Lecture #4: IoT edge security systems

Cristian Hesselman, Elmer Lastdrager,
Ramin Yazdani, Etienne Khan, Ting-Han Chen

University of Twente | May 17, 2022

UNIVERSITY OF TWENTE.

SIDN LABS

Key concept: gateway

RSITY OF TWENTE.

SDN LABS

Today's agenda

- Admin
- Introduction to today's lecture
- Paper on FIAT
- Break
- Paper on DeadBolt
- Feedback

Admin

UNIVERSITY OF TWENTE.

SDN LABS

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
2	May 3	Lecture: IoT and Internet Core Protocols
3	May 10	Lecture: IoT Botnet Measurements 1
4	May 17	Lecture: IoT Edge Security Systems
5	May 24	Lecture: IoT Device Security
6	May 31	Lecture: IoT Botnet Measurements 2
7	Jun 1	Guest lecture #1: naval systems, Dr. Sorin Iacob, Thales
8	Jun 5	Lecture: IoT Security in Non-Carpeted Areas
9	Jun 12	Guest lecture #2: the Internet ecosystem, Marco Davids, SIDN Labs
10	Jun 14	Lecture: IoT Honeypots (re-sit)

UNIVERSITY OF TWENTE.

SIDN LABS

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: **Fri June 23, 2023, 23:59 CEST**
- All to be submitted through CANVAS

UNIVERSITY OF TWENTE.

SDN LABS

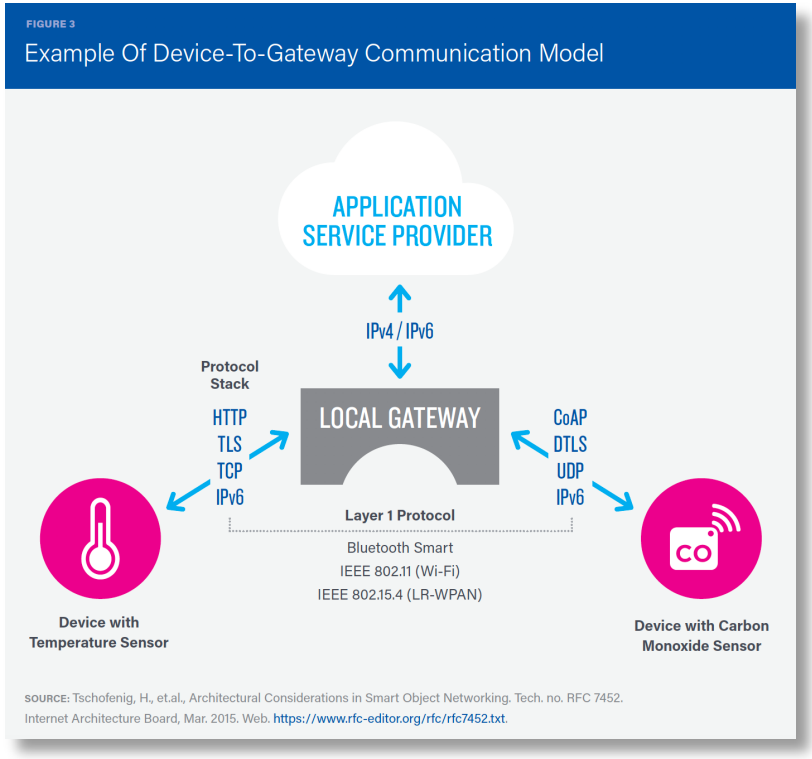
Introduction to today's lecture

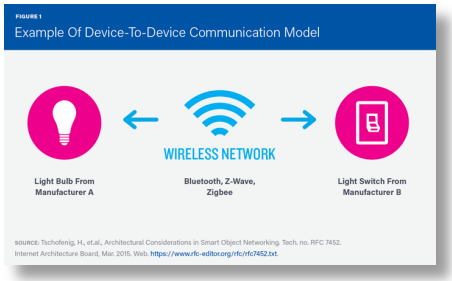
UNIVERSITY OF TWENTE.

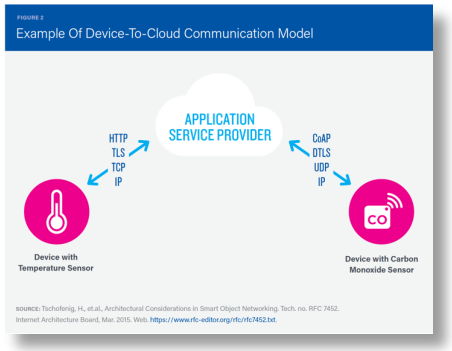
SIDN LABS

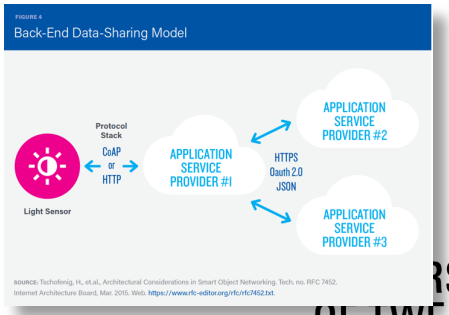
Motivation for today: important IoT comms model

- Security
- Protocol translation
- Cell phone
- Hub device









H. Tschofenig,, J. Arkko, D. Thaler, D. McPherson, “Architectural Considerations in Smart Object Networking”, RFC7452, March 2015
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

