Rebuilding Trust Across the Enterprise

Jonathan Moore and Matthew Erickson
SpiderOak, Inc.

Insider Threats

Insider threats are one of the primary threats to the mission today. Current IT systems make it difficult to impossible to fully reconcile organizational security policy with full technical enforcement. System administrators, software and cloud vendors, and others have de facto access to information they don't have a need-to-know.

This leads to a large and costly set of mitigations across the enterprise, from increased auditing and compliance measures to two-man-rule administrative systems, physical duplication, and compartmentalization of IT resources. Even with all this time, money, and effort spent, malicious actors with privileged access still can find ways to abuse the system. Additionally, the cumbersome nature of more secure options such as virtual or physical duplication of resources slows down execution speed. When IT cannot keep up with mission needs due to the level of security the mission requires, it is effectively as damaging as a Denial-of-Service attack from an external threat.

Increase Speed and Rebuild Trust

One can model security as a stack of five elements: authority, identity, confidentiality, integrity, and availability (Figure 1). **Authority**, on the top of the stack, is the ultimate goal—authority manages the rules and roles governing access to information. To achieve this, one needs to reason about the roles applied to users (**identity**), keep information safe from unauthorized users (**confidentiality**), ensure the information or the rules governing it is not tampered with (**integrity**), and finally that the information simply remains in existence and accessible (**availability**).

Figure 1

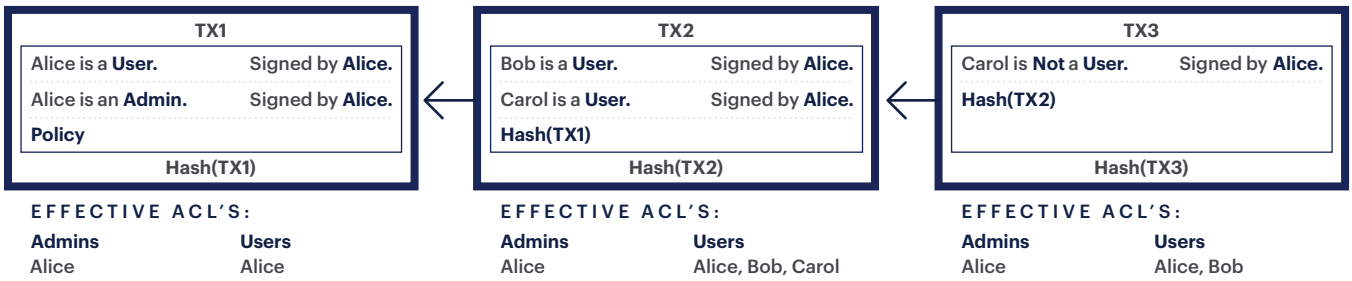
Traditional systems assign IT infrastructure the task of maintaining the whole security system, and the news is rife with evidence it is not keeping up to modern demands.

What if we made availability the sole requirement from IT infrastructure? Using distributed ledger technology (DLT, otherwise known as blockchain), we can ensure that real-world authority within the software and network environment aligns with the organizational security policy. This is known as SpiderOak's Trusted Application Platform (TAP).

Increase Speed and Rebuild Trust, continued

Each modification to the authority of the system is represented as a transaction that cryptographically links to the previous modification (Figure 2). These transactions are then transmitted to all the members of the group and independently verified through a flexible and programmable policy engine. Trying to modify the state of the authority within the system by submitting incorrect transactions or trying to alter already-committed transactions will cause the endpoints to reject the transactions. This keeps malicious actors from modifying the authority within the system even if they have full control over the infrastructure.

Figure 2



Another advantage of the TAP is the ease of key management. Each group defined by a distributed ledger has assured agreement on who are supposed to be in the group. In TAP, user identities are public keys. When we leverage the fact that all members of the group are in cryptographic agreement on the public keys for everyone in the group, it becomes relatively trivial for the members of the group to negotiate a shared key to secure the data shared between them, keeping data safe from prying eyes even if stored on untrusted infrastructure.

The SpiderOak Solution: Trusted Application Platform (TAP)

SpiderOak provides a prebuilt platform for leveraging DLT to manage authority over information. Instead of worrying about keys and blockchain transactions, developers using our system have only to reason about managing users and sending messages within spaces (i.e. Compartments). All key negotiation and distributed network transactions happens under the hood.

TAP provides easy horizontal scalability within an organization; DLT-defined groups are computationally inexpensive and easy to configure. Instead of clients having to keep track of a small number of large, unwieldy ledgers, the usual workflow is many small, simple ledgers that are easy to replicate across devices. Endpoints only receive traffic from the groups they are a part of, preventing an unnecessary "firehose" of all the data flowing through a large organization.

The DLT endpoint client scales from small embedded ARM/Linux devices to supporting large servers. We can bring secure message passing and file storage to wherever your devices are located.

SpiderOak Share, the initial TAP application, is an easy to use file sharing application enabling group collaboration on files and documents across a team, an organization, or the world. It leverages the capabilities of our platform to ensure that the only people who can see data within a compartment are the users invited into the compartment.

Learn More

To learn more about how SpiderOak can provide your organization with a vastly improved security posture, please let us know.

Matthew Erickson, Director of
Client Services and Technology
SpiderOak Inc.
matt@spideroak-inc.com
o +1 (866) 432 9888 x703
m +1 (202) 244 8729