Fraunhofer AISEC

Bibliography

Fraunhofer AISEC

September 22, 2022

Alqattaa et al.: Analyzing the Latency of QUIC over an IoT Gateway **DBLP:conf/coins/AlqattaaLM22**

Ahmed Alqattaa, Daniel Loebenberger, and Lukas Moeges. "Analyzing the Latency of QUIC over an IoT Gateway". In: *IEEE International Conference on Omni-layer Intelligent Systems, COINS 2022, Barcelona, Spain, August 1-3, 2022*. IEEE, 2022, pp. 1–6. DOI: 10.1109/COINS54846.2022.9854951. URL: https://doi.org/10.1109/COINS54846.2022.9854951.

d'Aligny et al.: Who comes after us? The correct mindset for designing a Central Bank Digital Currency **schanzenbach2022cdbcprivacy**

Antoine d'Aligny, Emmanuel Benoist, Florian Dold, Christian Grothoff, Özgür Kesim, and Martin Schanzenbach. "Who comes after us? The correct mindset for designing a Central Bank Digital Currency". In: *SUERF Policy Note* 279 (2022). URL: https://www.suerf.org/docx/f_cd24c3cabd88307c9c9299817143ba5d_46097_suerf.pdf.

Heinl et al.: Remote Electronic Voting in Uncontrolled Environments: A Classifying Survey **heinl2022CSUR**

Michael P. Heinl, Simon Gölz, and Christoph Bösch. "Remote Electronic Voting in Uncontrolled Environments: A Classifying Survey". In: *ACM Comput. Surv.* (2022). Just Accepted. ISSN: 0360-0300. DOI: 10.1145/3551386. URL: https://doi.org/10.1145/3551386.

Kesim et al.: Zero-Knowledge Age Restriction for GNU Taler **schanzen2022talerage**

Özgür Kesim, Christian Grothoff, Florian Dold, and Martin Schanzenbach. "Zero-Knowledge Age Restriction for GNU Taler". In: *Proceedings of 27rd European Symposium on Research in Computer Security (ESORICS)*. Lecture Notes in Computer Science. Springer, 2022.

Kunz et al.: Application-Oriented Selection of Privacy Enhancing Technologies **kunz2022application**

Immanuel Kunz and Andreas Binder. "Application-Oriented Selection of Privacy Enhancing Technologies". In: *Annual Privacy Forum*. Springer. 2022, pp. 75–87.

Kunz et al.: A Continuous Risk Assessment Methodology for Cloud Infrastructures **kunz2022continuous**

Immanuel Kunz, Angelika Schneider, and Christian Banse. "A Continuous Risk Assessment Methodology for Cloud Infrastructures". In: *2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid)*. IEEE. 2022, pp. 1042–1051.

Lauf et al.: Donating Medical Data as a Patient Sovereignly: A Technical Approach **lauf2022donating**

Florian Lauf, Marcel Klöttgen, Hendrik Meyer zum Felde, and Robin Brandstädter. "Donating Medical Data as a Patient Sovereignly: A Technical Approach". In: *15th International Conference on Health Informatics (HEALTHINF 2022)*. 2022.

Müller et al.: Does Audio Deepfake Detection Generalize? muller2022does

Nicolas M Müller, Pavel Czempin, Franziska Dieckmann, Adam Froghyar, and Konstantin Böttinger. "Does Audio Deepfake Detection Generalize?" In: *Interspeech* (2022).

Müller et al.: Attacker Attribution of Audio Deepfakes muller2022attacker

Nicolas M Müller, Franziska Dieckmann, and Jennifer Williams. "Attacker Attribution of Audio Deepfakes". In: *Interspeech* (2022).

Selmke et al.: On the application of Two-Photon Absorption for Laser Fault Injection attacks Pushing the physical boundaries for Laser-based Fault Injection DBLP:journals/tches/SelmkePDSWMKS22

Bodo Selmke, Maximilian Pollanka, Andreas Duensing, Emanuele Strieder, Hayden Wen, Michael Mittermair, Reinhard Kienberger, and Georg Sigl. "On the application of Two-Photon Absorption for Laser Fault Injection attacks Pushing the physical boundaries for Laser-based Fault Injection". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2022.4 (2022), pp. 862–885. DOI: 10.46586/tches.v2022.i4.862-885. URL: https://doi.org/10.46586/tches.v2022.i4.862-885.

Weiss et al.: A Language-Independent Analysis Platform for Source Code weiss2022languageindependent

Konrad Weiss and Christian Banse. *A Language-Independent Analysis Platform for Source Code*. 2022. arXiv: 2203.08424 [cs.CR]. URL: https://doi.org/10.48550/arXiv.2203.08424.

Banse et al.: Cloud Property Graph: Connecting Cloud Security Assessments with Static Code Analysis banse2021cloudpg

C. Banse, I. Kunz, A. Schneider, and K. Weiss. "Cloud Property Graph: Connecting Cloud Security Assessments with Static Code Analysis". In: *2021 IEEE 14th International Conference on Cloud Computing (CLOUD)*. Los Alamitos, CA, USA: IEEE Computer Society, 2021, pp. 13–19. DOI: 10.1109/CLOUD53861.2021.00014. URL: https://doi.ieeecomputersociety.org/10.1109/CLOUD53861.2021.00014.

Banse: Data Sovereignty in the Cloud - Wishful Thinking or Reality? banse2021datsov

Christian Banse. "Data Sovereignty in the Cloud - Wishful Thinking or Reality?" In: *Proceedings of the 2021 on Cloud Computing Security Workshop*. CCSW '21. Virtual Event, Republic of Korea: Association for Computing Machinery, 2021, 153–154. ISBN: 9781450386531. DOI: 10.1145/3474123.3486792. URL: https://doi.org/10.1145/3474123.3486792.

Banse et al.: Automatisierte Compliance-Prüfung in Software-Artefakten banse2021bsi

Christian Banse, Florian Wendland, and Konrad Weiss. "Automatisierte Compliance-Prüfung in Software-Artefakten". In: *Deutschland. Digital. Sicher. 30 Jahre BSI*. SecuMedia Verlag, 2021. ISBN: 978-3-922746-83-6.

Boenisch: Privatsphäre und Maschinelles Lernen **boenisch2021**

Franziska Boenisch. "Privatsphäre und Maschinelles Lernen". In: 45th ser. (2021), pp. 448–452. DOI: https://doi.org/10.1007/s11623-021-1469-3.

Bramm et al.: CardioTEXTIL: Wearable for Monitoring and End-to-End Secure Distribution of ECGs **bramm2021cardiotextil**

Georg Bramm, Matthias Hiller, Christian Hofmann, Stefan Hristozov, Maximilian Oppelt, Norman Pfeiffer, Martin Striegel, Matthias Struck, and Dominik Weber. "CardioTEXTIL: Wearable for Monitoring and End-to-End Secure Distribution of ECGs". In: *IEEE 17th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*. 2021. DOI: toappear.

Fischer et al.: Mehr Flexibilität bitte! Post-Quanten-Kryptografie und Schutz vor Quantencomputerangriffen **fisgaz21**

Tilo Fischer, Stefan-Lukas Gazdag, Daniel Loebenberger, and Felix Schärtl. "Mehr Flexibilität bitte! Post-Quanten-Kryptografie und Schutz vor Quantencomputerangriffen". In: *iX: Magazin für professionelle Informationstechnik* 10/2021 (2021), pp. 122–125.

Garb et al.: FORTRESS: FORtified Tamper-Resistant Envelope with Embedded Security Sensor **Foliendemonstrator**

Kathrin Garb, Johannes Obermaier, Elischa Ferres, and Martin König. "FORTRESS: FORtified Tamper-Resistant Envelope with Embedded Security Sensor". In: *18th Annual International Conference on Privacy, Security and Trust (PST2021)*. 2021. DOI: toappear.

Garb et al.: Attacks and Countermeasures for Capacitive PUF-Based Security Enclosures **attacksOnEnvelope**

Kathrin Garb, Marc Schink, Matthias Hiller, and Johannes Obermaier. "Attacks and Countermeasures for Capacitive PUF-Based Security Enclosures". In: *2021 IEEE Physical Assurance and Inspection of Electronics (PAINE)*. 2021. DOI: toappear.

Gazdag et al.: Entangled Secrets: Quantum computers and the quest for quantum-resilient encryption **gazgru21a**

Stefan-Lukas Gazdag, Sophia Grundner-Culeman, Tobias Guggemos, Tobias Heider, and Daniel Loebenberger. "Entangled Secrets: Quantum computers and the quest for quantum-resilient encryption". In: *Linux Magazin* 247 (2021), pp. 16–19.

Gazdag et al.: Migration zu quantenresistenter IT **gazgru21**

Stefan-Lukas Gazdag, Sophia Grundner-Culeman, Tobias Guggemos, Tobias Heider, and Daniel Loebenberger. "Migration zu quantenresistenter IT". In: *Linux Magazin* 04/2021 (2021), pp. 16–19.

Gazdag et al.: A Formal Analysis of IKEv2's Post-Quantum Extension **gazgru21b**

Stefan-Lukas Gazdag, Sophia Grundner-Culemann, Tobias Guggemos, Tobias Heider, and Daniel Loebenberger. "A Formal Analysis of IKEv2's Post-Quantum Extension". In: *Annual Computer Security Applications Conference*. ACSAC. Virtual Event, USA: Association for Computing Machinery, 2021, pp. 91 –105. ISBN: 978-1-4503-8579-4. DOI: 10.1145/3485832.3485885. URL: https://doi.org/10.1145/3485832.3485885.

Abstract: Many security protocols used for daily Internet traffic have been used for decades and standardization bodies like the IETF often provide extensions for legacy protocols to deal with new requirements. Even though the security aspects for extensions are carefully discussed, automated reasoning has proven to be a valuable tool to uncover security holes that would otherwise have gone unnoticed. Therefore, Automated Theorem Proving (ATP) is already a customary procedure for the development of some new protocols, e.g., TLS 1.3 and MLS. IKEv2, the key exchange for the IPsec protocol suite, is expected to undergo significant changes to facilitate the integration of Post-Quantum Cryptography. We present the first formal security model for the IKEv2-handshake in a quantum setting together with an automated proof using the Tamarin Prover. Our model focuses on the core state machine, is therefore easily extendable, and aims to promote the use of ATP in IPsec-standardization. The security model captures gaps in the protocol, but treats the specific implementation (like fragmentation mechanisms, for example) as a black box. With IKE_INTERMEDIATE we showcase this approach on a recently proposed extension that significantly changes the protocol's state machine.