Poll: what would you do if…

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

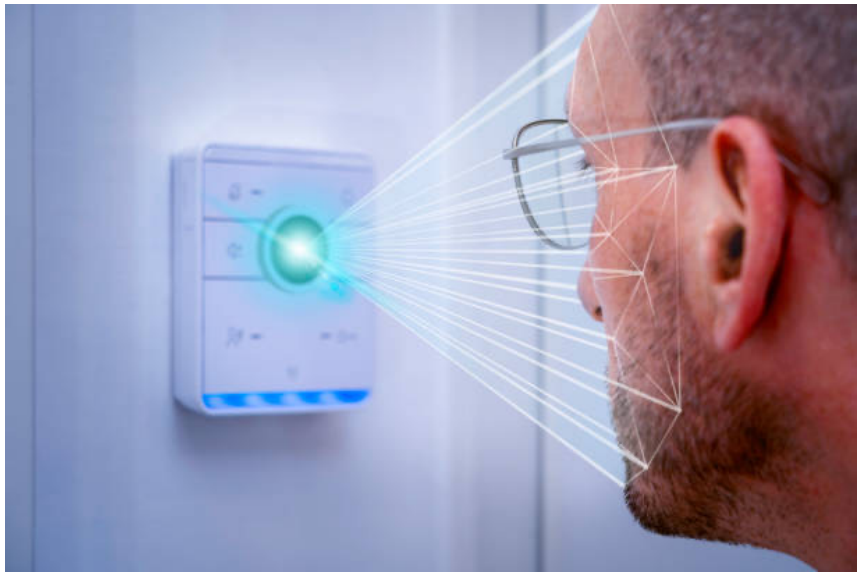
A. Device-to-device

B. Device-to-cloud

C. Device-to-gateway

D. Back-end data sharing

And of course: why? ☺



UNIVERSITY OF TWENTE.

SDN LABS

Today's papers

[FIAT] Y. Xiao and M. Varvello, "FIAT: Frictionless Authentication of IoT Traffic", Proceedings of the 18th International Conference on Emerging Networking EXperiments and Technologies (CoNEXT '22), 2022, https://doi.org/10.1145/3555050.3569126

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

Solid science [FIAT] and more practical work [DBolt]

Today's learning objective

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

- Different approaches, will give you a feel for the spectrum of possible gateway solutions (there are many more)

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

Y. Xiao and M. Varvello,

“FIAT: Frictionless Authentication of IoT Traffic

18th International Conference on Emerging Networking EXperiments and Technologies (CoNEXT ’22), 2022

UNIVERSITY OF TWENTE.

SIDN LABS

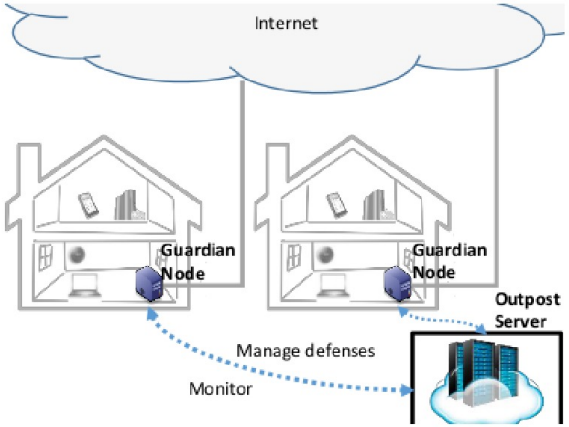
Differences in Edge Security Architectures

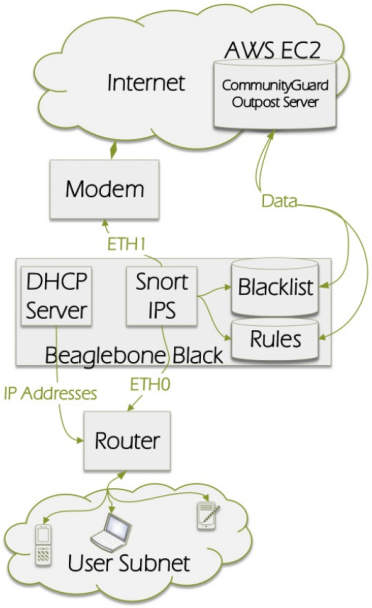
- Who should they protect?
- What type of counter measures should be considered? blocking, patching, notifying*, …
- What could be the implications of setting automatic security policies on devices? How would end users react to this?
- …

