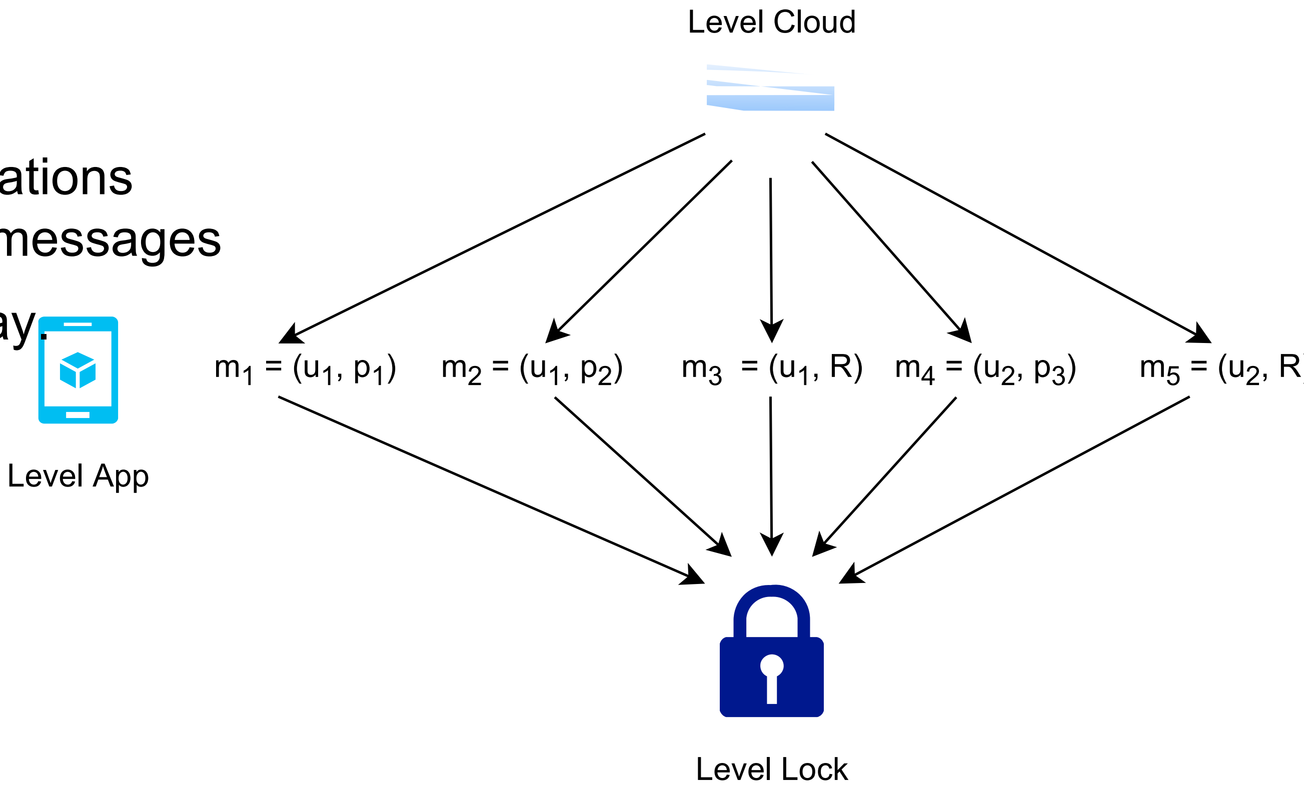


Mobile-as-a-Gateway IoT

# Flaw/Attack 4: Policy Synchronization

Prior “eventual consistency” model (temporal-order) fails

- More complicated causal relations between MaaG policy-sync messages
- Subject to reorder/drop/replay.



*Expected order: (m1, m2, m3)*

*Possibly actual: (m1, m3, m2)*

# Generality of the flaws

The flaws in 8 smart lock devices and 2 other IoT devices.

General across an even a wider device types, as long as they have the notion of access sharing.

