CHALLENGES OF MODERN TECHNOLOGY | Vol. 7, No. 3, 2016, 16-19 DOI: 10.5604/01.3001.0009.5444

Application of the Clark-Wilson Model for Business Intelligence System Security Improvement

Paweł Buława, Marcin Kowalczyk
Warsaw University of Technology,
Faculty of Electronics and Information Technology
Institute of Telecommunications
Nowowiejska 15/19, 00-665, Warsaw, Poland.
e-mail: pawel.bulawa@gmail.com, m.kowalczyk@tele.pw.edu.pl

This paper presents the theoretical issues of data security in information systems, a practical implementation of the Clark-Wilson model on the example of Business Intelligence tool, performing the function of a telecommunications operator sales module, and an evaluation of the increase of security of the system created, using risk analysis.
Keywords: IT security, data integrity, Clark-Wilson Model, Business Intelligence, Information Systems

Introduction

Each day companies accumulate significant volumes of data related to their activities. Efficient processing in compliance with all safety rules may be the key factor in maximizing a company's value, achieving higher profits, improving competitiveness and meeting the formal requirements imposed by law. In order to cope with these challenges, companies have to invest in complex systems that support them in these activities. One of the solutions are systems based on data warehousing integrated with advanced analysis and reporting Business Intelligence tools, in which one of the paramount issues is the security of the processed data. In general, the information security can be defined as its protection against accidental or deliberate destruction, disclosure or modification [3]. According to this definition, there are three main components of data security: confidentiality, integrity and availability, commonly known as the CIA triad [4]. Confidentiality means that only authorized persons have access to information, data integrity ensures that data is accurate and complete, and availability is responsible for access to resources in compliance with the user's needs. Further very important aspects in data security are threats and vulnerabilities. The security of a system can be compromised when a threat exploits a vulnerability. Generally, we do not have influence on threats. However, it is possible to eliminate or reduce the vulnerabilities which can be exploited by threats. Ross Anderson, a specialist in the field of security, says that security engineering requires interdisciplinary knowledge in fields such as cryptography and computer security, through resistance to encroachment in equipment and formal methods, to knowledge in the field of applied psychology, methods of organization, audit and law [5]. As a result, miscellaneous types of methods are used in order to provide the expected level of system security. The first group of methods contain mechanisms based on cryptography, widely used to prevent unwanted access to data sent between different systems or its parts, and also to protect data already stored in databases (and their backups as well) [4]. Another important issue is a clear and well defined security policy, and a mechanism that enforces it [6]. So called good practices and experience could be defined as a group of formal requirements, contained within this policy [2]. Finally, several theoretical data security models, such as the Clark-Wilson integrity model or the Chinese Wall Model [7], and types of access control (DAC—discretionary access control [6], RBAC—role-based access control [8]) were proposed and successfully deployed. Data models contain various sets of rules, which are commonly applied in real systems, depending on particular requirements. For example, creating the Chinese Wall model, based i.e. on mathematic law of intersection, allowed Brewer and Nash to find the solution for situations containing conflicts of interests (COI) [9]. These conflicts may arise when two or more organisations, competing with each other, share one system (very common in finance sector) [10]. By using this model it is possible to avoid COI by granting access for an organisation only to a particular subset of data [7]. Another data model mentioned above, the Clark-Wilson integrity model, uses RBAC and responds very well to the needs of commercial systems [2]. There are also physical protection measures, such as the control of physical access to equipment, mirroring of equipment or an emergency power supply (UPS) [3].

The Clark-Wilson Integrity Model

The Clark-Wilson model, in general, is based on two fundamental principles: well-defined transactions and the separation of duties [2]. The first one serves to ensure that data can be processed only in accordance with strictly defined rules, moreover, every operation will be logged in audit-logs. These logs could be analysed in an unusual situation or for preparing some reports. The second widely known principle—the separation of duties—is used to eliminate potential abuses that may occur when one employee performs all steps of a transaction independently. This rule enforces the division of a transaction, in which particular steps have to be performed by different employees. The next step of the transaction cannot

be started until the previous step has been properly executed. The Clark-Wilson data integrity model consists of [11]:

1. Two data items types:
   a) Constrained Data Items (CDIs);
   b) Unconstrained Data Items (UDIs).
2. Two classes of procedures:
   a) Integrity Verification Procedures (IVPs);
   b) Transformation Procedures (TPs).
3. A set of nine rules, including five Certification Rules (C) and four Enforcement Rules (E):