* https://holmes.distributit.nl

UNIVERSITY OF TWENTE. SDN LABS

Defending against DDoS



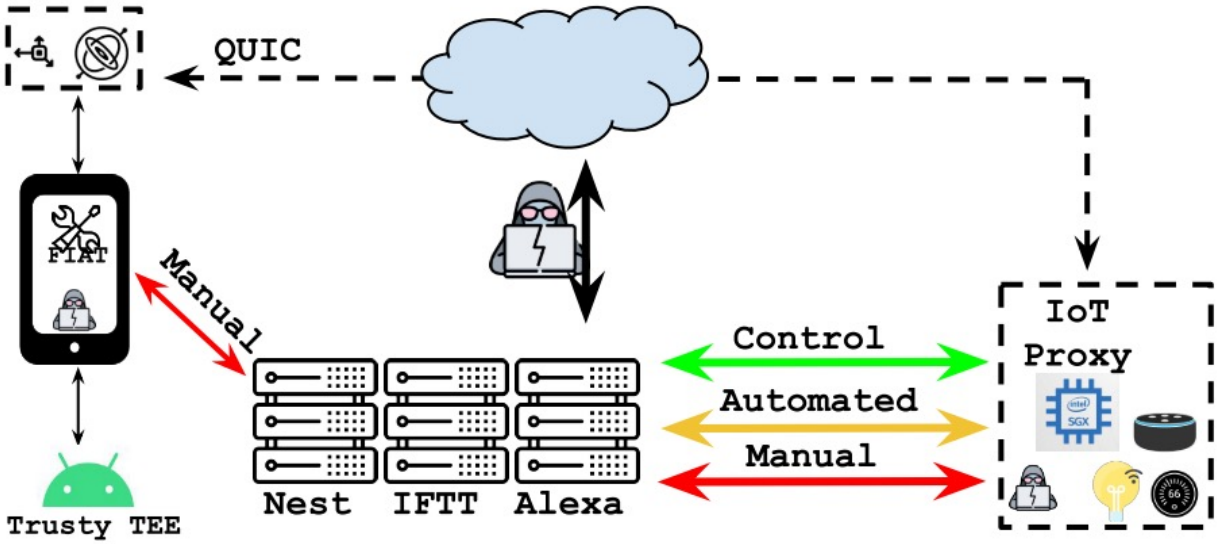


Additional reading: Stewart, Chase E., Anne Maria Vasu, and Eric Keller. "CommunityGuard: A crowdsourced home cyber-security system." *Proceedings of the ACM International workshop on security in software defined networks & network function virtualization*. 2017.

UNIVERSITY OF TWENTE.

SDN LABS

FIAT's Architecture



- Is this diagram clear?

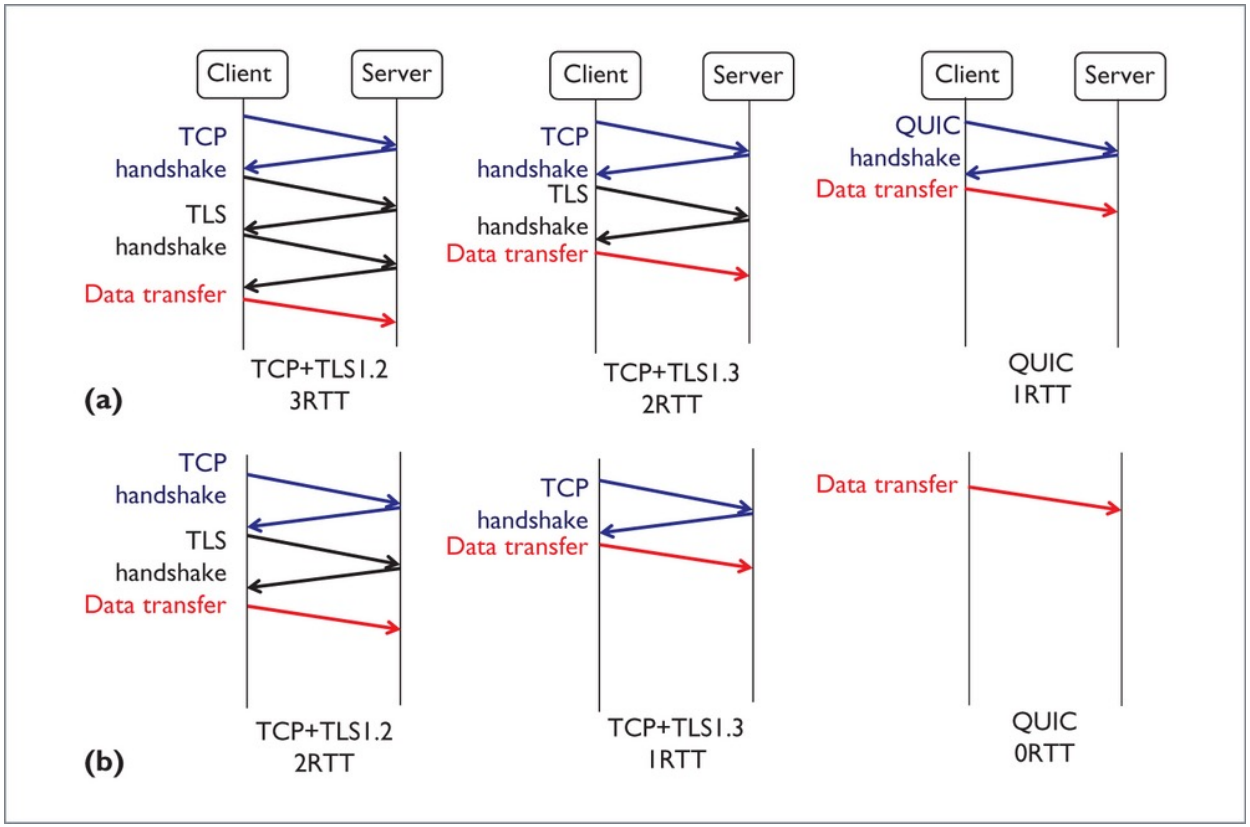
UNIVERSITY OF TWENTE.

SDN LABS

QUIC 0-RTT

Re-negotiation

Session resumption



Source: https://techcommunity.microsoft.com/t5/itops-talk-blog/smb-over-quic-files-without-the-vpn/ba-p/1183449

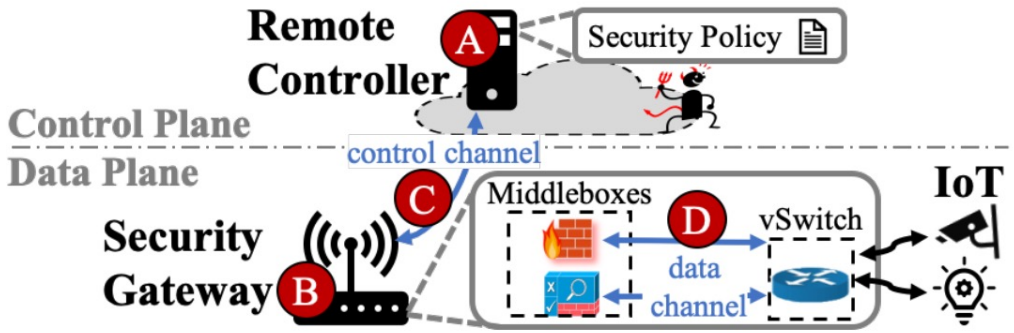
UNIVERSITY OF TWENTE.

