

Towards an Architecture for Trusted Edge IoT Security Gateways

Matt McCormack, Amit Vasudevan, Guyue Liu,
Sebastián Echeverría, Kyle O'Meara, Grace Lewis, Vyas Sekar

**Carnegie
Mellon
University**



Software Engineering Institute
CarnegieMellon

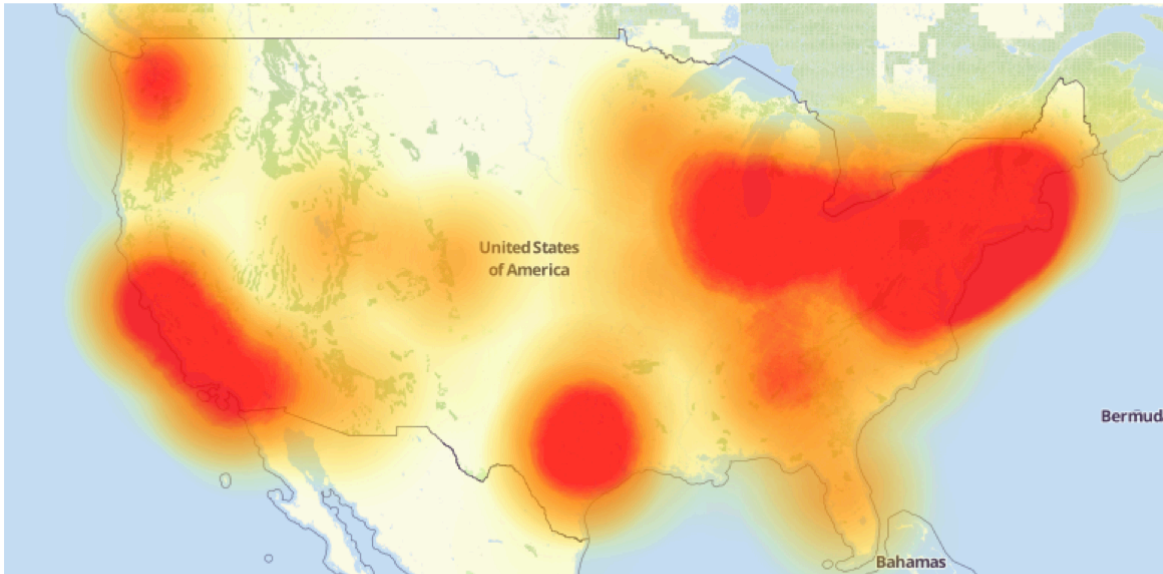
IoT Insecurity is Growing

Mirai Botnet Shows Just How Vulnerable the IoT Really Is

iotsecurityfoundation.org

**21 Hacked Cameras, DVRs Powered Today's
Massive Internet Outage**

OCT 16



krebsonsecurity.com

How a fish tank helped hack a casino

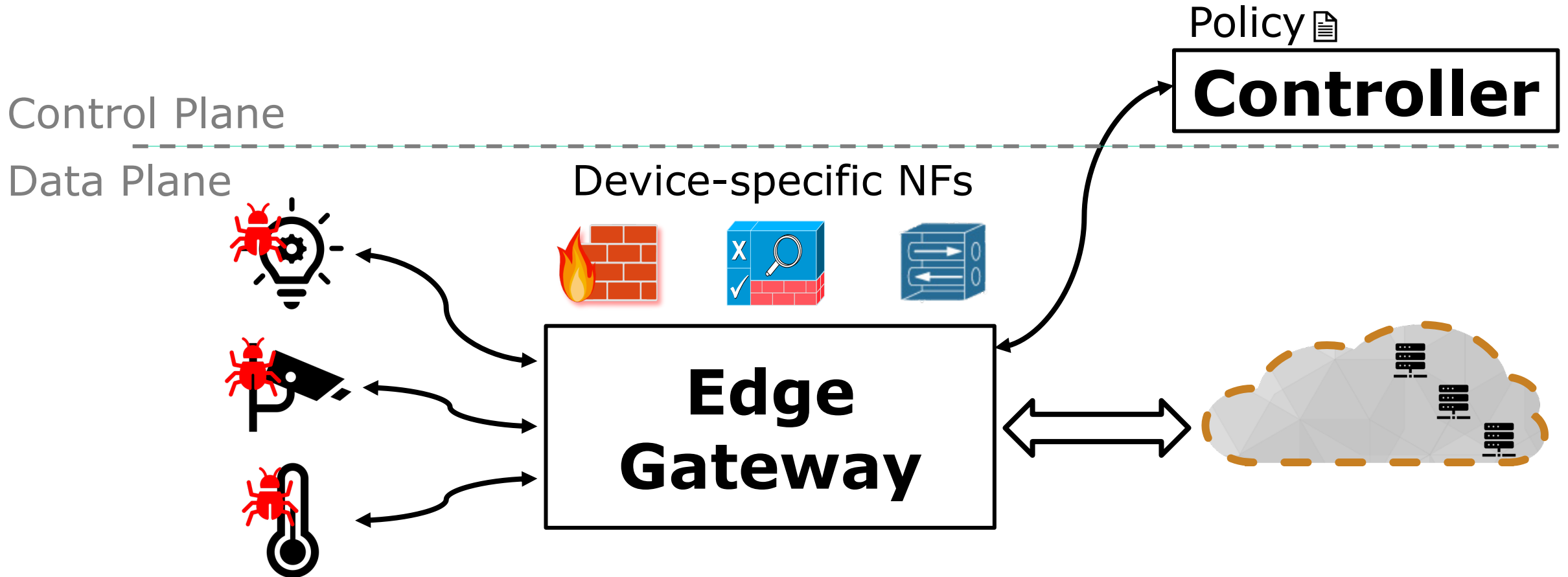
washingtonpost.com

**An Elaborate Hack Shows How
Much Damage IoT Bugs Can Do**

Rube-Goldbergesque IoT hacks are surprisingly simple to pull off—and can do a ton of damage.

