Clark-Wilson Security Integrity model

Franck Jeannot

Montréal, Canada, Mai 2019, U612, v1.0

Abstract

A review of Clark-Wilson Security Integrity model.

Keywords: Biba, Clark-Wilson, integrity verification procedures IVP, separation of duty, unconstrained data item UDI, Transformation Procedures, Well formed transactions

1. Introduction

The main integrity security models suggest different approaches to achieving computer integrity : *Biba (1977), Goguen and Meseguer (1982), Sutherland (1986),* ***Clark and Wilson*** *(1987-1989), and Brewer and Nash (1989).* Three of these models (Goguen and Meseguer's, Sutherland's, and Brewer and Nash's) were not originally intended as integrity models [1].

The Clark-Wilson model was developed to address security issues in commercial environments and, according to Dhillon (2007), « *is based on the assumption that bookkeeping in financial institutions is the most important integrity check*[2]. » The model uses two categories of mechanisms to realize **integrity** : **well-formed transactions** and **separation of duty**.

This integrity model provides a foundation for specifying and analyzing integrity policies for network enterprise systems. The **Clark and Wilson** model [3] is not stated in formal mathematical terms like the others, but formal axioms are not necessary to compare the advantages and disadvantages of each model. The core parts of this model involves transactions between systems. Integrity is addressed through the following **three goals** [3] :

1. Prevention of the modification of information by unauthorized users.

1. Source : Mayfield-1991, [1], par. 5.1 INTEGRITY MODELS, p 70
2. Source : Dhillon-2007, [2], p 37
3. Source : Summers-1997, [4], p 142 ; from [5]

2. Prevention of the unauthorized or unintentional modification of information by authorized users.
3. Preservation of the internal and external consistency

The Clark-Wilson model improves on *Biba* by focusing on integrity at the transaction level and addressing three major goals of integrity in a commercial environment. In addition to preventing changes by unauthorized subjects, Clark and Wilson realized that high-integrity systems would also have to prevent undesirable changes by authorized subjects and to ensure that the system continued to behave consistently. It also recognized that it would need to ensure that there is constant mediation between every subject and every object if such integrity was going to be maintained.

2. Definition

According to *De Capitani di Vimercati (2011)*, « *The Clark and Wilson model protects the integrity of commercial information by allowing only certified actions by explicitly authorized users on resources.* [6] »

3. Transformation Procedures

Clark and Wilson (1987) **Transformation Procedures (TP)** comprise a software-based access control mechanism. Clark and Wilson introduced Transformation Procedures to automate the concept of the well-formed transaction. The access privileges of a Transformation Procedure are determined external to the secure system and encoded in an access control triple of the form : (UserID, TPi, (CDIa, CDIb, CDIc, ...)), which relates a user, a Transformation Procedure, and the data objects that a Transformation Procedure may reference on behalf of that user. It appears that type enforcement and Transformation Procedures are quite similar ;both constrain access of a process to a storage object based on security attributes [4].

4. Principle of well-formed transaction

The principle of well-formed transaction is defined as a transaction where the user is unable manipulate data arbitrarily, but only in constrained (limitations or boundaries) ways that preserve or ensure the integrity of the data. A security system in which transactions are well-formed ensures that only legitimate actions can be

4. Source : Abrams-1995 [7], p 4/7

executed. Ensures the internal data is accurate and consistent to what it represents in the real world[5].

5. Separation of duty

The Clark-Wilson model was extended to cover separation of duty in 1993[6].

6. Mandatory access control

Like the Bell-Lapadula model for confidentiality, the Clark-Wilson Model is an example of MAC for integrity[7]. However, as per Prof. E. Stewart Lee - 1999 "*The Clark-Wilson integrity mechanisms differ in a number of important ways from the mandatory controls for military security as described in the Orange Book*" [11].
Dhillon (2007) also confirm « *...the model does impose a form of mandatory access control, but not as restrictive as the no read and no write down criteria of...*[8] ». In their original paper (Clark-Wilson-1987) state « *...understand that the mechanisms described in the previous section, in some respects, are mandatory controls.* » [3]

7. Data items and Model

In Clark-Wilson, each datum in the system is classified as either a *constrained data item* (**CDI**) or an *unconstrained data item* (**UDI**). CDIs must be protected, whilst UDIs are conventional data objects whose integrity is not assured under the model. No datum can be in both classes :

$$Data = CDI \cup UDI \wedge CDI \cap UDI = \varnothing \tag{1}$$

Operations on CDIs are performed by **TP**s and integrity verification procedures (**IVP**s). There are a set of requirements which the CDI can be processed in accordance to. Also, in order to enforce the sense of separation of duties, users may only invoke some Transformation Procedures ans a pre-specified set of data objects (or CDIs), as ther duties see fit.
The four requirements of this particular model are as follows :