C1: All IVPs must properly ensure that all CDIs are in a valid state at the IVP runtime.
C2: All TPs must be certified to be valid. That is, they must take a CDI to a valid final state, given that it is in a valid state to begin with. For each TP, and each set of CDIs that it may manipulate, the security officer must specify a 'relation' which defines that execution. A relation is thus of the form: (TPi, (CDIa, CDIb, CDIc, ...)), where the list of CDIs defines a particular set of arguments for which the TP has been certified.
E1: The system must maintain a list of relations specified in rule C2, and must ensure that the only manipulation of any CDI is by a TP, where the TP is operating on the CDI as specified in some relation.
E2: The system must maintain a list of relations in the form of: (UserID, TPi, (CDIa, CDIb, CDIc, ...)) which relates to a user, a TP and the data objects that the TP may reference on behalf of that user. It must ensure that only executions described in one of the relations are performed.
C3: The list of relations in E2 must be certified to meet the separation of duty requirement.
E3: The system must authenticate the identity of each user attempting to execute a TP.
C4: All TPs must be certified to write to an append-only CDI (the log) all information necessary to reconstruct the operation.
C5: Any TP that takes a UDI as an input value must be certified to perform only valid transformations, for any possible value of the UDI. The TP will either accept (convert to CDI) or reject the UDI.
E4: Only the agent permitted to certify entities may change the list of such entities associated with other entities: specifically, those associated with a TP. An agent that can certify an entity may not have any execute rights with respect to that entity.

Business Intelligence Systems

According to one of the definitions, Business Intelligence systems are the information systems processing both enterprises data as well as externally acquired data and information, taking into account widely understood informational and analytical needs of that company and its environment [12].

In other words, the system is a set of tools, practices and methods aimed at collecting and integrating data in order to provide information and knowledge to decision-makers. It is important to deliver the information on time and in an appropriate manner.

For the needs of this research, the system performing the function of a telecommunications operator sales module was developed (presented on Figure 1). The authors assumed that the set of six basic transactions met the minimal needs of the operator. The implemented functionality enables the addition and modification data of customer data, services, employees, sale transactions, customer service transactions and also user's right change. Each of these transactions can be performed by users having one of six roles (such as *Sales Consultant*, *Manager*, *IT Consultant* etc.) in the system, which is appropriate for a particular action, in accordance with the Clark-Wilson model rules.

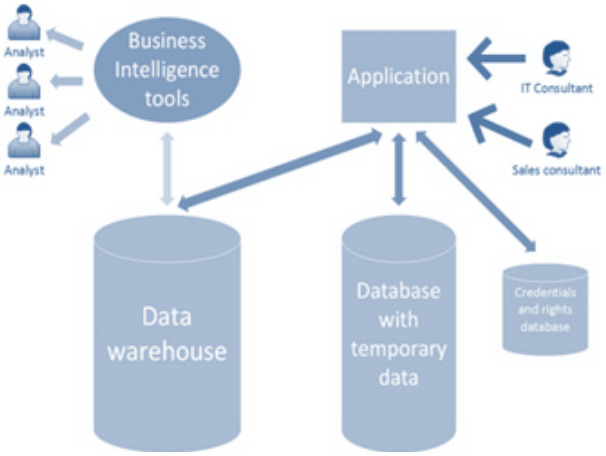

Figure 1. General architecture of system designed for research

Investigations and Results

Risk analysis was used to evaluate the security improvement obtained by applying the Clark-Wilson model. Risk analysis is part of the risk management process and includes the following activities [13]: identification and description of the environment, identification of threats, identification of vulnerabilities, identification of potential losses, risk assessment.

The risk analysis was performed using the L-RAC [13] methodology, including risk analysis and risk control. Having identified the threats and vulnerabilities (presented in Table 1), it is also required to estimate the realization probability of each threat.

Two approaches to risk analysis are possible: the quantitative method and qualitative method. Statistical data relating to the risks of a given period of time is necessary for the quantitative method. In the case of information systems, this approach is often impossible to apply, because when collecting data on specific threat, it is necessary to assume that the system and the environment around him is unchangeable which is not so in practice. As a result of the lack of historic data about the risks in this particular system, the qualitative approach was chosen. The examination was based on generally accepted ways of the estimation of the risk presented in the technical report ISO/IEC TR 13335-3 [14]. The quantitative method uses descriptive, arbitrarily chosen measures expressing the possibility of occurrence of a random event.

