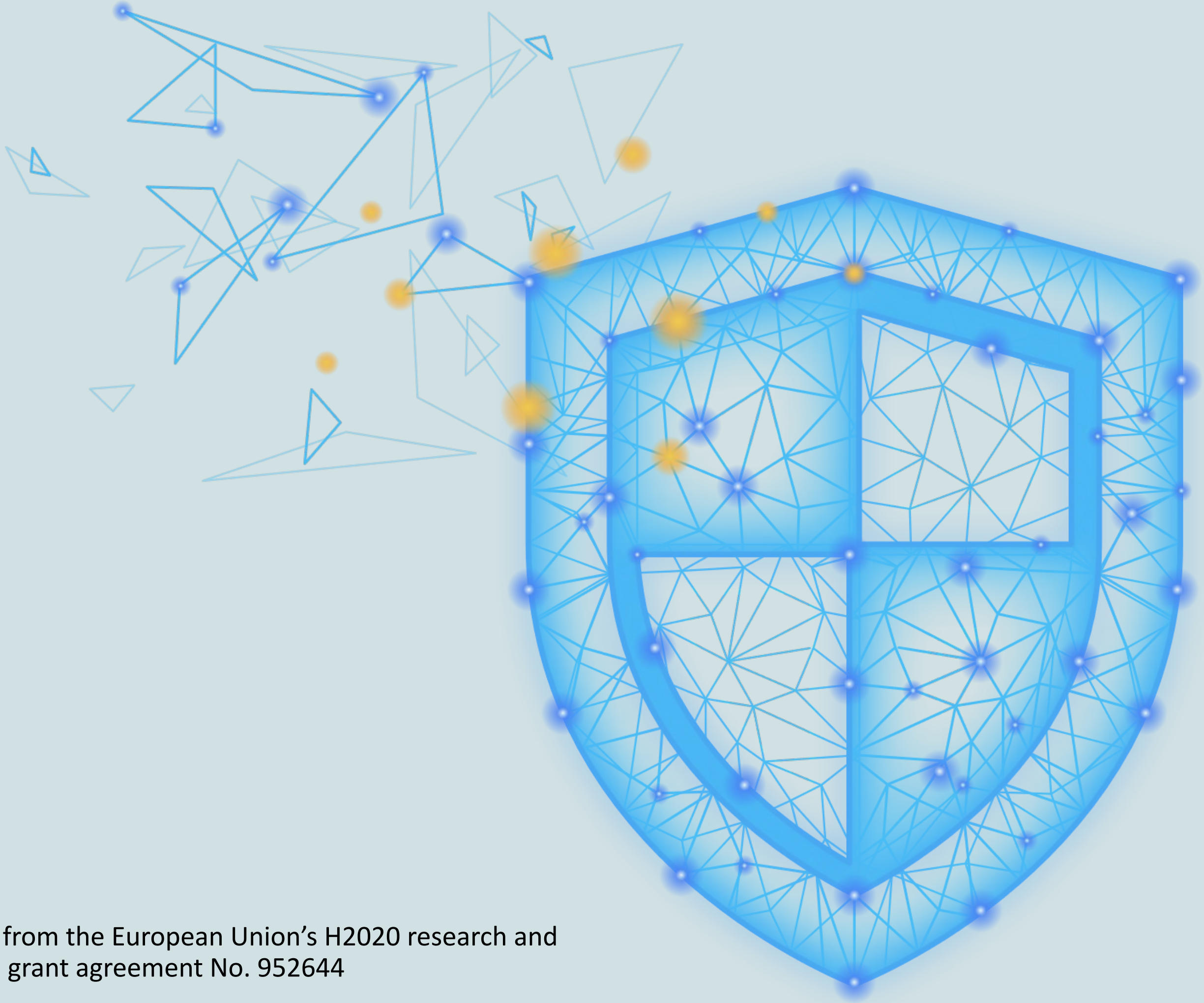
FISHY KERs

KER PITCH DECK



This project has received funding from the European Union's H2020 research and innovation programme under the grant agreement No. 952644

KER 1: FISHY PLATFORM

UNIQUE VALUE PROPOSITION

Platform designed to support the specific needs inherent to the heterogeneous and diverse supply chain scenario also suporting the hybrid model FISHY is envisioned to support.

