Trustless IoT: A Logic Driven Architecture for IoT Hubs

Soumya Basu Emin Gün Sirer

HotEdge
June 26, 2020

Internet of Things

- 5.8 billion IoT devices by the end of 2020
  - 20% increase from 2019
- Affects many major sectors of the economy

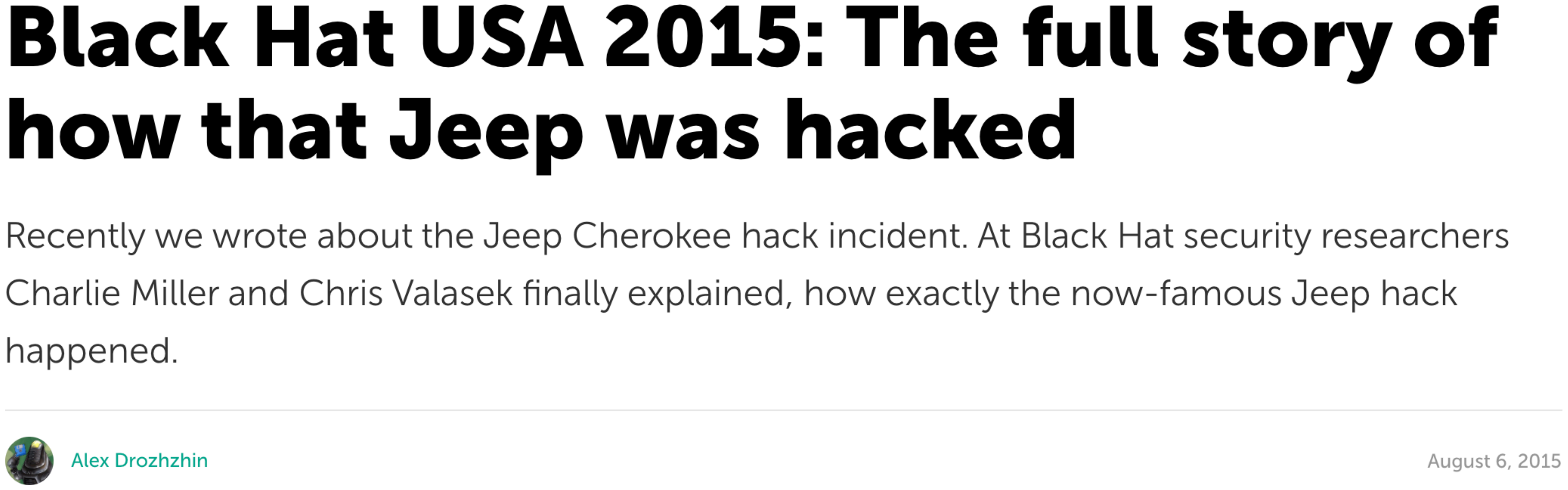
Emerging Architecture

- Centralized hubs are the dominant emerging architecture

- Small number of hubs effectively control 5.8 B devices
- Why hubs are here to stay:
  - Simplicity of administration and control
  - Limited vendors due to economies of scale
  - Limited communication modalities on devices

What about security?

- The state of IoT security is poor (the “s” is for security)
  - Device security
  - Hub security
- Many examples of unauthorized access to devices



Black Hat USA 2015: The full story of how that Jeep was hacked

Recently we wrote about the Jeep Cherokee hack incident. At Black Hat security researchers Charlie Miller and Chris Valasek finally explained, how exactly the now-famous Jeep hack happened.

Alex Drozhzhin

August 6, 2015

What about security?

