Key Establishment Protocols and Management Techniques

Reading

40m

Status | Incomplete

Introduction

Nowadays, more sensitive data is sent over the Internet, and people are heavily migrating their infrastructure to the cloud in different service models. As this happens, the need for the use of cryptographic keys grows. Faced with this reality, Cyber Security professionals actively protect this data with tried-and-true techniques used at different stages to ensure privacy.

However, cryptography may not make data protection and availability guarantees possible. As much as there is advanced technology against data breaches, the risk of leaks or information theft will still be significant without managing cryptographic keys.

Why is Managing Cryptographic Keys Necessary?

Management means protecting cryptographic keys from loss, theft, corruption, and unauthorized access.

Objectives of key management:

- Ensure keys are kept secure.
- Change keys regularly.
- Control how and to whom keys are assigned.
- Decide on the granularity of the keys.

In practice, managing cryptographic keys means assessing whether a key should be used for all backup tapes or whether each one should receive its own. Therefore, you must ensure that the cryptographic keys and anything related to them is appropriately controlled and protected.

Would it make sense to have a state-of-the-art lock on your front door but leave the keys under the rug? Data and assets need strong security but more importantly, good management.

> ℹ Remember the objectives of cryptography are confidentiality, integrity, authentication, and non-repudiation.

Cyber Security professionals must think about using a technology that guarantees data security coupled with efficient management.

Cryptographic Key Management

Cryptographic key management is challenging but possible, and managing cryptographic keys can be complicated. Access must be provided and you would have to ensure it is restricted.

Successful cryptographic management requires good practice in several areas.

First, you must choose the correct encryption algorithm and key size to ensure security. Then, it must ensure that the implementation of the corporate encryption strategy conforms to established standards for that algorithm, which means being approved by a recognized Certification Authority.

Finally, it must ensure efficient cryptographic key management associated with security policies and processes that can certify the productive use of the technology.

To have greater confidence in your cryptographic key management strategy, the first questions to ask yourself are the following:

> Refelction Questions: Where are the encryption keys kept? Who owns them?

Many management services retain private keys at the service layer, so your data may be accessible to administrators of that activity. This can be great for availability but not necessarily for confidentiality. So, as with any technology, the efficiency of encryption entirely depends on its implementation.

If it is not done correctly or if the components used are not adequately protected, it is at risk, and so is the data you're trying to secure.

This means that standardization is vital to create applicable policies and processes, reducing the possibility of loopholes that can result in cyberattacks and data theft.

Encryption creates opportunities for different companies and Cyber Security specialists, mitigating concerns like cyberattacks and creating an orderly, efficient, and strategic data access cycle.

Finally, in times of digital transformation and so many technological and market disruptions, cryptographic key management is vital to protect all data and encryption keys.

Further Reading

The following publication by NIST covers in detail general key management guidance and protection requirements for key information. You will want to familiarize yourself with both these sections.

> Read sections 5 and 6 of the following publication: Recommendations for Key Management, NIST SP 800-57 Part 1, and save this document to your PKM for future reference.

✓ Mark Completed

← Previous
Hash Functions, Data Integrity and Digital Signatures

Next
Data Integrity Email →

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W07D3

Wed Aug 7

Lectures (1)

Work (7)

6 hrs

- Configure Apache Web Server
- Capture an HTTP and an HTTPS Wireshark PCAP
- Report to IT Manager
- Hash Functions, Data Integrity and Digital Signatures
- Key Establishment Protocols and Management Techniques
- Data Integrity Email
- Project Reading

W07D3 Schedule »