TRIDEnT: Trustworthy collaboraRative Intrusion DETection

N. Alexopoulos, E. Vasilomanolakis, N. R. Ivánkó, T. Frieß, M. Mühlhäuser

Introduction

Cyber attacks and Intrusion Detection
- Cyber attacks are increasing in terms of numbers and sophistication
- Intrusion Detection Systems (IDSs) are nowadays considered mandatory
- However, isolated IDSs cannot provide strong detection accuracy and do not scale to large-scale networks

Collaborative Intrusion Detection Systems (CIDSs)
- CIDSs overcome these shortcomings by employing a synergetic network of multiple IDSs
- CIDSs create a holistic view of the monitored network
- Trust between collaborators is a vital, yet challenging issue

Motivation & Background

Motivation
- A CIDS infrastructure needs to be robust, accountable and resilient to internal attacks
- Existing approaches, based e.g. on Computational Trust, offer only a partial solution to the problem
- Blockchain technology can offer a secure-by-design platform

Background
- Blockchain technology offers a distributed ledger among peers
- The security guarantees of the ledger stem from the consensus protocol in use
- Blockchains can be classified as public or consortium:
  - in public blockchains membership is uncontrolled,
  - in consortium ones a pre-defined subset of peers is in charge of the process

TRIDEnT’s Architecture

General Idea:
- Use a blockchain as the collaborative mechanism
- Break down communication into two layers:
  - Alert exchange: on-demand data dissemination
  - Consensus: create global view of peer actions
- Store compact representations of alert data on the blockchain

Advantages:
- Public verifiability
- Accountability
- Data Integrity
- Resilience

Design Considerations

Blockchain governance:
- Public (e.g. Bitcoin or Ethereum) vs. Consortium (e.g. Hyperledger)
- Does open participation offer advantages?

Consensus algorithm:
- Proof of Work vs Proof of Stake vs PBFT etc.

Data on/off the ledger:
- Raw alerts vs compact representations (e.g. Bloom filters)

Data encryption – Privacy:
- Encrypted vs Plaintext alert data exchange

Next Steps

Future Work
- Proof of concept implementation of TRIDEnT using Hyperledger Fabric
- Include computational trust techniques in the architecture
- Experiment with various design alternatives

Related Publications