Kiteworks

Top 10 Trends in Data Encryption:

An In-depth Analysis on AES-256

In the wake of heightened cyber threats and the growing need for secure communication and data storage in an era of compliance, understanding these trends is crucial. This eBook is tailored to inform, educate, and guide those interested in data encryption, particularly in the Advanced Encryption Standard (AES)-256 standard, whether you are a cybersecurity enthusiast, a professional in the field, or a tech-savvy individual intrigued by the subject.

Origins of the AES Standard

AES has become the de facto worldwide encryption standard since its establishment by the U.S. National Institute of Standards and Technology (NIST) roughly two decades ago. This specification replaced the Data Encryption Standard (DES), a 56-bit key encryption model introduced in 1977 that was later cracked. As an interim measure, DES was strengthened into Triple DES, which employed three passes of the DES algorithm. AES, initially developed over six years with international cryptographic experts, provides encryption using key lengths of 128, 192, and 256 bits. The latter two key lengths are suitable for encrypting top-secret information.

However, as technology evolves, especially with the potential rise of quantum computers, new encryption challenges arise. Quantum computers pose a significant threat to asymmetric cryptography or public key encryption, like the RSA algorithm. Recognizing this, NIST initiated a project in 2016 to develop new public-key encryption algorithms, and out of 82 initial contributions, seven candidates are now under final consideration with a standard expected by 2024. Experts assert that transitioning to longer AES key lengths, like from AES-128 to AES-256, would offer the same security level as before quantum computing's advent.

From a technical perspective, the AES, based on the Rijndael block cipher created by Belgian cryptographers Joan Daemen and Vincent Rijmen, operates symmetrically, meaning the same key is used for both encryption and decryption. With up to 14 operational rounds based on key size, it employs a mix of substitution and permutation techniques. As of now, while various attacks have been attempted on AES, none have been computationally successful in decrypting data without the key.

10 Trends in Data Encryption— In Transit and At Rest

The eBook explores key trends such as authenticated encryption, quantum-resistant algorithms, hardware-based encryption, and more. Prepare to delve into these fascinating trends and gain valuable insights into how AES-256 contributes to maintaining the security and integrity of our digital world.

01 Introduction to Data Encryption and AES-256

Data encryption converts data into a code to prevent unauthorized access. It has become an indispensable security layer, especially with the increasing volumes of data produced daily. AES-256, a specification for the encryption of electronic data, is renowned for its robustness and wide usage in sensitive data protection. This 256-bit encryption standard is recognized globally and is used extensively by the U.S. government, making it a stalwart in data security.

Quantum AI: The Future of Cybersecurity

Listen to this Kitecast episode with Jean Phillip Bernier, the CEO and Founder of AnniQ and Spin Quantum Tech, who discussed advances in AI and quantum computing technology and what these mean for cybersecurity.

Listen to the Podcast

02 The Rise of Authenticated Encryption: AES-GCM

Authenticated encryption, which ensures ciphertext integrity, has seen an upsurge in usage. AES in Galois/Counter Mode (AES-GCM), with built-in authentication, is a top choice for symmetric block encryption. The integrated authentication in AES-GCM provides a significant advantage, removing the need for a separate integrity check and making encryption more efficient.

03 Post-quantum Cryptography

Quantum computing, while still nascent, presents a potential risk to many encryption algorithms. As this technology evolves, the need for quantum-resistant algorithms is gaining attention. AES-256 has so far demonstrated robustness against quantum threats, but continued research in this field is critical for maintaining the security of encrypted data in the quantum era.

04 Hardware-based Encryption

With data breaches and cyber threats on the rise, encryption at the hardware level is becoming increasingly important. Modern processors have started to integrate encryption algorithms, including AES-256, into their design. This trend provides an additional layer of security, ensuring that data remains encrypted even if a system's primary security measures are breached.

Navigating the Email Encryption/ Decryption Challenge

Email services employ different encryption standards that are incompatible with each other. As a result, organizations that do not have automatic decryption in place have few choices beyond the three below options:

50% of survey respondents ask senders to send a password-encrypted zip file when a recipient cannot decrypt an encrypted email.

35% ask the sender to resend the file(s) unencrypted in an unpublished shared drive link.

15% try signing up for a free encryption email outside of their company email.[1]

Download the Report

Source: Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report, July 2023.

05 Encryption in Cloud Services

As businesses increasingly move to the cloud, maintaining data security and privacy has become paramount. Cloud service providers are implementing stronger encryption algorithms like AES-256 to ensure data security. This trend not only protects data at rest but also safeguards it while in transit, providing comprehensive security coverage for cloud-based data.

