Lecture #7: IoT Edge Security Systems

Cristian Hesselman, Elmer Lastdrager, Ramin Yazdani, and Etienne Khan

University of Twente | May 26, 2021

Key concept: gateway

Today’s agenda

- Admin
- Introduction
- Paper #1: CommunityGuard
- Paper #2: DeadBolt
- Feedback

Admin

UNIVERSITY OF TWENTE.

SIDN LABS

Paper summaries

- You must have handed in your two summaries **before 7AM on the day of the lecture**
- Each summary can be at most 250 words, at most 1 single-sided A4 page
- You can add figures, and graphs from the paper or add your own if you like (e.g., concept maps)
- You can use the summaries during the oral exam
- Submit through CANVAS
- You **cannot** complete SSI without submitting 12 paper summaries!

Lab experiment

- Measure network traffic of **2+** IoT devices in groups of **two or three**, **one** report per team
- Use IoT devices **without a browser-like interface**
- Examples: camera, audio speaker, light bulb, thermostat, doorbell
- We have a couple of devices if you really can’t find an IoT device
- Do not use multi-purpose devices like tablets, phones, laptops
- Use WireShark, TCPdump, or (for example) a SPIN device.
- Etienne Khan available for assistance
- Lab report (PDF) and required files: **Sun June 20, 2021, 23:59 CEST**

Interactive lectures

- Overall objective: enable you to learn from each other and further increase your understanding of the papers, contributes to preparing yourself for the oral exam

- Interactive format
  - Teachers summarize two papers per lecture
  - Multiple-choice questions (not graded) and discussion
  - We ask at least one of you to share their thoughts on each paper (main lesson learned, etc.)
  - Enables you to learn from each other, so mandatory to participate

- A 7th “re-sit” lecture in case you miss a lecture (optional for everybody else), same format

Where are we now?

No.	Date	Contents
1	Apr 21	Course introduction Guest lecture #1: how the core of the internet is organized, Marco Davids (SIDN Labs)
2	Apr 28	Guest lecture #2: the relationship between regulation & IoT security, Eelco Vriezekolk, Agentschap Telecom (Dutch telecoms regulator)
3	May 6*	Lecture: IoT Concepts and Applications
4	May 12	Lecture: IoT Botnet Measurements
5	May 18	Lecture: IoT Honeypots
6	May 25*	Guest lecture #3: The Life Of An IoT Device, Eliot Lear, Cisco Systems
7	May 26	Lecture: IoT Edge Security Systems
8	Jun 2	Lecture: IoT Device Behavior
9	Jun 9	Lecture: IoT in Non-Carpeted Areas
10	Jun 16	Lecture: IoT Edge Security Systems (re-sit)

* Different lecture times/days. Default slot: Wednesdays 11:00 - 12:45

Introduction

Motivation for today: important IoT comms model

- Security
- Protocol translation
- Cell phone
- Hub device

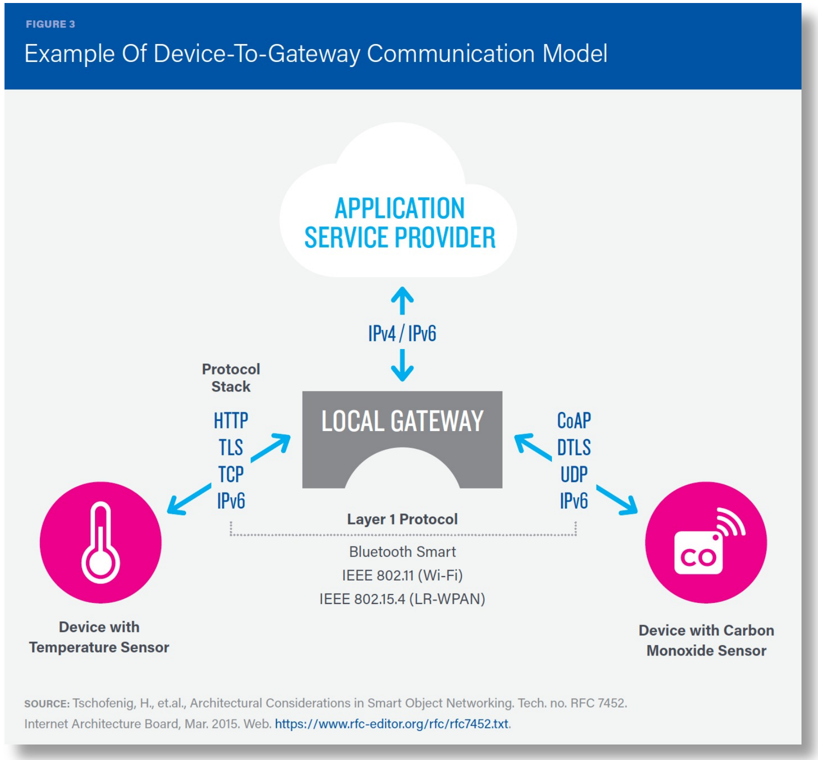


FIGURE 3

Example Of Device-To-Gateway Communication Model

SOURCE: Tschofenig, H., et.al., Architectural Considerations in Smart Object Networking. Tech. no. RFC 7452. Internet Architecture Board, Mar. 2015. Web. https://www.rfc-editor.org/rfc/rfc7452.txt.

