Lecture #9: IoT Edge Security Systems (re-sit)

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

University of Twente | June 17, 2020

UNIVERSITY OF TWENTE.

SIDN LABS

Important dates

- Lab assignment: deadline upcoming Sunday (21 June 23:59)
- Acknowledge integrity statement (deadline 22 June 07:00)
- Pick a time slot for your oral exam (deadline tomorrow, 18 June 16:00).
- Fill in the questionnaire for the course to give feedback

Interactive Lecture

- Goal: enable you to learn from each other and further increase your understanding of the papers (contributes to preparing yourself for the oral exam)

- Format:
  1. We'll ask someone to provide **their opinion** of the paper
  2. A summary by teachers (put any questions in the chat)
  3. Questions: discussion starters and fact questions
  4. Discussion (use your mic)
  5. We may ask someone specific to start the discussion

- Experimental format resulting from Corona pandemic, please provide feedback!

Today's papers

Are about measuring IoT edge security systems

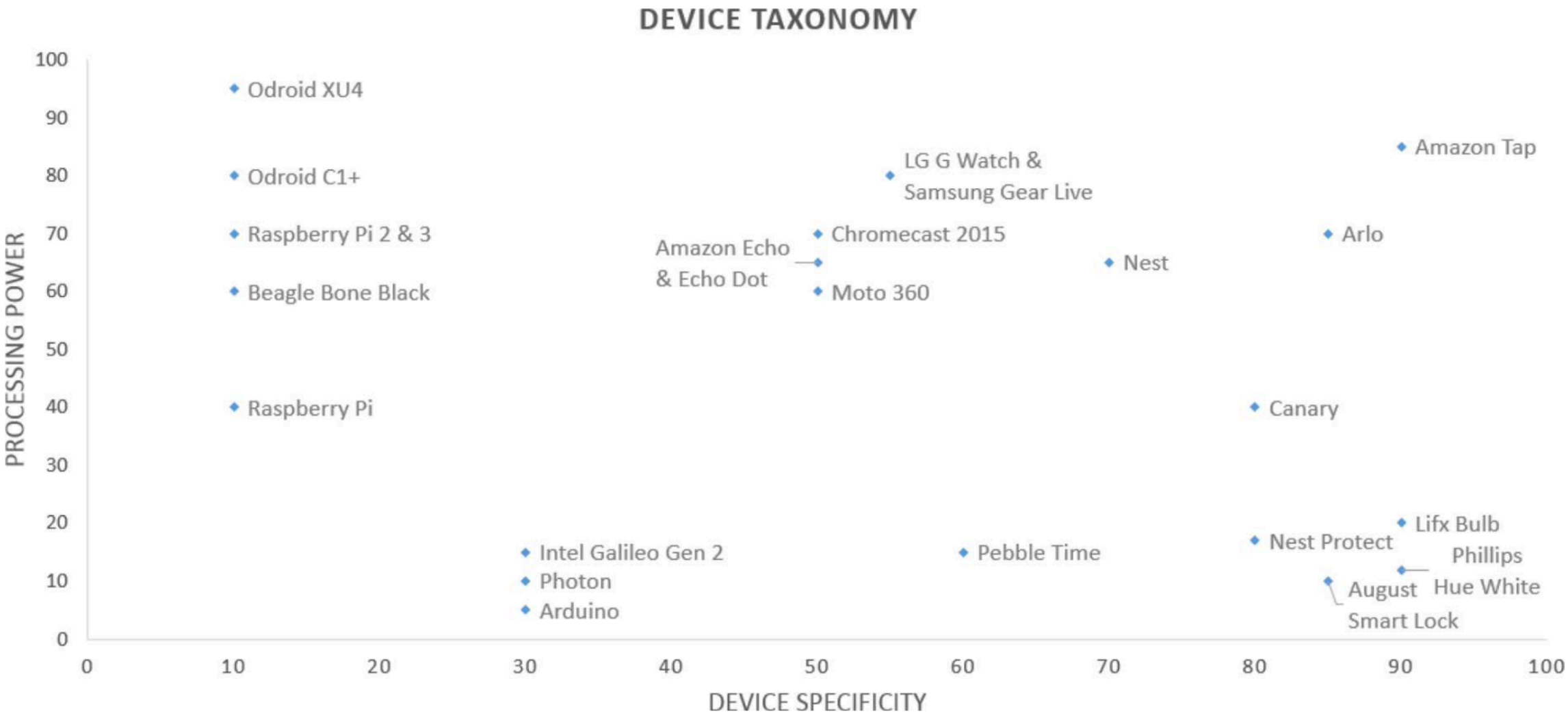
- [**Heimdall**] Javid Habibi, Daniele Midi, Anand Mudgerikar, and Elisa Bertino, "Heimdall: Mitigating the Internet of Insecure Things", IEEE Internet of Things Journal, Vol. 4, No. 4, Aug 2017

