MaDoS: Matter DoS Attacks via Secure Channel Status Reports

Farzam Zohdi, Daniele Antonioli

ACM AsiaCCS 2026, Bengaluru, India

Matter: The *de facto* smart home standard

- One interoperable **application layer** protocol
- **Security by design**
- Adopted by **600+ vendors** (Apple, Google, Amazon, …)
- Used daily by **billions** of heterogeneous devices

matter

WORKS WITH alexa

works with Google Home

Works with Apple Home

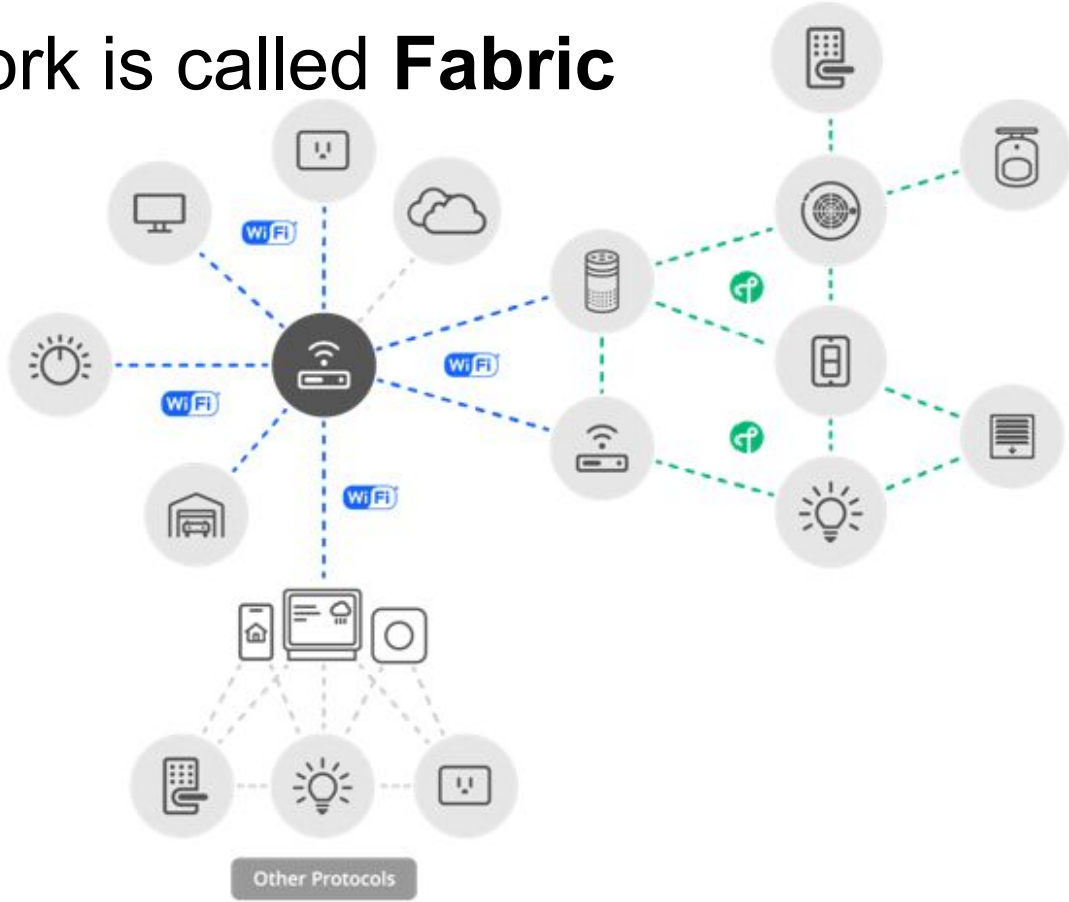
Works with Samsung SmartThings

Matter is open and versioned

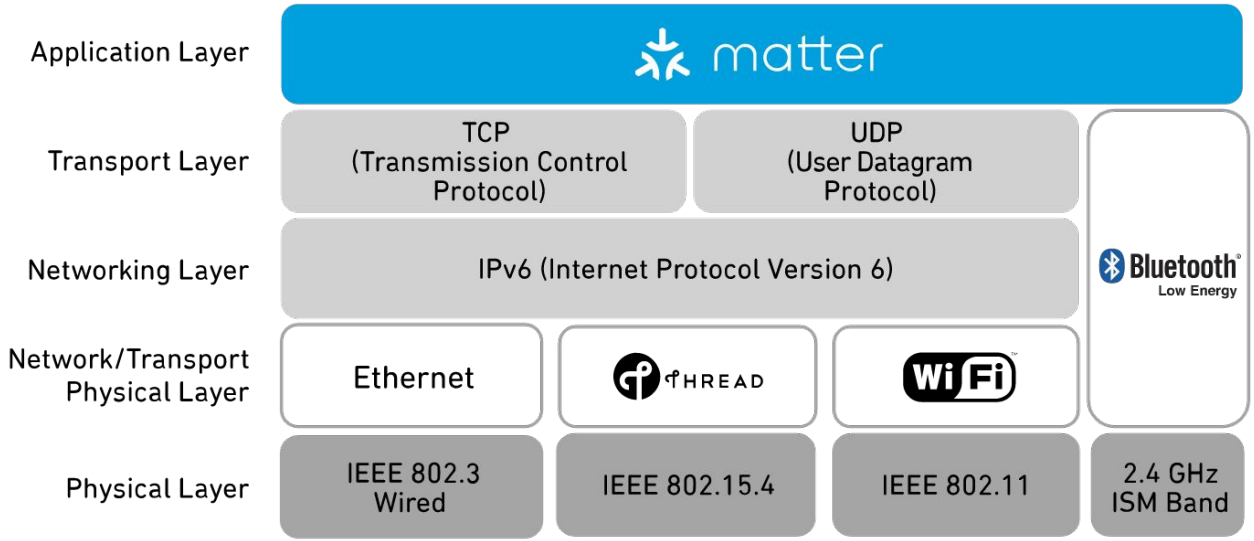
- Open specification
  - PDF by CSA
  - v1.0 (October 2022)
  - …
  - v1.5.1 (March 2025)
- Open SDK
  - project-chip
  - reference impl

