Handbook of

*Database Security*

*Applications and Trends*
Handbook of
Database Security
Applications and Trends

edited by

Michael Gertz
University of California at Davis
USA

Sushil Jajodia
George Mason University
USA

Springer
Preface

Motivation for the book

Database security has been gaining a great deal of importance as industry, military, and government organizations have increasingly adopted Internet-based technologies on a large-scale, because of convenience, ease of use, and the ability to take advantage of rapid advances in the commercial market. Along with the traditional security aspects of data integrity and availability, there is an increasing interest in research and development in data privacy. This is because today’s often mission-critical databases no longer contain only data used for day-to-day processing by organization; as new applications are being added, it is possible for organizations to collect and store vast amounts of data quickly and efficiently and to make the data readily accessible to the public, typically through Web-based applications. Unfortunately, if security threats related to the integrity, availability, and privacy of the data are not properly resolved, databases remain vulnerable to malicious attacks and accidental misuse. Such incidents, in turn, may translate into financial losses or losses whose values are obviously high but difficult to quantify, e.g., the loss of the public’s trust in the data management infrastructure and services offered by an organization.

In assembling this handbook, we have had a twofold objective: first, to provide a comprehensive summary of the results of research and development activities in various aspects of database security up to this point, and second, to point toward directions for future work in this important and fruitful field of research.

This handbook offers twenty three essays contributed by a selected group of prominent researchers. Given the dynamic nature of the field of database security, we have attempted to obtain a balance among various viewpoints by inviting multiple contributions on the same topic. We believe that this diversity provides a richness generally not available in one book. In some cases, authors have tried to reconcile their differences by contributing a single essay on a topic.
About the book

Essays in this handbook can be roughly divided into following eight areas:

**Foundations of Access Control**
- Recent Advances in Access Control by Sabrina De Capitani di Vimercati, Sara Foresti, and Pierangela Samarati
- Access Control Models for XML by Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, and Pierangela Samarati
- Access Control Policy Languages in XML by Naizhen Qi and Michiharu Kudo

**Trust Management and Trust Negotiation**
- Database Issues in Trust Management and Trust Negotiation by Dongyi Li, William Winsborough, Marianne Winslett, and Ragib Hasan

**Secure Data Outsourcing**
- Authenticated Index Structures for Outsourced Databases by Feifei Li, Marios Hadjileftheriou, George Kollios, and Leonid Reyzin
- Towards Secure Data Outsourcing by Radu Sion
- Managing and Querying Encrypted Data by Bijit Hore, Sharad Mehrotra, and Hakan Hacıgümüş

**Security in Advanced Database Systems and Applications**
- Security in Data Warehouses and OLAP Systems by Lingyu Wang and Sushil Jajodia
- Security for Workflow Systems by Vijayalakshmi Atluri and Janice Warner
- Secure Semantic Web Services by Bhavani Thuraisingham
- Geospatial Database Security by Soon Ae Chun and Vijayalakshmi Atluri

**Database Watermarking**
- Database Watermarking for Copyright Protection by Radu Sion
- Database Watermarking: A Systematic View by Yingjiu Li

**Trustworthy Record Retention and Recovery**
- Trustworthy Records Retention by Ragib Hasan, Marianne Winslett, Soumyadeb Mitra, Windsor Hsu, and Radu Sion
- Damage Quarantine and Recovery in Data Processing Systems by Peng Liu, Sushil Jajodia, and Meng Yu
Preface vii

Privacy

- Hippocratic Databases: Current Capabilities and Future Trends by Tyrone Grandison, Christopher Johnson, and Jerry Kiernan
- Privacy-Preserving Data Mining: A Survey by Charu C. Aggarwal and Philip S. Yu
- Privacy in Database Publishing: A Bayesian Perspective by Alin Deutsch
- Privacy Preserving Publication: Anonymization Frameworks and Principles by Yufei Tao

Privacy in Location-based Services

- Privacy Protection through Anonymity in Location-based Services by Claudio Bettini, Sergio Mascetti, and X. Sean Wang
- Privacy-enhanced Location-based Access Control by Claudio A. Ardagna, Marco Cremonini, Sabrina De Capitani di Vimercati, and Pierangela Samarati
- Efficiently Enforcing the Security and Privacy Policies in a Mobile Environment by Vijayalakshmi Atluri and Heechang Shin

Intended audience

This handbook is suitable as a reference for practitioners and researchers in industry and academia who are interested in the state-of-the-art in database security and privacy. Instructors may use this handbook as a text in a course for upper-level undergraduate or graduate students. Any graduate student who is interested in database security and privacy must definitely read this book.