Giehl et al.: Leveraging Edge Computing and Differential Privacy to Securely Enable Industrial Cloud Collaboration Along the Value Chain **giehl2021a4o**

Alexander Giehl, Michael P. Heinl, and Maximilian Busch. "Leveraging Edge Computing and Differential Privacy to Securely Enable Industrial Cloud Collaboration Along the Value Chain". In: *2021 IEEE 17th International Conference on Automation Science and Engineering (CASE)*. Lyon, France: IEEE, 2021, pp. 2023–2028. ISBN: 978-1-6654-1873-7. DOI: 10.1109/CASE49439.2021.9551656. URL: https://ieeexplore.ieee.org/document/9551656.

Hamburg et al.: Chosen Ciphertext k-Trace Attacks on Masked CCA2 Secure Kyber **DBLP:journals/tches/HamburgHPSSSSV21**

Mike Hamburg, Julius Hermelink, Robert Primas, Simona Samardjiska, Thomas Schamberger, Silvan Streit, Emanuele Strieder, and Christine van Vredendaal. "Chosen Ciphertext k-Trace Attacks on Masked CCA2 Secure Kyber". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2021.4 (2021), pp. 88–113. DOI: 10.46586/tches.v2021.i4.88-113. URL: https://doi.org/10.46586/tches.v2021.i4.88-113.

Hauschild et al.: ARCHIE: A QEMU-Based Framework for Architecture-Independent Evaluation of Faults **DBLP:conf/fdtc/HauschildGASO21**

Florian Hauschild, Kathrin Garb, Lukas Auer, Bodo Selmke, and Johannes Obermaier. "ARCHIE: A QEMU-Based Framework for Architecture-Independent Evaluation of Faults". In: *FDTC*. IEEE, 2021, pp. 20–30.

Heinl et al.: A Comparative Security Analysis of the German Federal Postal Voting Process **heinl2021DGO**

Michael P. Heinl, Simon Gölz, and Christoph Bösch. "A Comparative Security Analysis of the German Federal Postal Voting Process". In: *DG.O2021: The 22nd Annual International Conference on Digital Government Research*. DG.O'21. Omaha, NE, USA: Association for Computing Machinery, 2021, 198–207. ISBN: 9781450384926. DOI: 10.1145/3463677.3463679. URL: https://doi.org/10.1145/3463677.3463679.

Hemmert et al.: Quantencomputerresistente Kryptografie: Aktuelle Aktivitäten und Fragestellungen **hemloc21**

Tobias Hemmert, Mandred Lochter, Daniel Loebenberger, Marian Margraf, Stephanie Reinhardt, and Georg Sigl. "Quantencomputerresistente Kryptografie: Aktuelle Aktivitäten und Fragestellungen". In: *Deutschland. Digital. Sicher. 30 Jahre BSI*. SecuMedia Verlag, 2021, pp. 367–381. ISBN: 978-3-922746-83-6.

Herzinger et al.: Real-World Quantum-Resistant IPsec **gazher21**

Daniel Herzinger, Stefan-Lukas Gazdag, and Daniel Loebenberger. "Real-World Quantum-Resistant IPsec". In: *2021 14th International Conference on Security of Information and Networks (SIN)*. Vol. 1. 2021, pp. 1–8. DOI: 10.1109/SIN54109.2021.9699255.

Hetzelt et al.: VIA: Analyzing Device Interfaces of Protected Virtual Machines **hetzelt2021via**

Felicitas Hetzelt, Martin Radev, Robert Buhren, Mathias Morbitzer, and Jean-Pierre Seifert. "VIA: Analyzing Device Interfaces of Protected Virtual Machines". In: *37th Annual Computer Security Applications Conference (ACSAC 2021)*. 2021.

Hristozov et al.: The Cost of OSCORE and EDHOC for Constrained Devices **Hristozov2021**

Stefan Hristozov, Manuel Huber, Lei Xu, Jaro Fietz, Marco Liess, and Georg Sigl. "The Cost of OSCORE and EDHOC for Constrained Devices". In: *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy*. CODASPY '21. Virtual Event, USA: Association for Computing Machinery, 2021, 245–250. ISBN: 9781450381437. DOI: 10.1145/3422337.3447834. URL: https://doi.org/10.1145/3422337.3447834.

Küchler et al.: Does Every Second Count? Time-based Evolution of Malware Behavior in Sandboxes **kuechler2021does**

Alexander Küchler, Alessandro Mantovani, Yufei Han, Leyla Bilge, and Davide Balzarotti. "Does Every Second Count? Time-based Evolution of Malware Behavior in Sandboxes". In: *Network and Distributed Systems Security (NDSS) Symposium*. 2021.

Loebenberger: Langzeitsichere Kryptographie: Was Quantencomputer und andere Disruptionen für Verschlüsselung aus Sicht der Forschung bedeuten **loe21**

Daniel Loebenberger. "Langzeitsichere Kryptographie: Was Quantencomputer und andere Disruptionen für Verschlüsselung aus Sicht der Forschung bedeuten". In: *<kes> – Die Zeitschrift für Informationssicherheit* 37.1 (2021), pp. 55–58.

Madl: Security Concept with Distributed Trust-Levels for Autonomous Cooperative Vehicle Networks **madl2021citssecurity**

Tobias Madl. "Security Concept with Distributed Trust-Levels for Autonomous Cooperative Vehicle Networks". In: *2021 IEEE Intelligent Vehicles Symposium (IV)*. NAGOYA, JAPAN: IEEE, 2021, pp. 321–328. DOI: 10.1109/IV48863.2021.9576024.

Markert et al.: Language Dependencies in Adversarial Attacks on Speech Recognition Systems **markert21b_spsc**

Karla Markert, Donika Mirdita, and Konstantin Böttinger. "Language Dependencies in Adversarial Attacks on Speech Recognition Systems". In: *Proc. 2021 ISCA Symposium on Security and Privacy in Speech Communication*. 2021, pp. 25–31. DOI: 10.21437/SPSC.2021-6.

Markert et al.: Visualizing Automatic Speech Recognition – Means for a Better Understanding? **markert21_spsc**

Karla Markert, Romain Parracone, Mykhailo Kulakov, Philip Sperl, Ching-Yu Kao, and Konstantin Böttinger. "Visualizing Automatic Speech Recognition – Means for a Better Understanding?" In: *Proc. 2021 ISCA Symposium on Security and Privacy in Speech Communication*. 2021, pp. 14–20. DOI: 10.21437/SPSC.2021-4.

Meyer zum Felde et al.: Securing Remote Policy Enforcement by a Multi-Enclave based Attestation Architecture **meyerzumfelde2021securing**

Hendrik Meyer zum Felde, Mathias Morbitzer, and Julian Schütte. "Securing Remote Policy Enforcement by a Multi-Enclave based Attestation Architecture". In: *19th IEEE international conference on embedded and ubiquitous computing (EUC 2021)*. 2021.

Morbitzer et al.: SEVerity: Code Injection Attacks against Encrypted Virtual Machines **morbitzer2021severity**

Mathias Morbitzer, Sergej Proskurin, Martin Radev, Marko Dorfhuber, and Erick Quintanar Salas. "SEVerity: Code Injection Attacks against Encrypted Virtual Machines". In: *15th IEEE Workshop on Offensive Technologies (WOOT)*. 2021.

Müller et al.: Human perception of audio deepfakes **muller2021human**

Nicolas M Müller, Karla Markert, and Konstantin Böttinger. "Human perception of audio deepfakes". In: *1st International Workshop on Deepfake Detection for Audio Multimedia, ACM Multimedia* (2021).

Müller et al.: Adversarial Vulnerability of Active Transfer Learning **MB21**

N. Müller and K. Böttinger. "Adversarial Vulnerability of Active Transfer Learning". In: *Symposium on Intelligent Data Analysis 2021*. 2021.

Müller et al.: Speech is Silver, Silence is Golden: What do ASVspoof-trained Models Really Learn? **MuellerASV2021**

Nicolas Müller, Franziska Dieckmann, Pavel Czempin, Roman Canals, and Konstantin Böttinger. "Speech is Silver, Silence is Golden: What do ASVspoof-trained Models Really Learn?" In: *ASVSpoof 2021 Workshop*. 2021.

Schanzenbach et al.: Decentralized Identities for Self-sovereign End-users (DISSENS) **schanzen2021oid**

Martin Schanzenbach, Christian Grothoff, Hansjürg Wenger, and Maximilian Kaul. "Decentralized Identities for Self-sovereign End-users (DISSENS)". In: *Open Identity Summit 2021*. Ed. by Heiko Roßnagel, Christian H. Schunck, and Sebastian Mödersheim. Bonn: Gesellschaft für Informatik e.V., 2021, pp. 47–58.

Schink et al.: Security and Trust in Open Source Security Tokens **Schink_Wagner_Unterstein_Heyszl_2021**

Marc Schink, Alexander Wagner, Florian Unterstein, and Johann Heyszl. "Security and Trust in Open Source Security Tokens". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2021.3 (2021), 176–201. DOI: 10.46586/tches.v2021.i3.176-201. URL: https://tches.iacr.org/index.php/TCHES/article/view/8972.

Schulze et al.: DA3G: Detecting Adversarial Attacks by Analysing Gradients **Schulze2021**

Jan-Philipp Schulze, Philip Sperl, and Konstantin Böttinger. "DA3G: Detecting Adversarial Attacks by Analysing Gradients". In: *Computer Security – ESORICS 2021*. Springer, 2021. DOI: 10.1007/978-3-030-88418-5_27. URL: https://doi.org/10.1007/978-3-030-88418-5_27.

Selmke et al.: Breaking Black Box Crypto-Devices Using Laser Fault Injection **DBLP:conf/fps/SelmkeSHFD21**

Bodo Selmke, Emanuele Strieder, Johann Heyszl, Sven Freud, and Tobias Damm. "Breaking Black Box Crypto-Devices Using Laser Fault Injection". In: *Foundations and Practice of Security - 14th International Symposium, FPS 2021, Paris, France, December 7-10, 2021, Revised Selected Papers*. Ed. by Esma Aïmeur, Maryline Laurent, Reda Yaich, Benoît Dupont, and Joaquín García-Alfaro. Vol. 13291. Lecture Notes in Computer Science. Springer, 2021, pp. 75–90. DOI: 10.1007/978-3-031-08147-7_6. URL: https://doi.org/10.1007/978-3-031-08147-7_6.

Sperl et al.: Activation Anomaly Analysis **10.1007/978-3-030-67661-2_5**

Philip Sperl, Jan-Philipp Schulze, and Konstantin Böttinger. "Activation Anomaly Analysis". In: *Ma-*

chine Learning and Knowledge Discovery in Databases. Ed. by Frank Hutter, Kristian Kersting, Jefrey Lijffijt, and Isabel Valera. Cham: Springer International Publishing, 2021, pp. 69–84. ISBN: 978-3-030-67661-2.

