On Modeling-Enactment-Explainability Graphs

Joint NMRG-ZSM Meeting

Dublin, 9th November 2024

The Basic Graph

- Structured around three main functions
- Modeling
    - identifying the guidelines to be applied, expressed by intents
    - Translate them into policy rules
    - Evaluate their feasibility
    - Assign service levels
    - Set the automation mechanisms in support of the service levels
- Enactment
    - Apply the guidelines to a given situation, usually termed as policy decision
    - Driven by two main levers
        - Identity, so every entity involved in a particular decision is uniquely identified
        - Evidence, allowing to make the most complete evaluation possible of the status of such entity
- Explainability
    - Support the auditing processes, guaranteeing the evaluation of the decisions and related actions
    - In the light of the applicable models and evidence
    - Different levels can be considered
    - Involved identities and the relevant evidence for each decision

Modeling by Intent-Driven Smart Contracts

- Associate intent to the application of smart contracts.
  - A computer program stored in a DL
  - Wherein the outcome of any execution of the program is recorded by the DL

- Use smart contracts to circumscribe intent
  - Intent language is captured in the smart contract itself
  - Open to any application environment

Intents and Smart Contracts

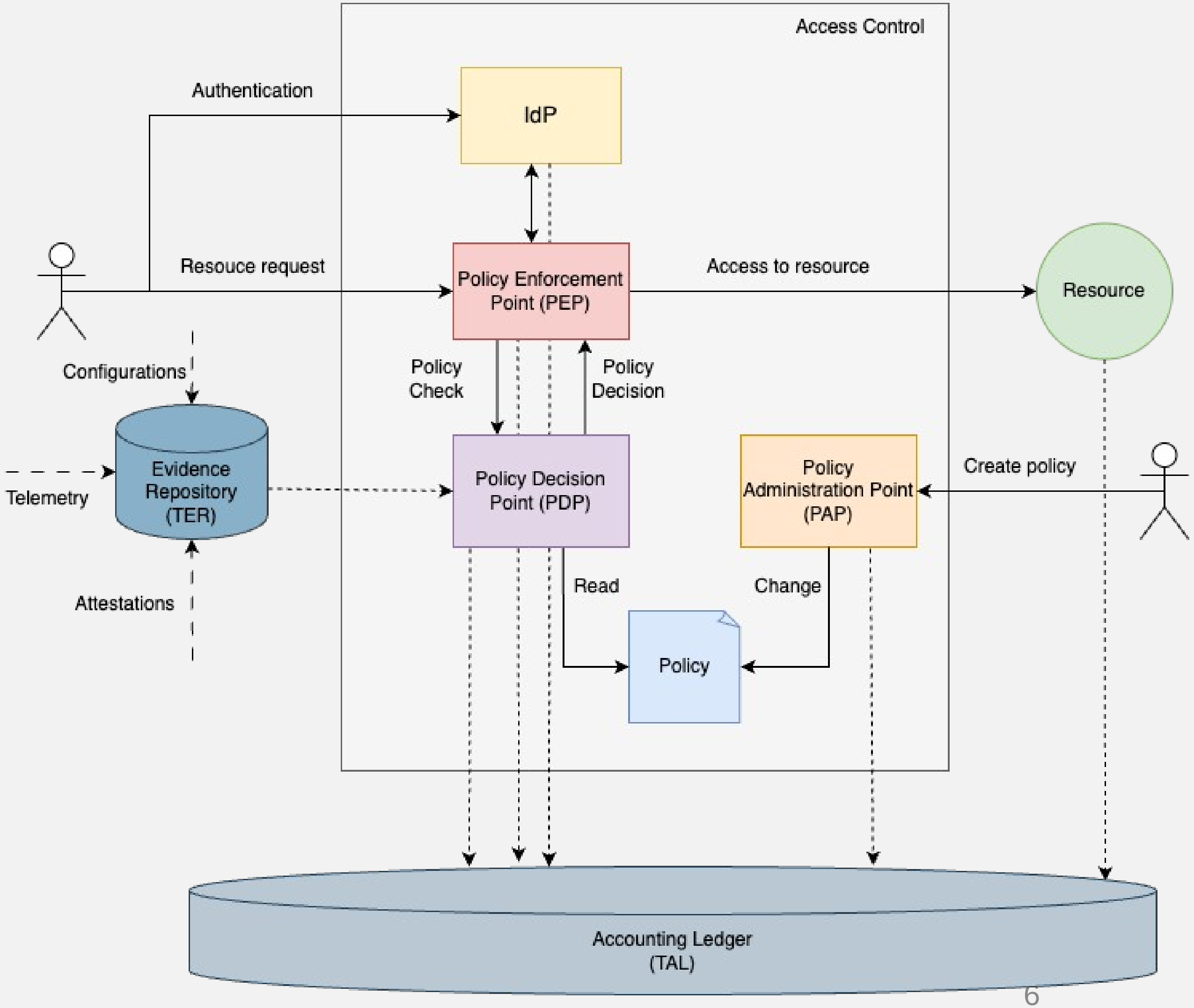
1. The user selects one or more smart contracts from a repository of provider offerings
   - This selection would include a parametrization (for example, with number of nodes, addresses, time frames…)
   - Some vocabulary to express composition
   - Associated to user, process and element identities
2. The provider checks this declaration
   - Verify the feasibility
   - Identify the applicable policy directives in the smart contracts.
3. The smart contract(s) are signed and registered
   - The intent can be declared as “compiled” or ”assimilated”

