Brewer and Nash security model

Franck Jeannot

Montréal, Canada, Janvier 2019, P460.BN, v1.0

Abstract

A review of Brewer and Nash security model (1989) and some later improvements.

Keywords: ACWSP: Aggressive Chinese Wall Security Policy, Brewer, Conflict Of Interest (COI), Conflict of Interest binary Relation (CIR), CWSP, Information flow, Lattice model, Nash, Chinese Wall, policy

1. Introduction

The **Brewer and Nash** [1] model was constructed to provide information security access controls that can change dynamically. This security model, also known as the **Chinese wall model** was designed to provide controls that mitigate **Conflict Of Interest** (COI) in commercial organizations, and is built upon an information flow model.

2. Brewer and Nash Model

In the Brewer and Nash Model, no information can flow between the subjects and objects in a way that would create a conflict of interest. This security policy was proposed initially to capture certain requirements in UK's financial sector.

It is a real commercial policy which can be formally modeled. Its basic idea is to keep company information confidential and prevent it from unauthorized access of consulting services.

This model, similar to the **Bell-LaPadula model**, allows dynamically changing permissions based on rule based assess control (based on a user's past activity). In this model, we have a wall, which segregates data types and we have a set of rules

[1] Dr. Mike Nash and Dr. David Brewer joined together in 1988 to create *Gamma Secure Systems Limited* http://www.gammassl.co.uk/corporate/index.php

that determine what subjects can access on the other side of the wall. These dynamic rules can change as the user accesses different information.

It is based on the information flow model, where no information can flow between subjects and objects in a way that would result in a conflict of interest. The model states that a subject can write to an object if, and only if, the subject can not read another object that is in a different data set.

This model combines elements of Discretionary Access Control (**DAC**) and Mandatory Access Control **MAC** but initially Brewer and Nash formalized the Chinese Wall policy in terms of a mandatory computer security model.

3. The Chinese Wall policy

The chinese wall policy builds on three level of abstraction :

- Objects : contain information about only one company (for example : files)
- Company groups : collect all objects concerning a particular company
- Conflict classes : cluster the groups of objects for competing

The essentials elements are :

- Subjects: Active entities accessing protected objects
- Objects: Data organized according to 3 levels (Information; DataSet; Conflict-of-Interest (CoI) classes)
- Access Rules: Read rule, Write rule
- Read Rule: Subject S can read object O only if O is from the same company information as some object read by S, or O belongs to a COI class within which S has not read any object.
- Write Rule: Subject S can write object O only if S can read O by the Brewer-Nash Read rule, and no object can be read which is in different company dataset to the one for which write access is requested.

The Chinese Wall Policy is a combination of free choice and mandatory control. Initially a subject is free to access any object it wishes. Once the initial choice is made, a Chinese Wall is created for that user around the dataset to which the object belongs.

This model:

- Dynamically assembles ACLs based on the objects that a subject accesses
- Is built upon an information flow model
- Restricts information from flowing in a way that would create a conflict of interest.

In this model, a subject with access to one company's data is not allowed to access a competitor's data.

4. Model improvements and variants

The *Chinese Wall* policy was first introduced by Brewer and Nash in 1989 [1].

The same year, Lin [2] announced a new model (ACWSP: Aggressive Chinese Wall Security Policy) to fix the errors of the Brewer-Nash model. The error being that the conflict of interest is a binary relation conflict of interest, and not an equivalence class (partitions).

In 1990, Meadows [3] published an extension of the Brewer-Nash Model to a Multilevel Context.

In 1992, Foley [4] proposed a variety of approaches for implementing Chinese Wall policies using multilevel techniques.

In 1992 and 1993, Sandhu [5] [6], improved upon this model by making a clear distinction between users, principals, and subjects, defines a **lattice-based security structure**, and shows how the Chinese Wall Policy complies with the Bell-Lapadula model (which was erroneously indicated not feasible in the Brewer-Nash initial model).

In 1996, Foley [7] proposed solutions to the implementation of a wide variety of different security policies in Unix with the *set-user-id* facility including the chinese wall policy.

In 2001, Atluri et al. [8] proposed an updated model for Decentralized Workflow Systems.

In 2002, Lin [9] published an analysis of Symmetric Binary Relations in the context of the Chinese Wall model.

In 2003, Lin [10] updated the ACWSP, specially with the notion of granulation.

In 2003, Hung [11] proposed solutions to apply the Chinese Wall policy to Web services.

In 2004, Minsky [12] proposed and updated model for a decentralized treatment of a highly Distributed chinese wall policy.

In 2004, Atluri et al. [13] proposed a decentralized control of workflows called *Decentralized workflow Chinese wall security model.*

In 2005, Loock and Eloff [14] proposed a new model of Chinese Wall Security Policy model, for a data mining environment.

In 2007, Lin provided [15] a short proof of a revisited version of the chinese wall.

In 2007, Kapadia et al. [16] proposed a discretionary access control framework based on the chinese wall model, but for distributed environments

In 2009, Gupta [17] proposed and update of the Chinese wall model for cloud computing.

In 2013, a less restrictive Chinese Wall policy was proposed by Sharifi and Tripunitara [18].

In 2015, Fehis et al. [19] proposed a new chinese wall security policy model based on the subject's wall and object's wall

In 2015, Crampton and Sellwood [20] proposed The relationships, paths and principal matching model (RPPM) that supports **separation of duty** and **Chinese Wall**.