Table 1. Threats and vulnerabilities identified for the designed system

No.	Threat	Vulnerabilities	Consequences
1.	Unauthorized access to the system	The acquisition of user account passwords through phishing System access granted by the system administrator The acquisition of user passwords through wiretapping communication between the user interface and database	Loss of confidentiality
2.	Unauthorized activities of unauthorized persons	Anonymous addition, edition or acceptance of data not intended for the intruder	Loss of confidentiality, integrity and availability
3.	Unauthorized activities of system users	Anonymous addition, edition or acceptance of data not intended for the user	Loss of confidentiality, integrity
4.	Malicious operations by system users	Anonymous addition, edition or acceptance of invalid data	Loss of integrity
5.	System users mistake	Anonymous addition, edition or acceptance of incorrect data	Loss of integrity
6.	The interruption of data bases	Lack of program verification for inputted data	Loss of integrity and availability
7.	Granting privileges to unauthorized persons	Anonymous granting of privileges to unauthorized persons as a result of mistakes made by the supervisor Anonymous granting of privileges to unauthorized persons as a result of intentional misconduct of the supervisor	Loss of confidentiality and integrity

In order to assess the risks several assumptions were taken [1]:

1. The resources—the importance of data from a particular transaction for the system—was rated on a scale from low (0 point), medium (1 pt), high (2 pts).
2. Each type of threat and each group of the resources concerned by threats were assigned a measure of the level of:
   a) threat on a scale: low (L), medium (M), high (H),
   b) resource vulnerability on a scale: low (L), medium (M), high (H).
3. An arbitrary risk point integer scale between 0 and 6 was adopted (calculated by adding weight from assumptions 1, 2a and 2b).

For each threat, vulnerability and resource a measure from 0 to 2 was assigned (presented in Table 2) [1].

Table 3. Threats and vulnerabilities with measures assigned

No.	Threat	Level	Vulnerabilities	Level
1.	Unauthorized access to the system	M	The acquisition of user account passwords through phishing	L
			System access granted by the system administrator	M
			The acquisition of user passwords through wiretapping communication between the user interface and database	M
2.	Unauthorized activities of unauthorized persons	L	Anonymous addition, edition or acceptance of data not intended for the intruder	M
3.	Unauthorized activities of system users	L	Anonymous addition, edition or acceptance of data not intended for the user	M
4.	Malicious operations by system users	L	Anonymous addition, edition or acceptance of invalid data	M
5.	System users mistake	L	Anonymous addition, edition or acceptance of incorrect data	H
6.	The interruption of data bases	H	Lack of program verification for inputted data	M
7.	Granting privileges to unauthorized persons	H	Anonymous granting of privileges to unauthorized persons as a result of mistakes made by the supervisor	M
			Anonymous granting of privileges to unauthorized persons as a result of intentional misconduct of the supervisor	

As a result, the authors received a table (Table 3) containing risk points (with a 0 to 6 importance range) that concern the functionality of 'a basic system' without additional mecha-

nisms related to the Clark-Wilson model (in opposition to the System proposed in Figure 1).

Table 3. Risk points for system without Clark-Wilson Model; R – resource, T – threat, V – vulnerability, S – sum, n – n/a

	T	1	1	1	2	3	4	5	6	7	7
R	V	1	2	3	1	1	1	1	1	1	2
1	1	2	3	3	2	2	2	3	n	n	n
2	1	2	3	3	2	2	2	3	n	n	n
3	1	2	3	3	2	2	2	3	n	n	n
4	0	1	2	2	1	1	1	2	2	n	n
5	0	1	2	2	1	1	1	2	2	n	n
6	2	3	4	4	3	3	3	4	n	5	5
S	109	11	17	17	11	11	11	17	4	5	5

Considering security mechanisms contained within the Clark-Wilson model and some others related to this model that were successfully deployed in the System from, the results are presented in Table 4:

Table 4. Risk points for system with Clark-Wilson Model; R – resource, T – threat, V – vulnerability, S – sum, n – n/a

	T	1	1	1	2	3	4	5	6	7	7
R	V	1	2	3	1	1	1	1	1	1	2
1	1	2	2	2	1	1	1	1	n	n	n
2	1	2	2	2	1	1	1	1	n	n	n
3	1	2	2	2	1	1	1	1	n	n	n
4	0	1	1	1	0	0	0	0	0	n	n
5	0	1	1	1	0	0	0	0	0	n	n
6	2	3	3	3	2	2	2	2	n	4	4
S	61	11	11	11	5	5	5	5	0	4	4

The total amount of risk points after the usage of the Clark-Wilson model fell from 109 points to 61. The system neutralized one of the vulnerabilities, and significantly minimized 8 of the 9 remaining vulnerabilities.