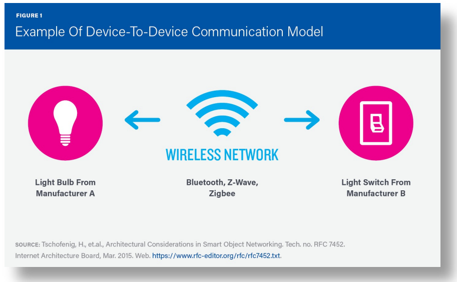


FIGURE 1

Example Of Device-To-Device Communication Model

WIRELESS NETWORK
Light Bulb From Manufacturer A
Bluetooth, Z-Wave, Zigbee
Light Switch From Manufacturer B

SOURCE: Tschofenig, H., et.al., Architectural Considerations in Smart Object Networking. Tech. no. RFC 7452. Internet Architecture Board, Mar. 2015. Web. https://www.rfc-editor.org/rfc/rfc7452.txt.

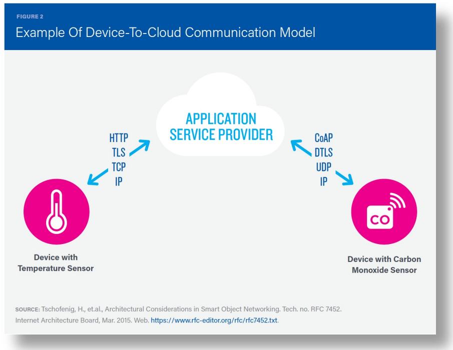


FIGURE 2

Example Of Device-To-Cloud Communication Model

APPLICATION SERVICE PROVIDER
HTTP
TLS
TCP
IP
CoAP
DTLS
UDP
IP
Device with Temperature Sensor
CO
Device with Carbon Monoxide Sensor

SOURCE: Tschofenig, H., et.al., Architectural Considerations in Smart Object Networking. Tech. no. RFC 7452. Internet Architecture Board, Mar. 2015. Web. https://www.rfc-editor.org/rfc/rfc7452.txt.

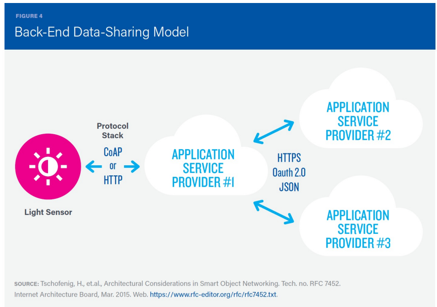


FIGURE 4

Back-End Data-Sharing Model

Protocol Stack
CoAP
or
HTTP
Light Sensor
APPLICATION SERVICE PROVIDER #1
HTTPS
Oauth 2.0
JSON
APPLICATION SERVICE PROVIDER #2
APPLICATION SERVICE PROVIDER #3

SOURCE: Tschofenig, H., et.al., Architectural Considerations in Smart Object Networking. Tech. no. RFC 7452. Internet Architecture Board, Mar. 2015. Web. https://www.rfc-editor.org/rfc/rfc7452.txt.

K. Rose, S. Eldridge, L. Chapin, “The Internet of Things: An Overview – Understanding the Issues and Challenges of a More Connected World”, ISOC Whitepaper, October 2015

Discussion

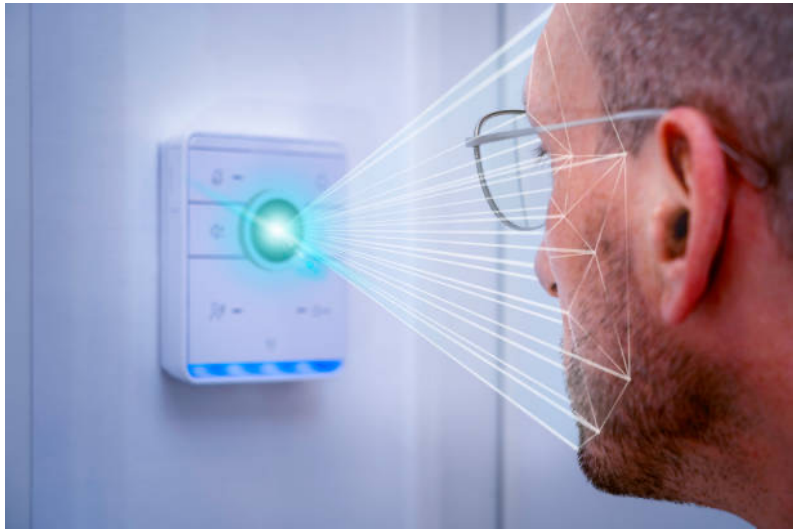
If you were the developer of a smart doorbell, which model would you use for your deployment?

A. Device-to-device

B. Device-to-cloud

C. Device-to-gateway

D. Back-end data sharing



And of course: **why?** ☺

Today’s papers

[CGuard] Chase E. Steward, Anne Maria Vasu, Eric Keller, “CommunityGuard: A Crowdsourced Home Cyber-Security System”, ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization (SDN-NFV Security), March 2017

[DBolt] R. Ko and J. Mickens, “DeadBolt: Securing IoT Deployments”, Applied Networking Research Workshop, Montreal, QC, Canada, July 16, 2018 (ANRW ’18)

Today’s learning objective

- After the lecture, you will be able to discuss the design, operation, and evaluation of CommunityGuard and DeadBolt, which are two example systems that protect users and the Internet from insecure IoT devices **at the edges** of the network (e.g., in home networks)

- CommunityGuard is collaborative system, while DeadBolt a system that largely runs in isolation in the local network

- Completely different approaches, give you a feel for the spectrum of possible solutions

- Contributes to SSI learning goal #1: “Understand IoT concepts and applications, security threats, technical solutions, and a few relevant standardization efforts in the IETF”

Paper #1: "CommunityGuard: A Crowdsourced Home Cyber-Security System", SDN-NFV Security, March 2017

UNIVERSITY OF TWENTE.

