Increasing trust and preserving privacy

Advancing remote attestation

Ionut Mihalcea & Thomas Fossati
+ Hannes Tschofenig
Intros

- Ionut Mihalcea (ionut.mihalcea@arm.com)
- Thomas Fossati (thomas.fossati@linaro.org)
- Hannes Tschofenig (hannes.tschofenig@gmx.net)
At an inflection point?

- Increasingly available
- Increasingly used

“Every authentication use case is also an attestation use case” (Dave Thaler)
Centralisation & Privacy Considerations

- Verification of attestation evidence
  - & centralisation (see also RFC 9518)
  - & privacy (see also Section 11 of RFC 9334 and Section 8 or EAT)
Tackling centralisation

- User-centrism?
- A neutral Verifier?
- What else is in the toolbox?

- **WEI**, a cautionary tale
Tackling privacy

- **Long history with Direct Anonymous Attestation (DAA)**
  - Adopted by TPM v1.2 specification
  - Implemented but not widely used.
  - FIDO offered different privacy solutions
    - Variant of DAA defined but deployments lacking
    - Lightweight alternative: "group" keys shared across a set of FIDO authenticators with identical characteristics

- **PrivacyPass is a recent effort**
  - Uses recently standardized privacy technologies, including BBS signatures, RSA Blind Signatures and Verifiable Random Functions.
  - Deployed by Apple and Cloudflare as a CAPTCHA replacement

- **Renewed excitement for privacy with “Verifiable Credentials” in OAuth/OpenID Connect**
  - Selective Disclosure (SD) JSON Web Token (JWT) in OAuth working group
  - Secure Patterns for Internet CrEdentials (SPICE) BOF to create a new working group in the IETF.
Rigorous designs

- Pressure to integrate Attestation into existing auth[nz] flows
  - Moving away from organic designs...
  - ... to more structured approaches
IETF
Cultivating Open Standards for an Open Source World
IETF principles

- **Open process** - *any interested person can participate* in the work, know what is being decided, and make his or her voice heard on the issue.

- **Technical competence** - The issues on which the IETF produces its documents are *issues where the IETF has the competence needed to speak to them*, and that the IETF is willing to listen to technically competent input from any source.

- **Rough consensus and running code** - We make *standards based on the combined engineering judgement* of our participants and *our real-world experience* in implementing and deploying our specifications.
Attestation in IETF

RATS WG

Endorser
Reference Value Provider
Verifier Owner
Relying Party Owner

Endorsements
Reference Values
Appraisal Policy for Evidence
Appraisal Policy for Attestation Results

Verifier
Evidence
Attestation Results

Attester
Relying Party

OAuth, TLS, EST, ACME, ...
Remote attestation for credential issuance
Example: EST & CMP

draft-tschofenig-lamps-nonce-cmp-est

draft-ietf-lamps-csr-attestation
Remote attestation for credential issuance
Example: ACME

Client (Attester) -> Server (Relying Party) -> Verifier

1. Nonce in ACME authorization challenge
2. Evidence in response payload
3. Attestation result

TPM Attestation Statement
Android Key Attestation Statement
FIDO U2F Attestation Statement
...
Remote attestation for credential issuance

Example: OAuth 2.0

OAuth 2.0
Client (Attester)

Verifier

Authorization server (Relying Party)

(1) Nonce in Dynamic Client Registration

(2) Evidence in Dynamic Client Registration

(3) Attestation result

draft-tschofenig-oauth-attested-dclient-reg

TDX token (EAT)
Arm CCA token (EAT)
PSA Attestation token (EAT)
TPM2.0 evidence
DICE evidence
...
Remote attestation for secure channel establishment
Example: TLS

1. Attestation evidence
2. Attestation result
3. Request attestation credentials in TLS handshake
4. Attestation result as TLS credential

draft-fossati-tls-attestation
Formal verification

- Specification
- Formal Verification*
- Implementation
- Deployment

* Usable Formal Methods Proposed Research Group
Join us!

- RATS WG
- IETF Hackathon
- CCC Attestation
- Specification
- Implementation
- Formal Verification
- CCC Formal Methods
- UFMRG
Join us!

RATS WG

CCC Attestation