References

[1] D. F. C. Brewer, M. J. Nash, The Chinese Wall Security Policy., in: IEEE Symposium on Security and Privacy, IEEE Computer Society, 1989, pp. 206–214. doi:10.1109/SECPRI.1989.36295.
URL http://dblp.uni-trier.de/db/conf/sp/sp1989.html#BrewerN89

[2] T. Y. Lin, Chinese wall security policy-an aggressive model, in: Fifth Annual Computer Security Applications Conference, ACSAC 1989, 4-8 December, 1989, Westward Look Resort, Tucson, Arizona, USA, 1989, pp. 282–289. doi:10.1109/CSAC.1989.81064.
URL https://doi.org/10.1109/CSAC.1989.81064

[3] C. A. Meadows, Extending the brewer-nash model to a multilevel context, in: Proceedings of the 1990 IEEE Symposium on Security and Privacy,Oakland, California, USA, May 7-9, 1990, 1990, pp. 95–103. doi:10.1109/RISP.1990.63842.
URL https://doi.org/10.1109/RISP.1990.63842

[4] S. N. Foley, Aggregation and separation as noninterference properties, J. Comput. Secur. 1 (2) (1992) 159–188.
URL http://dl.acm.org/citation.cfm?id=2699868.2699871

[5] R. S. Sandhu, Lattice-based enforcement of Chinese Walls, Computers & Security 11 (8) (1992) 753–763. doi:10.1016/0167-4048(92)90131-A.
URL https://doi.org/10.1016/0167-4048(92)90131-A

[6] R. S. Sandhu, Lattice-Based Access Control Models, Computer 26 (11) (1993) 9–19. doi:10.1109/2.241422.
URL https://doi.org/10.1109/2.241422

[7] S. Foley, Building chinese walls in standard unix, in: In Supplement to the Proceedings of the 1996 IEEE Symposium on Security and Privacy (Five-Minute, 1996.

[8] V. Atluri, S. A. Chun, P. Mazzoleni, A Chinese Wall Security Model for Decentralized Workflow Systems, in: Proceedings of the 8th ACM Conference on Computer and Communications Security, CCS '01, ACM, New York, NY, USA, 2001, pp. 48–57. doi:10.1145/501983.501991.
URL http://doi.acm.org/10.1145/501983.501991

[9] T. Y. Lin, Placing the chinese walls on the boundary of conflicts - analysis of symmetric binary relations, in: 26th International Computer Software and Applications Conference (COMPSAC 2002), Prolonging Software Life: Development and Redevelopment, 26-29 August 2002, Oxford, England, Proceedings, 2002, pp. 966–974. doi:10.1109/CMPSAC.2002.1045131.
URL https://doi.org/10.1109/CMPSAC.2002.1045131

[10] T. Y. Lin, Chinese Wall Security Policy Models: Information Flows and Confining Trojan Horses, in: Data and Applications Security XVII: Status and Prospects, IFIP TC-11 WG 11.3 Seventeenth Annual Working Conference on Data and Application Security, August4-6, 2003, Estes Park, Colorado, USA, 2003, pp. 275–287. doi:10.1007/1-4020-8070-0_20.
URL https://doi.org/10.1007/1-4020-8070-0_20

[11] P. C. K. Hung, G. Qiu, Specifying conflict of interest assertions in ws-policy with chinese wall security policy, SIGecom Exchanges 4 (1) (2003) 11–19. doi:10.1145/844357.844362.
URL http://www.sigecom.org/exchanges/volume_4/4.1-Hung.pdf

[12] N. H. Minsky, A Decentralized Treatment of a Highly Distributed Chinese-Wall Policy, in: POLICY, IEEE Computer Society, 2004, pp. 181–184.

[13] V. Atluri, S. A. Chun, P. Mazzoleni, Chinese wall security for decentralized workflow management systems, Journal of Computer Security 12 (6) (2004) 799–840.
URL http://content.iospress.com/articles/journal-of-computer-security/jcs217

[14] Loock, Eloff, A new Access Control model based on the Chinese Wall Security Policy Model (2005).
URL https://www.researchgate.net/publication/220803268_A_new_Access_Control_model_based_on_the_Chinese_Wall_Security_Policy_Model

[15] T. Y. Lin, Chinese wall security policy-revisited a short proof, 2007 IEEE International Conference on Systems, Man and Cybernetics (2007) 3027–3028.

[16] A. Kapadia, P. Naldurg, R. H. Campbell, Distributed enforcement of unlinkability policies: Looking beyond the chinese wall, in: 8th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2007), 13-15

June 2007, Bologna, Italy, 2007, pp. 141–150. doi:10.1109/POLICY.2007.16.
URL https://www.cs.indiana.edu/~kapadia/papers/policy07.pdf

[17] Gupta, Chinese Wall Security Policy (2009).
URL https://scholarworks.sjsu.edu/cgi/viewcontent.cgi?referer=https://www.google.ca/&httpsredir=1&article=1053&context=etd_projects

[18] A. Sharifi, M. V. Tripunitara, Least-restrictive Enforcement of the Chinese Wall Security Policy, in: Proceedings of the 18th ACM Symposium on Access Control Models and Technologies, SACMAT '13, ACM, New York, NY, USA, 2013, pp. 61–72. doi:10.1145/2462410.2462425.
URL https://www.researchgate.net/publication/262364319_Least-restrictive_enforcement_of_the_Chinese_wall_security_policy

[19] S. Fehis, O. Nouali, T. Kechadi, A new Chinese wall security policy model based on the subject's wall and object's wall, in: 2015 First International Conference on Anti-Cybercrime (ICACC), 2015, pp. 1–6. doi:10.1109/Anti-Cybercrime.2015.7351943.
URL https://www.insight-centre.org/sites/default/files/publications/16.016_fehis-saad-ieee-paper_final-2015.pdf

[20] J. Crampton, J. Sellwood, Relationships, Paths and Principal Matching: A New Approach to Access Control, arXiv e-prints (2015) arXiv:1505.07945arXiv:1505.07945.