**Motivation**

Corporate abuses by Enron and WorldCom have given rise to recent regulations which require many corporations to ensure trustworthy long-term retention of their routine business documents.

- Sarbanes-Oxley Act (2002)

Due to widespread news coverage of collusion between auditors and the companies they audit, and a lack of tools to address such corruption, there has been interest within the file systems and database communities in built-in mechanisms to detect or even prevent tampering.

**Information Accountability** has been important since ancient times.

Information accountability mirrors the relationship between the law and human behavior more closely.

**Compliant records** are those required by law to follow certain “processes by which they are created, stored, accessed, maintained, and retained.” It is common to use Write-Once-Read-Many (WORM) storage devices to preserve such records.

**Information Accountability vs Restriction**

Information restriction entails rendering retained records immutable and controlling access to them. This approach appears to be the prevailing viewpoint for achieving privacy and security.

Information accountability assumes that information should be transparent so as to easily determine whether a particular use is appropriate under a given set of rules.

**Objectives**

**Dragoon: Database Forensic Analysis safeguard Of arizOnA**

**Dragoon** is a prototype continuous assurance auditing system that is highly customizable in terms of offering a tunable trade-off between level of security and forensic cost. A beta version of **Dragoon** is available at [http://www.cs.arizona.edu/projects/cas/dragoon/](http://www.cs.arizona.edu/projects/cas/dragoon/). It is lightweight, scalable, and adequately addresses aspects of information accountability.

**Dragoon** can effectively realize appropriate use (i.e., guarantees no unauthorized modifications—insertions, deletions, updates) in high-performance databases. It protects against a variety of threats (including master-thieves) via tamper detection and forensic analysis algorithms. **Dragoon** can also successfully deal with the aftermath of information restriction failures thereby rendering complex security problems tractable.

**Dragoon** is a valuable information accountability solution in the particular area of correct storage, use, and maintenance of relational databases.

---

**Dragoon: An Information Accountability System for High-Performance Databases**

Kyriacos E Pavlou and Richard T Snodgrass
The University of Arizona Department of Computer Science

**Reference Architecture**

The Total Chain Computation Phase

Figure 2 shows the reference architecture of **Dragoon** with the colored arrows showing behavior of information during the Total Chain Computation phase. All records of the monitored database are hashed and the resulting crypto-strong hash value is periodically noted. The hash value and the returned unique notary ID are stored in a secure database called DragoonDB.

**Forensic Analysis Algorithms**

**Corruption Diagrams**

**Taxonomy of Corruption Types**

**Contributions**

The **Dragoon** prototype system with advanced tamper detection capabilities and forensic analysis tools is useful in a variety of sectors. **Dragoon** can:

- ensure record compliance for financial and medical institutions,
- serve as an unbiased witness to databases storing sensitive information, e.g., court-submitted data from police databases,
- ensure non-deviation from standard operating procedures in biosciences labs (provenance of results),
- detect bugs silently corrupting databases,
- can be deployed in the cloud (vid. DMC’12)

- automate some of the forensic work required in the aftermath of a database corruption saving both time and money,
- provide advantages over information restriction approaches which rely on special hardware (prohibitive costs for small institutions, limited shelf-life, relatively complex), and
- mirror the relationship between the law and human behavior more closely.

**References**


