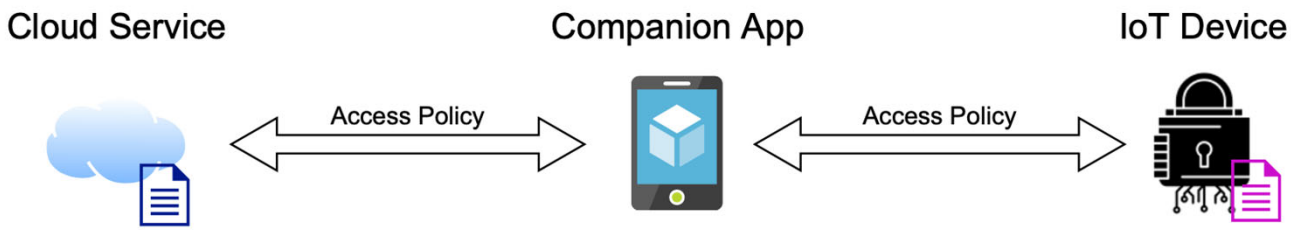
Dilemma in IoT Access Control: Revealing Novel Attacks and Design Challenges in Mobile-as-a-Gateway IoT

Luyi Xing*, Xin'an Zhou‡, Jiale Guan*, Zhiyun Qian‡

‡UC Riverside and *Indiana University Bloomington

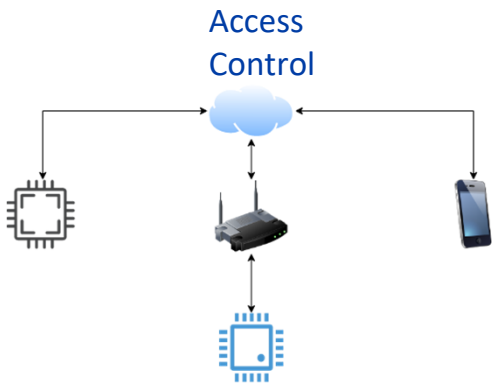
What is Mobile-as-a-Gateway (MaaG) IoT?

1. MaaG IoT devices leverage users' mobile phones to act as "Internet gateways" to communicate with the modern IoT cloud infrastructure.
2. MaaG IoT devices lack persistent Internet connectivity.

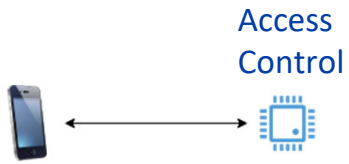


Different Architectures of IoT

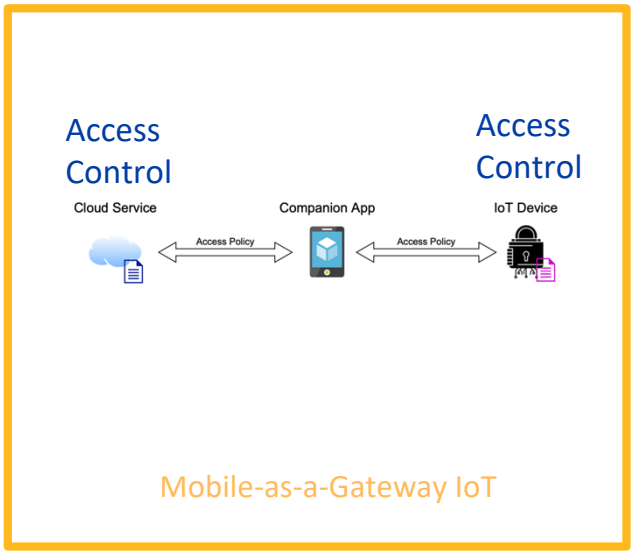
1. Always connected to the cloud. (“always-connected”)
2. No connection to the cloud. (“no-cloud”)
3. Mobile-as-a-Gateway IoT.



