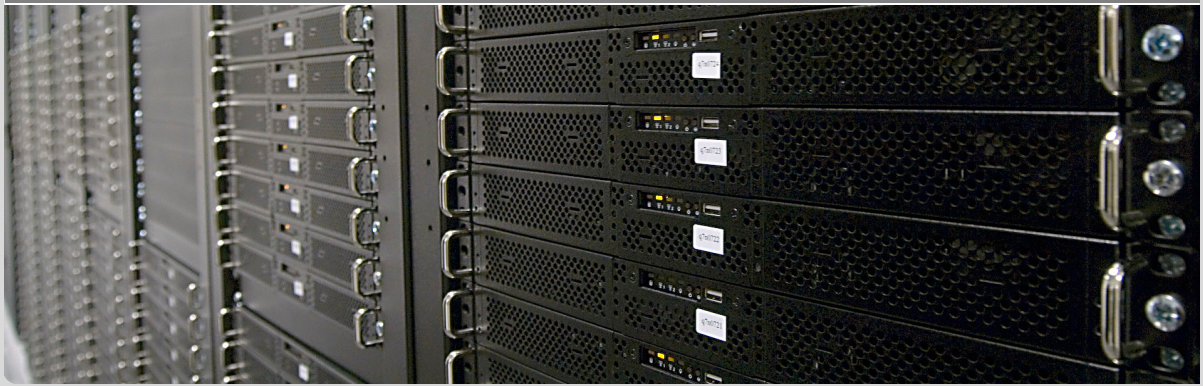
Karlsruhe Institute of Technology

Steinbuch Centre for Computing

Levels of Assurance

Marcus Hardt | 2.3.2015



Levels of Assurance

- My motivation for LoA
  - DFN operates two federations test and advanced
  - Our synchrotron wants to enable Umbrella users, we have to drive them into the technical and legal situation to actually do it
- LoA Definition (RFC 4949, NIST SP 800-63)
  - Entity Authentication Assurance for remote authentication.
  - Descended from a specific legal, technical and business context in the US
  - Does not fulfill the requirements for a comprehensive identity assurance metric
  - LoA is only focused on the quality of the identity vetting
  - Example
    - LOA 1: Some assurance that this is the same Claimant who participated in previous transactions
    - LOA 2: Single factor network authentication
    - LOA 3: Multi-factor remote network authentication
    - LOA 4: Strong multi-factor cryptographic authentication

Vectors of Trust

- Motivation: Existing LoA definition is not enough
- Status: Discussion at ietf-mailinglist and github [1]
- Idea: Introduce linear independent components (of a vector) to describe trust
  - Core components: Identity proofing (P), Credential strength (C), Assertion presentation (A)
  - Under discussion: Operational management, Incident response, Token proofing
  - Example: pseudonymous, multi-factor, strong assertion P1:C3:A2
- Who can assert an IdP? Trustmark providers?
- VoT discussion is based on earlier discussions around and ISO/IEC 29003, 29115
  - Mainly driven by US requirements and handling risks and associated cost
  - Research communities rather don't appear
  - Discussion appears pretty theoretical
- Example Identity Proofing:
  - 0: No proofing is done, data is not guaranteed to be persistent across sessions
  - 1: Attributes are self-asserted but consistent over time, potentially pseudonymous
  - 2: Identity has been proofed either in person or remotely using trusted mechanisms (such as social proofing)
  - 3: There is a legal or contractual relationship between the identity provider and the identified party (such as signed/notarized documents, employment records)
- Short summary of VoT discussions in [3]
- Interesting who was active on the list: mitre.org (Justin Richer), cisco, lockstep.au, kanatara, u-texas/ medical, safe-biopharma, osu.edu, sk.ee, terena, govt nz

IGTF-LoA (4)

- Background: Grid security operations, extensive experience in incident handling
- Motivation: Integrate grid requirements and existing userbases
- Deals extensively with hows and whats of user identification (this would "simply" be a P=4 in the current VoT discussion)
- In general
  - High-detail level specification of operational requirements, IT-system security, credential strength, site-security (audits), ...
- Specifies four levels of assurance
  - Aspen (SLCS)
    - Lifetime: 1Ms
    - Loss: change authenticator, expiration time short so as to not revoke
    - Identifier: bound to a passport-identified owner at time of issuance
  - Birch (MICS)
    - Lifetime: 400days
    - Loss: change authenticator + revoke existing ones
    - Identifier: bound to a passport-identified owner
  - CEDAR (IGTF)
    - Lifetime: 400days
    - Loss: change authenticator + revoke existing ones
    - Identifier: bound to a passport-identified owner
  - DOGWOOD (IOTA)
    - Designed to work with most existing IdPs
    - Lifetime: permanent credential lifetime, but there's an enforced contractual relation between user and IdP
    - Loss: Don't create new credentials
    - Identifier: must contain ID-vetting entity and guarantee permanent uniqueness of user-id
    - Identifier: contains (possibly pseudonymous) identifier, with guaranteed permanent uniqueness of user-id
    - should be used in conjunction with assertions from other sources

References

1 https://github.com/vectorsoftrust/strawman/blob/master/VectorsOfTrust.md

2 http://dx.doi.org/10.6028/NIST.SP.800-63-2

3 https://altmode.wordpress.com/2015/01/08/level-of-assurance-alternatives-a-modest-proposal

4 http://wiki.eugridpma.org/pub/Main/IGTFLoAGeneralisation/Evolving-Assurance-IGTF-summary-20150121.pdf