

## Publikationen

- A. Walz and A. Sikora, "Maximizing and Leveraging Behavioral Discrepancies in TLS Implementations using Response-Guided Differential Fuzzing," in Proceedings of the 52nd IEEE International Carnahan Conference on Security Technology (ICST 2018), 22 - 25 October 2018, Montréal, Canada
- T. Müller, A. Walz, M. Kiefer, H. D. Doran and A. Sikora, "Challenges and Prospects of Communication Security in Real-Time Ethernet Automation Systems," in Proceedings of the 14th IEEE International Workshop on Factory Communication Systems (WFCS 2018), 13 - 15 June 2018, Imperia, Italy
- A. Yushev, M. Barghash, M. P. Nguyen, A. Walz, A. Sikora, "TLS-over-CAN: An Experimental Study of Internet-Grade End-to-End Communication Security for CAN Networks," in Proceedings of the 15th International Conference on Programmable Devices and Embedded Systems (PDeS 2018), 23 - 25 May 2018, Ostrava, Czech Republic
- Z. Amjad, et al. "Low Latency V2X Applications and Network Requirements: Performance Evaluation.", Intelligent Vehivles Symposium (IV), IEEE, 2018
- L. Zimmermann, A. Scholz, A. Sikora, J. Aghassi-Hagmann, "A Hybrid System Architecture for the Readout of a Printed Physical Unclonable Function", in Proceedings of the International Conference on Electronics Technology (ICET), May 2018, Chengdu, China
- D. Westhoff, Gedanken zu Autonomieverschiebungen durch Informations- und Kommunikationstechnologie, Buchkapitel in: In 'Das Streben nach Autonomie - Reflexionen zum Digitalen Wandel, Nomos Verlag, pp. 65- 77, Hrsg. T. Breyer-Mayländer, März 2018
- D. Westhoff, M. Zeiser, "Measuring the World - How the Smartphone Industry Impacts Cyber Deterrence Credibility", International Journal of Cyber Warfare and Terrorism (IJCWT), issue 8(2)
- L. Tajan, M. Kaumanns, D. Westhoff, "Pre-Computing Appropriate Parameters: How to Accelerate Somewhat Homomorphic Encryption for Cloud Auditing", IFIP International Conference on New Technologies, Mobility & Security, Paris, France, February 2018 (**best paper award**)
- A. Walz, A. Sikora, "Exploiting Dissent: Towards Fuzzing-based Differential Black Box Testing of TLS Implementations", to appear in IEEE Transactions on Dependable and Secure Computing (TDSC), [Preprint available here](#).
- J. Betz, M. Zeiser, D. Westhoff, "Cache Covert Channel Mitigation in Cloud Virtualization with XEN's Credit Scheduler", IEEE Global Communications Conference (GLOBECOM2017), Communication & Information Systems Security Symposium, Singapore, December 2017 (accepted)
- Johann Betz, Dirk Westhoff, Günter Müller: Survey on covert channels in virtual machines and cloud computing. Trans. Emerging Telecommunications Technologies 28(6) (2017)
- A. Walz, A. Sikora, "eTPL: An Enhanced Version of the TLS Presentation Language Suitable for Automated Parser Generation", 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2017), [Preprint available here](#)
- L. Tajan, D. Westhoff, C. Reuter, F. Armknecht, "Private Information Retrieval and Searchable Encryption for Privacy-Preserving Multi-Client Cloud Auditing" (accepted), 11th International Conference for Internet Technology and Secured Transactions (ICITST-2016), Barcelona, Spain, December 2016