- [**NOF**] C. Dietz, R. Labaca Castro, J. Steinberger, C. Wilczak, M. Antzek, A. Sperotto, and A. Pras, "IoT-Botnet Detection and Isolation by Access Routers," 2018 9th International Conference on the Network of the Future (NOF), Poznan, 2018, pp. 88-95

“Heimdall: Mitigating the Internet of Insecure Things”

Javid Habibi, Daniele Midi, Anand Mudgerikar, and Elisa Bertino

UNIVERSITY OF TWENTE.
SDN LABS



UNIVERSITY OF TWENTE.

SDN LABS

Quiz

What is the main differences between Heimdall profiles and MUD profiles?

A. Heimdall uses XML to describe profiles
B. Heimdall includes traffic statistics on a protocol level
C. MUD profiles include DNS hostnames and are thus more stable
D. They provide the same functionality

Heimdall

- Create a profile for each monitored IoT device
- Whitelist approach
- Profile statistics (pps per protocol, in/out)
- Learning / enforcement phase
- Modes: Maximum throughput or real time validation
- Limits remote logins to list of allowed IP’s

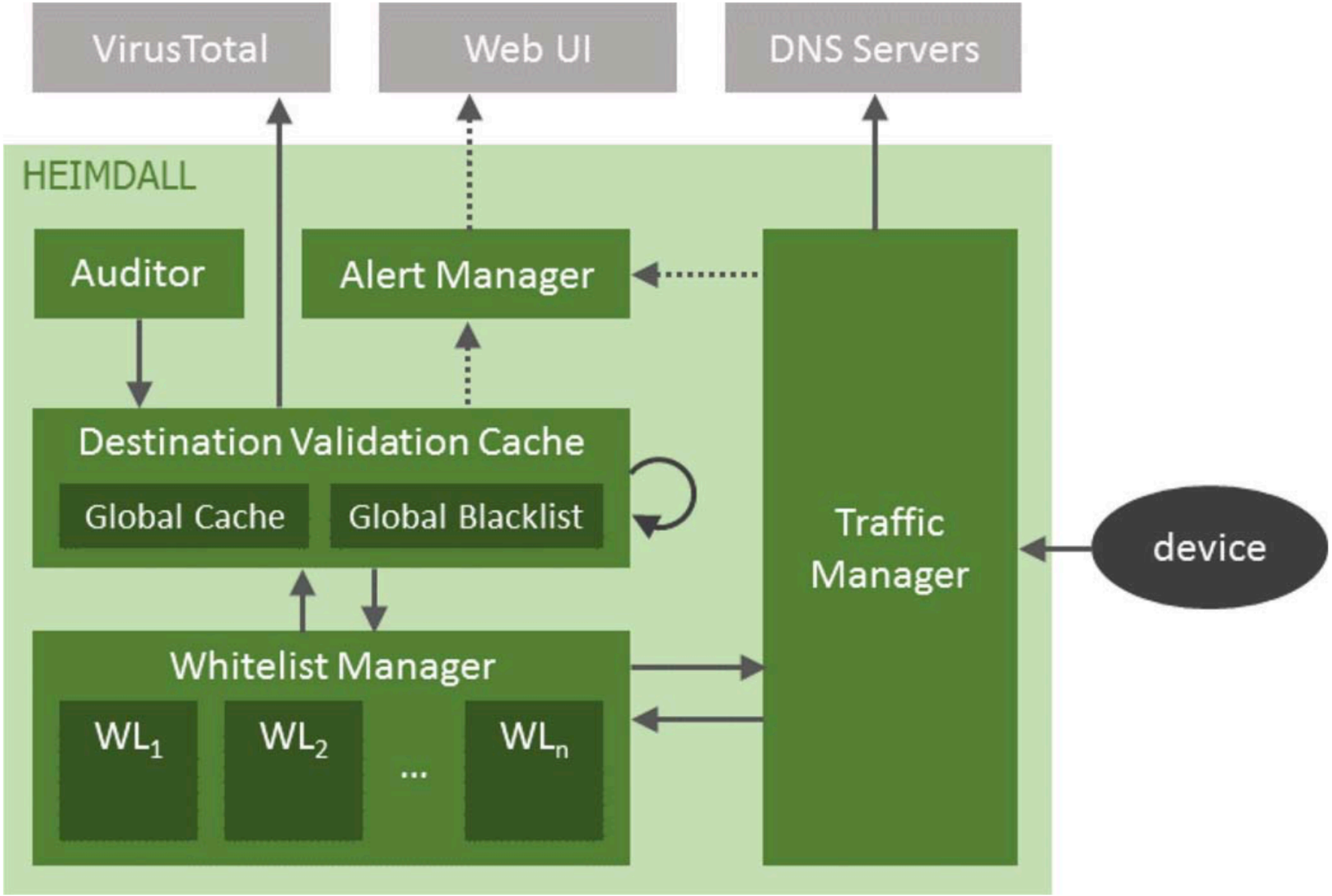
Two modes

Maximum throughput

- Use auditor to check asymmetrically
- Potentially allow malicious traffic for short interval

Real time validation

- Evaluate all traffic before allowing to pass (symmetric)
- Slow due to checks and possible Virus Total query
- DNS lookup interception (MITM?)


VirusTotal
Web UI
DNS Servers
HEIMDALL
Auditor
Alert Manager
Destination Validation Cache
Global Cache
Global Blacklist
Whitelist Manager
WL1
WL2
...
WLn
Traffic Manager
device

Quiz

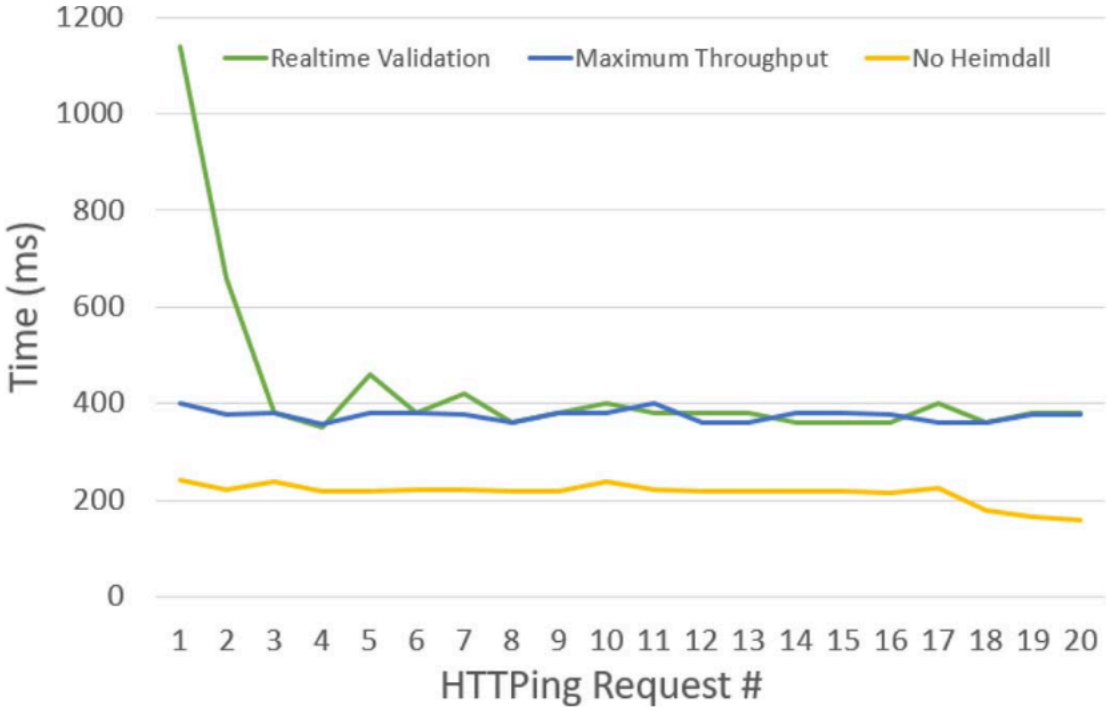
Why does Heimdall use a global blacklist when they claim a whitelist approach?

