Lecture #6: IoT edge security systems

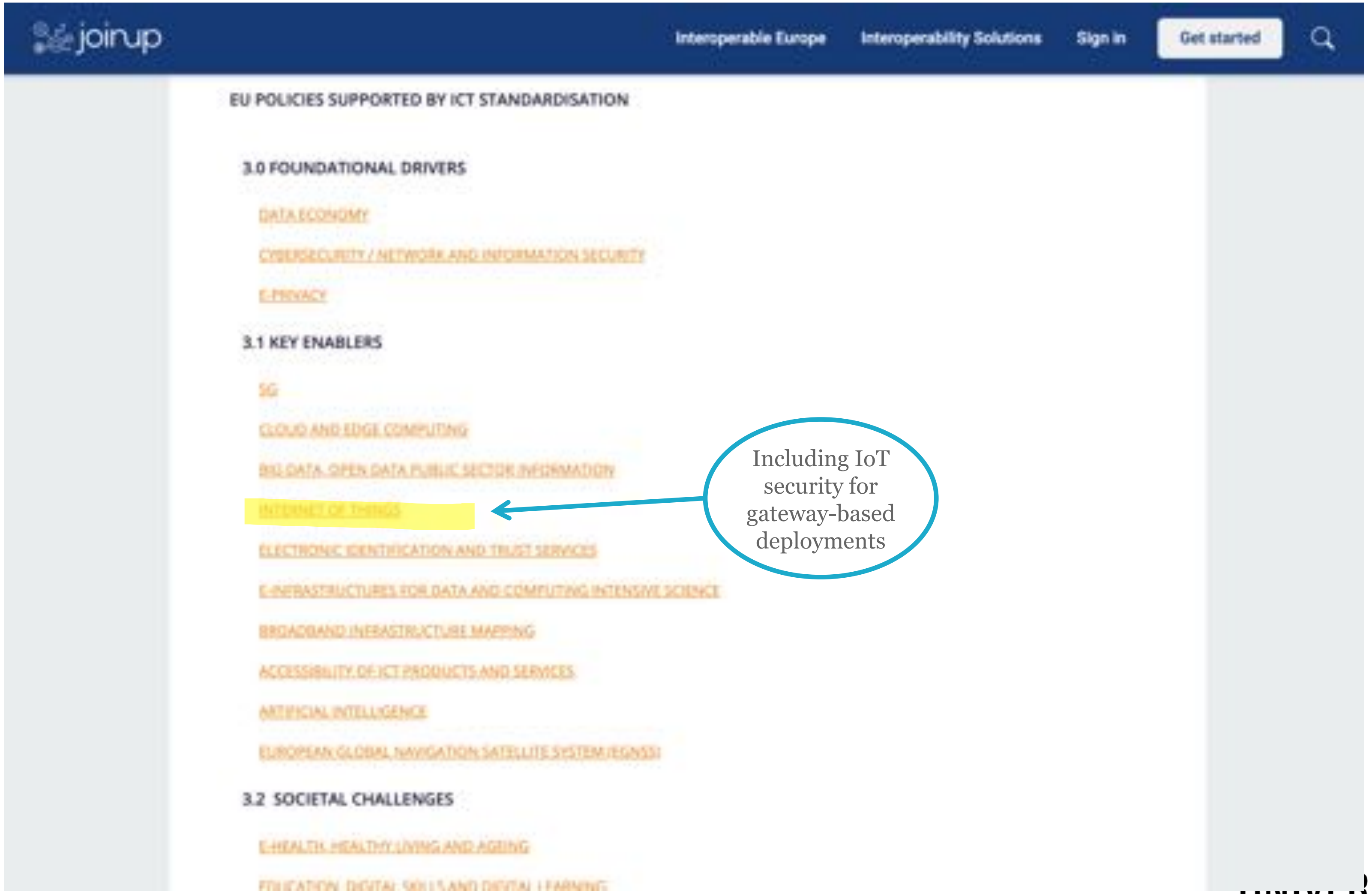
Cristian Hesselman, Elmer Lastdrager, Ramin Yazdani, and Etienne Khan

University of Twente | June 1, 2022

Key concept: gateway

EU’s rolling plan for ICT standardization, May 25, 2022

https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2022



EU POLICIES SUPPORTED BY ICT STANDARDISATION

3.0 FOUNDATIONAL DRIVERS

- DATA ECONOMY
- CYBERSECURITY / NETWORK AND INFORMATION SECURITY
- E-PRIVACY

3.1 KEY ENABLERS

- 5G
- CLOUD AND EDGE COMPUTING
- BIG DATA, OPEN DATA PUBLIC SECTOR INFORMATION
- INTERNET OF THINGS
- ELECTRONIC IDENTIFICATION AND TRUST SERVICES
- E-INFRASTRUCTURES FOR DATA AND COMPUTING INTENSIVE SCIENCE
- BROADBAND INFRASTRUCTURE MAPPING
- ACCESSIBILITY OF ICT PRODUCTS AND SERVICES
- ARTIFICIAL INTELLIGENCE
- EUROPEAN GLOBAL NAVIGATION SATELLITE SYSTEM (EGNSS)

3.2 SOCIETAL CHALLENGES

- E-HEALTH, HEALTHY LIVING AND AGEING
- EDUCATION, DIGITAL SKILLS AND DIGITAL LEARNING

Including IoT security for gateway-based deployments

Today’s agenda

- Admin
- Introduction to today’s lecture
- Paper on attack resilient IoT architecture
- Break
- Paper on DeadBolt
- Feedback

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 7	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 15	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

Where are you with your lab assignment?

