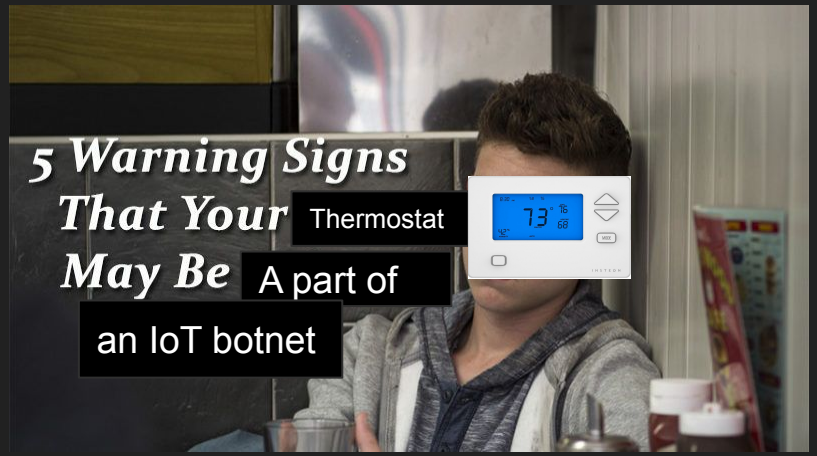
Don’t Talk Unless I Say So! Securing the Internet of Things with Default-Off Networking

James Hong, Amit Levy, Laurynas Riliskis, and Philip Levis

Presented by Mike Hegarty

Introduction

- New field of smart appliances(lights, HVAC, locks, dishwashers, etc)
- New Smart devices lead to new avenues of vulnerabilities
- However these devices mostly do one thing over the network.
- Propose a default off method of networking IoT devices.



Default Off === Whitelisting

Blacklist vs Whitelist in Networking

Blacklisting: Maintaining a list of entities or users who are not allowed to use or connect to your service.

ex: Casino that bans cheaters

+Simple for end users.
+Universal
-New/unknown threats won't be on blacklist

Whitelisting: Maintaining a list of entities or users who are allowed to use or connect to your service. All other entities cannot connect.