Acknowledgements

We are extremely grateful to all those who contributed to this handbook. It is a pleasure to acknowledge the authors for their contributions. Special thanks go to Susan Lagerstrom-Fife, Senior Publishing Editor for Springer, and Sharon Palleschi, Editorial Assistant at Springer, whose enthusiasm and support for this project were most helpful.

Davis, California, and Fairfax, Virginia
September 2007

Michael Gertz
Sushil Jajodia
<table>
<thead>
<tr>
<th></th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Recent Advances in Access Control</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Sabrina De Capitani di Vimercati, Sara Foresti, and Pierangela Samarati</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Access Control Models for XML</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, and Pierangela Samarati</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Access Control Policy Languages in XML</td>
<td>55</td>
</tr>
<tr>
<td></td>
<td>Naizhen Qi and Michiharu Kudo</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Database Issues in Trust Management and Trust Negotiation</td>
<td>73</td>
</tr>
<tr>
<td></td>
<td>Dongyi Li, William Winsborough, Marianne Winslett and Ragib Hasan</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Authenticated Index Structures for Outsourced Databases</td>
<td>115</td>
</tr>
<tr>
<td></td>
<td>Feifei Li, Marios Hadjileftheriou, George Kollios, and Leonid Reyzin</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Towards Secure Data Outsourcing</td>
<td>137</td>
</tr>
<tr>
<td></td>
<td>Radu Sion</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Managing and Querying Encrypted Data</td>
<td>163</td>
</tr>
<tr>
<td></td>
<td>Bijit Hore, Sharad Mehrotra, and Hakan Hacıgümüş</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Security in Data Warehouses and OLAP Systems</td>
<td>191</td>
</tr>
<tr>
<td></td>
<td>Lingyu Wang and Sushil Jajodia</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Security for Workflow Systems</td>
<td>213</td>
</tr>
<tr>
<td></td>
<td>Vijayalakshmi Atluri and Janice Warner</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Secure Semantic Web Services</td>
<td>231</td>
</tr>
<tr>
<td></td>
<td>Bhavani Thuraisingham</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Geospatial Database Security</td>
<td>247</td>
</tr>
<tr>
<td></td>
<td>Soon Ae Chun and Vijayalakshmi Atluri</td>
<td></td>
</tr>
</tbody>
</table>
12 Security Re-engineering for Databases: Concepts and Techniques ... 267
   Michael Gertz and Madhavi Gandhi

13 Database Watermarking for Copyright Protection ..................... 297
   Radu Sion

14 Database Watermarking: A Systematic View ............................. 329
   Yingjiu Li

15 Trustworthy Records Retention ........................................... 357
   Ragib Hasan, Marianne Winslett, Soumyadeb Mitra, Windsor Hsu, and
   Radu Sion

16 Damage Quarantine and Recovery in Data Processing Systems ....... 383
   Peng Liu, Sushil Jajodia, and Meng Yu

17 Hippocratic Databases: Current Capabilities and Future Trends .... 409
   Tyrone Grandison, Christopher Johnson, and Jerry Kiernan

18 Privacy-Preserving Data Mining: A Survey .............................. 431
   Charu C. Aggarwal and Philip S. Yu

19 Privacy in Database Publishing: A Bayesian Perspective ............. 461
   Alin Deutsch

20 Privacy Preserving Publication: Anonymization Frameworks and
   Principles .................................................. 489
   Yufei Tao

21 Privacy Protection through Anonymity in Location-based Services .. 509
   Claudio Bettini, Sergio Mascetti, and X. Sean Wang

22 Privacy-enhanced Location-based Access Control .................... 531
   Claudio A. Ardagna, Marco Cremonini, Sabrina De Capitani di
   Vimercati, and Pierangela Samarati

23 Efficiently Enforcing the Security and Privacy Policies in a Mobile
   Environment .................................................. 553
   Vijayalakshmi Atluri and Heechang Shin

Index ............................................................................. 575
List of Contributors

Charu C. Aggarwal
IBM T. J. Watson Research Center, Hawthorne, NY, e-mail: charu@us.ibm.com

Claudio A. Ardagna
Dipartimento di Tecnologie dell’Informazione, Università degli Studi di Milano, Crema, Italy, e-mail: ardagna@dti.unimi.it

Vijayalakshmi Atluri
Rutgers University, Newark, NJ, e-mail: atluri@cimic.rutgers.edu

Claudio Bettini
DICo, University of Milan, Italy, e-mail: bettini@dico.unimi.it

Sabrina De Capitani di Vimercati
Dipartimento di Tecnologie dell’Informazione, Università degli Studi di Milano, Crema, Italy, e-mail: decapita@dti.unimi.it

Soon Ae Chun
City University of New York, College of Staten Island, Staten Island, NY, e-mail: chun@mail.csi.cuny.edu

Marco Cremonini
Dipartimento di Tecnologie dell’Informazione, Università degli Studi di Milano, Crema, Italy, e-mail: cremonini@dti.unimi.it