- Still trying to find the instructions on the SSI site
- Designing measurement setup
- Analyzing measurements
- Writing lab report
- Just need to click “submit” in Canvas

Introduction to today’s lecture

Motivation for today: important IoT comms model

- Security
- Protocol translation
- Cell phone
- Hub device

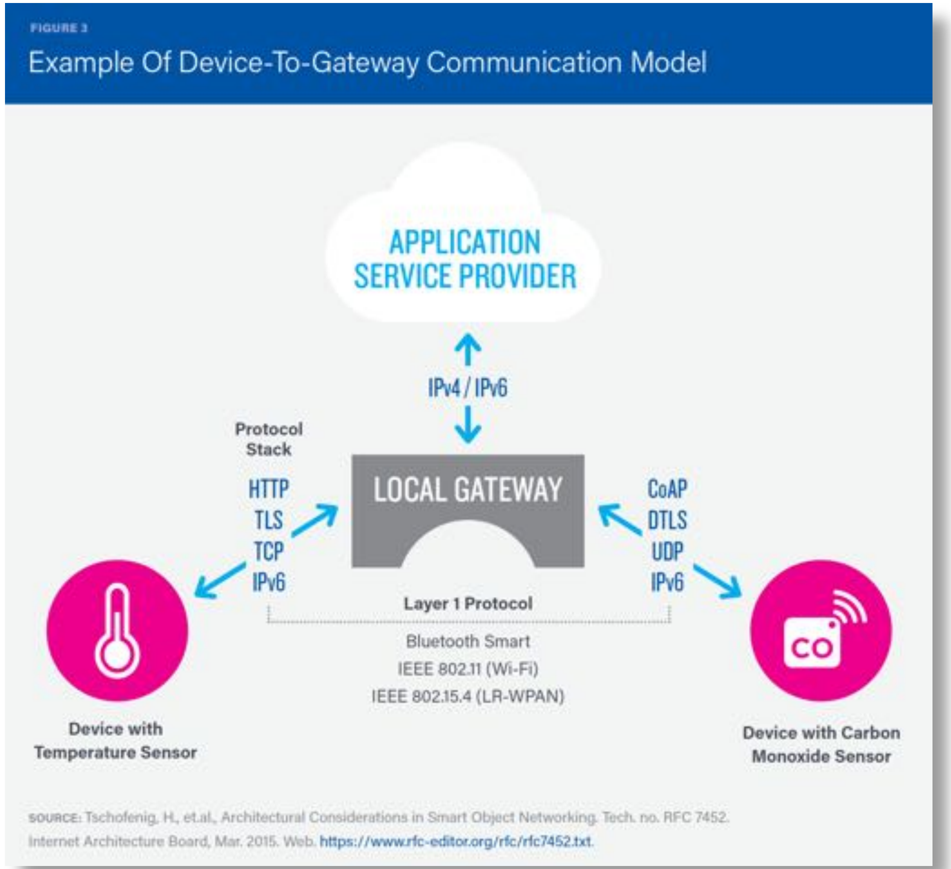


FIGURE 3

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.

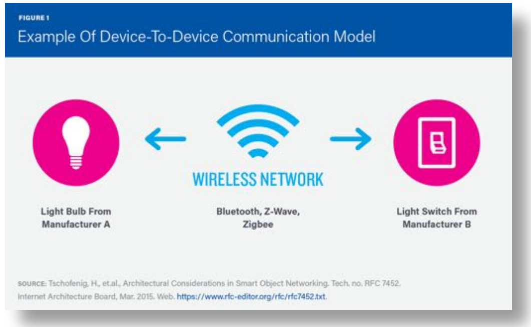


FIGURE 1

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.

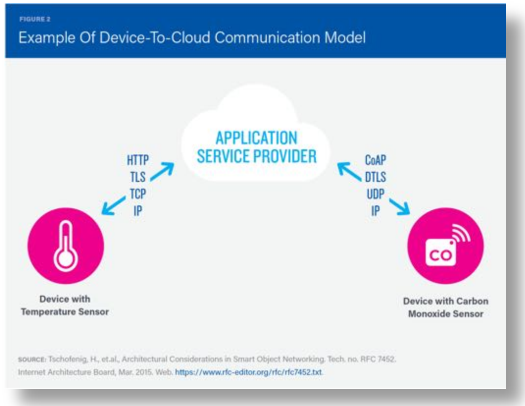


FIGURE 2

Example Of Device-To-Cloud Communication Model

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

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.

