KalKi: High Assurance Software-Defined IoT

Sebastian Echeverria

[DISTRIBUTION STATEMENT A

This material is based upon work funded and supported by the Department of Defense under Contract No. FA87 Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construe Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATE ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER E IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE ME DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMA INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Pl notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic fo formal permission. Permission is required for any other use. Requests for permission should be directed to the So Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon Universi

DM19-1077

© 2019 Carnegie Mellon University

- Security concerns over **untrusted supply chai** obstacle.

- We are developing a **solution that remains re** **trustworthy**, even in the presence of a powerfu

© 2019 Carnegie Mellon University

devices to breach networks

arstechnica

arstechnica

Latest Mirai variant targets routers and other IoT devices using 13 exploits

cyware.com

A 100,000-router b
feeding on a 5-yea
bug in Broadcom c

arstechnica

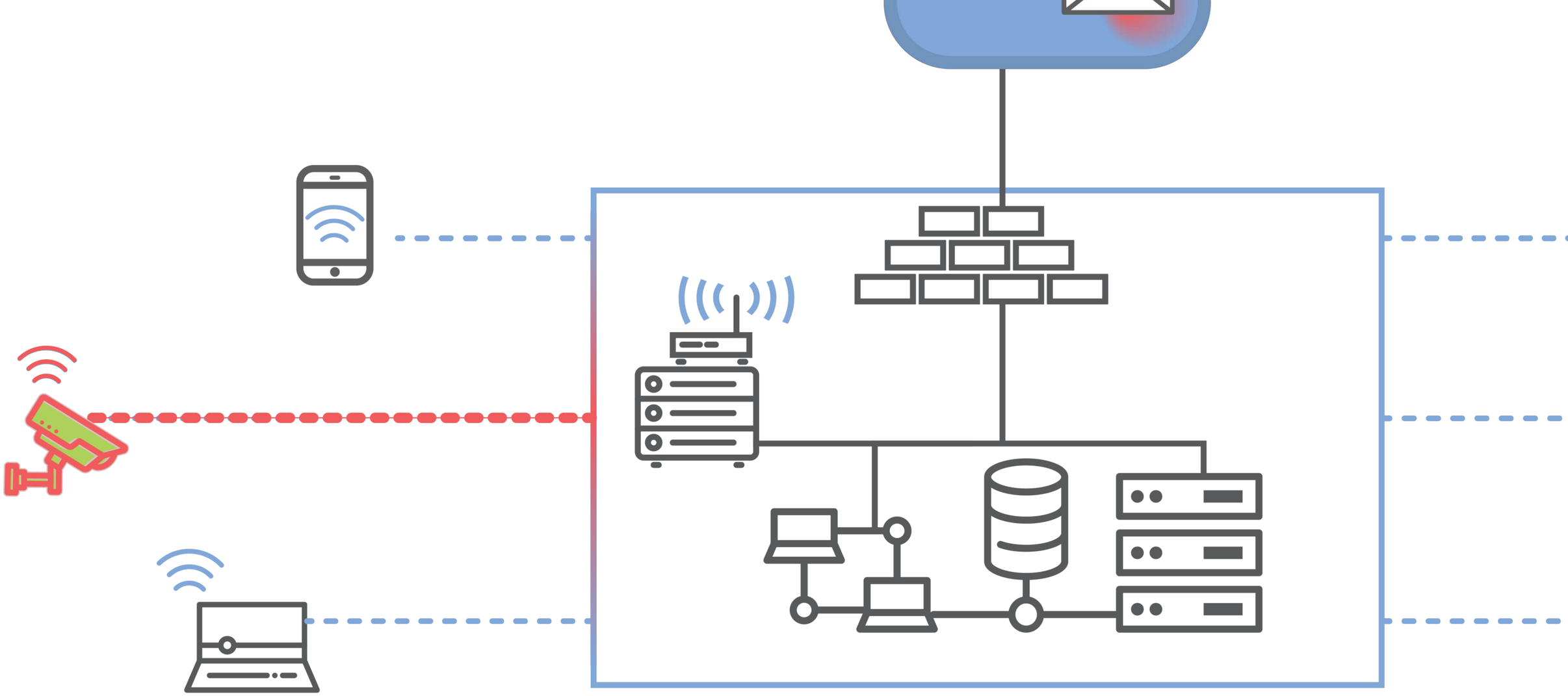
Your smart air conditioner could help bring down

