Beyond the Hype: Empirical Analysis of Matter Standard's Security and Privacy

An operational assessment of the Matter protocol

25 Matter devices · 14 non-Matter devices · 4 ecosystems

Andrew Losty, Tianrui Hu, Daniel J. Dubois, Narmeen Shafqat, Aanjhan Ranganathan, David Choffnes, Anna Maria Mandalari

UCL | Northeastern University | NUST Pakistan

Beyond the Hype: Empirical Analysis of Matter Standard's Security and Privacy

Venue: Internet Measurement Conference (IMC) 2026 , Karlsruhe, Germany
Submission: Paper

ACM ISBN 979-8-4007-2327-8/26/10
https://doi.org/10.1145/3777912.3809142
https://conferences.sigcomm.org/imc/2026/

IMC 26 conference
October 2026 ·
Karlsruhe, Germany

Analysis of Matter security and Privacy

Beyond the Hype: Empirical Analysis of Matter Standard's Security and Privacy

Andrew Losty
andrew.losty.23@ucl.ac.uk
University College London
United Kingdom

Tianrui Hu
hu.tian@northeastern.edu
Northeastern University
United States

Daniel J. Dubois
d.dubois@northeastern.edu
Northeastern University
United States

Narmeen Shafqat
narmeen_shafqat@mcs.edu.pk
NUST
Pakistan

Aanjhan Ranganathan
aanjhan@northeastern.edu
Northeastern University
United States

David Choffnes
choffnes@ccs.neu.edu
Northeastern University
United States

Anna Maria Mandalari
a.mandalari@ucl.ac.uk
University College London
United Kingdom

ABSTRACT

The rapid growth of the Internet of Things (IoT) has created fragmented smart home ecosystems, with platforms such as Apple Home, Google Home, and Samsung SmartThings historically relying on proprietary protocols and device-specific implementations that limited interoperability. The Matter standard defines a common, secure application-layer framework enabling cross-platform interoperability for Internet of Things (IoT) devices. It is developed under the Connectivity Standards Alliance (CSA), an industry consortium comprising more than 860 member organizations. This study empirically analyzes Matter and non-Matter ecosystems, focusing on security and privacy. We evaluate 25 Matter devices and 14 non-Matter devices with comparable functionality, examining network traffic during commissioning, device control, and data transmission. Our evaluation shows that Matter improves security and privacy through AES-128-CCM encryption, device attestation, and secure commissioning. Its local-first design further reduces cloud dependency and limits data exposure.
However, we identify several risks. Persistent multicast DNS broadcasts reveal detailed device metadata, and rotating key identifiers are inconsistently implemented, with some devices failing to renew keys for extended periods. We also observe ecosystem-specific differences in commissioning behavior. In addition, many devices maintain persistent connections to vendor or third-party cloud services. Firmware maintenance is inconsistent, as most devices in our study run early versions of Matter and do not receive updates over the observation period. Finally, traffic patterns in encrypted unicast communication can still reveal device types and user activities to an in-network adversary.

CCS CONCEPTS

• **Security and privacy → Security protocols**; • **Networks → Home networks**; **Application layer protocols**; **Network measurement**.

KEYWORDS

Internet of Things, Matter Standard, Security, Privacy, Network Traffic Analysis

ACM Reference Format:
Andrew Losty, Tianrui Hu, Daniel J. Dubois, Narmeen Shafqat, Aanjhan Ranganathan, David Choffnes, and Anna Maria Mandalari. 2026. Beyond the Hype: Empirical Analysis of Matter Standard's Security and Privacy. In *Proceedings of the 2026 ACM Internet Measurement Conference (IMC '26), October 12–16, 2026, Karlsruhe, Germany.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3777912.3809142

IMC '26, October 12–16, 2026, Karlsruhe, Germany

ACM ISBN 979-8-4007-2327-8/26/10
https://doi.org/10.1145/3777912.3809142

1 INTRODUCTION

The architecture of smart home Internet of Things (IoT) infrastructure may be undergoing a profound and fundamental transformation. Historically, smart home IoT platforms evolved independently as manufacturers sought to differentiate their products through proprietary security, privacy implementations and operational features. This resulted in a fragmented smart home ecosystem, in which competing platforms such as Apple Home, Google Home, Samsung SmartThings, and Amazon Alexa relied on vendor-specific implementations that severely limited interoperability.