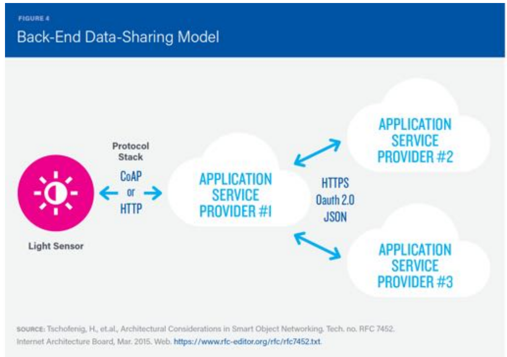


FIGURE 4

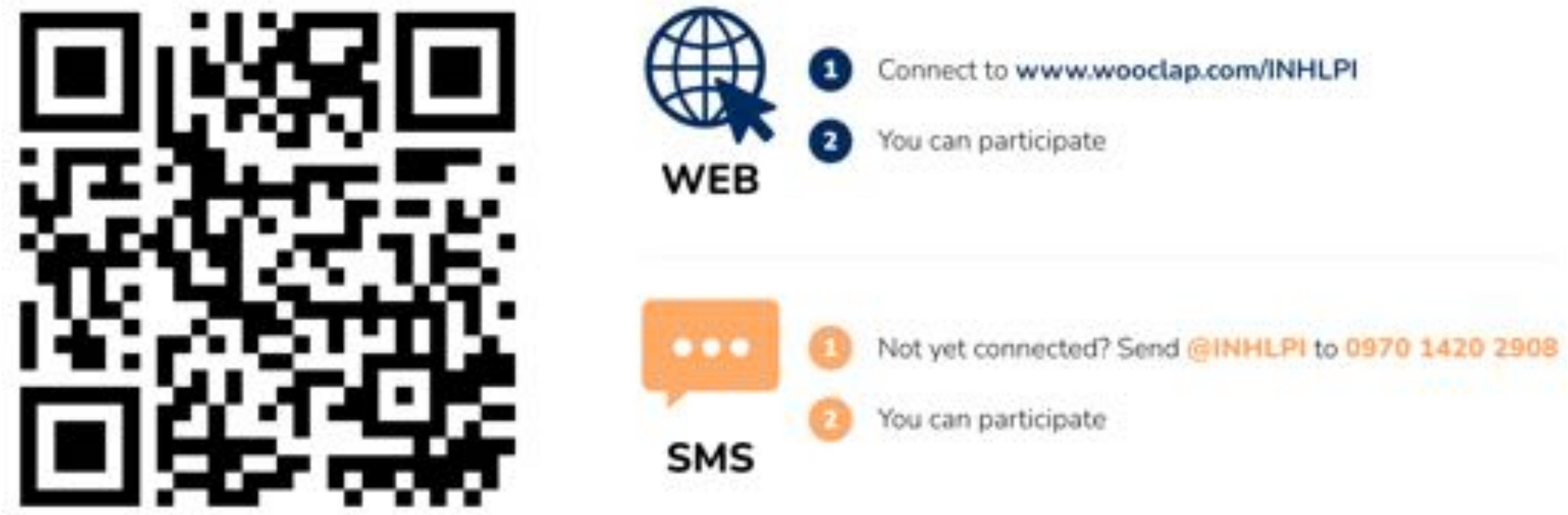
Back-End Data-Sharing Model

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

Wooclap quizzes



WEB

1 Connect to www.wooclap.com/INHLPI

2 You can participate

SMS

1 Not yet connected? Send @INHLPI to 0970 1420 2908

2 You can participate

Multiple-choice questions: 30 seconds
Open questions: 1.5 minutes

Today’s papers

[ARA] H. M. J. Almohri, L. T. Watson and D. Evans, “An Attack-Resilient Architecture for the Internet of Things,” in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3940-3954, 2020

[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 ARA 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 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”

“An Attack-Resilient Architecture for the Internet of Things”

IEEE Transactions on Information Forensics and Security,
vol. 15, pp. 3940-3954, 2020

UNIVERSITY
OF TWENTE.

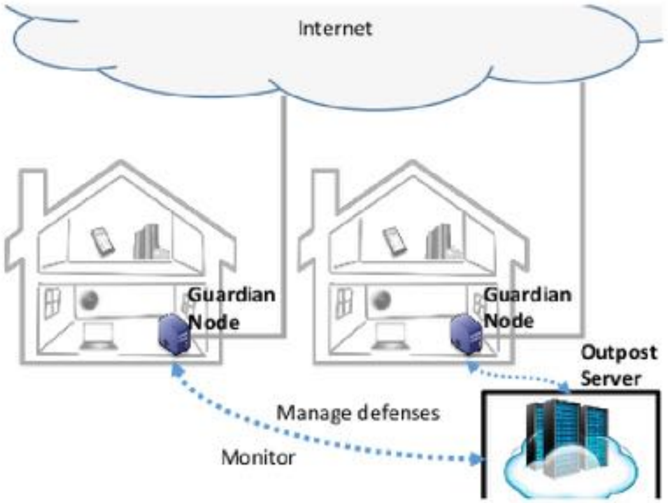
SIDN LABS

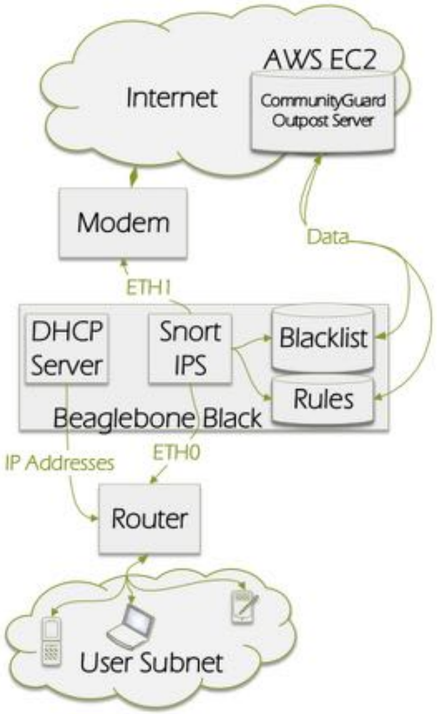
Differences in Edge Security Architectures