A Matter network is called **Fabric**

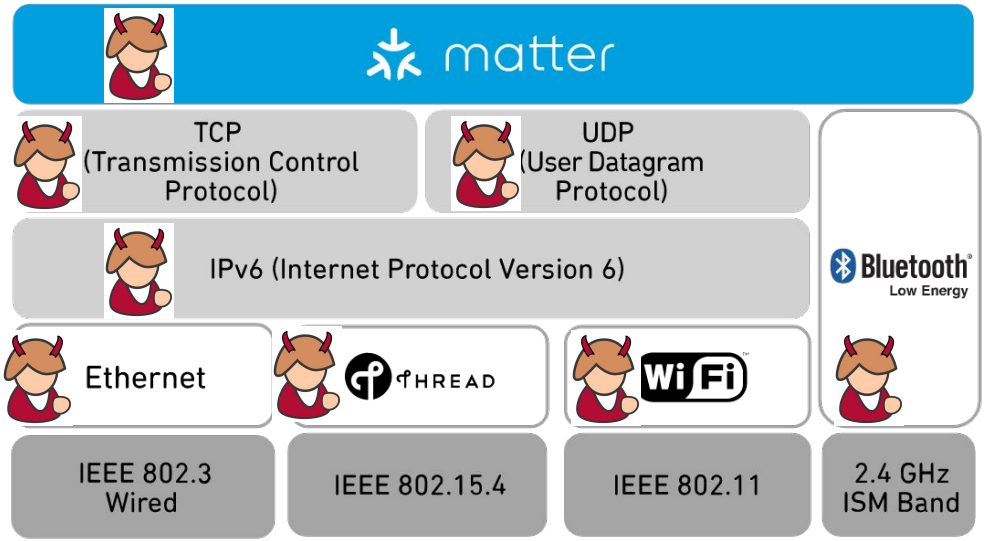
- Controller
- Commissioner
- End node
- …



Matter Stack: Interoperable and Vendor-Agnostic

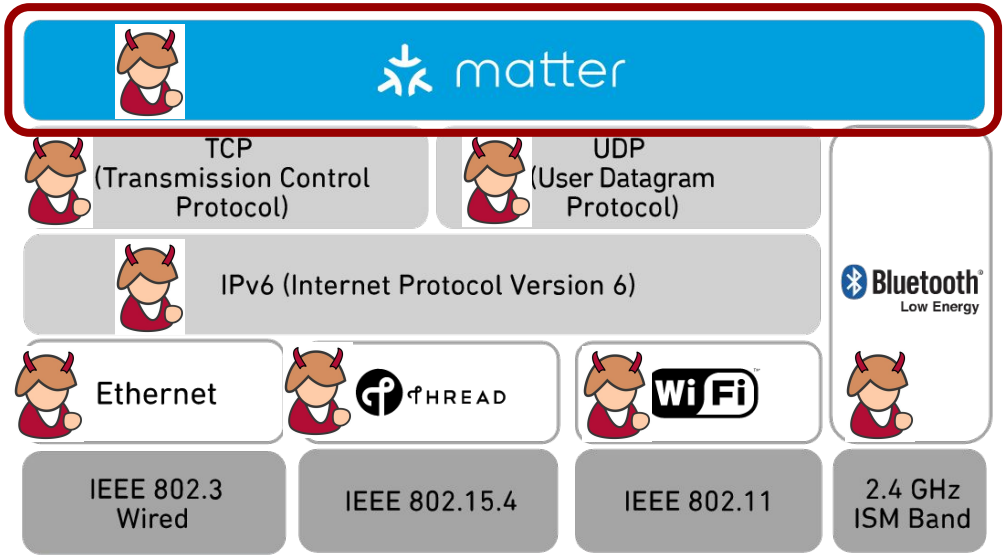


Matter is a Huge Attack surface!



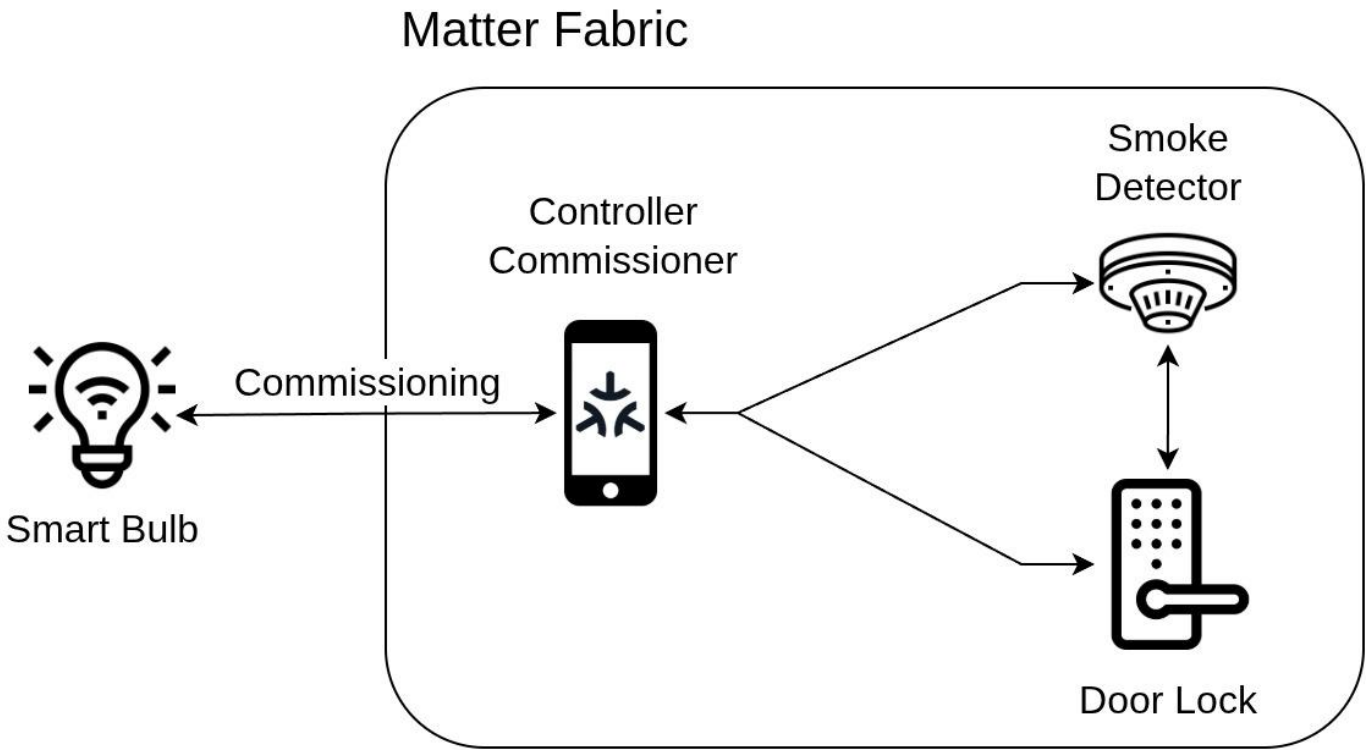
Security, **privacy**, and **safety** implications!