To address these limitations, major IoT stakeholders collaboratively developed the Matter standard [4]. This effort culminated in the release of the Matter specification in October 2022. The specification enhances interoperability by defining a unified communication protocol that enables seamless interaction among devices from different manufacturers. Furthermore, it strengthens security by incorporating mandatory encryption, standardized authentication mechanisms, and uniform commissioning procedures.

In this paper, our main goal is to study how Matter behaves in real consumer environments by analyzing the privacy and security properties of 25 Matter devices across four major smart home ecosystems, and comparing them with 14 non-Matter devices from both the same manufacturers and other vendors offering equivalent functionality. We also study how ecosystem behavior, Matter/non-Matter hybrid-stack operation, and exposure to realistic adversarial conditions influence the privacy and security guarantees that Matter aims to provide. More specifically, we investigate the following four research questions.

RQ1: Do Matter-enabled devices offer improved security and privacy compared to similar non-Matter devices? The Matter standard provides a unified and secure communication framework for smart

1

Pre-Standards - Smart Home Architecture: A Fragmented Landscape

Smart home ecosystems defined by fierce vendor competition driving innovation but creating highly fragmented landscape.

Classifier	Feature
Interoperability	**Fragmented.** Isolated, incompatible ecosystems with no cross-platform device communication; strong vendor lock-in.
Security Architecture	**Inconsistent.** No mandatory security baseline; patchy compliance with ISO/IEC 27001, NIST CSF, ETSI EN 303 645, and the EU Cyber Resilience Act.
Market & Competition	**Highly competitive.** Fierce rivalry between Amazon, Google, Apple, Samsung and thousands of OEMs, driving rapid innovation and strong product differentiation.
Developer & Manufacturer Experience	**High overhead.** Fragmented SDKs and toolchains; separate device variants required per ecosystem; duplicated engineering effort.
Regulatory Alignment	**Weak.** Inconsistent adherence to established security and privacy frameworks; no industry-wide compliance baseline.

Matter Protocol: A Unified Smart Home Standard

Post 2022 the Connectivity Standards Alliance (CSA), launch Matter. Provides an open, royalty-free standard designed to unify smart home interoperability across major platforms.

Classifier	Feature
Interoperability	**Unified.** Single open standard enables native cross-platform operation across all major ecosystems; eliminates vendor lock-in.
Security Architecture	**Strengthened.** Mandatory certificate-based authentication and end-to-end encryption; improved alignment with ISO/IEC 27001 and ETSI EN 303 645.
Market & Competition	**Consolidation.** Reduced differentiation; smaller OEMs face high certification cost.
Developer & Manufacturer Experience	**Simplified, Single SDK,** and single device variant - reduced market fragmentation; Simplified certification and compliance processes Overhead for smaller manufacturers.
Regulatory Alignment	**Under Investigation.** Better structural compliance; however, the degree of alignment with major regulatory frameworks to be determined. CSA, JC-STAR

Non-Matter / Matter Device Set

Non-Matter Devices

Category	Device	App
Bulb	TP-Link Kasa bulb	TP-Link Kasa
Bulb	Sengled bulb	Sengled Home
Bulb	Gosund bulb	Gosund, Tuya
Bulb	Wiz bulb	WiZ Connected
Bulb	Smartlife bulb	Smartlife
Bulb	Yeelight bulb	Yeelight
LED Strip	Govee LED strip	Govee Home
LED Strip	Magic home strip	Magic Home
Plug	TP-Link Kasa plug	TP-Link Kasa
Plug	Meross plug	Meross
Plug	Wemo plug	Wemo
Plug	Amazon plug	Alexa
Misc	Meross door opener	Meross
Misc	August lock	August

Matter Devices

Category	Device	App
Bulb	TP-Link Tapo bulb*	TP-Link Tapo
Bulb	Sengled bulb*	None
Bulb	Linkind bulb	
Bulb	Orein bulb	AiDot
Bulb	Consciot bulb	
LED Strip	Govee LED strip	Govee Home
Plug	TP-Link Tapo plug	TP-Link Tapo
Plug	Meross plug	Meross
Plug	Eightree plug	Smartlife
Plug	Sengled plug	None
Plug	Sailsco plug	None
Plug	Xenon plug	None
Plug	Moes plug Tuya	Tuya
Plug	Linkind plug	AiDot
Plug	Cync plug	Cync
Plug	Leviton plug*	My Leviton
Plug	UseeLink plug	None

Matter Bridges and Controllers

Type	Device	App/Ecosystem
Bridge	Aqara bridge*	Aqara
Bridge	Aqara bridge M2*	Aqara
Bridge	Switchbot bridge*	Switchbot
Bridge	Philips bridge*	Philips Hue
Bridge	Smartlife bridge	Smartlife
Bridge	Third Reality Bridge	Third Reality
Bridge	Meross bridge	Meross
Controller	Apple HomePod mini	Home
Controller	Google Nest mini	Google Home
Controller	Amazon Echo	Alexa
Controller	Aeotec SmartThings	SmartThings

RQ1 Security/Privacy evaluation

Does Matter improve security and privacy?