Hacked appliances could overwhelm the grid, resear

cnet.com

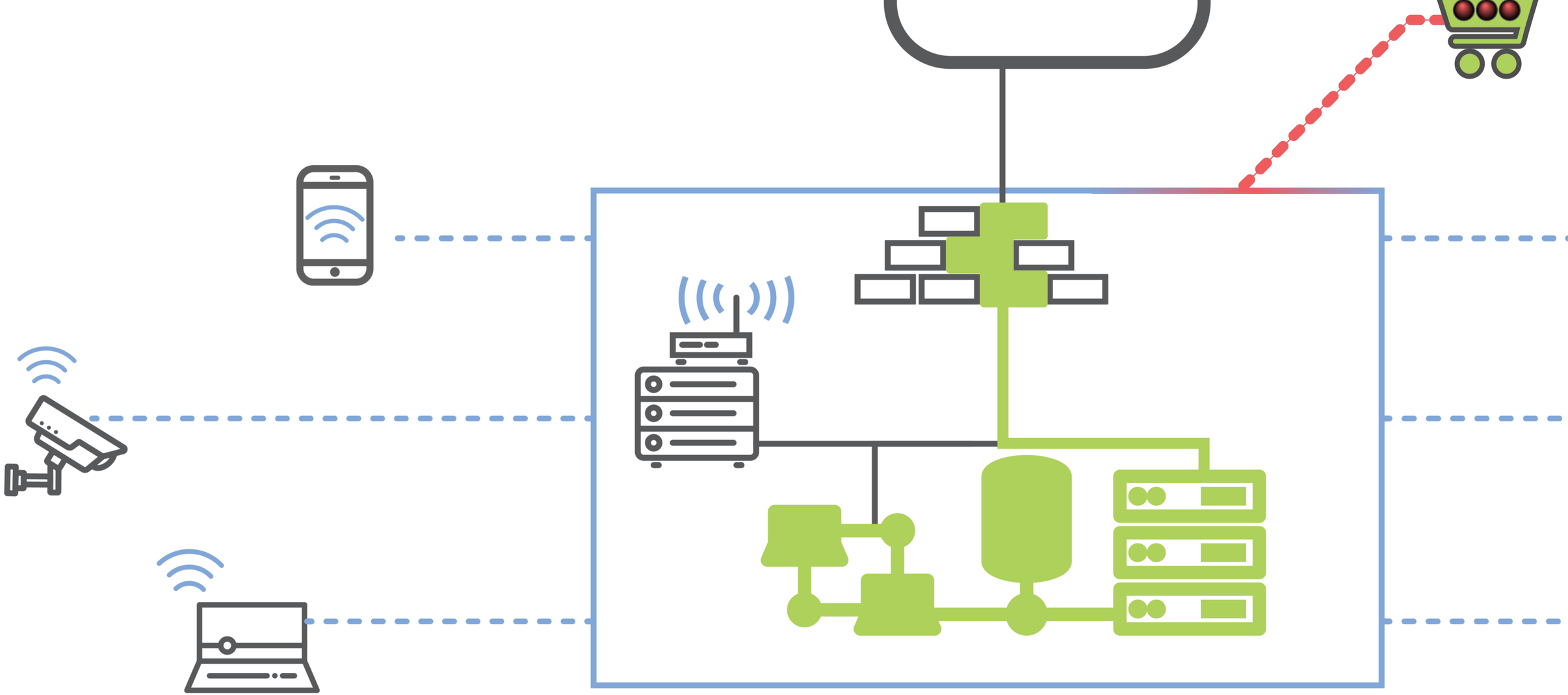
© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Appr



© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Appr



© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Appr

Solution: Move Security Enforcement to the Network

Create an IoT security platform highly resilient to a collection of presc

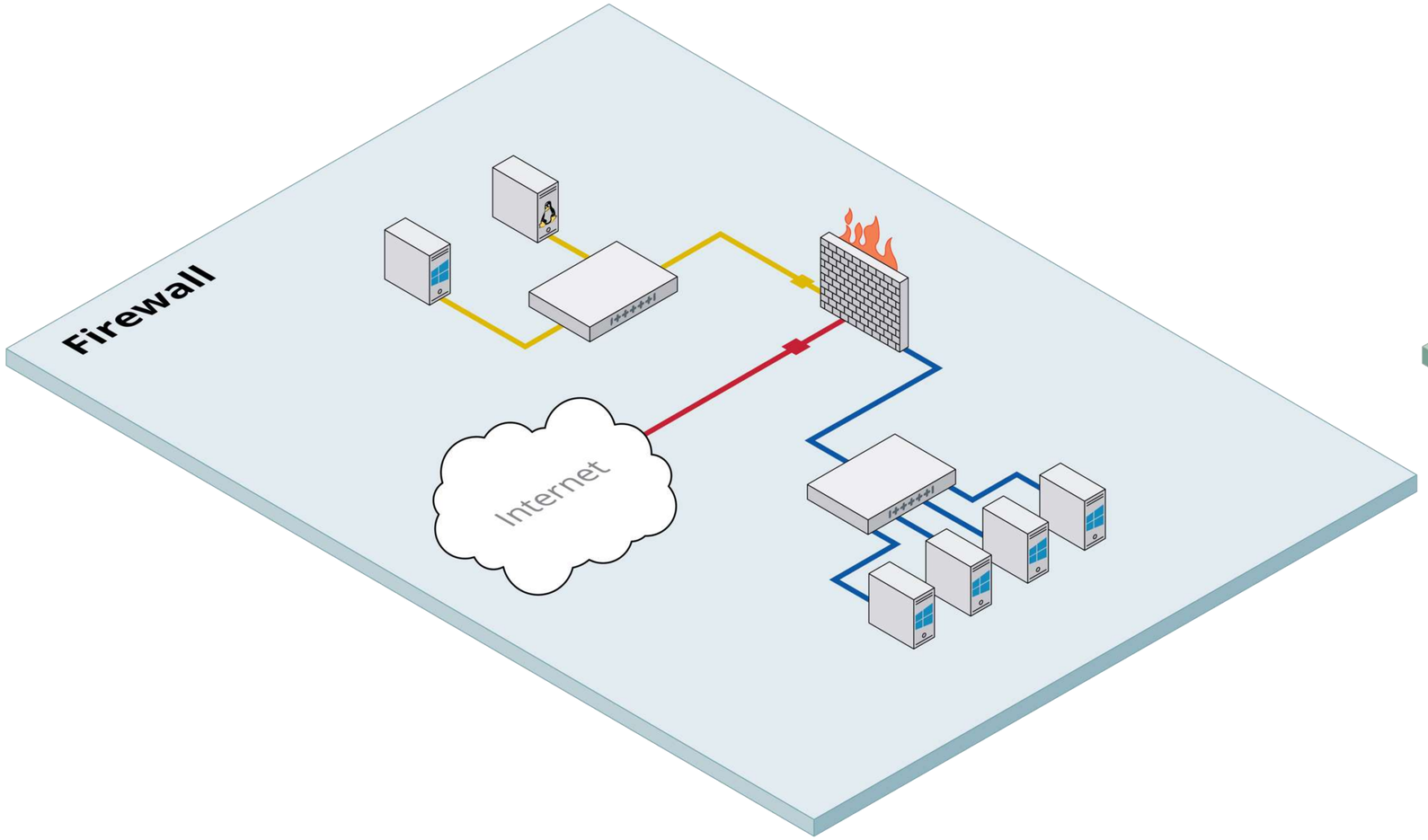
- Enables the integration of IoT devices into DoD networks
- Protects the networks even if the IoT devices are not fully trusted o