- M. Zeiser, D. Westhoff, "Re-visited: On the Value of purely Software-based Code Attestation for Embedded Devices" International Conference on Innovations for Community Services, 16th I4CS, 27.-29. June, 2016, Vienna, Austria
- P. Nguyen, M. Schappacher, A. Sikora, V.F. Groza, "Extensions of the IEEE802.15.4 Protocol for Ultra-Low Energy Real-Time Communication", Proc. I2MTC, 2016 IEEE International Instrumentation and Measurement Technology Conference, 23.-26. May 2016, Taipei (Taiwan)
- D. Rahusen, D. Jäckle, "Flexible and Open Source Usage of LoRaWAN", Embedded World Conference, 23.-25. Feb. 2016, Nürnberg
- A. Walz, O. Kehret, A. Sikora, "Comparison of Cryptographic Implementations for Embedded TLS", Embedded World Conference, 23.-25. Feb. 2016, Nürnberg
- F.T. Mamo, A. Sikora, "An Overview on Alliances and Ecosystems for Home and Building Automation", Embedded World Conference, 23.-25. Feb. 2016, Nürnberg
- A. Riske, M. Schappacher, A. Sikora, "Entwicklung eines DGPS-gestützten Fahrdynamikmesssystems unter Verwendung des FPGAs Zynq-7000 mit einem Dual-Core Bare-Metal asymmetrischen Multiprozessorsystem", MPC-Workshop 5. Feb. 2016, Karlsruhe

<https://ivesk.hs-offenburg.de/nc/publikationen/>

17 Dez 2018 15:23:36

- Johann W. Betz, Dirk Westhoff, CPU-based Covert- and Side-Channels in Cloud Ecosystems, 2nd BW-CAR Symposium on Information and Communication Systems (SInCom), Konstanz, Nov. 2015.
- Sascha Niro, Jose López, Dirk Westhoff, Andreas Christ: A Keyless Gossip Algorithm Providing Lightweight Data Privacy for Prosumer Markets, IEEE SASO Workshop, Cambridge MA, September 2015
- Asif Mohammad, Jürgen Stader, Dirk Westhoff, A Privacy-friendly Smart Metering Architecture with few-instance Storage. IEEE I4CS, July 8-10, 2015, Nuremberg, Germany
- Oliver Stecklina, Stephan Kornemann, Felix Grehl, Ramona Jung, Dennis Schweer, Thorsten Kranz, Gregor Leander, Katharina Mollus, Dirk Westhoff: Custom-fit Security for Efficient and Pollution-Resistant Multicast OTA-Programming with Fountain Codes. IEEE I4CS, July 8-10, 2015, Nuremberg, Germany
- N. Minh Phuong, M. Schappacher, A. Sikora, "Erweiterungen des IEEE802.15.4 für extrem energiesparende echtzeitfähige Funkkommunikation", VDE Mikrosystemteknikkongress, 26.-28. Oktober 2015, Karlsruhe, S. 696-699
- A. Sikora, S. Toumassian, "Dynamic Thermal Management for Homogeneous Embedded Multicore Processors: Thermal Modeling, System Environment, and Measurement Results", Int'l Journal of Computer and Electrical Engineering, Vol7, No. 4, August 2015, pp.223-231.
- A.K. Nsiah, A. Sikora, A. Walz, A. Yushev, "Embedded TLS1.2 Implementation for Smart Metering & Smart Grid Applications", Journal of Electronic Science and Technology, Vol. 13, No. 4, Dec. 2015, pp.373-378
- F.T. Mamo, A. Sikora, "Implementation of Standardized 6LoWPAN Based Application Layer Protocols", 8th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS2015), 24-26 September 2015, Warsaw, Poland, pp. 817-822
- Johann W. Betz, Dirk Westhoff: C3-Sched - A Cache Covert Channel robust Cloud Computing Scheduler, ICITST, pp. 55-61, Technical Co-Sponsored by IEEE UK/RI Computer Chapter, London, U.K., Dec. 2014.