SDN LABS

Attack Vectors

What are the potential attack vectors to be considered by edge (bolt-on) security architectures?

Attack Vectors



*Source: [HotEdge20]**

* **Additional reading:** McCormack, Matt, et al. "Towards an Architecture for Trusted Edge {IoT} Security Gateways." *3rd USENIX Workshop on Hot Topics in Edge Computing (HotEdge 20)*. 2020.

UNIVERSITY OF TWENTE. SDN LABS

Gateway Vulnerabilities

TALOS-2018-0627/CVE-2018-3963
TALOS-2018-0633/CVE-2018-3968
TALOS-2018-0634/CVE-2018-3969
TALOS-2018-0653/CVE-2018-3985
TALOS-2018-0671/CVE-2018-4002
TALOS-2018-0672/CVE-2018-4003
TALOS-2018-0681/CVE-2018-4011
TALOS-2018-0683/CVE-2018-4012
TALOS-2018-0686/CVE-2018-4015
TALOS-2018-0702/CVE-2018-4030
TALOS-2018-0703 /CVE-2018-4031

Source: https://www.newegg.com/insider/cujo-smart-home-network-security/

Local and remote code execution, boot and safe browsing bypass

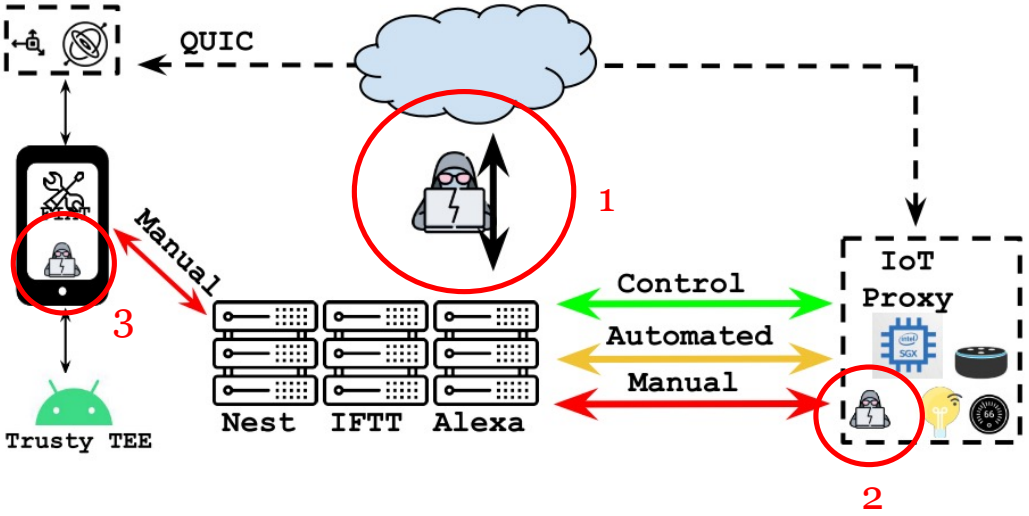
Read more on: https://blog.talosintelligence.com/vuln-spotlight-cujo

UNIVERSITY OF TWENTE.
SDN LABS

Attacker Model

The attacker is considered to be able to :

1. compromise any IoT account of the user,
2. control the home network,
3. compromise any of the devices associated with FIAT.

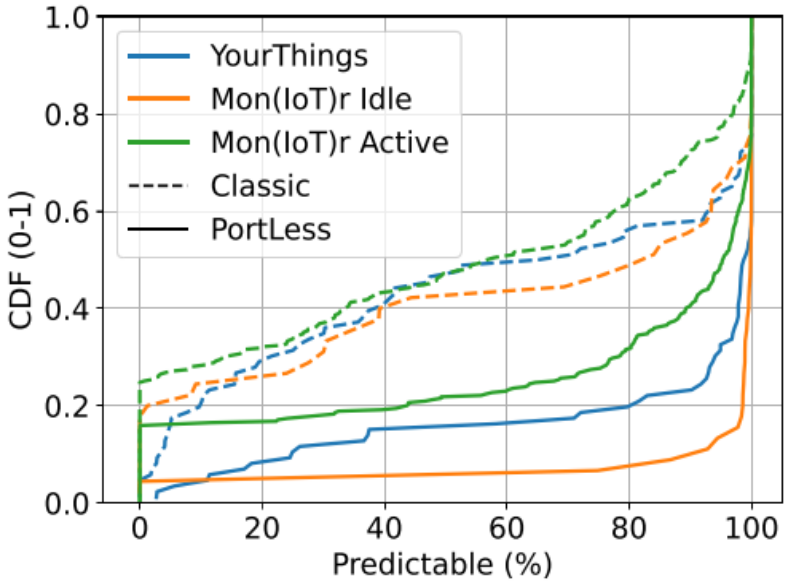


UNIVERSITY OF TWENTE.

SDN LABS

Traffic Predictability

- Do you agree that IoT traffic is predictable?
- Could there be a bias in the measured devices?
- Flow definition:
  - Classic: < *ip_src, ip_dst, port_src, port_dst, proto, size* >
  - Portless: < *ip_src, domain_name, proto, size* >



UNIVERSITY OF TWENTE.

