Master Thesis

Attacking Blockchain-Based Business Processes

The state of the art in blockchain-based business process execution encompasses the automatic generation of smart contracts from business process models. Various tools implementing this approach exist [1]. This aims at reducing the complexity and reducing security risks by generating secure code patterns. However, the security of these approaches has never been formally proven (tools focusing on model-checking these approaches exist [2]) nor empirically studied. In this topic, we aim to survey common smart contract attack scenarios and use them to attack blockchain-based business process tools. We aim to evaluate the attacks feasibility, impact, and efficiency. Beyond this, we ask if attacks specific to process execution exist.

Contact

Every theses starts with an exposé, where you shape the topic towards your interest (in consultation with us). If you’re interested, please contact us as outlined at https://www.cs.cit.tum.de/en/isdo/teaching/theses/.

Recommended Prerequisites

Familiarity with blockchain technology, foundations in IT security, industrious interest in exposing security holes.