06 The Use of Homomorphic Encryption

Homomorphic encryption allows computations to be done on encrypted data without decrypting it, thereby providing a new layer of security. This approach can be utilized with AES-256, allowing for secure computations on encrypted data. While it is computationally intensive, advances in processing capabilities are making homomorphic encryption more practical for a variety of applications.

07 IoT and Encryption

The Internet of Things (IoT) has grown exponentially, with devices collecting vast amounts of data. This data is often sensitive, making encryption critical. AES-256 is widely used due to its superior security, ensuring that data remains safe even as it moves between multiple IoT devices and systems.

08 Regulatory Influence on Encryption Standards

Governments worldwide are becoming more concerned about data privacy, pushing companies to adopt robust encryption standards. AES-256 is frequently recommended in these regulations due to its proven security. Regulatory compliance is an increasingly significant factor in encryption decisions, and the robustness of AES-256 makes it a common choice.

09 AI and Machine Learning in Encryption

Artificial intelligence (AI) and machine learning (ML) technologies are being integrated into encryption algorithms. These technologies can enhance AES-256 encryption by automating key management, detecting anomalies, and improving encryption efficiency. While this is a developing field, the potential to enhance data security through AI and ML is significant.

10 Privacy-preserving Computation Techniques

Secure multi-party computation (SMPC) and zero-knowledge proofs (ZKPs) allow for data privacy while enabling computation, enhancing the security and versatility of data encryption. These techniques can work in tandem with AES-256, adding another layer of privacy protection. As more data moves online, these privacy-preserving techniques are becoming increasingly important in the encryption landscape.

Kiteworks' End-to-End Encryption for Sensitive Content Communications

The Kiteworks platform provides end-to-end encryption across multiple communication channels, including email, file sharing, managed file transfer, and web forms. This ensures that sensitive data is always protected, regardless of the communication method used. Following are highlights of Kiteworks' end-to-end encryption capabilities, which are augmented with advanced security technology layers.

Kiteworks Uses Double Encryption

Kiteworks uses advanced encryption methods to secure data. This includes double encryption, where data is encrypted twice for added security. The first layer of encryption occurs when data is transferred over the network. The second layer of encryption is applied when data is at rest, stored on the server. Using double encryption, Kiteworks ensures that even if one layer is compromised, the data remains secure.

End-to-end Email Encryption

Kiteworks' encryption is also seamless and integrates into native email clients such as Outlook and Gmail. This means that users can send and receive encrypted emails directly from their preferred email client, without needing to use a separate application or plugin. This seamless integration enhances user experience and ensures that encryption is used consistently across all email communications.

File Sharing Encrypted: From First to Third Parties

In addition to email encryption, Kiteworks also provides end-to-end encryption for file sharing. This includes both internal file sharing within the organization and external file sharing with third parties. The platform encrypts files before they are sent and keeps them encrypted while they are stored on the server. Only the intended recipient, who has the correct decryption key, can decrypt and access the files.

Managed File Transfer Secure Encryption Transmission

For managed file transfer, Kiteworks uses secure protocols such as SFTP and HTTPS to ensure that data is encrypted during transmission. The platform also supports automated file transfers, where files are encrypted, transferred, and decrypted automatically according to a predefined schedule or trigger.

Web Forms Encrypted From Submission to Storage

Kiteworks' end-to-end encryption for web forms means that any data entered into a web form is encrypted before it is sent over the network and remains encrypted while it is stored on the server. This protects sensitive data such as personal information, credit card numbers, and passwords from being intercepted or accessed by unauthorized individuals.

Wrapped in Security Layers and Advanced Security Technology

Beyond encryption, Kiteworks uses other advanced security technologies to protect data. This includes a hardened virtual appliance, which is a secure, self-contained system that runs the Kiteworks platform. The hardened virtual appliance has built-in security features such as a network firewall, intrusion detection system, and web application firewall. These features protect the system from external threats and minimize vulnerabilities. Kiteworks also enables seamless integration of technologies such as content disarm and reconstruction (CDR), advanced threat protection (ATP), and data loss prevention (DLP).

Kiteworks also has an ongoing bug bounty program and performs regular penetration testing to identify and fix potential security vulnerabilities. The platform also supports one-click appliance updates, which make it easy to apply the latest security patches and updates.

AES-256 Encryption: Tried and Tested Requirement

The world of data encryption is dynamic, reflecting both the evolution of technology and the shifting landscape of threats. AES-256 continues to play a crucial role in maintaining data security in this complex context. As encryption trends evolve and new methods emerge, the importance of robust, tried-and-tested encryption standards like AES-256 cannot be overstated. AES-256 encryption in Kiteworks is one of a much larger set of security layers that enables organizations across industry sectors to protect sensitive content communications privacy while maintaining compliance with cybersecurity standards and data privacy regulations.

Kiteworks

www.kiteworks.com

August 2023