Security and Privacy in the Internet of Things

Elisa Bertino
CS Department and Cyber2SLab
bertino@purdue.edu

PURDUE UNIVERSITY

CERIAS

The IoT – Wikipedia

- The **Internet of Things** (**IoT**) is the network of physical objects or "things" embedding electronics, software, and network connectivity, which enables these objects to collect and exchange data.
- The IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems.
- When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities.

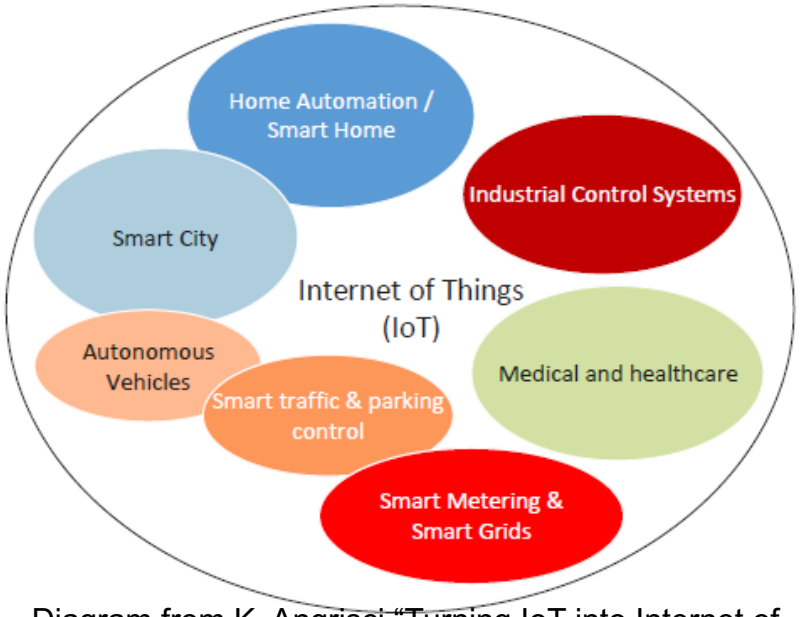
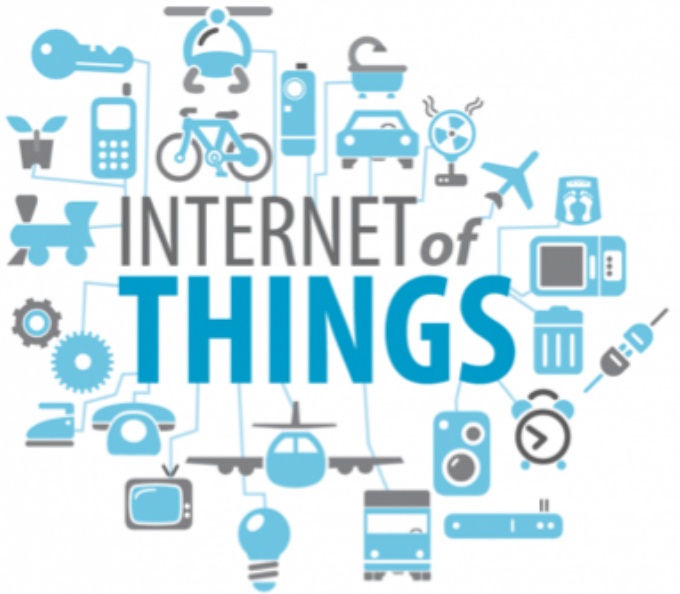


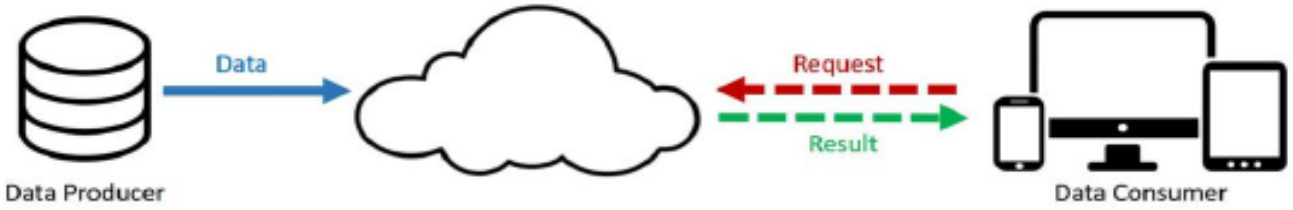
Diagram from K. Angrisci "Turning IoT into Internet of Vulnerabilities: IoT Botnets"