Aspect	Non-Matter Devices	Matter Devices
Local Protocol	Varies — often proprietary	**UDP/TCP port 5540 (IANA Registered)**
Encryption	**Varies — often no encryption**	**AES-128-CCM (Mandatory) AES-256-CCM (Optional)**
Service Discovery	Various local protocols	**UDP port 5353 (mDNS)**
Attestation	Proprietary	**x.509.3 Certificate (DAC)**
Internet Dependency	**Often required for operation & control**	**Not required — local-first design**

✓ **Matter devices encrypt all operational comm. Matter's secure communications is confirmed for all devices.**

- All tested devices used encrypted Matter communication (UDP/TCP 5540)
- No plaintext operational commands observed
- Device authentication via certificate-based DAC (X.509v3)
- Operational payloads remained inaccessible during capture

RQ2 mDNS operation observation (i)

Do ecosystem-specific interpretations of the Matter standard introduce measurable vulnerabilities in device behavior?

- mDNS advertisement intervals for Matter devices are implementation dependent
- Specification does not tightly define VID/PID advertisements,
- Advertisement intervals are not specified,
- Post-commissioning advertising is a vendor choice.

TXT	Description	Mandatory
VP=5010+264	Vendor ID = Tapo and Product ID P110M	Optional
DT=266	Device Type 266 = Plug-in Unit / Smart Plug	Optional
DN=Smart Wi-Fi Plug	Device Name = DN=Smart Wi-Fi Plug	Optional
SII=5000	SII = Sleep Idle Interval (SII)	Optional
SAI=300	SAI = Sleep Active Interval (SAI)	Optional
T=1	Support for TCP (1) in addition to UDP for commissioning	Optional
D=3045	Discriminator = 3045	**Mandatory**
CM=0	Indicates if the device is currently in commissioning mode	**Mandatory**
RI=01006533A2200699921EAA2D89535640AD55	Rotating Device ID - Used for privacy to prevent long-term tracking of devices	Optional
PH=36	Pairing Hint –supported pairing modes 36 = QR code + manual code	Optional
PI=	Pairing Instruction e.g. optional text (“Hold button for 5 seconds”)	Optional

x **Persistent mDNS Advertisements Enable Device Fingerprinting**

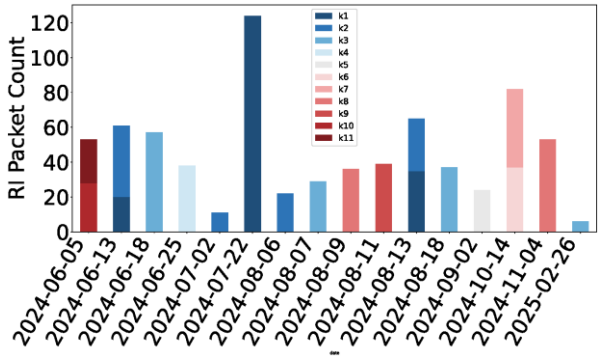
Example: The commissioned TP-Link Tapo P110M continues to broadcast identifying information through Matter mDNS advertisements.

Vendor ID (5010)
Product ID (262)
Device Type (266)
Device Name (*Smart Wi-Fi Plug*)

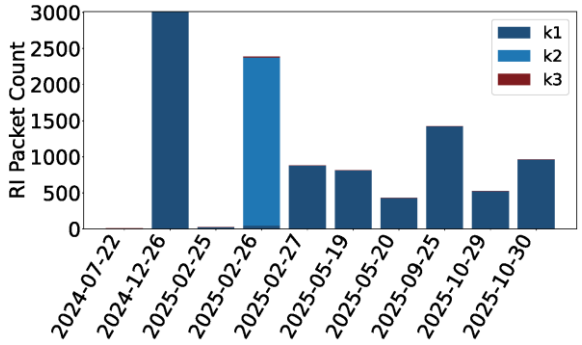
RQ2 mDNS operation observation (ii)

Do ecosystem-specific interpretations of the Matter standard introduce measurable vulnerabilities in device behavior?

