DISPATCH/
SECDISPATCH @IETF124

A standard for transparency and falsifiability for privacy and security infrastructure

https://datatracker.ietf.org/doc/draft-laurie-tmif/

Ben Laurie, Tiziano Santoro, Pauline Anthonysamy, Sarah de Haas
Google, LLC

I E T F®

Motivation

- Users desire transparency about privacy claims with the sensitive data being processed by "black box" systems.
- There is no industry-consistent and agreed-upon mechanism or standard for services to reassure users and make **verifiable claims** about data privacy.
- This work aims to build trust by providing a standard mechanism for services to make **falsifiable claims** about their transparency.
- This allows for independent verification and auditing, moving the model from "trust us" to "verify us."

Background

- **Proposal:** A "Transparency Metadata Interchange Format" (TMIF) - a standard JSON format.
- Services ("claimants") can host this metadata to formally describe their **transparency levels and make falsifiable claims.**
- This enables independent auditors ("evaluators") to assess and verify these claims using tools like Remote Attestation and TEEs.
- **Draft Pointer:** https://datatracker.ietf.org/doc/draft-laurie-tmif/

Background

The current goals of the standard are the following:

- Define a **target system** (e.g. what are the usual components of a system that claims provable transparency)
- Define a **set of metadata** to include in the protocol that contribute to falsifiability as a metric
- Define **additional metadata** that do not directly contribute to falsifiability but may be useful to communicate

Background - Example falsifiability metadata

- **Open Sourcing privacy-critical system components:** whether or not the system open sources certain key components that allow falsifiability of e.g. information flow
- **Full OSS including workload:** Does the system provide OSS repos for the entire stack
- **Reproducible builds:** Can the OSS components be built to binaries that match the attested binaries

I E T F®

Desired dispatch outcome

- Assign to an existing working group
    - Trusted Execution Environment Provisioning (TEEP)
    - Secure Evidence and Attestation Layer (SEAL)
    - Supply Chain Integrity, Transparency, and Trust (SCITT)
    - Remote ATtestation ProcedureS (RATS)

- or

- Informational RFC