Title: TACK
Emerging Technology Space: Key pinning
Author: Trevor Perrin

"Key pinning" has proven its worth in recent years: Chrome's preloaded pins have detected multiple CA failures, and are being transformed via HPKP into a flexible system for pin assertion and discovery.

Chrome/HPKP key pinning requires a site to declare a set of "pinned" public keys. When visiting that site, browsers will only proceed if the validated certificate chain contains a pinned key (either as a CA key or the TLS key). A typical site might pin keys for one or two CAs and a TLS key.

TACK is a proposal to expand the key pinning arsenal by allowing pinning to a self-chosen signing key. This key provides signatures on the site's TLS key. A TACK signature can be delivered in the TLS handshake, but is separate from the site's certificate chain.

This has several benefits:

First, pinning is decoupled from CAs: A site can achieve flexible pins and easy TLS key changes based on an offline signing key. Sites thus avoid CA lock-in and exposure to CA failures.

Second, pinning is decoupled from certificate chains: Browsers have substantial latitude in constructing chains for a given cert, so CA pinning requires great care to avoid "under-pinning" (denial of service) or "over-pinning" (unnecessary attack surface). TACK ignores the cert chain (except for the TLS key), so is unaffected by these complications, and remains secure even if chain validation has security flaws.

Third, TACK has mechanisms to enhance the security and safety of pinning, including support for distributed backup and delegation of signing keys, and procedures for handling key rollover, key compromise, and key loss events.

In sum, TACK provides the "layer of indirection" benefits of pinning CA keys but uses simpler mechanisms optimized specifically for pinning, thus achieving greater flexibility, safety, and security.