- Jose M. Lopez, Thomas Rübsamen, Dirk Westhoff: Privacy-friendly cloud audits with Somewhat Homomorphic and Searchable Encryption. I4CS 2014: 95-103
- Katharina Mollus, Dirk Westhoff, Tobias Markmann: Curtailing Privilege Escalation Attacks over Asynchronous Channels on Android. IEEE I4CS, Reims, France, June 2014
- J.-M. Bohli, F. Kaspar, D. Westhoff: Software-Technologien und -Prozesse: IT-Sicherheit und Privatheit in Zeiten von Big Data. 4. Konferenz STeP 2014, Hochschule Furtwangen. De Gruyter Oldenbourg 2014, ISBN 978-3-11-035865-0
- A. Sikora, "Sicherheitsarchitekturen für die vernetzte Heim- und Gebäudeautomatisierung", VDE Kongress, 20.-21.10.2014, Frankfurt, Konferenzbeitrag 5.3.4, S. 1-5.
- D. Jäckle, A. Sikora, "Thermal Modeling of Homogeneous Embedded Multi-Core Processors", 3rd International Conference on Advances in Computing, Communications and Informatics (ICACCI-2014), Greater Noida, Delhi, India, September 24-27, 2014, pp. 588 - 593.
- A. Yushev, P. Lehmann, A. Sikora, "6LoWPAN with RPL Performance Measurements in an Automated Physical Testbed", 2nd IDAACS Symposium Wireless Systems within the IEEE International Conferences on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS WIRELESS 2014), 11. - 12. September 2014, Offenburg, Germany, pp. 29-33.
- M. Aref, A. Sikora, "Free Space Range Measurements with Semtech LoRa technology", 2nd IDAACS Symposium Wireless Systems within the IEEE International Conferences on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS WIRELESS 2014), 11. - 12. September 2014, Offenburg, Germany, pp. 19-23.
- A. Moschevikin, M. Serezhina, A. Sikora, "On the Possibility to Use Leaky Feeders for Positioning in Chirp Spread Spectrum Technologies", 2nd IDAACS Symposium Wireless Systems within the IEEE International Conferences on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS WIRELESS 2014), 11. - 12. September 2014, Offenburg, Germany, pp. 56-65.
- F. Ihle, A. Sikora, "Optimierung von Startup-Zeiten für Embedded Linux", Embedded Systems Symposium, 16.-17. Juli 2014, München.
- S. Gutjahr, A. Sikora, "TLS1.2 für Embedded", Embedded Systems Symposium, 16.-17. Juli 2014, München.
- Q. Huan, A. Sikora, V. Groza, P. Zand, "Simulation & Analysis of WirelessHART Nodes for Real-Time Actuator

Application", 2014 IEEE Int'l Instrumentation and Measurement Technology Conference (I<sup>2</sup>MTC), May 12-15, 2014, Montevideo (Uruguay), pp. 1590-1594.

- A. Sikora, M. Schappacher, L. Möllendorf, "Automated RF Emulator for a highly scalable IEEE802.11p communication and localization subsystem", 6th Intl Workshop on Communication Technologies for Vehicles (Nets4Cars/Nets4Trains 2013/Nets4Aircraft), 6.-7. Mai 2014, Offenburg, S.11-22.
- T. Kuehbeck, G. Hakobyan, A. Sikora, C. Chibelushi, M. Moniri, "Evaluation of Performance Enhancement for Crash Constellation Prediction via C2C Communication - A simulation model based approach", 6th Intl Workshop on Communication Technologies for Vehicles (Nets4Cars/Nets4Trains 2013/Nets4Aircraft), 6.-7. Mai 2014, Offenburg, S. 57-68.
- A. Sikora, "Advances in wireless communication", Embedded World Conference, 25.-27. Februar 2014, Nürnberg.
- F.T. Mamo, M. Dold, A. Sikora, "Implementation issues of BSI-enabled wireless metering", Embedded World Conference, 25.-27. Februar 2014, Nürnberg.
- N. Anantalapochai, A. Sikora, "Development of a Flexible Application Layer for Wireless M-Bus, OMS, and DSMR Protocols", Embedded World Conferenc, 25.-27. Februar 2014, Nürnberg.
