Request Musings

Anna Fritz

September 19, 2022

The purpose of this document is to describe the format of the request and present some examples scenarios to showcase how the request may change. For the past year or so, our ideas about the request have fluctuated. We believed each request should include a nonce for freshness and a signature by the relying party (attester) to ensure authenticity and integrity. However, the specific format of the request remained undecided.

1 Request Format

In recent meetings with NSA and MITRE (8/1/22) we envisioned the request would be a list of protocols as this representation would be suitability abstract to capture the variety of attestation scenarios. With this in mind, we concluded the request will be composed of four attributes. These items are:

- nonce
- list of protocols (terms)
- situational identifier
- signature (by relying party)

Interestingly, the main component of the request is a list of protocols as opposed to a list of ASPs, a list of targets, or a list of evidence. With a list of protocols, the request is able to relay specific ASPs and measurement targets together. Requesting evidence might be a useful concept but evidence reflect concrete values and we believe it is more useful to request abstract values in the form of terms. With these abstract terms, the target has the opportunity

to map requested terms to one or many suitable attestation components that may satisfy the requested term.

It is important to note that any naming conflicts will be resolved within the domain of interpretation. Therefore, when the appraiser requests a term, the target will interpret the term such that it reflects the appraiser's intended meaning.

The situational identifier is a mutable field in the ISAKMP security association. We choose to include the situational identifier in the request to allow the appraiser to communicate how they wish to proceed. For example, if the appraiser is strictly willing to only accept a requested term, they may communicate that through the situational identifier. Additional work remains to capture and classify situational identifiers.

Negotiation Situations

I believe there are three different circumstances where negotiation will occur. These include the following:

1. Appraiser is aware of target's infrastructure.
2. Appraiser is unaware of target's infrastructure.
3. Target's infrastructure has unknowingly changed.

In the first case, the appraiser is aware of the target's infrastructure so they may request a list of term or terms that they know are useful when making a trust decision. This may include measuring the target's whole infrastructure or some useful portion of it. In the second case, the appraiser has no knowledge of the target's infrastructure and is therefore unaware of useful terms to request. In this case, the appraiser *may* request the empty list where the target may then respond with some predetermined list of protocols that describe their infrastructure. This second case is more difficult capture and the request therefore could be enforced in a variety of ways. During the third case, the target must somehow communicate that their infrastructure has changed. This case is difficult and requires further considerations as trusting that the target will report when their infrastructure is changed poses additional problems.