Conclusions

The study showed how highly effective the Clark-Wilson model can be in the case of commercial systems. Most of the vulnerabilities which could be exploited by threats causing the violation of the integrity of the data warehouse was been eliminated or reduced. The study was conducted in order to examine the impact of the Clark-Wilson model application in a real business intelligence system with previously estimated risk points. With the list of 10 vulnerabilities having impact on the realization of selected threats, lowering the risk of execution or total liquidation was observed for 9 of them, representing 90% of vulnerabilities. Results in the vast majority are caused directly by implementation of the Clark-Wilson model. Importantly, the application of these rules, in addition to purely programmatic mechanisms, increases the awareness of personal responsibility for mistakes and abuses. Analysis of the results shows that the most important security rules include: the division of transactions to at least two steps and scrupulous log of every change made within data in the system. The first mechanism, in addition to verification of the data editing process, and also in combination with the second one has a psychological significance. None of the people will want to take responsibility for acceptance of abuse. The mechanisms also increase security against any case of unauthorized access or unauthorized alteration by an authorized user of the system, because it cannot result in any change to the end of the process, without the cooperation with the other person. Logging all events in the system can also be helpful in case of an ordinary incident. It allows to error diagnoses and enables its fast correction.

References

[1] Buława P.: Implementation and evaluation of the effectiveness of Clark-Wilson data security model on the example of real Business Intelligence system; Master Thesis, 2015.

[2] Liderman K., Bezpieczeństwo informacyjne, Wydawnictwo Naukowe PWN SA, 2012.

[3] Molski M., Opala S., Elementarz bezpieczeństwa systemów informatycznych, MIKOM, 2002

[4] Kenan K., Cryptography in the database: The last line of defence, Pearson Education, Inc 2006

[5] Anderson R., Security Engineering, Wiley, 2001

[6] United States Departement of Defense, Trusted Computer System Evaluation Criteria (The Orange Book), 1983, 1985

[7] Brewer D. F. C., Nash M.J., The Chinese Wall Security Policy, Proceedings of IEEE Symposium on Security and Privacy, 1989

[8] Ferraiolo D. F., Kuhn D. R., Role Based Access Controls, 15th National Computer Security Conference, 1992

[9] Ferraiolo D. F., D. Kuhn D. R., Chandramouli R., Role-based Access Control, Artech House, 2003

[10] Krause M., Tipton H.F., Handbook of information security management, CRC Press LLC, 1997

[11] Clark D., Wilson D., A Comparison of Commercial and Military Computer Security Policies. Proc. IEEE Symposium on Research in Security and Privacy, 1987.

[12] Sierocki R., Przegląd koncepcji systemów informatyczno-analitycznych przedsiębiorstw. [W:] Nowoczesne technologie informacyjne w zarządzaniu., Prace Naukowe AE we Wrocławiu nr 1044, Wrocław, s. 295., 2004.

[13] Liderman K., Analiza ryzyka i ochrona informacji w systemach komputerowych, Wydawnictwo Naukowe PWN SA, 2008.

[14] ISO/IEC TR 13335-3:1997—Guidelines for the Management of IT Security—Part 3: Techniques for the Management of IT Security.

Authors

M.Sc. Eng. Paweł BUŁAWA

Graduated the Faculty of Electronics and Information Technology at Warsaw University of Technology (WUT), Poland, received his MSc in 2015. His professional interests include IT security and database systems.

Ph.D. Marcin KOWALCZYK

works as an Assistant Professor in the Institute of Telecommunications in the Warsaw University of Technology (WUT), Poland. He graduated the Faculty of Electrical Engineering, Automatic Control and Computer Science of the Kielce University of Technology and PhD studies at Faculty of Electronics and Information Technology at the WUT, where he received his PhD in 2010. His professional interests include optical communications, microwave electronics and database systems. He is author or co-author more than 50 scientific papers.