Feasibility Analysis: What-If

- Synthetic environment (NDT), replica of the real infrastructure
  - Updated by data flows
  - Sandbox to test configurations and their potential impact
- Guided by the what-if loop
  1. Request to the NDT indicating the scenario and metrics
  2. NDT adapts the request and executes the concrete scenario
  3. DT sends back the required metrics

Identity-Based Enactment

- Identify each involved entity
  - Users
  - Components in the system
  - NFs
  - Connections
  - Models
  - Data
- Support identity traceability
  - Relate each element and action to their *origin*
  - An **individual** actor: user and/or system component
  - Recursion becomes essential
- Execute smart contracts
  - Intent declarations associated with identities
  - Features and services they provide
  - As attributes
  - Policy as code



The Data Enabling Enactment

Trusted network paths

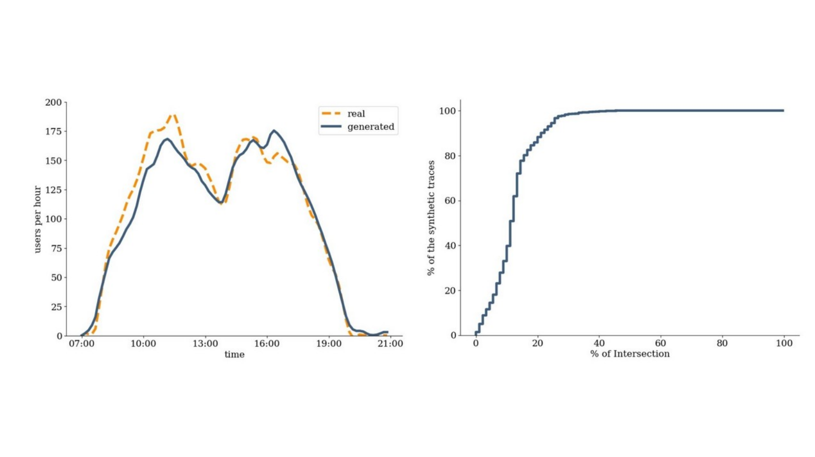
- Means for assessing specific properties on a particular network path
  - Whatever their nature, generally related to a security posture
  - Geolocation
  - Versioning / patch level
  - Supported features
  - . . .
- Attestation of the path components
  - When constructing the path
  - Relaying on remote attestation
- Attestation of the path behavior
  - During its use
  - Relaying on in-band proof of transit

Accountable data

- Provenance: *A documented trail accounting for the origin of a piece of data and where it has moved from to where it is presently*
  - Assurance of the origin and integrity of datasets
  - Native support, avoiding transitive trust
  - Low impact on data models
  - Recursion
- Whenever the dataset is used beyond an original online flow
  - Use of data intermediaries, such as data lakes
  - Audit trails, including forensics evidence
  - Concurrency
  - Integration with pub/sub and time series DBs
- Applicable in other potential cases, beyond telemetry
  - Identity propagation from control to data plane
  - Extended accountability for data flows
  - . . .

Applying Evidence in Explainability

- Identify events
  - Actions (*verbs*)
  - Actors (*subjects*)
  - Targets (*objects*)
- And track back
  - Applicable intent declaration
  - Available evidence
- Rely on accounting records
  - Raw events and smart contract execution
  - Semantically sound
  - Identity-based
  - Transparent
- Generative mechanisms
  - Intent declaration language(s)
  - Telemetry, event and action ontologies
  - Synthetic augmentation for privacy preservation and training data production



And a Few Conclusions

- An ongoing research effort on combining network management activities in a common loop
  - Disaggregated as they are now
- Focused on three essential challenges
  - Identity management (especially, non-human ones)
  - Data flows (and their semantics)
  - Trust links (dynamically managed)
- And willing to apply the most fashionable technologies
  - Smart contracts
  - Generative AI
  - Transparent registries
  - . . .