- Who should they protect?
- What type of attacks should they mitigate?
- What type of counter measures should be considered? blocking, notifying*, …
- …

* https://holmes.distributit.nl

Defending against DDoS



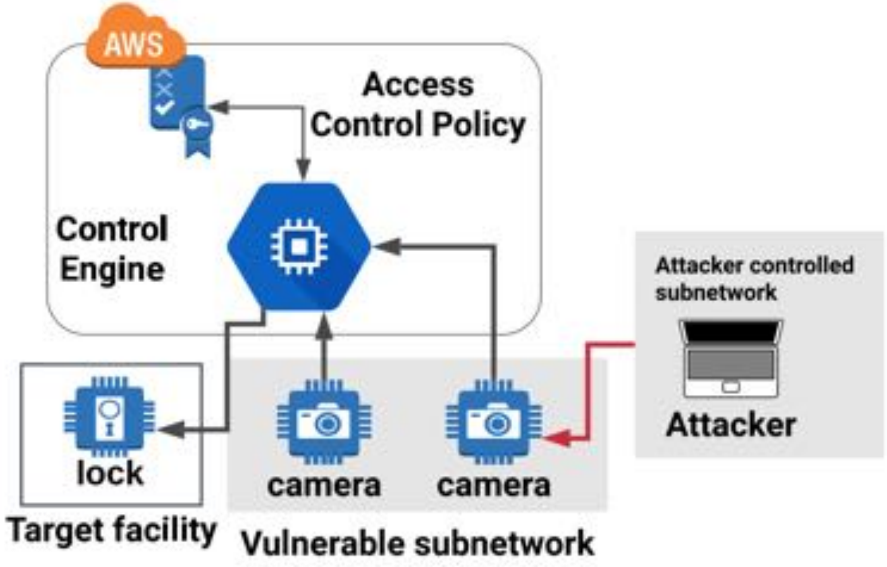


Additional reading: Stewart, Chase E., Anne Maria Vasu, and Eric Keller. "CommunityGuard: A crowdsourced home cyber-security system." *Proceedings of the ACM International workshop on security in software defined networks & network function virtualization.* 2017.

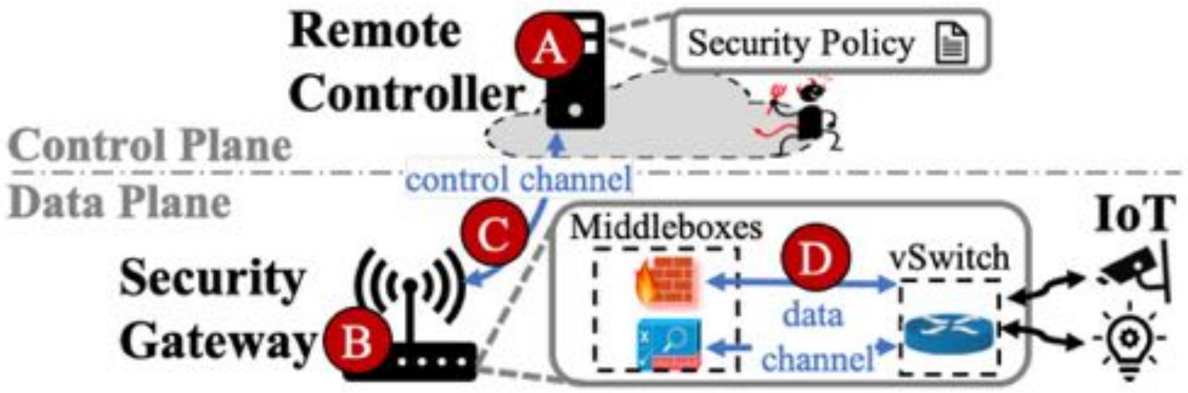
Attack Vectors

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

Attacks on Edge-Security Systems



[ARA]



[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.

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

Local and remote code execution, boot and safe browsing bypass

Read more on: https://blog.talosintelligence.com/2019/03/vuln-spotlight-cujo.html

Data Source

[ARA] uses application layer data. Some other papers use network layer data.

What are the upsides and downsides of each approach?

