УДК 004.056
DOI https://doi.org/10.17721/ISTS.2020.4.53-57

V. I. Ignisca, orcid.org/ 0000-0001-9295-0983,
veravialkova@gmail.com
D. Vdovenko, orcid.org/0000-0002-3263-867X,
vdovenko.danylo@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ANALYSIS OF METHODS DATA SECURITY

The article analyzes the main methods of information protection, from which it is possible to conclude that no method of data protection is ideal for all situations. It is important to choose an enterprise solution that provides comprehensive functionality, a flexible range of data protection options, broad support for platform and data types, and proven success in production implementations. The choice of method of information protection should take into account many circumstances that may arise during the implementation of a particular method. Due to the variety of data generated today, in addition to increasing the number of new platforms, flexibility can be a critical aspect of the data protection solution. A careful review of the requirements should make it easy to compare them with the relevant data protection methods, and it is necessary to make sure that the solution includes everything necessary to meet these requirements. Choosing the right method of information protection becomes much more difficult when more complex environments with many conflicting variables are involved, as it must support several options to provide flexibility to protect and meet data confidentiality, integrity and availability requirements. Only the integrated use of different measures can ensure reliable protection of information, because each method or measure has weaknesses and strengths. In some situations, internal security policies or regulations may forcibly change one method of data protection to another. Today, most standards, such as PCI DSS and HIPAA, allow a combination of the aforementioned methods, but these standards usually lag behind available or new data protection technologies. The set of methods and means of information protection includes software and hardware, protective transformations and organizational measures. A set of such methods, which are focused on protecting information, should protect them depending on whether the information is stored, moved or copied, accessed or used.

Keywords: *start-up, information interaction, customer journey map, forecasting.*

1. INTRODUCTION

Modern corporate solutions and solutions for enterprises require flexibility, versatility, stability and a high level of security to protect information. Information security solutions should ensure the integrity, confidentiality and availability of information. Compliance with information properties such as privacy, integrity, and accessibility is critical.

Information security can be presented in certain forms, such as, common forms and methods include: data management, network firewalls, intrusion prevention systems (IPS), semantic security at the row and column level (RLS / CLS), identity management (IDM), role-based access control (RBAC), activity monitoring, encryption, tokenization, encryption, data masking and more. The set of methods and means of information protection includes software and hardware, protective transformations and organizational measures. A set of such methods that focus on protecting information should protect them depending on whether the information is stored, moved or copied, accessed or used [1].

Organizational measures for information protection include a set of actions for the selection and verification of personnel involved in the preparation and operation of programs and information, clear regulation of the development and operation of the information system. Only the integrated use of different measures can ensure reliable protection of information, because each method or measure has weaknesses and strengths. Technical (hardware) means. These are different types of devices (mechanical, electromechanical, electronic, etc.), which hardware solve the problem of information protection [2].

Software includes programs for user identification, access control, encryption of information, removal of residual information such as temporary files, test control of the security system.

Mixed hardware and software implement the same functions as hardware and software separately

and have common properties. Organizational means consist of organizational and technical (preparation of premises with computers, laying of cable system taking into account requirements of restriction of access) and organizational and legal.

2. ANALYSIS OF INFORMATION PROTECTION METHODS

Dynamic data masking. Data is created that is completely or partially disguised when users or services without access to view it receive it. This technology does not change the data of the original text during storage on media (Figure 1). In most cases, this method is used as additional protection, most databases use this technology for viewing mode [3].

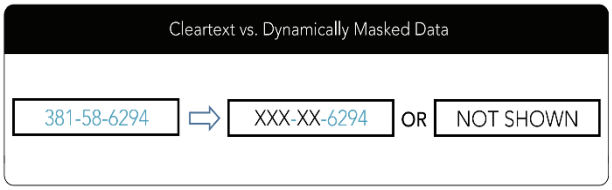

Fig. 1. An example of dynamic data masking

Static data masking. When using this method, the data cannot be reset. This method uses one-way hash algorithms along with encryption technology to achieve a result when the hash value is represented in binary form and cannot be stored using the original data type (Figure 2). Most static data masking tools generate data that is similar to the original and can be stored using the same data type and set of characters.

