SPROV 2.0: A Highly-Configurable Platform-Independent Library for Secure Provenance

Ragib Hasan*, Radu Sion†, Marianne Winslett‡
*University of Illinois at Urbana-Champaign, †Stony Brook University, ‡Johns Hopkins University

Will you spend $101 million to buy a fake painting?
Obviously, No! Buyers look for provenance, i.e. records of the paintings ownership, exhibition, and sales history. A painting without secure provenance is deemed fake.

Problem Definition: How to make digital history trustworthy?

Approach: Make data provenance tamper-evident.

Provenance: from Latin provenire = ‘come from’, defined as “(i) the fact of coming from some particular source or quarter; origin, derivation. (ii) the history or pedigree of a work of art, manuscript, rare book, etc.; a record of the ultimate derivation and passage of an item through its various owners” (Oxford English Dictionary)

In other words, Who owned it, what was done to it, how was it transferred ...

So, we need provenance of provenance, i.e. a model for Secure Provenance with Confidentiality, Integrity, and Privacy guarantees.

Solution

SPROV 2.0 Architecture

The Goals: Design a highly configurable architecture for providing secure provenance functionality to existing systems.

Approach: Divide functionality into plugins for cryptographic operations and storage management.

How SPROV 2 Works
1. Provenance system (e.g. PASS) creates a new provenance record, and hands off the data to SPROV2
2. SPROV2 applies crypto-plugins to create checksums and encrypt the record
3. Storage method plugins handle chain storage / IO

Cryptographic Plugins:
- Linear provenance chains
- Spiral provenance chains
- Co-provenance chains
- Encryption

Storage Plugins:
- Berkeley DB storage
- Local file storage
- Cloud storage

Status:
- Under development
- To be deployed with PASS

For further details http://dais.cs.uiuc.edu/provenance and http://tinyurl.com/secprov