KER 1: FISHY PLATFORM

SOLUTION BENEFITS

CYBERSEC INFORMATION READINESS

Offers enhanced security and real time monitoring of all elements of IT chain, providing security from blockchain-oriented threats with interledger components

AUTOMATION OF CYBERSEC PIPELINES

Guaranteeing data security in a manufacturing context, ensuring data sharing with external entities and cybersecurity of IoT devices, as well as edge and cloud infrastructures.

FLEXIBLE AND RESOURCEFUL FRAMEWORK

The FISHY framework considers all the supply chain components, from the IoT ecosystem to the infrastructure connecting them, addressing security and privacy functionalities related to risks and vulnerabilities management, accountability, and mitigation strategies as well as security metrics and evidence-based security assurance.

KER 1: FISHY PLATFORM

INNOVATION SCOPE

INNOVATION

Frontend designed to support the specific needs inherent to the heterogeneous and diverse supply chain scenario also supporting the hybrid model FISHY is envisioned to support.

PROBLEM

Different actors use IT systems of different providers and technologies which makes difficult the protection of the whole IT chain. There is no end-to-end solution appropriately addressing the cybersecurity of supply chains.

SOLUTION

Easing FISHY platform usability, making the whole system user-friendly and ready to be used for different users according to their expected profile and thus permitted functionalities

VALUE

Enhanced customer experience: Easy access to the supply chain cybersecurity in a single window with meaningful and useful output

KER 1: FISHY PLATFORM

REFERENCES FROM OUR EARLY ADOPTERS

FARM 2 FORK

The FISHY platform supports the administrators of the IT systems of the three type of actors of the F2F chain to monitor the security of the IoT solution they operate in a flexible and credible way, supporting also blockchain-relevant trust/security management

SMART FACTORIES

The FISHY Platform can centralize the management of users, including different user profiles, and support the system's administrators in their responsibility of monitoring the security of the IoT devices and systems they operate

CONNECTED AUTOMOTIVE

The FISHY Platform is an entry point for users and can centralise certain security aspects of the supply chain of software versions of IoT devices embedded in vehicles, while enabling the management of in-vehicle user identities and facial identities, having appropriate forms for the management of this data

KER 2: TRUST & INCIDENT MANAGER

UNIQUE VALUE PROPOSITION

Improve your monitoring and gathering metrics all across your supply chain infrastructure, performing analysis, raising alerts, proposing mitigation actions

fishy-project.eu @H2020Fishy @FISHY Project @FISHY H2020 zenodo @FISHY H2020 @FISHY-Project

KER 2: TRUST & INCIDENT MANAGER

SOLUTION BENEFITS

CONTINUOUS MONITORING OF INFRASTRUCTURE

An array of both open-source and custom built solutions cast a wide net of detection and assessment, covering a variety of cybersecurity concerns of administrators of IT systems

IMMEDIATE NOTIFICATION OF ANOMALIES

Detected events and generated alerts are not only stored, but immediately propagated through a notification channel, enabling both prompt informing of system administrators and immediate mitigations of other automated systems in the platform.

AUTOMATED RECOMMENDATIONS

Providing automated recommendations to address detected events over mitigating actions

KER 2: TRUST & INCIDENT MANAGER

INNOVATION SCOPE

INNOVATION

Architecture designed for supply chains, instead of single network, storage component with an integrated pub-sub layer, and a ML-based incident detection system.

PROBLEM

The vulnerability assessment spread across several components of different technologies, owned by different parties and with different objectives cannot be done in an individual way but covering all the different aspects and constraints together.