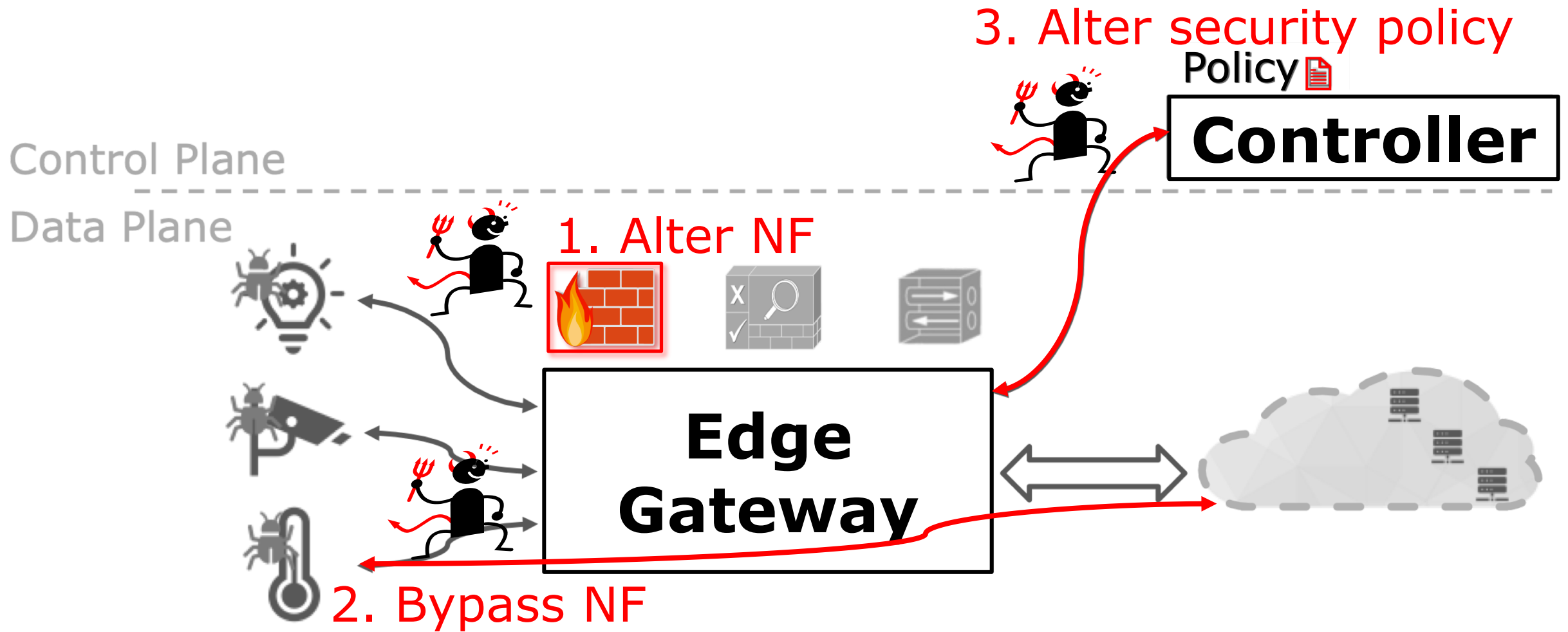
wired.com

Prior Work: “Bolt-on” Security Gateways