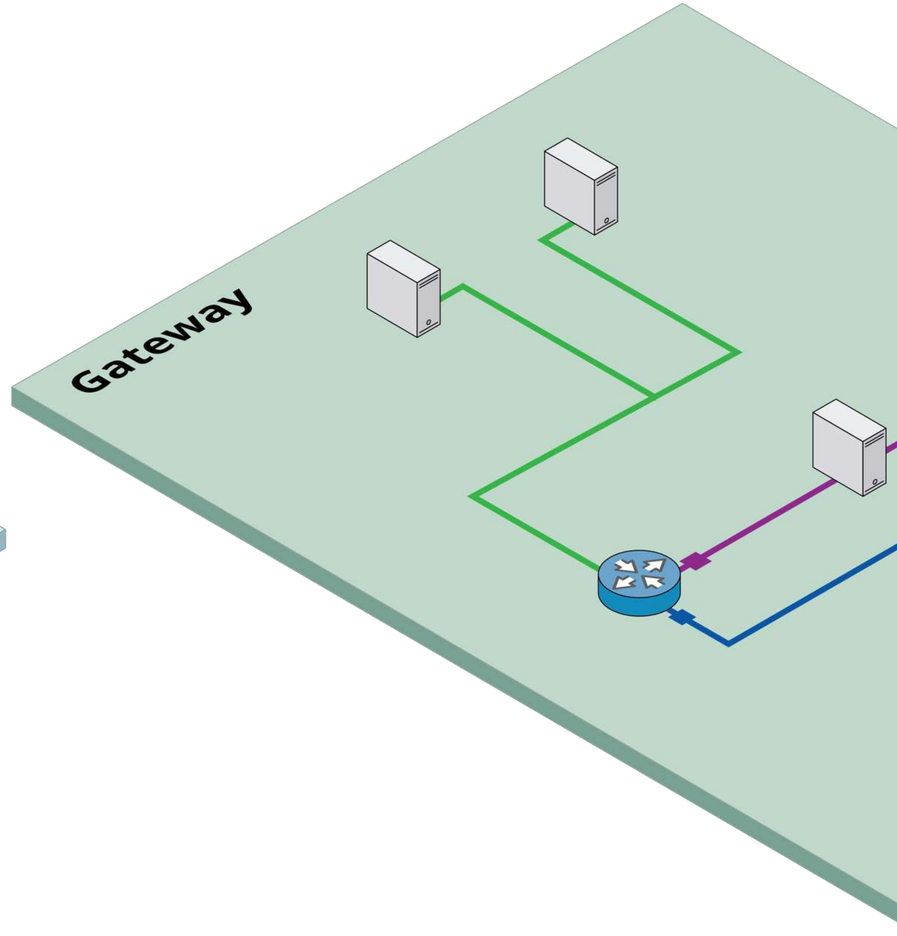
The term “KalKi” is of Sanskrit origin, and it is the name of an a
the god Vishnu, the destroyer of filth and bringer of purity, truth a