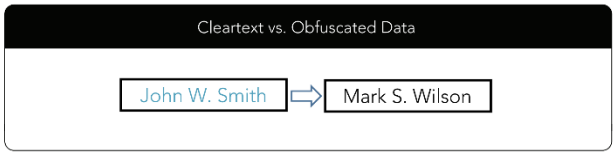

Fig. 2. An example of static data masking

Encryption technology uses mathematical algorithms and cryptographic keys to convert data into binary ciphertext (Figure 3). Resetting the data is possible only with the correct key with the algorithm. There are many forms of data encryption, various key benefits and other parameters.

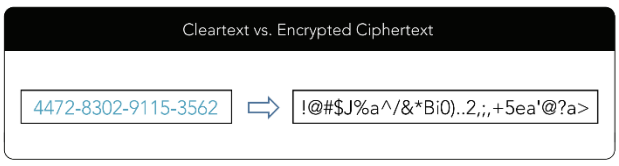

Fig. 3. An example of encryption technology

Tokenization. This method replaces a randomly or in some way generated value (token) with the value of the original text, stores this value in a table that corresponds to the value of the original text to the generated token (Figure 4).

The type and length of the token data remain the same as the original text, the token search table becomes the "key", which allows you to get the value of the original text from the token. With the increase in the number of such tokenized data and tables, along with the complexity of the IT infrastructure, leads to the fact that token search tables make it impossible to quickly and efficiently search.

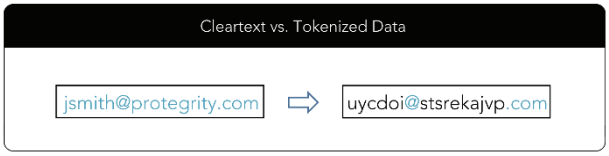

Fig. 4. An example of data tokenization

Encryption while preserving the data format. This method combines the advantages of both encryption (using a mathematical algorithm for encryption) and tokenization (the same type of data is stored).

Format encryption requires the same CPU cycles for encryption and then additional processing to convert binary ciphertext to the same data type as the original text and avoid possible "collisions" (same output for two different input values) by converting a larger binary fields in a smaller alphanumeric or alphanumeric data type.

Deidentification is a more general term for "anonymizing" data, used, for example, to display user data that is almost impossible to identify using available data.

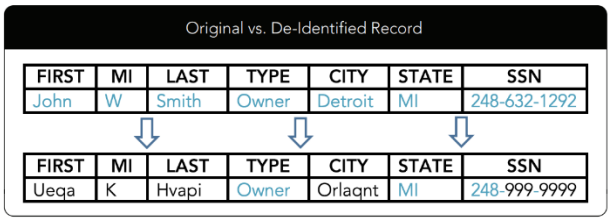

Fig. 5. An example of data deidentification

For sufficient identification or anonymity of field records to be protected in databases, these fields must be defined in the organization's data security policy. The data classification scheme should specify a minimum list of fields to be protected (for example, credit card number, last name, first name, etc.), as well as a list of recommendations for additional fields for less secure or more widely

available systems. These additional fields (for example, city, e-mail address, telephone number, etc.) will also be protected in cases where this is clearly justified by the security policy of the organization or enterprise [4].

3. DATA CLASSIFICATION AND DATA SECURITY POLICY

The data classification scheme should also determine which data should be protected on media, during data transmission and during their use [5]. The protection method should be platform-specific, using a centralized approach focused on maintaining multiple data protection options as needed.

Data protection on media.