Device Policies

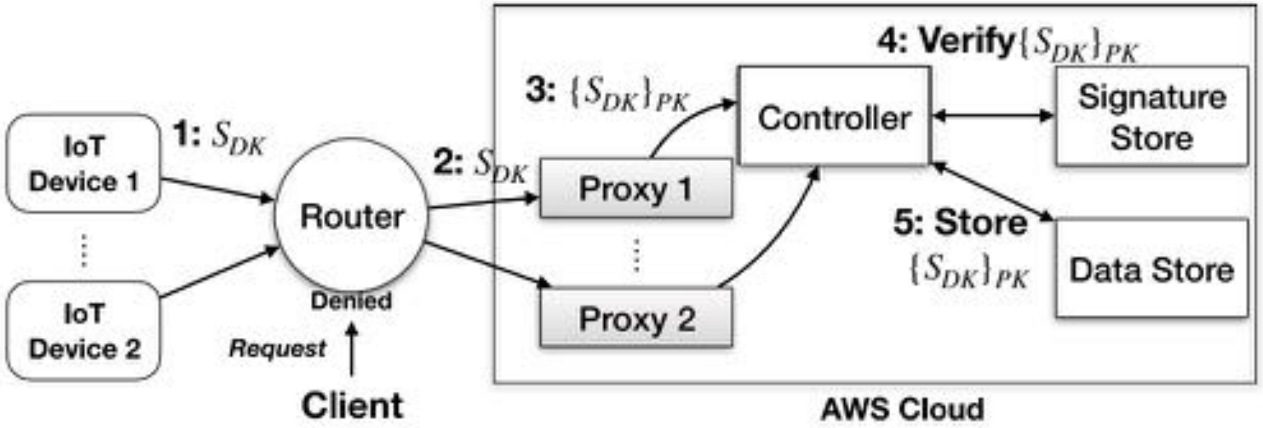
What could be the implications of automatically setting security policies on devices?

How would end users react to this?

Sequence Signing

- Devices are supposed to sign sequences using their private keys. Is that feasible?

- Are we capable of modifying devices (e.g., running sequence managers on devices)?



Machine Learning

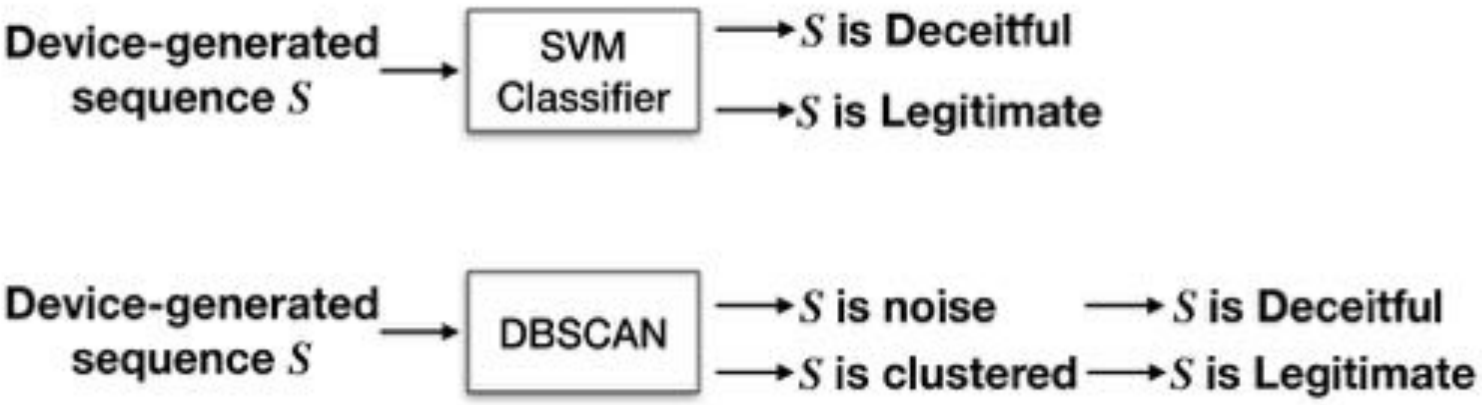
- [ARA] heavily relies on machine learning:
  - Binary classifier (SVM)
  - Density-based clustering (DBSCAN): >70% success, is that good?

- 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? What about ethics?

Machine Learning

- Why running two algorithms?
- What is the message of this figure?



Device-generated sequence S → SVM Classifier → S is Deceitful / → S is Legitimate

Device-generated sequence S → DBSCAN → S is noise → S is Deceitful / → S is clustered → S is Legitimate

Quiz

Which of the following is **<u>not</u>** considered by the architecture in the paper?

A. The controller only being accessible by the administrators
B. Detecting anomalous data exchanges between IoT devices
C. Impersonating IoT devices by forging MAC addresses
D. Detection of fabricated messages by compromised IoT devices

Lessons Learned

- One edge solution doesn't fit all purposes.

- Application data used in this paper is of a high value in making device policies, however this might not always be available.

- Countermeasures to deal with compromised devices should consider potential impacts on the end-user.

Coffee break

“DeadBolt: Securing IoT Deployments”

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

UNIVERSITY OF TWENTE.

SIDN LABS

Discussion: what are Deadbolt’s key components?

Discussion: what are Deadbolt's key components?

- Trusted gateway (AP)

- (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?