- R. Werner, A. Sikora, "Development of an energy autonomous water meter supporting Wireless M-Bus Mode Q and P", Embedded World Conference, 25.-27. Februar 2014, Nürnberg.
- A. Sikora, R. Werner, P. Lehmann, J.O. Grafmüller, "Entwurf, Entwicklung und Verifikation eines energieautarken funkbasierten Wasserzählers mit energiezustandsabhängigen Routing", 7. GMM Workshop Energieautarke Sensorik, 24./25. Februar 2014, Magdeburg, S. 47-51 .
- A. Sikora, "Systemintegration von Telehealth- und Telecare-Komponenten für ein dezentrales Monitoring", 7. Deutscher AAL-Kongress 2014, Berlin, 21.-22. Januar 2014, Paper S21.4.
- Dirk Westhoff, Osman Ugus: Malleability Resilient (Premium) Concealed Data Aggregation. IEEE WoWMoM 2013 (D-SPAN 2013), Madrid, Spain, June 2013
- A. Sikora, M. Schappacher, "A highly scalable IEEE802.11p communication and localization subsystem for autonomous urban driving", 2nd Int'l Conference on Connected Vehicles & Expo (ICCVE 2013), Las Vegas, Dec, 2-6, 2013.
- M. Schappacher, A. Sikora, "Results of Cooperative Localization and Communication System for C2X-Applications", Wireless Congress 2013, 6.-7. Nov. 2013, München.
- A. Sikora, D. Rahusen, "New Trends in Wireless M-Bus Development", Wireless Congress 2013, 6.-7. Nov. 2013, München.
- A. Mikov, A. Moschevikin, A. Fedorov, A. Sikora, "A Localization System Using Inertial Measurement Units from Wireless Commercial Hand-held Devices", 4th Int'l Conference on Indoor Positioning and Indoor Navigation (IPIN 2013), technically co-sponsored by IEEE GRSS, 28-31 October 2013, Montbéliard, France.
- A. Sikora, "Implementation of Standardized Secure Smart Meter Communication", 35th International Telecommunications Energy Conference (INTELEC2013), 13.-17. October 2013, Hamburg.
- A. Sikora, R. Werner, P. Villalonga, A. Cisneros, P. Becker, D. Hoffmann, A. Willmann, "Development of an Energy-Autarkic Water Meter Using Wireless M-Bus based on TinyOS platform", VDE Mikrosystemtechnik-Kongress, 14.-16. Okt 2013, Aachen.
- A. Sikora, M. Dold, "Architecture and Development of Secure Communication Solutions for Smart Grid Applications", 2013 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE2013), 11.-13. October 2013, Kuala Lumpur (Malaysia), published in: Journal of Communications, Vol. 8, No. 8, August 2013, pp.490-497.
- A. Sikora, "Smart Meter Gateway als Vorbild für die Automation", atp edition 9/2013, S. 58-65.
- A. Sikora, R. Werner, J.O. Grafmüller, "Design and Implementation of an Energy Aware Routing Extension for Energy Autarkic Wireless M-Bus Networks", International Workshop on Energy Efficient Wireless Communications and Networking (EEWCN 2013), 22-25 August 2013, Mysore (India).
- A. Sikora, M. Schappacher, "A Highly Scalable IEEE802.11p Subsystem Using Communication and Localization for Increased Vehicular Safety", 2013 Int'l Conf. on Control, Robotics and Cybernetics (ICRC 2013), Malé (Maldives), published in: International Journal of Electrical Energy, Vol.1, No.2, June 2013, ISSN: 2301-3656.

- A. Moschevikin, A. Galov, S. Reginya, A. Volkov, A. Sikora, "The Impact of NLOS Components in Time-of-Flight Networks for Indoor Positioning Systems", 7th IEEE Int'l Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2013), September 2013, Berlin.
- A. Sikora, A. Yunitasari, M. Dold, "GPRS and UMTS Services for Ultra Low Energy M2M-Communication", 7th IEEE Int'l Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2013), September 2013, Berlin.