© 2019 Carnegie Mellon University

- Are not device-specific
- Cannot adapt to changing security states

- Can become compromi

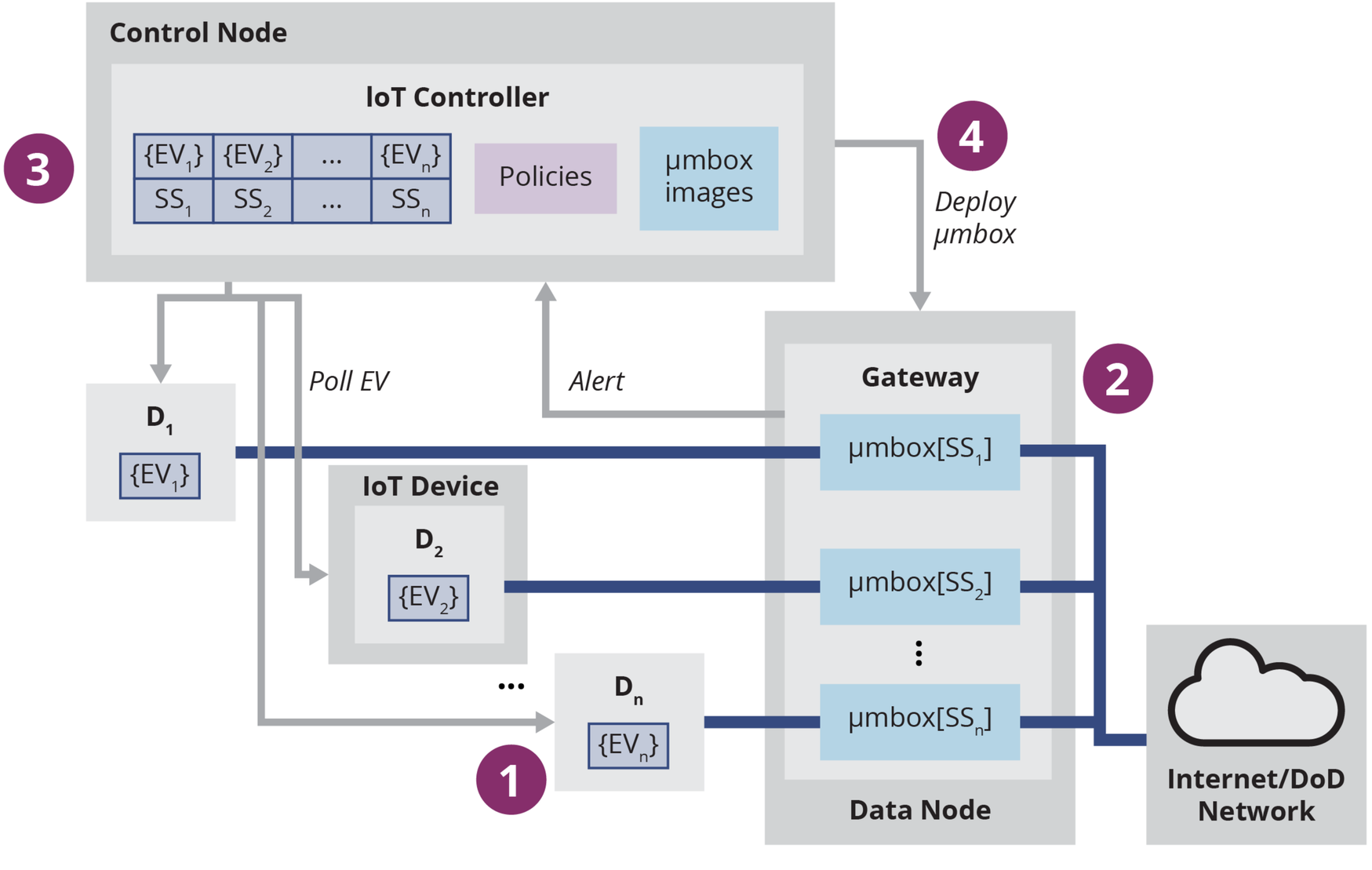




© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Appr

create a highly dynamic IoT security platform.



1. Each IoT devi
set of environ

2. Network traffic
tunneled throu
implement the
for the device'
µmbox[SS_1]
µmbox[SS_2]

3. IoT controller m
statespace cor
security state (
SS = {Norma

4. Changes in the
evaluated by p
the deploymen

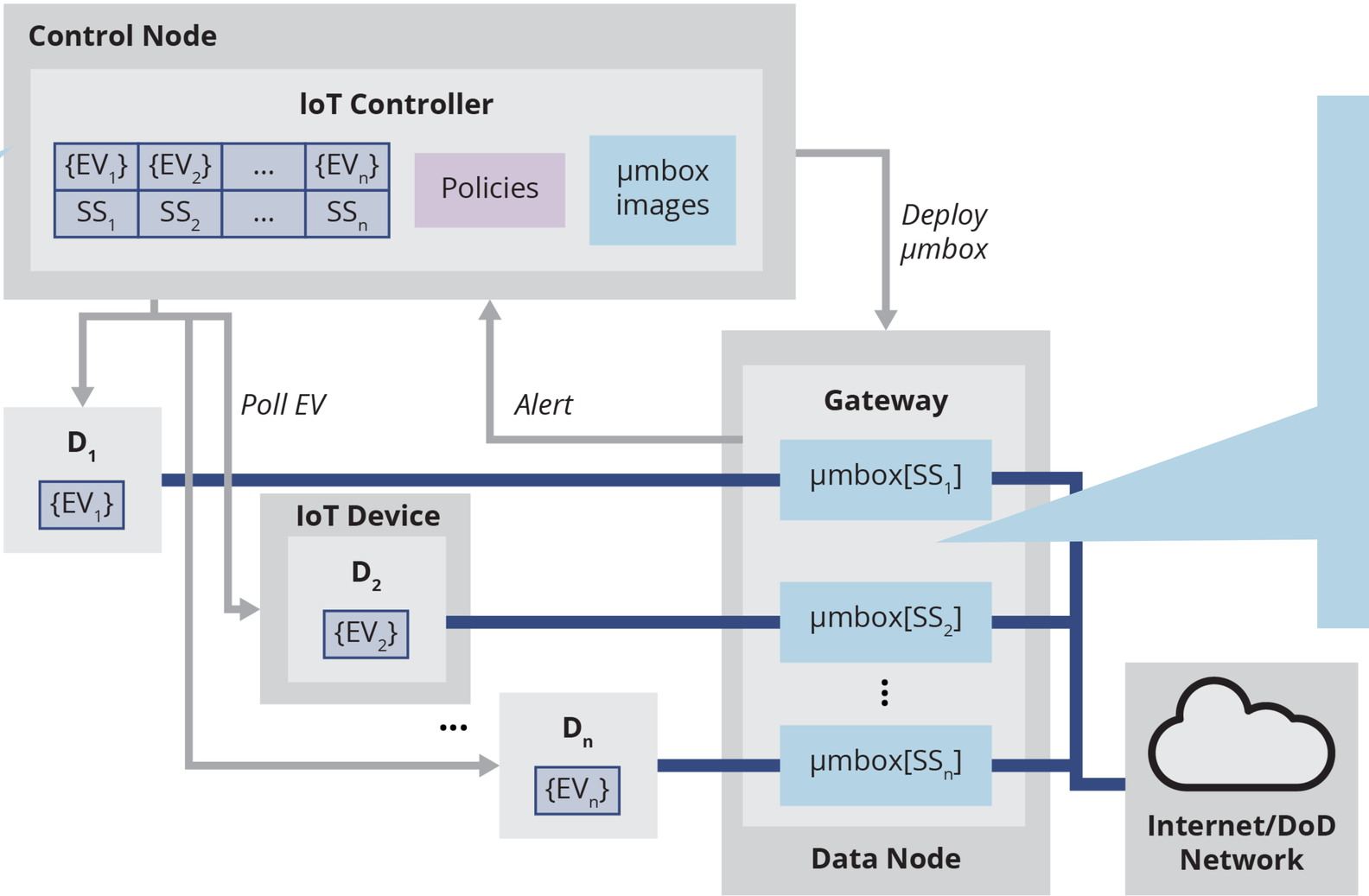
© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Appr