Abstract: Inspired by recent advances in coverage-guided analysis of neural networks, we propose a novel anomaly detection method. We show that the hidden activation values contain information useful to distinguish between normal and anomalous samples. Our approach combines three neural networks in a purely data-driven end-to-end model. Based on the activation values in the target network, the alarm network decides if the given sample is normal. Thanks to the anomaly network, our method even works in semi-supervised settings. Strong anomaly detection results are achieved on common data sets surpassing current baseline methods. Our semi-supervised anomaly detection method allows to inspect large amounts of data for anomalies across various applications.

Striegel et al.: Evaluating Augmented Reality for Wireless Network Security Education **striegel_evaluating_2021**

Martin Striegel, Jonas Erasmus, and Parag Jain. "Evaluating Augmented Reality for Wireless Network Security Education". en. In: *{IEEE} Frontiers in Education {FIE}*. 2021. DOI: toappear.

Tatschner et al.: The Stream Exchange Protocol: A Secure and Lightweight Tool for Decentralized Connection Establishment **tatschnerMDPI2021**

Stefan Tatschner, Ferdinand Jarisch, Alexander Giehl, Sven Plaga, and Thomas Newe. "The Stream Exchange Protocol: A Secure and Lightweight Tool for Decentralized Connection Establishment". In: vol. 21. 15. 2021. DOI: 10.3390/s21154969. URL: https://www.mdpi.com/1424-8220/21/15/4969.

Abstract: With the growing availability and prevalence of internet-capable devices, the complexity of networks and associated connection management increases. Depending on the use case, different approaches in handling connectivity have emerged over the years, tackling diverse challenges in each distinct area. Exposing centralized web-services facilitates reachability; distributing information in a peer-to-peer fashion offers availability; and segregating virtual private sub-networks promotes confidentiality. A common challenge herein lies in connection establishment, particularly in discovering, and securely connecting to peers. However, unifying different aspects, including the usability, scalability, and security of this process in a single framework, remains a challenge. In this paper, we present the Stream Exchange Protocol (SEP) collection, which provides a set of building blocks for secure, lightweight, and decentralized connection establishment. These building blocks use unique identities that enable both the identification and authentication of single communication partners. By utilizing federated directories as decentralized databases, peers are able to reliably share authentic data, such as current network locations and available endpoints. Overall, this collection of building blocks is universally applicable, easy to use, and protected by state-of-the-art security mechanisms by design. We demonstrate the capabilities and versatility of the SEP collection by providing three tools that utilize our building blocks: a decentralized file sharing application, a point-to-point network tunnel using the SEP trust model, and an application that utilizes our decentralized discovery mechanism for authentic and asynchronous data distribution.

Vintila et al.: MESH: A Memory-Efficient Safe Heap for C/C++ **vintila2021**

Emanuel Q. Vintila, Philipp Zieris, and Julian Horsch. "MESH: A Memory-Efficient Safe Heap for C/C++". In: *Proceedings of the 16th International Conference on Availability, Reliability and Security*. ARES '21. Vienna, Austria: ACM, Aug. 2021. ISBN: 978-1-4503-9051-4. DOI: 10.1145/3465481.3465760. URL: https://doi.org/10.1145/3465481.3465760.

Vintila et al.: MESH: A Memory-Efficient Safe Heap for C/C++ **vintila2021mesh**

Emanuel Q. Vintila, Philipp Zieris, and Julian Horsch. "MESH: A Memory-Efficient Safe Heap for C/C++". In: *Proceedings of the 16th International Conference on Availability, Reliability and Security*. ARES '21. Vienna, Austria: ACM, Aug. 2021. ISBN: 978-1-4503-9051-4. DOI: 10.1145/3465481.3465760. URL: https://doi.org/10.1145/3465481.3465760.

Bramm. et al.: cipherPath: Efficient Traversals over Homomorphically Encrypted Paths **bramm2020cipherpath**

Georg Bramm. and Julian Schütte. "cipherPath: Efficient Traversals over Homomorphically Encrypted Paths". In: *Proceedings of the 17th International Joint Conference on e-Business and Telecommunications - Volume 3: SECRYPT*. INSTICC. SciTePress, 2020, pp. 271–278. ISBN: 978-989-758-446-6. DOI: 10.5220/0009777802710278.

Dorp et al.: Comparative analysis of random generators **dorgat20**

Johannes vom Dorp, Joachim von zur Gathen, Daniel Loebenberger, Jan Lür, and Simon Schneider. "Comparative analysis of random generators". In: *Algorithmic Combinatorics – Enumerative Combinatorics, Special Functions and Computer Algebra*. Ed. by Veronika Pillwein and Carsten Schneider. Springer International Publishing, Dec. 2020, pp. 181–196. URL: http://dx.doi.org/10.1007/978-3-030-44559-1_10.

Dörr et al.: Towards Resistant Audio Adversarial Examples **DMMB20**

Tom Dörr, Karla Markert, Nicolas M. Müller, and Konstantin Böttinger. "Towards Resistant Audio Adversarial Examples". In: *1st Security and Privacy on Artificial Intelligent Workshop (SPAI'20)*. ACM AsiaCCS. Taipei, Taiwan, 2020. DOI: https://doi.org/10.1145/3385003.3410921.

Fischer et al.: A Study About the Different Categories of IoT in Scientific Publications **sfischer2020IoTstudy**

Sebastian Fischer, Katrin Neubauer, and Rudolf Hackenberg. "A Study About the Different Categories of IoT in Scientific Publications". In: *CLOUD COMPUTING 2020, The Eleventh International Conference on Cloud Computing, GRIDs, and Virtualization*. 2020, pp. 24–30.

Abstract: The Internet of Things (IoT) is widely used as a synonym for nearly every connected device. This makes it really difficult to find the right kind of scientific publication for the intended category of IoT. Conferences and other events for IoT are confusing about the target group (consumer, enterprise, industrial, etc.) and standardisation organisations suffer from the same problem. To demonstrate these problems, this paper shows the results of an analyses over IoT publications in different research libraries. The number of results for IoT, consumer, enterprise and industrial search

queries were evaluated and a manual study about 100 publications was done. According to the research library or search engine, different results about the distribution of consumer-, enterprise- and industrial- IoT are visible. The comparison with the results of the manual evaluation shows that some search queries do not show all desired publications or that considerably more, unwanted results are returned. Most researchers do not use the keywords right and the exact category of IoT can only be accessed via the abstract. This shows major problems with the use of the term IoT and its minor limitations.

Franzen et al.: FridgeLock: Preventing Data Theft on Suspended Linux with Usable Memory Encryption **ramenc_2019**

Fabian Franzen, Manuel Andreas, and Manuel Huber. "FridgeLock: Preventing Data Theft on Suspended Linux with Usable Memory Encryption". In: *Proceedings of the 10th ACM on Conference on Data and Application Security and Privacy*. CODASPY '20. New Orleans, LA, USA: ACM, 2020, p. 6.

Garb et al.: Temporary Laser Fault Injection into Flash Memory: Calibration, Enhanced Attacks, and Countermeasures **KO20**

Kathrin Garb and Johannes Obermaier. "Temporary Laser Fault Injection into Flash Memory: Calibration, Enhanced Attacks, and Countermeasures". In: *26th IEEE International Symposium on On-Line Testing and Robust System Design (IOLTS)*. 2020.

Giehl et al.: Integrating security evaluations into virtual commissioning **giehl2020seccom**

Alexander Giehl, Norbert Wiedermann, Makan Tayebi Gholamzadeh, and Claudia Eckert. "Integrating security evaluations into virtual commissioning". In: *2020 IEEE 16th International Conference on Automation Science and Engineering Proceedings*. Hong Kong: IEEE, 2020. ISBN: 978-1-7281-6904-0. DOI: 10.1109/CASE48305.2020.9217004. URL: https://ieeexplore.ieee.org/document/9217004.

Hansch: Automating Security Risk and Requirements Management for Cyber-Physical Systems **Hansch2020automating**

Gerhard Hansch. "Automating Security Risk and Requirements Management for Cyber-Physical Systems". Dissertation. Göttingen, Germany: Georg-August-Universität Göttingen, Dec. 2020. DOI: 10.24406/AISEC-N-608669. URL: http://hdl.handle.net/21.11130/00-1735-0000-0005-1517-A.

Heinl et al.: AntiPatterns Regarding the Application of Cryptographic Primitives by the Example of Ransomware **heinl2020SSE**

Michael P. Heinl, Alexander Giehl, and Lukas Graif. "AntiPatterns Regarding the Application of Cryptographic Primitives by the Example of Ransomware". In: *Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES 2020)*. ARES '20. Virtual Event, Ireland: Association for Computing Machinery, 2020. ISBN: 9781450388337. DOI: 10.1145/3407023.3409182. URL: https://doi.org/10.1145/3407023.3409182.

Heyszl et al.: Investigating Profiled Side-Channel Attacks Against the DES Key Schedule DBLP:journals/tches/HeyszlMUSWGFDKK20

Johann Heyszl, Katja Miller, Florian Unterstein, Marc Schink, Alexander Wagner, Horst A. Gieser, Sven Freud, Tobias Damm, Dominik Klein, and Dennis Kügler. "Investigating Profiled Side-Channel Attacks Against the DES Key Schedule". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2020.3 (2020), pp. 22–72. DOI: 10.13154/tches.v2020.i3.22-72. URL: https://doi.org/10.13154/tches.v2020.i3.22-72.

Hiller et al.: Review of error correction for PUFs and evaluation on state-of-the-art FPGAs HKS20

Matthias Hiller, Ludwig Kürzinger, and Georg Sigl. "Review of error correction for PUFs and evaluation on state-of-the-art FPGAs". In: *Journal of Cryptographic Engineering* (2020).

Hinterberger et al.: IoT Device IdentificAtion and RecoGnition (IoTAG) sfischer2020IoTAG

Lukas Hinterberger, Sebastian Fischer, Bernhard Weber, Katrin Neubauer, and Rudolf Hackenberg. "IoT Device IdentificAtion and RecoGnition (IoTAG)". In: *CLOUD COMPUTING 2020, The Eleventh International Conference on Cloud Computing, GRIDs, and Virtualization*. 2020, pp. 17–23.

Abstract: To ensure the secure operation of IoT devices in the future, they must be continuously monitored. This starts with an inventory of the devices, checking for a current software version and extends to the encryption algorithms and active services used. Based on this information, a security analysis and rating of the whole network is possible. To solve this challenge in the growing network environments, we present a proposal for a standard. With the IoT Device IdentificAtion and RecoGnition (IoTAG), each IoT device reports its current status to a central location as required and provides information on security. This information includes a unique ID, the exact device name, the current software version, active services, cryptographic methods used, etc. The information is signed to make misuse more difficult and to ensure that the device can always be uniquely identified. In this paper, we introduce IoTAG in detail and describe the necessary requirements.

