Distributed Authority for Key Management

Jonathan Moore and Matthew Erickson
SpiderOak, Inc.

The Public Key Infrastructure (PKI)

Certificates have formed the basis for network-based identity, authentication, and authorization for decades, initially as small, local office deployments and then expanding to encompass the entire Internet today. The traditional architecture for managing certificates has been X.509's PKI, but that is no longer sufficient in our modern, adversarial world.

In conventional PKI, there is a well-defined system for signing certificates which creates a chain of authority and trust. However, certificate distribution is out of scope for the PKI trust model and is usually performed only during the specific transaction when the need for secure communications arises. It is this on-demand property that causes most of the problems with the PKI security architecture. Specifically:

1. When receiving a certificate, it is hard to know if one is getting the same certificate as everyone else. **An adversary can send an incorrectly issued certificate as part of their attack.**

2. Even if there is a valid trust chain, it is hard to know if it is the intended trust chain. **An attacker can create a valid certificate simply by exploiting the most poorly protected authority in a valid chain-of-trust.**

3. By default, failure to connect to a revocation server typically does not result in a failed certificate validation, which is not the desired reaction to a potential attack. **An attacker can use revoked certificates by blocking communication to revocation servers.**

4. There is no clear audit trail for issued certificates. **It is difficult to detect a certificate that was improperly issued.**

These issues allow attackers to subvert the security of conventional PKI. The architecture relies on over 650 independent authorities that have "because I say so" authority over the validity of certificates with a weak to non-existent revocation model. Any authority can issue certificates representing any subject with zero oversight. Many of these authorities are foreign national governments and are known for inadequate or questionable validation of certificate recipients.

The Distributed Ledger Model

By contrast, in a distributed ledger-based approach, key distribution is a foundational building block of the authority model with authority determined ahead-of-time and not at the time of transaction. All valid signatures and revocations concerning a certificate are published to the ledger, eliminating the issues outlined above with the current model.

Our proven approach can provide the distributed-ledger key management infrastructure required to better protect digital identities and the chains-of-trust they are based on. Our platform manages PKI on blockchains which act as directories per organizational group or team. This approach ties authorization and keys together, removing the need for often-mishandled traditional certificate chains. To fraudulently use a malicious certificate, an adversary would need to insert it into the blockchain, which is protected by a policy-engine and strong cryptography.

Revocation in the blockchain model is vastly simpler than in the traditional PKI approach. Instead of providing yet another potentially compromised source of trust for clients to validate just-in-time, revocation events are inserted directly onto the chain and replicated throughout the distributed ledger. This makes it impossible for clients to miss crucial revocation updates and inadvertently accept invalid certificates. On our platform, revocation also triggers a key rotation event, ensuring that access to cyphertext is also revoked.

In addition to confidentially handling keys within each directory, our platform enables sharing identities across directories. This provides a way to transfer trust in an individual from team to team. Our system scales up to fit organizations with an unlimited number of users, as well as scales out to enable widely-ranging collaborative efforts between any number of organizations.

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