We focus on Matter protocol security

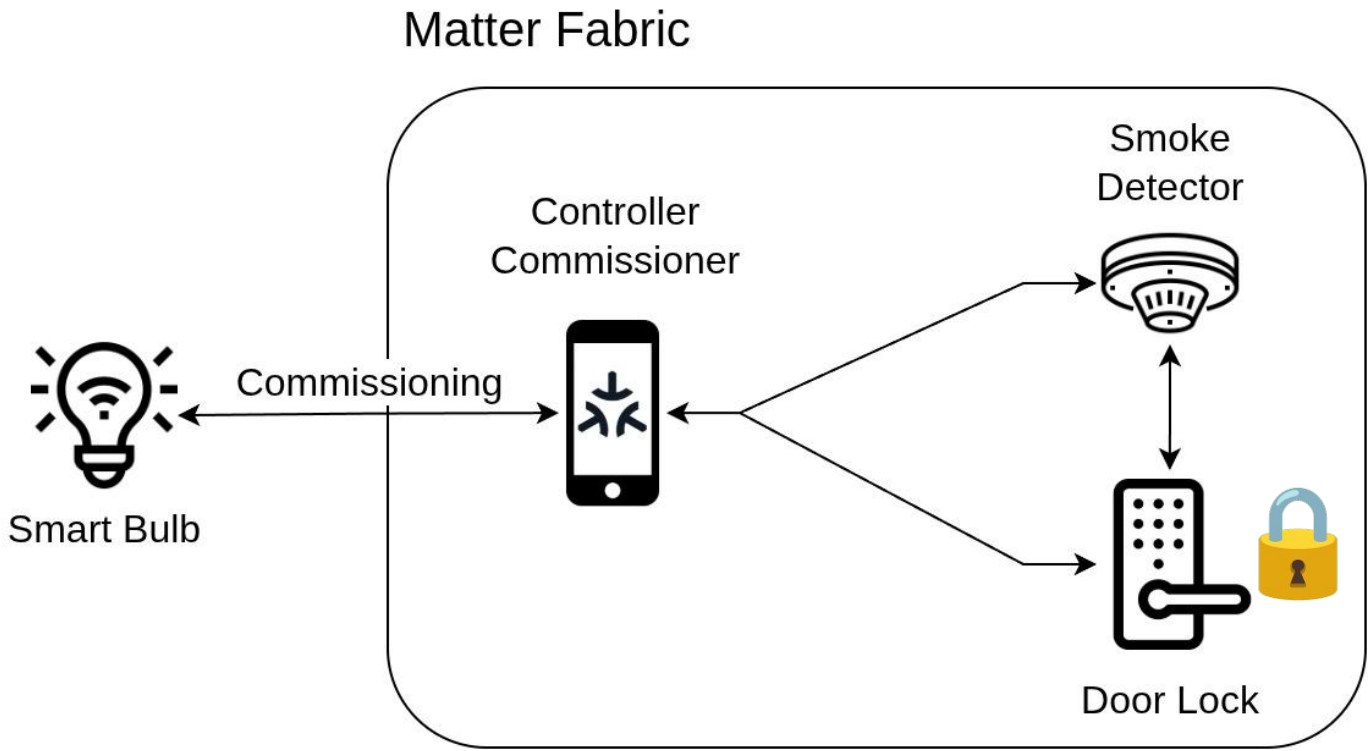


Attacks work **regardless of** the underlying layers.