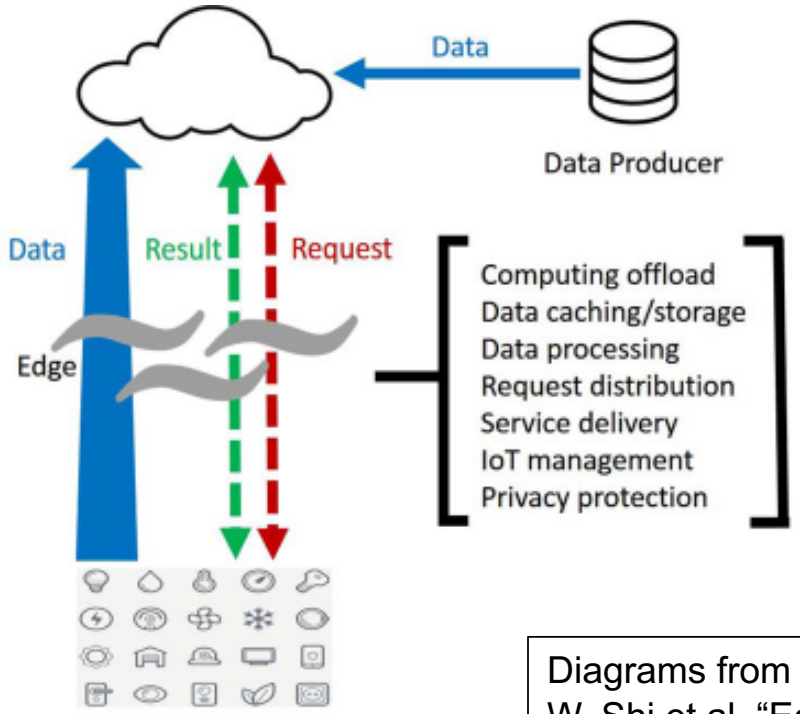
PURDUE UNIVERSITY

Edge Computing

Conventional cloud computing paradigm

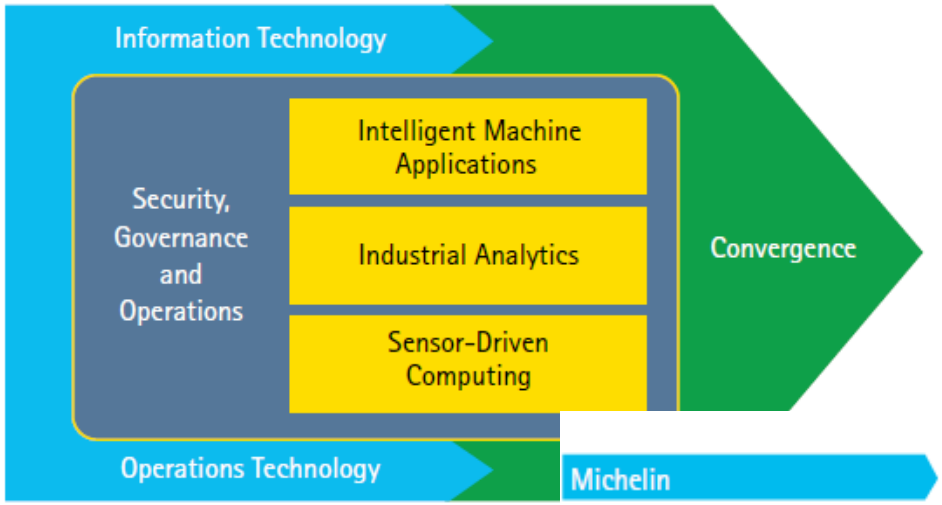


Edge computing paradigm



Diagrams from paper:
W. Shi et al, “Edge Computing: Vision and Challenges”, IoT Journal, Oct. 2016

Industrial IoT (IIoT)



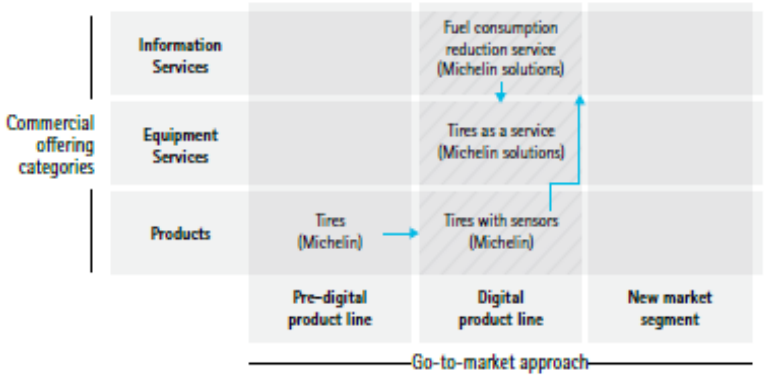
Operational Efficiency

New Services and Pricing Options

Unconventional Growth

Michelin

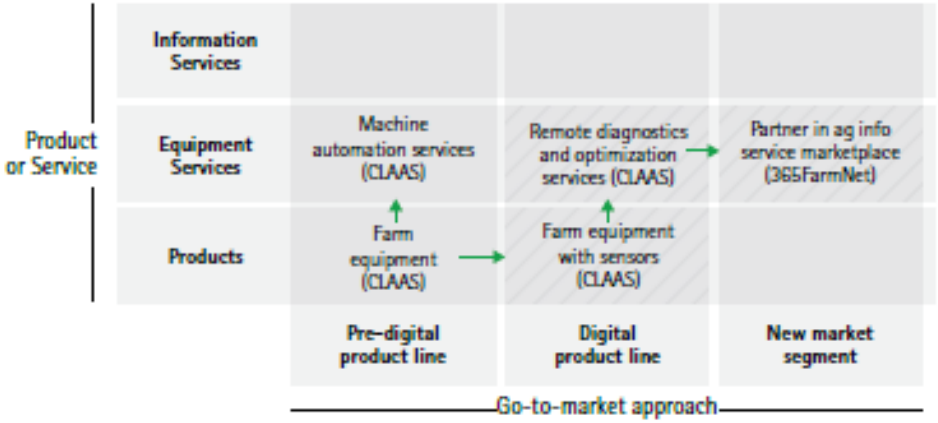
Michelin is helping truck fleet managers reduce fuel consumption and costs and allowing them to pay for tires on a kilometers-driven basis.



Diagrams and examples from Accenture "Driving the Unconventional Growth through the Industrial Internet of Things", 2015, downloaded from https://www.accenture.com/us-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Driving-Unconventional-Growth-through-IIoT.pdf

CLAAS

Farmers can operate CLAAS equipment on autopilot, receive advice on how to improve crop flow and minimize grain losses, or automatically optimize equipment performance. The company is now partnering with other organizations to provide information services to growers via a marketplace called 365FarmNet.



PURDUE UNIVERSITY

Industrial IoT (IIoT)

Evolution of a Connected Business Model: Stages of IIoT Maturity

The Bsquare IIoT Maturity Index outlines the stages commonly associated with Industrial IoT technology adoption. Each phase typically builds on the previous one, allowing organizations to drive maximum value as they progress through the index.

5 — Enhancing On-Board Intelligence
Processing data on or very close to the connected equipment, sometimes called distributed intelligence or edge computing.

4 — Automation
Orchestrates automated, complex actions across multiple internal systems such as inventory, support, or service ticketing systems.

3 — Data Analytics
Delivers insight, prediction, and optimization with applied data analytics, such as machine learning and artificial intelligence.

2 — Real-Time Monitoring
Data is monitored and visualized to initiate use cases for desired business outcomes. Achieves awareness of equipment status and refines business processes.

1 — Device Connectivity & Data Forwarding
Sensor data is transmitted and stored for analysis and action.

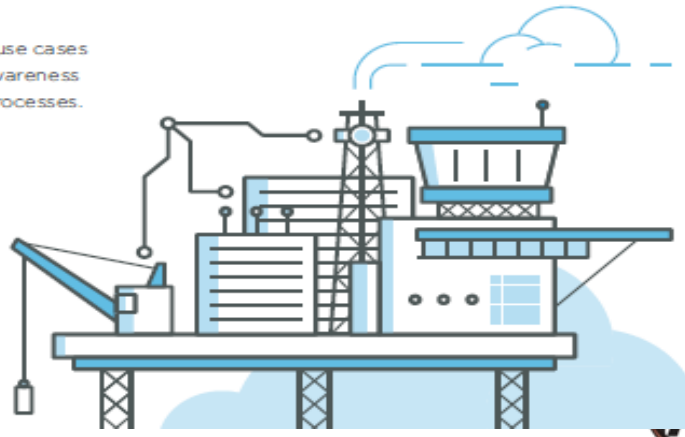


Diagram from BSQUARE. Annual IIOT Maturity Survey. 2017

IoT - Risks

IoT dramatically expands the attack surface

- IoT systems do not have well defined perimeters
- IoT systems are highly dynamic and continuously evolve because of mobility
- IoT are highly heterogeneous with respect to:
  - ❑ Communication
  - ❑ Platform
  - ❑ Devices
- IoT systems may include physically unprotected portions
- IoT systems are highly autonomous and control other autonomous systems
- IoT systems may include “objects” not designed to be connected to the Internet
- Human interaction with all the devices is not scalable

IoT - Risks

The OWASP Internet of Things Top 10 - 2014

1. Insecure Web Interface
2. Insufficient Authentication/Authorization
   Including authentication bypass vulnerabilities in firmware
3. Insecure Network Services
4. Lack of Transport Encryption
5. Privacy Concerns
6. Insecure Cloud Interfaces
7. Insecure Mobile Interfaces
8. Insufficient Security Configurability
9. Insecure Software/Firmware
10. Poor Physical Security

