Lecture #6: IoT Edge Security Systems

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

University of Twente | May 27, 2020

UNIVERSITY OF TWENTE.

SIDN LABS

Lab assignment

- MUD descriptions: you'll need to generate them yourselves, tools are available
- IoT devices: you'll need to work with the actual hardware, no emulations (unless as an extra)
- Use IoT devices without a browser-like interface, such as light bulbs, audio speakers, doorbells
- Do not use multi-purpose devices like tablets, phones, laptops
- At least 2 IoT devices per group of 3 and at least 3 devices per group of 4
- Etienne Khan available for assistance

UNIVERSITY OF TWENTE.

SDN LABS

Paper summaries

- You must have handed in your two summaries BEFORE this lecture
- You can use the summaries during the oral exam (“open book”)
- You **cannot** complete SSI without submitting 12 paper summaries!

UNIVERSITY OF TWENTE.

SIDN LABS

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. 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!

UNIVERSITY OF TWENTE. SIDN LABS

“CommunityGuard: A Crowdsourced Home Cyber-Security System”, SDN-NFV Security, 2017*

Chase E. Stewart, Anne Maria Vasu and Eric Keller

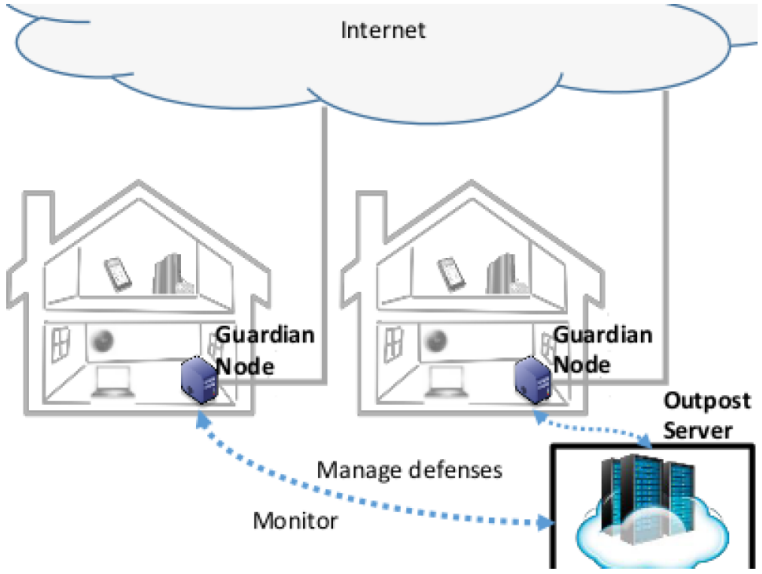
UNIVERSITY OF TWENTE.

SDN LABS

* Figures are from this paper, unless stated otherwise

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 amount of subnets that deploy it

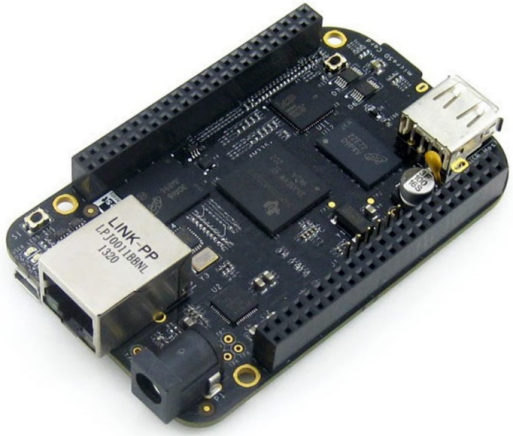


UNIVERSITY OF TWENTE.
SDN LABS

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

UNIVERSITY OF TWENTE.

SDN LABS

Question

Who should be responsible for running the CommunityGuard Outpost Server?