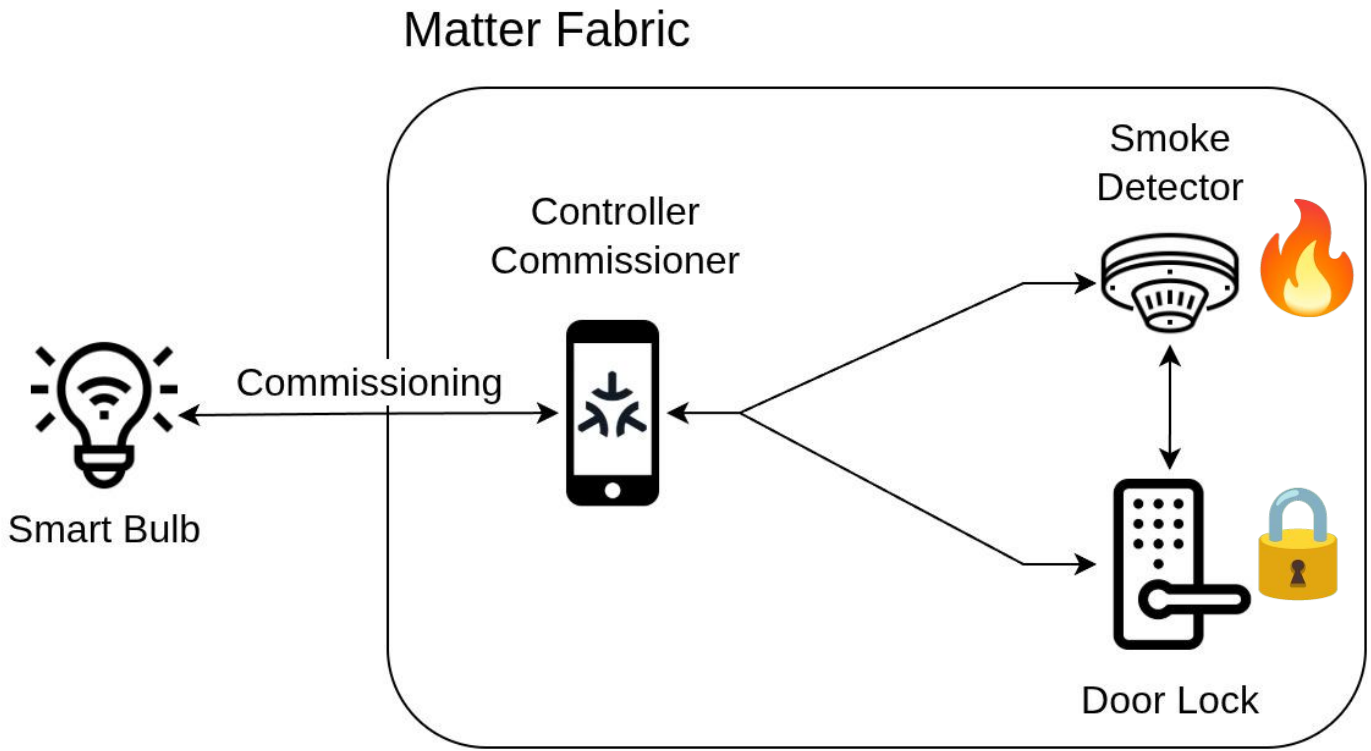
Matter Safety Critical Example



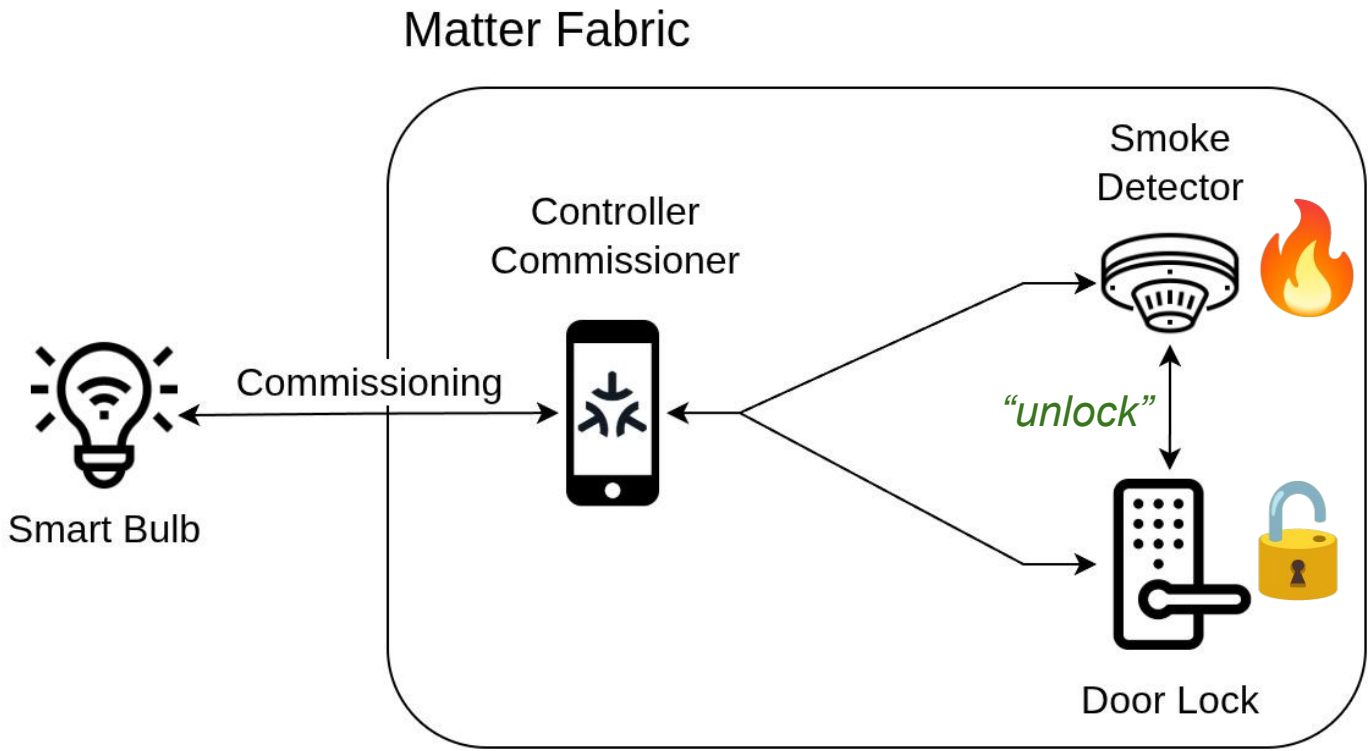
Matter Safety Critical Example



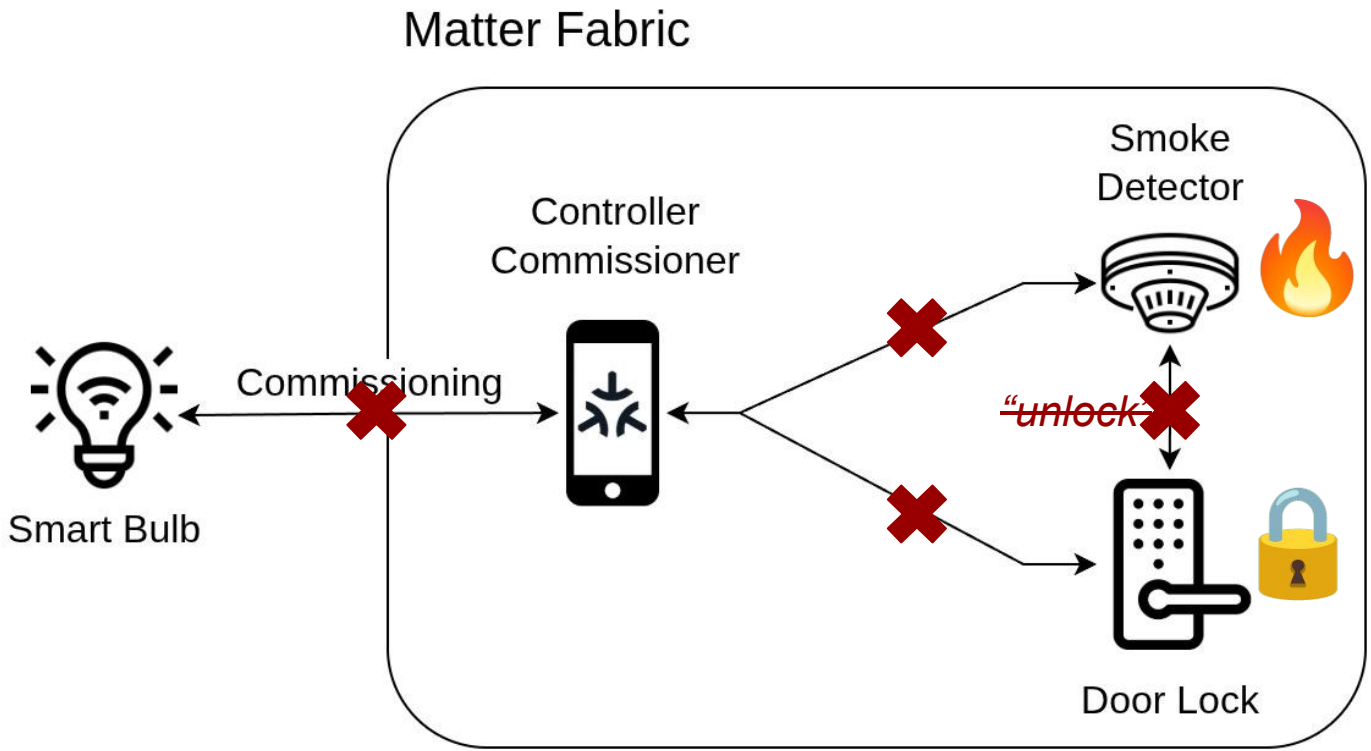
Matter Safety Critical Example



Matter Safety Critical Example



What about (D)DoS? **MaDoS attacks!**



Motivation: Matter (D)DoS Attacks

- No prior work on Matter (D)DoS despite
  - being safety-critical
  - listed as significant risk in the Matter specification
  - affecting the entire ecosystem
- Related work
  - Fuzzing: Ma, et al. (USENIX 24') **[1]**
  - Formal analysis: DKN, et al. (Cryptology ePrint Archive 25') **[2]**
  - Vendor specific attacks: Shafqat, et al. (SPW 24') **[3]**