ex: Invite only party

+Prevents remote threats
-Needs to be personalized for end user

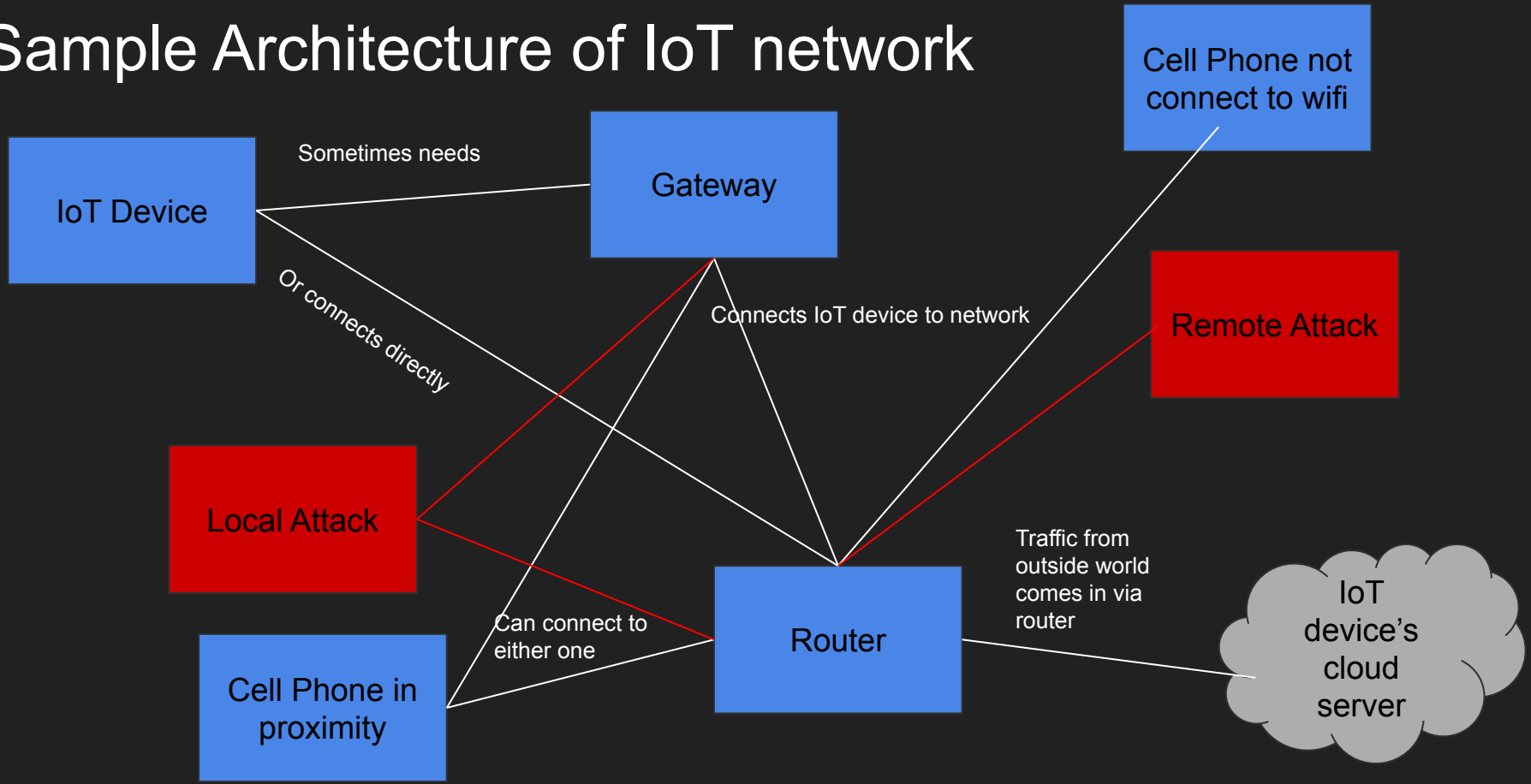
Drawbacks of updating for system security?

What about for end user convenience?

Previous attacks

- Previous attacks on IoT devices expose flaws
  - Mirai botnet
  - Miele commercial dishwasher attack
- Two Serious types of threats:
  - Financial/physical damage
    - Insulin pump, Thermostat in food storage
  - Networking
- Would these attacks be possible in whitelisted system?