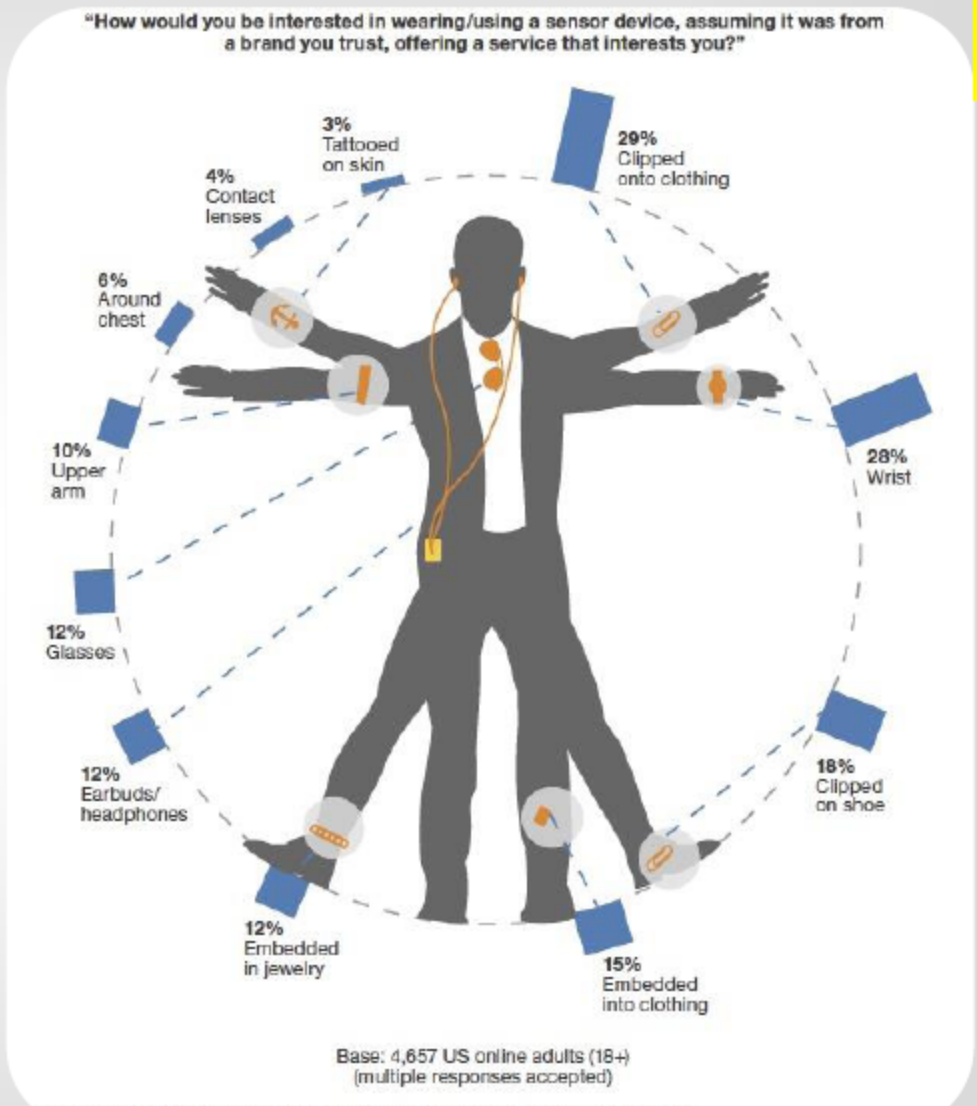
PURDUE UNIVERSITY

CERIAS

IoT – Privacy Risks

Individuals as sources of multiple data sets

- Wearable devices collect huge amounts of personal data as well data about the user environment
- Major privacy concerns arise for health-related data from the use of medical devices and fitness applications
- Privacy-sensitive information can be easily disclosed to third parties
- Threats arise for enterprise perimeters



PURDUE UNIVERSITY

Specific Security Challenges of IIoT

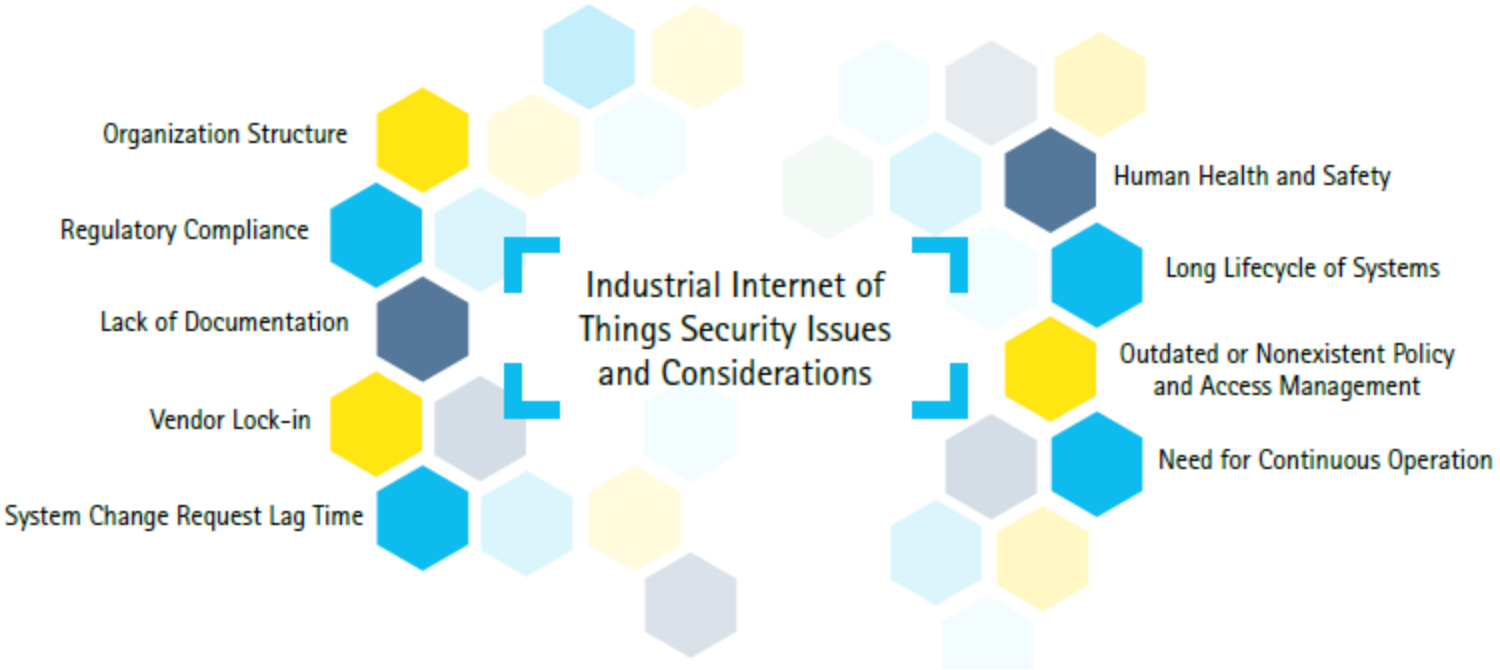


Diagram from Accenture "Driving the Unconventional Growth through the Industrial Internet of Things", 2015, downloaded from https://www.accenture.com/us-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Driving-Unconventional-Growth-through-IIoT.pdf