[1] From One Thousand Pages of Specification to Unveiling Hidden Bugs: Large Language Model Assisted Fuzzing of Matter IoT Devices
[2] What's the Matter? An In-Depth Security Analysis of the Matter Protocol
[3] Seamlessly Insecure: Uncovering Outsider Access Risks in AiDot-Controlled Matter Devices

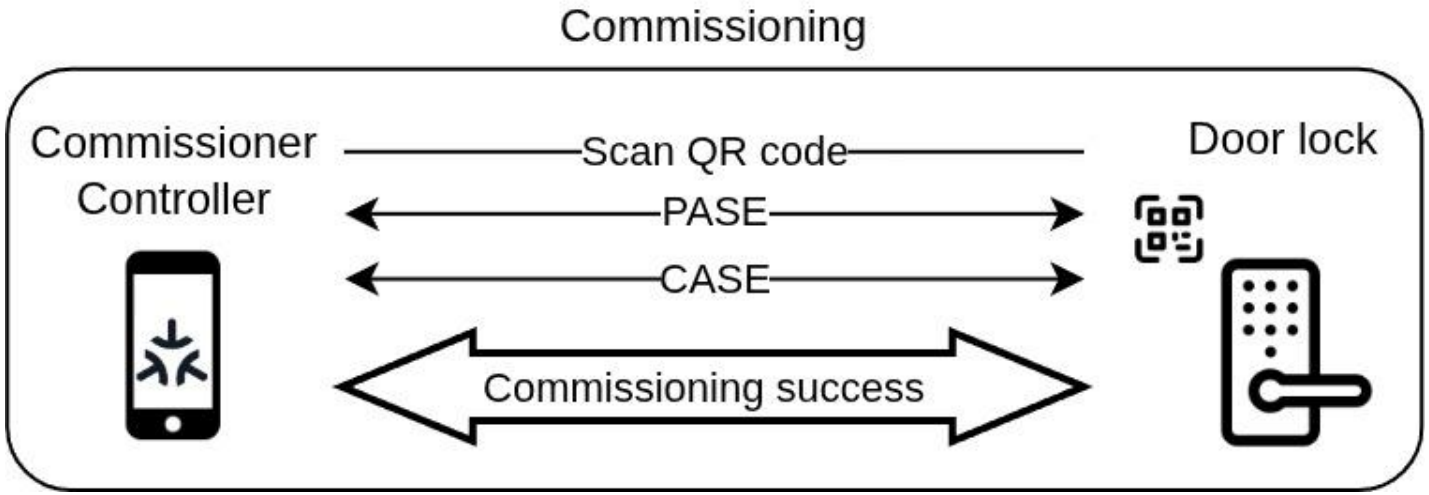
MaDoS Contributions

- First assessment of (D)DoS threats against Matter
- MaDoS: 3 new DoS attacks via Matter Status Reports
- 2 novel DoS vulnerabilities in the Matter specification
- `mados`: low-cost and open-source toolkit to test MaDoS attacks
- Evaluate 13 popular devices including all Matter versions
- 2 countermeasures to fix root causes
- Responsible disclosure to CSA