The use of a particular method of data protection on media depends on the environment and the criteria that the method must meet. Full encryption is a common choice for portable media such as laptop hard drives or flash cards. Incomplete data encryption of certain fields has disadvantages, such as: changing the data type in VarByte (binary), larger field size, problems with systems or applications that do not support binary data fields. **Tokenization.** It's a modern solution for data protection on media. Gained popularity for the following reasons:

• data can be easily moved between systems open to databases or programs where access to the original text values is not required;

• if necessary, it is possible to find the correspondence of the original data using the correspondence table;

• Data type, field size, or supported character sets do not change.

Data protection during transportation.

Network traffic encryption protocols (SFTP, HTTPS, SSL, TLS) are most commonly used when transporting data, but field-level protection such as tokenization or encryption can also be used to add an extra layer of security to data transported between systems.

Data protection during use.

The biggest problem in protecting particularly sensitive data fields is when used by users or the corporate environment [6]. Usually only 1% to 3% of the total data in a large database guarantees the use of an incomplete type of information protection. In addition, 80% to 90% of all information required for business activities can be submitted in a secure form. Therefore, only 10% to 20% of the information required for operational activities will require access to 1%–3% of data that will require additional processing.

Sensitive user data fields, such as credit card numbers and other vulnerable data, require access to the original text, so both encryption and tokenization can be used without compromising the reference integrity of the data.

Incomplete data encryption gives users greater access to data, while improving the overall security framework and adhering to security policies and regulations.

Data security policy sequence.

It is equally important to consider the ability to consistently apply data security policies at all of the above stages and in all environments of the organization. The same method of protection, limited rights of access to information, accountability and audit, protection against unauthorized protection, etc. must be applied consistently throughout the flow of data exchange [7]. Data must be equally secure, processes must be consistent with security policies from start to finish, regardless of the platform used for data processing, analysis and storage.

The choice of method of information protection should take into account many circumstances that may arise during the implementation of a particular method.

The choice of the necessary method of information protection becomes much more difficult when more complex environments with numerous conflicting variables are involved. A solution for a particular enterprise or organization must support several options to provide flexibility to protect and meet the requirements of confidentiality, integrity and availability of data.

When protecting small field data (1 or 2 characters), encryption is the best option, as even small fields such as Boolean logical fields can be encrypted (with an initialization vector). Tokenization is limited by the width of the token search table used and is typically used for fields with three or more characters, but very large fields, such as more than 100 characters and can contain hundreds or thousands of characters, are not suitable for tokenization.

There are several approaches to consider for the protection of sensitive data using external cloud services, in addition to the obvious transition to management using a contractual approach. New, lower data processing costs can be provided by the heads of information security departments, finding a way to achieve the same or even improve the level of information protection through the use of cloud services [7].

Protect data fields of different sizes

When protecting small field data (1 or 2 characters), encryption is the best option, as even small fields

such as Boolean logical fields can be encrypted (with an initialization vector).

If you want to use a protected field often enough, encryption can be faster than tokenization, especially for large fields, because encryption takes the same time to process a 2-character field and a 16-character field. However, for standard structured fields of limited length (3 to 15 characters), tokenization is an ideal solution.

Storage regulations have a significant impact when it is necessary to transport information between several services, such as in some cloud applications. They often require data deidentification, but in some cases they do not allow certain particularly sensitive data to be transported between media at all.

4. CONCLUSION

The paper proposes analyzes of the main methods of information protection, from which it is possible to conclude that no method of data protection is ideal for all situations. It is important to choose an enterprise solution that provides comprehensive functionality, a flexible range of data protection options, broad support for platform and data types, and proven success in production implementations.

Due to the variety of data generated today, in addition to increasing the number of new platforms, flexibility can be a critical aspect of the data protection solution. A careful review of the requirements should make it easy to compare them with the relevant data protection methods, and it is necessary to make sure that the solution includes everything necessary to meet these requirements.