defined IoT security platform using uberSpark/uberXMHF, a framework
secure software stacks.

Control Node Properties

- Policy data integrity, including security state machine



© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Appr

Initial Threat Model to guide development

Policy Model to set conditions to change security state, and actions to be taken

Initial Architecture and prototype of the IoT Security Platform

FUNCy Views (Secure) system architecture: hardware-assisted, low-latency, low-TCB, compartmentalization of legacy code on x86 platforms

© 2019 Carnegie Mellon University

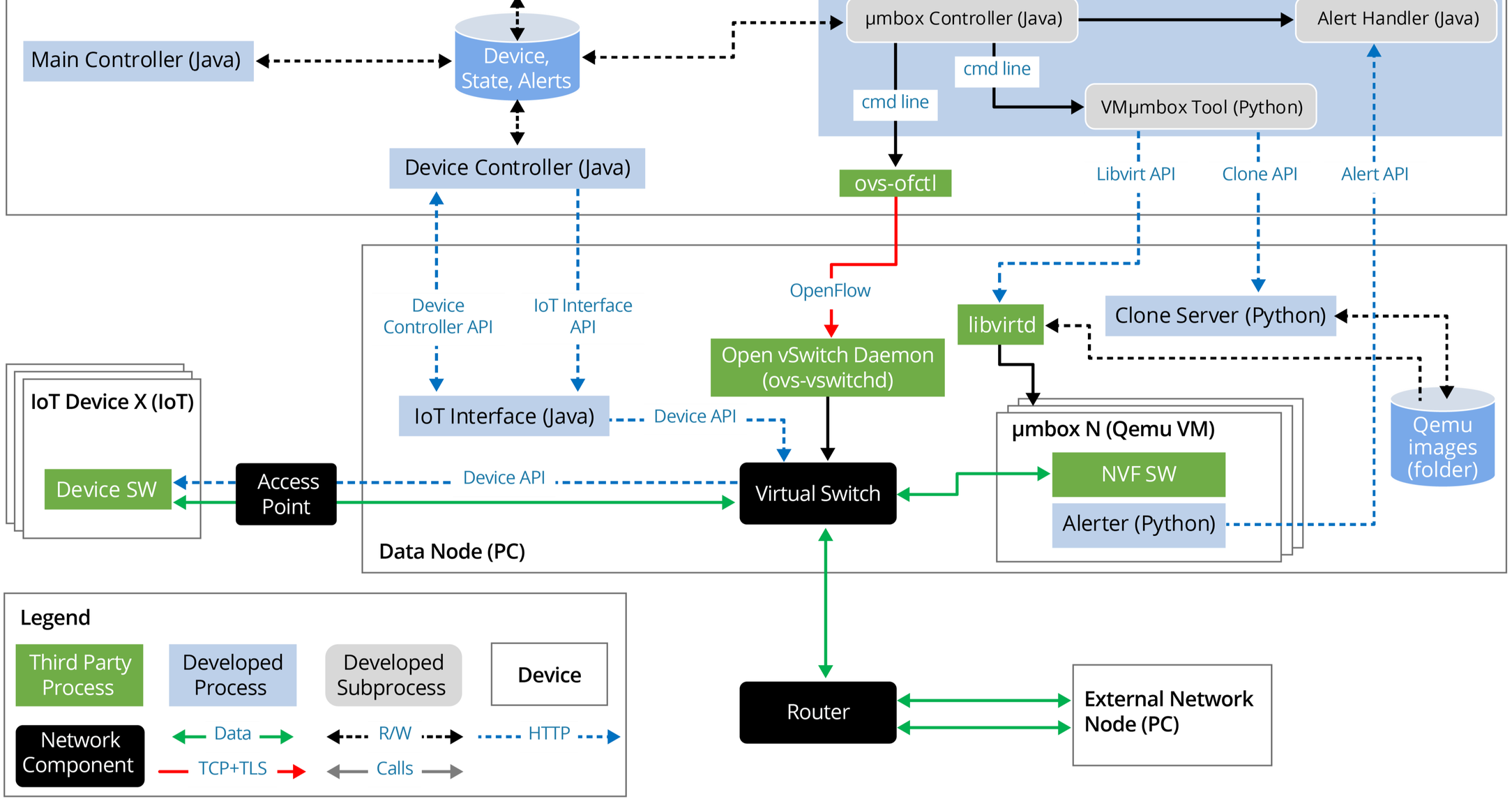
IoT Security Platform prototype full development