Longitudinal study: June 2024 – November 2025



(a) Linkind Matter Plug: 11 rotations over 266 days



(b) Cync Matter Plug: Three key rotations, Single key for 263 days

X Matter mDNS advertisements reveal inconsistent use of privacy enabling rotating device id

- mDNS shows inconsistent use of Rotating Device Identifiers (RDI)
- RDI is used to reduce long-term tracking
- Behavior varies across vendors/devices
- Linkind Plug: 11 rotations in 266 days
- Cync Plug: 3 rotations, ~263-day stable ID

Matter Spec §5.4.2.4.5 — What RDIs should do:

- RDIs rotate at pre-defined moments based on a lifetime counter incremented with each advertising session
- Purpose: **prevent long-term tracking** and **device fingerprinting** across different networks and time periods

RQ2 Software version Status

Version	Date	Type of Update	New Device Types
1.0	Sept 2022	Major: Initial launch of the Matter standard.	Lights, Switches, Smart-Plugs, Door locks
1.1	May 2023	Minor: Enhancements, fixes, improved reliability	No new Device Types
1.2	Oct 2023	Major: Added new device types.	Fans, Air Purifiers, Robot Vacuums, Smoke/CO_2 Detectors
1.3	April 2024	Major: Additional features and categories. Added Scenes - devices can be grouped	Energy Management, Electric Vehicle Chargers, Water Management Devices, Household Appliances
1.4	Nov 2024	Major: Expanded features including energy management.	Routers, Access Points, Solar Power, Batteries, Heat Pumps
1.4.1	May 2025	Minor: Improvements: easier set-up, adds terms-and-conditions, multi-QR-code, NFC tag support.	No new Device Types
1.4.2	Aug 2025	Maintenance: Improved Security, Wi-Fi-only commissioning, + Improved Scenes Management	No new Device Types

1.5	Nov 2025	Largest functional update since launch	Cameras (incl. Video Doorbells, Floodlight Cameras, Intercoms), Closures (garage doors, awnings, gates)

Background update

Amazon: Echo devices (claimed 100M+ devices,

Apple: Apple TV, HomePod from iOS 16.1

Google: Nest Hub 2nd gen, Nest Hub Max, 1.56.324896

Samsung SmartThings Hub (2nd & 3rd gen) Aeotec Smart Home Hub

Philips Hue Hue Bridge v2, Hue Bridge Pro

Ikea DIRIGERA Hub

RQ2 Software update Status

ID	Device	Vendor ID	Product ID	Firmware 1	Firmware 2	Certificate ID	Date	Version
1	Consciot bulb	4456	1029	2.00.00		CSA23188MAT40701-24	11/09/2022	1.0
1	Consciot bulb	4456	1029		3.00.00	CSA252C0MAT45586-24	05/21/2025	1.4
2	Cync plug	4921	172	1.01.120	1.01.120	CSA23D82MAT41891-24	11/14/2023	1.1
3	Govee strip	4999	25056	1.01.03	1.01.03	CSA22178MAT40178-24	12/14/2022	1.0
4	Leviton plug	4251	4098	2.1.0	2.1.0	CSA23581MAT41094-24	05/16/2023	1.0
5	Linkind plug	4456	1024	1.00.00	1.00.00	CSA23494MAT41007-24	04/24/2023	1.0
6	Meross plug	4933	40961	9.3.26	9.3.26	CSA22335MAT40335-24	12/23/2022	1.0
7	Moes plug	4991	635	1.2.6	1.2.6	CSA23408MAT40921-24	04/12/2023	1.0
8	Orein bulb	4456	1002	2.00.00		CSA22089MAT40089-24	09/11/2022	1.0
8	Orein bulb	4456	1002		3.00.00	CSA252B0MAT45570-24	21/05/2025	1.4
9	Sengled bulb	4448	36869	v1.0.0.5	v1.0.0.5			1.0
10	Tapo bulb	5010	769	1.3.0	1.3.0	CSA25199MAT45291-24	22/03/2025	1.3
11	Tuya plug	4891	8204	V1.0	V1.0	CSA23562MAT41075-24	08/05/2023	1.0
12	Meross plug	4933	40962	9.3.26	9.3.26	CSA22337MAT40337-24	12/23/2022	1.0
13	Tapo plug	5010	264	1.0.0		CSA23545MAT41058-24	05/02/2023	1.0
13	Tapo plug	5010	264		1.3.0	CSA2510FMAT45153-24	03/05/2025	1.3
14	Eightree plug	5242	851	1.2.6	1.2.6	CSA240E5MAT42904-24	09/02/2024	1.2
15	Sengled plug	4448	36885	V1.0.0.5	V1.0.0.5	CSA23830MAT41343-24	07/07/2023	1.0
16	Sailsco plug	5393	1871	1.2.6	1.2.6	CSA240E5MAT42904-24	09/02/2024	1.2
17	Xenon plug	5249	4216	1.2	1.2	?	04/12/2023	1.2
18	Meross bridge	4933	8193	9.3.5	9.3.5	CSA24334MAT43495-24	06/14/2024	1.2