“always-connected”



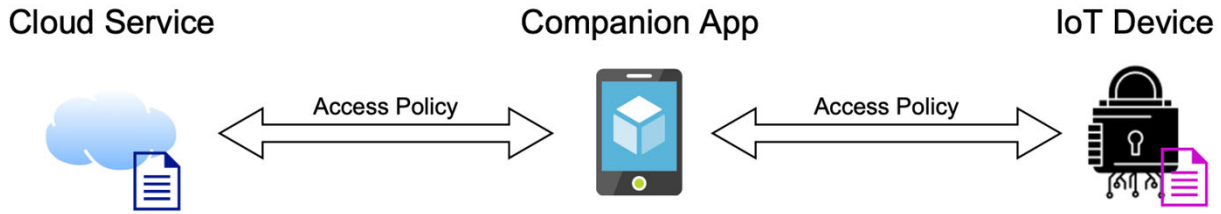
“no-cloud”



Mobile-as-a-Gateway IoT

Different Architectures of IoT

1. Always connected to the cloud. (“always-connected”)
2. No connection to the cloud. (“no-cloud”)
3. Mobile-as-a-Gateway IoT.



Mobile-as-a-Gateway IoT

Dilemma: Remote access control management vs. offline availability

1. Remotely share/revoke access to/from an invitee. (Good for Airbnb business)
2. Offline availability: Access the IoT device even without Internet connections.
3. Contradicting with each other?

Research targets and results

1. We pick 10 popular real-world MaaG IoT devices (smart locks and item trackers).
2. We can identify critical flaws in their access control management.

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

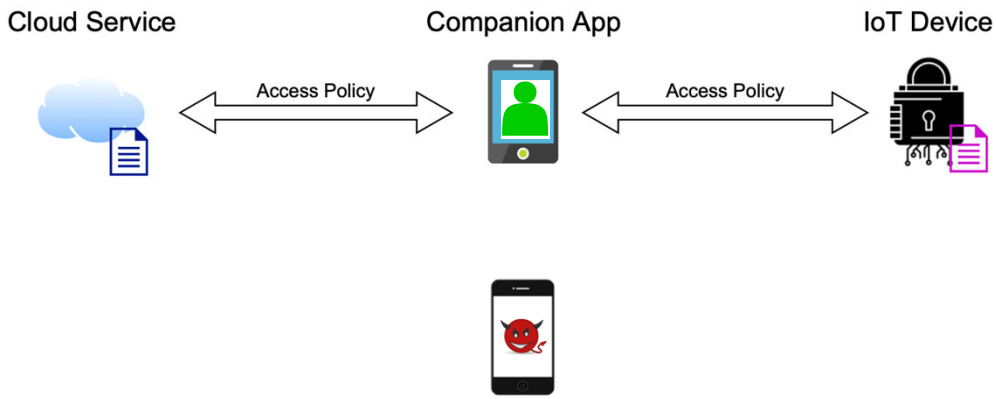
Trust your home to Schlage.