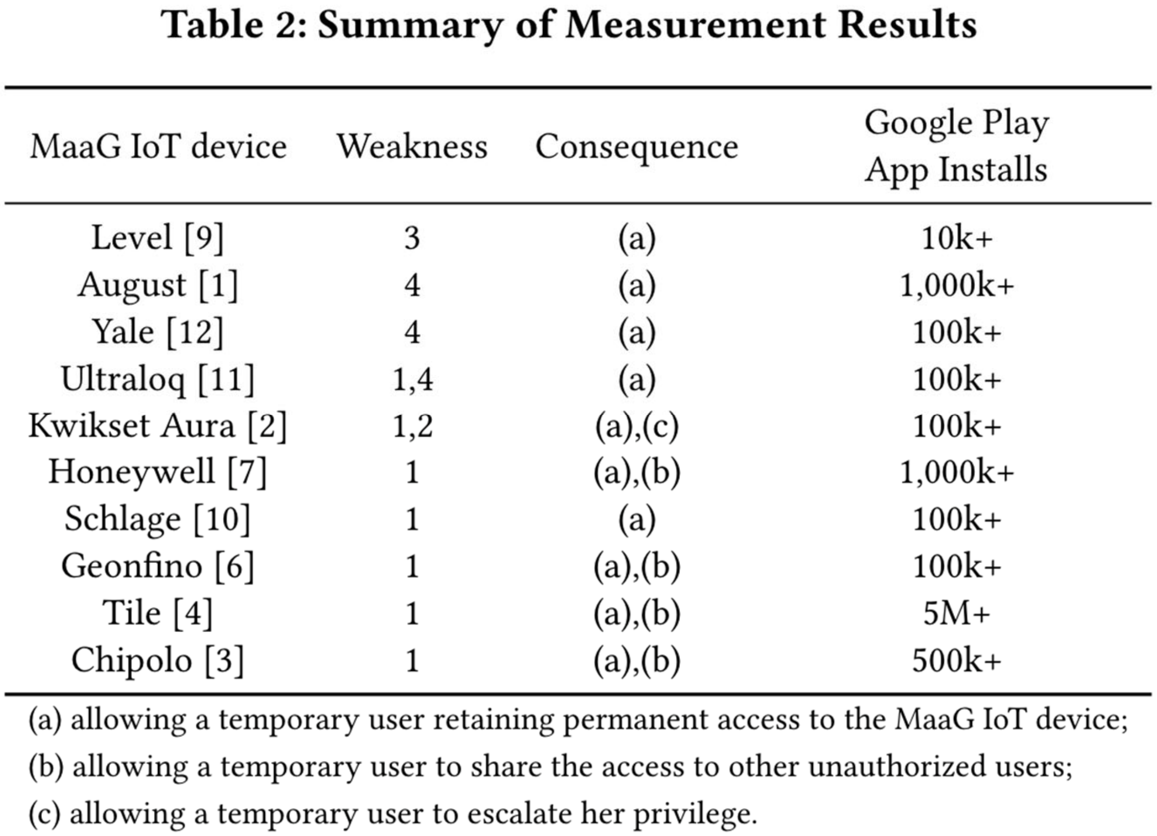


**Table 2: Summary of Measurement Results**

| MaaG IoT device | Weakness | Consequence | Google Play<br>App Installs |
|---|---|---|---|
| Level [9] | 3 | (a) | 10k+ |
| August [1] | 4 | (a) | 1,000k+ |
| Yale [12] | 4 | (a) | 100k+ |
| Ultraloq [11] | 1,4 | (a) | 100k+ |
| Kwikset Aura [2] | 1,2 | (a),(c) | 100k+ |
| Honeywell [7] | 1 | (a),(b) | 1,000k+ |
| Schlage [10] | 1 | (a) | 100k+ |
| Geonfino [6] | 1 | (a),(b) | 100k+ |
| Tile [4] | 1 | (a),(b) | 5M+ |
| Chipolo [3] | 1 | (a),(b) | 500k+ |

(a) allowing a temporary user retaining permanent access to the MaaG IoT device;
(b) allowing a temporary user to share the access to other unauthorized users;
(c) allowing a temporary user to escalate her privilege.

# Generality of the flaws

Access model translation and synchronization are essential concerns for MaaG IoT

- The de facto standard that the IoT cloud maintains a primary copy of access control policies (facilitate remote management)
- IoT devices enforce the policy independently (the offline access requirement)

# Responsible Disclosure

We have reported all product vulnerabilities to related 10 IoT vendors.

- 9 replied.
- 8 vendors acknowledged the vulnerabilities.

At least four vendors have patched their products (e.g., August/Yale, Level, and Geonfino).

# Black Hat Sound Bytes (Key Takeaways)

Security design challenges in the Mobile-as-a-Gateway IoT architecture

1. Asymmetric access models (cloud vs. device)
2. Asymmetric access models are difficult to ensure semantic consistency and coordinate
3. AMT and Policy Synchronization are challenging

**Full Paper:**

**https://www.xing-luyi.com/uploads/2/5/6/4/25640947/ccs_22_maag_iot.pdf**

# Q&A

## Luyi Xing (luyixing@indiana.edu)

## Full paper:

## https://www.xing-luyi.com/uploads/2/5/6/4/25640947/ccs_22_maag_iot.pdf