Exploring Trust Contexts in Attested TLS Environments

Pavel Nikonorov

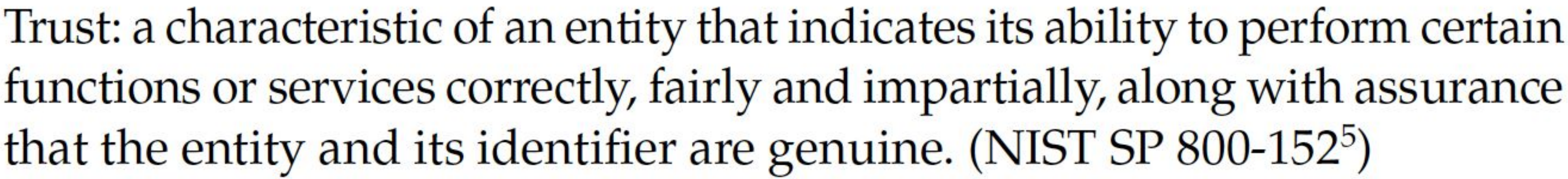
GENXT

pioneering company in the adoption of confidential cloud technologies in biomedical research.

genxt.network

TRUST = confidence in a security aspect protection [1]

within a defined context [2]

[1] 

Trust: a characteristic of an entity that indicates its ability to perform certain functions or services correctly, fairly and impartially, along with assurance that the entity and its identifier are genuine. (NIST SP 800-152[5])

[2] “Trust in Computer Systems and the Cloud”, Mike Bursell

TLS Trust Contexts

1. **Identity & Authenticity of the Remote Service**
   (if the cert is **not self-signed)**

2. **Data Confidentiality & Integrity**
   during transmission only

Data owner can’t control the data usage
after the data was shared

Attested-TLS + PKI — Trust Contexts

1. **Remote Identity and Authenticity**
2. **Confidentiality & Integrity for Data-in-Transit**
3. **Workload Run-Time Memory Isolation**

Yet it does not cover the workload software trustworthiness within any possible context

Attested TLS + PKI – Trust Anchors

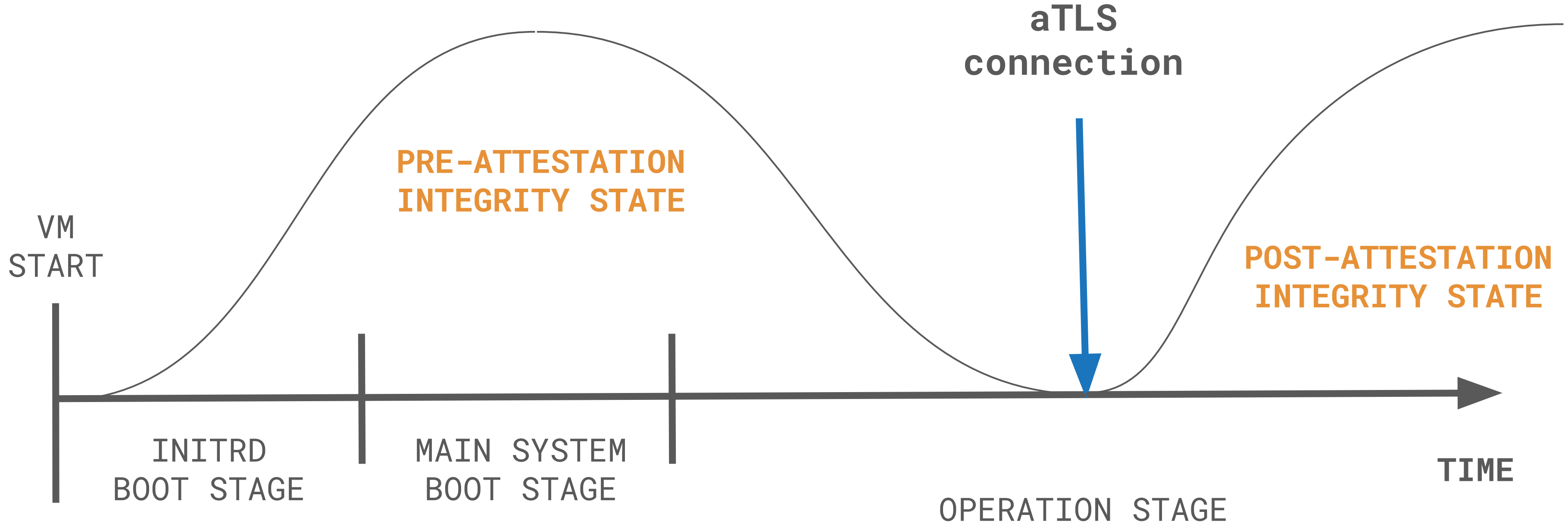
1. PKI/CA root certificates
2. CPU/GPU VCEKs
3. Required:

   Curated registry of verified software, configuration and security policy files

Additional Trust Context Required

- confidentiality of ephemeral private keys
- only white-listed events permitted, including binaries execution, network and disk access
- enforcement of data owner’s privacy policy
- automated response to malicious activity

Time as a Critical Dimension in Trust



Inferring Trust in Attested TLS Environments

1. Store reference checksums of audited software
2. Include TEE Report, TPM Quote, and IMA log in Attested TLS Evidence
3. Verify the whole software stack, configuration and policy files of a remote VM against reference checksums
4. Infer trust based on the whole verification chain

Discussion / Open questions

1. **Schema for reference store of the checksums**

   Current idea is to leverage GA4GH Tool Registry Service API

   https://github.com/ga4gh/tool-registry-service-schemas

2. **Formalisation of Attested-TLS trust contexts**

   Our take on that in

   https://f1000research.com/posters/13-1317

   WP: https://shorturl.at/zRKe2

   Contributions/feedback/critics are welcome!

Seeking collaborators passionate about trusted computing!

knowledgeable in at least one of:

- Trust Models & Frameworks
- Formal Methods for Security Analysis and Verification
- Reference Stores and Provenance Tracking

Contacts

Pavel Nikonorov, pavel@genxt.network

linkedin.com/in/pavelnikonorov