SIDN LABS

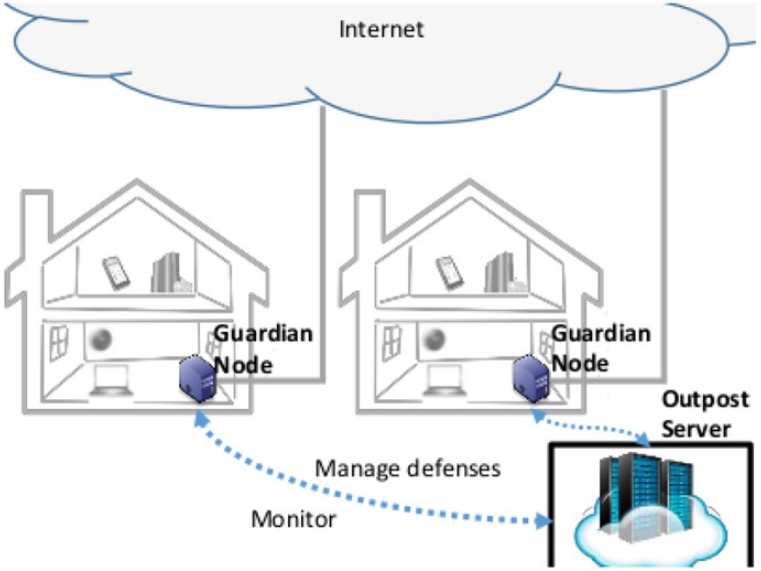
Concept

- Significant part of the IoT targets home networks (little or no IT security knowledge)

- Possibility to launch powerful DDoS attacks using these devices [MIRAI]

- A device residing between a home router and the cable modem connected to cloud

- Efficiency proportional to the number of subnets that deploy it



C-Guard Architecture

BeagleBone Black used as guardian node

- on-board 10/100 Mbps Ethernet port
- another interface was added using an USB to 10/100 Mbps Ethernet adapter
- runs Snort IPS/IDS

Source: https://images-na.ssl-images-amazon.com/images/I/71PDU796juL._AC_SL1500_.jpg

Community Outpost running on a cloud server

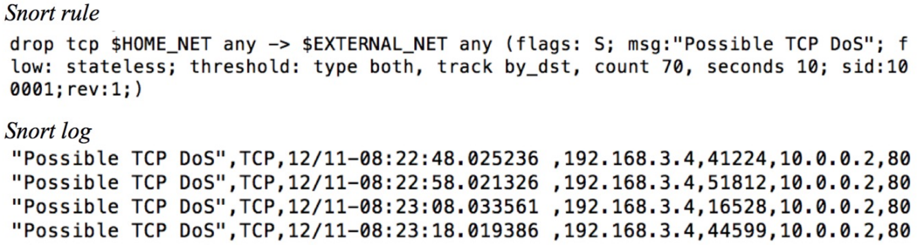
- needs to be scalable and secure (obvious attack target)

Source: https://snort.org/assets/SnortTM.png

Snort

- Operating modes:
    - packet sniffer (like tcpdump)
    - packet logger (e.g., for network traffic debugging)
    - rule-based network Intrusion Prevention System (IPS)
- Outline of a Snort rule

```
[action][protocol][sourceIP][sourceport] -> [destIP][destport] ( [Rule options] )
```



Snort rule

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (flags: S; msg:"Possible TCP DoS"; f
low: stateless; threshold: type both, track by_dst, count 70, seconds 10; sid:10
0001;rev:1;)
```

Snort log

