Chapter X

Chinese Wall Security Policy Model: Granular Computing on DAC Model

Tsau Young Lin, San Jose State University, USA

Abstract

In 1989, Brewer and Nash (BN) proposed the Chinese Wall Security Policy (CWSP). Intuitively speaking, they want to build a family of impenetrable walls, called Chinese walls, among the datasets of competing companies so that no datasets that are in conflict can be stored in the same side of Chinese walls. Technically, the idea is: \((X, Y) \notin CIR \) (\(=\) the binary relation of conflict of interests) if and only if \((X, Y) \notin CIF \) (\(=\) the binary relation of information flows). Unfortunately, BN’s original proof has a major flaw (Lin, 1989). In this chapter, we have established and generalized the idea using an emerging technology, granular computing.
Introduction

Recent events, such as e-commerce and homeland security, have prompted us to revisit the idea of the Chinese Wall Security Policy Model (Lin, 2001). “The Chinese wall policy combines commercial discretion with legally enforceable mandatory controls...perhaps, as significant to the financial world as Bell-LaPadula’s policies are to the military” (Bell, 1987, p. 000). This is asserted in the abstract of Brewer and Nash’s (BN’s) (1989) article. It is still valid today.

Background

Chinese Wall Security Policy (CWSP) Model

Let us start with recalling the proposal of Brewer and Nash (BN). In 1989, BN proposed a very intriguing commercial security model, called Chinese Wall Security Policy (CWSP) Model. Intuitively speaking, the idea was to build a family of impenetrable walls, called Chinese walls, among the datasets of competing companies so that no datasets that are in conflict can be stored in the same side of Chinese walls. The intent of the proposal was a good one. In their model, BN assumed the set $O$ of corporate datasets could be partitioned into pairwise disjoint subsets, called conflict of interest (CIR) classes. Such a collection of pairwise disjoint subsets is referred to in mathematics as a partition and is known to induce an equivalence relation and vice versa (see for example, Brualdi, 1992). So, BN has assumed CIR is an equivalence relation that is a reflexive, symmetric, and transitive binary relation. Considering the real-world meaning, would conflict be reflexive? Appealing to common sense, there is no dataset that is self-conflict, so CIR is unlikely an equivalence relation. Observing this fact, in the same year, we presented a modified model at the Aerospace Computer Security Application Conference; the model was called Aggressive Chinese Wall Security Policy (ACWSP) model (Lin, 1989b). In that paper, we did not bring out the essential strength of the ACWSP model. A relatively inactive decade has passed. Due to the recent development of granular computing, we refined the idea of ACWSP and successfully captured the intuitive intention of BN theory and outlined it in COMPSAC and RSCTC (Lin, 2002a, b). Though the collection of CIR-classes is not a partition, it
Related Content

Integration Stages of Project Risk Management (PRM) into Enterprise Risk Management (ERM)

Trust Models for Ubiquitous Mobile Systems
[www.irma-international.org/chapter/trust-models-ubiquitous-mobile-systems/23168/](www.irma-international.org/chapter/trust-models-ubiquitous-mobile-systems/23168/)

A Mark-Up Language for the Specification of Information Security Governance Requirements
Anirban Sengupta and Chandan Mazumdar (2013). *Privacy Solutions and Security Frameworks in Information Protection* (pp. 103-123).
[www.irma-international.org/chapter/mark-language-specification-information-security/72740/](www.irma-international.org/chapter/mark-language-specification-information-security/72740/)

Security Issues and Possible Countermeasures for a Mobile Agent Based M-Commerce Application
[www.irma-international.org/chapter/security-issues-possible-countermeasures-mobile/23220/](www.irma-international.org/chapter/security-issues-possible-countermeasures-mobile/23220/)
Enhanced Security for Electronic Health Care Information Using Obfuscation and RSA Algorithm in Cloud Computing
International Journal of Information Security and Privacy (pp. 59-69).