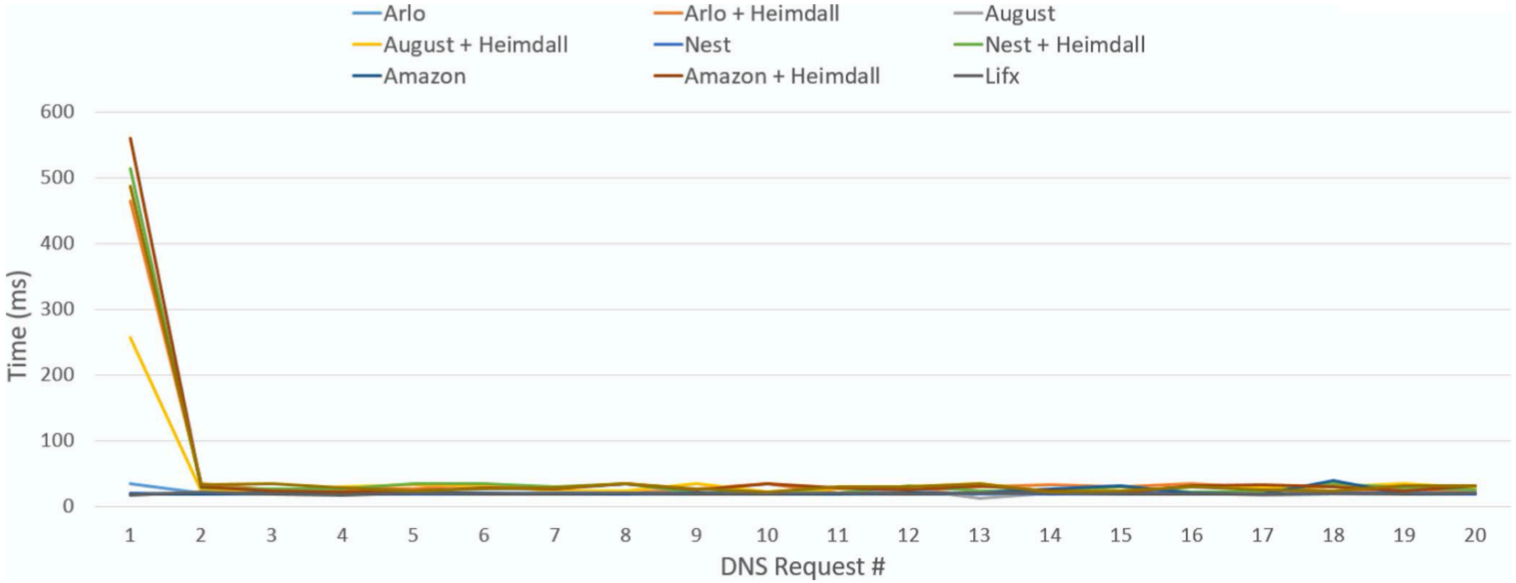
A. It's used for caching purposes
B. The whitelists are only per-device
C. Without a blacklist, new devices (learning phase) could be infected
D. The auditor has no access to individual whitelists

Evaluation

1h, 24h, 1 week.

1. Validation of no interruptions by Heimdall
   - Also check with ‘evil’ Raspberry pi
2. Measuring overhead in DNS lookups
3. Measuring network overhead





UNIVERSITY OF TWENTE.

