DELL CONTROLVAULT™

LOCKING DOWN YOUR USERS' CREDENTIALS

In a sense, controlling access to your PCs and critical data is like locking your front door to deter an intruder. How strong is the lock? Is your key kept secure or simply hidden under the welcome mat? From a hacker's perspective, user credentials are either well secured or they aren't, and you can't afford any middle ground. That's why we offer Dell™ ControlVault™, a unique hardware-based security solution that provides a hardened and secure bank for storing and processing user credentials. ControlVault keeps passwords, biometric templates, and security codes within firmware and locked away from a malicious application attack.

ISOLATING SECURITY OPERATIONS

Dell ControlVault helps protect secure operations by isolating them from the Windows® environment and memory, which is notoriously unsecure. Instead, all processing and storage of critical data takes place on a processing and memory chip — providing a protective and secure boundary. This isolation removes the processing and storage of identity and biometric information away from unsecured operating systems and physical hard drives.

DELL CONTROLVAULT TECHNICAL FUNCTIONS

Securing Encryption Keys

Most applications using encryption will store keys on the hard drive. This is a problem: Even if the encryption key itself is concealed with another key, the encryption key is still on the hard drive and out in the open. Obscurity? Yes. Security? No. Even if the key is hidden among other data, hackers have programs that can search the hard drive and quickly locate the key. On the other hand, ControlVault lets applications store keys within the ControlVault protected boundary. Access to the keys is strictly controlled by an authorization scheme. No application can access the keys without satisfying the authentication requirements set up by the owner or IT manager of a particular ControlVault. And the small memory footprint of Dell's ControlVault helps ensure low impact to overall system performance.

Controlling Access To Reference Templates

To verify authentication, a reference template, which is created and stored at time of enrollment, must be accessed. Applications usually store this template on the hard drive — and expose it to the following threats:

- Modification. A non-authorized user can replace the original reference template.
- Extraction. A template, such as a fingerprint template, can be copied, creating a privacy issue for the user who may want to prevent others from getting a digital copy.

ControlVault minimizes these threats. It allows applications to store templates inside the ControlVault-protected boundary. Template access is then controlled by an authorization scheme. Accordingly, no application is able to access the keys without satisfying the authentication requirements set up by the owner or IT manager of a particular ControlVault.

Isolating Usage of Keys and Templates

Even if a key or template is stored securely, other solutions subject them to sniffing or modification risks as they are pulled out into the open during a security operation. ControlVault doesn't take these risks. It isolates all usage of keys and templates from the host. In some cases, it performs key encryption inside the chip's boundary, so certain types of keys never are exposed to an insecure host. For example, fingerprint templates are never exposed outside the ControlVault security boundary — final matching takes place inside the chip. However, ControlVault presently does not perform high bandwidth bulk encryption.

Sealing Off Code Execution

Many applications execute their secure operations on the host x86 processor, which exposes it to sniffing of interim values and modification of the final result. In contrast, ControlVault executes operations and stores credentials within its secure boundary. This allows credentials to be kept secure and protects against any inspection or modification of the execution process.

Securing Code Storage

Many applications store code on the hard drive, which makes it vulnerable to an attacker who may replace parts of the code with alternate code to force an unintended result. ControlVault stores the execution code for secure processes within the secure boundary. Malicious applications cannot access this stored code.

HOW DOES CONTROLVAULT DIFFER FROM TRUSTED PLATFORM MODULE (TPM)?

ControlVault and TPM both store keys, but ControlVault:

- Can store and execute code using a secure processor
- Uses personal authentication (FP, SC, Contactless) to access credentials vs. TPM's 160-bit password
- Stores all credential types to allow single point of migration
- Supports broad crypto algorithm (i.e. Suite B, native ECC)

LEARN MORE AT DELL.COM/Latitude