Journal of Computer Security 17 (2009) 1–3
DOI 10.3233/JCS-2009-0326
IOS Press

Preface

It is our great pleasure to present the special issue of the *Journal of Computer Security* devoted to secure data management and more particularly to data disclosure. Before you start reading the papers, let us briefly introduce privacy and security issues in data management and give you some history of the Secure Data Management workshop, which is the origin of the four papers presented in this issue. We will then introduce the data disclosure topic and finally the papers themselves.

Proliferation of information and communication technologies brings along a number of security and privacy issues. Personalized services, such as reward programs (e.g. frequent flyer/buyer cards) require collection, processing, and often even wide dissemination of personal data and sensitive information. With the omnipresent connectivity, people are ever more using electronic technologies in the business-to-consumer and business-to-business setting. Examples are financial transactions, credit card payments, business transactions, email, document exchange, and even management of health records. Furthermore, new technologies, such as ambient intelligence and ubiquitous computing, are used for the purpose of monitoring and recording behaviors of individuals who may not even be aware of. The collected data typically includes personal information and it is essentially privacy sensitive. The flow of this information gets out of the individuals' control thereby endangering people's privacy.

Therefore, there is an obvious need for secure data management technologies that support these new services but ensure people's privacy. The field of secure data management covers applications ranging from e-government and e-health via enterprise document management to management of people's personal information in local databases, on the Internet, and in ubiquitous computing environments. The interesting technical problems range from traditional ones such as, access control (including different variations, such as dynamic, context-aware, role-based), database security (e.g. efficient database encryption schemes, search over encrypted data, etc.), via data disclosure control, to policy management and enforcement.

Bearing in mind the above considerations we have initiated a series of Secure Data Management (SDM) workshops to address the aforementioned research questions. The first workshop was held in conjunction with the *30th International Conference on Very Large Databases* (VLDB) in 2004. Since then every year the workshop is organized with the VLDB conference. The aim of the workshop is to bring together people from the security research community and data management research community in order to exchange ideas on the aforementioned topics. The participants

from both academia and industry provided an excellent forum for discussing practical experiences and theoretical research efforts that can help in solving the critical problems in secure data management. Each workshop resulted in an LNCS proceedings published by Springer that collected high quality papers selected from a number of submissions.

In this special edition of the *Journal of Computer Security* you can find extended and revised versions of four selected papers from the third and fourth SDM workshops. For this special issue, we have chosen one from several topics the SDM workshop addresses, and that is data disclosure. Nowadays, there is an increasing number of large databases different organizations are creating to maintain information about their customers. This information is used for various purposes and also analyzed to extract valuable nonobvious information for their businesses. However, these databases can be easily misused to reveal sensitive information of individual users. Therefore, the issues around data disclosure control become very important.

This special issue starts with a paper addressing a data disclosure metric. In particular, it deals with an aspect of anonymity called indistinguishability. Chao Yao et al. introduce the notion of indistinguishability as the property that the attacker cannot see the difference among a group of individuals. This property is applicable to generalized private tables, but also to sets of views obtained by multiple queries over a private database table. The paper also describes practical algorithms for checking the database views against three indistinguishability metrics introduced.

We continue this special issue with a paper addressing the anonymization of incremental data, where a dataset is continuously incremented with new data (in contrast to a static data release). Ji-Won Byun et al. discuss several inference attacks as well as the ways of detecting these attacks. Based on these ideas, the paper presents secure anonymization algorithms for incremental datasets and empirically evaluates the presented approach.

The third paper of this special issue discusses control mechanisms for data disclosure caused by answering queries to an XML database. Namely, Böttcher and Hartel introduce an audit framework to determine the 'suspicious' user queries that returned results being sufficient to derive disclosed secret information.

The final paper addresses a different security aspect of data disclosure. Cheng and Tan consider query assurance in data outsourcing scenarios. Their paper addresses the threat that a publisher may return incorrect query results to the users, whether intentionally or under the influence of an adversary. They introduce an authentication scheme for outsourced multi-dimensional databases that verifies completeness and authenticity of query results. The scheme supports a wide range of query types including window, range, and kNN queries on multi-dimensional databases. The paper also presents results from a performance study on kNN queries.

We hope that this special issue on secure data management is of great interest to this research community and will trigger new research in this field. Finally, let us

thank the authors and reviewers for their valuable time and contributions, as well as Sushil Jajodia for giving us the opportunity of publishing this special issue. Enjoy reading the papers!

Milan Petković
Willem Jonker