Dashboard Update

Creation of Policies and µmboxes for four representative IoT devices

Experiment to Test different scenarios an red team attacks

© 2019 Carnegie Mellon University



- Abl
  spe
- Sup
  poli
  sec
- Run
  har

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Appr

KalkiDashboard

Home | FUNCy View | DB Management

UNTS

State Reset

Udoo Neo

Type: **Udoo Neo**
IP Address: **10.27.151.101**
Tags:

Security State: **Normal**
Group: **N/A**

Alert History | Status History | Alert Conditions | State Transitions Reference | umBox Instances

Refresh

Show 10 entries Search:

Time	Attributes
Sep 13th 19, 9:40:36 am	accelerometerX: 0.013663999999999999 accelerometerY: -0.040504 accelerometerZ: -0.98576 gyroscopeX: 1.75 gyroscopeY: 0.8125 gyroscopeZ: 0.25 magnetometerX: 59.6 magnetometerY: 115.5 magnetometerZ: 53.900000000000006 tempinput: 0.0 tempmax: 0.0 tempmax_hyst: 0.0
Sep 13th 19, 9:40:26 am	accelerometerX: 0.010003999999999999 accelerometerY: -0.041968 accelerometerZ: -0.995764 gyroscopeX: 2.1875 gyroscopeY: 0.625 gyroscopeZ: -0.1875 magnetometerX: 67.3 magnetometerY: 115.5 magnetometerZ: 40.7 tempinput: 0.0 tempmax: 0.0 tempmax_hyst: 0.0

Showing 1 to 2 of 2 entries Previous 1 Next

Carnegie Mellon University

KalkiDashboard

Hom

Device List

Show 10 entries

Device	Security State	Latest Alert
DLC	Normal	no alert history
Kalki	Normal	no alert history
PHLE	Normal	no alert history
UNTS	Normal	unts-acceleration