SDN LABS

Security Analysis

Changing reliability of ip/domain

Firmware update

DNS poisoning attack

IP-only communication

Remote login and takeover (infection)

Attack scenario against Heimdall itself?

How would you ‘attack’ Heimdall?

Discussion

Heimdall relies heavily (completely) on VirusTotal.

DNS poisoning vs (e.g.) EDNS Client Subnet / DNSSEC

Global whitelist / blacklist & device-specific whitelist? Why?

Prevent attack traffic to legitimate destination?

“IoT-Botnet Detection and Isolation by Access Routers”, 9th International Conference on the Network of the Future, 2018*

C. Dietz, R. Labaca Castro, J. Steinberger, C. Wilczak, M. Antzek, A. Sperotto, and A. Pras

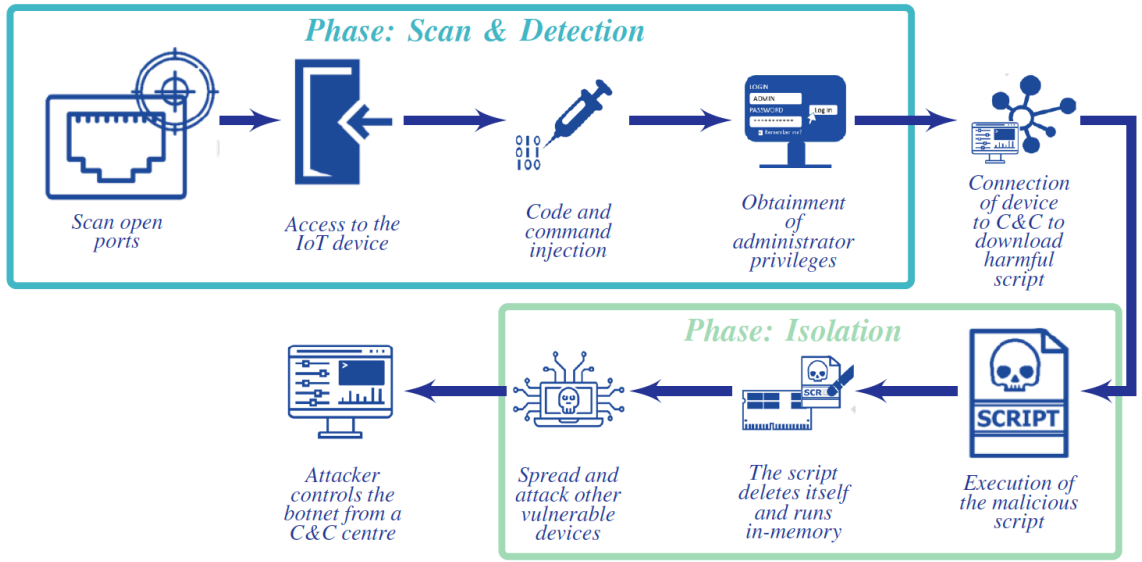
* Figures are from this paper, unless stated otherwise

UNIVERSITY OF TWENTE.

SDN LABS

Combating IoT Botnets

- Focus on the SmartHome IoT devices and the Mirai botnet family
- Botnets have similar behavior when compromising new devices
- Aims to provide an automated solution with the least amount of user interaction needed
- Two main phases: scanning & isolation

