Zettaset

WHITE PAPER

Ensuring Data Integrity Against The New Cyber Threat

The Integrity of Your Data is At Stake

Cyberattacks are not just increasing in frequency, they are becoming more sophisticated. Meanwhile, cybersecurity professionals are faced with new challenges protecting data on massive data storage and cloud platforms.

But these cyberattackers are no longer limited to re-selling credit card and social security numbers. A new form of attack is causing even greater concern to industries worldwide: malicious modification of data, and subsequent loss of data integrity.

Data integrity means that data is authentic, valid, and protected from unauthorized modification, deletion, or corruption. Data integrity attacks are becoming one of the greatest concerns of leading security experts.

NSA director Mike Rogers brought the threat of large-scale data manipulation to everyone's attention in mid-2017, stating it was a "worst-case-scenario[1]" Prior to Rogers' remarks, former Director of National Intelligence James Clapper stated his concerns with the threat of data modification and tampering in 2016[2]. Clapper remarked that "Decision-making by senior government officials, corporate executives, investors or others will be impaired if they cannot trust the information they are receiving." Lieutenant General Vincent R. Stewart, USMC called these types of attacks "fifth generation warfare" where "the goal is panic and paralysis and to rob the enemy of the ability to think and act[3]."

This growing trend of tampering with data by modifying the contents of an encrypted file has the potential to affect any organization.

Examples of data modification include:

- Malicious insiders inflicting financial damage on a company by tampering with the data that it relies on to make critical business decisions
- Politically-motivated sabotage of government databases that include personally identifiable information such as tax records, social security data, and national security data such as TSA no-fly lists
- Organized crime altering financial services databases to hide fraudulent activities such as embezzlement and money laundering
- Changing blood work, prescription, or medical record data to negatively impact the care a particular patient or group of patients receives

How to Mitigate the Threat of Data Modification

Encryption is a powerful and proven method of protecting plain text from being deciphered and read by an unauthorized party. However, most commonly used encryption modes (such as AES-CBC) do not protect encrypted data from being modified or deleted and thus offer no integrity protection. By using a plain counter mode, the data is encrypted but there are no notifications if data tampering does occur.

---

1 http://www.washingtontimes.com/news/2017/may/9/mike-rogers-nsa-chief-senate-cyberattack-infrastru/
2 https://www.cnbc.com/2016/03/09/the-next-big-threat-in-hacking--data-sabotage.html
3 https://itspmagazine.com/from-the-newsroom/the-security-threat-that-lies-ahead-data-integrity

A man-in-the-middle attack, for instance, can replace the encrypted bits in-transit in a data center. This results in the decrypted data being different than the original plain text. Without dedicated data integrity protection, the receiver has no way to verify that decrypted cipher text is the same as the original plain text. Choosing a stronger data encryption mode like Galois/Counter Mode (GCM) provides added protection for encrypted data. Next-generation data encryption using GCM enables the administrator to know if and when any unauthorized data modification occurs.

The Solution: Zettaset XCrypt™ Object with AEAD

Object storage is a computer data storage architecture that manages data as objects, as opposed to other storage architectures like file systems which manage data as a file hierarchy, or block storage which manages data as blocks within sectors and tracks. Each object typically includes the data itself, a variable amount of metadata, and a globally unique identifier. Object-storage systems allow retention of massive amounts of unstructured data.

Greater possibilities for data analytics, and the ability to store an object anywhere within a distributed data pool, makes object storage technology particularly enticing for companies that provide storage services. Object storage has been widely adopted for high-volume cloud services, such as storing photos on Facebook, songs on Spotify, or files in online collaboration services like Dropbox. It is also used by Amazon Simple Storage Service (S3), the largest provider of cloud storage, as well as by most of its competitors.

To avoid exposing object data to vulnerabilities like unauthorized modification, you'll need a next-generation encryption solution with AEAD: Authenticated Encryption with Associated Data. AEAD protects against unauthorized modification of the cipher text itself, and also protects any unencrypted text (associated data) accompanying the cipher text. AEAD encryption using GCM is a major recent advancement in cryptography, but is not yet widely available.

XCrypt Object from Zettaset is one of the few encryption solutions with built-in GCM and AEAD. XCrypt Object encrypts object data and also protects the integrity of that data, ensuring that the data being decrypted is valid and has not been tampered with. In addition, XCrypt Object has been optimized for scalability and ease of use in object data environments.

The business benefits of the XCrypt Object data encryption and integrity solution include:

- Detecting data tampering attempts on encrypted data
- Reducing the negative impacts on brand, and reputation of a data corruption attack
- Improving trustworthiness and reliability of data
- Reducing downtime associated with restoring data to its pre-attack state

Learn more about Zettaset XCrypt Object, and how it can provide unparalleled encryption and integrity protection for your data. Visit http://www.zettaset.com/

465 Fairchild Drive, Suite 234, Mountain View, CA 94043
www.zettaset.com // +1.650.314.7920 // Fax: +1.650.314.7950 // sales@zettaset.com

About Zettaset

A leader in data protection, Zettaset's XCrypt™ line of encryption products are optimized for unmatched performance and infinite scalability to address the demanding data protection requirements of today's high-volume compute, storage, and cloud environments.