IRIS User-centric design and validation of a DLT/Blockchain-based auditing tool for incident response traceability and accountability

João Rodrigues1 , Gonçalo Cadete1 , Duarte M. Nascimento1 , Roland Kromes2, Carmela Occhipinti3, Lorena Volpini3

1. INOV – INESC Inovação 2. Cyber Security Group, Delft University of Technology 3. CyberEthics Lab 1.

Introduction

Incident Response, in the context of disaster management, security and infrastructure protection, implies designing and executing automatic and semi-automatic response workflows. Enabling accountability of related actions is necessary to ensure that the relevant stakeholders operate in a risk-controlled environment. Existing logging solutions for incident response workflows allow for some degree of assurance regarding traceability and accountability, by enabling post-incident analysis of the incident context and operators' actions. In the scope of the IRIS European Union's Horizon 2020 project, a Data Protection and Accountability (DPA) module was designed to support auditing functions for incident response, ensuring accountability and traceability based on a combination of distributed ledger technologies (DLT), blockchain, self-encryption, and secret key sharing technologies. The DPA enables secure, immutable, and resilient distributed logging for incident response workflows, optimized for cooperating networks of CERT/CSIRTs. The DPA solution will be demonstrated and evaluated in two realistic pilots in two European smart cities, featuring scenarios of autonomous transportation vehicles and smart grid infrastructures. To assess the progress beyond the state-of-the-art, societal acceptance and design science research methodologies will be used to elicit and validate the specific operational requirements of incident response stakeholders.

2. Data Protection and Accountability Solution (DPA

The DPA enables the traceable, immutable and safe storage of audit data, with access control policies enforced by several nodes. It leverages the capabilities of the Hyperledger Fabric (HLF) permissioned blockchain to provide an auditing service that respects the societal, ethical, and legal implications of auditing procedures involving multiple organizations. The DPA consists of three sub-modules: the Hyperledger Fabric blockchain; the Crypto-tools; and an off-chain database. Hyperledger Fabric is a private, permissioned blockchain whose architectural flexibility allows the DPA to be adapted to different enterprise architectures. Crypto-tools is the sub-module of the DPA that enriches the HLF network with cryptographic self-encryption and secret key sharing capabilities. Blockchain/DLT technologies such as HLF present performance challenges for constant storage of data, or storage of large amounts of data. Therefore, encrypted audit data is stored in a scalable off-chain database, mitigating the risk of the DPA becoming a performance bottleneck.

3. Conclusion

An effective accounting and traceability solution for incident response is crucial for enabling post-incident analysis of the incident's context and operators' actions. The DPA is an auditing solution designed for the aforementioned purpose. A user-centric approach, that considers

aspects of societal acceptance as well as the best practices of user-centric design, is essential to maximize the solution value and the exploitation potential in future operational deployments. From a social values standpoint, the DPA directly contributes at promoting accountability in automated and semi-automated incident response, by ensuring and furthering the core properties of information security (confidentiality, integrity, availability, authenticity, and non-repudiation). Although the desirability of promoting accountability in settings where high responsibilities are at stake may appear as prevailing and self-evident, from a user-centric perspective, value tensions may affect social acceptance (e.g., accountability-independence). Such an approach makes it possible to consider scenarios in which the accountability pressure may produce changes in users' behavior which are relevant to security - the non-repudiation property ensured by the DPA may inhibit actions which are riskier from the point of view of potential individual responsibility but that are more effective responses to threats. Furthermore, when adopting a socio-technical system perspective, the chance of exploring broader social implications may arise (e.g., changes in collective perceptions of avoidability, individual responsibility).

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 101021727. This article reflects only the authors' views and the Research Executive Agency and the European Commission are not responsible for any use that may be made of the information it contains.