tile by Life360

chipolo

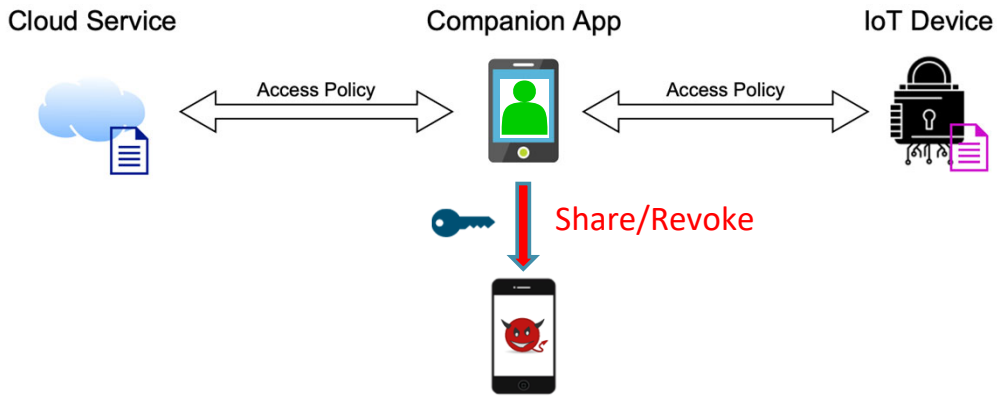
Threat Model

1. The attacker (temporary user) has full access to their own mobile device.
   E.g., through jailbreaking/rooting.
2. The cloud service, the owner's mobile phone, and the IoT device are benign.



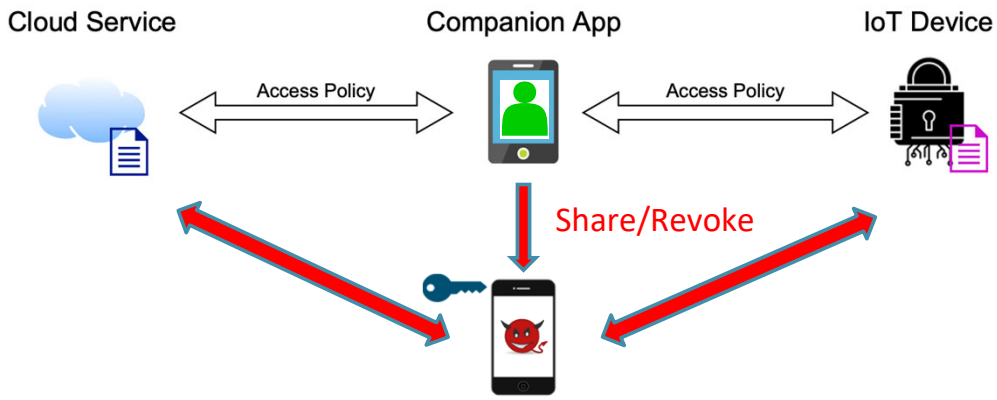
Threat Model

1. The attacker (temporary user) has full access to their own mobile device.
   E.g., through jailbreaking/rooting.
2. The cloud service, the owner's mobile phone, and the IoT device are benign.



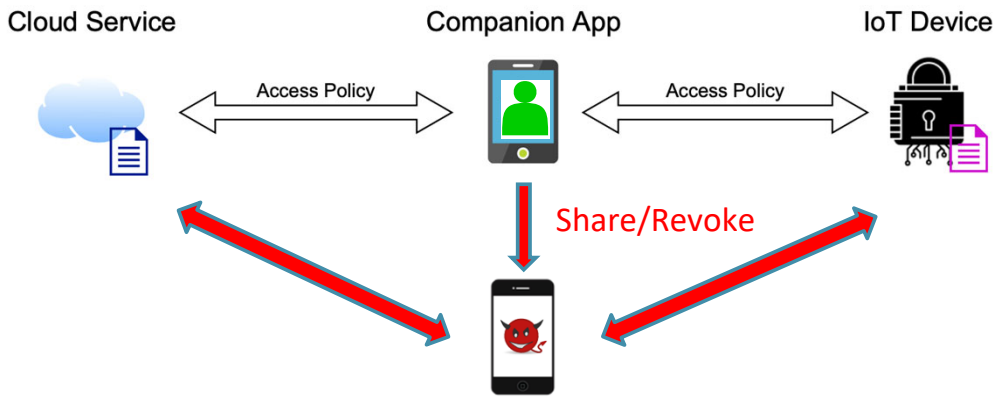
Threat Model

1. The attacker (temporary user) has full access to their own mobile device.
   E.g., through jailbreaking/rooting.
2. The cloud service, the owner's mobile phone, and the IoT device are benign.



Attack scenario

1. After the access is shared to the attacker, can the attacker:
   I. retain access permanently,
   II. distribute such access further,
   III. escalate their privilege?



