WHITE PAPER

Anqlave Data Vault* (ADV*) with Intel® Software Guard Extensions (Intel® SGX)

Executive Summary

Anqlave Data Vault* (ADV*) helps solve the secret-management problem by allowing users to create, store, transport, and use secrets with improved security. ADV helps ensure that secrets are not available in plaintext, whether at rest, in motion, or in use. Secrets receive protection at rest and in motion using encryption, and they are used inside protected memory regions, called enclaves, which are created using Intel® Software Guard Extensions (Intel® SGX).

ADV centralizes secret creation and management and allows for decentralized use of secrets. This decoupling allows users to create portable enclaves, or "penclaves," which can be ported from one Intel SGX–enabled machine to another. Penclaves have wide applicability and form the basis for keyless cryptography as a service and confidential, distributed machine learning (ML). They also play a key role in enabling elastic, confidential cloud computing.

The Secret-Management Problem

A secret is anything that one system uses to authenticate or authorize itself with another; for example, user names and passwords, API tokens, Transport Layer Security (TLS) certificates, and cryptographic keys. Secrets end up being stored and used in a wide variety of insecure places.

Perimeter-defense systems are not sufficient to protect secrets on the server side. Notably, large companies have been in the news for insecure password-management practices. Helping protect secrets from insiders who have easy access to those secrets, or who can conduct sophisticated memory scraping attacks, is critical.

Application secrets can get carelessly strewn in all sorts of places. Database user names and passwords are often hardcoded into the source code, or they are in configuration files. Locations of key files and certificates are also often stored in configuration files. These end up in version-control systems or even in shared folders or wikis. It can be a challenge to manage these secrets and to determine if your system has been compromised.

ADV uses a two-pronged approach to secret management. First, it centralizes the secret-lifecycle-management activities to a single hardened, fault-tolerant, and robust service. Second, ADV helps ensure that secrets are encrypted at rest, in motion, and in use. This protects the secrets from insiders with root or administrative privileges—even those who can conduct sophisticated memory scraping attacks.

Authors

Pralhad Deshpande, Ph.D., Product Lead, Anqlave

Celina Miranda, Architecture Lead, Anqlave

Rodel Miguel, Engineering Lead, Anqlave

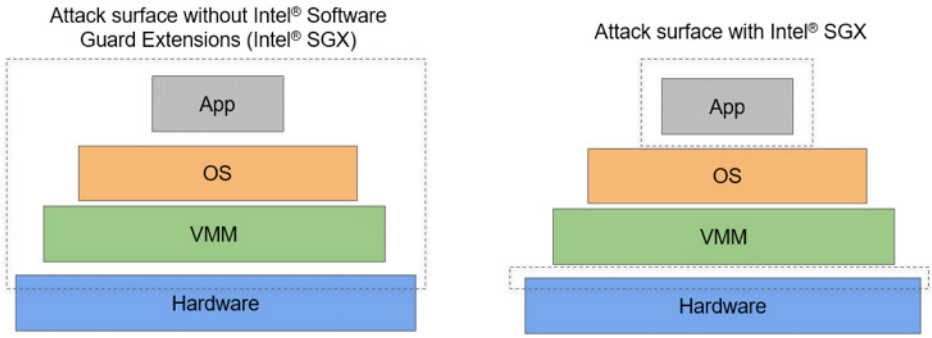

Figure 1. Reduction of attack surface with Intel® Software Guard Extensions (Intel® SGX)

About Intel SGX Technology

The traditional Intel® architecture follows a hierarchical privilege mode. Various software processes operate at different privilege levels. Less-privileged software processes do not have any privacy from more-privileged processes. Thus, a typical application's security depends on the integrity of the operating system (OS), virtual machine manager (VMM), and BIOS.

Intel SGX is available on Intel® Xeon® E processors. It enables application code and data isolation in applications even in the presence of a compromised OS, hypervisor, or privileged administrator. An Intel SGX enclave operates within a private region of memory that is designed to be inaccessible to any other process, irrespective of privilege levels. As a result, an application running inside an Intel SGX enclave has a reduced attack surface limited to itself and excludes other external processes. Even if the VMM or BIOS are compromised, or an insider has access to OS root privileges, the Intel SGX–protected application can still operate with integrity.