To protect data in web services, the best solution is to use methods to protect information using tokens, because modern enterprise and enterprise solutions require flexibility, versatility, stability and a high level of information protection.

REFERENCES

[1] Averchenkov VI Information security audit.– M.FLINTA, 2016 – 269 p.c.

[2] Gvozdeva, T.V. Design of information systems / T.V. Gvozdev, B.A. Ballod. – M .: Fenix, 2009. – 512 p.

[3] Protegrity. Methods of Data Protection [Electronic resource] / Protegrity Access mode to the resource: http://sfbay.issa.org/comm/presentatio ns/2015/Methods%20of%20Data%20Protection%20White%20Paper%20-%20Protegrity%20Sept%2020 15.pdf.

[4] Goodson, John A Practical Guide to Data Access (+ DVD-ROM) / John Goodson, Rob Steward. – M .: BHV-Petersburg, 2013. – 304 p. Голицына, О. Л. Основы алгоритмизации и программирования / О. Л. Голицына, И. И. Попов. – М.: Форум, 2010. – 432 с.

[5] Pollis, Gary Software Development. Based on the Rational Unified Process (RUP) / Gary Pollis et al. – M .: Binom-Press, 2011. – 256 p.

[6] Vsyakikh, Ye.I. Practice and problems of modeling business processes. – M .: Book on Demand, 2008. – 246 p.

[7] Internet Engineering Task Force. JSON Web Token (JWT) [Electronic resource] / Protegrity – Access mode to the resource: https://tools.ietf.org/html/rfc7519.

Стаття надійшла до редколегії 07.12.2020

Аналіз методів захисту даних

Проаналізовано основні методи захисту інформації, з яких можна зробити висновок, що жоден метод захисту даних не ідеальний для всіх ситуацій. Важливо вибрати корпоративне рішення, яке надає широкі функціональні можливості, гнучкий спектр варіантів захисту даних, широку підтримку платформ і типів даних, а також доведений успіх у виробничих реалізаціях. У випадку вибору методу захисту інформації слід ураховувати багато обставин, які можуть виникнути під час упровадження певного методу. Завдяки різноманітності даних, що генеруються нині, крім збільшення кількості нових платформ, гнучкість може бути критичним аспектом рішення щодо захисту даних. Ретельний огляд вимог має полегшити їхнє порівняння з відповідними методами захисту даних, і необхідно переконатися, що рішення містить усе необхідне для задоволення цих вимог. Вибір правильного методу захисту інформації стає набагато складнішим, коли задіяні більш складні середовища з багатьма конфліктуючими змінними, оскільки він повинен підтримувати кілька варіантів, щоб забезпечити гнучкість захисту та задоволення вимог щодо конфіденційності, цілісності та доступності даних. Тільки комплексне використання різних заходів може забезпечити надійний захист інформації, оскільки кожен метод або захід має слабкі та сильні сторони. У деяких ситуаціях політика чи правила внутрішньої безпеки можуть примусово змінити один спосіб захисту даних на інший. Сьогодні більшість стандартів, таких як PCI DSS та HIPAA, дозволяють поєднувати зазначені вище методи, але ці стандарти зазвичай відстають від наявних або нових технологій захисту даних. Сукупність методів та засобів захисту інформації включає програмно-апаратні засоби, захисні перетворення й організаційні заходи. Набір таких методів, орієнтованих на захист інформації, має захищати їх залежно від того, зберігається, переміщується чи копіюється інформація, доступ до неї чи використання.

Ключові слова: *стартап, інформаційна взаємодія, карта шляху клієнта, прогнозування.*

Vira Ignisca,
PhD, associate professor of Dept. of cyber security and information protection of Faculty of Informational Technology of Taras Shevchenko National University of Kyiv.

Віра Ігніска,
кандидат технічних наук, доцент кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

Danylo Vdovenko,
Student of Faculty of Informational Technology of Taras Shevchenko National University of Kyiv.

Данило Вдовенко,
студент факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.