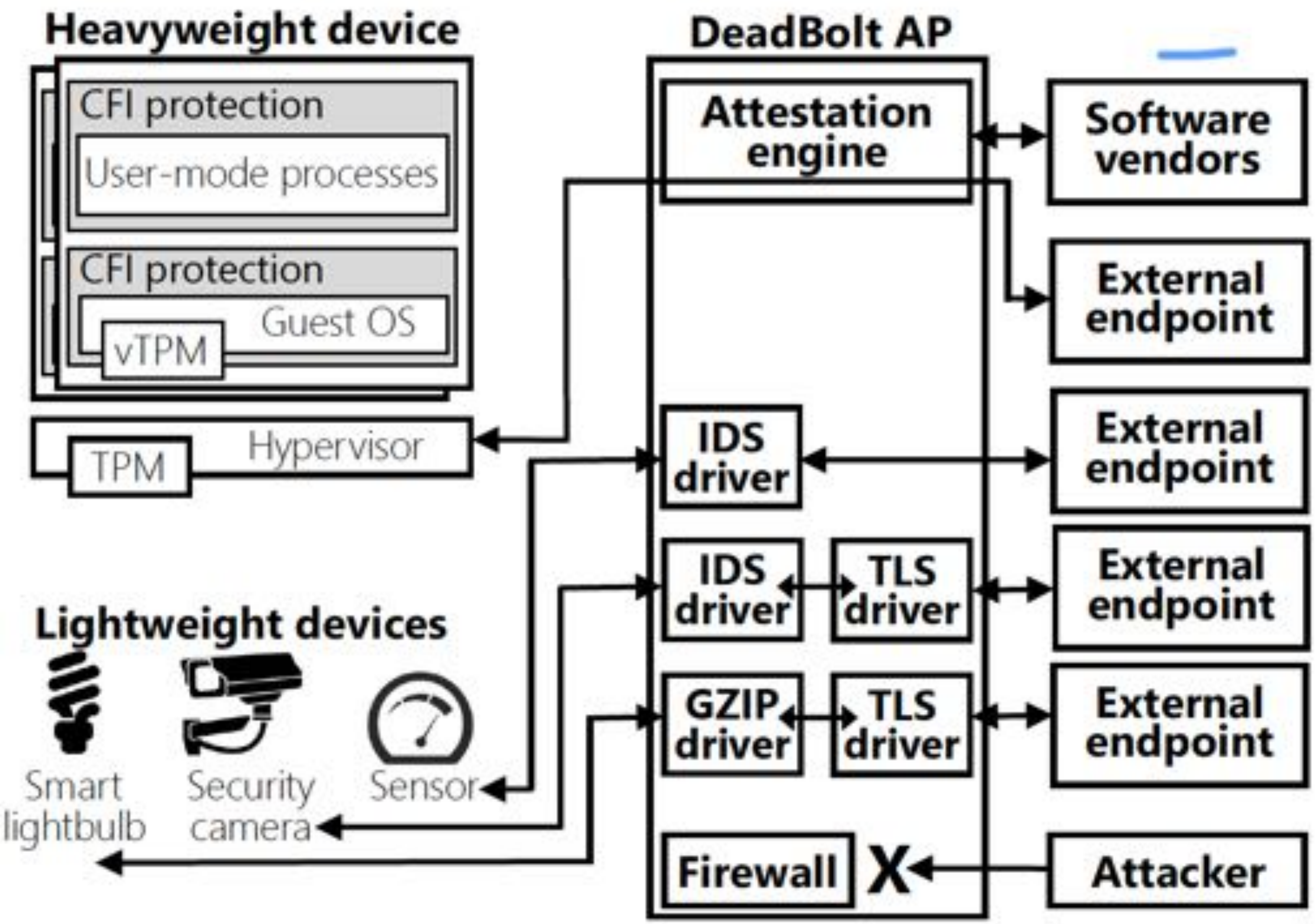
- Virtual network functions (e.g., encryption, scanning for malicious packets)

- Remote attestation (static) with device quarantining

- Protect against program flow attacks (dynamic attestation)

- Fast patching (VM swap for heavy weight devices)

So, what about that DeadBolt architecture?