IoT – Privacy and Safety Risks

Privacy

- The toy collects information, such as name and age, from the child
- A human can ask information to the toy and thus get information about the child – the device does not authenticate the voice of the individual asking the information and thus confidential data can be extracted from the toy if lost or unattended
- Insecure key management

Safety

- It is possible to inject malicious voice and thus ask the child to do unsafe actions (e.g. open the door)

PURDUE UNIVERSITY

Slide based on paper by J.Valente and A. A. Cardenas. Security & Privacy of Smart Toys. In 1st Workshop on Internet of Things Security and Privacy (IoTS&P '17). ACM 2017.

CERIAS

Question:

We have a lot of security techniques

Can we apply them to the IoT?

Security Framework for IoT

Prepare and Prevent

nesCheck
• static analysis and dynamic instrumentation for nesC memory safety
[ASIACCS2017]

OptAll
• security provisioning based on game theory
[ACM/IEEE IoTDI 2017]
[ACM TOPS 2017]
[ESORICS 2017]

LTEInspector
• systematic testing of 4G LTE
[NDSS 2018]

Monitor and Detect

Kalis
• knowledge-driven adaptable IDS for IoT
[ICDCS 2017]

Heimdall
• whitelist-based anomaly detection defense for IoT routers
[IoT Journal 2017]

Diagnose and Understand

Fine-Grained Analysis
• node- vs link-related packet dropping attacks
• interference location
[SECON 2014]
[ACM ToSN 2016]
• statistical model based on variance
[SP4SC (IEEE FiCloud'16)]

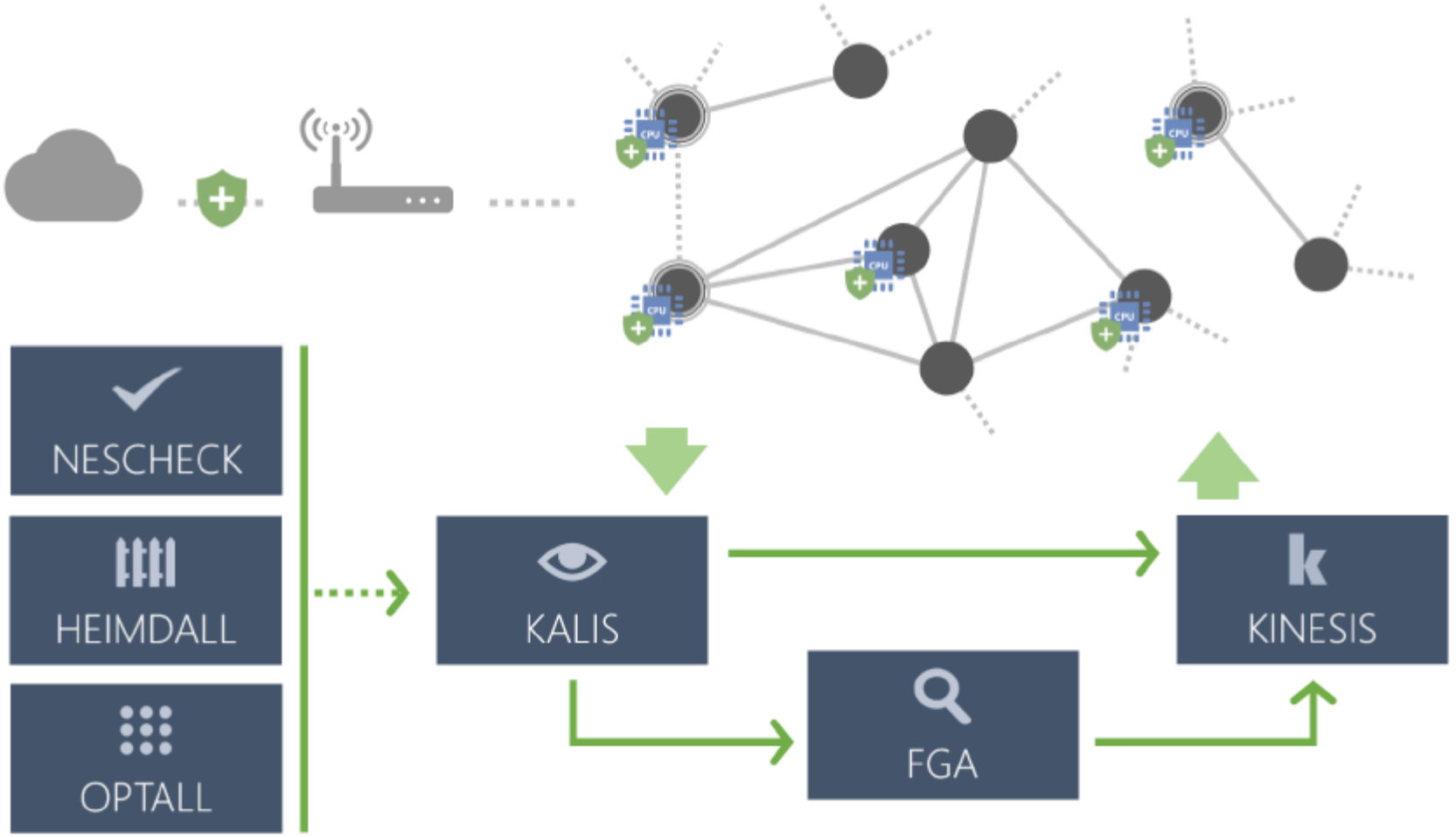
React, Recover and Fix

Kinesis
• automated response system
[ACM SenSys 2014]
[ACM ToSN 2017]