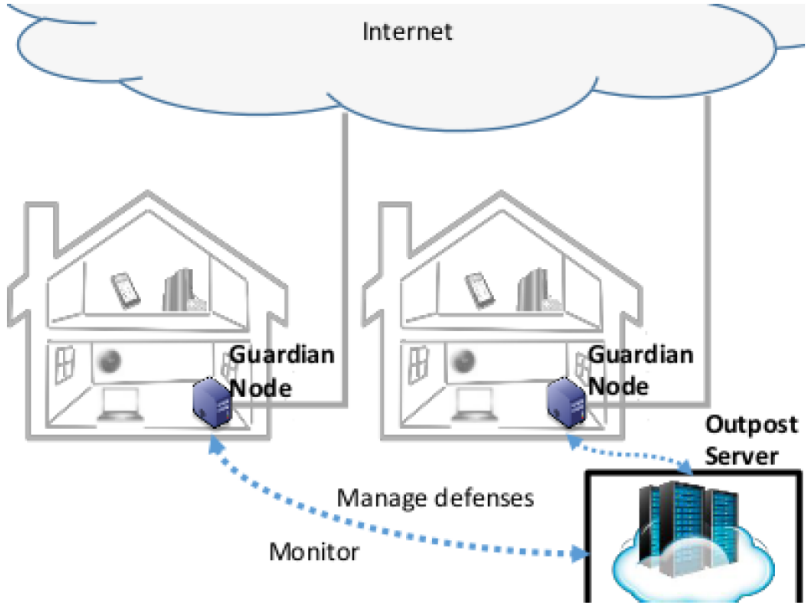


UNIVERSITY OF TWENTE.

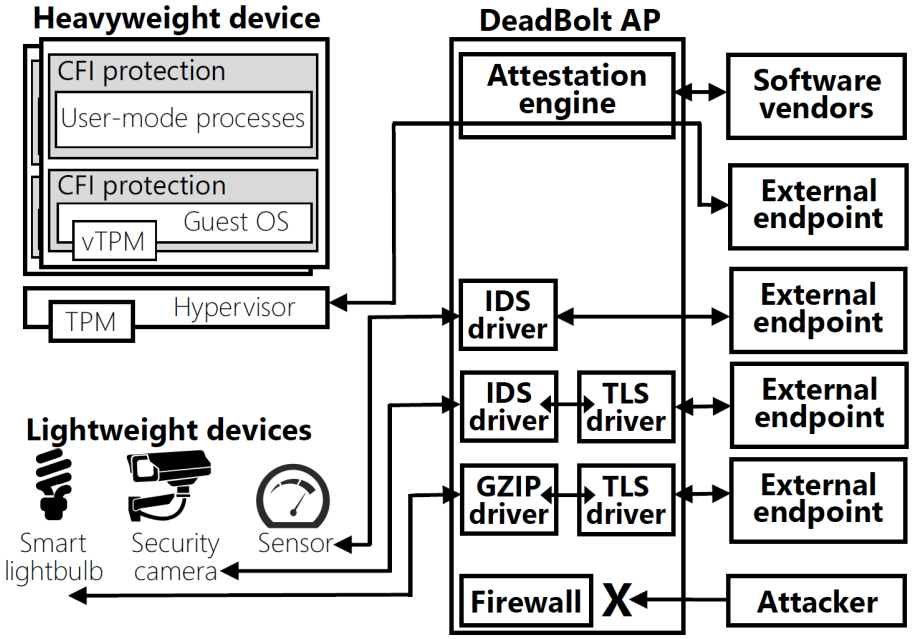
SDN LABS

Recap

- Two other edge security systems discussed in Lecture#6



Source: "CommunityGuard: A Crowdsourced Home Cyber-Security System"



Source: "DeadBolt: Securing IoT Deployments"

UNIVERSITY OF TWENTE.

SDN LABS

Quiz

Why DHCP lease table and ARP cache are used to scan connected IoT devices?