A: Specific IoT device vendors

B: ISPs

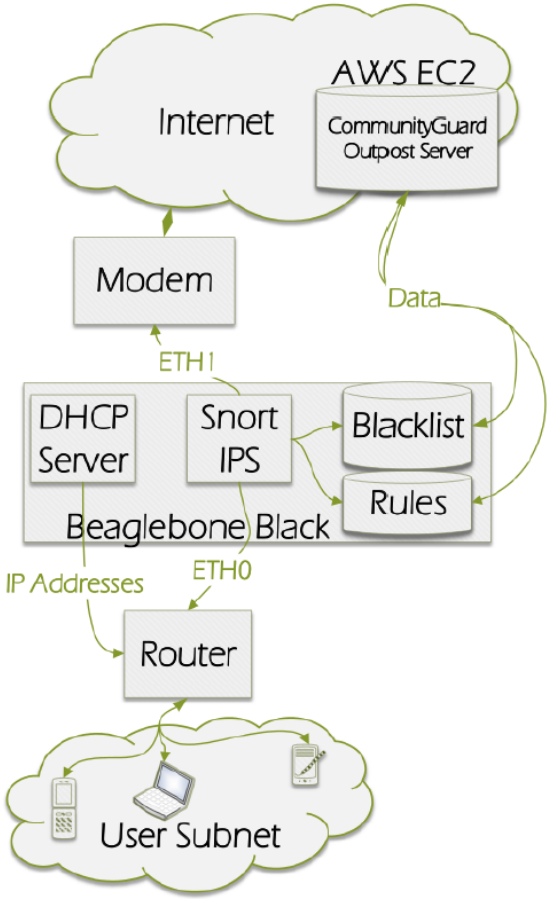
C: Cloud providers

D: ...

C-Guard Prototype

Three 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



UNIVERSITY OF TWENTE.