Hristozov et al.: Protecting RESTful IoT Devices from Battery Exhaustion DoS Attacks HristozovEtAl2020

Stefan Hristozov, Manuel Huber, and Georg Sigl. "Protecting RESTful IoT Devices from Battery Exhaustion DoS Attacks". en. In: *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. San Jose, CA, USA, 2020. URL: tobepublishedinMay.

Huber et al.: The Lazarus Effect: Healing Compromised Devices in the Internet of Small Things 10.1145/3320269.3384723

Manuel Huber, Stefan Hristozov, Simon Ott, Vasil Sarafov, and Marcus Peinado. "The Lazarus Effect: Healing Compromised Devices in the Internet of Small Things". In: *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '20. Taipei, Taiwan: Association for Computing Machinery, 2020, 6–19. ISBN: 9781450367509. DOI: 10.1145/3320269.3384723. URL: https://doi.org/10.1145/3320269.3384723.

Kunz et al.: Privacy Smells: Detecting Privacy Problems in Cloud Architectures **kunz2020privacysmells**

I. Kunz, A. Schneider, and C. Banse. "Privacy Smells: Detecting Privacy Problems in Cloud Architectures". In: *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. 2020, pp. 1324–1331. DOI: 10.1109/TrustCom50675.2020.00178.

Kunz et al.: Selecting Privacy Enhancing Technologies for IoT-Based Services **kunz2020selecting**

Immanuel Kunz, Christian Banse, and Philipp Stephanow. "Selecting Privacy Enhancing Technologies for IoT-Based Services". In: *International Conference on Security and Privacy in Communication Systems*. Springer. 2020, pp. 455–474.

Kunz et al.: Towards Tracking Data Flows in Cloud Architectures **kunz2020towards**

Immanuel Kunz, Valentina Casola, Angelika Schneider, Christian Banse, and Julian Schütte. "Towards Tracking Data Flows in Cloud Architectures". In: *2020 IEEE 13th International Conference on Cloud Computing (CLOUD)*. IEEE. 2020, pp. 445–452.

Kunz et al.: An Edge Framework for the Application of Privacy Enhancing Technologies in IoT Communications **kunz2020edge**

Immanuel Kunz, Philipp Stephanow, and Christian Banse. "An Edge Framework for the Application of Privacy Enhancing Technologies in IoT Communications". In: *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE. 2020, pp. 1–6.

Kuzhiyelil et al.: Towards Transparent Control-Flow Integrity in Safety-Critical Systems **KZK+20**

Don Kuzhiyelil, Philipp Zieris, Marine Kadar, Sergey Tverdyshev, and Gerhard Fohler. "Towards Transparent Control-Flow Integrity in Safety-Critical Systems". In: *Proceedings of the 23rd International Conference on Information Security*. ISC '20. Bali, Indonesia: Springer, 2020, pp. 290–311. ISBN: 9783030629748. DOI: 10.1007/978-3-030-62974-8_17. URL: https://doi.org/10.1007/978-3-030-62974-8_17.

Markert et al.: Adversarial Attacks on Speech Recognition Systems: Language Bias in Literature **MMB20**

Karla Markert, Donika Mirdita, and Konstantin Böttinger. "Adversarial Attacks on Speech Recognition Systems: Language Bias in Literature". In: *ACM Computer Science in Cars Symposium (CSCS)*. Online, 2020.

Markert et al.: Visualizing Automatic Speech Recognition **MPSB20**

Karla Markert, Romain Parracone, Philip Sperl, and Konstantin Böttinger. "Visualizing Automatic Speech Recognition". In: *Annual Computer Security Applications Conference (ACSAC)*. Online, 2020.

Müller et al.: Data Poisoning Attacks on Regression Learning and Corresponding Defenses **MKB20**

N. Müller, D. Kowatsch, and K. Böttinger. "Data Poisoning Attacks on Regression Learning and Corresponding Defenses". In: *25th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC)*. 2020.

Müller et al.: Defending Against Adversarial Denial-of-Service Data Poisoning Attacks **MRB20**

N. Müller, S. Roschmann, and K. Böttinger. "Defending Against Adversarial Denial-of-Service Data Poisoning Attacks". In: *DYNAMICS Workshop, Annual Computer Security Applications Conference (ACSAC)*. 2020.

Neubauer et al.: Security Risk Analysis of the Cloud Infrastructure of Smart Grid and IoT - 4-Level-Trust-Model as a Security Solution **sfischer2020**

Katrin Neubauer, Sebastian Fischer, and Rudolf Hackenberg. "Security Risk Analysis of the Cloud Infrastructure of Smart Grid and IoT - 4-Level-Trust-Model as a Security Solution". In: *International Journal on Advances in Internet Technology* 13.1 (2020), pp. 11–20.

Obermaier et al.: Analysis of Firmware Protection in State-of-the-Art Microcontrollers **ObermaierSchink2020Embedded**

Johannes Obermaier and Marc Schink. "Analysis of Firmware Protection in State-of-the-Art Microcontrollers". In: *Proceedings of the 2020 Embedded World Conference*. EWC '20. Nuremberg, Germany: WEKA Fachmedien, Feb. 2020.

Abstract: Embedded devices have to face many security threats that affect the confidentiality of their firmware and may even endanger the user's privacy. For this purpose, almost every microcontroller features read-out protection mechanisms. They aim at securing the code, algorithms, and cryptographic keys against unauthorized access. Despite data sheets are promising strong security, research has shown repeatedly that this is often far from being true. In this work we want to shed light onto the "how" researchers and hobbyists approach embedded system security testing. We present and analyze several conceptual and implementation issues in state-of-the-art microcontrollers. While some concepts deliver a high level of security, others can be broken with low effort and almost no cost or complexity. These results demonstrate that securing a microcontroller may not be as easy as often perceived, as there are many potential pitfalls on the user's and chip developer's side. However, security testing could often have discovered such issues beforehand if done thoroughly.

Radev et al.: Exploiting Interfaces of Secure Encrypted Virtual Machines **radev2020exploiting**

Martin Radev and Mathias Morbitzer. "Exploiting Interfaces of Secure Encrypted Virtual Machines". In: *Proceedings of the 4rd Reversing and Offensive-oriented Trends Symposium*. ROOTS '20. Vienna, Austria: ACM, 2020.

Schanzenbach: Towards Self-sovereign, decentralized personal data sharing and identity management **schanzen2020diss**

Martin Schanzenbach. "Towards Self-sovereign, decentralized personal data sharing and identity management". Dissertation. München: Technische Universität München, 2020.

Sperl et al.: Optimizing Information Loss Towards Robust Neural Networks **SB20**

P. Sperl and K. Böttinger. "Optimizing Information Loss Towards Robust Neural Networks". In: *DYNAMICS Workshop, Annual Computer Security Applications Conference (ACSAC)*. 2020.

Sperl et al.: DLA: Dense-Layer-Analysis for Adversarial Example Detection **SKCLB20**

P. Sperl, C-Y. Kao, P. Chen, X. Lei, and K. Böttinger. "DLA: Dense-Layer-Analysis for Adversarial Example Detection". In: *5th IEEE European Symposium on Security and Privacy (EuroS&P)*. 2020.

Strieder et al.: Machine Learning of Physical Unclonable Functions using Helper Data, Revealing a Pitfall in the Fuzzy Commitment Scheme **DBLP:journals/iacr/StriederFP20**

Emanuele Strieder, Christoph Frisch, and Michael Pehl. "Machine Learning of Physical Unclonable Functions using Helper Data, Revealing a Pitfall in the Fuzzy Commitment Scheme". In: *IACR Cryptol. ePrint Arch.* 2020 (2020), p. 888. URL: https://eprint.iacr.org/2020/888.

Striegel et al.: Secure and user-friendly over-the-air firmware distribution in a portable faraday cage **DBLP:conf/wisec/StriegelHJMS20**

Martin Striegel, Johann Heyszl, Florian Jakobsmeier, Yacov Matveev, and Georg Sigl. "Secure and user-friendly over-the-air firmware distribution in a portable faraday cage". In: *WiSec '20: 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Linz, Austria, July 8-10, 2020*. Ed. by René Mayrhofer and Michael Roland. ACM, 2020, pp. 173–183. DOI: 10.1145/3395351.3399342. URL: https://doi.org/10.1145/3395351.3399342.

Unterstein et al.: Retrofitting Leakage Resilient Authenticated Encryption to Microcontrollers **DBLP:journals/tches/UntersteinSSTIH20**

Florian Unterstein, Marc Schink, Thomas Schamberger, Lars Tebelmann, Manuel Ilg, and Johann Heyszl. "Retrofitting Leakage Resilient Authenticated Encryption to Microcontrollers". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2020.4 (2020), pp. 365–388. DOI: 10.13154/tches.v2020.i4.365-388. URL: https://doi.org/10.13154/tches.v2020.i4.365-388.

Unterstein et al.: Secure Update of FPGA-based Secure Elements using Partial Reconfiguration **conf/trudevice20/UntersteinSZJTP20**

Florian Unterstein, Tolga Sel, Thomas Zeschg, Nisha Jacob, Michael Tempelmeier, Michael Pehl, and Fabrizio De Santis. "Secure Update of FPGA-based Secure Elements using Partial Reconfiguration". In: *TRUDEVICE 2020: 9th Workshop on Trustworthy Manufacturing and Utilization of Secure Devices* (2020). URL: https://eprint.iacr.org/2020/833.

Unterstein et al.: Secure Update of FPGA-based Secure Elements using Partial Reconfiguration **DBLP:journals/iacr/UntersteinSZJTP20**

Florian Unterstein, Tolga Sel, Thomas Zeschg, Nisha Jacob, Michael Tempelmeier, Michael Pehl, and Fabrizio De Santis. "Secure Update of FPGA-based Secure Elements using Partial Reconfiguration". In: *IACR Cryptol. ePrint Arch.* 2020 (2020), p. 833. URL: https://eprint.iacr.org/2020/833.

Wagner et al.: Applicability of Security Standards for Operational Technology by SMEs and Large Enterprises **Wagner2020Applicability**

Patrick Wagner, Gerhard Hansch, Christoph Konrad, Karl-Heinz John, Jochen Bauer, and Jörg Franke. "Applicability of Security Standards for Operational Technology by SMEs and Large Enterprises". In: *IN PRESS, 25th IEEE Conference on Emerging Technologies and Factory Automation*. ETFA '20. Vienna, Austria: IEEE, Sept. 2020, pp. 1544–1551. DOI: 10.1109/ETFA46521.2020.9212126.