A: Using DHCP lease table helps discover more vulnerabilities

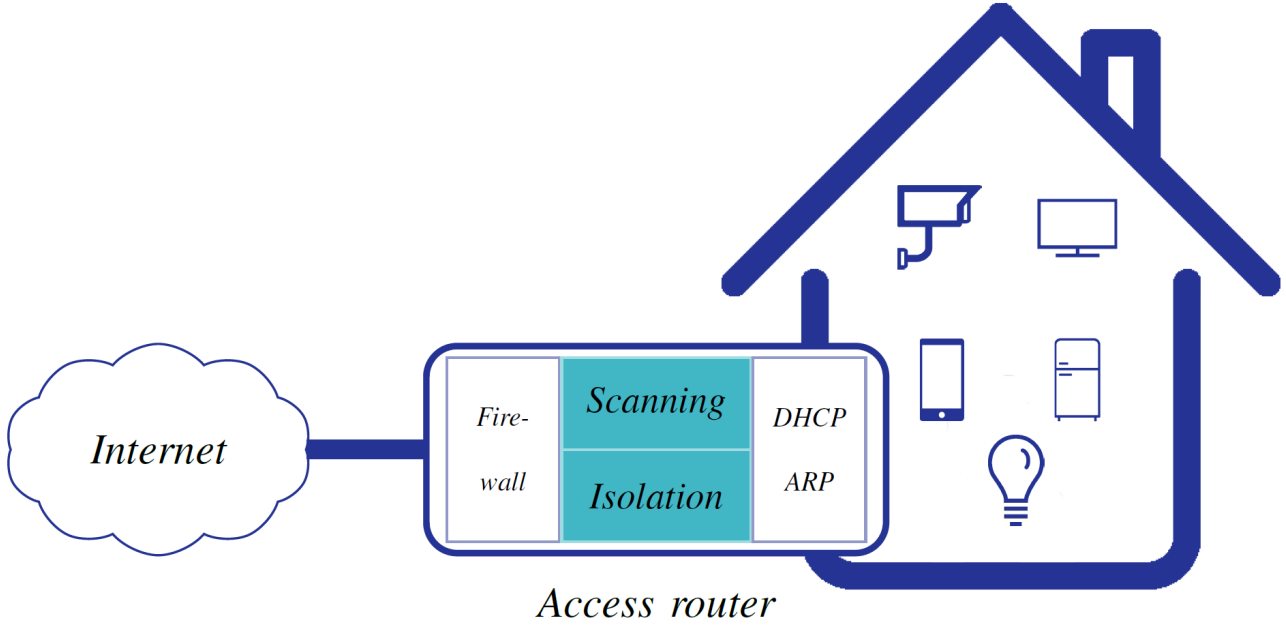
B: To make the scans more resource efficient

C: To cover devices which are not connected using WiFi/Ethernet

D: All of the above

Approach

- Scanning and detection of vulnerable devices
- Isolation of vulnerable devices
- CVE-based update mechanism
- Optimizing the scans



UNIVERSITY OF TWENTE.

SDN LABS

Isolation Approach

- All blocking actions reported to the user via email
- Additionally displayed on a web interface
- The user can also whitelist devices

Discussion

- How would a user with minimum to no IT security knowledge react to the isolation?

- How scalable is it to consider remote management from ISPs?

Evaluation

Evaluation criteria:

- i) Resource efficiency
- ii) Scalability
- iii) Platform independence
- iv) Extendability
- v) Dynamic device discovery
- vi) Ease of Deployment
- vii) Timeliness
- viii) Cost-consciousness
- ix) Open source

Would you expect any other one?

Testbeds

Testbed1: Representing a home network

- 1 access router running OpenWRT
- 1 IP camera
- 2 emulated TinyCore systems
- 1 regular personal computer

Testbed2: A virtualized network of three homes

- 1 Mirai C&C server
- 1 emulated router representing ISP network
- 3 TinyCore systems representing IP cameras

UNIVERSITY OF TWENTE.

SDN LABS

Evaluation Results

Testbed 1:

Resource efficiency:

