Signet-ring: A Framework for Authenticating Sources and Lineages of Digital Objects

Mahesh Arumugam[*], Catherine Jimerson, Diamond Rorie,
Amangeet Samra, Amrita Mande, Daniel Aranki

School of Information
UC Berkeley

Abstract

Verifying sources of information is vital in assessing the credibility of facts and data in our increasingly digital world; often, the verification of the sources is as necessary as the information they provide. To battle misinformation and disinformation through digital objects, it is salient to provide consumers the ability to verify whether or not information (or data) provided by such sources was altered prior to its use (e.g., publication). Furthermore, if such an object is altered, it would also be essential to provide a means to trace back such information throughout its editing lineage in a verifiable manner. This research aims to fill the gaps in verifiable proof of sources of information, software supply-chain, and objects in other similarly critical domains.

We propose Signet-ring, a framework that provides referenceable documentation of the relationship between a digital object and its sources. In addition, the framework documents the object's lifetime as it goes through various edits (lineage), including those by others within the framework. As such, Signet-ring provides a verifiable means for anyone to authenticate the sources of any digital object registered to it and track the object's progression in time. This framework can be used, for example, by journalists and publishers to verify the sources of their materials (e.g., videos or images) and provide this proof to their readers for their verification. This, in turn, introduces a new layer of trust to the public in the reporting they consume.

Another noteworthy use case for Signet-ring is aiding the assurance process in software supply chains. The various stages and components of software can be certified using Signet-ring to provide verifiable checkpoints of revisions that pass assurance guarantees. For example, consider a program or a change-list (e.g., a pull request) that one person authentically creates and registers within Signet-ring. Suppose this code becomes visible, and any third-party modifications (not authenticated by the framework) are available. Then, only the change within the framework will have a traceable relationship to the source and its lineage. Thus, the framework enables various stakeholders to verify the relationship between sources and software objects, including changes made to revisions of software with certified assurances.

In this presentation, we present the architecture of the Signet-ring. Signet-ring registers and authenticates all participants in the origination and publication process, potentially including the sources, publishers, and applications. It manages the following critical workflows: (1) documentation and verification of the relationships between objects and sources (certification), (2) documentation and verification of the relationships between different related objects (lineage), and (3) authentication of sources to each other (handshake). Furthermore, Signet-ring supports the lifecycle management of source identities (using cryptographic keys) and relationships between objects and sources. This lifecycle management includes the revocation of source identity keys and previously accepted object-source relationships.

[*] Corresponding author: `aumahesh@berkeley.edu`.