Verifiable Labels - A Decentralised Website Reputation System

Degree programme: Master of Science in Engineering
Specialisation: Computer Science
Thesis advisor: Prof. Dr. Annett Laube
Expert: Prof. Dr. Ulrich Ultes-Nitsche

Phishing attacks exploit weaknesses in digital identity systems, exposing users to fraud despite measures like costly TLS certificates. The Verifiable Labels (VL) system addresses this by introducing a cryptographic reputation system that logs participating website's behavior on a distributed ledger, empowering users to assess credibility. This thesis develops a decentralized VL prototype, an Ethereum smart contract, Python library, and user clients to enhance online trust.

Problematic

Phishing attacks have become prevalent in our day and age. By playing a game of disguise and impersonating trustworthy companies in the hopes of obtaining their users' login credentials, these attacks take advantage of the lack of stark identities in communication systems. The Internet is one of the most targeted communication systems, where each webpage seeks to guide its users through corporate designs or digital certificates—the primary touch-points for non-technical users. Many organizations invest in costly Transport Layer Security (TLS) certificates with Extended Validation (EV) to safeguard their identity and earn user trust. However, the Certificate Authority (CA) system and the Domain Name System (DNS) have increasingly proven inadequate and outdated for establishing true authenticity. These systems fail to prevent malicious actors from imitating legitimate websites, exposing the entire Internet infrastructure to a plethora of attacks.

Concept

To address this, the Verifiable Labels (VL) system draws inspiration from real-world labeling practices to fortify digital identities. It focuses on websites that demand user trust, such as those requesting payment or sensitive information. The VL system introduces a cryptographic reputation mechanism, requiring self-declared labeling entities to publicly log their behavior in a distributed ledger, forming an immutable chain of cryptographic events. This empowers users to independently assess the credibility of websites and make informed trust decisions. Additionally, it offers security businesses a powerful tool for identifying high-risk websites and take action against phishing threats faster.

Outcome

This Master's thesis presents the theoretical foundation and practical realization of the Verifiable Labels system in a decentralized infrastructure, including the development of a minimal viable prototype that meets all cryptographic requirements. The prototype features an Ethereum smart contract, a Python library enabling seamless integration of Verifiable Labels into software, and three user clients tailored to different use cases. The entire code base is rigorously unit tested, ensuring reliability and adherence to expected behavior. Together, these components demonstrate the potential of VL as a new approach to restoring trust in online interactions.

Maël Gassmann
mael@gassm.ch