Zettaset
The Leader in Big Data Security

WHITE PAPER

Protecting Data Integrity Against the New Cyber Threat

February 2016

Abstract

While it's well known that cyber attackers attempt to steal valuable data that can be re-sold, such as credit card and social security numbers, a new form of attack is causing even greater concern to business and government: malicious modification of data, and subsequent loss of data integrity.

Cyberattacks are increasing in frequency and their impact can be immense. Considering the financial effect that a major data breach can have on a company, information security has become a critical function for reducing the risk and the potential impact of these incidents.

The growth of Big Data and petabyte-scale data storage, new open source database and distribution schemes like Hadoop and NoSQL, and the increasing adoption of cloud services by enterprises further complicate the data security challenge.

"Decision-making by senior government officials, corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving."

While it's well known that attackers attempt to steal valuable data that can be re-sold, such as credit card and social security numbers, there's a growing trend by attackers to tamper with data by modifying the contents of an encrypted file, completely undetected. Examples 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

A Growing Concern: Attacks That Modify and Corrupt Data

The attacks that are becoming of greatest concern to leading security experts don't involve the theft of data, but the manipulation and modification of it; changing the perception of what is real and what is not, and compromising integrity. Data integrity means that data is authentic, valid, and protected from unauthorized modification, deletion, and corruption.

Director of National Intelligence James Clapper has singled out cyberattacks that alter data for destructive purposes as a rising and unacceptable threat, saying "Decision-making by senior government officials, corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving."

Encryption is a powerful and proven method of protecting plain text from being deciphered and read by an unauthorized party. A security best practice is to require that encrypted data remain unmodified to maintain integrity and ensure that it is valid and authenticated. 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.

How can this happen? For example, a man-in-the-middle attack can replace the bits in-transit in a Hadoop cluster, which results in the decrypted data being different than the original plain text. Without data integrity protection, the receiver has no way to verify that decrypted cipher text is the same as the original plain text.

The Solution: Zettaset BDEncrypt Plus with AEAD

To avoid exposing data to vulnerabilities such as unauthorized modification, choose an encryption solution with AEAD: Authenticated Encryption with Associated Data. AEAD prevents tampering with the cipher text itself, and also protects any unencrypted text (associated data) accompanying the cipher text. AEAD encryption is one of the more important recent advances in cryptography, but is not yet widely available.

BDEncrypt Plus from Zettaset is one of the few encryption solutions with built-in AEAD. BDEncrypt Plus encrypts data and also protects the integrity of that data. Integrity is the "plus" that ensures that the data being decrypted is valid and has not been tampered with. In addition, BDEncrypt Plus has been optimized for scalability and ease of use in Big Data environments like Hadoop.

The business benefits of the BDEncrypt Plus 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 BDEncrypt Plus, and how it can provide unparalleled encryption and integrity protection for your data.

Check out the explainer video and see how BDEncrypt Plus works.

Visit http://www.zettaset.com/

Zettaset
465 Fairchild Drive, Suite 207, Mountain View, CA 94043 // www.zettaset.com
USA: +1.650.314.7920 // Fax: +1.650.314.7950 // sales@zettaset.com