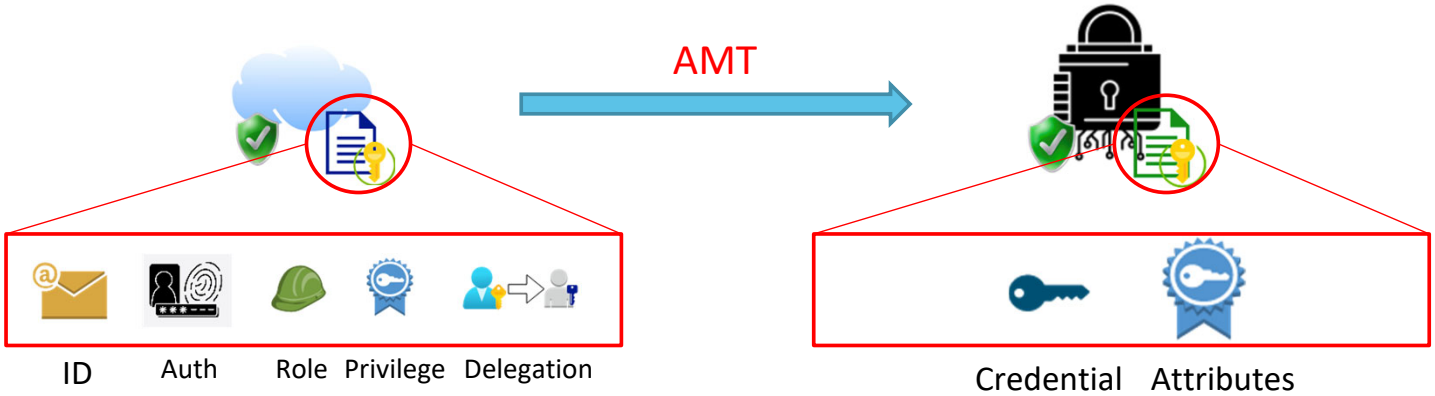
Security Flaws

1. Flaws in MaaG Access Model Translation

2. Flaws in MaaG Policy Synchronization

Flaws in MaaG Access Model Translation

1. Access models are different for the cloud and for the IoT device.
   I. Why? Because IoT devices lack I/O interfaces, need to reduce cost…
   II. Thus, it needs Access Model Translation.



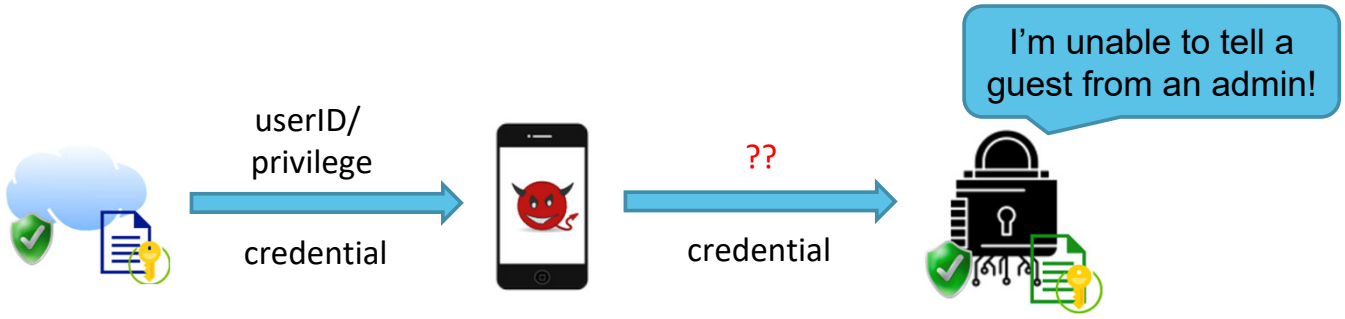
Flaws in MaaG Access Model Translation

2. Is the AMT process semantically sufficient?

   E.g., Does the translated attributes maintain user IDs/privileges?