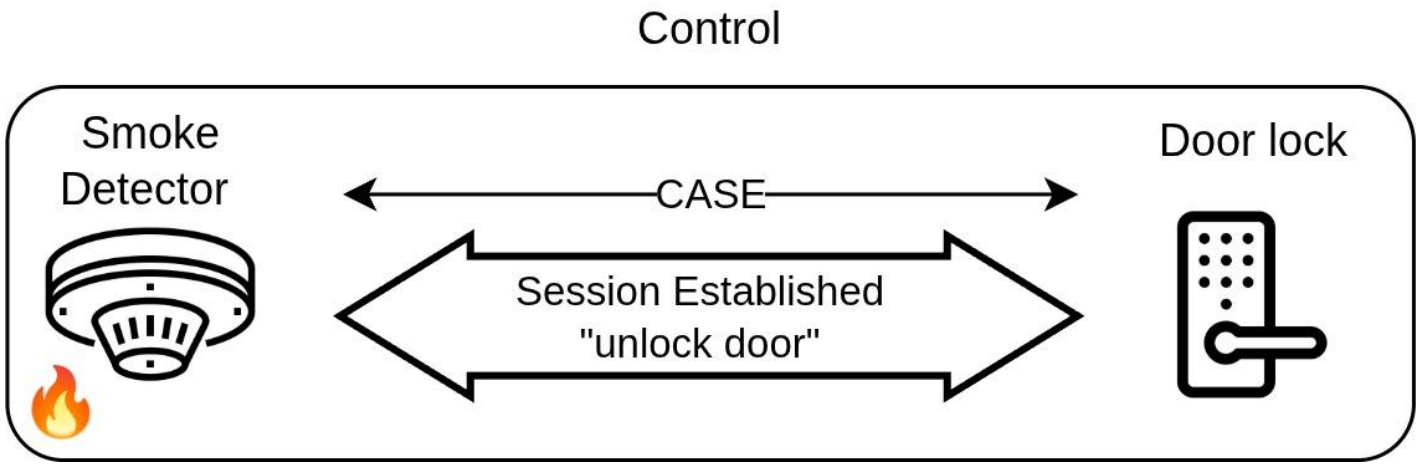
Matter Communication Security

- Three secure session est. protocols
  - PASE: *Passcode* Authenticated Session Est.
  - CASE: *Certificate* Authenticated Session Est.
  - CASE Resume
- Commissioning into the fabric
  - PASE, CASE
- Secure fabric communication
  - CASE, CASE Resume

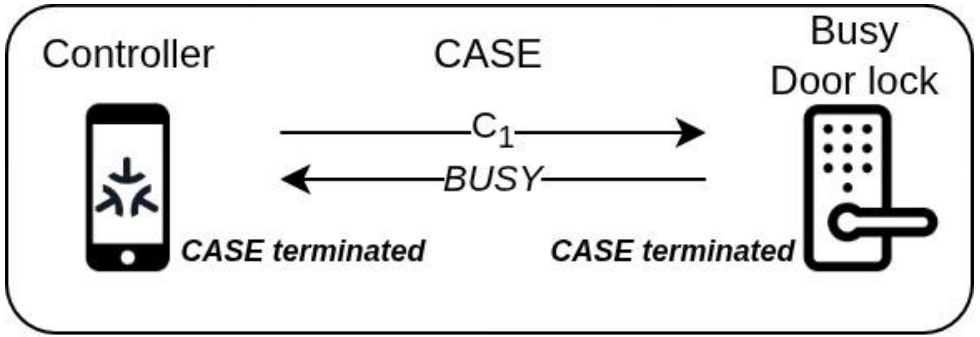
Matter Commissioning (PASE, CASE)



Matter Sessions (CASE, CASE Resume)



Matter PASE and CASE Status Reports



Status report	Type
No shared trust root	Error
Invalid parameter	Error
Device is busy	Error
Session established	Succes

MaDoS Protocol-level Threat model

- System model
  - Matter Fabric
  - Uncompromised devices and credentials
- Attacker model
  - Dolev-Yao (sniffing, sending packets, …)
  - Access to the network (BLE, Wi-Fi, …)
  - No knowledge of Matter fabric keys or certificates
- Attacker goals
  - Disrupt PASE, CASE, and CASE Resume
  - DoS on devices
  - DDoS on Matter fabric

MaDoS Vulnerabilities

V1: Unencrypted and unauthenticated status reports can terminate CASE, CASE Resume, and PASE, even if the other AL messages are AEAD-encrypted

V2: The status reports' semantics enable message confusion

MaDoS Vulnerabilities

V1: Unencrypted and unauthenticated status reports can terminate CASE, CASE Resume, and PASE, even if the other AL messages are AEAD-encrypted

