iTrust6G – Project Scope and Ambitions

Mir Ghoraishi – iTrust6G Coordinator

Gigasys Solutions (mir@gigasys.es)

Co-funded by

the European Union

6GSNS

iTrust6G

iTrust6G

Intelligent Trust and Security Orchestration for 6G Distributed Cloud Environments

- **SNS-JU-2023 Stream B-01-04 Call**
- Kick off on January 1, 2024; for a duration of 30 months.
  - **Website:** www.sns-iturst6g.com
  - **X**: https://twitter.com/iTrust6G (@iTrust6G)
  - **LinkedIn**: https://www.linkedin.com/in/sns-itrust6g-project-1342a92a8/

- **Consortium**:

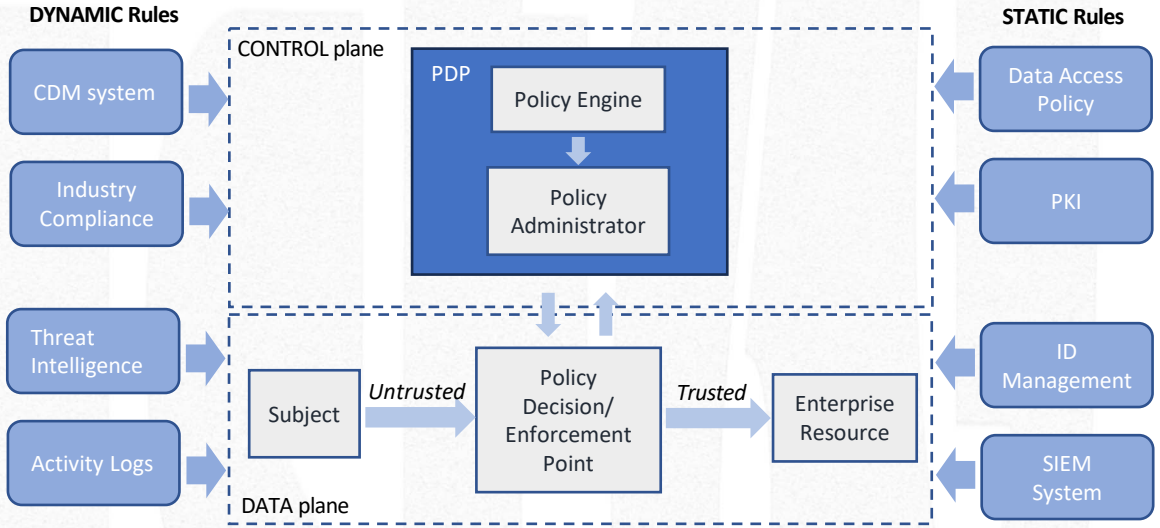
GigaSys Solutions, i2cat, Telefónica, Lenovo, NTUA, PDM 28 Years Challenging Innovation, Politecnico di Torino, adrestia

  - Project Coordinator: Dr Mir Ghoraishi (Gigasys Solutions)
  - Technical Manager: Dr Shuaib Siddiqui (i2CAT)

iTrust6G in a Nutshell

iTrust6G aims to design and develop a network architecture capable of supporting the zero-trust principles and framework, to increase the trustworthiness of 6G networks

- Subjects are applications deployed on 6G platform and "hardware provided at the edge“
- Enterprise resources refer to assets of the 6G platform provider
- Policy Engine and Policy Administrator (PDP) reflect the notion of intent explored by the telco community



A Zero Trust “Never-trust, Always-verify” architecture, is basically a holistic active defence strategy for managing risk, complementing established state-of the-art information security practices
This holistic view also means that network products will follow zero trust framework and enablers

Logical components in NIST SP800.207 ZTA framework

Zero Trust Tenets and Components

Basic Zero Trust tenets:

- ❑ All data sources and computing services are considered assets/resources
- ❑ All communication is secured regardless of network location.
- ❑ Access to individual enterprise resources is granted on a per-session basis.
- ❑ Access to resources is determined by dynamic policy including the observable state of client identity, application/service, and the requesting asset
- ❑ The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
- ❑ All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
- ❑ The network collects information on the current state of assets, infrastructure, communications

Key Components:

- ❑ Identity and Access Management
- ❑ Continuous Monitoring (CDM)
- ❑ Authentication & Encryption
- ❑ Policy Enforcement
- ❑ Micro-Segmentation
- ❑ Visibility and Analytics

iTrust6G Pillars and Objectives

1. Design an End-to-End system security architecture that capitalises on zero trust principles
2. Exploit AI to detect novel threats from operated assets and generate pertinent cyber threat intelligence
3. Conceive novel Trust Algorithms (TA) exploiting AI integrated into trust management system (TM)

4. Intelligent solutions for AI-driven security orchestration, across extreme edge, edge and public clouds
5. Intent-based security policies/engine, for explainable and automated E2E security orchestration
6. A solution for dynamic, configurable placement of network functions over network slices and applications, to secure service design

7. Trial-based validation of solutions in trusted execution environments (TEE) and on specialized hardware (accelerators, etc.), based on defined use-cases requirements

iTrust6G Pillars

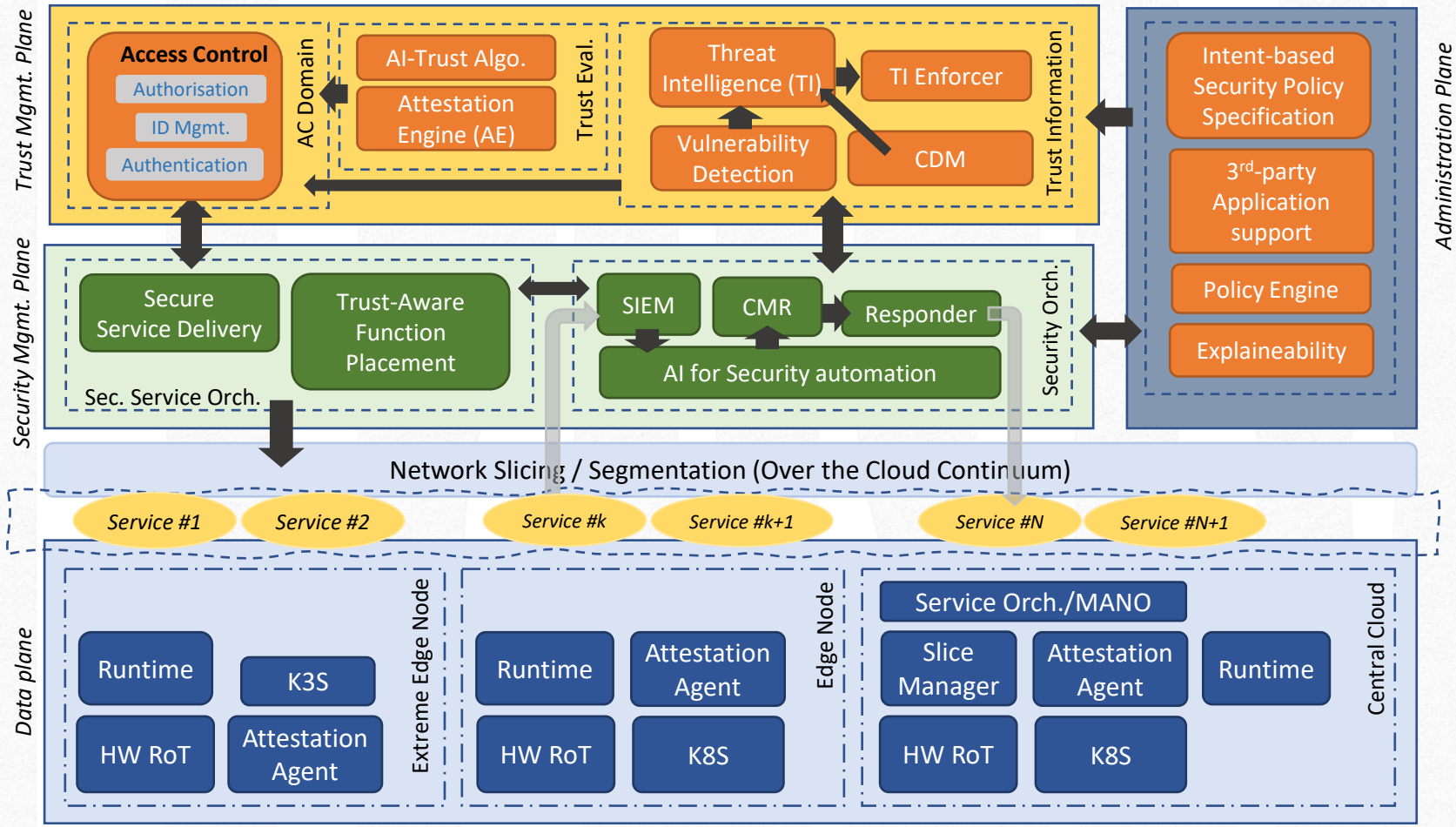
- Zero-trust and incorporation of AL/ML for anomaly/threat detection & prediction
- Continuous threat assessment, and compliance for asset protection
- Intent-based security policy for explainable, AI/ML-enabled E2E security orchestration
- Enhanced observability via programmable interfaces and secure multi-tenancy support