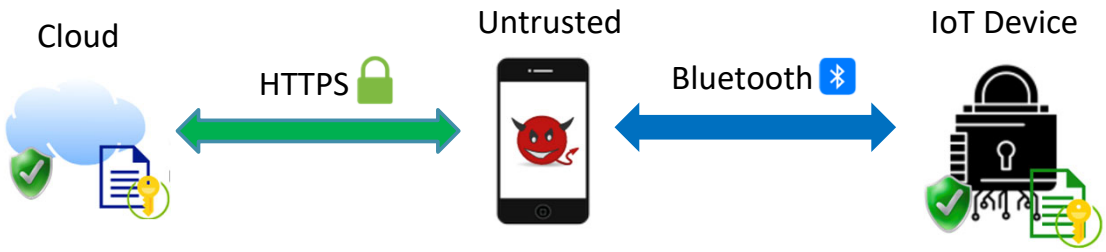
3. Unfortunately, NO.

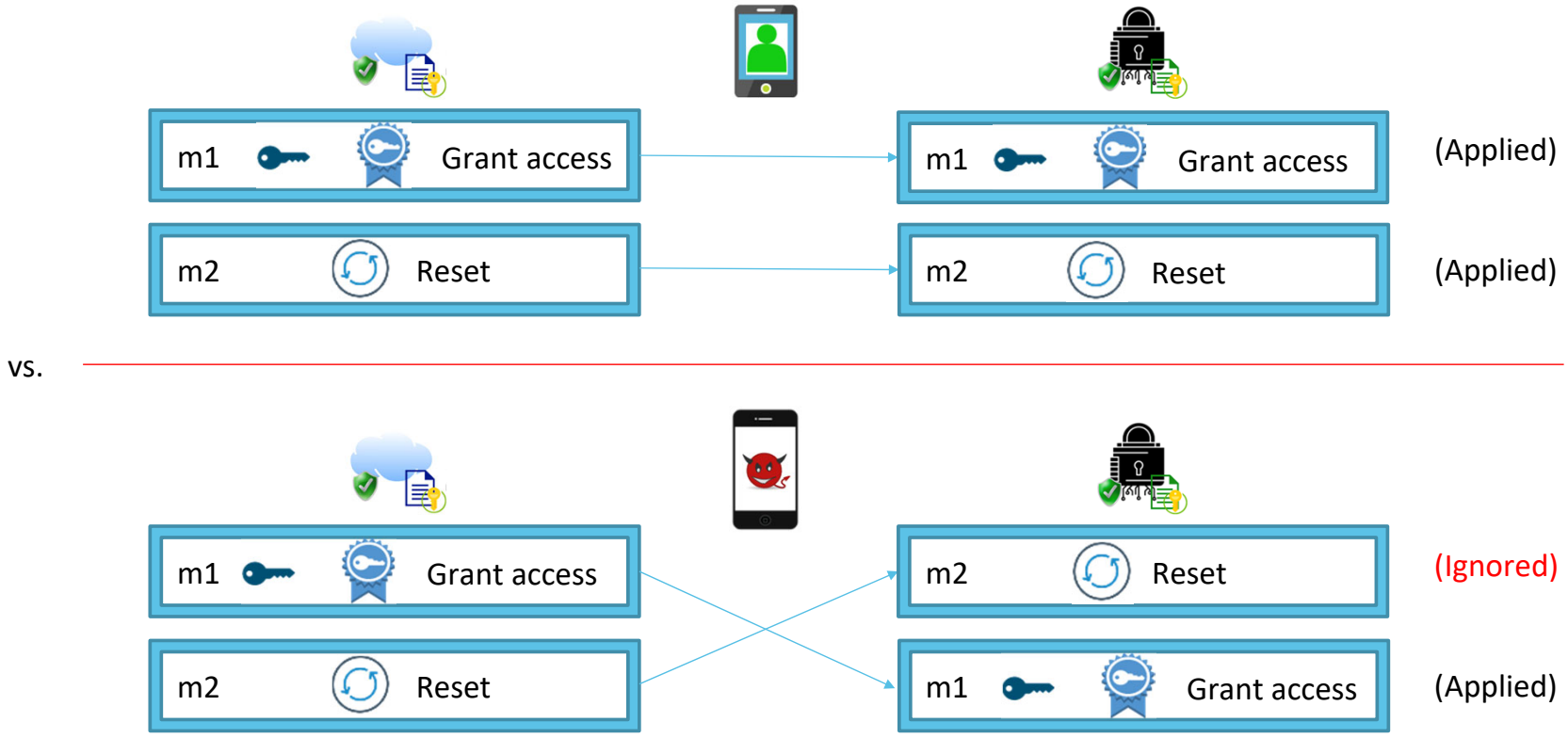
   More generally, loss of semantics in the AMT process.