50%

on Matter 1.0
(original 2022 firmware)

11%

on version 1.4 (latest)

16%

devices received updates
during study period

50%

3 of 6 bridges updated
(higher security exposure)

RQ3 Local first communications

Do Matter devices follow local-first design in practice?

Device	Controllable offline?	Post-reboot	After 1 hr	After 18 hrs
Sengled bulb, Tapo plug, Meross plug	✓ Yes	✓ Yes(1/2)	✓ Yes(1/2)	✓ Yes
Linkind plug	✓ Yes (2s delay)	✓ (2s delay)	✓ (2s delay)	✓ (2s delay)
Cync plug	✓ Yes	✓ (30s delay)	✓ Yes	✓ Yes
Aqara Bridge	Some features	✓ Yes	Some features	Some features
All other devices & bridges	✓ Yes	✓ Yes	✓ Yes	✓ Yes

✓ **Validation of Matter's Local-First Design**
Most evaluated devices remained fully functional during offline operation.

Yes(1/2) indicates control succeeded in only 1 out of 2 post-reboot/timeout conditions

⚠ **Boot delays reveal cloud-first firmware**
Some vendors treat local operation as fallback,
not primary mode.

Firmware updates still require internet unless OTA via controller.

RQ4 Detection of device type / operation through traffic analysis

Is encrypted Matter traffic susceptible to inference analysis

Although payloads are encrypted, packet sizes and timing patterns are reproducible and reveal detailed device behavior to an in-network or proximity adversary.

Example: Off events exhibit a consistent sequence of packet sizes, with X and Y vendor-specific packet-size variations.

Device	MAC OUI	Off (121,129,X,96,104,96,Y)	On (121,129,X,96,104,96,Y)	Dim / Hue
TP-Link bulb	Tp-Link	131, 235	235, 183	183 / 133
Sengled bulb	Espressif	158, 158	210, 158	158 / 133–188
Linkind / Orein / Consciot bulbs	Espressif	210, –	210, 158	158 / 133–188
Govee LED strip	Shenzhen	183, 183	235, 183	183 / 210–265
TP-Link Tapo plug	Tp-Link	156, –	156, –	N/A
Meross plug	Meross	156, –	156, –	N/A
Eightree / Sailsco plug	TuyaSmart	190, –	216, –	N/A
Sengled / Xenon / Tuya plug	Espressif	183, –	209, –	N/A
Leviton plug (firmware-upgraded)	Leviton	133, 132	159, 131/157	158 / N/A

~94% **Bulb vs Plug classification**

52.6% **Vendor identification**

High Reliability **State inference (On/Off/Dim/Hue)**

Recommendations & Conclusion

For Manufacturers

- Limit mDNS to required discovery only
- Implement frequent RDI rotation
- Use RFC 7217 randomised IPv6 interface IDs
- Deliver timely, secure firmware updates
- Allow users to disable sensitive broadcasts
- Support local-network OTA updates
- Ensure companion apps use Matter pairing

For Standardisation & Regulatory Bodies

- Mandate use of latest Matter specification versions
- Publish formal privacy & security best-practice docs
- Expand certification to cover privacy-sensitive features
- Require support for local-only communication
- Require local-network software update capability

Conclusion: Matter improves several long-standing IoT security problems, but its practical security and privacy properties depend heavily on vendor implementations. Stronger adherence to the specification — and clearer regulatory mandates — will be necessary if Matter is to deliver on its long-term goals.

200+ Device IoT Research Testbed for Security, Privacy and Operational Analysis

1

SafeNetIoT
SECURING THE IOT

2

3

Follow us:
https://safenetiot.github.io/
https://www.youtube.com/watch?v=0fg0acuRbUA

Contacts:
andrew.losty.23@ucl.ac.uk