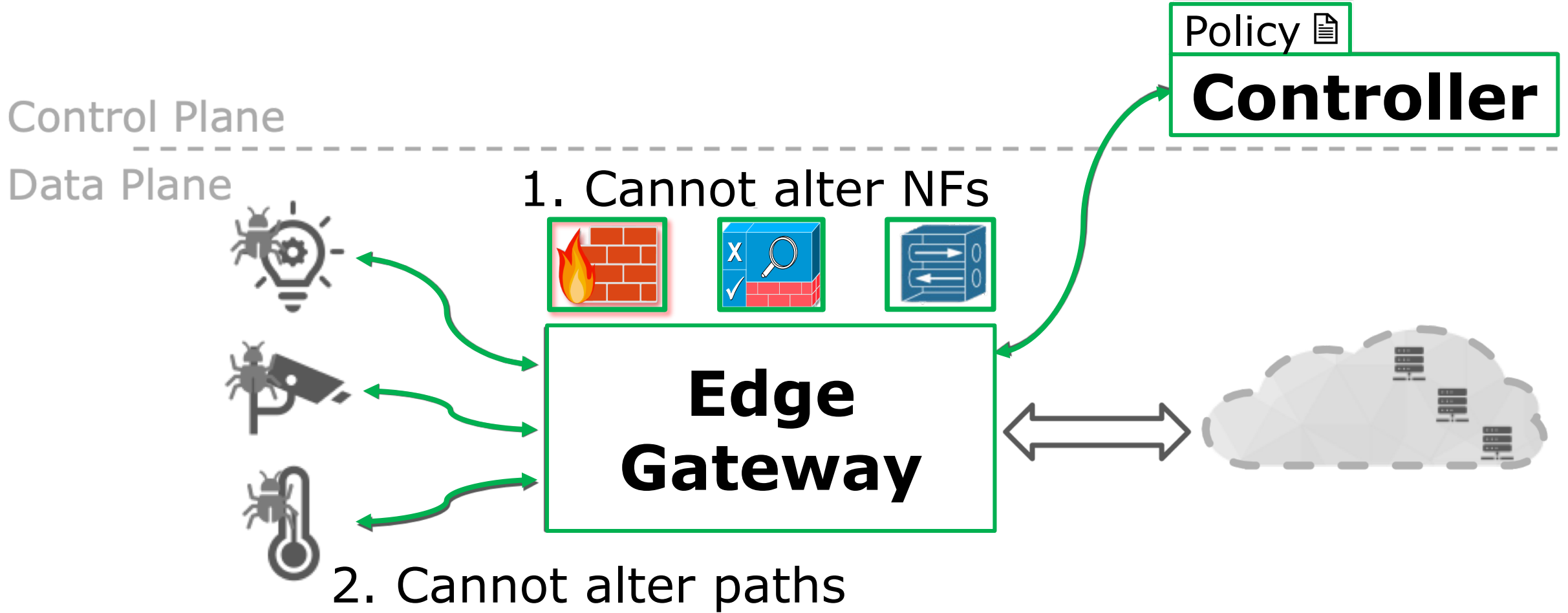
Advantages: practical, deployable, agile