PURDUE UNIVERSITY

CERIAS

Security Framework for IoT



PURDUE UNIVERSITY

CERIAS

Monitor and Detect

Heimdall

D. Midi, A. Mudgerikar,

J. Habibi, E. Bertino

PURDUE UNIVERSITY

CERIAS

Mirai Botnet

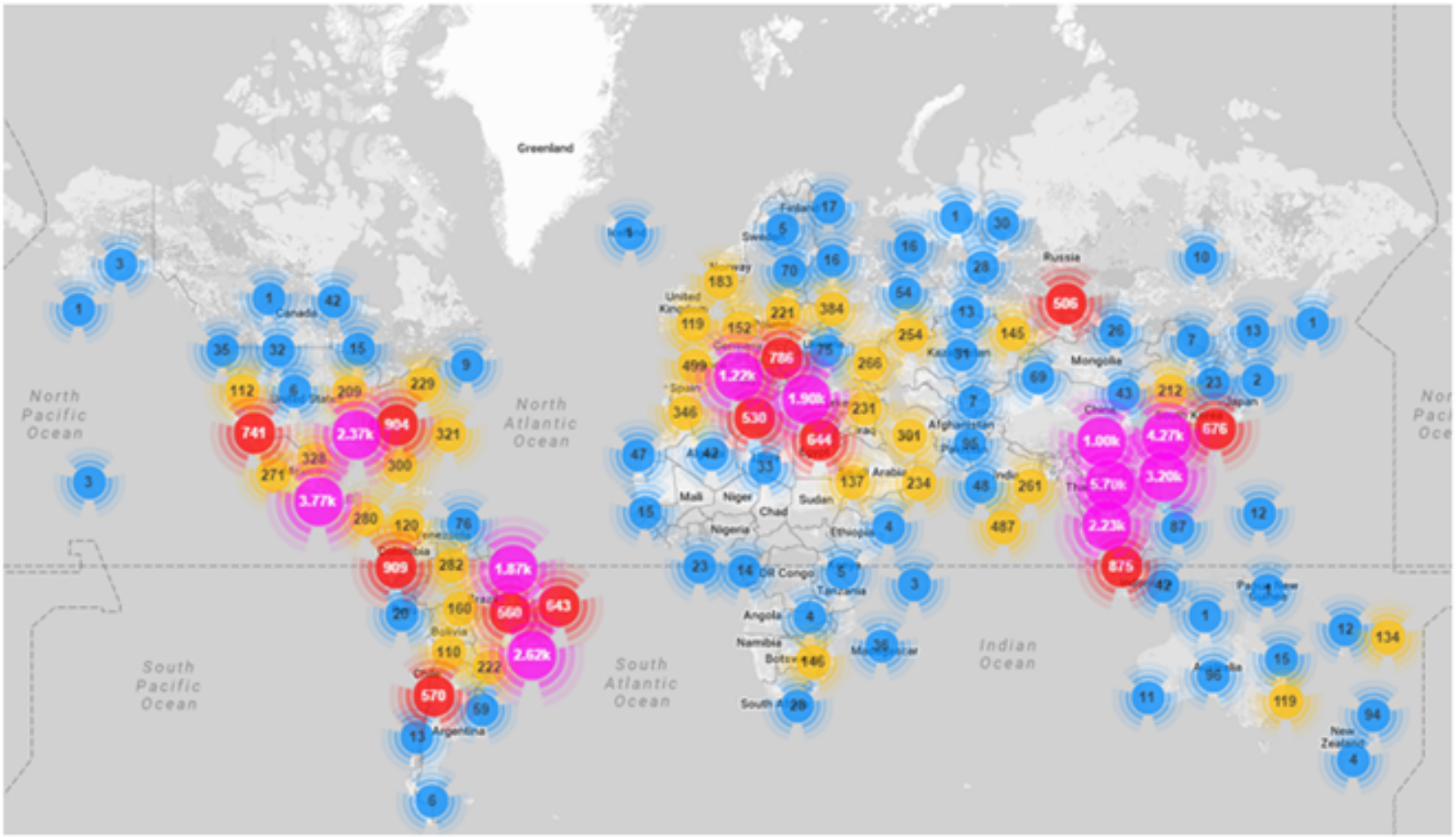
- Mirai is a piece of malware designed to launch multiple types DDoS attacks
- The malware scans the internet for telnet servers then attempts to log in and infect them using a list of hard-coded passwords (most of which correspond to internet connected CCTV systems and routers)
- A botnets using the Mirai malware was responsible for the largest DDoS attack ever recorded, which peaked at 1.1 Tbps
- It exploits well-known hardcoded login credentials in IoT devices
- It uses segmented command-and-control which allows the botnet to launch simultaneous DDoS attacks against multiple, unrelated targets

Mirai Botnet

C

USER:	PASS:
root	xc3511
root	vizxv
root	admin
admin	admin
root	888888
root	xmhdipc
root	default
root	juantech
root	123456
root	54321
support	support
root	(none)
admin	password
root	root
root	12345
user	user
admin	(none)
root	pass
admin	admin1234
root	1111
admin	smcadmin
admin	1111
root	666666
root	password
root	1234
root	klv123
Administrator	admin
service	service
supervisor	supervisor
guest	guest
guest	12345
guest	12345

USER:	PASS:
admin1	password
administrator	1234
666666	666666
888888	888888
ubnt	ubnt
root	klv1234
root	Zte521
root	hi3518
root	jvbzd
root	anko
root	zlxx.
root	7ujMko0vizxv
root	7ujMko0admin
root	system
root	ikwb
root	dreambox
root	user
root	realtek
root	00000000
admin	1111111
admin	1234
admin	12345
admin	54321
admin	123456
admin	7ujMko0admin
admin	1234
admin	pass
admin	meinsm
tech	tech
mother	fucker



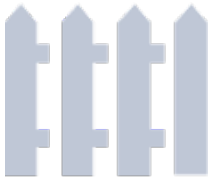
Geo-locations of all Mirai-infected devices uncovered as of October 2016

from I. Zeifman, D. Bakerman, B. Herzberg. Breaking Down Mirai: An IoT DDoS Botnet Analysis. Imperva, October 2016. Available at https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

PURDUE UNIVERSITY

CERIAS

Heimdall



attack analysis + defense technique for IoT botnets

- evaluation of DDoS attack throughput of off-the-shelf IoT hardware;
- design and implementation of a router whitelist-based anomaly detection defense.

PURDUE UNIVERSITY

CERIAS

IoT – Communication "Architectures"

- *Device-to-device*: Two or more IoT devices communicate directly with each other, rather than via an intermediary like an application server.
- *Device-to-cloud:* In this model, an IoT device directly communicates with an application server in the Internet (cloud) and exchanges messages such as devices status and control commands. Connection is via some home gateway.
- *Device-to-gateway:* In this model, an application layer gateway (ALG) is used, which is a computer system with two or more network interfaces. IoT devices are directly connected to an ALG that mediates between the IoT devices and an application server in the cloud.

IoT Botnet Defense Design

- Challenges
  - Closed devices
  - Heterogeneity of platforms, OSes, network stacks
  - Cloud-based load balancing for services
- Advantages
  - High behavioral specificity on average
  - Anomaly detection does not need complex inference models
  - *No device-to-device communication makes it possible defense at gateway*
  - Consistency allows pre-computed profiles and profile sharing

Defense Design

- Whitelist-based approach
  - Our analysis shows it is effective
- But… naïve design does not work
  - Separation of learning and enforcement has problems
    - Profile pollution during learning
    - Handling firmware updates