V2: The status reports' semantics enable message confusion

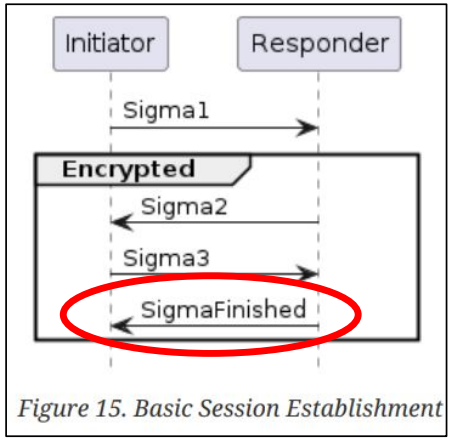


Figure 15. Basic Session Establishment

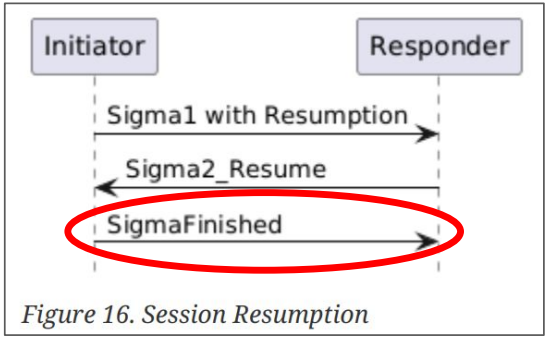
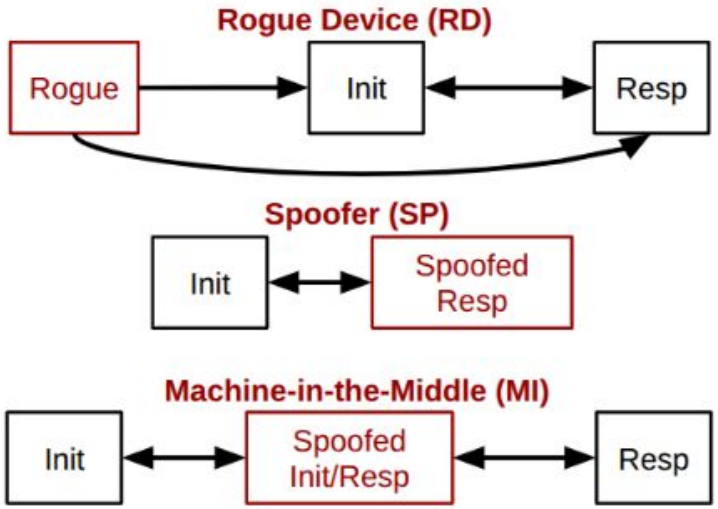


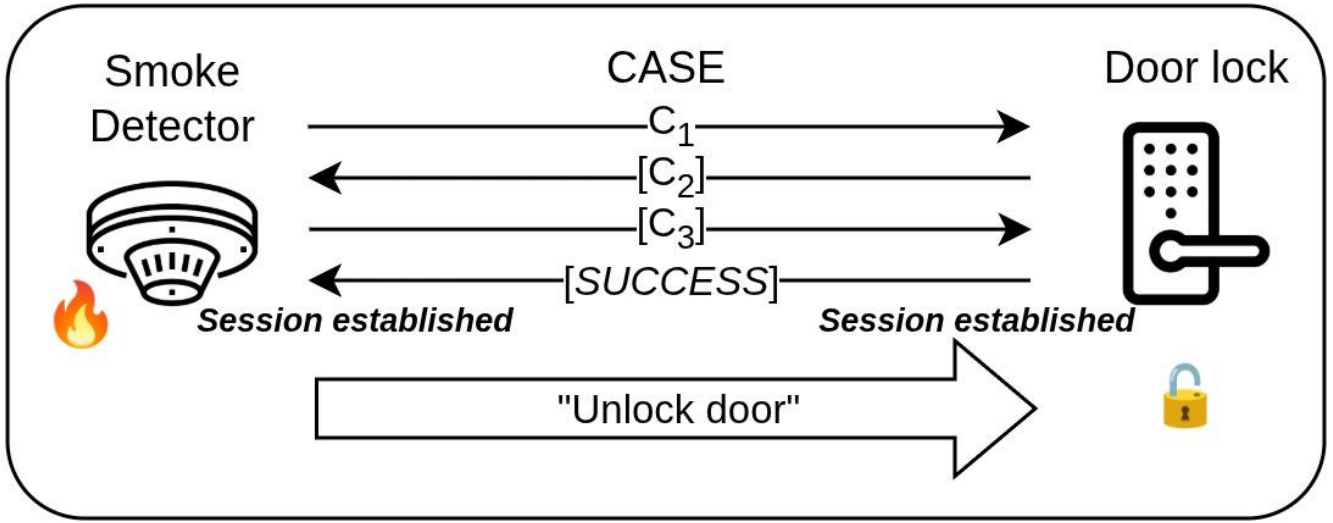
Figure 16. Session Resumption

MaDoS Attacks

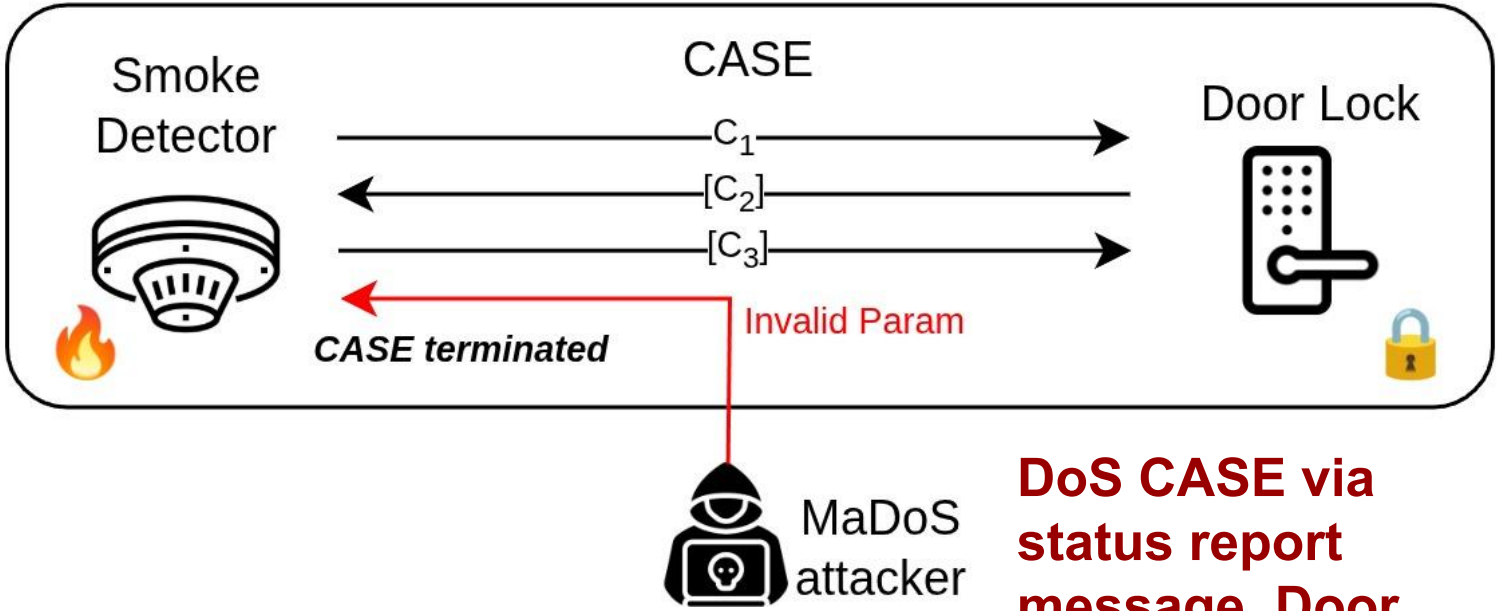
- Three attacks
  - Rogue Device
  - Spoofer
  - Man-in-the-middle
- Forty attack instances
  - Target PASE, CASE, and CASE Resume
  - Using different Status Reports
- Outcomes
  - DoS PASE, CASE, and CASE Resume