Problem: Edge Gateways are Insecure



Our Vision: Trusted “Bolt-on” Security

3. Cannot alter policy



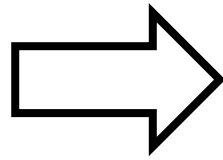
Requirements

Holistic Coverage

- Data plane
- Control plane

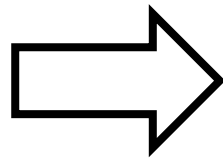
Aligns with “Bolt-on” Security Gateways

- General
- Legacy compatible
- Performant



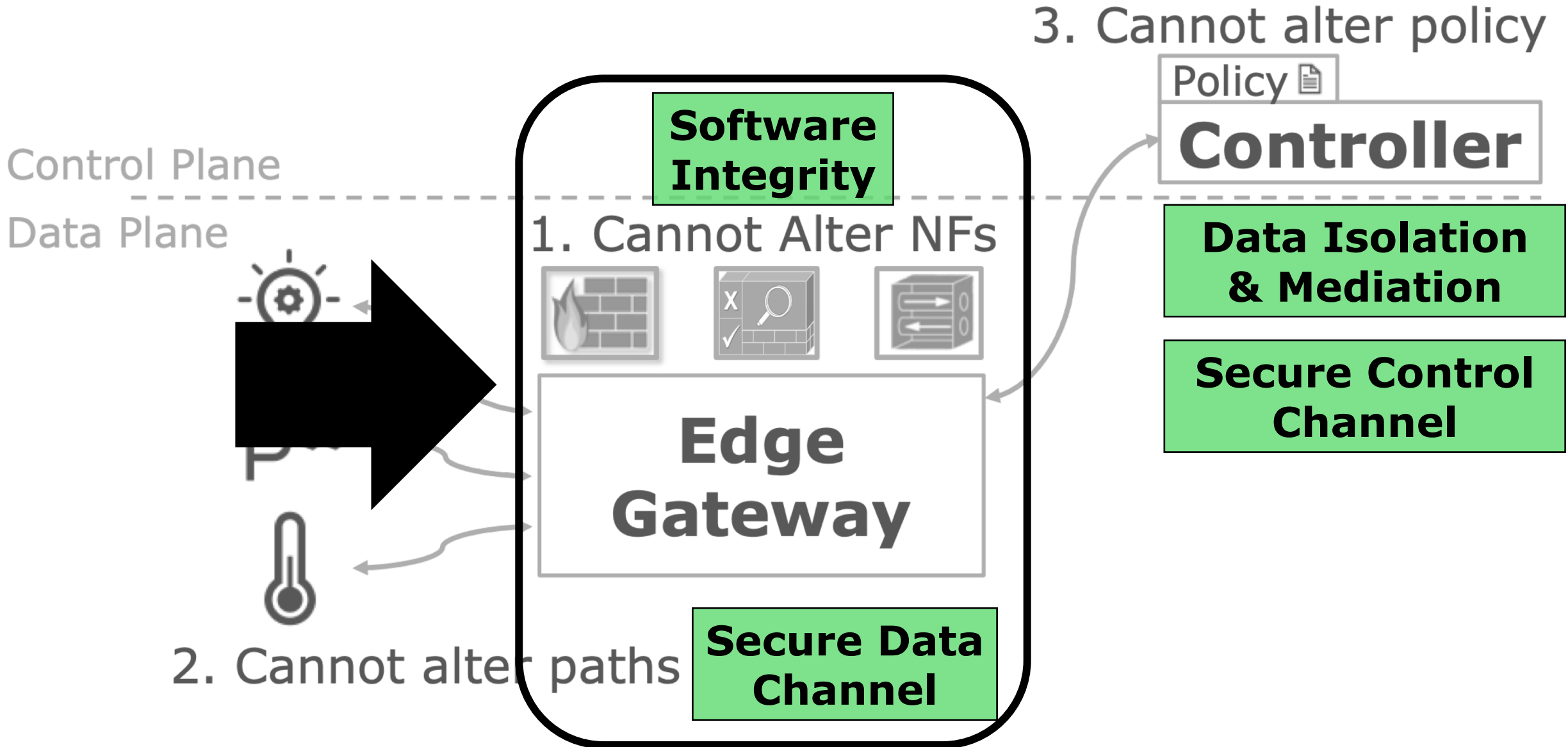
Contributions

Key security properties of a trusted gateway

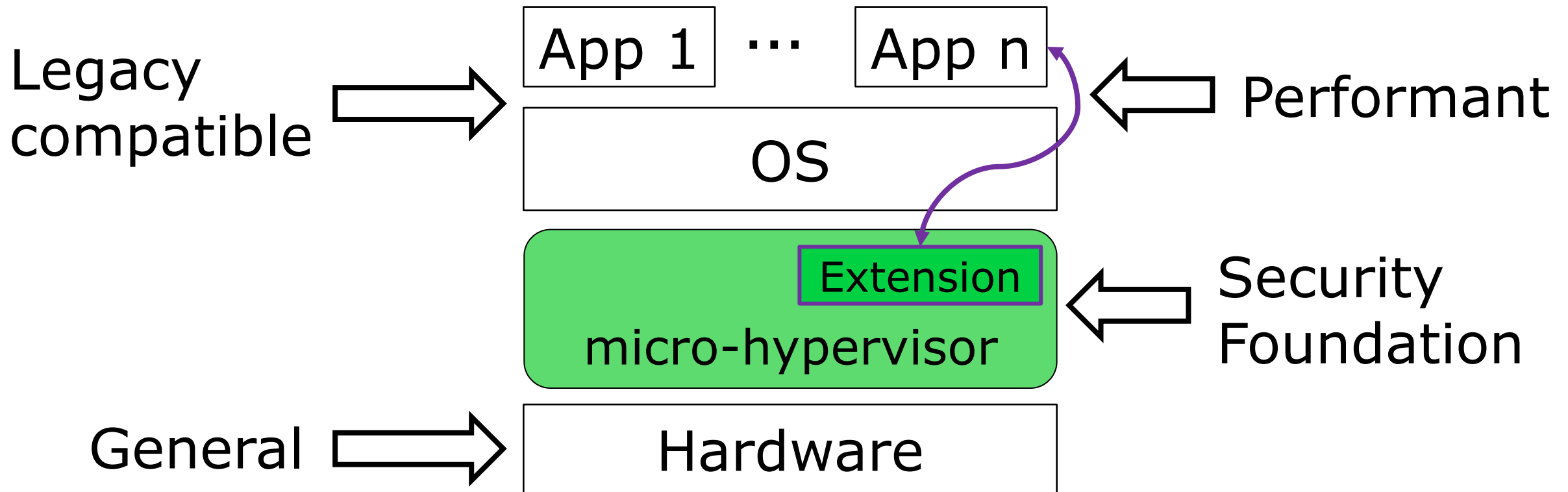


Trusted gateway architecture built on a micro-hypervisor

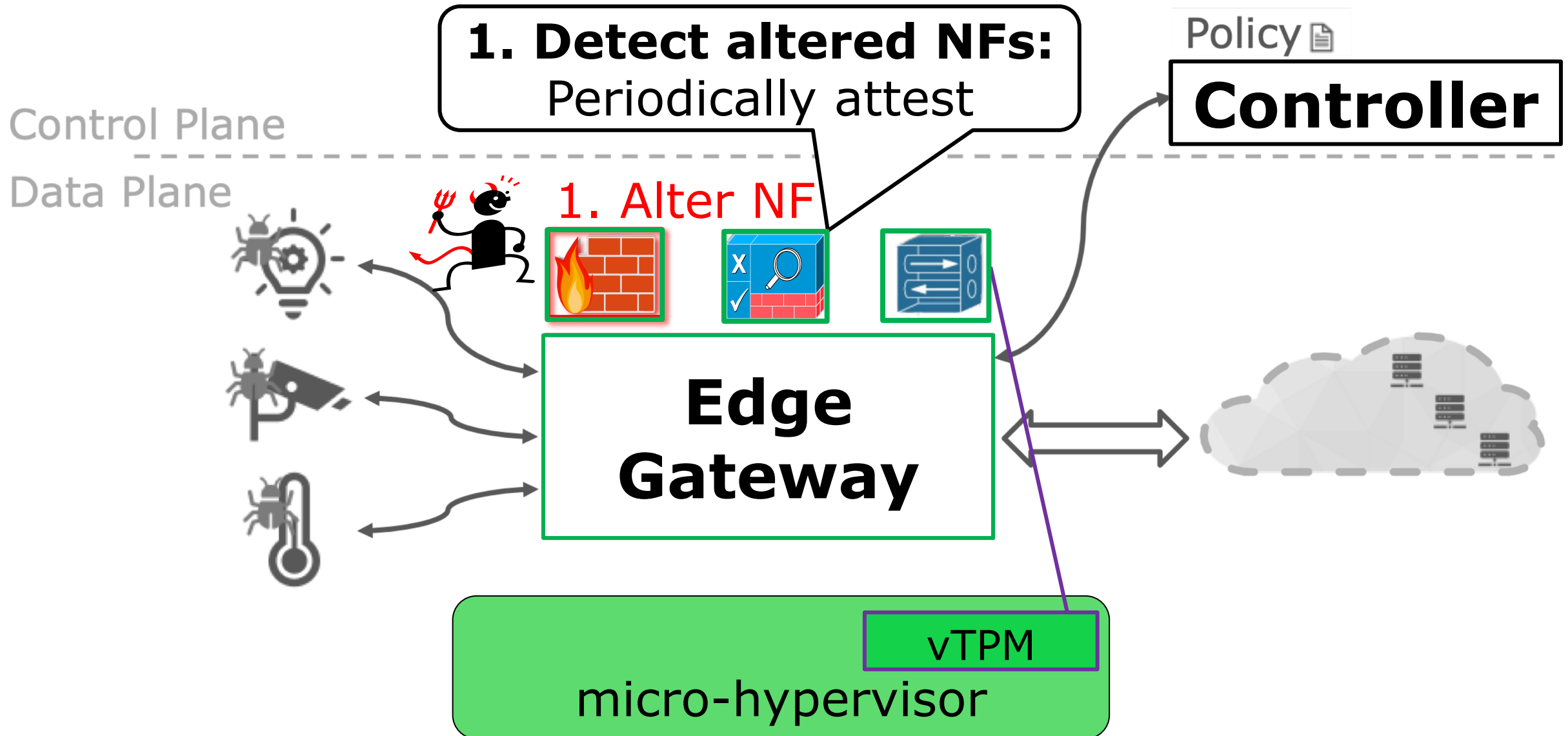
Foundational Security Properties



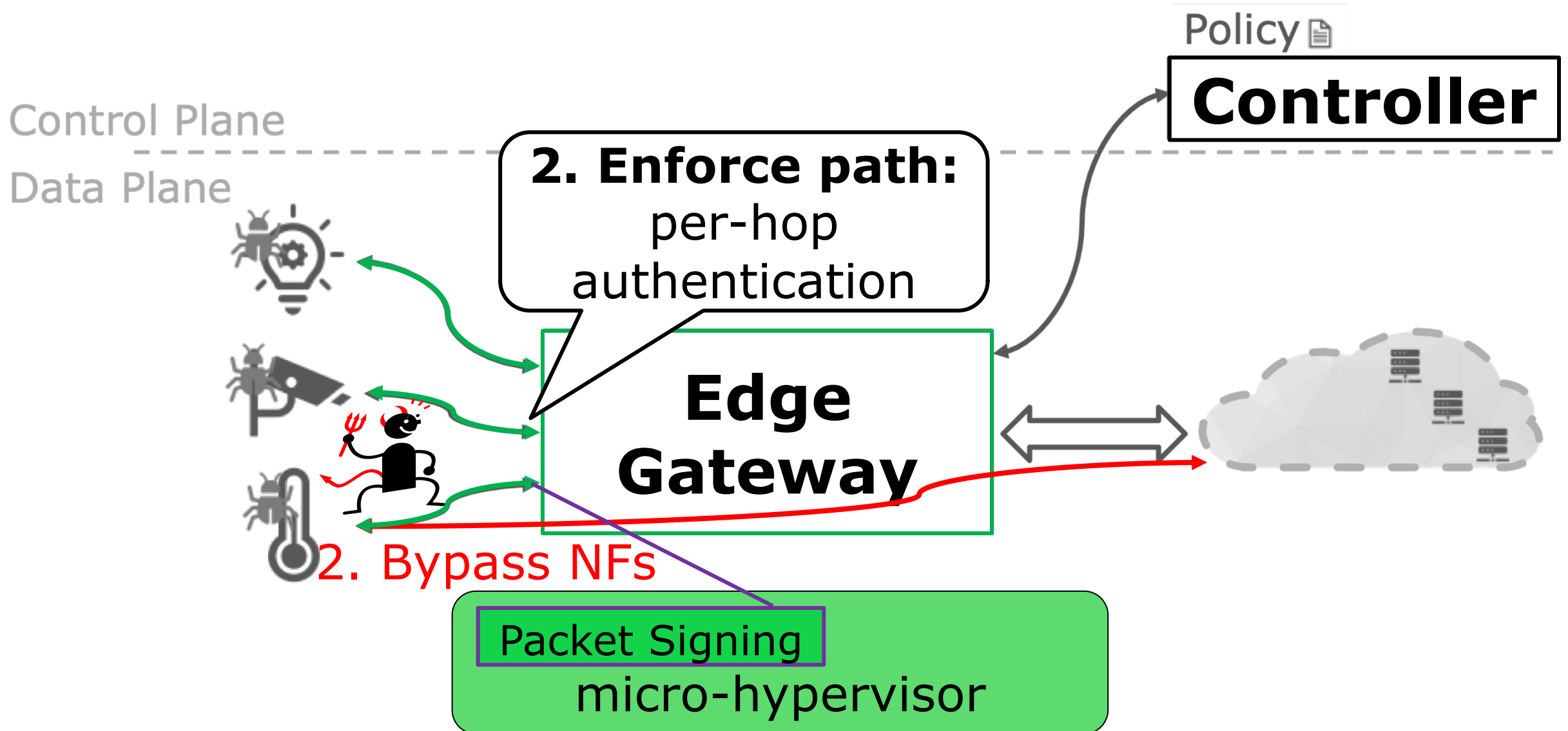
Background: Extensible Micro-Hypervisor



Trusted Data Plane Approach



Trusted Data Plane Approach



Promising Preliminary Results

Prototype on Raspberry Pi 3

- Micro-hypervisor: uberXMHF (<https://uberxmhf.org>)



Data plane: Packet Signing Extension

- OVS & Docker: +13% latency

Control plane: Policy Extension

- Custom controller: +17% latency

Conclusions

- Edge gateways offer hope for IoT security
 - Currently these gateways lack trust
- Vision for trusting edge IoT security gateways
 - Defined a holistic adversary model to derive our foundational trust properties
 - High-level architecture for trusted data and control plane built on top of a micro-hypervisor
- Thank you!
 - Contact: mccorm1@andrew.cmu.edu