SIDN LABS

Traffic Predictability

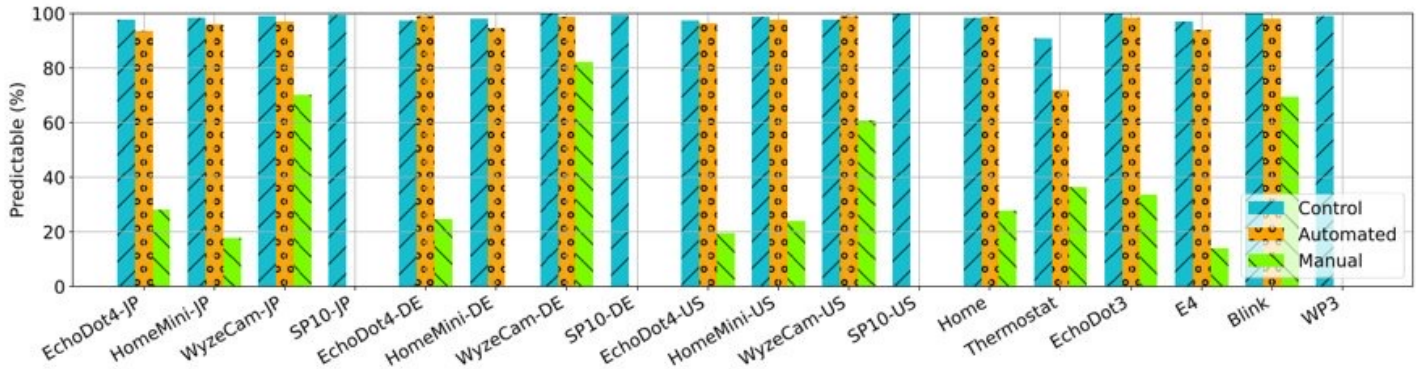
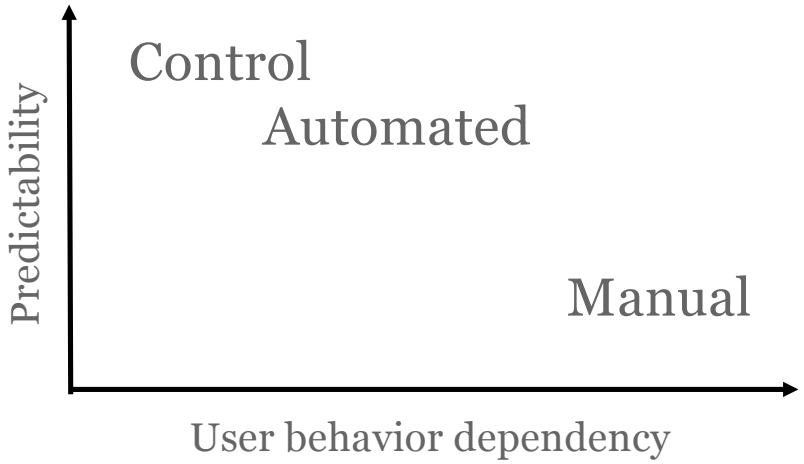


Figure 2: Predictability of control, automated, and manual traffic in our testbed using the PortLess flow definition.



UNIVERSITY OF TWENTE.

SDN LABS

Traffic Predictability

- Nest thermostat is equipped with a motion sensor and is capable to turn its screen off when no mobile phone is in the same LAN.

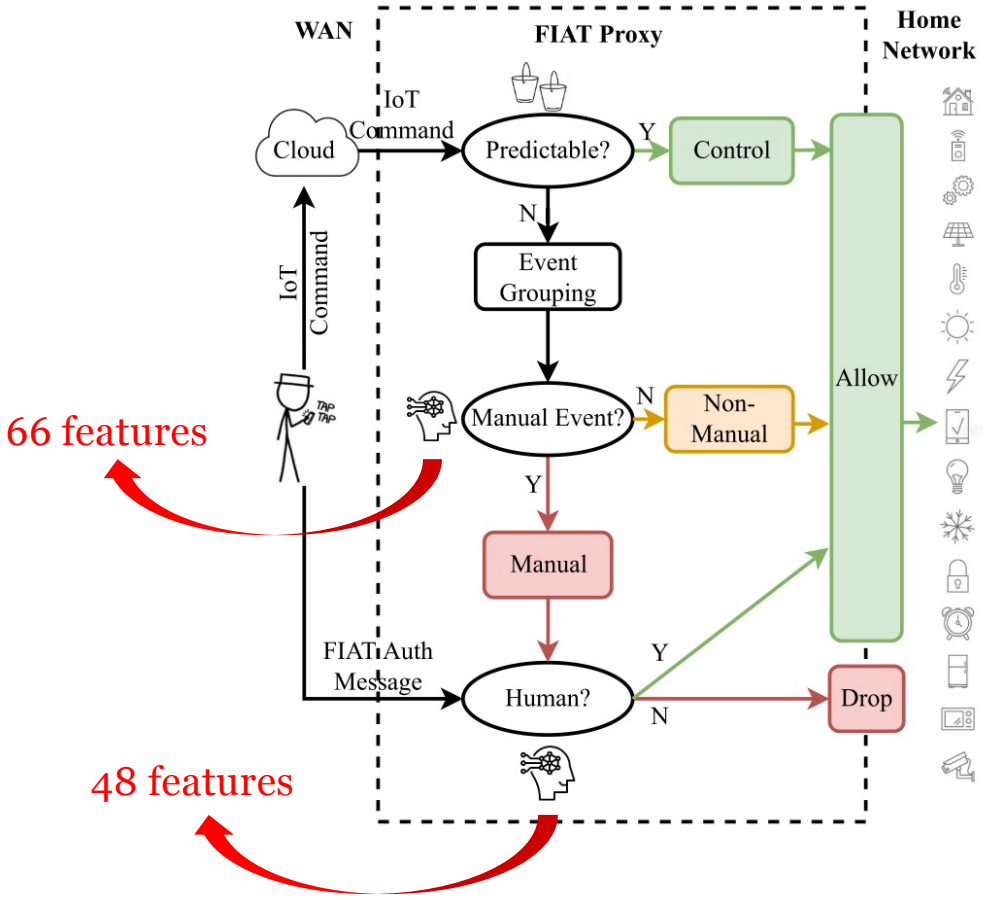
- Cameras (WyzeCam and Blink) have higher manual traffic predictability since video streams are typically constant rate.