SDN LABS

Quiz

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

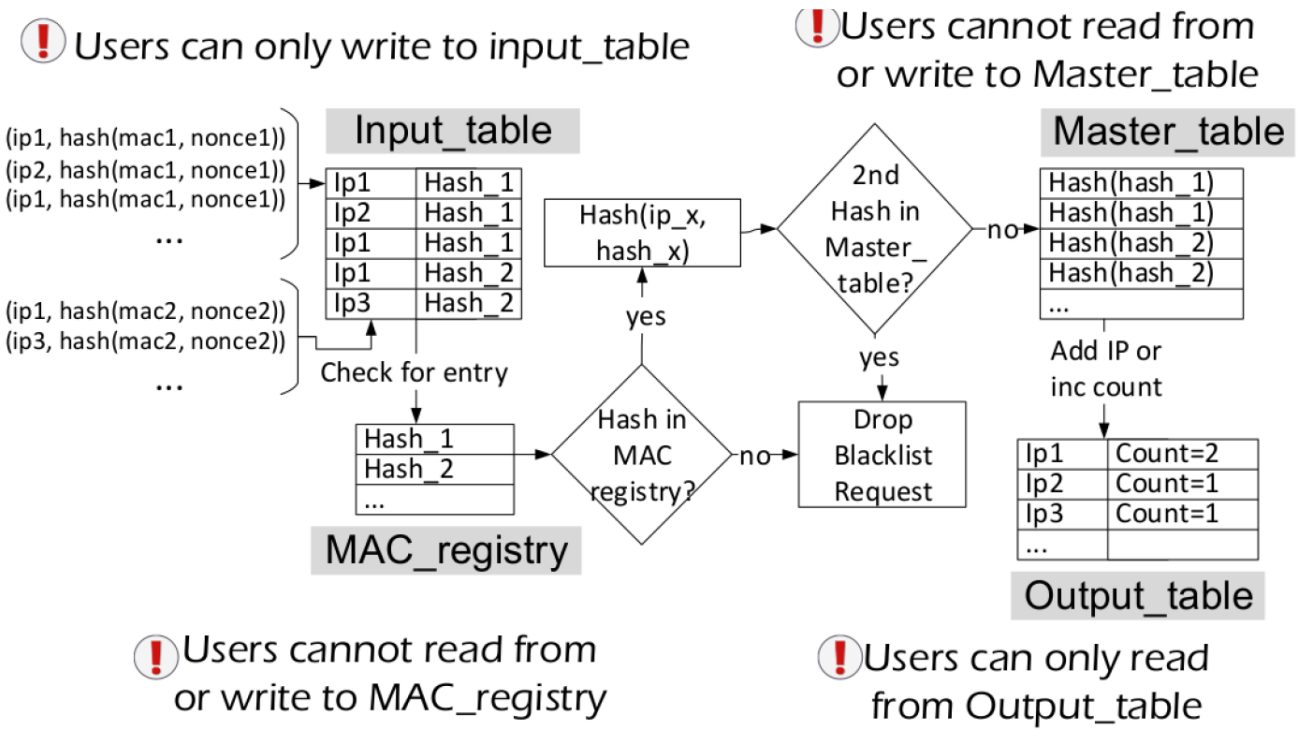
A: getting access to user data

B: infecting other networks with Malware

C: removing malicious IP addresses from blacklist

D: trying to blacklist legitimate IP addresses

Server Blacklist

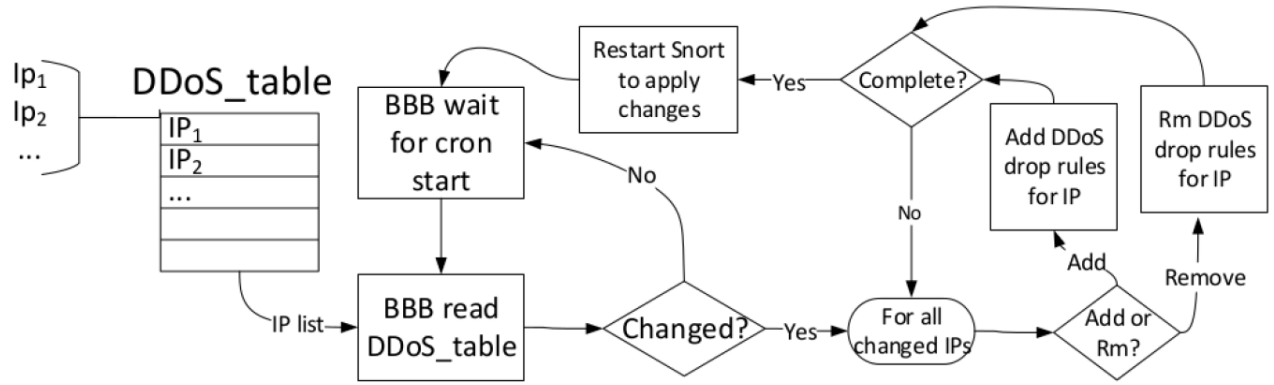


UNIVERSITY OF TWENTE.

SDN LABS

Outgoing DDoS Prevention

Developers add DDoSed server IPs to table



Users can only read from DDoS_table

UNIVERSITY OF TWENTE.

SDN LABS

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

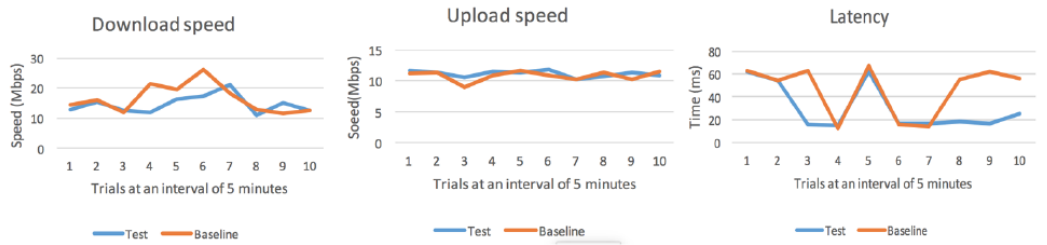
Performance

Limiting factors:

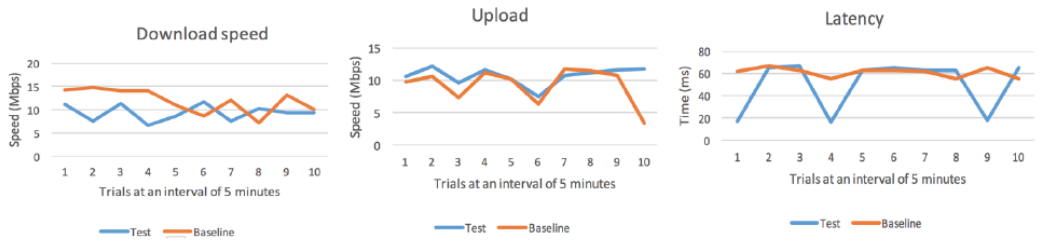
- USB to Ethernet adapter
- Slow SD card writes

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

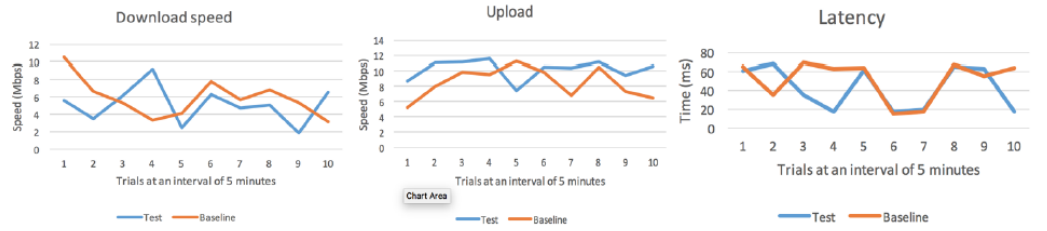
Low Load



Average Load



Heavy Load



UNIVERSITY OF TWENTE.

