Developments in Device Identities and IoT network security

May 14, 2025

Device Identity Forum, IETF SETTLE, Manysecured SUIB

Michael Richardson <mcr+ietf@sandelman.ca>

https://www.sandelman.ca/SSW/talk/2025-ripe90-iot/

Agenda for 2025-05-14 -- RIPE 90

- Device Identity Forum
- IETF SETTLE
- Secure Useable Intranet Browser
- IETF IoTOPS updates
- Questions (5min)

IoTSecurityFoundation.org Device Identity Forum

Announced at CyberUK, 2025-05-07:

https://iotsecurityfoundation.org/iot-security-foundation-launches-device-identities-working-group-at-cyberuk-2025-to-strengthen-iot-security/

Also https://www.sandelman.ca/deviceidentityforum/

Inaugural Meeting 2025-05-15 (tomorrow) at 14:00 WEST (Lisbon) time. (Sorry, opposite Routing/Cooperation)

Chaired by Michael Richardson (SSW) and Richard Seward (Device Authority)

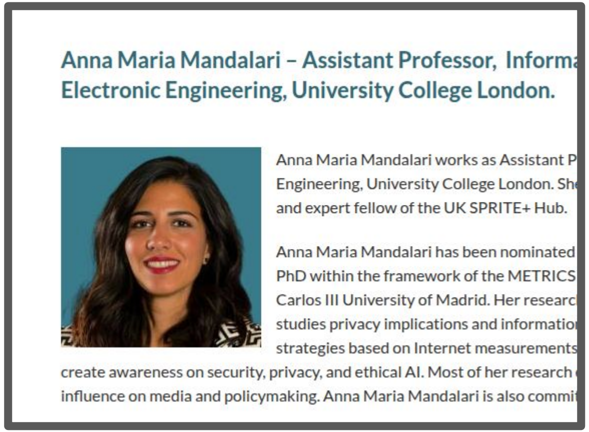
Expected to operate for a few years, with monthly virtual meetings.

60% technical marketing: bring a common, visually understandable message to many other aspects of the IoT industry: *Device Identities are Necessary and Easy*. Also think: visio stencils/SVG.

40% profile/technical, like: what is a good validity lifetime for a private PKI’s subordinate CAs? How many levels of subordinate CA? How to manage trust anchors, software signing keys…

Who is the IoT Security Foundation?

- Formed in 2015.
- Annual Fall Conference
- "help *make it safe to connect*" so the many benefits of IoT can be realized.
    - Through a dedicated program of guidance, reports, events, training, standards, advocacy and so much more, we represent a collaborative international response to the wicked challenge of IoT insecurity.
- Security Best Practice – Why & How?
- The IoT Security Assurance Framework
- IoT Security Self Certification
- No Universal Default Passwords
- Keeping Software Security Updated
- Vulnerability Reporting and Disclosure Policy



Anna Maria Mandalari – Assistant Professor, Informa
Electronic Engineering, University College London.

Anna Maria Mandalari works as Assistant P
Engineering, University College London. Sh
and expert fellow of the UK SPRITE+ Hub.

Anna Maria Mandalari has been nominated
PhD within the framework of the METRICS
Carlos III University of Madrid. Her researc
studies privacy implications and informatio
strategies based on Internet measurements
create awareness on security, privacy, and ethical AI. Most of her research
influence on media and policymaking. Anna Maria Mandalari is also commi

Steering Board member

We are the Super Blue Team, and we're here to help. The Internet of Things Security Foundation (IoTSF) is a not-for-profit, global membership association working to make the connected world ever-more secure.

