Advancements in Data Encryption Up the Data Defense Game

From credit card transactions to online loan applications and sensitive emails, billions of pieces of valuable information cross the internet every hour. Keeping that data safe from unauthorized access requires increasingly sophisticated tools. As the challenges to data security grow more intense, advancements in data encryption rise to meet them.

In the movies, messengers transmitted important documents in a briefcase, handcuffed to the messenger's wrist and accessible only via a key. The messenger made certain that no one tampered with the document during transit and that only the intended recipient opened the briefcase to retrieve and read its contents.

Encryption performs roughly the same function in the digital sense. The sender uses a "key" to encrypt the data, turning it into ciphertext. Only a person with the corresponding key can decipher the text back into its original form, or plaintext.

Data Encryption Challenges

As the digital environment evolves, keeping that data safe grows more complex. Encryption methods must account for challenges such as the following:

- Quantum computing – Typically, hackers use a brute force attack, attempting keys until they find a key that works. As computers grow more powerful, that process takes less and less time.

  While still an emerging technology, experts fear that the capabilities of quantum computers will prove too powerful for traditional encryption. Consequently, the security industry must develop quantum-resistant encryption.

- Cloud computing – As the remote workforce continues to expand and companies turn to outsourcing, sensitive data spends more time in the cloud. Third-party vendors complicate the cloud security landscape, opening up more points of vulnerability.
- Regulatory compliance – As technology evolves, so do concerns about data privacy. With regulations such as CCPA coming into force in 2020, encryption plays an even greater role than ever. Organizations that enforce encryption may avoid fines even in the event of a breach.

In response to these challenges and others, the data security community continually researches advancements in data encryption. Gaining an understanding of the technology can help organizations determine which types of encryption will best meet their security needs.

Homomorphic Encryption

Traditional encryption methods only protect data while in transit or in storage. In order to work with the data, users must decrypt it, leaving the data vulnerable to attack. Homomorphic encryption, on the other hand, allows data to be processed and analyzed without first decrypting the data.

Dr. Craig Gentry, the creator of homomorphic encryption, uses a simple analogy to describe it. He explains it as a glovebox. Anyone can put their hands in the gloves to manipulate what's inside the box, but they cannot remove anything from the box. Only someone with the key can open the box and remove the materials inside.

Thus, analysts can perform analysis on data in the cloud without exposing sensitive details. For the financial and healthcare industries, in particular, this provides much-needed security. Currently, homomorphic encryption takes too long for practical use, but researchers continually look for ways to speed the process.

Honey Encryption

To counter a brute force attack, honey encryption delivers believable plaintext in response to random decryption keys. That is, attackers attempt to use an incorrect key or password. In response, they receive fake data that appears to indicate a correct guess. With the fake data in hand, they end the attack.

Honey encryption can prove particularly useful for protecting data in the cloud and for protecting password vaults from breach.

Blockchain

The same technology that brought us bitcoin offers promise for data encryption. The blockchain cryptography that protects all transactions in the chain uses a digital signature. This digital signature acts like a package seal, ensuring that no one has tampered with the transaction and providing independent data verification.

Moving Target Defense

While not specifically an encryption method, moving target defense (MTD) deserves mention. This security strategy uses encryption but acts like a shell game, fragmenting data and keeping it moving across nodes and containers.

This strategy works particularly well for data in storage. With data in constant movement, attackers must deal with an attack surface that changes by the minute or even by the millisecond.

Stay Abreast of Advancements in Data Encryption

The world of data encryption involves complex technology designed to address increasingly complex threats. The email and data security experts at Messaging Architects will help you navigate the encryption options and determine the best solution to help you keep your sensitive data safe.