SDN LABS

Lessons Learned

- 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)

UNIVERSITY OF TWENTE. SIDN LABS

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?

UNIVERSITY OF TWENTE.

SIDN LABS

“DeadBolt: Securing IoT Deployments”, Applied Networking Research Workshop, Montreal, QC, Canada, July 16, 2018 (ANRW ’18)

UNIVERSITY OF TWENTE.

SDN LABS

Quiz: key IoT issue

What's the key IoT issue that Deadbolt's security services aim to tackle?

A. Autonomy of IoT devices

B. Heterogeneity of IoT devices

C. Invisibility of IoT devices

D. Interoperability of IoT devices

UNIVERSITY OF TWENTE. SIDN LABS

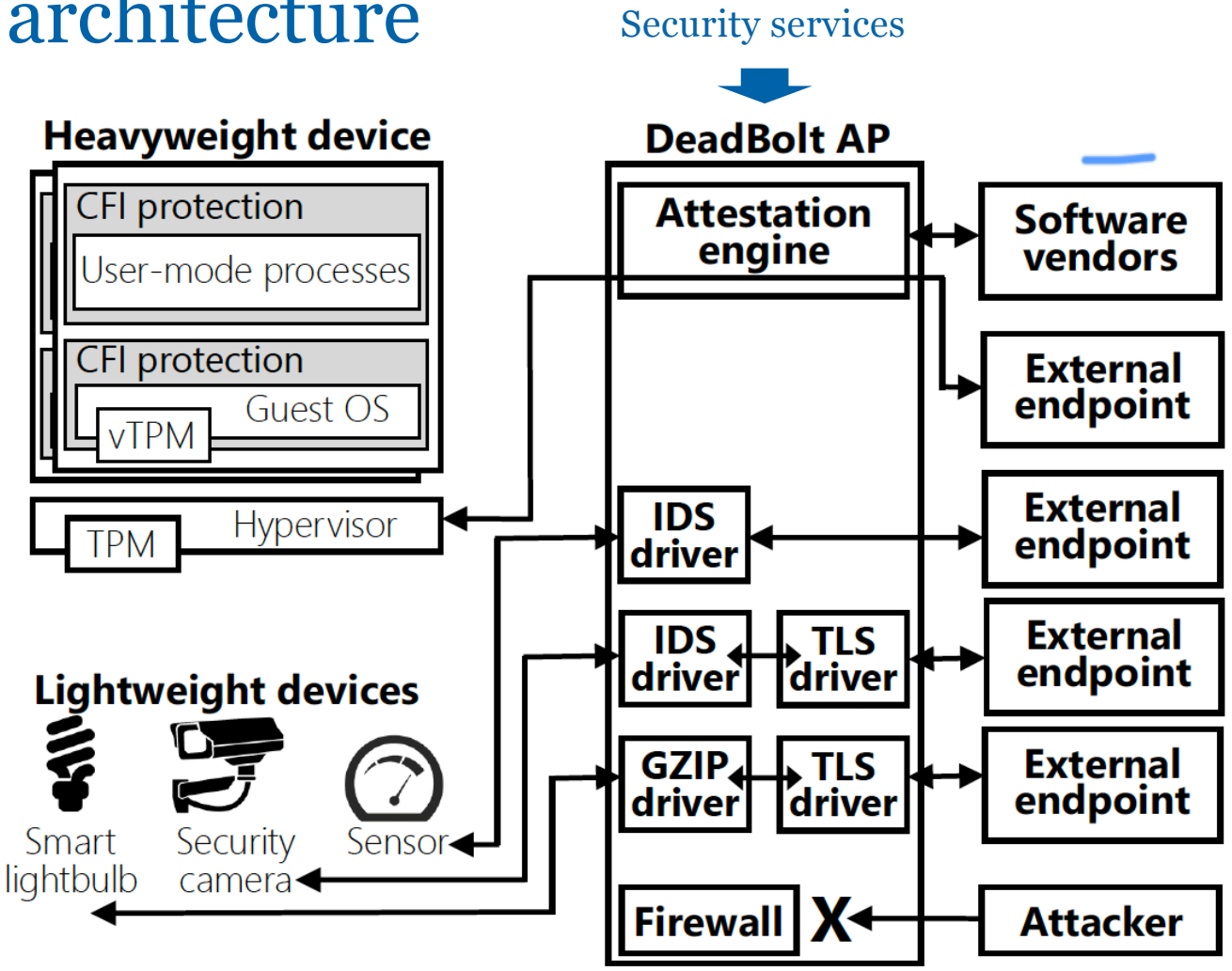
DeadBolt key concepts

- Security functions
  - Verification that device software is up to date
  - Protection against remote exploits (control flow attacks)
  - TLS to exchange data
  - Deny-by-default firewall

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

UNIVERSITY OF TWENTE. SDN LABS

DeadBolt architecture



OF TWENTE.

SIDN LABS

Quiz: operation

At what level in the protocol stack does DeadBolt operate?

A. Network level

B. Application level

C. Both

D. Neither

Quiz: fast patching

What steps does Deadbolt go through to patch devices?

A. AP blocks device, sends the firmware to the device, deblocks it after update

B. Device launches a new VM, updates it, then swaps new and primary VMs