Once an application runs inside an Intel SGX enclave, all the system memory that is allocated to it is automatically encrypted by the CPU core. Snooping the system memory is ineffective because the attacker will not be able to access the decrypted memory. Intel SGX can also thwart other attacks, including those using memory scraping, ptrace-based tools and other reverse engineering tools.

Anqlave Data Vault (ADV)

ADV centralizes secret management to a single system. The ADV secret-management system allows authorized users to interact with the ADV service to perform lifecycle-management activities for your most sensitive data, code, keys, and intellectual property (IP).

Instead of secrets being created everywhere and stored in a variety of places, ADV centralizes secret creation and secret lifecycle management to a single system. Secrets are created and used inside Intel SGX enclaves and do not leave the encrypted Intel SGX environment. Secrets are not made available in plaintext, and they can only be referred to by their names for lifecycle-management purposes and for syncing with other Intel SGX enclaves that are signed by the same author as the ADV enclave.

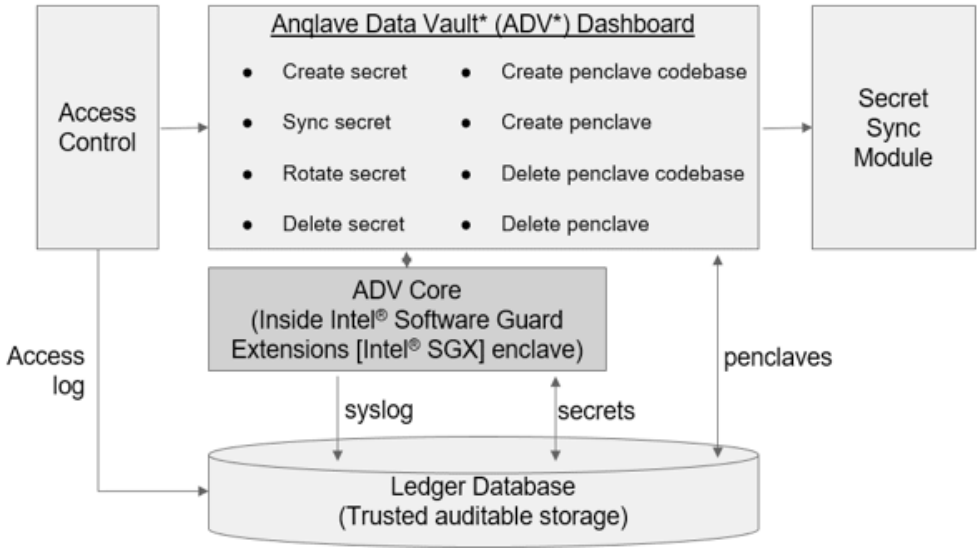

Figure 2. Anqlave Data Vault* (ADV*) architecture

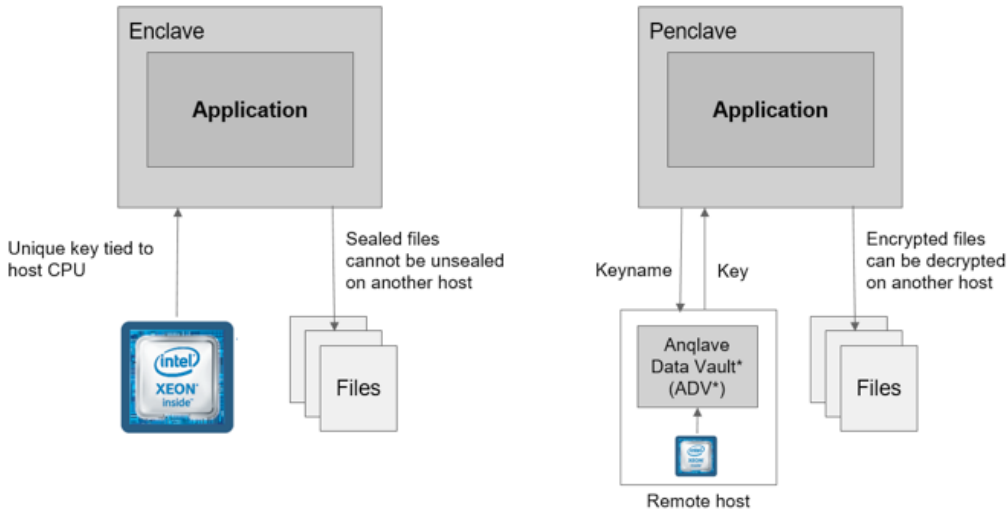

Figure 3. The difference between an enclave and a penclave

Penclaves and the Elastic Intel SGX–Capable Cloud

An application running inside an Intel SGX enclave ends up getting tied to a single host. This is because a unique hardware-rooted key is used to seal and unseal files that this enclave writes to durable storage.

