Musings on Gathering and Bundling Evidence

Perry Alexander
palexand@ku.edu

March 23, 2015

Abstract

This document captures discussions on evidence bundling in semantic remote attestation. Evidence Bundling is described as aggregation of evidence from multiple sources into a trustworthy package. This necessarily includes primary evidence from the system being appraised and meta-evidence describing the evidence gathering process. This is a living document and will be updated frequently.

1 Introduction

Consider the problem of determining the status of virus checking on a remote system. This might occur when a new computer is asking to join a controlled network such as a university wireless system. The appraiser representing the university wireless system wants to determine the status of an attestation manager representing the new computing system.

On the appraiser side a trivial protocol runs sending a request (`r`) to a target (`t`) and in response receiving a protocol (`Some q`) or refusal to participate (`None`):

```
do { sndRequest(r,t);
     q <- rcvProt(t)
     e <- case q of
            Some p : sndRemote(p,t)
            None : None
          end;
     case e of
       Some v : appraise(v)
       None : None
     end
}
```

If the request returns a protocol (`p`), the appraiser sends the protocol to execute on the target. Evidence (`e`) is received from the target and appraised if it is valid evidence.

On the attestation manager, a protocol runs that receives a request from the appraiser (`a`), evaluates its privacy policy (`priv`) with respect to the request and the appraiser's ID. If its privacy policy is respected and the appraiser trusted, it returns a single attestation protocol (`p0`). Otherwise, it refuses to participate (`None`):

```
do { (r,a) <- rcvRequest;
     p <- if (priv r a) then Some p0 else None;
     sndProt(p,a);
     (q,a) <- rcvRemote;
     e <- if p=q then execute(q) else None;
     sndEvidence(e,a)
}
```

There is no negotiation, just a simple determination if the request satisfies the target's privacy policy. If so, the only protocol that can be returned and executed is `p0`.

The interface between this negotiation protocol and the attestation protocol resulting from it is the `execute` function that causes the attestation protocol to run on the attestation manager.

To consider bundling, we look at several examples of an attestation protocols (`p0`) for determining the status of a target's virus checking software.

First is a protocol that assesses several properties and runs locally on the attestation manager's system:

```
do { id <- getVCID;
     sig <- getSigFileEvidence;
     src <- getSigFileSrc;
     e <- createEvidence(id,sig,src);
     returnEvidence(e)
}
```

This protocol gets the checker ID (`getVCID`), checks the signature file (`getSigFileEvidence`), and checks the source of the signature file (`getSigFileSrc`). Then it bundles all evidence into a single evidence package (`createEvidence`) and returns it (`returnEvidence`) to be sent back to the appraiser by the negotiation protocol. The appraiser then consumes the resulting evidence to perform appraisal (`appraise`).

The evidence returned has approximately the following form:

$$\langle (id, sig, src), \{||(id, sig, src)|, PCRComp_0|\}_{AIK_0^-} \rangle$$

where (id, sig, src) is primary evidence and hashes and signatures are meta-evidence. An appraiser can check: (i) primary evidence to assess the measured virus checking subsystem; and (ii) the signature on the quote to determine its authenticity and *PCRComp* to assess the platform construction. This is a trivial example of what we call bundling—combining primary evidence and meta-evidence in the same evidence package.

Another protocol represents simply telling the appraiser a virus checker is running:

```
do { id <- getVCID;
     e <- createEvidence(id);
     returnEvidence(e)
}
```

This simpler protocol generates less evidence than the first, but may be more acceptable to the target system. The appraiser could determine this is insufficient or limit access to resources and services based on its appraisal.

A more interesting case for the attestation protocol happens in the presence of more complex bundling:

```
do { id <- getVCID;
     sig <- getSigFileEvidence;
     src <- getSigFileSrc;
     srcQuote <- appraiseSrc(src);
     e <- createEvidence(id,sig,src,srcEvidence)
     returnEvidence(e)
}
```

In this case the `appraiseSrc` function does a full appraisal of the signature file server, `src`. The function communicates its need for evidence from the signature file source to the appraiser associated with the attestation manager. That attestation manager then executes a similar negotiation protocol as the one that started the appraisal process. The resulting evidence, `srcEvidence`, has the form:

$$\langle (e), \{||e|, PCRComp_1|\}_{AIK_1^-} \rangle$$

is signed by the signature file server, not the original appraisal target with its own AIK. Thus, the information from the encapsulated quote is bundled in the outer quote:

$$b = \langle (e), \{||e|, PCRComp_1|\}_{AIK_1^-} \rangle$$

$$\langle (id, sig, src, b), \{||(id, sig, src, b)|, PCRComp_0|\}_{AIK_0^-} \rangle$$

The appraiser must somehow interpret the quote from the signature file server without *a priori* knowledge of its identity.

This more general version of the bundling problem requires:

- Strong identification of the signature file server to the appraiser
- Nested evaluation of the privacy policy for the "other" attestation manager before executing the entire attestation protocol.

An alternative implementation would have the attestation manager return the identity of the signature server and allow the appraiser to negotiate separately with the signature server. This could be called *flattening* the protocol if there is a desire to name it.

```
do { sndRequest(r0,t0);
     q0 <- rcvProt(t0);
     e0 <- case q0 of
             Some p : sndRemote(p,t0)
             None : None
           end;
     r1 <- appraise(e0);

     sndRequest(r1,t1);
     q1 <- rcvProt(t);
     e1 <- case q1 of
             Some p : sndRemote(p,t1)
             None : None
           end;
     appraise(e1)
}
```

Is this flattening operation—eliminating hierarchy in the attestation protocol—a general operation or something that applies only here? If it is not general, can we live with its limitations? Can we assert any correctness properties for it? Could there be an interesting man-in-the-middle attack where the outer attestation manager could negotiate in bad faith and return instructions to the appraiser that produce a bad result?

A Glossary

Primary Evidence Evidence describing the measured application.

Meta-Evidence Evidence describing properties of other evidence.

Negotiation Protocol Sequence of events used to determine what protocol(s) to run and when to run it/them.

Attestation Protocol Sequence of events used to gather and prepare evidence by invoking attestation service providers.

Attestation Protocol Block (APB) See Attestation Protocol Instance (API).