In unity we have strength. We each have a valuable role in keeping the digital world secure. Our stakeholders include IoT hardware and software product vendors, network operators, system specifiers, integrators, distributors, retailers, insurers, local authorities, academic institutions, government agencies security professionals, researchers and risk managers – anybody with an interest in cyber safety, security and privacy.

https://iotsecurityfoundation.org/

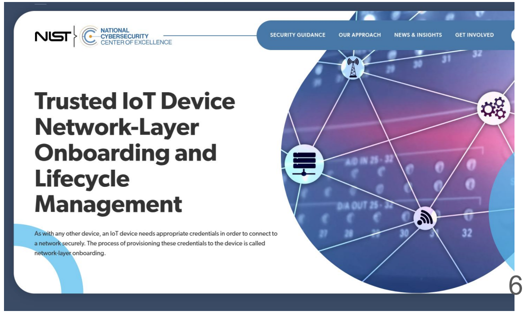
What is this forum about? What are Device Identities?

- Device Identities are cryptographically strong credentials that are installed into devices.
- They identify both the unique identity of the device (“serial number”), as well as point to the device type.
- The credential can be in a Secure Element, TPM, Trusted Execution Environment (or not).
- They credential can be used to sign Evidence for Remote Attestation (the “AK” in a TPM).
    - External Endorsements can be attached to this key
- They can be provisioned in the factory (IDevID), or in the field (LDevID) in both greenfield and brownfield situations.
- Today: RSA, EcDSA (EdDSA). Later on, we’ll need Quantum-Safe versions.

Why is the forum starting/occurring now?

- It was time. It took some in-person time to properly explain (vs COVID)
- The NIST NCCoE IoT Onboarding project identified a new for more understanding of factory installed identities.
- Maturation and deployment of: DPP (Wi-Fi EasyConnect), CSA MATTER, BRSKI, OPC UA and other onboarding protocols have **device identity** as a core requirement
  - This should be easy.
  - It is easy, but people don't know that.
- UK,California,CRA and other jurisdictions putting new requirements on IoT devices…
  - but how can operators know what device is which?

https://www.nccoe.nist.gov/projects/trusted-iot-device-network-layer-onboarding-and-lifecycle-management



Trusted IoT Device Network-Layer Onboarding and Lifecycle Management

As with any other device, an IoT device needs appropriate credentials in order to connect to a network securely. The process of provisioning these credentials to the device is called network-layer onboarding.

What is the forum going to do?

1. White paper(s) explaining how to do device identities.
   a. This is likely in the form of success stories. Maybe like *The Goal* https://en.wikipedia.org/wiki/The_Goal_(novel)
   b. NDA-free Technical explanations of what to do, what the choices are. A menu of a few choices, rather than starting from scratch each time: “Yes, I’ll have the Quarter Pounder without onions”
   c. Something something Quantum-Safe something.
   d. Certificate, CA lifetimes, Brownfield updates, ways to connect to MUD
   e. The connection between device identities, IDS and asset management
2. Creating a common language to talk about device identities.
   a. English words and sentences.
   b. Elevator pitches suitable for C* Suites.
   c. Common icons for important ideas/things
   d. Some reusable slideware collateral for use in (outward) facing presentations
3. A common place to talk about limitations, confusions and other obstacles.
   a. With, ideally, Chapter House rules on attribution.

Please sign up, even if you can’t make it, so you can be contacted.
Or unicast me: mcr+ietf@sandelman.ca

IETF related things

Proposed new IETF WG: SETTLE

`SEcure access To Tls Local rEsources`

https://mailarchive.ietf.org/arch/browse/settle/

https://github.com/danwing/settle-charter/blob/main/charter.md

How do I, or rather, my non-technical neighbour, get a certificate for their new device such that they can access the device via a “standard” web browser?

We’ve been here before: IOTOPS presentations about SUIB, also RIPE IoT presentations about same.

IETF IoTOPS WG rechartered

Now able to do some protocol work:

- device lifecycle: discovery of software updates, configuration backup/restore, end of life, …
- New home for MUD work!

RFC7228bis (taxonomy of constrained devices), is much expanded.

Discussion!

sandelman.ca/deviceidentityforum