12.5% (16MB) out of 63% total RAM usage

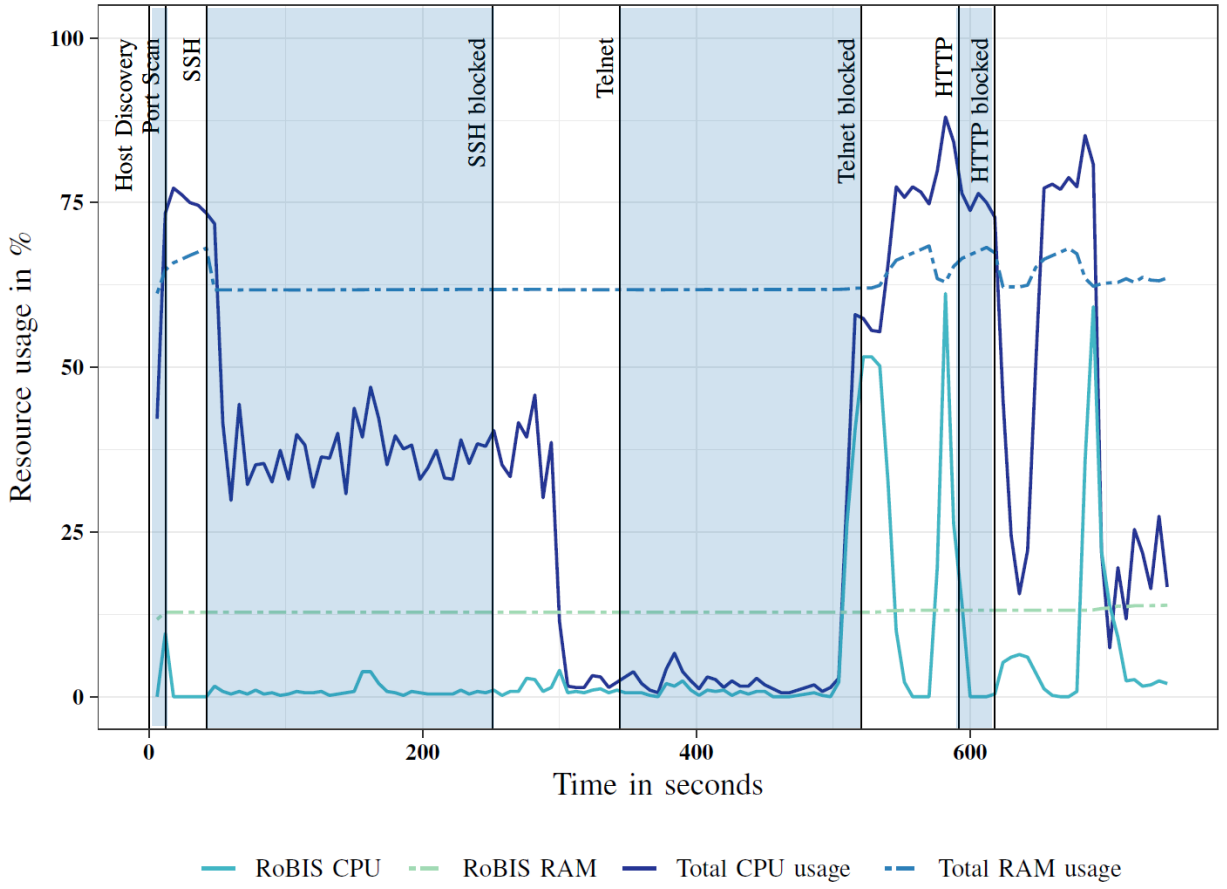
1~ 5% of CPU usage on average

“Our experiments reported that the authentication of SSH is one of the reasons why the CPU load is high, whereas Telnet and HTTP checks turn the CPU usage back to normal.”(?)

Timeliness:

A full cycle needs roughly 10 mins

Hourly checking for newly discovered vulnerabilities



UNIVERSITY OF TWENTE.

SDN LABS

Evaluation Results

Testbed 2:

	Test setup			Result		
Test	**Device 1**	**Device 2**	**Device 3**	**Device 1**	**Device 2**	**Device 3**
1	not protected	not protected	not protected	compromised	compromised	compromised
2	protected	protected	protected	no compromise	no compromise	no compromise
3	protected	not protected	protected	no compromise	compromised	no compromise
4	not protected	protected	not protected	compromised	not compromised	compromised

UNIVERSITY OF TWENTE.

SDN LABS

Key Takeaways

- IoT security systems can be implemented with a low cost if placed closer to the edge devices
- Privacy concerns are reduced when there is no cooperation between SmartHomes or with a central node
- Simple steps in securing IoT devices can avoid large scale attacks

Discussion

- What are the advantages/disadvantages of the four edge security systems discussed during this course?

- Do we really need a cooperative/distributed solution such as one discussed in CommunityGuard paper?

- Why aren't these systems yet deployed in practice?

Volg ons

SIDN.nl

@SIDN

SIDN

Discussion & feedback

1. Don't forget to hand in your lab assignment in time!
2. Submit the integrity statement.
3. Sign up for a timeslot for the oral exam.

Next week: oral exams.

UNIVERSITY OF TWENTE.

SIDN LABS