Alin Deutsch
Department of Computer Science and Engineering, University of California San Diego, La Jolla, CA, e-mail: deutsch@cs.ucsd.edu

Sara Foresti
Dipartimento di Tecnologie dell’Informazione, Università degli Studi di Milano, Crema, Italy, e-mail: foresti@dti.unimi.it
Madhavi Gandhi
Department of Mathematics and Computer Science, California State University, East Bay, CA, e-mail: madhavi.gandhi@eastbay.edu

Michael Gertz
Department of Computer Science, University of California at Davis, Davis, CA, e-mail: gertz@cs.ucdavis.edu

Tyrone Grandison
IBM Almaden Research Center, San Jose, CA, e-mail: tyroneg@us.ibm.com

Hakan Hacıgümüş
IBM Almaden Research Center, San Jose, CA, e-mail: hakanh@acm.org

Marios Hadjileftheriou
AT&T Labs Inc., e-mail: marioh@research.att.com

Ragib Hasan
Department of Computer Science, University of Illinois at Urbana-Champaign, IL, e-mail: rhasan@cs.uiuc.edu

Bijit Hore
Donald Bren School of Computer Science, University of California, Irvine, CA, e-mail: bhore@ics.uci.edu

Windsor Hsu
Data Domain, Inc., e-mail: windsor.hsu@datadomain.com

Sushil Jajodia
Center for Secure Information Systems, George Mason University, Fairfax, VA, e-mail: jajodia@gmu.edu

Christopher Johnson
e-mail: chrisjohnson@alum.berkeley.edu

Jerry Kiernan
IBM Almaden Research Center, San Jose, CA, e-mail: jkiernan@us.ibm.com

George Kollios
Computer Science Department, Boston University, Boston, MA, e-mail: gkollios@cs.bu.edu

Michiharu Kudo
Tokyo Research Laboratory, IBM, Japan, e-mail: kudo@jp.ibm.com

Dongyi Li
Department of Computer Science, University of Texas at San Antonio, TX, e-mail: dli@cs.utsa.edu

Feifei Li
Department of Computer Science, Florida State University, FL, e-mail: lifeifei@cs.fsu.edu
Yingjiu Li
School of Information Systems, Singapore Management University, 80 Stamford Road, Singapore, e-mail: yjli@smu.edu.sg

Peng Liu
Pennsylvania State University, PA, e-mail: pliu@ist.psu.edu

Sergio Mascetti
DICI, University of Milan, Italy, e-mail: mascetti@dico.unimi.it

Sharad Mehrotra
Donald Bren School of Computer Science, University of California, Irvine, CA, e-mail: sharad@ics.uci.edu

Soumyadeb Mitra
Department of Computer Science, University of Illinois at Urbana-Champaign, IL, e-mail: mitral@cs.uiuc.edu

Stefano Paraboschi
University of Bergamo, Dalmine, Italy, e-mail: parabosc@unibg.it

Naizhen Qi
Tokyo Research Laboratory, IBM, Japan, e-mail: naishin@jp.ibm.com

Leonid Reyzin
Computer Science Department, Boston University, Boston, MA, e-mail: reyzin@cs.bu.edu

Pierangela Samarati
Dipartimento di Tecnologie dell’Informazione, Università degli Studi di Milano, Crema, Italy, e-mail: samarati@dti.unimi.it

Heechang Shin
Rutgers University, Newark, NJ, e-mail: hshin@cimic.rutgers.edu

Radu Sion
Network Security and Applied Cryptography Lab, Stony Brook University, NY, e-mail: sion@cs.stonybrook.edu

Yufei Tao
Department of Computer Science and Engineering, Chinese University of Hong Kong, Sha Tin, New Territories, Hong Kong, e-mail: taoyf@cse.cuhk.edu.hk

Bhavani Thuraisingham
University of Texas at Dallas, TX, e-mail: bhavani.thuraisingham@utdallas.edu

Lingyu Wang
Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC H3G 1M8, Canada, e-mail: wang@ciise.concordia.ca

X. Sean Wang
Department of Computer Science, University of Vermont, VT, e-mail: xywang@emba.uvm.edu
Janice Warner
Rutgers University, Newark, NJ, e-mail: janice@cimic.rutgers.edu

William Winsborough
Department of Computer Science, University of Texas at San Antonio, TX, e-mail: wwinsborough@acm.org

Marianne Winslett
Department of Computer Science, University of Illinois at Urbana-Champaign, IL, e-mail: winslett@cs.uiuc.edu

Meng Yu
Western Illinois University, Macomb, IL, e-mail: m-yu2@wiu.edu

Philip S. Yu
IBM T. J. Watson Research Center, Hawthorne, NY, e-mail: psyu@us.ibm.com