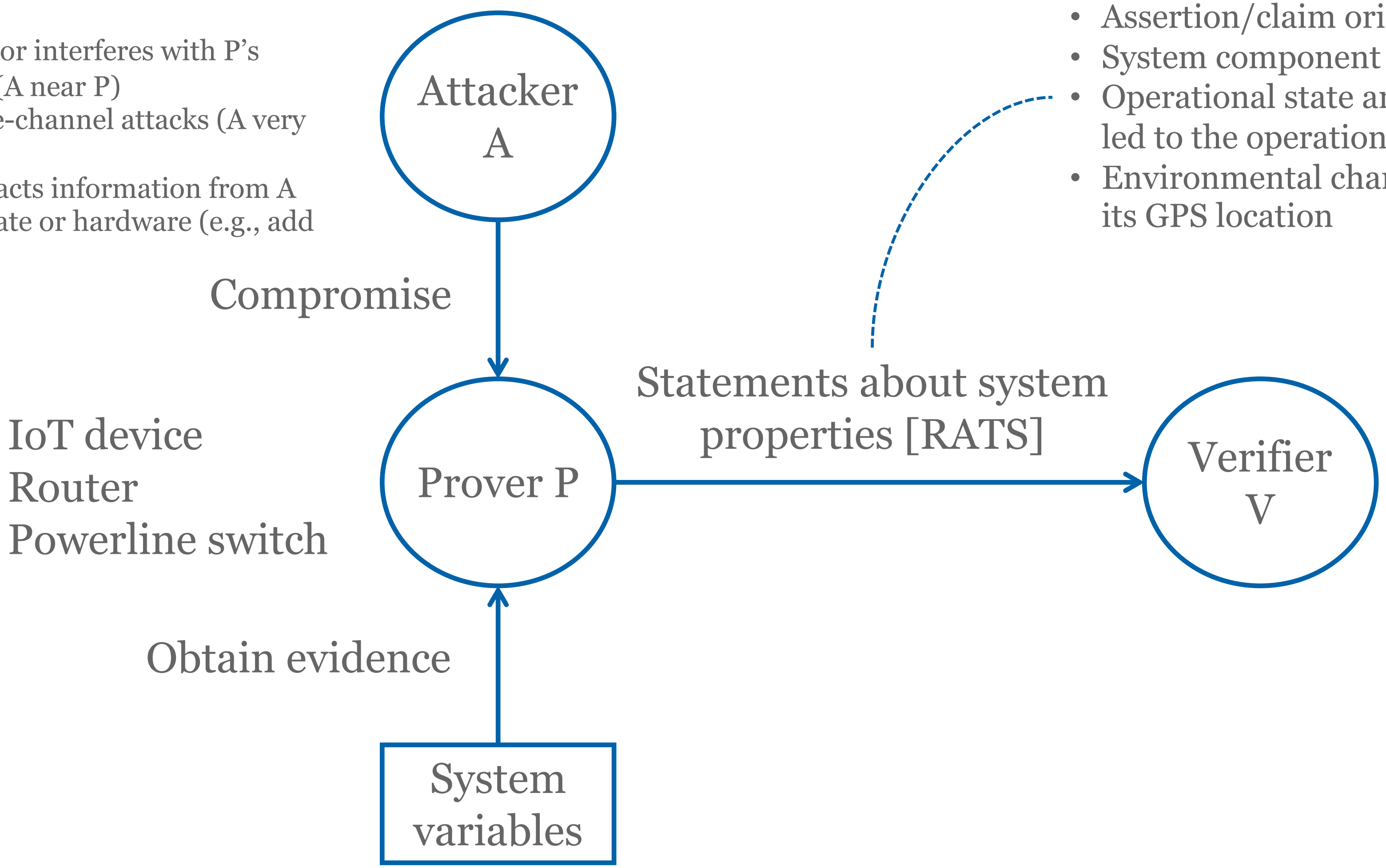


Remote attestation

EXTRA TIME

- A remotely infects P with malware (cf. Stuxnet)
- A eavesdrops on or interferes with P's communication (A near P)
- A carries out side-channel attacks (A very near P)
- A physically extracts information from A
- A modifies P's state or hardware (e.g., add memory)

- 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



Attacker A

Compromise

IoT device
Router
Powerline switch

Prover P

Statements about system properties [RATS]

Verifier V

Obtain evidence

System variables

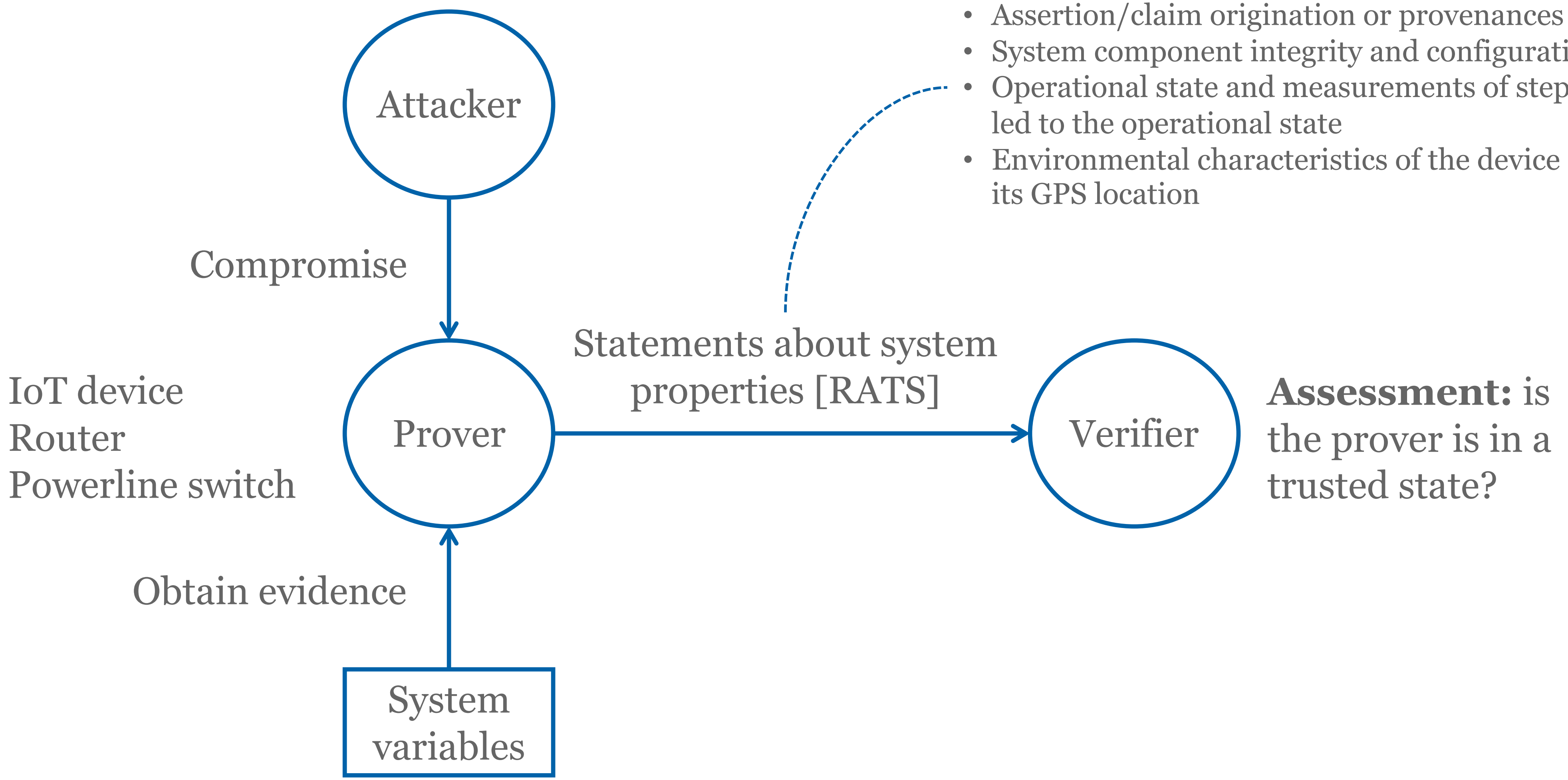
Assessment: is the prover is in a trusted state?

