RATS Privacy Framework

draft-ounsworth-rats-privacy-framework

Mike Ounsworth, Hannes Tschofenig
Guiliano Lehmann

The Core Problem

The core problem is that the RATS Architecture does not account for the possibility that **a Verifier (or Relying Party) could be malicious** (either actively or passively) and forcing the Attester to disclose information against its own interests.

“Coercive use of RATS”

We claim that this aligns with the 2023 IAB Statement on the risks of attestation [1].

[1]: https://datatracker.ietf.org/doc/statement-iab-statement-on-the-risks-of-attestation-of-software-and-hardware-on-the-open-internet/

Example 1a: The Problem

<Mobile Device>

<Web Service>

"What hardware are you running?"

"FunPhone 7”

"Sorry, FunPhone’s manufacturer has not paid the licencing fee for this service"

ACCESS DENIED

Reasonable for a private (enterprise) service, but IAB argues this is not reasonable for a public Internet service.

Goal is to give the Attester more control over when it will agree to provide attestation.

Example 1b: The Problem

<HSM>

<Attacker>

"What firmware are you running?"

"Firmware 1.2.3”

"Thanks! So vulnerable to any CVE since 2019…"

hack hack hack

“What firmware are you running now?”

“Firmware‾″ ¿□□”

“Excellent”

Example 1: Solution

<HSM>

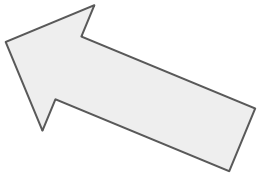
<Attacker>

"What firmware are you running?"

"Sorry,

You're not authorized to

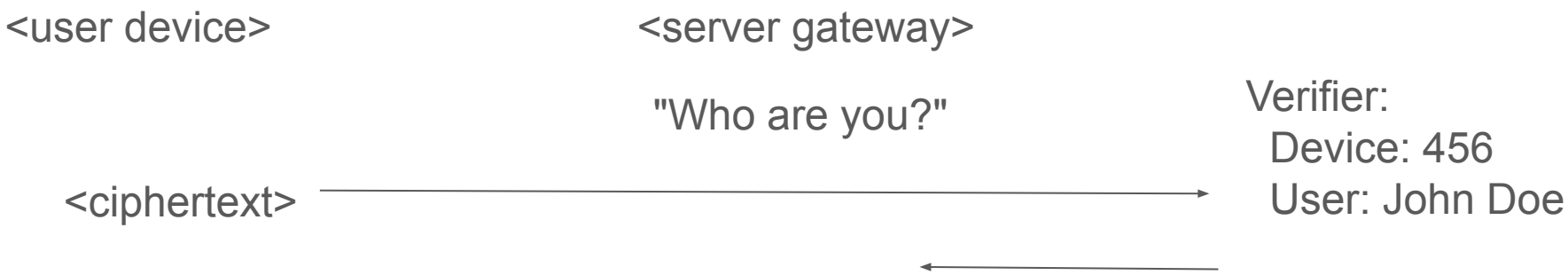
view that claim"



This concept of “Authorized to view a claim” does not exist in RATS today.

The problem: What about Confidentiality of Evidence?

The ideal scenario is:



RFC9334 and RFC9771 (EAT) do allow for this, but only really mention it in passing and do no not provide a strong framework or implementation guidance for when and how Evidence should be encrypted.

Side benefit: where Evidence contains PII, doing object-level Evidence encryption helps control which systems are “infected with PII” from a legal perspective.

General Shape of Solution

To protect against coercive use of RATS (ie a malicious **Verifier / RP)**, you need:

- **Confidentiality**
  Encrypt the evidence only for an intended and authorized Verifier / RP.
  (technically already supported by RATS / EAT, but not well formalized)
- **Integrity**
  RATS already requires Evidence / Attestation Results to be signed ✅
- **Authentication / Authorization**
  RATS currently has no concept that the Verifier / Relying Party needs to authenticate itself to the Attester, or that it may not be authorized to view certain Evidence.

Our draft

… is a rough -00, but the general idea is:

- Introduce the idea that “Release of Evidence to a Verifier” is a step that carries all the usual privacy implications (Confidentiality, Integrity, Authorization).
- Add a concept that some claims can be sensitive.
- Add a mechanism for an Attester to encrypt Evidence for a Verifier.
  - Takes care of Confidentiality against a passive eavesdropper.
  - Provides a natural point for an Attester to enforce Authorization by checking the Verifier encryption key against a trust store.
  - (Evidence already has Integrity thanks to signatures)
- Introduce Selective Disclosure and Zero-Knowledge Proof frameworks for Attestation Results.

- We submit this as an -00 for RATS WG Adoption.
  - Privacy is of course a complex multi-headed topic, so the draft can grow to cover more of the attack surface.

The Framework (in more detail)

First is a conceptual framework for classifying Evidence claims and Attestation Result claims as identity-related information, Attester Identifiers, Fingerprints, Vendor Info, or unclassified.

Second is a threat framework that separates disclosure to Verifiers, disclosure to Relying Parties, and disclosure to eavesdroppers.

Third is a technical framework whereby an attesting client (RATS Attester or Presenter) maintains one or more trust anchor stores for Trusted Verifiers and encrypts sensitive Evidence for authorized Verifiers.

Fourth is a technical framework for minimizing Attestation Results before they are disclosed to Relying Parties. This includes conventional data minimization, Selective Disclosure, and Zero-Knowledge Proofs.

The draft

draft-ounsworth-rats-privacy-framework

What the draft is not:

- A protocol

What the draft is:

- A technology-agnostic framework for adding a privacy layer to a remote attestation protocol.
- A discussion-starter for what privacy considerations are not currently well-addressed by RATS.