GNU Taler Real-Time Auditor

Degree programme: BSc in Computer Science
Thesis advisors: Prof. Dr. Emmanuel Benoist, Prof. Dr. Christian Grothoff
Expert: Han Van der Kleij

The GNU Taler auditor was improved, and now works in real-time. To achieve this, six helper programs responsible for analysing different parts of a GNU Taler Exchange were adapted. Additionally, a single page application was created, which shows auditing results as soon as they are detected.

Introduction

GNU Taler provides a way to pay digitally and anonymously. This means, that any purchases customers make with GNU Taler cannot be traced back to them. GNU Taler is neither a blockchain, nor based on some decentralised ledger; instead, it uses a concept called blind signatures to provide privacy to payers.

Motivation

Conscientious and thorough auditing is vital for any serious payment system and the assumption it's useless or unnecessary is beyond naive and will inevitably lead to disaster. Cases like the Wirecard fraud make it clear that there is a real need for automated systems to verify the integrity of payment services. This is exactly what a GNU Taler auditor does.

Architecture

The auditor's responsibility is monitoring and auditing the operation of a GNU Taler exchange, by verifying signatures, computing balances and properties. Its logic is split into six programs, referred to as helpers, that run on a job scheduler. The auditor works in real-time, and its results are made available through a website for easy monitoring. The auditor can detect a variety of misbehaviours, both from customers or merchants and from exchanges themselves.

Inconsistencies that the GNU Taler auditor can detect include, but are not limited to:

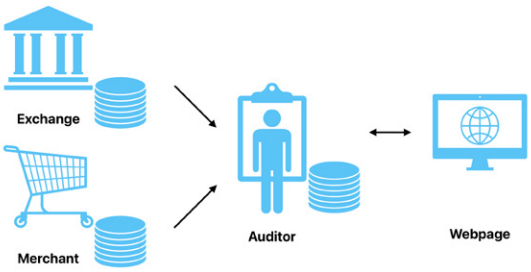
- double spending attempts
- money printing
- invalid wire transfers
- internal system failures
- and many more...

Enabling the real-time functionality are PostgreSQL triggers, which fire as soon as new data is added to the exchange. Event handlers listen to those triggers and kick the helpers into action. Every helper has its own unique trigger, meaning only the helpers that actually analyse the new data are woken up, while the others keep sleeping.

Monitoring

While it's true that the auditor detects any suspicious behaviour in real-time, all that data is stored in its own PostgreSQL database, which is not particularly insightful for humans. To remedy this, a webpage was built that continuously fetches new results from the auditors database and displays them in an easily digestible way. It groups all inconsistencies and suspicious findings, and has indicators for different severity levels.

With this webpage, operators or regulators of a GNU Taler exchange can react swiftly in case of a serious inconsistency and thus minimise the potential for financial loss. Also, the auditor's database may be accessed via a RESTful API, which makes it easy to integrate it into existing monitoring infrastructure.



The flow of data between different actors

Nicola Sacha Eigel
IT Security

Cédric Vincenz Zwahlen
IT Security