SOLUTION

Monitoring and gathering metrics from supply chain infrastructure, performing analysis, raising alerts, proposing mitigation actions

VALUE

Combination of multiple different tools (vuln. estimation, IDS, SIEM) to provide as large of a coverage of cybersecurity as possible.

FiSHY

KER 2: TRUST & INCIDENT MANAGER

REFERENCES FROM OUR EARLY ADOPTERS

FARM 2 FORK

The Trust and Incident Manager is able to detect diverse types of attacks based on continuous monitoring of specific points/security probes defined by the F2F IT systems' operators which deliver to the TIM information about the current operation (in the format of log files) and define rules based on which incident/threats are detected, triggering notification delivery to the operator/ID administrator (appropriate user) of the FISHY platform

SMART FACTORIES

The component is used to continuously perform vulnerability scans, classify vulnerabilities (risk-based) and send reports to the IRO component. Specifically, TIM will open incidents when an IoT device not registered to FISHY is detected and escalate the level of criticality if the incident is not dealt with

CONNECTED AUTOMOTIVE

The component is used to assess the risk of attacks by analysing the logs that the SADE services will have available. It is expected that the component will collect the logs from one of the enabled services, analyse them and generate a mitigation response which can be via REST API or by passing messages in a specific RabbitMQ queue. Another possible use case is to generate intents in the IRO in such a way that the mitigation policies are acted upon by this component

KER 3: Intent-based Resilience Orchestration

UNIQUE VALUE PROPOSITION

Automation of the interactions between the user defining high level intents and the system applying high level policies

FiSHY

KER 3: Intent-based Resilience Orchestration

SOLUTION BENEFITS

CONFIGURABLE AUTOMATION

Set, modify or delete security policies at scale using high level intent language

TRANSPARENCY AND CONTROL

Using other modules of FISHY to monitor the IT infrastructure, IRO shows notifications and alerts about the network condition, recommand actions, and react based on the situation

SECURITY ENFORCEMENT

Using predefined policies, IRO can react to detected threats automatically or after confirmation from the user, and enforce security rules using other FISHY components

FiSHY

KER 3: Intent-based Resilience Orchestration

INNOVATION SCOPE

INNOVATION

Solution translating high-level intents into configured policies, and interact with the system response using AI techniques, and able to incorporate smart contracts

PROBLEM

The continuous detection of vulnerabilities in production infrastructures and during software development phases, appearing in the infrastructure when new services or features are added, or simply when new vulnerabilities are discovered in existing (outdated) services.

SOLUTION

Automation of the interactions between the user defining high level intents and the system applying high level policies

VALUE

The user does not need to know the intermediate technical steps to perform an intent

fishy-project.eu @H2020Fishy @FISHY Project @FISHY H2020 zenodo @FISHY H2020 @FISHY-Project

FISHY

KER 3: Intent-based Resilience Orchestration

REFERENCES FROM OUR EARLY ADOPTERS

FARM 2 FORK

The IRO offers to the administrators of the F2F IT solutions: a) the capability to register their system and define the rules to be monitored; and b) to receive notifications, alerts and suggestions for actions and security audits of their systems

SMART FACTORIES

This component allows for the registration of systems and devices to FISHY, to be communicated to the EDC and SPI components respectively. It will also, together with the Dashboard, to send notifications, alerts and suggestions for actions and security audits to users according to their profile

CONNECTED AUTOMOTIVE

The use of this component is indirect and allows the generation of policy definitions to be applied by the EDC. The intents are generated by other components based on the analysis and processing of the data obtained from the infrastructure of the SADE use case by these other components

KER 4: Security Assurance & Certification

UNIQUE VALUE PROPOSITION

Auditing and reasoning security metrics tailored to the pilots infrastructure, and collecting certifiable evidence from the pilots infrastructure

KER 4: Security Assurance & Certification

SOLUTION BENEFITS

CUSTOM RULES AUDIT

The custom-based rules are described using a high level language named Event Calculus logic