ADV helps enterprises create penclaves. The keyname is embedded in a penclave. At runtime, a penclave establishes a secure connection with ADV and fetches a key corresponding to the keyname. This key is then used by the application running inside the penclave to encrypt and decrypt files that are stored in durable storage.

Penclaves allow applications running inside Intel SGX enclaves to seamlessly move from one host to another. Elasticity is fundamental to cloud applications, and application portability across various machines is key to elasticity. Penclaves enable seamless provisioning and decommissioning of Intel SGX–based applications in the cloud.

Creating Penclaves

Figure 4 shows a dashboard that is used to create penclaves with ADV. A user can choose a base image from those available, point to an ADV service to do key management, choose a keyname to which the ADV service has a reference, and enter the desired name for the penclave binary image. With the click of a button, the user is able to create a penclave image that can then be downloaded onto an Intel SGX–enabled deployment machine. The keyname is embedded in the penclave. At runtime, the penclave establishes a secure connection with the referenced ADV service and fetches the key corresponding to the keyname. This key is then used by the application running inside the penclave to encrypt and decrypt files that are stored in durable storage.

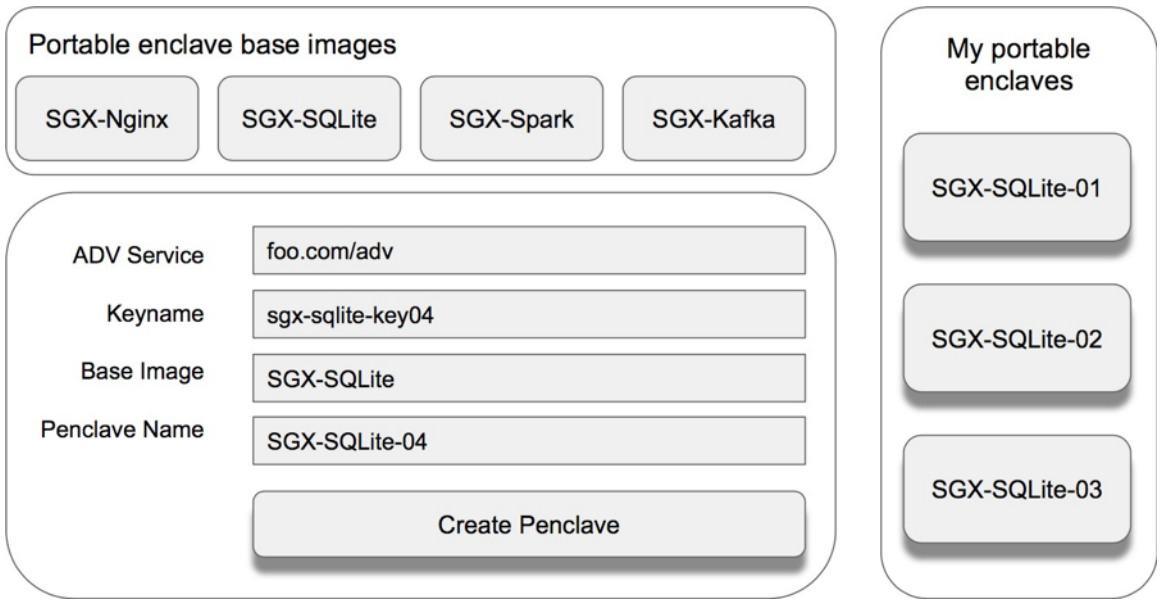

Figure 4. A dashboard to create portable enclaves ("penclaves")

