**Intent-based Resilience Orchestration in Supply Chains**

**Mounir Bensalem (TUBS)**

Network management and orchestration require high efforts and time from customers and network administrators in order to achieve the business goals. In the supply chains, networks have introduced new challenging requirements considering the heterogeneity of infrastructure, considering different owners, various and geographically distributed devices, and multiple users. Automation is one of the Key Exploitable Results of the FISHY project, which allows customers, i.e. network administrators, to minimize their operation time while being able to manage large and complex networks.

Intent-based resilience orchestration (IRO) has been introduced in FISHY to automatically translate high-level business intents into detailed networking policies, in order to guarantee network resilience. To this end, an important feature of the envisioned intent-based orchestration consists of alerting the user about the state of the supply chain, using the data collected by monitoring tools, performance analysis and proposed mitigation actions. This solution provides a holistic easy-to-use interface, where alerts and recommendations can be used to define the right business intents, without spending significant time on network management.

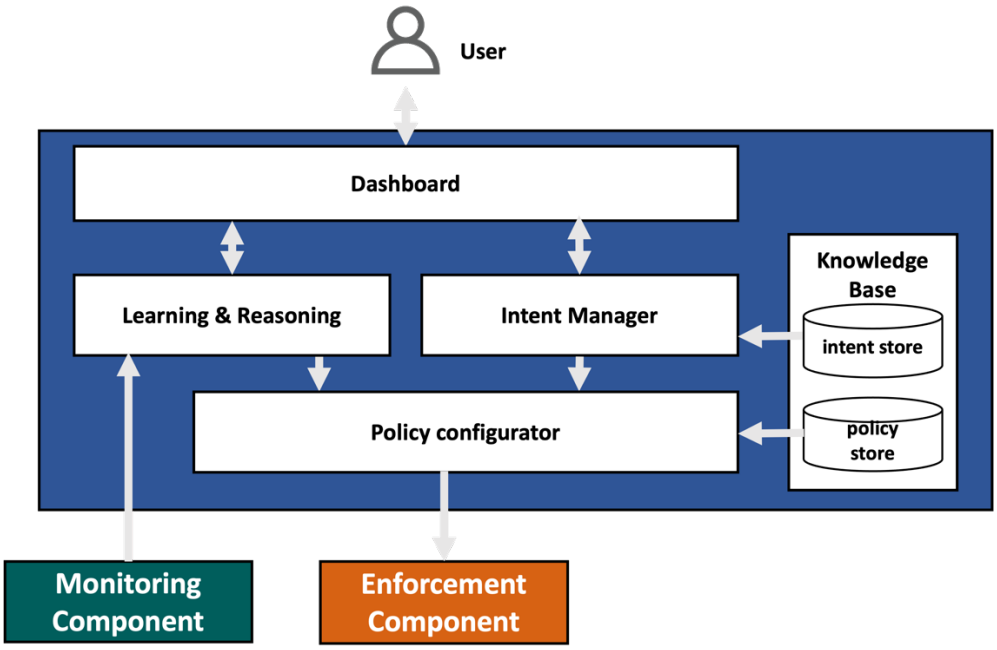
Key enabling factors for intent-based resilience orchestration are: intent and policy definition, network programmability, as well as supply chain security monitoring. In order to make the whole FISHY platform to properly work, intents related to access control and security should be previously defined and appropriately understood in order to be mapped into lower level policies that will be able to specify and configure the network to satisfy business requirements. To this end, another FISHY component, the Enforcement and Dynamic Configuration (EDC), is used by the orchestrator to compile business intents into configured policies. The EDC is using a capability driven approach in order to model network security functions and provide an enforcement mechanism for security policies. Such component is deployed on premises where devices can be configured, which allows the IRO to separately manage policy configuration of each supply chain organization. Network programmability is also an important requirement for intent-based orchestration, where virtual and physical network elements can be programmed to allow the automatic updates inquired by IRO through the enforcement component. Furthermore, network monitoring tools play an important role in gathering and tracking the data related to network devices, applications and users, which represents the essence of any business decision related to the network.

In summary, the IRO is a centralized and high level FISHY component that provides an easy-to-use interface for the user to both check the alerts generated by various monitoring tools and security analytics, as well as define their business requirements through a high-level intent language. IRO consists of several modules that are designed to efficiently enable its functionalities, and can be described as follows:

- **Dashboard:** an easy-to-use interface
- **Intent Manager:** translates the input text in the intent into a structured format containing several fields such as the intent type and parameters.
- **Policy Configurator:** is responsible for matching the extracted requirements from the input intent with exploitable policies, where it configures the required policies stored in a knowledge base to satisfy the user requirements.
- **Learning & reasoning**: is a component that receives information from the monitoring component, checks if an alert or recommendation has to be sent to the user via the Dashboard, and then reacts based on that. The learning and reasoning can automatically react to alerts when

a predefined intent has been given by the user, where it triggers the policy configurator to configure policies and pass them to the enforcement component.

- **Knowledge Base:** stores intent structures, corresponding workflows and security policy templates.




A complete intent-based orchestration solution can play an important role in assuring the security and resilience of supply chains by allowing a rapid response to business requirements, while providing a holistic view of the network infrastructure through gathered metrics. A robust security automation enabled by both threat detection tools and policy enforcement mechanism can reduce troubleshooting and operation time, and errors induced by the human intervention.