In Database We Trust?

Lance Feagan
IBM China Research Lab
399 Keyuan Road, Shanghai, China
feaganlw@cn.ibm.com

The Problem

Traditionally, cyber intruders have sought to either exfiltrate proprietary information for financial gain or destroy data to create disruption. Large-scale data exfiltration is difficult because network administrators actively monitor and restrict the content and destination of outbound network flows. And, while an attack that destroys data may be disruptive in the short-term, the loss of data is readily detected and resolved by restoring from backups. As the concept of total warfare between nation states has emerged, the long-term objective of distorting adversaries' perception has become an attractive attack. A data manipulation attack is attractive because it is difficult to detect, especially if the alterations are subtle, and yet the impact can be significant. For example, by altering the economic output indicators of a nation or corporation, an attacker can manipulate interest rates and stock prices to their financial gain and others' losses, potentially destabilizing a nation. By altering data in the systems of reference an organization relies on, an attacker can alter the perception and understanding of the world of both the victim and those who depend on information and policy disseminated from that organization.

The Idea

To combat this threat, a new class of systems that can provide assurances on the origin, integrity, and authenticity of information must be created. Ultimately, a comprehensive, end-to-end information flow, involving source management systems, compilers, operating systems, processors, and applications must be developed. As the initial step, we should create a distributed database, in essence a ledger of events, that ensures the following properties:

1. The origin, integrity, and authenticity of all data transferred between a client and a server can be verified,
2. The origin, integrity, and authenticity of every database transformation can be verified by any client,
3. The entire content and history of the database can be verified by any client to be free from alteration.

Next generation database systems should eschew reliance on a central authority for access control and privilege enforcement and instead rely on cryptographic methods. Distributed consensus should be preferred to a single arbiter when determining the content and ordering of events. Blockchain systems have begun work in this direction, but are far from being usable as an operational database. Significant performance and security challenges have yet to be through explored.

In addition to querying the current values, these new systems should support efficient point-in-time queries of historical values as well as the predecessor transactions leading to the current value (lineage). We need to consider how to support both process-oriented (coarse grained) and data-oriented (fine grained) provenance subject. This will enable us to use provenance to assess data quality, serves as an audit trail, enables reproducibility, and allows us to attribute changes accurately. Graph database-like links between transactions over time are one approach that could enable us to efficiently traverse lineage while applying filters at each node. This is useful for answering provenance-like queries used during transaction processing, such as determining the potential for fraud of the current transaction by analyzing previous transactions for amounts, location, and participants, sometimes branching out and following other types of links in the graph of historical transaction relationships.

The Disruption

As the frequency and scale of attacks by advanced persistent threats escalates, every organization, from corporations moving to the cloud to national defense and security organizations, will eventually be infiltrated. Current systems of record do not provide assurances on the origin, integrity, and authenticity of all data that can be verified by any client. The novel systems of record that address this challenge, therefore, will represent both a technological disruption and a new-market disruption. Eventually, the market for untrusted databases will disappear as a result of this technology. The question is “After you realize that you are under attack, how confident are you that the data you have is correct?” If the attack has gone on for an extended period of time, which most current do, all of your backups may contain the same altered data and therefore are useless.

Final Thoughts

The viability of the world's current security posture in the cloud is predicated on the ability to recover after an attack has taken place. Successful recovery depends on the ability to discern actions that have occurred on the system that are legitimate from those that are illegitimate. Current systems of record do not possess the necessary trusted computing capabilities to ensure discernment of the legitimate from the illegitimate. In a world with an ever growing pool of capable, advanced persistent threats, only the naive will continue to trust their existing systems of record to provide them with accurate information. Truly, the digital world we have created is not built upon bedrock. For decades, we have built upon sand because it was expedient and we were ignorant. The tide is rising and we can no longer afford to ignore it.

8th Biennial Conference on Innovative Data Systems Research (CIDR ’17) January 8-11, 2017, Asilomar, California, USA.