EVENT COLLECTION ENGINE

Using the Elasticsearch stack as main pool of data collection, connecting with external data pools using message broker AMQTP technologies

SMART RULE MANAGEMENT

The audit component is integrated in Drools rules management system

KER 4: Security Assurance & Certification

INNOVATION SCOPE

INNOVATION

Component architecture tailored to supply chains needs focussing especially to regulatory obligations (e.g., GDPR) and violations/compliance of service level agreements

PROBLEM

The SACM is trying to address the real-time monitoring (in terms of violation or satisfaction) problem of custom-based rules regarding security aspects (including the Confidentiality, Integrity, Availability triangle). Furthermore, it addresses the lack of evidence-based, certifiable view of the security posture of complex ICT systems.

SOLUTION

SACM has 4 main components : The Security Metrics, the auditing component, the evidence-collection engine and the certification component.

VALUE

Easy management of evidence produced by monitoring and assistance with compliance to certification standards, and ensure the truthfulness of the collected data

fishy-project.eu @H2020Fishy @FISHY Project @FISHY H2020 zenodo @FISHY H2020 @FISHY-Project

KER 4: Security Assurance & Certification

EARLY ADOPTERS

FARM 2 FORK

The SACM decides whether the security rules defined by the IT systems' operators have been violated or not in a certain timeframe, and provides details about any incident detected based on this rules as well as about policies that have been enforced as a response to an incident.

SMART FACTORIES

This component can check if the volume of telemetry is lower as the minimum historic and communicates with the Trust Incident Manager to analyze the impacts.

CONNECTED AUTOMOTIVE

This component certifies the software versions installed on each vehicle managed on the FISHY platform, and obtains the installed devices from the vehicles and the list of versions certified as safe by the manufacturer, comparing the version with the listing. When it does not match, the module sends a message to the SADE REST API to control the risk

KER 5: Security & Privacy Dataspace Infrast

UNIQUE VALUE PROPOSITION

Organizing data related to infrastructure events and enforcing privacy and Access Control rules, including Identity Management, by translating high level intents into configured policies, and interacting with the system response using AI techniques

fishy-project.eu @H2020Fishy @FISHY Project @FISHY H2020 zenodo @FISHY H2020 @FISHY-Project

KER 5: Security & Privacy Dataspace Infras

SOLUTION BENEFITS

ACCESS CONTROL

Advanced policy and rules definition and enforcement technology

IDENTITY MANAGEMENT

Identity Management strategy, which is fundamental in a supply chain environment where different users' perspectives and demands must coexist

DATA SANITIZATION AND FLOW CONTROL

Data sanitization and flow control from low-level on-premise components, according to previously defined privacy rules.

KER 5: Security & Privacy Dataspace Infrast

INNOVATION SCOPE

INNOVATION

An enhanced framework for system events' management, including metrics from different sources and promoting co-relation with added semantics, incorporating new pre-processing mechanisms (anonymization, new metadata models…)

PROBLEM

Current information systems development frameworks promote using highly distributed components that better fit the virtualization-based infrastructure and the IoT paradigm. Interconnected components and modules will expose entry points and data (at local or global levels), enlarging the potential surface attack. Missing that goal can expose the system to a high risk of being untrustable and rejected by final users.

SOLUTION

Organizing data related to infrastructure events and enforcing privacy and Access Control rules, including Identity Management

VALUE

Secure data transfer between monitored infrastructure and FISHY platform, with data anonymization

KER 5: Security & Privacy Dataspace Infrast

EARLY ADOPTERS

FARM 2 FORK

This component applies security policies to mitigate risks, attacks or intrusions detected, applying security configurations when a non-compliance situation is detected.

SMART FACTORIES

The module is used to receive from IRO the registration of new IoT devices and keeps an updated list of registered devices

CONNECTED AUTOMOTIVE

This component applies security policies to mitigate risks, attacks or intrusions detected, applying security configurations when a non-compliance situation is detected.