Sample Architecture of IoT network



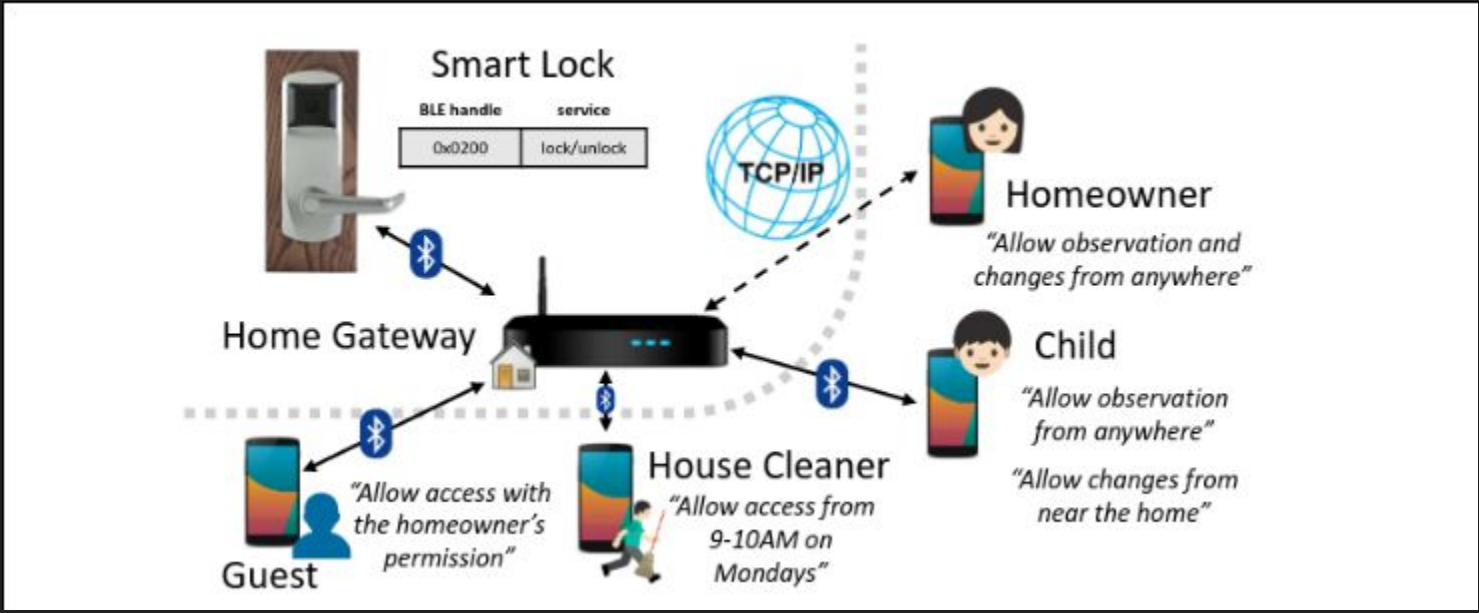
Problem with whitelisting

- Whitelisting by definition would solve a lot of previously seen issues
- Requires more from the end-user
  - gross mac addresses,configuring the router, etc
- Harder sell for IoT companies

Introducing: Bark

- Bark disguises complex networking rules into simple sentences.
- Rules are made answering the questions of who, what, where, when and how.
    - Think of it like the game Clue, where you try to solve for different pieces of evidence then put your accusation together into a sentence containing them all

Example Use Case: Smart Lock



Bark Policy Language: types

1. Who
    - refers to principals, which are devices and apps, and contains the necessary information to abstract the different ways things could be addressed from the end users.
    - Could be a mac address, ip/domain name, etc.
2. What
    - refers to a service offered by the who.
    - Could be a TCP port, a Bluetooth UUID, etc.
3. Where
    - relates to the first hop gateway a who connected with.
4. How
    - The operation that the who wants to do
    - HTTP: GET,POST,DELETE; DNS: query; BLE: read, write, subscribe; etc
5. When
    - time restriction/timeout as well as boolean conditions

Bark Policy Language: Rules

- Rules are defined with subjects, actions, objects, and conditions.
  - Subject: a who and a where
  - Object: who, where, what.
  - Action: how
  - Condition: algebraic expression of
  - boolean whens
- Groups
- All vs One

