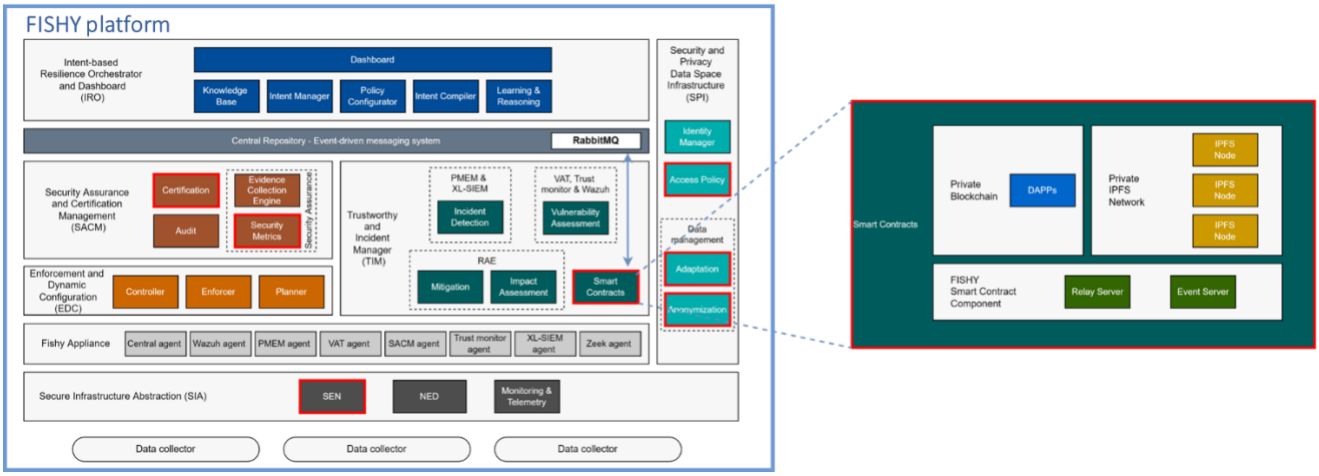
Using blockchain technology to secure security information



FISHY aims at delivering a coordinated cyber resilient platform towards establishing trusted supply chains of ICT systems. FISHY detects security threats and recommends or enforces (depending on the user's preferences and settings) policies and mitigation actions. As FISHY is a digital platform itself, FISHY consortium decided that to maximise the offerings towards our potential customers, the detected events as well as the recommended policies are stored in blockchain. This gives us the opportunity to provide to our customers evidence that any recommendation they received or information about an attack detection is validated by our blockchain, thus avoiding disputes about this security information.

To do this, we have included in our platform architecture shown in the figure, the so call "Smart Contracts" component which is responsible for ensuring the integrity of a) the recorded security events and b) the enforced or recommended mitigation policies. The Smart Contracts component communicates directly with the Central Repository of the FISHY platform (to receive this information) and stores it in the blockchain. The different events/policies along with the relevant information which can be large and thus not appropriate for being stored in blockchain (for example a log file showing the detected anomaly) will be stored in a private IPFS network. We store in the blockchain a) the ID of the security event/policy and b) the corresponding link in the IPFS system.

As shown in the right hand of the figure, the "Smart Contract" component consists of multiple sub-components: IPFS, DAPPs (Decentralized Apps), Relay Server, Event Server. The DAPPs sub-component consists of the Smart Contracts that contain the logic for storing the original source of the data (IPFS link) and retrieving it. The DAPPs component is deployed in a private blockchain network, namely Quorum. This private blockchain network solution uses the IBFT (Istanbul Byzantine Fault Tolerance) consensus mechanism. This mechanism is one of the best regarding performance and transaction speed, therefore making the overall implementation very fast. The IPFS is a P2P (peer-to-peer) distributed file system that is used to store and access any type of data (e.g. files, JSON, jpeg etc.). In FISHY, we use it to store the information that accompanies/describes a security event and a policy. This way, the required time to store the information is reduced, compared to the case where we store information in the blockchain, and allows for larger data sizes. The events/policies become accessible via a link, which is stored in the blockchain. The IPFS guarantees that if any change happens to the source data, it will be detectable.

The addition of the Smart Contracts component to the FISHY platform allows:

- The verification that a security event/policy is detected by FISHY and
- The guarantee that the details of an event/policy are not tampered with (these details are accessed through the link stored in the blockchain).

For more information, visit https://fishy-project.eu/library/deliverables and check D3.3 and D3.4!

Aggelos Orfanoudakis (SYNELIXIS)