MaDoS Rogue Device Attack



MaDoS Rogue Device Attack



DoS CASE via status report message. Door still locked!

Evaluation Scenarios 1 to 13

	Target				MIp			MIc/MIcr		SPcI	
ES	Device	App	Role	Ver	BLE	Wi-Fi	Thd	Wi-Fi	Thd	Wi-Fi	Thd
1	iPhone 16 Pro Max	iOS Home	I	1.4	✓	✓	✓	✓	✓	✓	✓
2	iPhone 13	iOS Home	I	1.4	✓	✓	✓	✓	✓	✓	✓
3	Pixel 8, Nest Hub	Google Home	I	1.4	✓	✓	✓	✓	✓	✓	✓
4	Linux machine	CHIP-Tool	I	1.4	✓	✓	✓	✓	✓	✓	✓
5	Pixel 8, Echo	Alexa	I	1.3	✓	✓	✓	✓	✓	✓	✓
6	ESP32-C6	Light	R	1.4	✓	✓	✓	✓	✓	✓	✓
7	ESP32-C6	Light	R	1.2	✓	✓	✓	✓	✓	✓	✓
8	ESP32-C6	Door lock	R	1.4	✓	✓	✓	✓	✓	✓	✓
9	ESP32-H2	Light	R	1.4	✓	n/a	✓	n/a	✓	n/a	✓
10	ESP32-H2	Door lock	R	1.4	✓	n/a	✓	n/a	✓	n/a	✓
11	Nanoleaf bulb	3.2.0	R	1.0	✓	n/a	n/a	n/a	✓	n/a	✓
12	Aqara Sensor P2	1.0.0.0	R	1.0	✓	n/a	n/a	n/a	✓	n/a	✓
13	LEDVANCE Plug EU	1.1.0	R	1.1	✓	n/a	n/a	✓	n/a	✓	n/a

Evaluation Scenarios 14 to 25

	Setup				Attack				
ES	Initiator (I)	Ver	Responder (R)	Ver	RDpI	RDpR	RDcI	RDcR	RDcrR
14	CHIP-Tool	1.4.2	ESP32-C6 Light	1.4.2	100%	100%	100%	100%	100%*
15	CHIP-Tool	1.4.2	Linkind Bulb	1.4	n/a	n/a	100%	100%	100%*
16	CHIP-Tool	1.4.2	LEDVANCE Plug EU	1.1	n/a	n/a	100%	100%	100%*
17	iOS Home	1.4	ESP32-C6 Light	1.4.2	100%*	100%*	100%*	100%*	100%*
18	iOS Home	1.4	Linkind Bulb	1.4	n/a	n/a	100%*	100%*	100%*
19	iOS Home	1.4	LEDVANCE Plug EU	1.1	n/a	n/a	100%*	100%*	100%*
20	Amazon Alexa	1.4.1	ESP32-C6 Light	1.4.2	100%*	100%*	100%*	100%*	100%*
21	Amazon Alexa	1.4.1	Linkind Bulb	1.4	n/a	n/a	100%*	100%*	100%*
22	Amazon Alexa	1.4.1	LEDVANCE Plug EU	1.1	n/a	n/a	100%*	100%*	100%*
23	Google Home	1.5	ESP32-C6 Light	1.4.2	100%*	100%*	100%*	100%*	100%*
24	Google Home	1.5	Linkind Bulb	1.4	n/a	n/a	100%*	100%*	100%*
25	Google Home	1.5	LEDVANCE Plug EU	1.1	n/a	n/a	100%*	100%*	100%*

Evaluation summary table

Attack\Vendor	Apple	Google	Amazon	Nanoleaf	Aqara	Espressif
RD	🟢	🟢	🟢	🟢	🟢	🟢
SP	🟢	🟢	🟢	🟢	🟢	🟢
MI	🟢	🟢	🟢	🟢	🟢	🟢

🟢: Vulnerable regardless of

- Matter version (v1.0 - v1.5)
- Link-Layer (BLE, Wi-Fi, and Thread)

MaDoS Conclusion and Q&A

- First assessment of (D)DoS threats against Matter
- MaDoS: 3 new DoS attacks via Matter Status Reports
- 2 novel DoS vulnerabilities in the Matter specification
- `mados`: low-cost and open-source toolkit to test MaDoS attacks
- Evaluate 13 popular devices including all Matter versions
- 2 countermeasures to fix root causes
- Responsible disclosure to CSA