8. Dissemination of project results, contributions to standardisation, exploitation of results and innovation management.

iTtrust6G Innovations

- Enabling trust in 6G platforms towards services operated across the cloud-edge continuum through integration of ZT principles and framework, into the 6G network
- Secure management of diverse set of resources and of multiplicity of criteria to evaluate trust
  - The secure management relates to the E2E security orchestration, i.e., the homogeneous and integrated management of security threats and counter-measures
  - Employment of programmability models to gain an intrinsic visibility inside network services.
- Application of AI/ML to support trust inference from diversified sources
  - New methodologies for trust evaluation: indicators from the supply-chain (NIS2-friendly), integrity metrics (remote attestation), cyber-threat intelligence information, and other metrics related to security posture
- Policy framework to support operator security compliance and to account for potential threats (considering NIS2 framework), at design and run time
  - Intent-based security specification/trust-policy specification
  - Explainability of decision made during the security policy enforcement to reinforce the trust of 6G platform
- Leveraging mechanisms for conformity and trust enabling continuous monitoring of the threat surface of the system
  - Achieved through security programmability, permitting the insertion of additional security monitoring capability
- Ensuring intelligent and secure service orchestration in 6G network operations
  - Accessible in its specification (intent-based security policy) and with an understandable enforcement (explainability)
  - Security incident automation, forensics, and integration based on secure orchestration

iTrust6G Architecture



iTrust6G building blocks span across Infrastructure, Network Service, and Application Domains

iTrust6G Use Cases

iTrust6G vision and concept will be realized through a balanced mix of activities for design and specification of the various solutions, implementation, and demonstration in testbed.

Use Case #1

Dynamic security orchestration and trust establishment in multi-stakeholder and multi-domain environment

The objective is to validate the intent-based security policy enforcement and trust establishment in a multi-stakeholder environment.

Use Case #2

Operational security and trust re-evaluation

The objective is to validate the robustness of iTrust6G operational security mechanisms in presence of attacks including attack detection, mitigation, and forensics.

Use Case #3

Programmable security as a service

The objective is to validate the flexibility and agility of the programmability of security mechanisms at multiple levels based on the status of the application service.

Thank you!

www.sns-itrust6g.com

@iTrust6G

LinkedIn: SNS iTrust6G Project

info@sns-itrust6g.com

Co-funded by
the European Union