- The state of IoT security is poor (the “s” is for security)
  - Device security
  - Hub security
- Many examples of unauthorized access to devices

Black Hat USA 2015: The full story of

h

Re

Ch

ha

Alex Drozhzhin

August 6, 2015

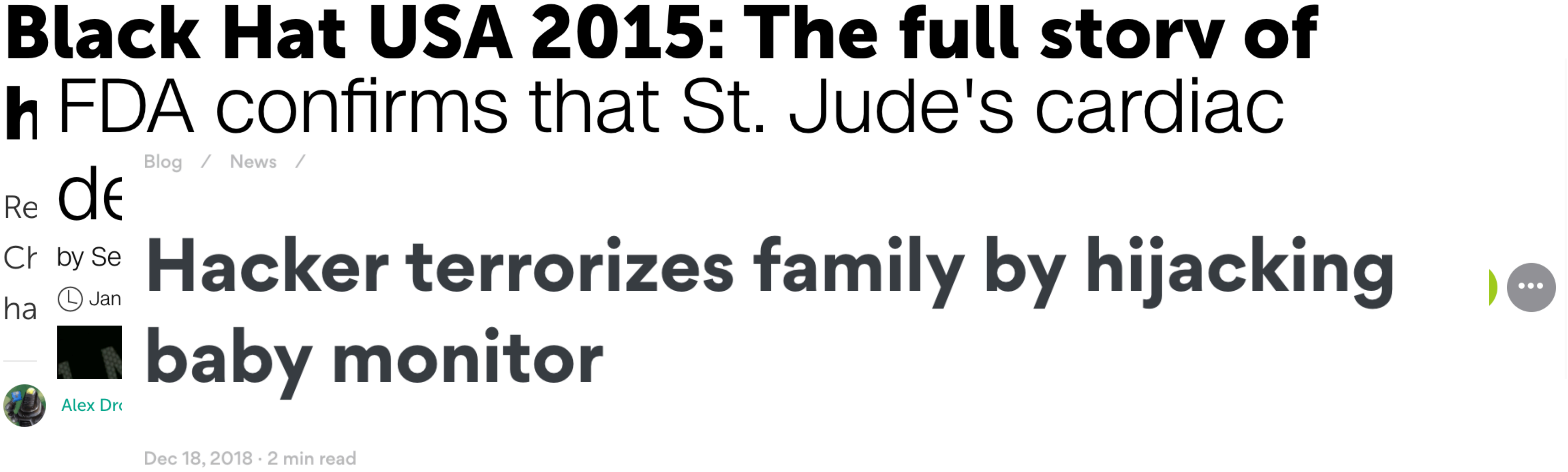
FDA confirms that St. Jude's cardiac devices can be hacked

by Selena Larson @selenalarson

January 9, 2017: 3:53 PM ET

What about security?

- The state of IoT security is poor (the “s” is for security)
    - Device security
    - Hub security
- Many examples of unauthorized access to devices



Black Hat USA 2015: The full story of

h

FDA confirms that St. Jude's cardiac

de

Re

Ch

ha

by Se

Jan

Alex Dr

Blog / News /

Hacker terrorizes family by hijacking baby monitor

Dec 18, 2018 · 2 min read

Why is security poor?

- Root cause: Implicit full trust in the hub
- Hubs are:
  - In the TCB of every device
  - Always on and internet connected
  - Can commandeer any action on any actuator
- Hub compromise can hurt national security

OrbanHub Proposal

- A modified IoT architecture where hubs cannot misbehave
  - Byzantine hub is constrained in its actions
- Safety: No command executed by any device unless authorized by user policy
- Liveness: All commands that should be executed will eventually execute
- Lightweight, incrementally deployable