```
"Possible TCP DoS",TCP,12/11-08:22:48.025236 ,192.168.3.4,41224,10.0.0.2,80
"Possible TCP DoS",TCP,12/11-08:22:58.021326 ,192.168.3.4,51812,10.0.0.2,80
"Possible TCP DoS",TCP,12/11-08:23:08.033561 ,192.168.3.4,16528,10.0.0.2,80
"Possible TCP DoS",TCP,12/11-08:23:18.019386 ,192.168.3.4,44599,10.0.0.2,80
```

- Community rules

    https://www.snort.org/downloads/community/snort3-community-rules.tar.gz

Discussion Question #1

Who should be responsible for running the CommunityGuard Outpost Server?

A: Specific IoT device vendors

B: ISPs

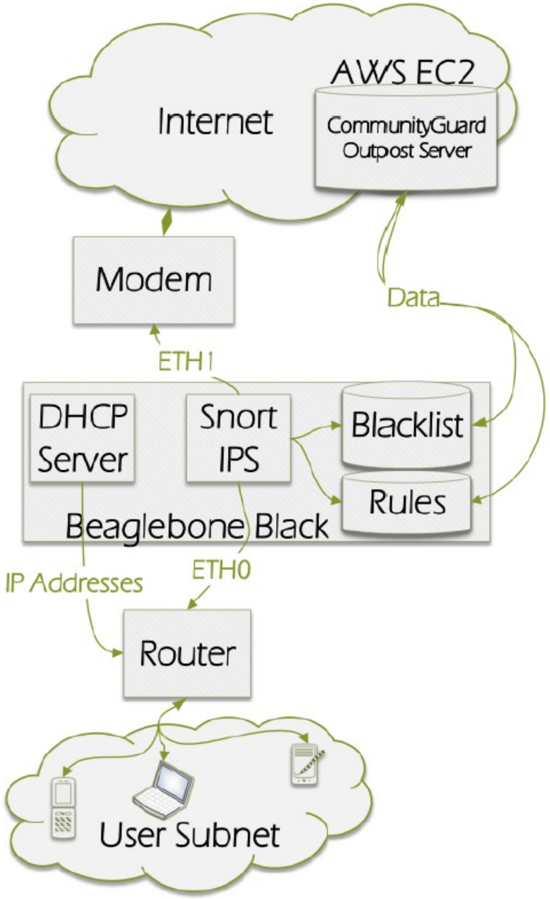
C: Cloud providers

D: …

C-Guard Prototype

Cron jobs running on Guardian Node:

- Updating Snort rules from rule repositories
- Exchanging information about malicious traffic with the Outpost Server
- Generating new anti-DDoS rules using DDoS server beacons



Quiz

Which of the following is **not** considered as a potential malicious activity from users in the paper?

A: getting access to user data

B: infecting other networks with Malware

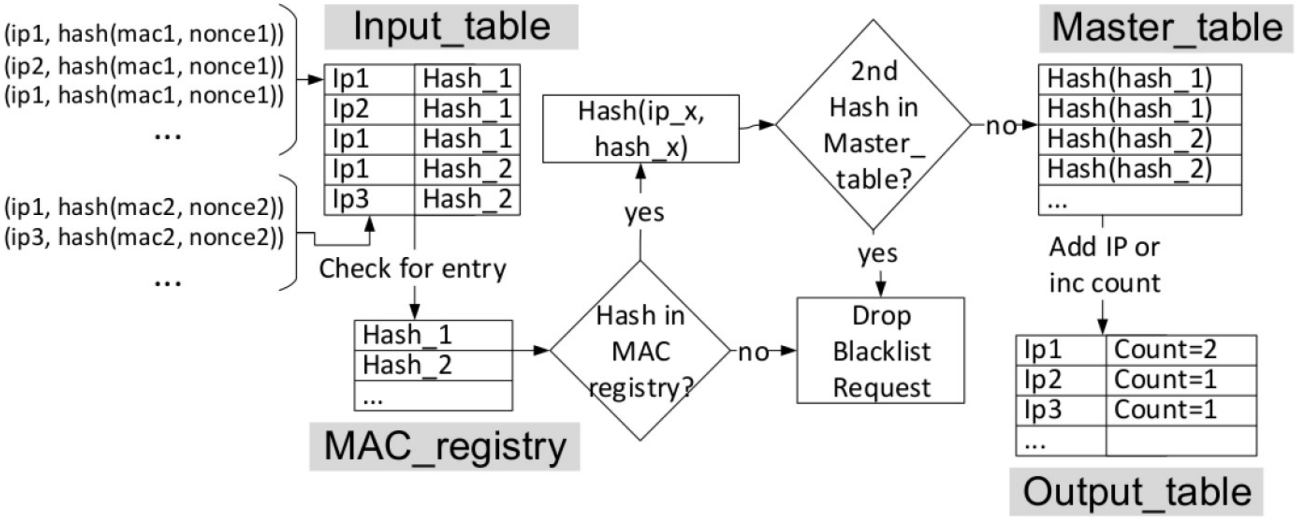
C: removing malicious IP addresses from blacklist

D: trying to blacklist legitimate IP addresses

Server Blacklist

❗ Users can only write to input_table

❗ Users cannot read from or write to Master_table



Input_table

Ip1	Hash_1
Ip2	Hash_1
Ip1	Hash_1
Ip1	Hash_2
Ip3	Hash_2

MAC_registry

Hash_1
Hash_2
…

Master_table

Hash(hash_1)
Hash(hash_1)
Hash(hash_2)
Hash(hash_2)
…

Output_table

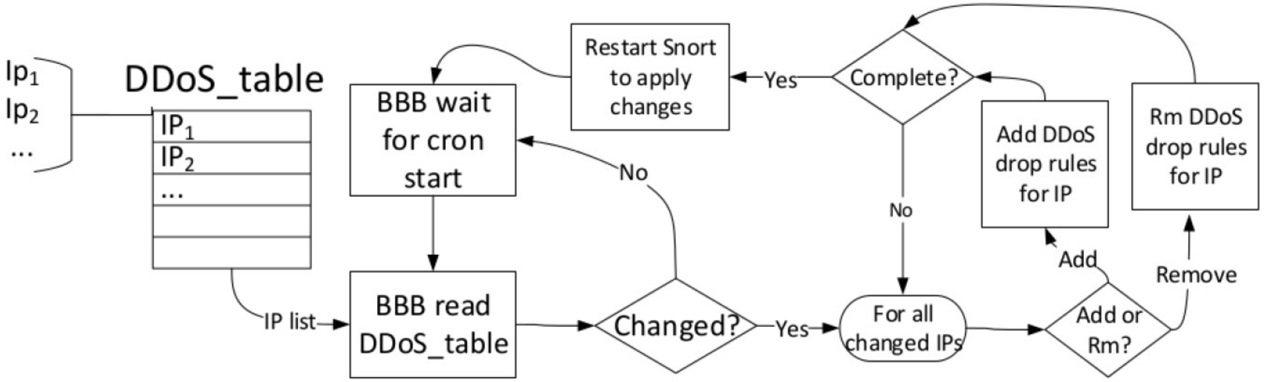
Ip1	Count=2