Abstract: Establishing adequate cybersecurity for their operational technology (OT) is an existential challenge for manufacturing enterprises. Domain-specific security standards should provide essential support in this challenge. However, they cannot be implemented equally for enterprises of all sizes. We investigate to what extent domain-specific security standards for operational technology are applicable by small and medium-sized as well as large manufacturing enterprises, and how their individual need for action can be identified and addressed.We support our investigation with the results of two independent surveys among manufacturers about their needs for cybersecurity support. In the course of this investigation, we learned that most domain-specific security standards are well applicable to large enterprises. In contrast, small and medium-sized enterprises (SME) seek the support of security experts, who, for their part, are often struggling with a lack of experience in operational technology. To facilitate this cooperation, we provide an introduction for OT- and cybersecurity-experts to the respective basic concepts of their collaborators.

Wilke et al.: SEVurity: No Security Without Integrity - Breaking Integrity-Free Memory Encryption with Minimal Assumptions **wilke2020sevurity**

Luca Wilke, Jan Wichelmann, Mathias Morbitzer, and Eisenbarth Thomas. "SEVurity: No Security Without Integrity - Breaking Integrity-Free Memory Encryption with Minimal Assumptions". In: *2020 IEEE Symposium on Security and Privacy, SP 2020, San Francisco, CA, USA, MAY 18-20, 2020*. IEEE. 2020.

Angermeier et al.: Modeling security risk assessments **AngermeierBeilkeHanschetal.2019**

Daniel Angermeier, Kristian Beilke, Gerhard Hansch, and Jörn Eichler. "Modeling security risk assessments". In: *17th escar Europe : embedded security in cars (Konferenzveröffentlichung)*. 2019. DOI: 10.13154/294-6670.

Auer et al.: A Security Architecture for RISC-V based IoT Devices **ASK19**

Lukas Auer, Christian Skubich, and Matthias Hiller. "A Security Architecture for RISC-V based IoT Devices". In: *Design, Automation & Test in Europe Conference & Exhibition (DATE)*. 2019.

Bogad et al.: Harzer Roller: Linker-Based Instrumentation for Enhanced Embedded Security Testing **harzer**

Katharina Bogad and Manuel Huber. "Harzer Roller: Linker-Based Instrumentation for Enhanced Embedded Security Testing". In: *Proceedings of the 3rd Reversing and Offensive-oriented Trends Symposium*. ROOTS '19. Vienna, Austria: ACM, 2019.

Cho et al.: Towards Quantum-resistant Virtual Private Networks **chogaz19**

Joo Cho, Stefan-Lukas Gazdag, Alexander von Gernler, Helmut Grießer, Sophia Grundner-Culemann, Tobias Guggemos, Tobias Heider, and Daniel Loebenberger. "Towards Quantum-resistant Virtual Private Networks". In: *31. Krypto-Tag, Berlin, Germany, October 17-18, 2019*. Ed. by Marcel Selhorst, Daniel Loebenberger, and Michael Nüsken. Gesellschaft für Informatik e.V. / FG KRYPTO, 2019. DOI: 10.18420/cdm-2019-31-22. URL: https://doi.org/10.18420/cdm-2019-31-22.

Engelmann et al.: Clear Sanctions, Vague Rewards: How China's Social Credit System Currently Defines" Good" and" Bad" Behavior **engelmann2019clear**

Severin Engelmann, Mo Chen, Felix Fischer, Ching-yu Kao, and Jens Grossklags. "Clear Sanctions, Vague Rewards: How China's Social Credit System Currently Defines" Good" and" Bad" Behavior". In: *Proceedings of the Conference on Fairness, Accountability, and Transparency*. 2019, pp. 69–78.

Fischer et al.: Stack overflow considered helpful! deep learning security nudges towards stronger cryptography **fischer2019stack**

Felix Fischer, Huang Xiao, Ching-Yu Kao, Yannick Stachelscheid, Benjamin Johnson, Danial Razar, Paul Fawkesley, Nat Buckley, Konstantin Böttinger, Paul Muntean, et al. "Stack overflow considered helpful! deep learning security nudges towards stronger cryptography". In: *28th {USENIX} Security Symposium ({USENIX} Security 19)*. 2019, pp. 339–356.

Fischer et al.: IoTAG: An Open Standard for IoT Device IdentificAtion and RecoGnition **sfischer2019IoTAG**

Sebastian Fischer, Katrin Neubauer, Lukas Hinterberger, Bernhard Weber, and Rudolf Hackenberg. "IoTAG: An Open Standard for IoT Device IdentificAtion and RecoGnition". In: *SECURWARE 2019, The Thirteenth International Conference on Emerging Security Information, Systems and Technologies*. 2019, pp. 107–113.

Abstract: With the increasing amount of Internet of Things (IoT) devices in smart homes, insecure and old devices are leading to big security issues. A private network can be attacked over an insecure IoT device, to use it in a botnet or infect it with ransomware and compromise the whole network. Non-technical users do not know which devices in their homes are secure and how to keep track of all the old and new ones. We have built a typical smart home as a test environment to evaluate a scoring system for the security of the whole network. First, all devices are discovered with nmap and then all the possible information, like the open ports or the Wi-Fi technology, are retrieved. In the next step, all the information leads to an overall score for each device. Combined together, the final score for the whole network is created. A non-technical user can now determine,

if the network is secure or not. We show the proof of concept of the scoring system with our test environment. However, some challenges exist. Not all information can be retrieved by just scanning the devices over the network. Some devices just return hostnames like "ESP 6A786B". It is nearly impossible to tell the kind of device and the manufacturer. Additionally, no information about the running firmware is provided. To calculate a meaningful score, much more information has to be collected. To collect the missing data, we introduce the first version of a new, open standard for IoT Device IdentificAtion and RecoGnition (IoTAG). This JSON based model provides all the important information about the device. Besides the device name, type and the manufacturer, it shows a list of the services, the firmware version and the supported encryption. IoTAG allows to create an overview of the whole IoT network and the development of an automated scoring system. In the future, additional information about security vulnerabilities can be collected from the Internet, to warn the user about insecure devices.

Fischer et al.: Analyzing power consumption of TLS ciphers on an ESP32 **fislin19**

Tilo Fischer, Hendrik Linka, Michael Rademacher, Karl Jonas, and Daniel ERROR Cannot find 'sis.bcf'!Loebenberger "Analyzing power consumption of TLS ciphers on an ESP32". In: *30. Krypto-Tag, Berlin, Germany, March 28-29, 2019*. Ed. by Franziskus Kiefer and Daniel Loebenberger. Gesellschaft für Informatik e.V. / FG KRYPTO, 2019. DOI: 10.18420/cdm-2019-30-04. URL: https://doi.org/10.18420/cdm-2019-30-04.

Gazdag et al.: Post-Quantum Software Updates: A case study on Code Signing with Hash-based Signatures **gazloe19**

Stefan-Lukas Gazdag and Daniel Loebenberger. "Post-Quantum Software Updates: A case study on Code Signing with Hash-based Signatures". In: *INFORMATIK 2019: Konferenzbeiträge der 49. Jahrestagung der Gesellschaft für Informatik*. Ed. by Klaus David, Kurt Geihs, Martin Lange, and Gerd Stumme. Vol. P-294. Lecture Notes in Informatics. Bonn: Köllen Druck+Verlag GmbH, 2019, pp. 459–472. ISBN: 978-3-88579-688-6.

Giehl et al.: Edge-computing enhanced privacy protection for industrial ecosystems in the context of SMEs **giehl2019vappiano**

Alexander Giehl, Peter Schneider, Maximilian Busch, Florian Schnoes, Robin Kleinwort, and Michael F. Zaeh. "Edge-computing enhanced privacy protection for industrial ecosystems in the context of SMEs". In: *12TH CMI Conference 2019*. Copenhagen, Denmark: IEEE, 2019. DOI: 10.1109/CMI48017.2019.8962138.

Giehl et al.: A framework to assess impacts of cyber attacks in manufacturing **giehl2019secveri**

Alexander Giehl, Norbert Wiedermann, and Sven Plaga. "A framework to assess impacts of cyber attacks in manufacturing". In: *2019 11th International Conference on Computer and Automation Engineering Proceedings*. Perth, Australia: ACM, 2019. ISBN: 978-1-4503-6287-0. DOI: 10.1145/3313991.3314003. URL: https://doi.org/10.1145/3313991.3314003.

Gross et al.: Breaking TrustZone Memory Isolation through Malicious Hardware on a Modern FPGA-SoC **DBLP:conf/ccs/GrossJZS19**

Mathieu Gross, Nisha Jacob, Andreas Zankl, and Georg Sigl. "Breaking TrustZone Memory Isolation through Malicious Hardware on a Modern FPGA-SoC". In: *Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop, ASHES@CCS 2019, London, UK, November 15, 2019*. Ed. by Chip-Hong Chang, Ulrich Rührmair, Daniel E. Holcomb, and Patrick Schaumont. ACM, 2019, pp. 3–12. DOI: 10.1145/3338508.3359568. URL: https://doi.org/10.1145/3338508.3359568.

Gruber et al.: Differential Fault Attacks on KLEIN **DBLP:conf/cosade/GruberS19**

Michael Gruber and Bodo Selmke. "Differential Fault Attacks on KLEIN". In: *Constructive Side-Channel Analysis and Secure Design - 10th International Workshop, COSADE 2019, Darmstadt, Germany, April 3-5, 2019, Proceedings*. Ed. by Ilia Polian and Marc Stöttinger. Vol. 11421. Lecture Notes in Computer Science. Springer, 2019, pp. 80–95. DOI: 10.1007/978-3-030-16350-1_6. URL: https://doi.org/10.1007/978-3-030-16350-1_6.

Gruber et al.: Differential Fault Attacks on KLEIN **GruberS19**

Michael Gruber and Bodo Selmke. "Differential Fault Attacks on KLEIN". In: *Constructive Side-Channel Analysis and Secure Design - 10th International Workshop, COSADE 2019, Darmstadt, Germany, April 3-5, 2019, Proceedings*. Ed. by Ilia Polian and Marc Stöttinger. Vol. 11421. Lecture Notes in Computer Science. Springer, 2019, pp. 80–95. DOI: 10.1007/978-3-030-16350-1_6. URL: https://doi.org/10.1007/978-3-030-16350-1_6.

Hansch et al.: Deriving Impact-driven Security Requirements and Monitoring Measures for Industrial IoT **hansch2019deriving**

Gerhard Hansch, Peter Schneider, and Gerd Brost. "Deriving Impact-driven Security Requirements and Monitoring Measures for Industrial IoT". In: *5th ACM Cyber-Physical System Security Workshop*. CPSS '19. Auckland, New Zealand: ACM, July 2019. ISBN: 978-1-4503-6787-5/19/07. DOI: 10.1145/3327961.3329528.

