Tokenization vs encryption

Technology, Information Technology

The paper " Tokenization vs. Encryption" is a wonderful example of an assignment on information technology. 1. Tokenization

1. 1. Benefits of Tokenization

1. 1. 1. Reduced Exposure to security threats

Tokenization minimizes the exposure of data to destruction and theft by storing data in a separate location from the tokens. It restores the real sensitive data through detokenization after the use of the token using the tokenization system.

1. 1. 2. Simplicity

Creation and maintenance of tokens are simpler than encryption since it uses a simple identifier as opposed to the encryption key. Likewise, detokenization uses the same identifier to convert the tokens to the original data, which is simpler than the use of decryption key in encryption and decryption processes.

1. 2. Weaknesses of Tokenization

1. 2. 1. Limited Data

Tokenization is not able to operate on all the data to be protected especially in larger institutions. This will imply the creation of numerous tokens, which may not be easy to manage.

1. 2. 2. Limited Compatibility

Tokenization works well with a few specific applications and technologies of data processing, but not all. The acquisition of relevant applications for its operation is very costly.

2. Encryption

2. 1. Benefits of Encryption

2. 1. 1. Improved Security

Encryption provides more secure data than tokenization from the end to the point of data processing. It can, therefore, prevent unauthorized access to the information unless one has the decryption key.

2. 1. 2. Integration with Technologies

Encryption and decryption mechanisms are able to integrate well with the existing processes and technologies.

2. 2. Weaknesses of Encryption

2. 2. 1. Vulnerability to Malware

Data encryption exposes the data to attack by sniffer malware through breaches of security best practices. Sniffers are able to grab information from the memory once the decryption is complete (Bergstein 2004, p43). This nullifies the value of the encryption solution.

2. 2. 2. Increased Processing Cost

The process of encryption and decryption introduces additional overhead, as it requires more resources. The resources include the encryption and decryption application, as well as the secure storage media.

3. A choice between Encryption and Tokenization

Even though both encryption and decryption perform the function of data protection, tokenization is the best method, considering its treatment of data. It stores the original data in a separate location from the tokens, such that any destructive event on the tokens cannot affect the original data. In encryption, the original data is encrypted and no copy of it is left in its original form. Failure to decrypt it means that the data is lost permanently (Agre & Rotenberg 1998, p. 55). Secondly, it is easier to map back the token to its original sensitive data than performing the decryption. This is because, in tokenization, the process uses reliable random numbers, unlike the complicated decryption keys. Thirdly, encryption exposes the data to malware attacks (Bergstein 2006, p47). Malware sniffers are able to read the data immediately after its decryption, thus losing the whole data. In tokenization, it is not possible for the malware sniffer to realize when the mapping of the tokens takes place, as it uses random numbers. With all the benefits of tokenization, it is safer and more reliable to protect data through the tokenization system (Schmitt & Stahl 2012, p. 42). Tokenization system is under dynamic development that is likely to make the future versions of the systems more robust.