Chapter 2.30
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) ∉ CIR (= the binary relation of conflict of interests) if and only if (X, Y) ∉ 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 is a binary granulation.* Roughly, a binary granulation of U is a collection of subsets, called granules, that is not quite a partition but the set of the center (or core) of each granule forms a partition; see the main text below. In terms of binary granulation, we can capture the spirit of Chinese wall security policy (CWSP). The methodology is more than CWSP; it has profound impacts on the analysis of information flow in DAC.

With mild assumptions on DAC (Discretionary Access Control) model, we can actually regulate *malicious* Trojan horses so that information, no matter how it flows, will not flow into "enemy" hands; it will flow only among "friends".

Granular Computing

Mathematically, DAC model has a structure, that is, a subset of binary neighborhood systems (BNS), or binary granulations (Lin, 1988, 1989a, 1998a). Seymour Ginsburg observed that this is a list structure (verbally 1989); however, we have not used the list structure because a list may involve linear ordering. The study of such a structure has gained much attention recently and is named granular computing. It has originated from four facets: Let us speak in the chronological order. The first one is Hsiao. In his attribute based database model, Hsiao clustered the attribute domain into semantically related granules (equivalence classes) (Demurjian & Hsiao, 1988; Hsiao & Harary, 1970; Lin, 1992; Wong & Chiang, 1971). Clustering is an important technique in database theory; it partitions a dataset such that semantically related data are stored in physical proximity. The second one, probably the deepest one, is used in the design of fuzzy logic control systems. It decomposes the input space into finite fuzzy granules (Lin, 1996, 1997). The explicit discussion of such a notion of granularity, scientifically (for a different purpose), is in the article of Zadeh (1979) and, more recently, in (Zadeh, 1998, 2002). The third groups are from the theory of data. Pawlak (1982) and Lee (1983) nearly simultaneously observed independently that attributes of a relation induce partitions on the set of entities (Pawlak, 1982; Lee, 1983) and studied relational tables from such observations. Pawlak called his idea rough set theory, while Lee called his study algebraic theory of relational databases. The last faucet comes from approximate retrieval (Chu & Chen, 1992; Lin, 1988, 1989a; Motro, 1986). For developing a theory of approximate retrieval in databases, Motro, in essence, introduced the notion of metric space into databases. We observed that the notion of metric spaces does not naturally exist in a data model, so we imported the notion of (pre-) topological spaces into the attribute domains and called them neighborhood systems