Abstract: The emerging Industrial Internet of Things (IIoT) is characterized by heterogeneous systems, loose topologies, cross-company data flows, changing entities, and high cybersecurity requirements. This development makes a sound security architecture an even more pressing matter than before. The design of a valid security architecture should always reflect the protection needs, enable the derivation of security requirements, and ways to validate their effectiveness. While access management at the application layer is well established, securing the underlying network layers of an increasing number of communication links remains an open question. Currently, adapting to the dynamics of rapid technology changes requires reiterating time- and resource-intensive threat and risk analyses. Therefore, we introduce and apply a lightweight, graph-based process to create easy-to-build and machine-readable models of the reviewed IIoT systems, highlighting the assets they contain. Such a model allows us to derive abstract security requirements in a semi-automatic way. We use these requirements to propose appropriate protection and advanced monitoring measures as well as methods to validate their effective implementation. The catalog provided in this paper represents a security toolbox for these two security layers, tailored for the IIoT domain. Finally, it allows

for deriving rules for current anomaly detection solutions. Thus, we support the often-laborious definition and prioritization of monitoring rules by an impact-based automated approach. By connecting the catalog with the lightweight impact analysis, we provide a framework that dynamically derives recommendations and requirements from a variety of monitoring measures and techniques. Thereby we provide a general methodology that helps operators to strengthen the overall security of their IIoT systems.

Hansch et al.: A Unified Architecture for Industrial IoT Security Requirements in Open Platform Communications **hansch2019aunified**

Gerhard Hansch, Peter Schneider, Kai Fischer, and Konstantin Böttinger. "A Unified Architecture for Industrial IoT Security Requirements in Open Platform Communications". In: *24th IEEE Conference on Emerging Technologies and Factory Automation*. ETFA '19. Zaragoza, Spain: IEEE, Sept. 2019.

Abstract: We present a unified communication architecture for security requirements in the industrial internet of things. Formulating security requirements in the language of OPC-UA provides a unified method to communicate and compare security requirements within a heavily heterogeneous landscape of machines in the field. Our machine-readable data model provides a fully automatable approach for security requirement communication within the rapidly evolving fourth industrial revolution, which is characterized by high-grade interconnection of industrial infrastructures and self-configuring production systems. Capturing security requirements in an OPC-UA compliant and unified data model for industrial control systems enables strong use cases within modern production plants and future supply chains. We implement our data model as well as an OPC-UA server that operates on this model to show the feasibility of our approach. Further, we deploy and evaluate our framework within a reference project realized by 14 industrial partners and 7 research facilities within Germany.

Heinl et al.: MERCAT: A Metric for the Evaluation and Reconsideration of Certificate Authority Trustworthiness **heinl2019CCSW**

Michael P. Heinl, Alexander Giehl, Norbert Wiedermann, Sven Plaga, and Frank Kargl. "MERCAT: A Metric for the Evaluation and Reconsideration of Certificate Authority Trustworthiness". In: *Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop*. CCSW'19. London, United Kingdom: Association for Computing Machinery, 2019, 1–15. ISBN: 9781450368261. DOI: 10.1145/3338466.3358917. URL: https://doi.org/10.1145/3338466.3358917.

Immler et al.: Secure Physical Enclosures from Covers with Tamper-Resistance **ION+19**

Vincent Immler, Johannes Obermaier, Kuan Kuan Ng, Fei Xiang Ke, Jin Ju Lee, Yak Peng Lim, Wei Koon Oh, Keng Hoong Wee, and Georg Sigl. "Secure Physical Enclosures from Covers with Tamper-Resistance". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2019.1 (2019).

Immler et al.: New Insights to Key Derivation for Tamper-Evident Physical Unclonable Functions **IU19**

Vincent Immler and Karthik Uppund. "New Insights to Key Derivation for Tamper-Evident Physical Unclonable Functions". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2019), pp. 30–65.

Knoblauch et al.: Reducing implementation efforts in continuous auditing certification via an Audit API **banse2019wetice**

Dorian Knoblauch and Christian Banse. "Reducing implementation efforts in continuous auditing certification via an Audit API". In: *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. 2019.

Morbitzer: Scanclave: Verifying Application Runtime Integrity in Untrusted Environments **morbitzer2019scanclave**

Mathias Morbitzer. "Scanclave: Verifying Application Runtime Integrity in Untrusted Environments". In: *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. 2019.

Morbitzer et al.: Extracting Secrets from Encrypted Virtual Machines **morbitzer2019extract**

Mathias Morbitzer, Manuel Huber, and Julian Horsch. "Extracting Secrets from Encrypted Virtual Machines". In: *Proceedings of the Ninth ACM on Conference on Data and Application Security and Privacy*. CODASPY '19. Richardson, Texas, USA: ACM, 2019, p. 10. ISBN: 978-1-4503-6099-9. DOI: 10.1145/3292006.3300022. URL: https://doi.org/10.1145/3292006.3300022.

Müller et al.: Distributed Anomaly Detection of Single Mote Attacks in RPL Networks **MDKB19**

N. Müller, P. Debus, D. Kowatsch, and K. Böttinger. "Distributed Anomaly Detection of Single Mote Attacks in RPL Networks". In: *16th International Conference on Security and Cryptography (SECRYPT)*. 2019.

Müller et al.: A Privacy Policy Dataset for GDPR compliance **MKDMB19**

N. Müller, D. Kowatsch, P. Debus, D. Mirdita, and K. Böttinger. "A Privacy Policy Dataset for GDPR compliance". In: *22nd International Conference on Text Speech and Dialogue (TSD)*. 2019.

Müller et al.: Identifying Mislabeled Instances in Classification Datasets **MM19**

N. Müller and K. Markert. "Identifying Mislabeled Instances in Classification Datasets". In: *2019 International Joint Conference on Neural Networks (IJCNN)*. 2019.

Neubauer et al.: Risk Analysis of the Cloud Infrastructure of Smart Grid and Internet of Things **sfischer2019SmartGridIoT**

Katrin Neubauer, Sebastian Fischer, and Rudolf Hackenberg. "Risk Analysis of the Cloud Infrastructure of Smart Grid and Internet of Things". In: *CLOUD COMPUTING 2019, The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization*. 2019, pp. 82–87.

Abstract: Cloud Computing (CC), Internet of Thing (IoT) and Smart Grid (SG) are separate technologies. The digital transformation of the energy industry and the increasing digi- talization in the private sector connect these technologies. At the moment, CC is used as a service provider for IoT. Currently in Germany, the SG is under construction and a cloud connection to the infrastructure has not been implemented yet. To build the SG cloud, the new laws for privacy must be implemented and therefore it's important to know which data can be stored and distributed over a cloud. In order to be able to use future innovative services, SG and IoT must be combined. For this, in the next step we connect the SG infrastructure with the IoT. A potential insecure device and network (IoT) should be able to transfer data to and from a critical infrastructure (SG). In detail, we focus on two different connections: the communication between the smart meter switching box and the IoT device and the data transferred between the IoT and SG cloud. In our example, a connected charging station with cloud services is connected with a SG infrastructure. To create a really smart service, the charging station needs a connection to the SG to get the current amount of renewable energy in the grid. Private data, such as name, address and payment details, should not be transferred to the IoT cloud. With these two connections, new threads emerge. In this case, availability, confidentiality and integrity must be ensured. A risk analysis over all the cloud connections, including the vulnerability and the ability of an attacker and the resulting risk are developed in this paper.

Neubauer et al.: Work in Progress: Security Analysis for Safety-critical Systems: Smart Grid and IoT **sfischer2019SecurityAnalysisSmartGridIoT**

Katrin Neubauer, Sebastian Fischer, and Rudolf Hackenberg. "Work in Progress: Security Analysis for Safety-critical Systems: Smart Grid and IoT". In: *32nd GI/ITG International Conference on Architecture of Computing Systems May 20 – 21, 2019, Technical University of Denmark, Copenhagen, Denmark Workshop Proceedings*. 2019, pp. 101–106.

Abstract: Internet of Thing (IoT) and Smart Grid (SG) are separate technologies. The digital transformation of the energy industry and the increasing digitalization in the private sector connect these technologies. Currently in Germany, the SG is under construction. In order to use future innovative services, SG and IoT must be combined. For this, we connect the SG Infrastructure with the IoT. A potential insecure device and network (IoT) should be able to transfer data to and from a critical infrastructure (SG). Open research question in this context are the security requirements architecture SG and IoT and the mechanism for authentication and authorisation in future application (SG and IoT). Due to the increasing networking of the systems (SG and IoT) new threats and attack vectors arise. The attacks to the architecture influence the target of authenticity, security and privacy. For the security analysis we focus on two communication points: the communication between the smart meter gateway, and the IoT device. In our example, a connected charging station with cloud services is connected with a SG infrastructure. To create a really smart service, the charging station needs a connection to the SG to get the current amount of renewable energy in the grid. With this two connections, new threats emerge. A security analysis over all the connections, including the vulnerability and the ability of an attacker, is developed in this paper. The analysis shows us

challenges of the communication between IoT and SG. For this, we defined technical and organizational requirements for authentication and authorization. Current authentication and authorization mechanisms are no longer sufficient for the defined requirements. We present the Role-based trust model for Safetycritical Systems for these defined requirements. The new trust model is integrated into a role-based access control model. It defines data classes, which separate the sensitive and non-sensitive information.

Obermaier: Breaking and Restoring Embedded System Security - From Practical Attacks to Novel PUF-Based Physical Security Enclosures **phd-johannes-obermaier**

Johannes Obermaier. "Breaking and Restoring Embedded System Security - From Practical Attacks to Novel PUF-Based Physical Security Enclosures". Dissertation. München: Technische Universität München, 2019.

Ohlendorf et al.: Digitale Identitäten auf dem Smartphone **ohlendorf2019digitale**

Tim Ohlendorf, Wolfgang Studier, and Marian Margraf. "Digitale Identitäten auf dem Smartphone". In: *Datenschutz und Datensicherheit-DuD* 43.1 (2019), pp. 17–22.

Pfeiffer et al.: Security-Management-as-a-Service **pfeiffer2019security**

Stefan Pfeiffer and Martin Seiffert. "Security-Management-as-a-Service". In: *Datenschutz und Datensicherheit-DuD* 43.1 (2019), pp. 23–27.