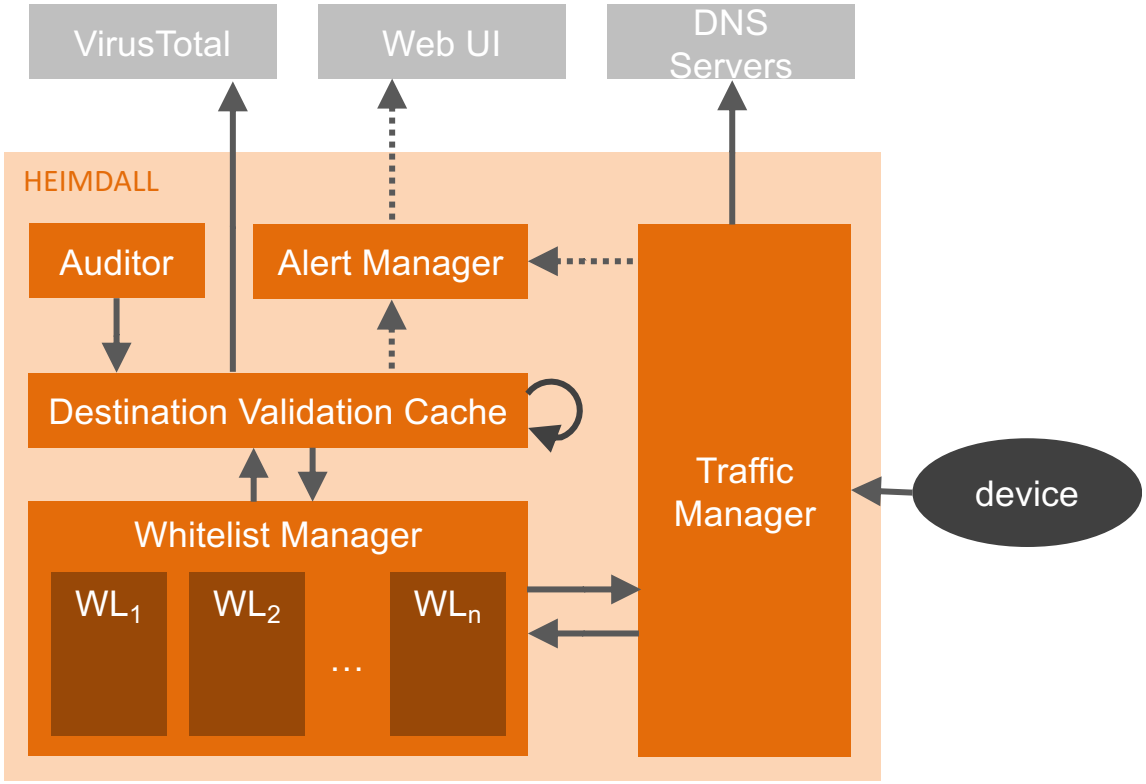
Defense Design

- Complex continuous approach is effective
  - No separation of learning and enforcement phases
  - Continuous validation of DNS requests
  - Use knowledge from 3rd party aggregation services
  - Resilience to DNS Poisoning attacks
- Multi-tiered policy enforcement
  - Real-time validation vs. Max throughput
  - Instant global blacklisting for subsequently compromised destinations

Implementation

- Hardware & Software
  - Linksys WRT 1900AC router, running OpenWRT Chaos Calmer
  - Python custom proxy + IPTables utility
- VirusTotal
  - Free 3rd party security analysis service, aggregating over 60 sources

Architecture

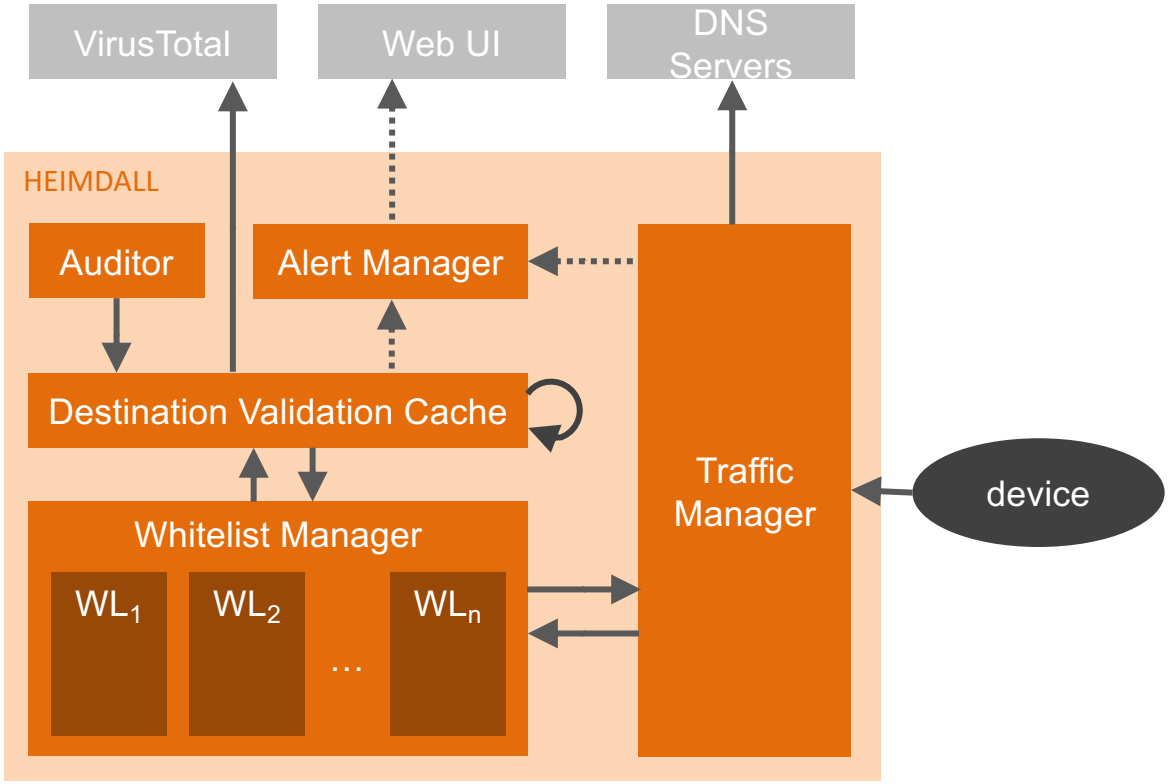



```
function TrafficMgr.onTraffic(request req, device D, dest d)
    if d in Blacklist then
        drop(D, d)
        return
    end if
    r = WhitelistManager.onTraffic(D, d)
    if r == REJECT then
        drop(D, d)
        return
    end if
    let req from D go to d
    intercept response R (don't let go to D yet)
    if req is DNSQuery then
        if r.IP != null then
            if r.IP != R.IP then
                r' = WhitelistManager.onTraffic(D, R.IP)
                if !r' then
                    if !selfCorrection then
                        drop(D, d)
                        return
                    end if
                    rewriteReply(R, r.IP)
                end if
            end if
        end if
        WhitelistMgr.associateForSession(r.IP, WL_D.d)
    end if
    release R
end function
function TrafficMgr.drop(device D, dest d)
    send(D, "Destination Unreachable")
    sendAlert(D, d)
end function
```

