Distributed Authority for Secure Compartmentalization of Data

Jonathan Moore and Matthew Erickson
SpiderOak, Inc.

Common Methods for Compartmentalization

Compartmentalization of data has long been used as means to mitigate both insider and external threats. By segmenting access, services and even networks the goal is to reduce the scope of a compromise to a limited set of data. Traditional approaches, however, continue to have significant weaknesses and operational downsides that prevent them from being completely sufficient given the sophistication of today's adversaries and motivated insiders.

The most common approach to segmenting access to data is to employ an Access Control List (ACL) where the authority granted to individual users is centrally managed. An ACL approach has a number of weaknesses:

1. Due to their level of privilege, an administrator account can be used as a single point of failure. Either as the target of an attack by an adversary or via the abuse of an insider a compromised administrator account can defeat some or all of the protections an ACL provides.
2. Defects in the software used to implement the ACL or in the underlying operating system can allow an attacker to circumvent the protections of an ACL.
3. A compromise of the management system at a high enough level of privilege will allow an attacker access to all "compartments" of data.

Virtualization is another common approach to the same challenge. It solves some of the problems inherent with ACLs by providing an added layer of separation, but it is not without its own downsides, including:

1. Virtualization introduces complexity and administrative overhead. This generally translates to reduced mission speed and higher costs.
2. Virtualized systems still have multiple single points of failure. For example, multiple virtual machines on a single host can be impacted by a virtualization breakout attack. Similarly, a compromise of the virtualization host results in a compromise of all guest virtual machines.
3. Hardware vulnerabilities such as Spectre and Meltdown can be used by an adversary to defeat attempts to compartmentalize access to data.

Securing the world's data.

SpiderOak.com
⟶

Common Methods for Compartmentalization, continued

Another method of compartmentalization of data is to use enclaved networks, data centers and/or physical space.

1. Physical separation, while strengthening defense by eliminating shared hardware or software, creates significant barriers to information sharing and collaboration.

2. The complete separation of networks and data centers also comes at a very high price, which makes it impractical in many scenarios.

3. The time required to establish new physical infrastructure for a mission may make it impossible to fulfill IT needs within a mission timeframe.

In all these scenarios, system administrators remain threats. Existing solutions to this problem include requiring two or more administrators for any action (known as “no-lone-zones”), limiting access of admins to computer terminals, or simply ignoring the problem outright. None of these are suitable solutions and exfiltration of sensitive data remains an ongoing problem.

The Distributed Ledger Model

In contrast to these existing methods, a distributed ledger approach can provide compartmentalization of data that does not suffer from a single point of failure and is both fast and cost-effective. Compartments are defined using an irrefutable distributed ledger, enabling complete confidence in who is allowed to participate. Once the list of allowed users is defined, it becomes easy for those parties to negotiate shared encryption keys to secure the data being collaborated on.

Our approach allows for the instant provisioning of cryptographically secure collaboration spaces for use in scenarios where certainty about who has access to that space is a mission requirement. Cryptographic segmentation based on secure private blockchain technology, utilizing FIPS 140-2 encryption, is used to enforce strong assurances of confidentiality, integrity, immutability, and authority.

Software-based collaboration spaces created with this approach are:

1. Fast to deploy and user-friendly, increasing mission speed;

2. Inexpensive compared with virtualization and physical separation;

3. More effective as they rely on a distributed authority model to enforce ‘need to know access’ to compartments; and

4. Not impacted by compromises in the underlying infrastructure (networks, server and I/T staff).

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
м +1 (202) 244 8729