Ip2	Count=1
Ip3	Count=1
…	

❗ Users cannot read from or write to MAC_registry

❗ Users can only read from Output_table

Outgoing DDoS Prevention

❗ Developers add DDoSed server IPs to table



❗ Users can only read from DDoS_table

Evaluation

- Test setup including 2 Guardian Nodes

- A few manually written Snort rules to treat safe traffic as malicious

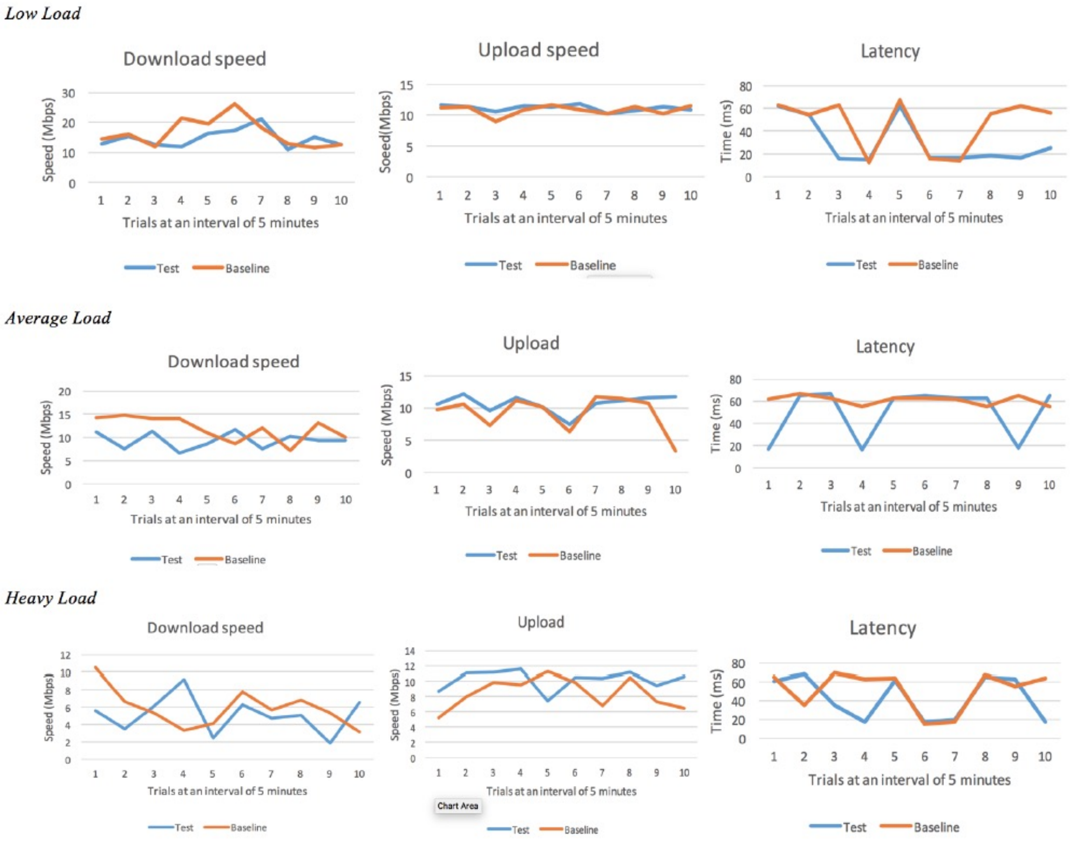
- Manually added DDoSed (TCP SYN) IP addresses to the database

- Legitimate traffic between the attacking node and the target was still allowed while attack traffic was dropped

Performance

- Limiting factors:
  - ○ USB to Ethernet adapter
  - ○ Slow SD card writes

- Sometimes the test case performs better than baseline which might be due to network fluctuations.



Discussion

- How would you attack the CommunityGuard system?
- What are the advantages/disadvantages of deploying an edge security system in this way?
- Would you implement such a system at your home?

Key takeaways

- Residential IoT networks need a default and simple security mechanism due to the lack of expertise compared to enterprises.

- DDoS attacks are easier to mitigate using a cooperative framework, however building trust in such a system is not straightforward.

- Adding an edge security system (using mechanisms proposed in this paper) introduces a negligible performance downgrade (if proper hardware is used)

Paper #2: “DeadBolt: Securing IoT Deployments”, Applied Networking Research Workshop, Montreal, QC, Canada, July 2018