PURDUE UNIVERSITY

CERIAS

Architecture

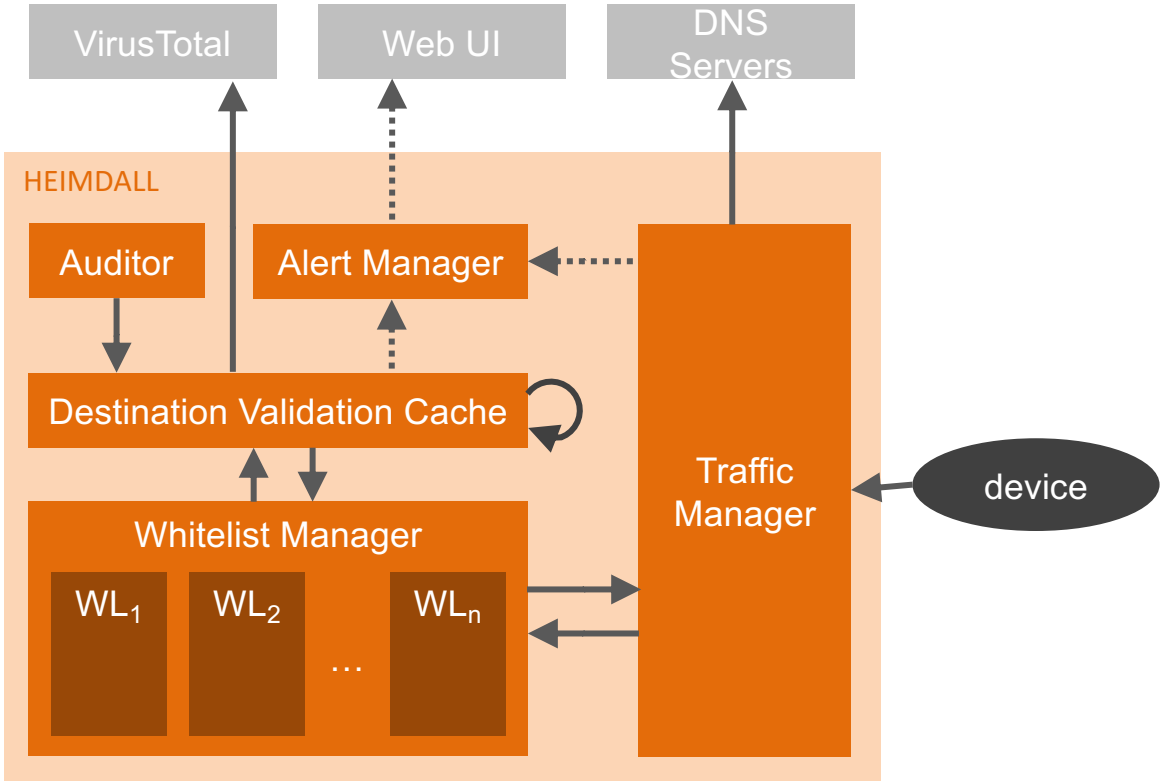



```
function WhitelistMgr.onTraffic(device D, dest d)
    create empty WL_D if not exists
    if d not in WL_D then
        if realTimeValidation then
            if d not in DestCache then
                DestCache.checkDest(d)
            end if
            if d malicious in DestCache then
                return REJECT
            end if
        end if
        add d to WL_D
    end if
    return APPROVE
end function
```

PURDUE UNIVERSITY

CERIAS

Architecture




```
function AUDITOR.AUDIT
    for all entry in DestCache do
        DestCache.checkDest(d)
    end for
end function
function DESTCACHE.CHECKDEST(dest d)
    r = queryVirusTotal(d)
    if r benign then
        remove from DestCache.malicious[]
        add to DestCache.benign[]
    else
        if d in DestCache.benign[] then
            remove from DestCache.benign[]
            WhitelistManager.purgeFromAllWLs(d)
            sendAlert(d)
        end if
        add to DestCache.malicious[]
    end if
    return r
end function
```

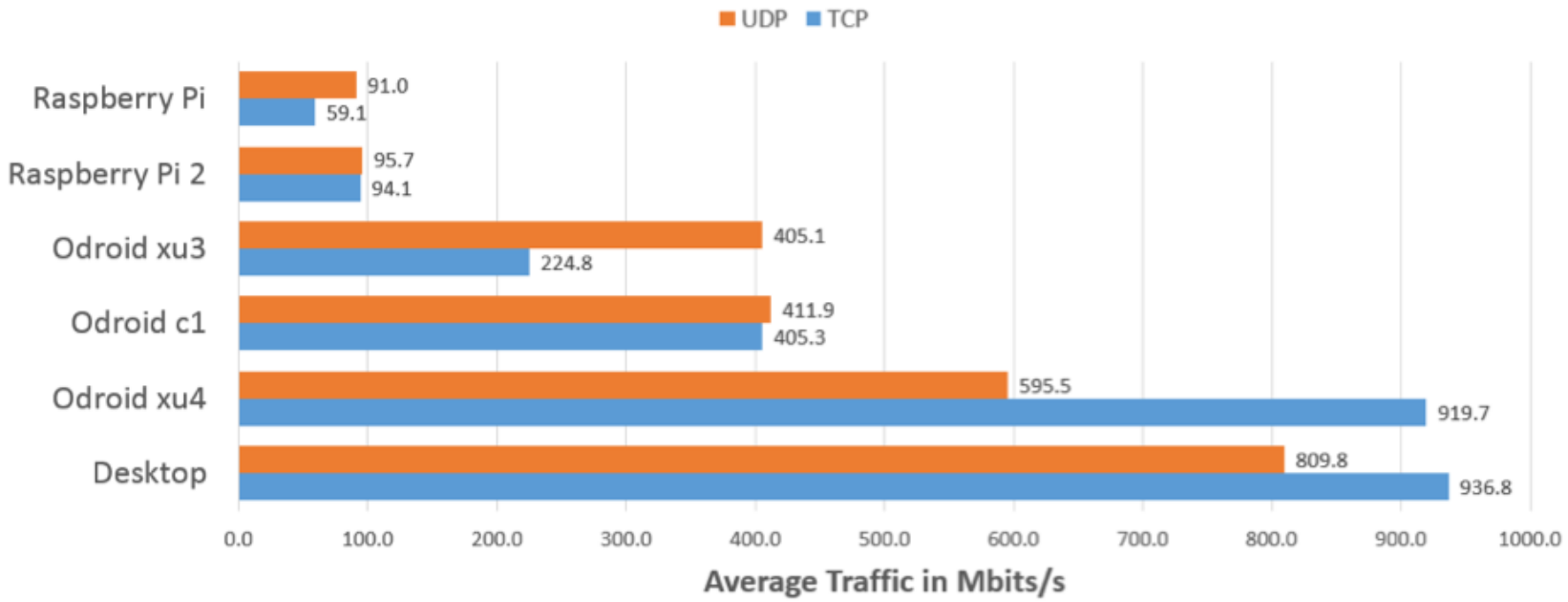
PURDUE UNIVERSITY

CERIAS

Experimental setup

- Off-the-shelf IoT devices
  - Nest Thermostat, August SmartLock, Lifx smart lightbulb,
    Arlo Home Security System, Amazon Dash Button
- Off-the-shelf IoT boards
  - Odroid Xu4, Odroid C1+, Rasperry Pi 2 & 3, Particle Photon, Arduino
- Traffic generator
  - For attack power analysis
- Traffic tracing
  - For defense evaluation