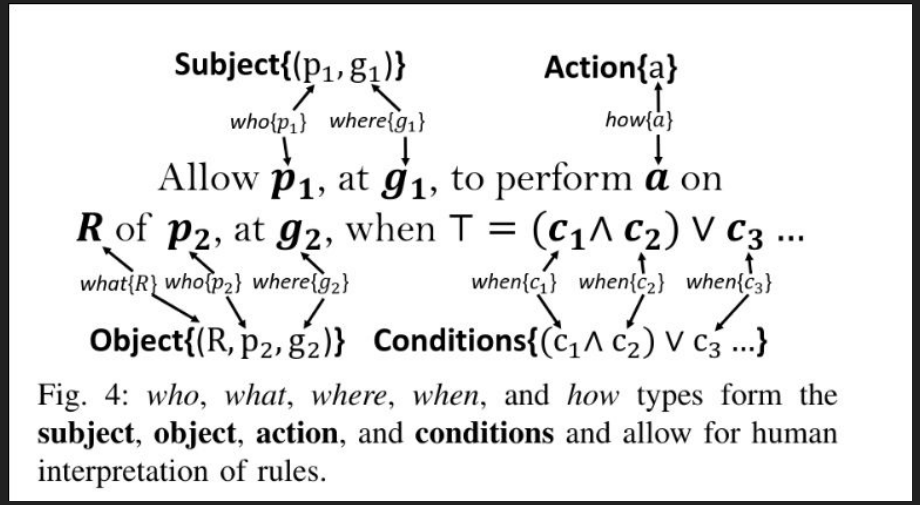


Fig. 4: *who*, *what*, *where*, *when*, and *how* types form the **subject**, **object**, **action**, and **conditions** and allow for human interpretation of rules.

Lock with Time Limitation

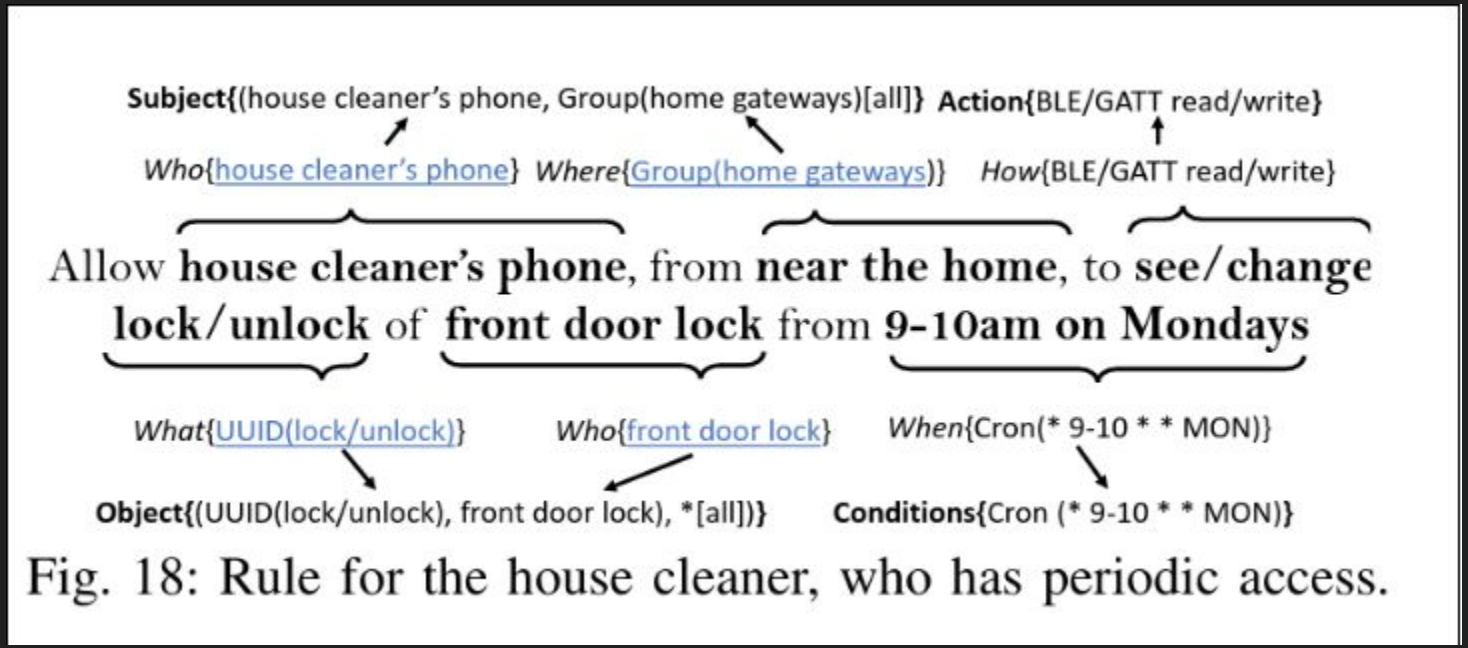


Fig. 18: Rule for the house cleaner, who has periodic access.