* Figures are from this paper, unless stated otherwise

Quiz: key security objective

Deadbolt's key security objective is to protect against:

A. Remote attackers

B. Misconfigured IoT firmware

C. Outdated software on IoT devices

D. Rogue gateways

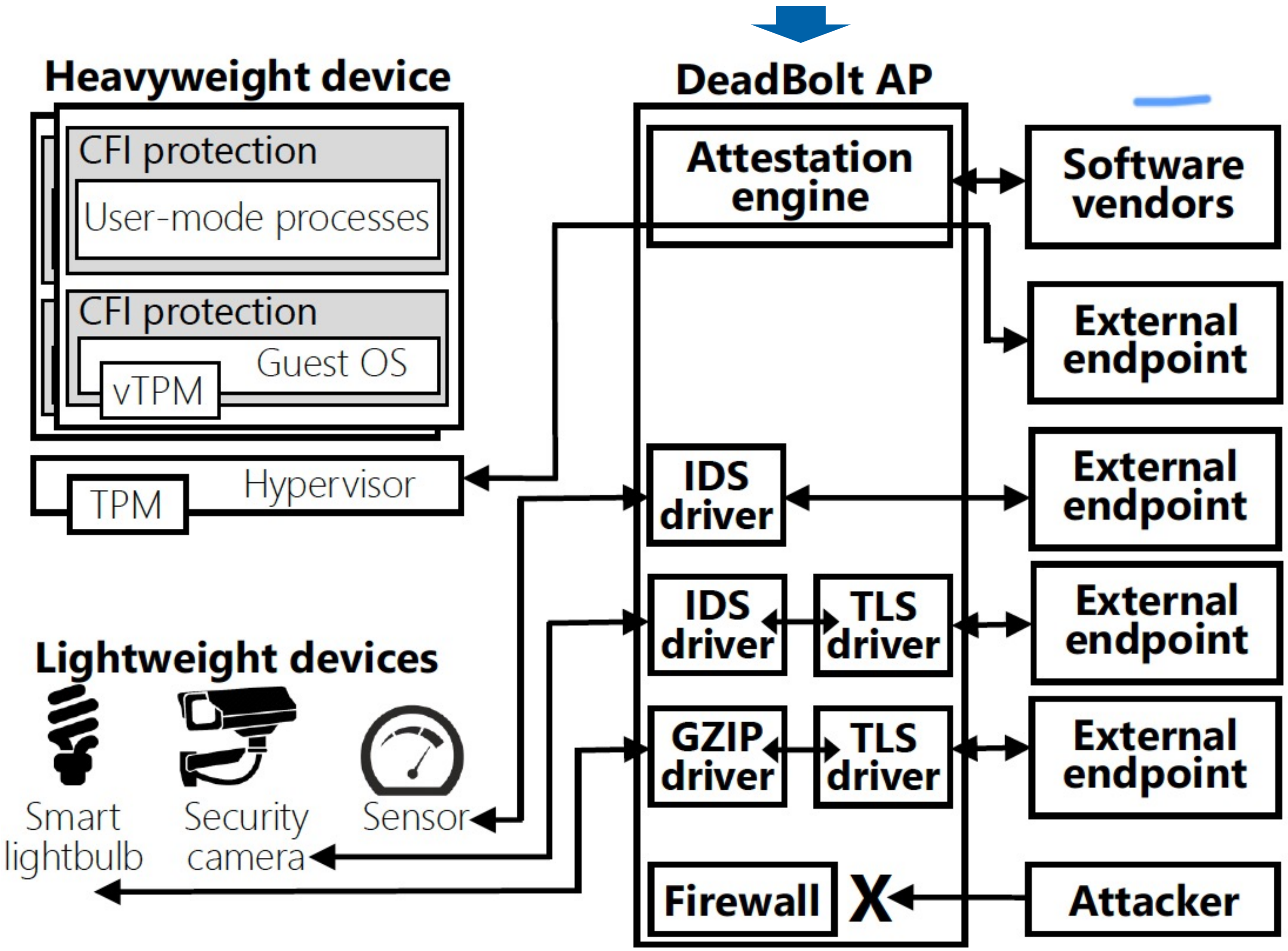
DeadBolt key concepts

- Components
  - Trusted gateway (AP)
  - Light weight IoT devices → third party virtual device derivers (proxies)
  - Heavy weight IoT devices → VMs

- Security functions
  - Software updates (VM swap for heavy weight devices, security-focused VNFs for light-weight)
  - Static attestation and runtime (against control flow attacks)
  - Quarantining and deny-by-default traffic pass through
  - TLS to exchange data

DeadBolt architecture

Security services



Discussion: Deadbolt’s key security mechanism

In your opinion, what’s DeadBolt’s most important security mechanism?

A. Verification that device software is up to date

B. Protection against remote exploits (control flow attacks)

C. TLS to exchange data

D. Deny-by-default traffic policy

E. Other

Quiz: operation

At what level in the protocol stack does DeadBolt operate?

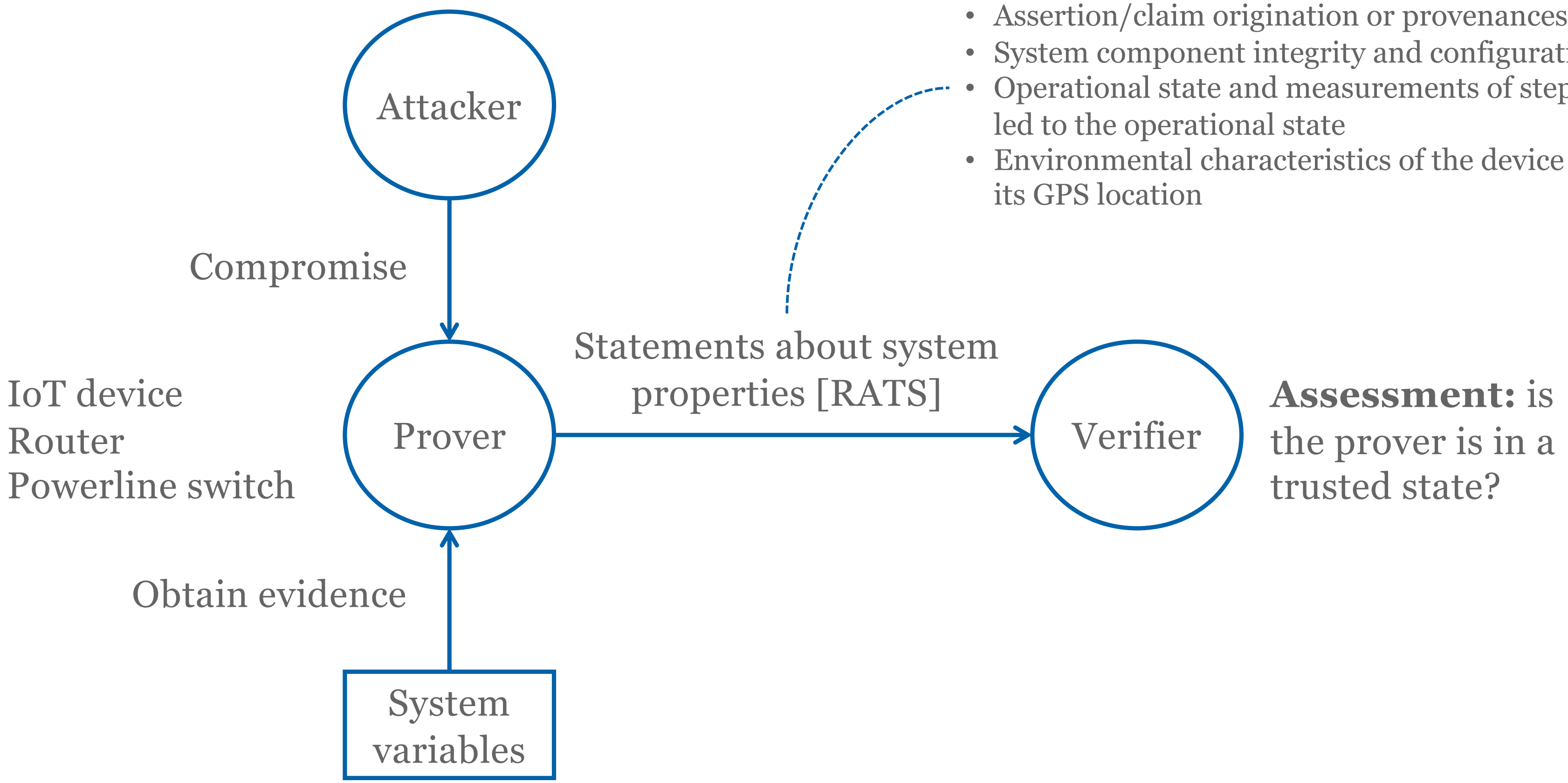
A. Network level

B. Application level

C. Both

D. Neither

Remote attestation



Attacker

Compromise

IoT device
Router
Powerline switch

Prover

Obtain evidence

System variables

Statements about system properties [RATS]

Verifier

Assessment: is the prover is in a trusted state?

- Composition and make of system components