Machine Learning

- [FIAT] heavily relies on machine learning.
- Can we blindly trust machine learning algorithms to detect and take actions on anomalies in the IoT?
- Do we want machine learning for the IoT security? If so, should we focus on explainable ML?
- Are all IoT devices smart phone dependent?

FIAT's IoT Proxy

- Grouping unpredictable traffic into events with a threshold of 5 seconds?
- Number of ML features?
- Unpredictable manual events are dropped (and the user is notified) if FIAT does not verify a human activity. Is this any problematic?



App Dependency

- [FIAT] heavily relies on the assumption that an IoT device is used with a companion APP. Is this a fair assumption?

Sugawara et al. "Light commands: laser-based audio injection attacks on voice-controllable systems." Proceedings of the 29th USENIX Conference on Security Symposium, 2020.

Breaking Into a Smart Home With A Laser - Smarter Every Day 229

https://www.youtube.com/watch?v=ozIKwGt38LQ&ab_channel=SmarterEveryDay

Key Takeaways

- Edge security deployments need to consider multiple relevant attacker models.

- ML introduces some benefits, but it has its own challenges when dealing with network traffic.

Coffee break

UNIVERSITY OF TWENTE.

SIDN LABS

“DeadBolt: Securing IoT Deployments”

Applied Networking Research Workshop, Montreal, QC, Canada, July 2018

UNIVERSITY OF TWENTE.

Wooclap quizzes

Copy participation link

1. Go to wooclap.com
2. Enter the event code in the top banner

Event code
CPSKTX

1. Send @CPSKTX to 0970 1420 2908
2. You can participate

UNIVERSITY OF TWENTE.

SIDN LABS

Discussion: what are Deadbolt's key components?

Discussion: what are Deadbolt's key components?

- Trusted gateway (AP)
- Bolts: (third party) virtual device derivers (proxies) → light weight IoT devices
- Virtual Machines (VMs) → heavy weight IoT devices

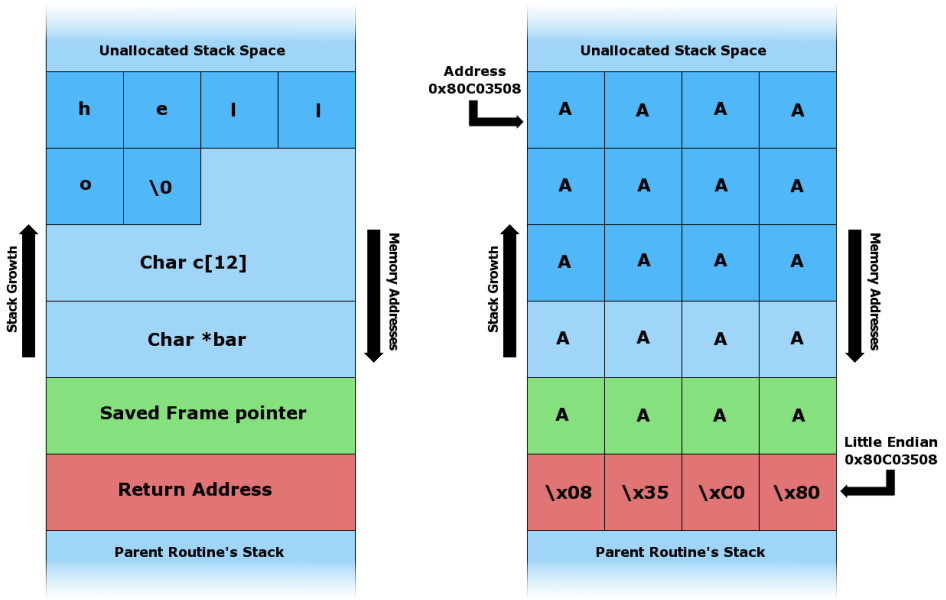
Discussion: what are Deadbolt's key functions?

Discussion: what are Deadbolt's key functions?

