Trustworthy Workload Identity Extensions for WIMSE

IETF 123 Madrid

Setting Context

- Myself
  - Sr. Principal Cybersecurity Architect, JPMorgan Chase
  - Ex-Windows Platform Integrity and Azure Attestation Architect at Microsoft
  - Almost 20 years of involvement with trustworthy and confidential computing
  - Trustworthy Workload Identity SIG Chair and the Confidential Computing Consortium
- Problem Domain
  - Thousands of applications
  - Over a hundred jurisdictions
  - Several “high-risk locations”

”Here is some software we’d like you to run on your reverse proxy. We are not going to tell you what it does, but if you don’t do what we say, you don’t get to operate in our country.”

Confidential Computing and WIMSE

- **Confidential Computing**: Protection of data in use by running software in a hardware-based Trusted Execution Environment (TEE)
- Utilizes "**Remote Attestation"**: communicating with an external "Verifier" to map "evidence" to "attestation results"

Generally Compatible with WIMSE

- Requires the binding of credentials to workload instance – so does WIMSE
  - Confidential Computing mitigates credential extraction attacks, strengthening the binding
- **Agent, if used, MUST be part of the attested workload, not external to it**
  - **A TEE does not trust its hosting environment, and cannot let it establish identity on its behalf**
- Provenance can be discovered via unique credential identifier such as "jti" claim or unique certificate identifier

References and Contacts

- Confidential Computing Consortium (CCC):
  - https://confidentialcomputing.io
- TWI SIG at the CCC:
  - mailto:Trustworthy-Workload-Identity-SIG+subscribe@lists.confidentialcomputing.io
- TWI SIG Charter:
  - https://github.com/confidential-computing/governance/blob/main/SIGs/TWI/TWI_Charter.md
- Speaker:
  - mailto:mr.mark.novak@gmail.com