- Assertion/claim origination or provenances
- System component integrity and configuration
- Operational state and measurements of steps which led to the operational state
- Environmental characteristics of the device such as its GPS location

[Abera] T. Abera, N. Asokan, L. Davi, F. Koushanfar, A. Paverd, A. Sadeghi and G. Tsudik, “Things, Trouble, Trust: On Building Trust in IoT Systems”, Design Automation Conference (DAC), 2016
[RATS] IETF Remote ATtestation ProcedureS WG, https://datatracker.ietf.org/group/rats/about/

Remote attestation types

- Software-based, hardware-based, hybrid
- Static (software modules) and dynamic (control flow attestation)
- Attestation of device swarms

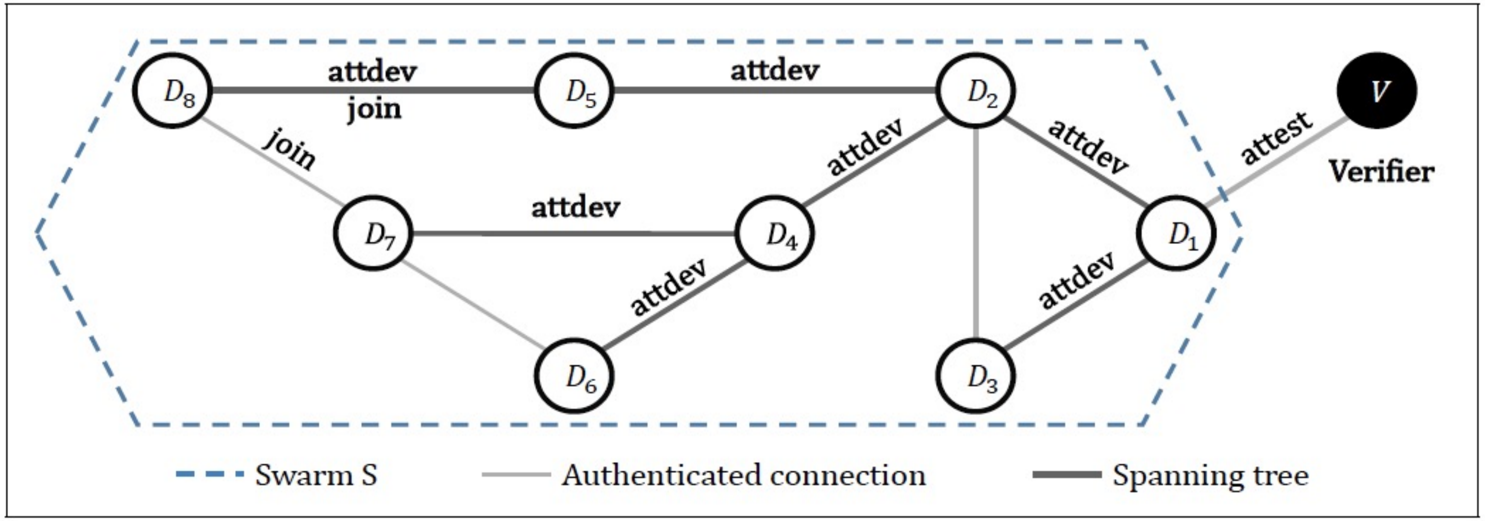


Figure 1: Swarm attestation (adapted from [3])

Gene Tsudik, “A Minimalist Approach to Remote Attestation”, https://www.youtube.com/watch?v=cL9I9OoXlVE&t=2967s

Quiz: attestation in DeadBolt

What’s the core component of the remote attestation functions that DeadBolt supports?

A. The trusted platform module

B. The device drivers

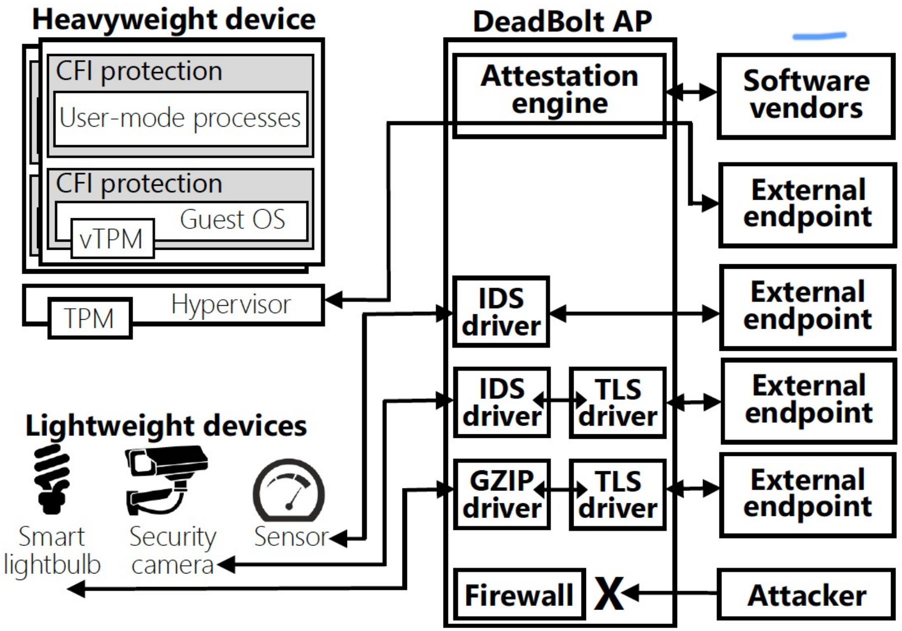
C. The firewall rules

D. The hypervisor

Discussion: pros/cons of DeadBolt design choices

- Quarantining
- Threat model
- Heaviness of heavy-weight devices
- Attestation for heavy-weight devices
- Trust model
- Description of code properties
- …

- Authors' conclusion: "We believe that DeadBolt is a practical approach for securing IoT deployments."



Key takeaways

- DeadBolt is an edge security system, device-to-gateway comms model