KER 6: Enforcement & Dynamic Config

UNIQUE VALUE PROPOSITION

Component architecture tailored to supply chains needs focussing especially to regulatory obligations (e.g., GDPR) and violations/compliance of service level agreements

FiSHY

KER 6: Enforcement & Dynamic Config

SOLUTION BENEFITS

SUPPORT FOR NEW SECURITY DEVICES

A capability model empowers the core of the EDC, allowing an administrator to add support for new types of security controls with ease. Adding new security devices is performed by describing what they offer (e.g., this device is a stateful firewall, supports traffic rate- limiting) without writing ad-hoc code logic

QUICK & EASY NETWORK DESCRIPTION

The use of a high-level policy language grants the administrators the ability to quickly and easily describe what the network functionalities are in a way closer to the human language, without worrying about their actual implementation, which is demanded to the EDC itself

PHYSICAL AND VIRTUALIZED SECURITY CONTROLS

The EDC seamlessly supports both physical and virtualized security controls and allows the administrators to configure mixed networks containing both types of devices

FiSHY

KER 6: Enforcement & Dynamic Config

INNOVATION SCOPE

INNOVATION

Framework leveraging a capability model instead of the traditional refinement techniques based on logic rules, making use of a highly flexible security capability model and an inferential engine to smartly refine high-level policies into low-level configurations.

PROBLEM

Correctly configuring network devices (particularly security controls) is a critical and, unfortunately, error-prone task, especially regarding the modern SDN-based infrastructures. An administrator must be aware of the entire network topology and the device configuration rules to avoid catastrophic mistakes, while the network size and heterogeneity keeps growing.

SOLUTION

Technology allowing an administrator to effortlessly configure various security controls (e.g., a firewall or a VPN terminator) through high-level declarative policies that are automatically translated into a series of optimal low-level configurations.

VALUE

Adding a new NSF type requires only describing its capabilities using a very simple model. Its innovative refinement process will consider the current network landscape topology and its configurations to avoid inconsistencies and issues in the deployed rules.

KER 6: Enforcement & Dynamic Config

EARLY ADOPTERS

FARM 2 FORK

The EDC decides the banning of specific IPs and blockchain wallet IDs when these are issuing an attack (defined by a predefined rule set by the system operator through the IRO). Other similar policies may be defined based on the specifics of the IT solutions in place.

SMART FACTORIES

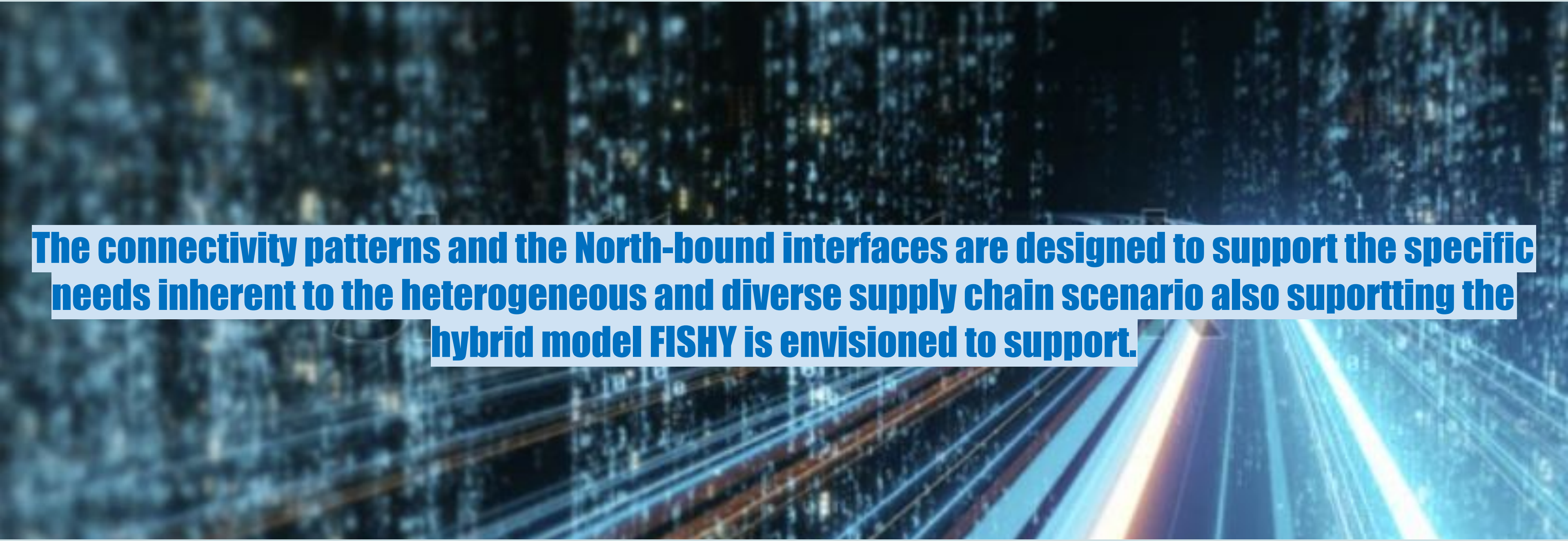
This component implements security policies to mitigate risks, attacks or intrusions detected, applying security configurations when a non-compliance situation is detected.