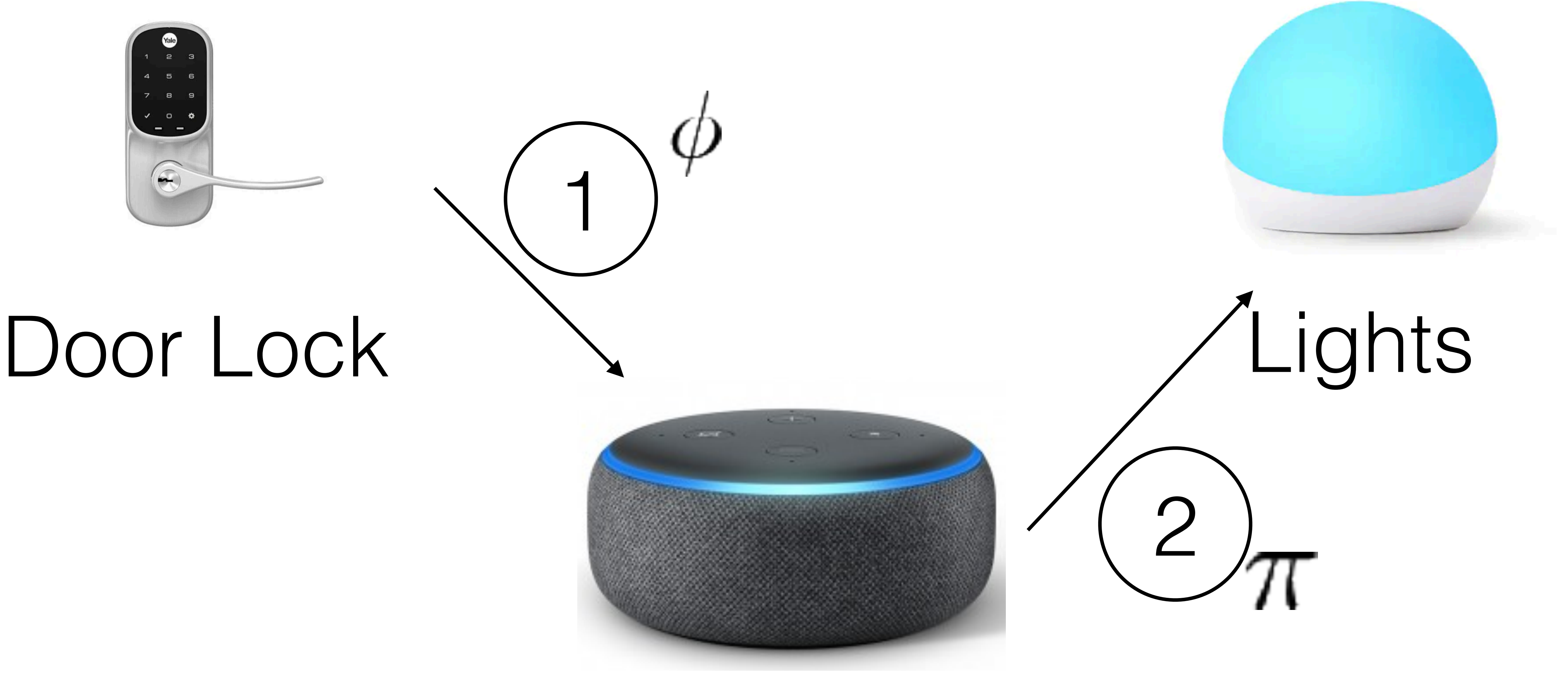
Guaranteeing Safety

- *Proof carrying statements* (PCS) ensure safety
    - Actions sent from the hub to actuators must be accompanied by a proof that they were authorized by the user's policy
- Sensors upload cryptographically signed statements that serve as inputs to proofs
- Hubs are tasked with creating PCS and cannot engage in actions unjustified by a policy

Sample Proof

- User policy: “If door is open, lights turn on” ($\rho : \phi \implies \tau$)
- Door sensor: Door is open. (ϕ)
- User inference (π):
    - Door sensor says $\phi \implies$ User says ϕ
    - User infers: $\rho \wedge \phi \implies \tau$ (“lights turn on”)
- Light actuator then turns on due to user inference

Control Flow



Hub

$$\rho : \phi \implies \tau$$

Guaranteeing Liveness

- All statements are logged using a hash chain
  - Hashchains constrain hub to deleting tail of log
- All devices are required to send periodic updates
  - Prevents hub from withholding update forever
- If a device is quiet, then failure alert is generated
  - Range of potential fallback mechanisms

New Way Forward

- IoT is becoming more ubiquitous
- Attacks become more lucrative
    - Security is a first class concern
- OrbanHub is a new, trustless IoT model
    - Works with existing architecture
    - Limited overhead on devices

Thank you!

- Questions?
- Contact: soumya@cs.cornell.edu