- Remote attestation is an interesting field of research to increase equipment trustworthiness

- Strong claim about practical applicability (in your teachers' opinion :-)

Feedback

Today’s objective revisited

- After the lecture, you will be able to discuss the design, operation, and evaluation of CommunityGuard and DeadBolt, which are two example systems that protect users and the Internet from insecure IoT devices **at the edges** of the network (e.g., in home networks)

- CommunityGuard is collaborative system, while DeadBolt a system that largely runs in isolation in the local network

- Completely different approaches, give you a feel for the spectrum of possible solutions

- Contributes to SSI learning goal #1: “Understand IoT concepts and applications, security threats, technical solutions, and a few relevant standardization efforts in the IETF”

Lecture feedback

1. To what extent do you think you’ll be able to discuss the design, operation, and evaluation of CommunityGuard? (A = 🟢, B = 🟠, C = 🔴)

2. To what extent do you think you’ll be able to discuss the design, operation, and evaluation of DeadBolt (A = 🟢, B = 🟠, C = 🔴)

Course feedback so far

- Clarity of learning goals?
- Relevance of topics?
- Alignment with prior knowledge?
- Amount of work and pace?
- Any issues with the lab assignment?
- Other?

Volg ons

.nl SIDN.nl

@SIDN

in SIDN

Discussion & feedback

Next lecture: **Wed Jun 2, 11:00-12:45**
Topic: IoT device behavior

UNIVERSITY OF TWENTE. SIDN LABS