[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/

UNIVERSITY OF TWENTE. SIDN LABS

EXTRA TIME

Remote attestation



Attacker

Compromise

IoT device
Router
Powerline switch

Prover

Obtain evidence

System variables

Statements about system properties [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

Verifier

Assessment: is the prover is in a trusted state?

[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

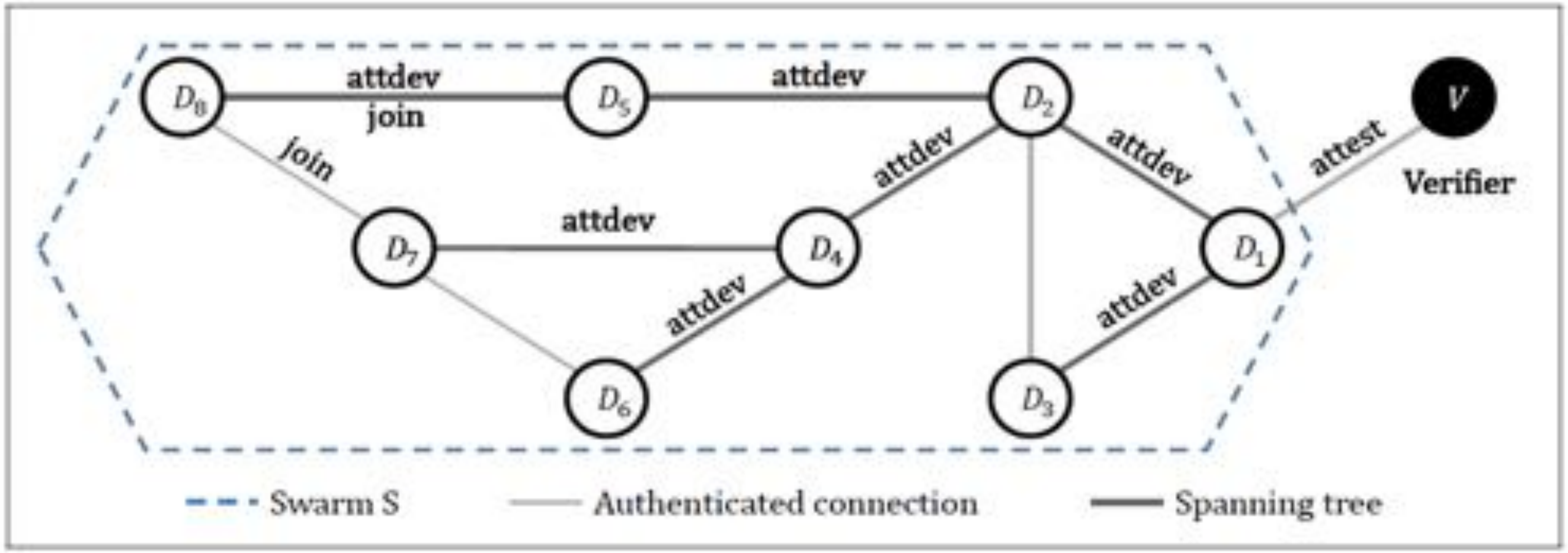


Figure 1: Swarm attestation (adapted from [3])

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

EXTRA TIME

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 :-)

Feedback

Today’s objective revisited

- After the lecture, you will be able to discuss the design, operation, and evaluation of ARA 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 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”

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?

UNIVERSITY OF TWENTE. SDN LABS

Volg ons

.nl SIDN.nl

@SIDN

in SIDN

See you next week!

Wed Jun 8, 10:45-12:30
Topic: IoT device security

UNIVERSITY OF TWENTE.

SIDN LABS