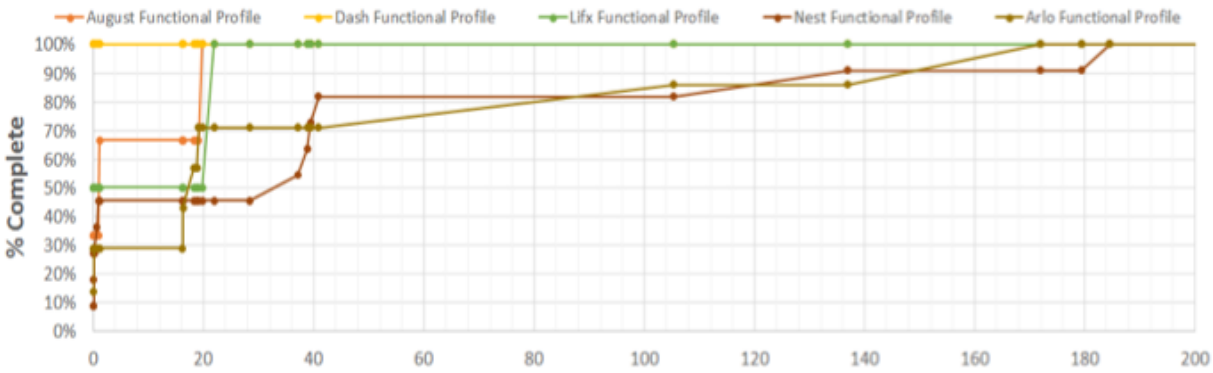
Attack Power of IoT Boards

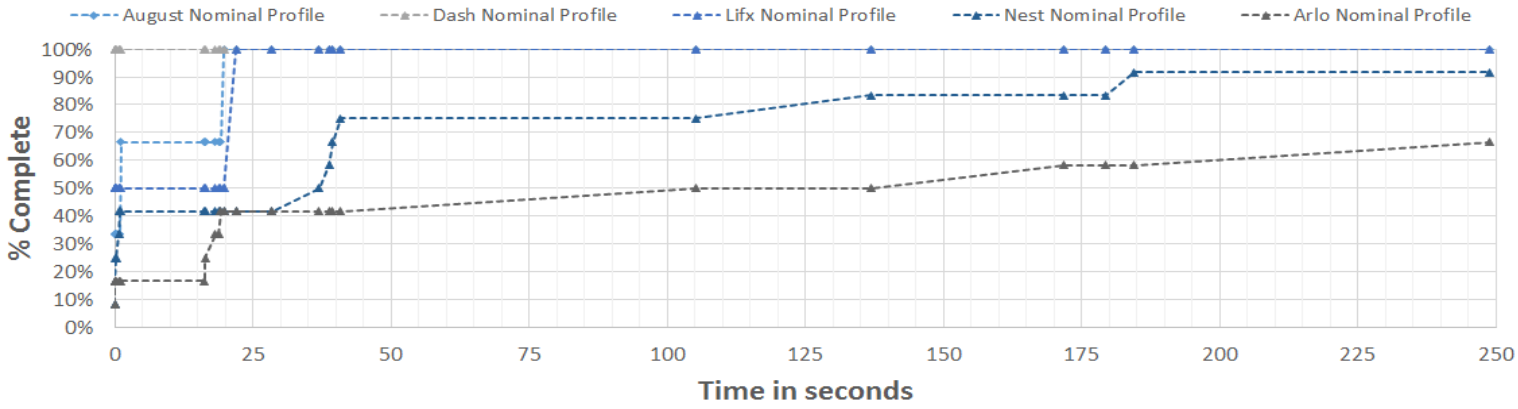


PURDUE UNIVERSITY

CERIAS

Functional vs. Nominal Whitelist Completeness





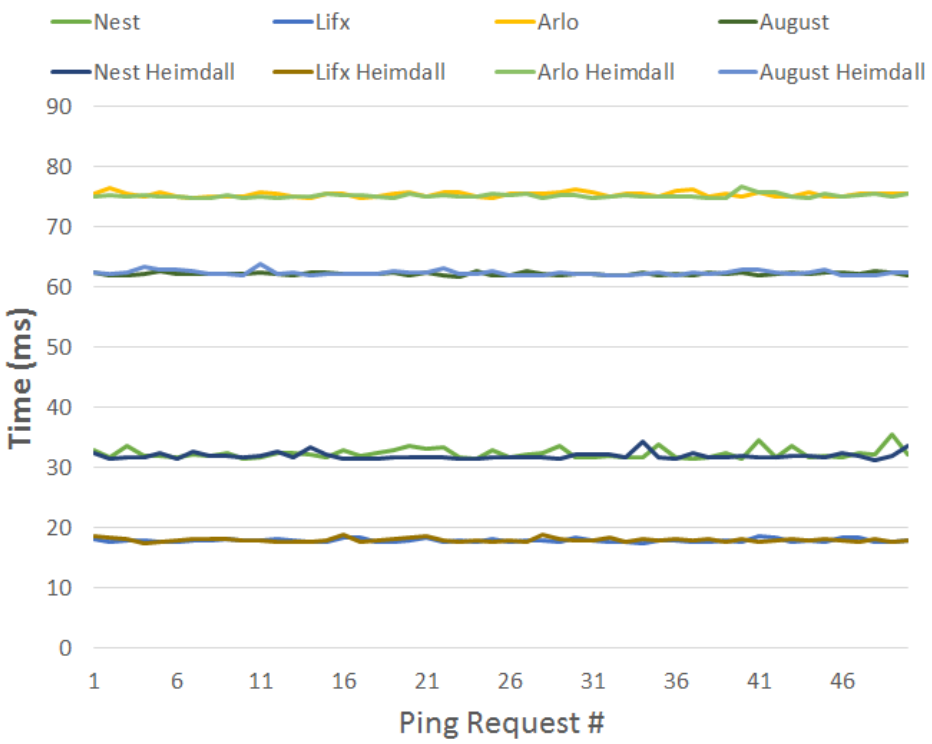
Experiment durations

1 hr, 24 hrs, 1 week

PURDUE UNIVERSITY

CERIAS

Heimdall Latency



PURDUE UNIVERSITY

CERIAS

Future Research Directions

- Mobility-aware Fine-Grained Analysis
  - Using 2-hop knowledge to construct geometric constraints w.r.t. fixed system of coordinates
- Attestation techniques for IoT
  - Extending Kalis to perform attestation
- Bring-Your-Own-IoT
  - Enabling containerization and AC policies onto IoT and wearables
- Cloud-enabled Heimdall and IoT Identity
  - Identifying IoT devices by traffic patterns, leveraging identity for cloud repository of policies
- Protecting IoT devices from input spoofing
- Protecting IoT devices from ransomware

Thank you!!

Any question?

PURDUE UNIVERSITY

CERIAS