Formal Verification of xXxXx, BSc proj (Autumn 2024)

Mathias Emil Lystlund Rasmussen

October 6, 2024

Contents

Abstract

Acknowledgement

1 Introduction

help library, or head to our plans page to choose your plan.

2 The Entity Attestation TOKEN(EAT) draft-ietf-rats-eat-31

Entity Attestation Token or EAT is a protocol ... . EAT provides

2.1 Motivation

2.2 Remote attestation

Remote Attestaion (RA) is a security concept/method used to verify the integrity and trustworthiness of a system. In RA, a peer (The Attester) produces "believeble" information about itself (evidence) to enable a remote peer (The relying party) to decide whether to consider the attester a trustworthy peer or not, and what level of access that the attester should have in your system.
The concept of Remote attestation is not new, and is used all over and in many systems. The problem with remote attestation is, that it has traditionally been implemented in a proprietary manner, instead of something that is standardized.[1][2]

2.3 Remote ATtestation procedureS (RATS)

As mentioned, the previous problem with attestation was that our systems were proprietary systems for special use cases as supposed to something that was broad and standardized. The Internet Engineering Task Force (IETF) took these prior examples of deployed systems of attestation and tried to standardized them.
So RATS is a standardized architecture (not a protocol), which purpose is to create standardized formats within existing/new protocols/systems, in order to achieve mutual attestation. [2][1]

In the RATS architecture the attester produces evidence about it self and sends it to a verifier. The verifier then evaluates the evidence to what is called "Attestation Result". The verifier then sends the attestation result to the relying party, that then decides what access to give the attester.[1][2]

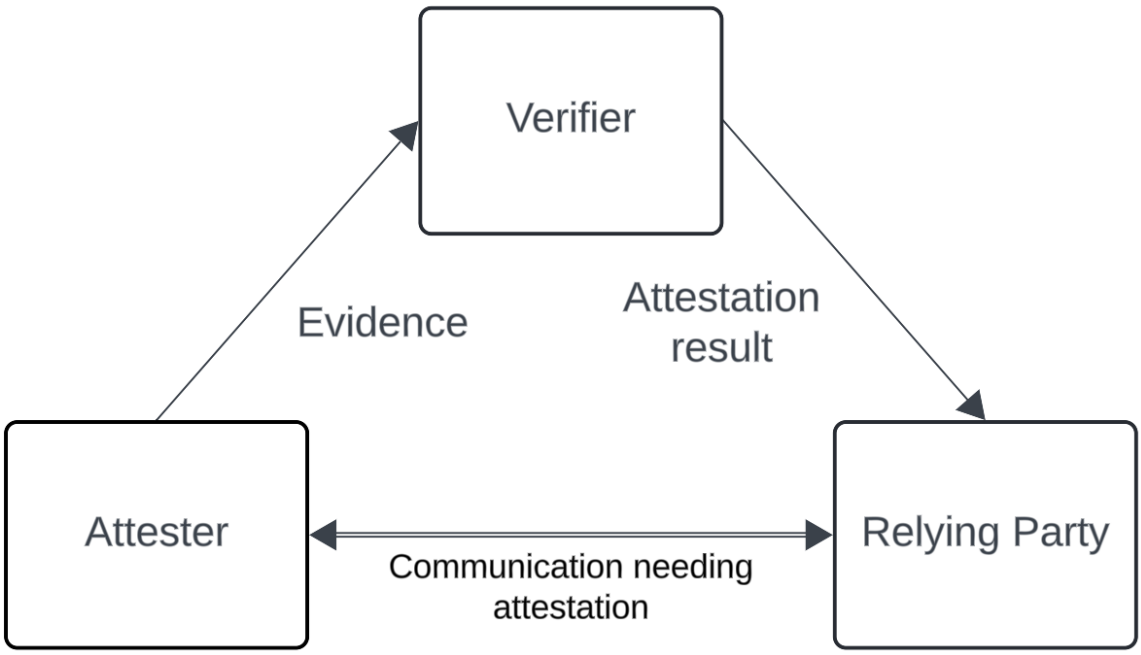

Figure 1: Simple RATS model

The attester can be any IoT device, computer, server etc, trying to gain access to a network, system, or resources and needs to be trusted by the system that it is interacting with. An attester ”can” contain a root of trust, which is a piece of hardware, software or both, designed to provide secure and verifiable information about the attesters state.

2.4 Layerd Attestation and Composite devices

2.5 EAT

The EAT protocol follows the operational model described in the RATS Architecture [1][3].

2.6 Jason web token (JWT)

A Jason Web Token or JWT, is a... Token based authentication...

References

[1] Birkholz Henk, Thaler Dave, Richardson Michael, Smith Ned, and Pan Wei. Remote attestation procedures (rats) architecture, 2023. URL: https://datatracker.ietf.org/doc/rfc9334/.

[2] Confidential Computing Consortium. Remote attestation procedures (rats) architecture, 2021. URL: https://www.youtube.com/watch?v=j30PhEWKgG4.

[3] Lundblade Laurence, Mandyam Giridhar, O'Donoghue Jeremy, and Wallace Carl. The entity attestation token (eat) draft-ietf-rats-eat-31, 2024. URL: https://datatracker.ietf.org/doc/draft-ietf-rats-eat/.