IRM PRESS
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.irm-press.com
ITB11706

This chapter appears in the book, *Web and Information Security*
edited by Elena Ferrari and Bhavani Thuraisingham © 2006, Idea Group Inc.

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) ∉ 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.

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

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*

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/chinese-wall-security-policy-model/31089

Related Content

TCP/IP Reassembly in Network Intrusion Detection and Prevention Systems
Xiaojun Wangand Brendan Cronin (2014). *International Journal of Information Security and Privacy (pp. 63-76).*
www.irma-international.org/article/tcpip-reassembly-in-network-intrusion-detection-and-prevention-systems/136366

Merkle Tree Authentication in UDDI Registries
Elisa Bertino, Barbara Carminatiand Elena Ferrari (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications (pp. 1321-1338).*
www.irma-international.org/chapter/merkle-tree-authentication-uddi-registries/23160

How Private Is Your Financial Data?: Survey of Authentication Methods in Web and Mobile Banking
Vidya Mulukutla, Manish Guptaand H. R. Rao (2017). *Identity Theft: Breakthroughs in Research and Practice (pp. 327-357).*
www.irma-international.org/chapter/how-private-is-your-financial-data/167234

Data-Embedding Pen
Seiichi Uchida, Marcus Liwicki, Masakazu Iwamura, Shinichiro Omachiand Koichi Kise (2013). *Multimedia Information Hiding Technologies and Methodologies for Controlling Data (pp. 396-411).*
www.irma-international.org/chapter/data-embedding-pen/70298

Blockchain Technology: Concepts, Components, and Cases
Somayya Madakamand Harshita (2021). *Industry Use Cases on Blockchain Technology Applications in IoT and the Financial Sector (pp. 215-247).*
www.irma-international.org/chapter/blockchain-technology/273817