CONNECTED AUTOMOTIVE

This component is mainly used to apply security policies on the infrastructure to mitigate possible risks, attacks or intrusions detected, providing security configurations when any security policy is not complied with.

KER 7: Secure Infrastructure Abstraction

UNIQUE VALUE PROPOSITION



The connectivity patterns and the North-bound interfaces are designed to support the specific needs inherent to the heterogeneous and diverse supply chain scenario also suportting the hybrid model FISHY is envisioned to support.

KER 7: Secure Infrastructure Abstraction

SOLUTION BENEFITS

NETWORK FUNCTION ORCHESTRATION

OSM-enabled network function orchestration

VIRTUALIZATION ENVIRONMENTS SUPPORT

Able to support virtualization environments based on VMs (OpenStack) and containers (Kubernetes)

SECURE MULTI-DOMAIN CONNECTIVITY

Secure multi-domain connectivity relaying on IPsec

KER 7: Secure Infrastructure Abstraction

INNOVATION SCOPE

INNOVATION

Seamless and transparent base infrastructure management, with multi-domain connectivity and functional orchestration aware of the FISHY framework

PROBLEM

Provide a common interface for the orchestration of the network-based functions used by FISHY, in all its phases (monitoring data collection, threat detection, policy translation and enforcement), including the deployment and management of functions using standard cloud-native interfaces, and multi-domain connectivity management.

SOLUTION

Model-based support for the management of network and computer infrastructure, with seamless support of multi-domain scenarios. SIA is the base for the FISHY Reference Framework (FRF) and sandbox environment.

VALUE

Abstract interface allowing the execution of verification, detection and mitigation actions on different types of underlying infrastructure (IoT, IaaS, baremetal, etc)

KER 7: Secure Infrastructure Abstraction

EARLY ADOPTERS

FARM 2 FORK

SIA is able to be a transceiver of information from cloud-based IT platforms that support IoT and blockchain technologies.

SMART FACTORIES

This component ensures the collection of telemetry from the IoT Hub and of information logs from the WLAN controller to then send them to the TIM, EDC or SACM components.

CONNECTED AUTOMOTIVE

SIA is used as part of the securitisation of services, facial identity management and certified version management in vehicles. Communication are done in a secure way through the NED, allowing restrictions or configurations to be applied if intrusions or risks are detected in the vehicle.

Thank you

Contact:

This project has received funding from the European Union's H2020 research and innovation programme under the grant agreement No. 952644