1. The system must separately identify and authenticate every user

5. Source : The Clark-Wilson Security Model by Sonya Q. Blake (May 17, 2000)
6. Source : Ge-2004 [8], par. 2.1 The Clark-Wilson model, p 5 ; [9]
7. Source : Rakkay-2009 [10], p 31
8. Source : Dhillon-2007 [2], p 38

2. The system must ensure that specified data systems can be manipulated only by restricted set of programs, and the data center controls must ensure that these programs meet the *well-formed transaction rules* which have already been identified as Transformation Procedures.
3. The system must associate with each user a valid set of programs to be run, and the data center must ensure that these sets meet the separation-of-duty rule.
4. The system must maintain and auditing log that records every program executed, and the name of the authorizing user.

8. Rules

The model consists of two sets of rules : **Certification Rules** (C) and **Enforcement Rules** (E) [9] .There are nine rules that ensure the external and internal integrity of the data items (C1 to C5 and E1 to E4) [3] [12].

Références

[1] Mayfield, Terry and E. Roskos, J and R. Welke, Stephen and M. Boone, John and W. McDonald, Catherine, Integrity in Automated Information Systems (09 1991).
URL http://www.csirt.org/color_%20books/C-TR-79-91.pdf

[2] Dhillon, G., Principles of information systems security: text and cases, John Wiley & Sons, 2007 (2007).
URL https://books.google.ca/books?id=mTkkAQAAIAAJ

[3] D. D. Clark, D. R. Wilson, A comparison of commercial and military computer security policies, 1987, pp. 184–195 (04 1987). doi:10.1109/SP.1987.10001.
URL https://groups.csail.mit.edu/ana/Publications/PubPDFs/A%20Comparison%20of%20Commercial%20and%20Military%20Computer%20Security%20Policies.pdf

[4] Summers, C Rita, Computer security : threats and safeguards (1997).

[5] Nikolai Bezroukov, The clark-wilson information integrity model (2018).
URL http://www.softpanorama.org/Access_control/Security_models/clark_wilson.shtml

9. https://en.wikipedia.org/wiki/Clark%E2%80%93Wilson_model#Rules

[6] S. De Capitani di Vimercati, P. Samarati, Clark and Wilson Model, Springer US, Boston, MA, 2011, pp. 208–209 (2011). doi:10.1007/978-1-4419-5906-5_814.
URL https://doi.org/10.1007/978-1-4419-5906-5_814

[7] D. Abrams, Marshall and V. Joyce, Michael, Trusted system concepts, Computers and Security 14 (1995) 45–56 (12 1995). doi:10.1016/0167-4048(95)97025-6.
URL https://www.acsac.org/secshelf/papers/trusted_system_concepts.pdf

[8] Ge, Xiaocheng and Polack, Fiona and Laleau, Régine, Secure Databases: An Analysis of Clark-Wilson Model in a Database Environment, in : A. Persson, J. Stirna (Eds.), Advanced Information Systems Engineering, Springer Berlin Heidelberg, Berlin, Heidelberg, 2004, pp. 234–247 (2004). doi:10.1007/978-3-540-25975-6_18.
URL http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.65.1843&rep=rep1&type=pdf

[9] Abrams, Marshall D. and Amoroso, Edward G. and Lapadula, Leonard J. and Lunt, Teresa F. and Williams, James G., Report of an integrity research study group, Comput. Secur. 12 (7) (1993) 679–689 (Nov. 1993). doi:10.1016/0167-4048(93)90085-J.
URL http://dx.doi.org/10.1016/0167-4048(93)90085-J

[10] Rakkay, Hind, Approches formelles pour la modélisation et la vérification du contrôle d'accès et des contraintes temporelles dans les systèmes d'information (01 2009).
URL https://publications.polymtl.ca/123/1/2009_HindRakkay.pdf

[11] Ernest Stewart Lee, Essays about computer security, University of Cambridge Computer Laboratory (1999) 181 (1999).
URL https://www.cl.cam.ac.uk/~mgk25/lee-essays.pdf

[12] Welch, Ian, Reflective enforcement of the clark-wilson integrity model (05 2019).
URL https://www.researchgate.net/publication/247375119_Reflective_Enforcement_of_the_Clark-Wilson_Integrity_Model