NIST
National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-92

Guide to Computer Security Log Management

Recommendations of the National Institute of Standards and Technology

Karen Kent
Murugiah Souppaya

NIST Special Publication 800-92

Guide to Computer Security Log Management

Recommendations of the National Institute of Standards and Technology

Karen Kent
Murugiah Souppaya

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2006

U.S. Department of Commerce

Carlos M. Gutierrez, Secretary

Technology Administration

Robert C. Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology

William Jeffrey, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-92
Natl. Inst. Stand. Technol. Spec. Publ. 800-92, 72 pages (September 2006)

Acknowledgements

The authors, Karen Kent and Murugiah Souppaya of the National Institute of Standards and Technology (NIST), wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content, especially Bill Burr, Elizabeth Chew, Tim Grance, Bill MacGregor, Stephen Quinn, and Matthew Scholl of NIST, and Stephen Green, Joseph Nusbaum, Angela Orebaugh, Dennis Pickett, and Steven Sharma of Booz Allen Hamilton. The authors particularly want to thank Anton Chuvakin of LogLogic and Michael Gerdes for their careful review and many contributions to improving the quality of this publication. The authors would also like to express their thanks to security experts Kurt Dillard of Microsoft, Dean Farrington of Wells Fargo Bank, Raffael Marty of ArcSight, Greg Shipley of Neohapsis, and Randy Smith of the Monterey Technology Group, as well as representatives from the Department of Energy, the Department of Health and Human Services, the Department of Homeland Security, the Department of State, the Department of Treasury, the Environmental Protection Agency, the National Institutes of Health, and the Social Security Administration, for their valuable comments and suggestions.

Trademarks

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.