



Ulrich Flegel, University of Dortmund, Germany

Privacy-Respecting Intrusion Detection

With our society's growing dependency on information technology systems (IT), IT security is crucial. To properly respond to misuse or abusive activity in IT systems, one needs to establish the capability to detect and understand improper activity. Intrusion Detection Systems observe activity occurring in the IT system, record these observations in audit data, and analyze collected audit data to detect misuse. Collecting and processing audit data for misuse detection conflicts with expectations and rights of system users regarding their privacy. A viable solution is replacing personal data with pseudonyms in audit data. Privacy-Respecting Intrusion Detection introduces technical purpose binding, restricting the linkability of pseudonyms in audit data, to the amount required for misuse detection. Also, it limits the recovery of original personal data to pseudonyms involved in a detected misuse scenario. This book includes case studies with constructively validated solutions by providing algorithms.

Contents: -Foreword by Richard A. Kemmerer, University of California, Santa Barbara, USA.- Introduction and Background.- Introduction.- Authorizations.- An Architectural Model for Secure Authorizations.- Traditional Security Objectives.- Personal Data Protection Objectives.- Technical Enforcement of Multilateral Security.- Pseudonyms - A Technical Point of View.- An Architectural Model for Pseudonymous Authorizations.- Comparing Architectures.- Audit Data Pseudonymization.- Set-Based Approach.- Requirements, Assumptions and Trust Model.- Modeling Conditions for Technical Purpose Binding.- Cryptographic Enforcement of Disclosure Conditions.- The Mismatch Problem.- Operational Pseudonymization and Pseudonym Disclosure.- Extensions.- Application to Unix Audit Data.- Unix Audit Data.- Syslog.- Instantiating the Set-Based Approach for Syslog Audit Data.- Implementation: Pseudo/CoRe.- Evaluation.- APES: Anonymity and Privacy in Electronic Services.- Evaluating the Design Using Basic Building Blocks.- Evaluating the Performance of the Implementation.- Refinement of Misuse Scenario Models.- Motivating Model Refinements.- Models of Misuse Scenarios.- Pseudonymization Based on Serial Signature-Nets.- Pseudonym Linkability.- Pseudonym Disclosure.- Summary.- Threshold Schemes for Cryptographic Secret Sharing.- References.- Index.

2007 Approx. 325 p. 61 illus. Hardcover
Advances in Information Security, Volume 35

► \$ 99.00

ISBN: 978-0-387-34346-4
forthcoming

Order Now!

Yes, please send me

— copies

Flegel, Privacy-Respecting Intrusion Detection (Adv. Info. Security. 35)

ISBN: 978-0-387-34346-4 ► \$ 99.00

Check / Money order enclosed

Please charge my credit card:

MasterCard

VISA

AmEx

Number

exp. Date

Please send order to:

Springer
Order Department
PO Box 2485
Secaucus, NJ 07096-2485

Name

Address

Address

(Sorry, we cannot deliver to P.O. boxes)

City / State / ZIP-Code

Country

Telephone / Email

Date

Signature

► Call toll-free 1-800-SPRINGER, 8:30 am – 5:30 pm ET
► Fax +1 (201) 348-4505 ► Email orders-ny@springer.com

CA, CO, MA, MO, NJ, and NY residents, please add sales tax. Canadian residents, please add 7% GST. Please add \$5.00 for shipping one book and \$1.00 for each additional book. Outside the US and Canada add \$10.00 for first book, \$5.00 for each additional book. All orders are processed upon receipt. If an order cannot be fulfilled within 90 days, payment will be refunded upon request. Prices are payable in US currency or its equivalent. Remember, your 30-day return privilege is always guaranteed.