- C. Ngamy, S. Jaeckel, A. Sikora, "Specification and Implementation of an AXI4-Burst-Master", 50. Workshop der MPC-Gruppe, Konstanz, 12. Juli 2013.
- A. Sikora, "Design, Simulation, and Verification of Highly Portable and Flexible Communication Stacks for Automatic Meter Reading (AMR)", Sensors 2013, May 2013, Nuremberg.
- A. Sikora, D. Lill, M. Schappacher, S. Gutjahr, E. Gerber, "Development of Car2X Communication and Localization PHY and MAC Protocol Following Iterative Spiral Model Using Simulation and Emulation", 5th Intl Workshop on Communication Technologies for Vehicles (Nets4Cars/Nets4Trains 2013), May 2013, Lille (France).
- N. Anantalapochai, A. Sikora, D. Eberlein, D. Kunz, "Integration of BACNET OPC UA-Devices Using a JAVA OPC UA SDK Server with BACNET Open Source Library Implementation", International Journal of Computing, 2013, Vol. 12, Issue 1, pp.7-15.
- A. Sikora, "Portable and Flexible Communication Protocol Stacks for Smart Metering Projects", Journal of Electronic Science and Technology, Vol. 11, No. 1, Mar 2013.
- A. Sikora, R. Werner, "Experiences with Open Source Network Operating Systems for Wireless Protocol Development", Embedded World Conference, 26.-28. Feb 2013, Nuremberg.
- D. Lill, A. Sikora, "Wireless M-Bus and its Real-World Flavors", Embedded World Conference, 26.-28. Feb 2013, Nuremberg.
- A. Hassan, A. Sikora, D.-S. Kunz, D. Eberlein, "Headless Android Systems for Industrial Automation and Control", 49. Workshop der MPC-Gruppe, Mannheim, 08.02.2013.
- M.G. Lima, A. Sikora, "Energy Optimized Point-to-Point Communication of Energy Autarkic Smart Meters Using Mobile Communication Infrastructure", Wireless Congress 2012: Systems & Applications, 14.11.2012, Munich.
- M. Schappacher, A. Sikora, "Network Simulation of Wireless M-Bus Networks", Wireless Congress 2012: Systems & Applications, 14.11.2012, Munich.
- A. Sikora, "Weiterentwicklung der Protokolle für die Primärkommunikation in Smart Metering & Smart Grid Anwendungen", VDE Kongress 2012, 5.11.2012, Stuttgart.
- A. Sikora, D. Lill, "Design, Simulation, and Verification Techniques for Highly Portable and Flexible Wireless M-Bus Protocol Stacks", ICSGCE 2012: 26–28 October 2012, Hong Kong.
- P. Digeser, A. Sikora, "Management of Routed Wireless M-Bus Networks for Sparsely Populated Large-Scale Smart-Metering Installations", International Conference on Security in Computer Networks and Distributed Systems (SNDS'12), October 2012.
- A. Sikora, R. Werner, P. Digeser, M. Klemm, M. Tubolino, "Model Based Development of a TinyOS-based Wireless M-Bus Implementation", 1st IEEE International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS'2012), Sep 20-21, 2012, Offenburg, Germany.
- A. Sikora, P. Villalonga, K. Landwehr, "Extensions to Wireless M-Bus Protocol for Smart Metering and Smart Grid Application", International Conference on Advances in Computing, Communications and Informatics, ICACCI-2012, 3-5 Aug 2012, Chennai, India.
- M. Klemm, A. Sikora, "Measurement Unit for Energy Efficient M2M Mobile Communication", 48. Workshop der MPC-Gruppe, Aalen, 06.07.2012.
- D. Jäckle, A. Sikora, "Experiences with a telecare platform integration of ZigBee sensors into a middleware platform", 6th European ZigBee Developers' Conference, 27.-28. Juni 2012, München.
