NIST Special Publication 800-121
Revision 2

Guide to Bluetooth Security

John Padgette
John Bahr
Mayank Batra
Marcel Holtmann
Rhonda Smithbey
Lily Chen
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-121r2

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

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

NIST Special Publication 800-121
Revision 2

Guide to Bluetooth Security

John Padgette
Accenture Federal Services
Arlington, VA

Rhonda Smithbey
Spanalytics
Richmond, VA

John Bahr
Bahr Engineering
Superior, CO

Lily Chen
Computer Security Division
Information Technology Laboratory

Mayank Batra
Qualcomm Tech. Intl., Ltd.
Cambridge, United Kingdom

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

Marcel Holtmann
Intel Corporation
Munich, Germany

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-121r2

May 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-121 Revision 2
Natl. Inst. Stand. Technol. Spec. Publ. 800-121 Rev. 2, 67 pages (May 2017)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-121r2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: 800-121r2comments@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

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 analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

Bluetooth wireless technology is an open standard for short-range radio frequency communication used primarily to establish wireless personal area networks (WPANs), and has been integrated into many types of business and consumer devices. This publication provides information on the security capabilities of Bluetooth and gives recommendations to organizations employing Bluetooth wireless technologies on securing them effectively. The Bluetooth versions within the scope of this publication are versions 1.1, 1.2, 2.0 + Enhanced Data Rate (EDR), 2.1 + EDR, 3.0 + High Speed (HS), 4.0, 4.1, and 4.2. Versions 4.0 and later support the low energy feature of Bluetooth.

Keywords

Bluetooth; information security; network security; wireless networking; wireless personal area networks

Acknowledgments

The authors, John Padgette of Accenture, John Bahr of Bahr Engineering (representing Philips Healthtech), Mayank Batra of Qualcomm, Marcel Holtmann of Intel, Rhonda Smithbey of Spanalytics, Lily Chen of the National Institute of Standards and Technology (NIST), and Karen Scarfone of Scarfone Cybersecurity, wish to thank their colleagues in the Bluetooth Security Experts Group (SEG) who contributed technical content and reviewed drafts of this document. The authors greatly appreciate the comments and feedback provided by Mark Nichols of Spanalytics, and the contributions of Alan Kozlay of Biometric Associates, LP. The authors would also like to acknowledge Catherine Brooks of the Bluetooth SIG technical staff for providing the new graphics.

Note to Readers

This document is the second revision to NIST SP 800-121, Guide to Bluetooth Security. Updates in this revision include an introduction to and discussion of Bluetooth 4.1 and 4.2 security mechanisms and recommendations, including Secure Connections for BR/EDR and low energy.

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.