C. Devices fetches the new firmware and then reboot to install

D. Devices launch a virtual driver, which fetches the firmware, and push it to the device

Remote attestation

- Relying party (verifier) assesses trustworthiness of remote (IoT) systems (provers) [Abera]
  - Software-based, hardware-based, hybrid
  - Attestation of device swarms, control flow attestation (hash over the execution path)

- Relying party requesting evidence about attributes, such as [RATS]:
  - 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/
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

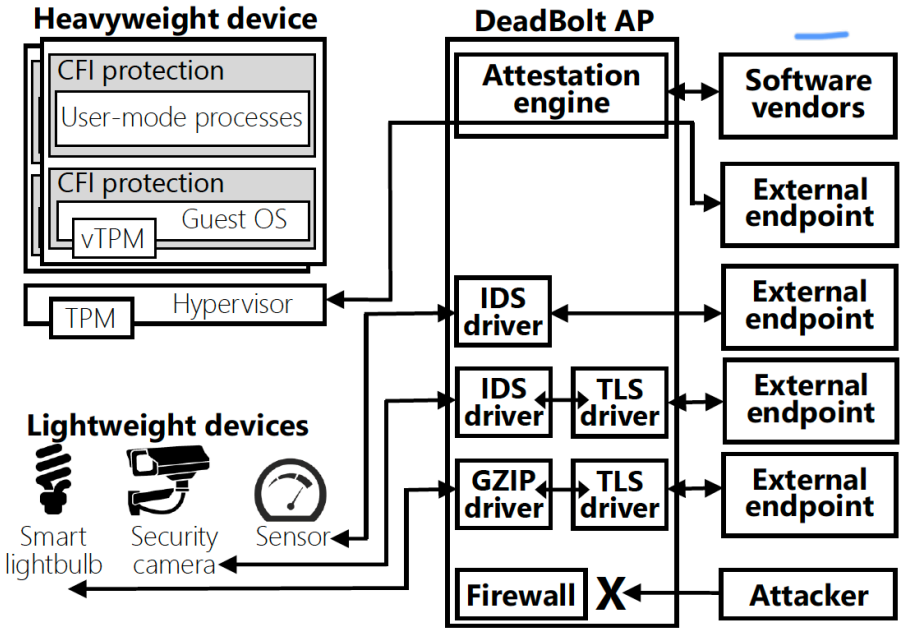
UNIVERSITY OF TWENTE.

SDN LABS

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."



UNIVERSITY OF TWENTE.

SDN LABS

Key takeaways

- DeadBolt is an edge security system, device-to-gateway comms model
- Remote attestation is an interesting feature, separate field of research
- Strong claim about practical applicability (in your teachers' opinion :-)

UNIVERSITY OF TWENTE.

SIDN LABS

Volg ons

SIDN.nl

@SIDN

SIDN

Discussion & feedback

Next lecture: **Wed Jun 3, 10:45-12:30**
Topic: IoT device behavior

UNIVERSITY OF TWENTE.

SIDN LABS

Before we go: status of your lab assignments?

- We usually get quite a few questions in class, but that's different now
- Thumbs up or down in the chat + group number
- Groups 1 through 11 (minus 3)

UNIVERSITY OF TWENTE.

SDN LABS