Group of Lights

Fig. 11: Rule for a switch and a group of lightbulbs.

2 Factor Authentication

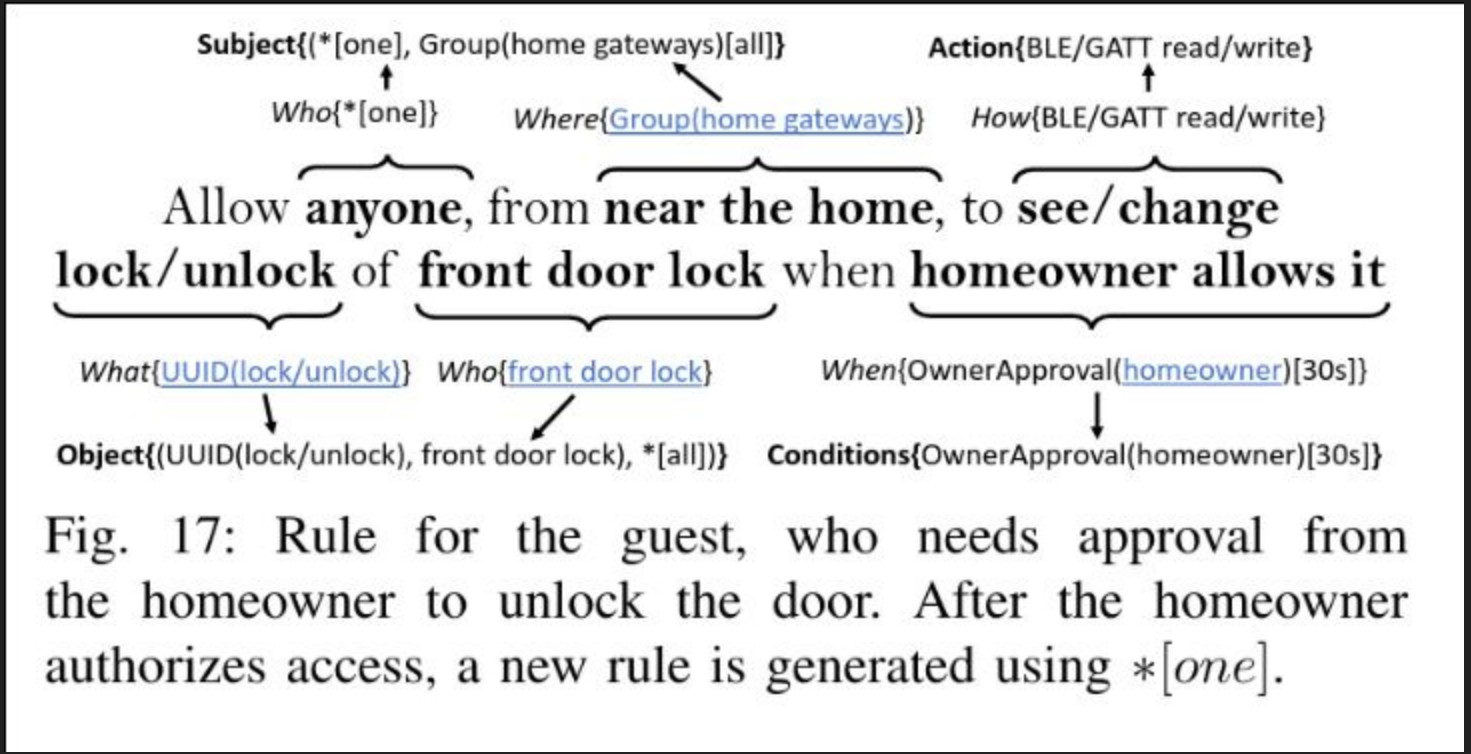


Fig. 17: Rule for the guest, who needs approval from the homeowner to unlock the door. After the homeowner authorizes access, a new rule is generated using $*[one]$.