Plaga et al.: Securing future decentralised industrial IoT infrastructures: Challenges and free open source solutions **PLAGA2019596**

Sven Plaga, Norbert Wiedermann, Simon Duque Anton, Stefan Tatschner, Hans Schotten, and Thomas Newe. "Securing future decentralised industrial IoT infrastructures: Challenges and free open source solutions". In: *Future Generation Computer Systems* 93 (2019). Ergebnispräsentation im Rahmen von IUNO AP4 in der April 2019 Ausgabe des Elsevier Future Generation Computer Systems Journal, pp. 596 –608. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2018.11.008. URL: http://www.sciencedirect.com/science/article/pii/S0167739X18314043.

Abstract: The next industrial revolution is said to be paved by the use of novel Internet of Things (IoT) technology. One important aspect of the modern IoT infrastructures is decentralised communication, often called Peer-to-Peer (P2P). In the context of industrial communication, P2P contributes to resilience and improved stability for industrial components. Current industrial facilities, however, still rely on centralised networking schemes which are considered to be mandatory to comply with security standards. In order to succeed, introduced industrial P2P technology must maintain the current level of protection and also consider possible new threats. The presented work starts with a short analysis of well-established industrial communication infrastructures and how these could benefit from decentralised structures. Subsequently, previously undefined Information Technology (IT) security requirements are derived from the new cloud based decentralised industrial automation model architecture presented in this paper. To meet those requirements, state-of-the-art communication schemes and their open source implementations are presented and assessed for their usabil-

ity in the context of industrial IoT. Finally, derived building blocks for industrial IoT P2P security are presented which are qualified to comply with the stated industrial IoT security requirements.

Schanzenbach et al.: ZKlaims: Privacy-preserving Attribute-based Credentials using Non-interactive Zero-knowledge Techniques **schanzen2019zklaims**

Martin Schanzenbach, Thomas Kilian, Julian Schütte, and Christian Banse. "ZKlaims: Privacy-preserving Attribute-based Credentials using Non-interactive Zero-knowledge Techniques". In: *Proceedings of the 16th International Conference on Security and Cryptography (SECRYPT 2019), part of ICETE*. 2019.

Schink et al.: Taking a Look into Execute-Only Memory **SchinkXom2019**

Marc Schink and Johannes Obermaier. "Taking a Look into Execute-Only Memory". In: *13th USENIX Workshop on Offensive Technologies (WOOT 19)*. Santa Clara, CA: USENIX Association, Aug. 2019. URL: https://www.usenix.org/conference/woot19/presentation/schink.

Schneider: Do's and Don'ts of Distributed Intrusion Detection in Cyber-Physical Systems **schneider2019**

Peter Schneider. "Do's and Don'ts of Distributed Intrusion Detection in Cyber-Physical Systems". In: *accepted at CyberHunt at BigData*. 2019.

Abstract: New methods for anomaly and intrusion detection systems for industrial use cases promise to detect yet unknown attack vectors. Advances in big data processing and machine learning brought many methods with great detection possibil- ities to reduce human workload required. However, many of the detection methods suffer from false positive alerts which counter this goal. As optimization of detection rates is often linked to an increase of false positive rates, we analyze their impact regarding attack detection throughout networks. This enables orchestrated distributed anomaly detection and better forensic analyses of attack strategies. For this purpose, we propose a concept for information aggregation enabling a compound analysis of the involved systems. Using simulations of different configurations, we estimate the impact of detection rates, false positive rates, as well as network topologies on the global system performance. By this study, we provide a method for analyzing the detection capabilities of specific distributed detection system setups allowing for the derivation of appropriate requirements before actual deployment.

Schneider et al.: Realistic Data Generation for Anomaly Detection in Industrial Settings Using Simulations **schneider2018datagen**

Peter Schneider and Alexander Giehl. "Realistic Data Generation for Anomaly Detection in Industrial Settings Using Simulations". In: *Computer Security*. Ed. by Sokratis K. Katsikas, Frédéric Cuppens, Nora Cuppens, Costas Lambrinoudakis, Annie Antón, Stefanos Gritzalis, John Mylopoulos, and Christos Kalloniatis. Cham: Springer International Publishing, 2019, pp. 119–134. ISBN: 978-3-030-12786-2.

Abstract: With the rise of advanced persistent threats to cyber-physical facilities, new methods for anomaly detection are required. However, research on anomaly detection systems for industrial networks suffers from the lack of suitable training data to verify the methods at early stages. This paper presents a framework and workflow to generate meaningful training and test data for

anomaly detection systems in industrial settings. Using process-model based simulations data can be generated on a large scale. We evaluate the data in regard to its usability for state-of-the-art anomaly detection systems. With adequate simulation configurations, it is even possible to simulate a sensor manipulation attack on the model and to derive labeled data.

Schulze et al.: Context by Proxy: Identifying Contextual Anomalies Using an Output Proxy SIGKDD19

Jan-Philipp Schulze, Artur Mrowca, Elizabeth Ren, Hans-Andrea Loeliger, and Konstantin Böttinger. "Context by Proxy: Identifying Contextual Anomalies Using an Output Proxy". In: *The 25th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*. KDD '19. Anchorage, AK, USA: ACM, 2019. ISBN: 978-1-4503-6201-6/19/08. DOI: 10.1145/3292500.3330780. URL: https://doi.org/10.1145/3292500.3330780.

Schütte et al.: liOS: Lifting iOS Apps for Fun and Profit schuette2019

Julian Schütte and Dennis Titze. "liOS: Lifting iOS Apps for Fun and Profit". In: *Proceedings of the International Workshop on Secure Internet of Things (SIoT)*. Luxembourg: IEEE, 2019.

Selmke et al.: Peak Clock: Fault Injection into PLL-Based Systems via Clock Manipulation selmke2019

Bodo Selmke, Florian Hauschild, and Johannes Obermaier. "Peak Clock: Fault Injection into PLL-Based Systems via Clock Manipulation". In: *Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop*. 2019. DOI: 10.1145/3338508.3359577. URL: https://doi.org/10.1145/3338508.3359577.

Sperl et al.: Side-Channel Aware Fuzzing Sperl2019

Philip Sperl and Konstantin Böttinger. "Side-Channel Aware Fuzzing". In: *Proceedings of 24rd European Symposium on Research in Computer Security (ESORICS)*. Lecture Notes in Computer Science. Springer, Sept. 2019.

Striegel et al.: Smart Intersections Improve Traffic Flow and Road Safety DBLP:journals/ercim/StriegelO19

Martin Striegel and Thomas Otto. "Smart Intersections Improve Traffic Flow and Road Safety". In: *ERCIM News* 2019.119 (2019). URL: https://ercim-news.ercim.eu/en119/special/smart-intersections-improve-traffic-flow-and-road-safety.

Striegel et al.: EyeSec: A Retrofittable Augmented Reality Tool for Troubleshooting Wireless Sensor Networks in the Field StriegelEtAl2019

Martin Striegel, Carsten Rolfes, Fabian Helfert, Max Hornung, Johann Heyszl, and Georg Sigl. "EyeSec: A Retrofittable Augmented Reality Tool for Troubleshooting Wireless Sensor Networks in the Field". In: *Proceedings of the 2019 International Conference on Embedded Wireless Systems and Networks, EWSN 2019, Beijing, China, February 25-27, 2019*. 2019, pp. 184–193.

Unterstein et al.: SCA Secure and Updatable Crypto Engines for FPGA SoC Bitstream Decryption **DBLP:conf/ccs/UntersteinJHGH19**

Florian Unterstein, Nisha Jacob, Neil Hanley, Chongyan Gu, and Johann Heyszl. "SCA Secure and Updatable Crypto Engines for FPGA SoC Bitstream Decryption". In: *Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop, ASHES@CCS 2019, London, UK, November 15, 2019*. Ed. by Chip-Hong Chang, Ulrich Rührmair, Daniel E. Holcomb, and Patrick Schaumont. ACM, 2019, pp. 43–53. DOI: 10.1145/3338508.3359573. URL: https://doi.org/10.1145/3338508.3359573.

Weiss et al.: Annotary: A Concolic Execution System for Developing Secure Smart Contracts **Weiss2019**

Konrad Weiss and Julian Schütte. "Annotary: A Concolic Execution System for Developing Secure Smart Contracts". In: *Proceedings of 24rd European Symposium on Research in Computer Security (ESORICS)*. Lecture Notes in Computer Science. Springer, Sept. 2019.

Wisiol et al.: Breaking the Lightweight Secure PUF: Understanding the Relation of Input Transformations and Machine Learning Resistance **wisiol2019BreakingLightweightSecurePUF**

Nils Wisiol, Georg T. Becker, Marian Margraf, Tudor A. A. Soroceanu, Johannes Tobisch, and Benjamin Zengin. "Breaking the Lightweight Secure PUF: Understanding the Relation of Input Transformations and Machine Learning Resistance". In: *Smart Card Research and Advanced Applications - 18th International Conference, CARDIS 2019, Prague, Czech Republic, November 11-13, 2019, Revised Selected Papers*. Ed. by Sonia Belaïd and Tim Güneysu. Vol. 11833. Lecture Notes in Computer Science. Springer, 2019, pp. 40–54. DOI: 10.1007/978-3-030-42068-0_3. URL: https://doi.org/10.1007/978-3-030-42068-0_3.

Xu et al.: Dominance as a New Trusted Computing Primitive for the Internet of Things **dominance**

Meng Xu, Manuel Huber, Zhichuang Sun, Paul England, Marcus Peinado, Sangho Lee, Andrey Marochko, Dennis Mattoon, Rob Spiger, and Stefan Thom. "Dominance as a New Trusted Computing Primitive for the Internet of Things". In: *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2019.

Böttinger et al.: Deep Reinforcement Fuzzing **refuzz**

Konstantin Böttinger, Rishabh Singh, and Patrice Godefroid. "Deep Reinforcement Fuzzing". In: *IEEE Symposium on Security and Privacy Workshops 2018*. 2018.

Bramm et al.: BDABE-Blockchain-based Distributed Attribute based Encryption. **bramm2018bdabe**

Georg Bramm, Mark Gall, and Julian Schütte. "BDABE-Blockchain-based Distributed Attribute based Encryption." In: *ICETE (2)*. 2018, pp. 265–276.

Fischer: Testing Cryptographically Secure Pseudo Random Number Generators with Artificial Neural Networks **Fischer2018**

Tilo Fischer. "Testing Cryptographically Secure Pseudo Random Number Generators with Artificial Neural Networks". In: *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. TrustCom '18. Newark, New Jersey: IEEE, 2018, pp. 1214–1223. DOI: 10.1109/TrustCom/BigDataSE.2018.00168.