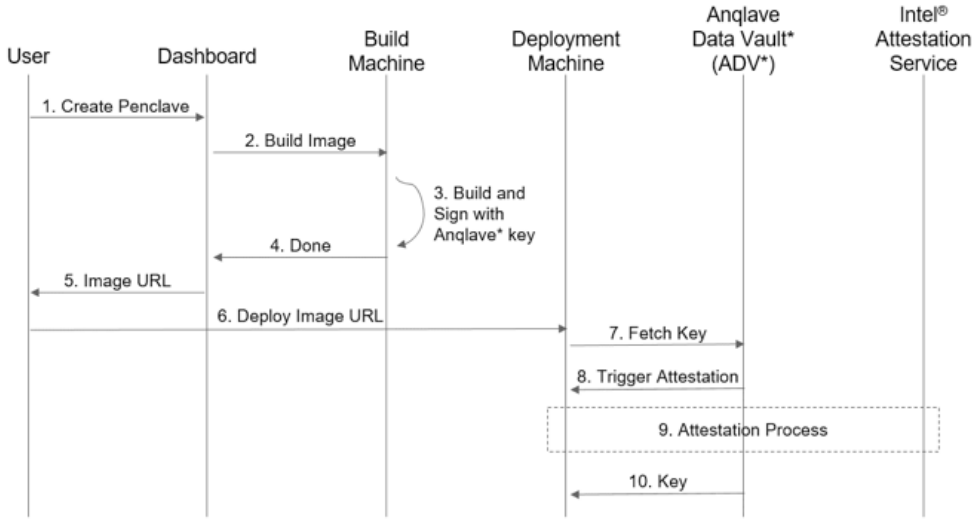

Figure 5. Diagram showing the interactions between various entities during the creation, deployment, and execution of a penclave

Figure 5 shows the interactions between various entities that lead to the creation, deployment, and execution of penclaves. A user interacts with the dashboard, feeds in appropriate information, and requests the creation of a penclave. The dashboard creates the penclave image on a build machine. The penclave is a binary with a reference to the ADV service and a keyname embedded into it. The image URL is returned to the user who can deploy the penclave binary image to any Intel SGX–enabled machine. At initialization time, the penclave process will attempt to fetch the key associated with the keyname from the ADV service. This will trigger an attestation process involving the deployment machine, the ADV service, and the Intel SGX attestation service. Upon successful attestation, ADV will deliver the key to the penclave running on the deployment machine.

Keyless Cryptography as a Service

Consider the highest-end databases that store the world's most valuable data. The keys used to encrypt and decrypt this data, whether to achieve transparent data encryption or to achieve geo-replication, have to be protected. The keys have to be stored securely and also used securely; the keys should not be available in plaintext and should be used by audited cryptographic algorithms that are executed in a secure runtime environment. The world's highest-end databases use hardware security modules (HSMs) with Federal Information Processing Standards (FIPS) 140-2 validated hardware cryptographic modules for secure storage and use of cryptographic keys.

HSMs with hardware cryptographic modules can be used to provide secure cryptography as a service. However, this concept has not penetrated the cloud environment. While solutions like Amazon Web Services (AWS) CloudHSM* can be used to perform key-management services, they are not used to perform cryptography as a service.[1] One reason for this is that cryptographic operations are so commonplace that invoking an over-the-network service each time degrades system performance.

Cryptography as a service should improve security and should not degrade system performance. This combination can be achieved by running FIPS 140-2-validated cryptographic modules inside secure execution environments locally on the application host itself. The localized interaction, without any network latency, helps to prevent degradation of system performance.