Showing 1 to 4 of 4 entries

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Appr

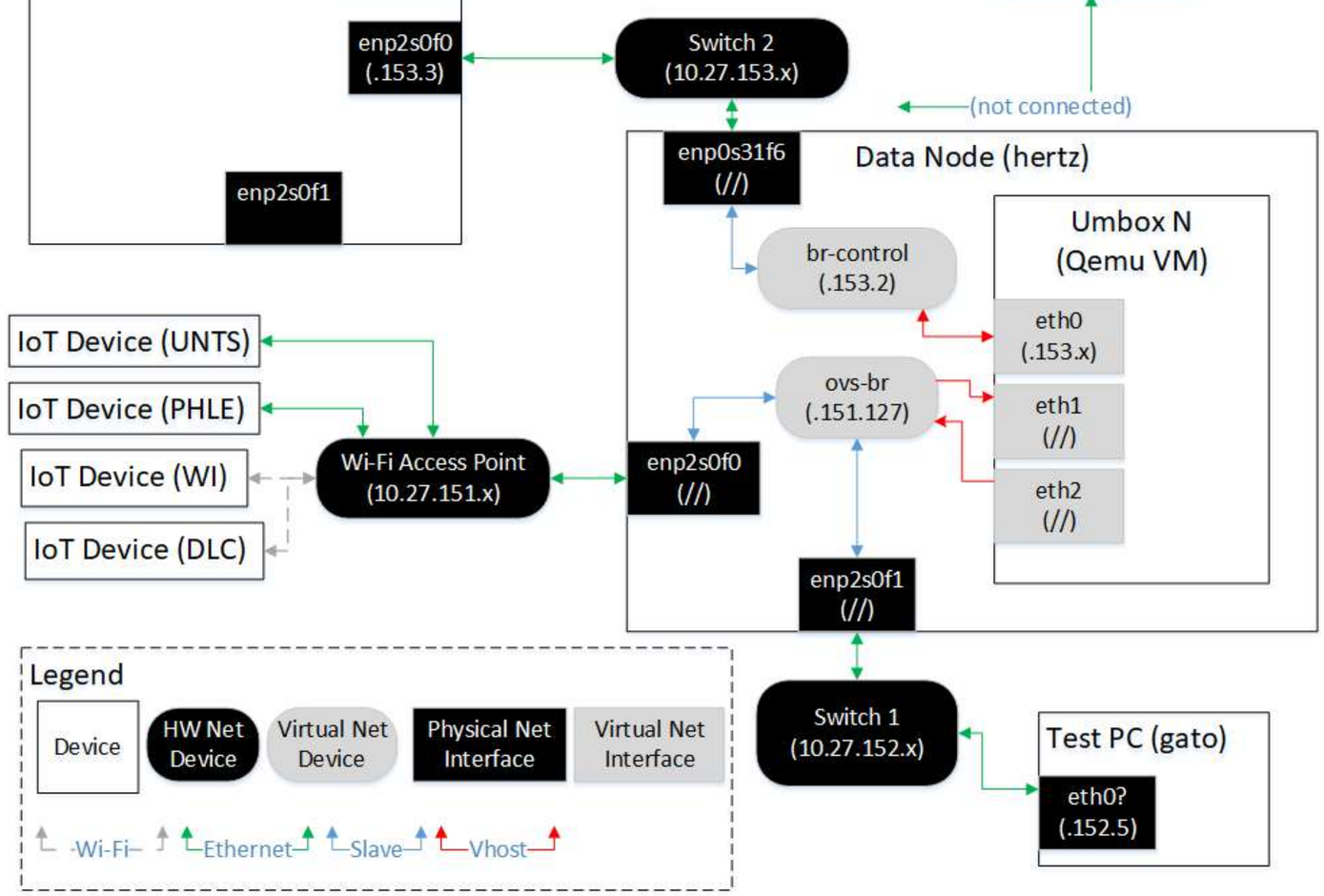
Smart Plug

Temperature Sensor

IP Camera

© 2019 Carnegie Mellon University

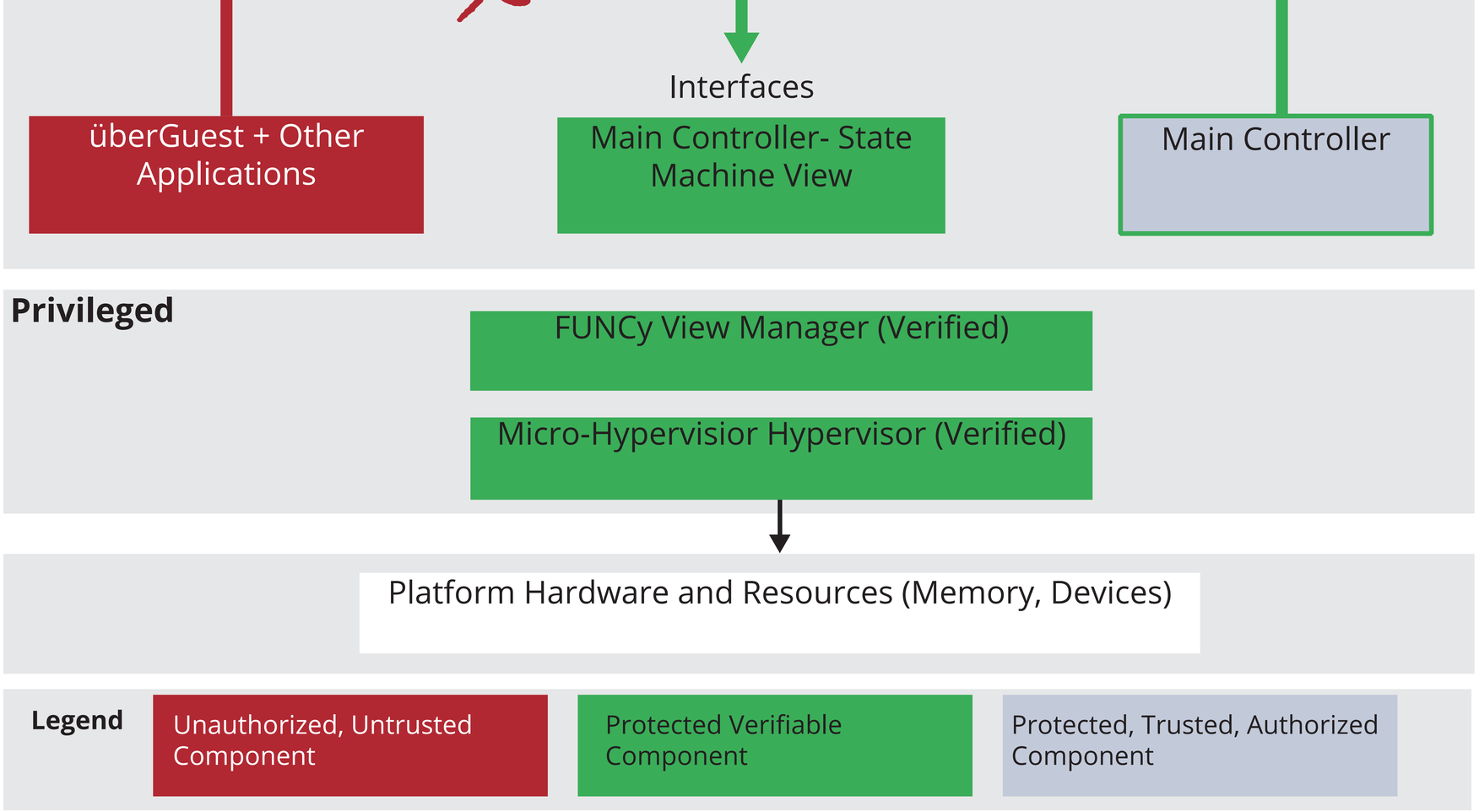
[DISTRIBUTION STATEMENT A] Appr



measure:

- Resiliency to attacks
- Performance (time to re
- Scalability (effect of the devices in performance