- Virtual network functions (e.g., encryption, scanning for malicious packets)
- Remote attestation (static) with device quarantining
- Protect against program flow attacks (dynamic attestation)
- Fast patching (VM swap for heavy weight devices)

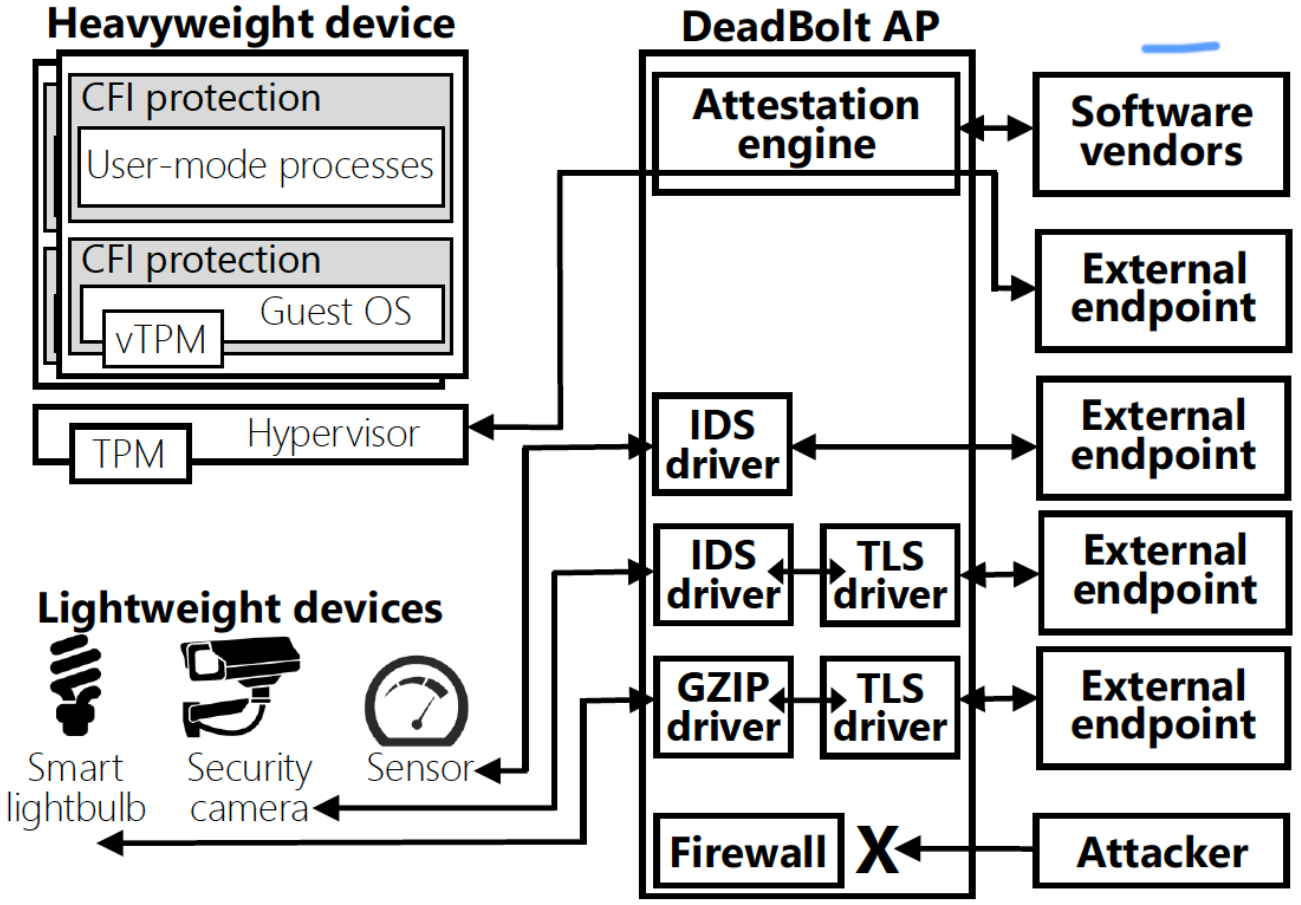
Discussion: what are Deadbolt's key functions?

- Virtual network functions (e.g., encryption, scanning for malicious packets)
- Remote attestation (static) with device quarantining
- Protect against program flow attacks (dynamic attestation)
- Fast patching (VM swap for heavy weight devices)