Flaws in MaaG Policy Synchronization

1. Policy sync messages must route through the untrusted mobile phone using two kinds of protocols.
   I. No direct connection between the cloud and the IoT device.
   II. Subject to reorder/drop/replay.





Result: User is still on the lock!

Mitigating Vulnerabilities in MaaG Access Control

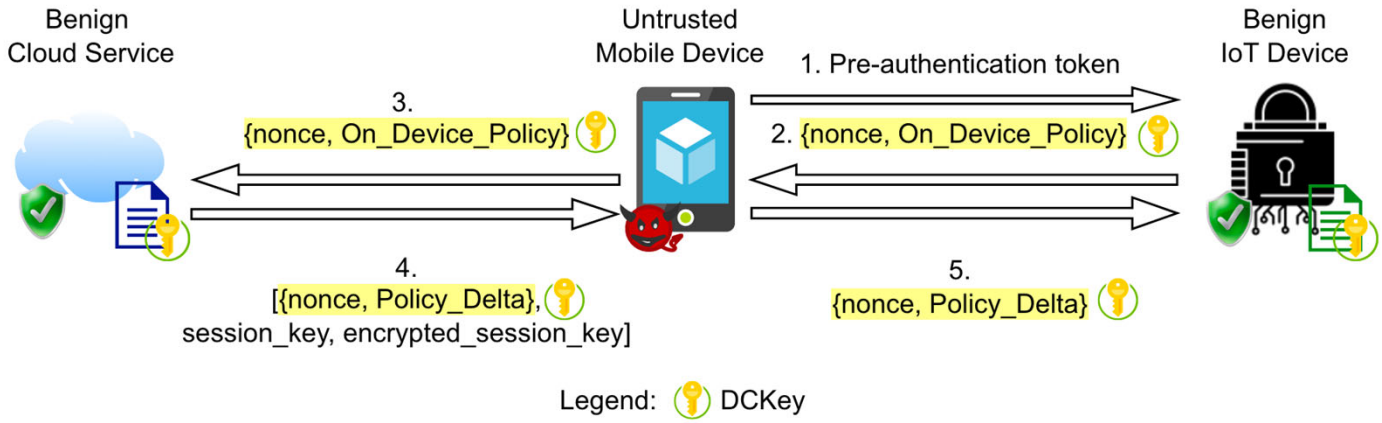


Figure 5: Secure Access Policy Synchronization (SAPS) Protocol

Key Takeaway

1. We find design level problems in the Mobile-as-a-Gateway IoT architecture.
2. Access Model Translation and Access Policy Synchronization are vulnerable for existing Mobile-as-a-Gateway IoT devices.
3. We design a novel protocol to mitigate these flaws.

Demo Time: August/Yale Smart Lock Attack

Video Link: https://youtu.be/LjpVVLhUrtk

Q&A Time