© 2019 Carnegie Mellon University



machines using t
FUNCy views

- Verified, lightw
  hypervisor prot
  access
- Unauthorized a
  can’t access St
  encapsulated a

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Appr

- Integrate überXMHF security properties into prototype
- Simplify integration of new devices and policies
- Increase performance and reduce resource utilization

- Transition activities — identify transition partners for validation, testi and adoption
  - Working with CMU liaisons for Navy (LCDR Christopher Lueken) and M (LCDR Jeff Greenwald)
  - Establishing contacts with organizations leading IoT projects, including Research Office (Durham), USAF Office of Scientific Research (Arlingto University
- Publication of results and open source release of platform code

© 2019 Carnegie Mellon University

NEAR

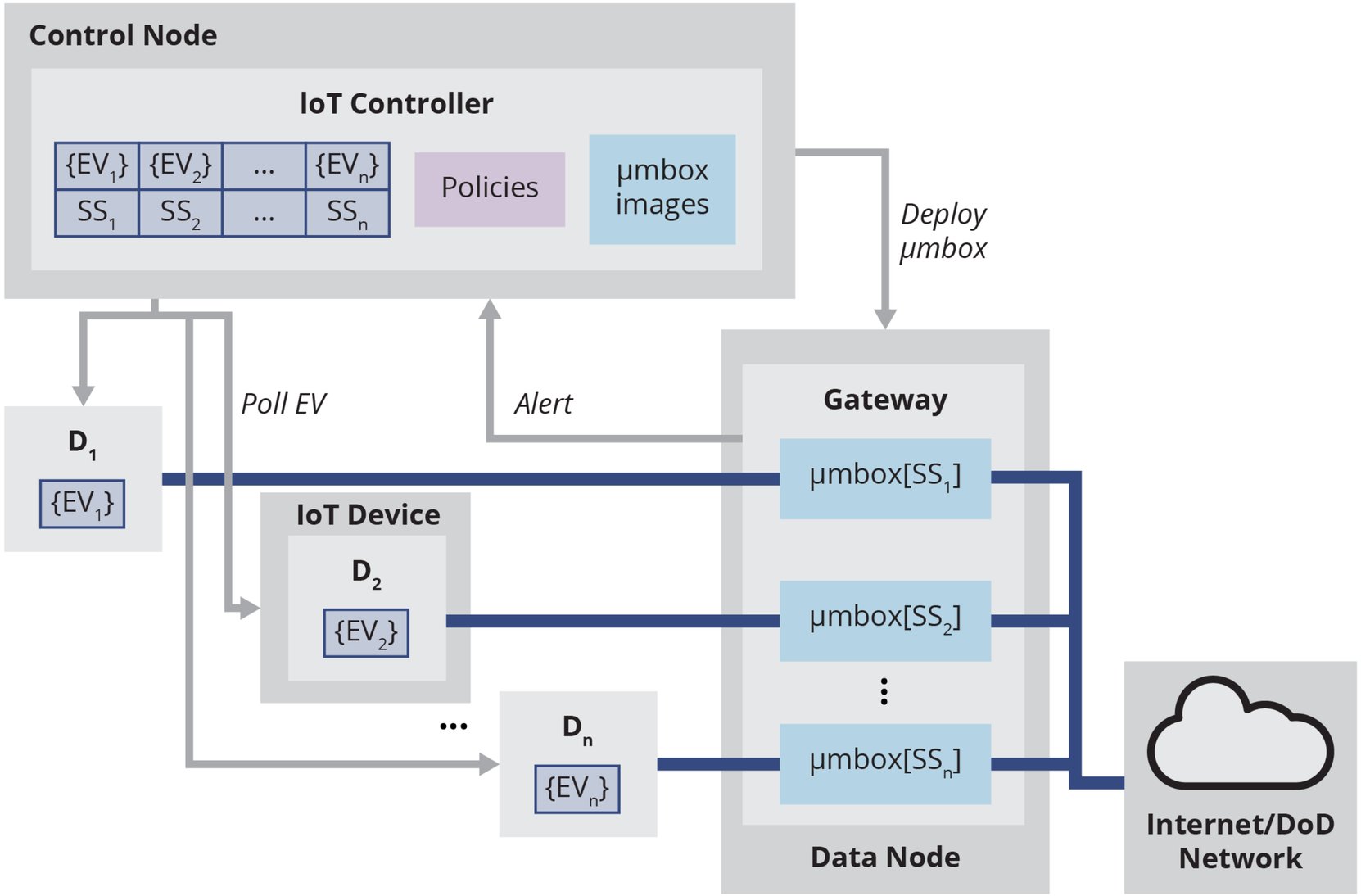
- Full platform tested with realistic IoT deployments
- Results published

MID

- Platform adapted and integrated into existing DoD networks

- AI tech
to auto
securit
protec

© 2019 Carnegie Mellon University



- Has flexible **po** states, transitio
- Reacts using **n** **environment** i
- Uses **different** **defenses** for e state
- Adapts to **devi** **vulnerabilities**
- Secures critical integration with **/überXMHF**

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Appr

Principal Investigator, SEI/SSD
secheverria@sei.cmu.edu

Chris Grabowski
SEI/SSD

Dr. Grace Lewis
SEI/SSD

SEI/SSD

Matthew McCormack
CMU/CyLab

Marc Novakouski
SEI/SSD

SEI/CER

Dr. Vyas
CMU/CyL

Dr. Amit
SEI/SSD

© 2019 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Appr