https://en.wikipedia.org/wiki/Stack_buffer_overflow

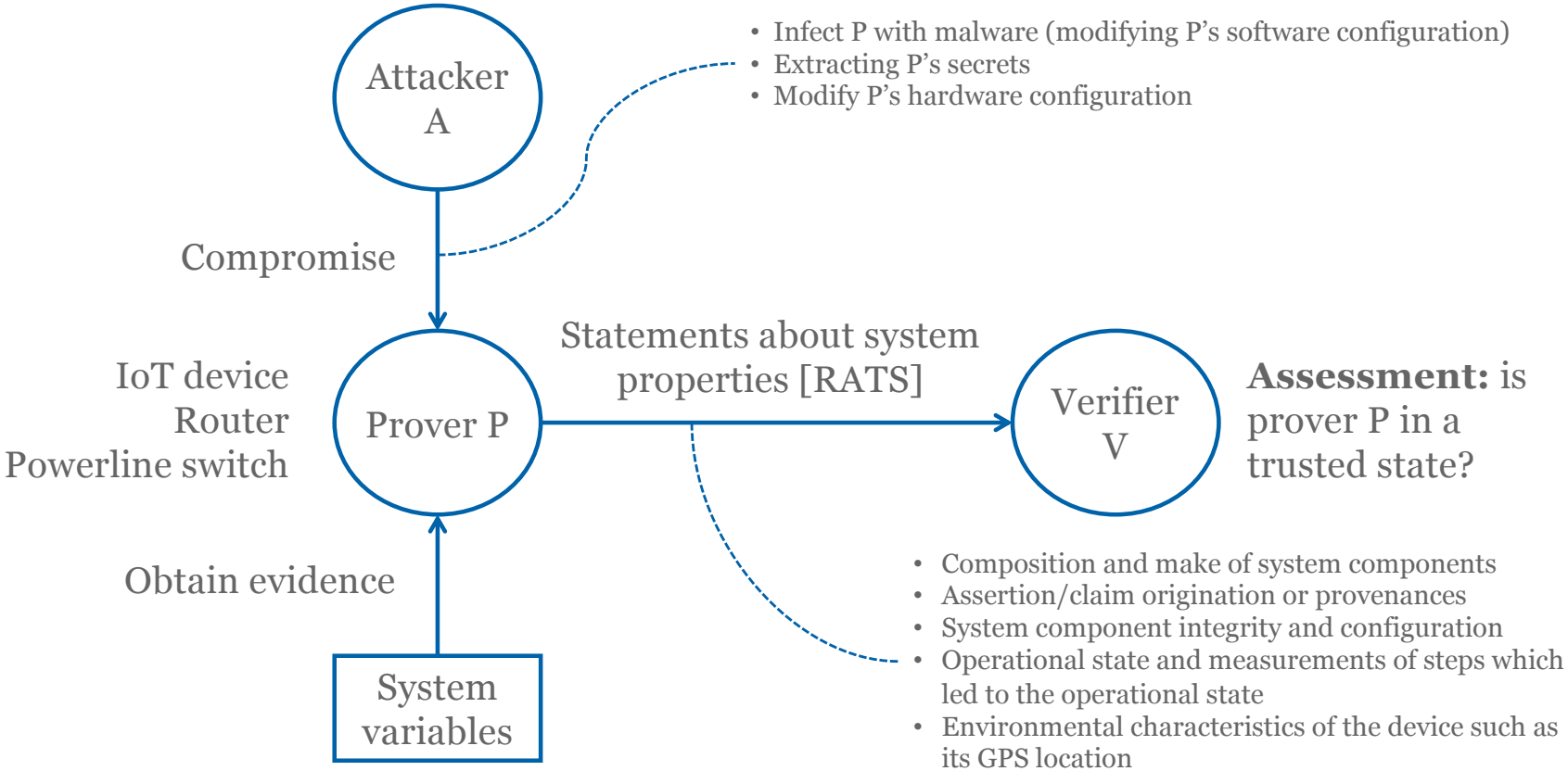
So, what about that DeadBolt architecture?



UNIVERSITY OF TWENTE.

SIDN LABS

Extra: remote attestation



[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

EXTRA TIME

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

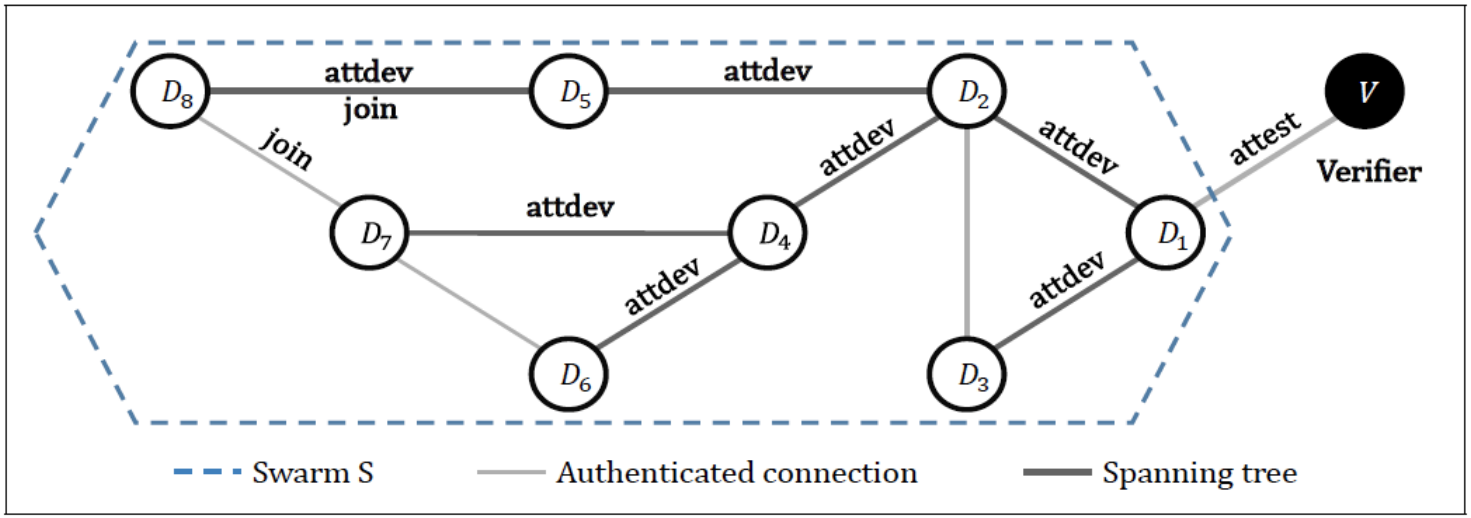


Figure 1: Swarm attestation (adapted from [3])

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

OF TWENTE.

SDN LABS

Discussion: what's your opinion on DeadBolt?

- Quarantining?
- Threat model?
- Trust model?
- Code protection properties?
- Pre-lecture discussion topic: what would it take to get DeadBolt deployed at a large scale?
- …

Further discussion?

Key takeaways

- DeadBolt is an edge security system, device-to-gateway comms model
- Adds remote attestation to IoT deployments
- Strong claim about practical applicability (in your teachers' opinion :-)

Today's learning objective revisited

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

- Different approaches, will give you a feel for the spectrum of possible gateway solutions (there are many more)

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

Volg ons

SIDN.nl

@SIDN

SIDN

See you next week!

Wed May 24, 10:45-12:30
Topic: IoT Device Security

No guest lecture on Mon May 22!

UNIVERSITY OF TWENTE.

SIDN LABS