- A. Sikora, "Security Solutions for Highly Dynamic Car2X Networks in the KoFAS initiative", 4th International Workshop, Nets4Cars/Nets4Trains 2012, Vilnius, Lithuania, April 25-27, 2012.
- A. Sikora, "Robotik und Embedded Internet im phaenovum Schülerforschungszentrum", 103. MNU Bundeskongress,

4.4.2012, Freiburg.

- A. Sikora, K. Landwehr, "Communication Solutions for Smart Gas Meters and Energy Efficient Embedded Services", ARTEMIS track, Embedded World Conference, 29.2.2012, Nürnberg.
- A. Sikora, M. Schappacher, "Network Simulation of Wireless Metering Networks", Embedded World Conference, 28.2.-1.3.2012, Nürnberg.
- A. Sikora, N. Braun, V. Bachmann, "Energy optimisation for GPRS based M2M communication", Embedded World Conference, 28.2.-1.3.2012, Nürnberg.
- H. Venkataraman, A. Chowdhary, G.-M. Muntean, A. Sikora, "COARSE - A Cluster-based Quality Oriented Adaptive Radio Resource Allocation Scheme", IET Communications 2012.
- A. Sikora, D. Lill, M. Schappacher, "Development of a Hardware-Software Co-Design for a real-time localization protocol for pedestrian safety", 47. Workshop der MPC-Gruppe, Offenburg, 03.02.2012.
- A. Sikora, N. Braun, S. Jaeckel, D. Jaeckle, "Gateway Architectures for Home Care Applications Using Wireless Sensor Networks", International Journal of Computing, 2011, Vol. 10, Issue 4, p. 367-372.
- T. Weinläder, D. Lill, A. Sikora, "Experiences with New SubGHz-Narrowband Transceivers", Wireless Congress 2011, München, 9.-10.11.2011.
- A. Sikora, "Results of UWB coexistence measurements", Wireless Congress 2011, München, 9.-10.11.2011.
- A. Sikora, "Pilot Installations for Combined Telecare and Telehealth Services", 45. Jahrestagung der Deutschen Gesellschaft für Biomedizinische Technik (DGBMT), 27.-30.9.2011, Freiburg, [www.bmt2011.de](http://www.bmt2011.de).
- A. Sikora, "Netzwerksimulation von Wireless-M-Bus- und OMS-Netzen", 2. OMS Kongress, 20.9.2011, ZVEI Frankfurt/Main.
- A. Sikora, "Wireless Network and Gateway Architectures for Home Care Applications", IEEE 6th International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2011) Prague, September 15-17, 2011.
- D. Lill, M. Schappacher, A. Gutjahr, A. Sikora, "Protocol and System Design of a Cooperative Pedestrian Safety System", 11th Int'l Conference on ITS Communication (ITST2011)", 23.-25.8.2011, St. Petersburg (Russia).
- A. Sikora, "Synchronization Techniques for Wired and Wireless Networks", Tutorial on the 11th Int'l Conference on ITS Communication (ITST2011)", 23.-25.8.2011, St. Petersburg (Russia).
- A. Rohleder, S. Jaeckel, A. Sikora, "Design and Test of a Gigabit Ethernet MAC for High-Speed HIL-Support", XLIV. Workshop MPC-Gruppe, Furtwangen, 9.7.2011.
- D. Lill, M. Schappacher, S. Islam, A. Sikora, "Wireless Protocol Design for a Cooperative Pedestrian Protection System", 3rd International Workshop on Communication Technologies for Vehicles (Nets4Cars 2011), 23.-24.3.2011, Oberpfaffenhofen.
- A. Sikora, "M2M - State of the Art", Embedded World Conference, Nürnberg, 1.-3.3.2011.
- N. Braun, A. Sikora, "Firmware update over the air for small microcontrollers", Embedded World Conference, Nürnberg, 1.-3.3.2011.
- D. Lill, A. Sikora, "Cooperative Wireless Sensing for Increased Traffic Safety", Embedded World Conference, Nürnberg, 1.-3.3.2011.