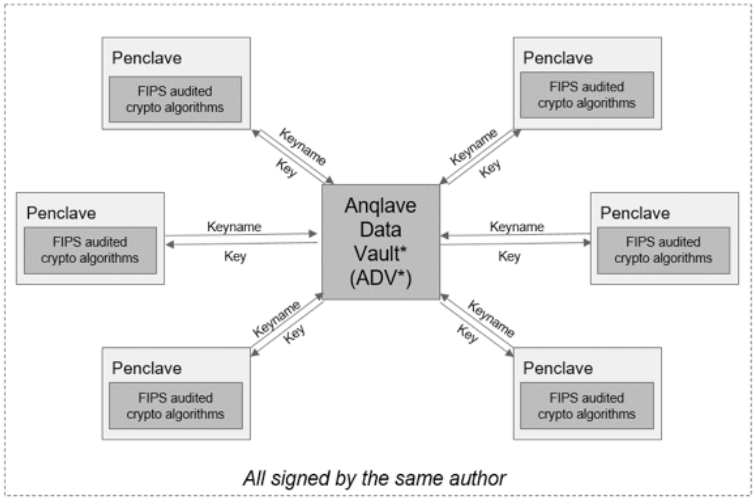

Figure 6. Anqlave Data Vault* (ADV*) enables keyless cryptography as a service; ADV is a centralized secret (key) management service, and penclaves are distributed through the cloud or enterprise environment

Providing FIPS 140-2-audited cryptographic routines as a service alleviates the burden on the application developer of getting cryptography right. Running these routines inside penclaves enables keyless cryptography as a service. Penclaves initialized with keynames can fetch appropriate keys from ADV over secure TLS links, and they can then use those keys inside Intel SGX enclaves. This form of cryptography, where the key is never available in plaintext, is called "keyless cryptography."

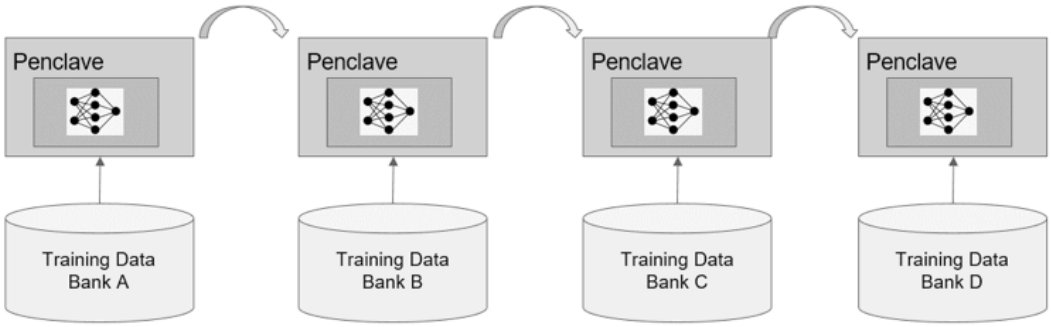

Figure 7. A penclave moves from one silo to another, consuming the training data and improving the model being trained

Confidential Machine Learning over Siloed Data

ADV and penclaves can help you implement confidential ML over siloed data. For various reasons, data might be locked in multiple data silos. The parties might not wish to share certain data because of confidentiality reasons, or because regulations demand so. Training a model over data within a single silo is much less effective compared to training it over the entire dataset.

One approach to train a model over the entire dataset is to encapsulate the ML algorithm into a penclave. A partially learned model can then be moved from one data silo to another. Once the model is trained over the entire dataset, all parties can use that model and achieve significantly better outcomes. This approach preserves the confidentiality of the model, which stays inside the penclave. The model can be used for standard ML tasks, but it cannot be seen by any party.

[1] Amazon. "AWS CloudHSM." https://aws.amazon.com/cloudhsm/.

Printed in USA 0819/CF/PRW/PDF Please Recycle 340844-002US