Cryptography and cloud security

Earlier in this course, you were introduced to the concepts of the shared responsibility model and identity and access management (IAM). Similar to on-premise networks, cloud networks also need to be secured through a mixture of security hardening practices and cryptography.

This reading will address common cloud security hardening practices, what to consider when implementing cloud security measures, and the fundamentals of cryptography. Since cloud infrastructure is becoming increasingly common, it's important to understand how cloud networks operate and how to secure them.

Cloud security hardening

There are various techniques and tools that can be used to secure cloud network infrastructure and resources. Some common cloud security hardening techniques include incorporating IAM, hypervisors, baselining, cryptography, and cryptographic erasure.

Identity access management (IAM)

Identity access management (IAM) is a collection of processes and technologies that helps organizations manage digital identities in their environment. This service also authorizes how users can leverage different cloud resources.

Hypervisors

A **hypervisor** abstracts the host's hardware from the operating software environment. There are two types of hypervisors. Type one hypervisors run on the hardware of the host computer. An example of a type one hypervisor is VMware®'s EXSi. Type two hypervisors operate on the software of the host computer. An example of a type two hypervisor is VirtualBox. Cloud service providers (CSPs) commonly use type one hypervisors. CSPs are responsible for managing the hypervisor and other virtualization components. The CSP ensures that cloud resources and cloud environments are available, and it provides regular patches and updates. Vulnerabilities in hypervisors or misconfigurations can lead to virtual machine escapes (VM escapes). A VM escape is an exploit where a malicious actor gains access to the primary hypervisor, potentially the host computer and other VMs. As a CSP customer, you will rarely deal with hypervisors directly.

Baselining

Baselining for cloud networks and operations cover how the cloud environment is configured and set up. A baseline is a fixed reference point. This reference point can be used to compare changes made to a cloud environment. Proper configuration and setup can greatly improve the security and performance of a cloud environment. Examples of establishing a baseline in a cloud environment include: restricting access to the admin portal of the cloud environment, enabling password management, enabling file encryption, and enabling threat detection services for SQL databases.

Cryptography in the cloud

Cryptography can be applied to secure data that is processed and stored in a cloud environment. Cryptography uses encryption and secure key management systems to provide data integrity

and confidentiality. Cryptographic encryption is one of the key ways to secure sensitive data and information in the cloud.

Encryption is the process of scrambling information into ciphertext, which is not readable to anyone without the encryption key. Encryption primarily originated from manually encoding messages and information using an algorithm to convert any given letter or number to a new value. Modern encryption relies on the secrecy of a key, rather than the secrecy of an algorithm. Cryptography is an important tool that helps secure cloud networks and data at rest to prevent unauthorized access. You'll learn more about cryptography in-depth in an upcoming course.

Cryptographic erasure

Cryptographic erasure is a method of erasing the encryption key for the encrypted data. When destroying data in the cloud, more traditional methods of data destruction are not as effective. Crypto-shredding is a newer technique where the cryptographic keys used for decrypting the data are destroyed. This makes the data undecipherable and prevents anyone from decrypting the data. When crypto-shredding, all copies of the key need to be destroyed so no one has any opportunity to access the data in the future.

Key Management

Modern encryption relies on keeping the encryption keys secure. Below are the measures you can take to further protect your data when using cloud applications:

- Trusted platform module (TPM). TPM is a computer chip that can securely store passwords, certificates, and encryption keys.
- Cloud hardware security module (CloudHSM). CloudHSM is a computing device that provides secure storage for cryptographic keys and processes cryptographic operations, such as encryption and decryption.

Organizations and customers do not have access to the cloud service provider (CSP) directly, but they can request audits and security reports by contacting the CSP. Customers typically do not have access to the specific encryption keys that CSPs use to encrypt the customers' data. However, almost all CSPs allow customers to provide their own encryption keys, depending on the service the customer is accessing. In turn, the customer is responsible for their encryption keys and ensuring the keys remain confidential. The CSP is limited in how they can help the customer if the customer's keys are compromised or destroyed. One key benefit of the shared responsibility model is that the customer is not entirely responsible for maintenance of the cryptographic infrastructure. Organizations can assess and monitor the risk involved with allowing the CSP to manage the infrastructure by reviewing a CSPs audit and security controls. For federal contractors, FEDRAMP provides a list of verified CSPs.

Key takeaways

Cloud security hardening is a critical component to consider when assessing the security of various public cloud environments and improving the security within your organization. Identity access management (IAM), correctly configuring a baseline for the cloud environment, securing hypervisors, cryptography, and cryptographic erasure are all methods to use to further secure cloud infrastructure.