Echo

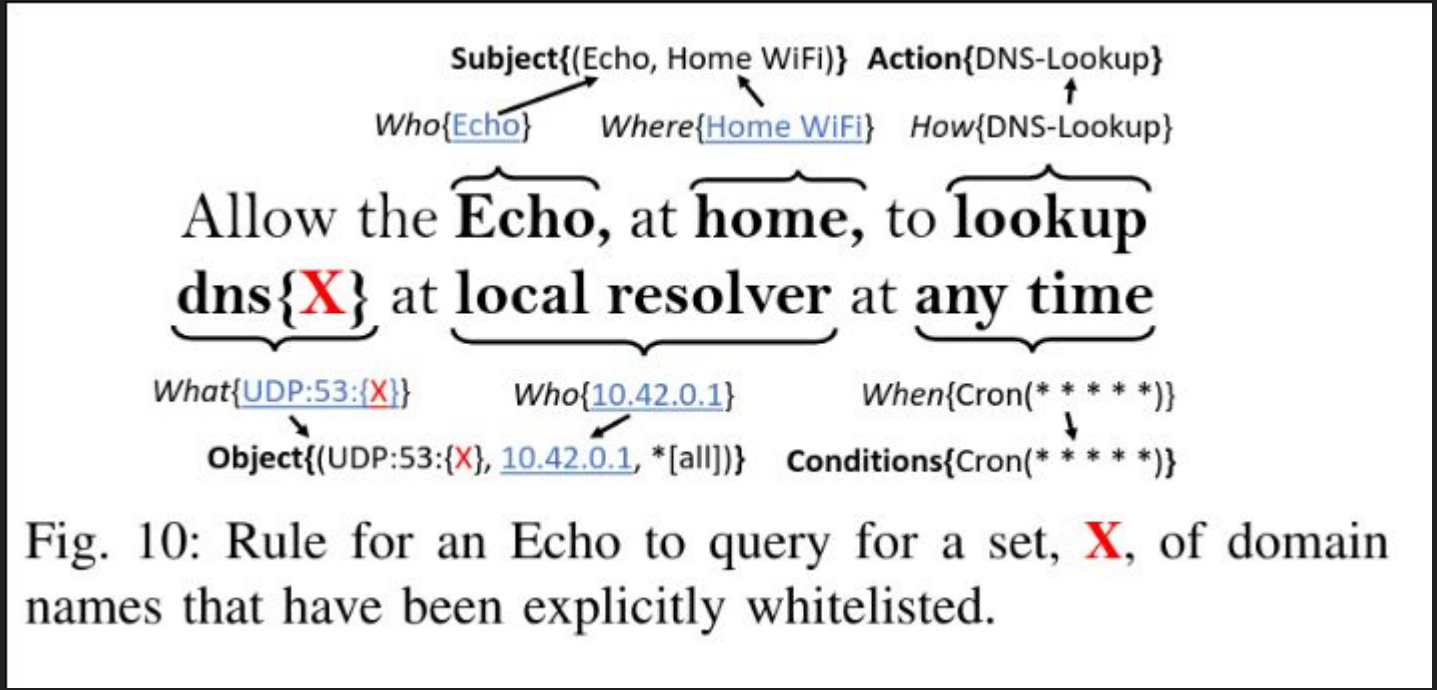


Fig. 10: Rule for an Echo to query for a set, **X**, of domain names that have been explicitly whitelisted.

Who would implement this system?

Questions

- @pcodes: Can this system scale in terms of human cost?
- @s-hanna15: Users don’t change default passwords won’t they do the same with Bark?
- @marcusgillesyoung: Path to adoption for Bark?

Critique

- Assumption that router won’t be compromised
- No meaningful results
- End users will make mistakes if given major role in maintaining security

Conclusion

- Default off networking aka whitelisting is a useful model for an IoT system where only a select number of outside devices should be communicating with said device.
- Bark implements default off networking in a end user readable yet powerful policy language.