OPPORTUNITIES AND CHALLENGES IN TRACING SECURITY BREACHES

Michael Gertz
Department of Computer Science, University of California at Davis, USA
gertz@cs.ucdavis.edu

Abstract: The closing session of the working conference was a panel discussion on challenges and recent developments in tracing security breaches of information systems that manage mission critical data. The panel members were (in alphabetical order): Cristina Buchholz (SAP, Germany), Michael Gertz (University of California at Davis, USA; panel chair) Sushil Jajodia (George Mason University, USA), Fred de Koning (Nyenrode University, The Netherlands), Leon Strous (De Nederlandsche Bank NV, The Netherlands).

Key words: Auditing, internal control, integrity

1. INTRODUCTION

In the area of (multi)database systems where data "flows" through different system components, the notion of *data provenance* has recently gained quite a lot of attention [1]. Data provenance is concerned with the development and realization of models to determine where a piece of data came from and the process by which it arrived in the database.

The idea of data provenance can naturally be applied in the context of data integrity. That is, given an information system managing mission critical data, one might be interested in why and how a certain piece of data got into or has been deleted from the database. Assume, for example, a scenario where a security breach has been identified based on some (missing) data in a database and the (missing) data clearly indicates a violation of data integrity (e.g., the data is plain wrong or anomalous). One

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35693-8_16
M. Gertz (ed.), *Integrity and Internal Control in Information Systems V*

important task of IT security personnel then is to determine the cause of the integrity violation. More precisely, it needs to be determined who is responsible for the possibly corrupted data and through which process the data entered the system (or has been deleted). This task is crucial in order to identify possible system vulnerabilities and to tighten the security of the system to avoid such integrity violations in the future.

The task of this panel was to identify models and techniques that are either already in place or need to be developed in order to address the issue of tracing security breaches such as the one described above. The following section outlines how the panel members viewed this problem and what techniques and requirements they identified in order to deal with this business security challenge.

2. DISCUSSION

The panel discussion included the presentation of specific real world scenarios as well as models and techniques that help dealing with tracing security breaches. The first scenario, presented by Leon Strous, was taken from the banking environment where debit card transactions play a major and crucial part of a bank's business. Of particular concern in this context are so called "ghost withdrawals or payments", that is, bank transactions that have been authorized and processed but have been denied by the cardholder. Such cases typically occur when a debit card has been stolen and the person who obtained the card was also able to obtain the cardholder's PIN number. A particularly interesting aspect of such a scenario is that in different countries, a different entity (i.e., either bank or cardholder) has to prove his right.

All panel members agreed on the observation that only log information maintained by different information systems components involved in processing the transaction is not sufficient to justify a decision on whether or not the transaction in question is a ghost transaction (besides the fact that the cardholder does not have direct access to this information). What is needed and is already in place, e.g., at some ATMs, are cameras or other types of sensoring techniques that help prove the case for either the cardholder or the bank. Such additional information is considered to be essential in order to better facilitate tracing such types of security breaches.

Another scenario given by Fred de Koning was an inventory management system where the current stock of a collection of items is supposed to be fully managed by an information system. Security breaches violating the integrity of the recorded data (typically number of items in stock) is often

not identified until a manual or automated count of items in stock and the comparison of the obtained numbers with those recorded in the database. In case there is an inconsistency among numbers, typically indicating that items, which are supposed to be in stock, are missing. Such items may have been stolen, their stock has purposely misreported, or miscalculated by the information system. Naturally, it is crucial for a company to trace back such integrity violations and to install mechanisms that prevent similar violations in the future. Since often humans are involved in processing items and stock numbers, it was the opinion of the panel members that in order to better facilitate the tracing of such security breaches, not only procedures need to be in place that frequently re-check stock numbers but also standard procedures (which ideally can be fully automated and/or monitored) by which humans and automated workflows have to process data.

After these specific real world scenarios, Sushil Jajodia presented a model that focuses on the accountability control objective in information systems. Obviously, accountability is an important factor in tracing security breaches and needs to be supported and implemented appropriately within the information system infrastructure. The proposed model, which is based on an apporach presented in [2], focuses in particular on audit trails as a mechanism for a complete reconstruction of every action taken against a database. More precisely, the model is concerned with modeling (1) who initiated a transaction, where and when; (2) the exact transactions and all its constituents; and (3) the data before the transaction and after the transaction. The core idea underlying the model is to record with every modification to the data the transaction time (to order every operation against a data item) and a valid time (to timestamp values of data items with their periods of validity in the real world). The second time dimension is different from the first one since an earlier value may be corrected later in time. Such a model naturally supports recording the whole history of data items, both in terms of their validity and when they have been modified. Database relations that incorporate both time dimensions are called bitemporal relations.

Obviously, this model supports tracing of the whole history of data items. A major challenge in fully utilizing this model in a complex information system infrastructure will be the correlation of data items and their time dimensions in case data items are moved from one component (database) to another through complex transactions. In this case, (perhaps heterogeneous) relations from different databases need to be correlated in order to fully obtain the path a data item took through the system.

The role of security and the aspect of tracing security breaches in particular were illustrated by Cristina Buchholz in the context of a Web

services infrastructure employed by SAP. The identification and tracing of integrity violations poses a major challenge in such an infrastructure since many components (in this case Web services and database backends) interact with each other through various channels. A solution to this challenge is the so called collaborative audit framework, which employs a logically centralized audit warehouse that manages audit data from diverse system components in the architecture.

Such a warehouse, in combination with the bitemporal relation approach described above, seems to provide a rich and useful framework for tracing data items and possible security breaches. Again, the challenge is to appropriately correlate (bitemporal) audit data and to eventually identify vulnerabilities in the information system infrastructure.

3. CONCLUSIONS

As the scenarios presented in this panel discussion indicated, there is a strong need for models and techniques to identify and trace security breaches in complex information system infrastructures managing mission critical data. A major challenge in achieving these objectives is not only an extensive auditing framework that allows monitoring and recording all types of transactions (including transaction environments) but also the correlation of audit records that perhaps originate from different system components. What is needed and thus provides an appropriate basis for developing respective models and techniques is an iterative framework to set up tracing mechanisms. The panel identified these aspects as important research and development issues industry will benefit from and thus should be actively pursued by academia and industry.

REFERENCES

[1] Buneman, P., Khanna, S., and Tan, W.-C.: Why and Where: A Characterization of Data Provenance. In *Database Theory - ICDT 2001, 8th International Conference*, LNCS 1973, 316-330, Springer, 2001

[2] Jajodia, S., Gadia, S.K. Bhargava, G.: Logical Design of Audit Information in Relational Databases. In *Information Security: An Integrated Collection of Essays* (Essay 25), available online at www.acsac.org.