IETF 108 Remote ATtestations and Procedures notes

Chairs: Nancy Cam-Winget, Kathleen Moriarty, Ned Smith
Notetakers: Michael Richardson, Robin Wilton, Chris Inacio
Jabber: Nancy Cam-Winget

meetecho: https://gce.conf.meetecho.com/conference/?group=rats&short=&item=1 (https://gce.conf.meetecho.com/conference/?group=rats&short=&item=1)

RATS agenda for Tuesday July 28, 2020

- Agenda bash (5min)

sample hum. FORTE had more than five masks.

- RIV - Guy Fedorkow (15 minutes)
  https://datatracker.ietf.org/doc/draft-ietf-rats-tpm-based-network-device-attest/ (https://datatracker.ietf.org/doc/draft-ietf-rats-tpm-based-network-device-attest/)

Remote Integrity Verification: standardizing appraisal of networked devices. Based on the method described in Bierholz RATS reference interaction model (see last agenda item). Based on using the TPM as the attesting module.

RIV aims to appraise:

- code
- credentials
- configuration
  of low-level components: firmware, bootloader and OS.

Hashes of attested objects are recorded in the Platform Configuration Register (PCRs) of a TPM (but the hash itself may need to be cross-checked against a lot of object-level measurements)

TCG specifies, quite tightly, some use of the PCRs for UEFI bios based machines. (Many machines not UEFI, and introduces more vendor variability.)

TCG Client Platform Specification docs contain details of which PCRs are used to record which hashes. *But* this isn’t ?binding/normative, so vendors may have to be flexible about register usage.

TCG has published specs for Reference Integrity Measurements and welcomes review https://trustedcomputinggroup.org/wp-content/uploads/TCG_RIM_Model_v1-r13_2feb20.pdf (https://trustedcomputinggroup.org/wp-content/uploads/TCG_RIM_Model_v1-r13_2feb20.pdf)

Q: has anyone read this draft who is not an author?
A: three people listed in ME, plus 3 in jabber… estimate 6-7.
** WGLC to be planned **

- CHARRA Update – Eric Voit (10min)
  https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/ (https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/)
  Slides: https://www.ietf.org/proceedings/108/slides/slides-108-rats-sessb-charra-update-00 (https://www.ietf.org/proceedings/108/slides/slides-108-rats-sessb-charra-update-00)
  Goals: support challenge-response and information retrieval from TPMs.
  Specify interface using YANG and RPC definitions for the Attester.

Two questions among the list of issues raised:
1 - Should the algorithm set defined in YANG be reduced to just those asymmetric algorithms currently exposed in the current TPM 1.2 and 2 specifications? **authors asking for response on the list, not necessarily a hum**

2 - Is a new log type needed for network device boot?

Mike Jones: RSA + SHA1; W3C did choose to list this although deprecated, because TPM 1.2 does include it. (But would prefer it if people moved off it)

Michael Richardson: If a device is out there, that should be the factor, not whether an algorithm has been deprecated. The appraisal policy isn't obliged to accept it. (There are multiple +1 on jabber about this)
Eric: an implementer can still exclude "unwanted" algorithms/devices by not listing them as "allowed algorithms".

Roman Danyliw (AD): What to encode the insecure algorithms, because perviously supported by TPM implementations, but document in the YANG model that these are deprecated and should not be used. But included because HW supports.

Eric: That's right and there's another mechanism to discover what algorithms are supported by the specific device. But don't necessarily have to approved by verifier.

Wei Pan: Issue #8: strongly suggest using TPM name as identifier rather than certificate name, because the certificate name can change.

Eric: on cert name; issuing a new cert means the YANG model tree has to be updated anyway, so this won't save much time. But can discuss on the list.

- Network Device Subscription – Eric Voit (10min) https://datatracker.ietf.org/doc/draft-birkholz-rats-network-device-subscription/ (https://datatracker.ietf.org/doc/draft-birkholz-rats-network-device-subscription/)

Goal: improve what is done using CHARRA, by overcoming a time constraint introduced by dependence on RPCs.
Extends draft-birkholz-rats-network-device-subscription draft in a couple of respects.

Dave Thaler: How is the flow described on "Fresh Security Telemetry" slide bootstrapped? Two things to make sure the draft covers (at least by citing another doc for more info): 1. how do you know who to subscribe to (first time). 2. what happens when attester reboots.
Eric: this assumes a CHARRA context is already in place.

If the attester just rebooted, you won't get a stream of stuff until you subscribe, (and something) how do you reestablish fresh stream data?
Eric: There are a couple of methods for detecting that, but its handled at the transport layer.

Adds a streaming source for attestation data (to complement challenge-response and time-based updates).
Also allows definition of an attestation key in the YANG model.

ACTION: Please indicate interest in potential adoption via the list.

- Interaction Model – Henk Birkholz (10min) https://datatracker.ietf.org/doc/draft-birkholz-rats-reference-interaction-model/ (https://datatracker.ietf.org/doc/draft-birkholz-rats-reference-interaction-model/)

  Summary of three RATS interaction models

  - Challenge-Response
  - Time-based
  - Streamed

  Fourth model written up by Surry University researchers to allow for Direct Anonymous Attestation (DAA) in which authentication secrets are attested for a group (that shares the same characteristics), rather than an individual device.

QUESTION: Where should the documentation of these interaction models be stored?
(1: stand-alone, one-ID for each model, 2: stand-alone: one I-D for all models, 3: all three models in architecture, 4: each model in a solution I-D)

Chair: Some documentation for the individual models already exists, so there's a question whether this additional material is useful. In the interests of time, take to list please.

Chat: couple of participants indicated that Option 3 was unpalatable.
Michael Richardson: Suggest asking (the list) for objections (e.g. which options are unacceptable)

Meeting closed at 13:52UTC