Gerd S. Brost et al.: An Ecosystem and IoT Device Architecture for Building Trust in the Industrial Data Space **brosthuber2018**

Manuel Huber Gerd S. Brost, Julian Schütte Michael Weiß Mykolai Protsenko, and Sascha Wessel. "An Ecosystem and IoT Device Architecture for Building Trust in the Industrial Data Space". In: *CPSS'18: The 4th ACM Cyber-Physical System Security Workshop*. CPSS'18. Incheon, Republic of Korea: ACM, 2018, pp. 39–50. ISBN: 978-1-4503-5755-5. DOI: 10.1145/3198458.3198459. URL: https://doi.org/10.1145/3198458.3198459.

Giehl et al.: Implementing a Performant Security Control for Industrial Ethernet **giehl2018impl**

Alexander Giehl and Sven Plaga. "Implementing a Performant Security Control for Industrial Ethernet". In: *2018 International Conference on Signal Processing and Information Security*. Dubai, United Arab Emirates: IEEE, 2018. DOI: 10.1109/CSPIS.2018.8642758. URL: https://doi.org/10.1109/CSPIS.2018.8642758.

Giehl et al.: Security verification of third party design files in manufacturing **giehl2018secver**

Alexander Giehl and Norbert Wiedermann. "Security verification of third party design files in manufacturing". In: *2018 10th International Conference on Computer and Automation Engineering Proceedings*. Best Presentation Award. Brisbane, Australia: ACM, 2018. ISBN: 978-1-4503-6410-2/18/02. DOI: 10.1145/3192975.3192984. URL: https://doi.org/10.1145/3192975.3192984.

Gräther et al.: Blockchain for Education: Lifelong Learning Passport **graether2018**

Wolfgang Gräther, Sabine Kolvenbach, Rudolf Ruland, Julian Schütte, Christof Torres, and Florian Wendland. "Blockchain for Education: Lifelong Learning Passport". In: *Proceedings of 1st ERCIM Blockchain Workshop 2018*. Reports of the European Society for Socially Embedded Technologies: vol. 2, no. 10. European Society for Socially Embedded Technologies (EUSSET), 2018.

Hänsch et al.: Programming Experience Might Not Help in Comprehending Obfuscated Source Code Efficiently **Haensch2018**

Norman Hänsch, Andrea Schankin, Mykolai Protsenko, Felix Freiling, and Zinaida Benenson. "Programming Experience Might Not Help in Comprehending Obfuscated Source Code Efficiently". In: *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Baltimore, MD: USENIX Asso-

ciation, 2018, pp. 341–356. ISBN: 978-1-931971-45-4. URL: https://www.usenix.org/conference/soups2018/presentation/hansch.

Hesselbarth et al.: Large Scale RO PUF Analysis over Slice Type, Evaluation Time and Temperature on 28nm Xilinx FPGAs **hesselbarth2018rosurvey**

Robert Hesselbarth, Florian Wilde, Chongyan Gu, and Hanley Neil. "Large Scale RO PUF Analysis over Slice Type, Evaluation Time and Temperature on 28nm Xilinx FPGAs". en. In: *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. Washington DC, USA, 2018. URL: tobepublishedinMay.

Abstract: Runtime accessible, general purpose, secure secret storage based on physical unclonable functions (PUFs) implemented within the programmable logic fabric is one of the most interesting applications of PUFs on field programmable gate arrays (FPGAs). To properly evaluate the quality of a PUF design, data from a large number of devices is required. This work therefore publishes a dataset containing 100 repeated measurements of 6592 ring oscillators (ROs) on 217 Xilinx Artix-7 XC7A35T FPGAs. This is both larger, and based on a more recent technology node than other publicly available datasets of related work. Apart from making the raw data publicly available, a thorough analysis is performed. The location and type of slice is found to affect the RO frequency by approx. 5 MHz, fast switching logic decreases the frequency by approx. 10 MHz, and ROs adjacent to clock routing resources showed an expected frequency of 20 MHz less than others on the device. We also address the time-to-response of ring oscillator PUFs (RO-PUFs), which can be large, by optimizing the evaluation time with regard to the measurement precision and found 70.71 μs to be optimal for the device and architecture under test. The temperature induced bit error rate was estimated to be 3.5 % and 5.8 % for temperature differences of 60 °C and 100 °C respectively. Finally, access to the FPGA array used to obtain the data will be granted to interested researchers.

Hristozov et al.: Practical Runtime Attestation for Tiny IoT Devices **HristozovEtAl2018**

Stefan Hristozov, Johann Heyszl, Steffen Wagner, and Georg Sigl. "Practical Runtime Attestation for Tiny IoT Devices". In: *NDSS Workshop on Decentralized IoT Security and Standards (DISS) 2018, San Diego, CA, USA*. 2018. ISBN: 1-891562-51-7. DOI: https://dx.doi.org/10.14722/diss.2018.23011. URL: www.ndss-symposium.org.

Huber et al.: Freeze and Crypt: Linux Kernel Support for Main Memory Encryption **fandc-cose**

Manuel Huber, Julian Horsch, Junaid Ali, and Sascha Wessel. "Freeze and Crypt: Linux Kernel Support for Main Memory Encryption". In: *Computers & Security* (2018). ISSN: 0167-4048. DOI: 10.1016/j.cose.2018.08.011. URL: http://www.sciencedirect.com/science/article/pii/S0167404818310435.

Immler et al.: Variable-Length Bit Mapping and Error Correcting Codes for Higher-Order Alphabet PUFs **IHL+18**

Vincent Immler, Matthias Hiller, Qinzhi Liu, Andreas Lenz, and Antonia Wachter-Zeh. "Variable-Length Bit Mapping and Error Correcting Codes for Higher-Order Alphabet PUFs". In: *Journal of Hardware and Systems Security (HASS)* 2.4 (2018).

Immler et al.: B-TREPID: Batteryless Tamper-Resistant Envelope with a PUF and Integrity Detection **IOK+18**

Vincent Immler, Johannes Obermaier, Martin König, Matthias Hiller, and Georg Sigl. "B-TREPID: Batteryless Tamper-Resistant Envelope with a PUF and Integrity Detection". In: *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. 2018, pp. 49–56.

Immler et al.: Your rails cannot hide from localized EM: how dual-rail logic fails on FPGAs—extended version **ISU18**

Vincent Immler, Robert Specht, and Florian Unterstein. "Your rails cannot hide from localized EM: how dual-rail logic fails on FPGAs—extended version". In: *Journal of Cryptographic Engineering* (2018).

Kalysch et al.: Tackling Androids Native Library Malware with Robust, Efficient and Accurate Similarity Measures **Kalysch2018**

Anatoli Kalysch, Oskar Milisterfer, Mykolai Protsenko, and Tilo Müller. "Tackling Androids Native Library Malware with Robust, Efficient and Accurate Similarity Measures". In: *Proceedings of the 13th International Conference on Availability, Reliability and Security*. ARES 2018. Hamburg, Germany: ACM, 2018, 58:1–58:10. ISBN: 978-1-4503-6448-5. DOI: 10.1145/3230833.3232828. URL: http://doi.acm.org/10.1145/3230833.3232828.

Kleber et al.: Secure Code Execution: A Generic PUF-driven System Architecture **KUH+18**

Stephan Kleber, Florian Unterstein, Matthias Hiller, Frank Slomka, Matthias Matousek, Frank Kargl, and Christoph Bösch. "Secure Code Execution: A Generic PUF-driven System Architecture". In: *Information Security Conference (ISC)*. Ed. by Liqun Chen and Mark Manulis. LNCS. Springer, 2018.

Koppermann et al.: Fast FPGA Implementations of Diffie-Hellman on the Kummer Surface of a Genus-2 Curve **koppermann2018kummer**

Philipp Koppermann, Fabrizio De Santis, Johann Heyszl, and Georg Sigl. "Fast FPGA Implementations of Diffie-Hellman on the Kummer Surface of a Genus-2 Curve". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2018.1 (2018), pp. 1–17. DOI: 10.13154/tches.v2018.i1.1-17. URL: https://doi.org/10.13154/tches.v2018.i1.1-17.

Matthias Niedermaier, Thomas Hanka, Sven Plaga, Alexander von Bodisco, Dominik Merli: Efficient Passive ICS Device Discovery and Identification by MAC Address Correlation **PlagaICS-CSR**

Matthias Niedermaier, Thomas Hanka, Sven Plaga, Alexander von Bodisco, Dominik Merli. "Efficient Passive ICS Device Discovery and Identification by MAC Address Correlation". In: *Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research 2018*. Electronic Workshops in Computing (eWiC). Zusammenarbeit mit der Hochschule Augsburg – status: präsentiert auf der ICS-CSR 2018/Hamburg (co-located with ARES 2018). Hamburg: British Computer Society Learning & Development Ltd., 2018. URL: https://ewic.bcs.org/category/19361 (visited on 09/09/2018).

Abstract: Owing to a growing number of attacks, the assessment of Industrial Control Systems (ICSs) has gained in importance. An integral part of an assessment is the creation of a detailed inventory of all connected devices, enabling vulnerability evaluations. For this purpose, scans of networks are crucial. Active scanning, which generates irregular traffic, is a method to get an overview of connected and active devices. Since such additional traffic may lead to an unexpected behavior of devices, active scanning methods should be avoided in critical infrastructure networks. In such cases, passive network monitoring offers an alternative, which is often used in conjunction with complex deep-packet inspection techniques. There are very few publications on lightweight passive scanning methodologies for industrial networks. In this paper, we propose a lightweight passive network monitoring technique using an efficient Media Access Control (MAC) address-based identification of industrial devices. Based on an incomplete set of known MAC address to device associations, the presented method can guess correct device and vendor information. Proving the feasibility of the method, an implementation is also introduced and evaluated regarding its efficiency. The feasibility of predicting a specific device/vendor combination is demonstrated by having similar devices in the database. In our ICS testbed, we reached a host discovery rate of 100% at an identification rate of more than 66%, outperforming the results of existing tools.

Morbitzer et al.: SEVered: Subverting AMD's Virtual Machine Encryption morbitzer2018

Mathias Morbitzer, Manuel Huber, Julian Horsch, and Sascha Wessel. "SEVered: Subverting AMD's Virtual Machine Encryption". In: *Proceedings of the 11th European Workshop on Systems Security*. EuroSec'18. Porto, Portugal: ACM, 2018. ISBN: 978-1-4503-5652-7. DOI: 10.1145/3193111.3193112. URL: https://doi.org/10.1145/3193111.3193112.

Obermaier et al.: An Embedded Key Management System for PUF-based Security Enclosures obermaier2018EKMS

Johannes Obermaier, Florian Hauschild, Matthias Hiller, and Georg Sigl. "An Embedded Key Management System for PUF-based Security Enclosures". In: *2018 7th Mediterranean Conference on Embedded Computing (MECO)*. 2018, pp. 1–6. DOI: 10.1109/MECO.2018.8406028.

Obermaier et al.: An Embedded Key Management System for PUF-based Security Enclosures OHHS18

Johannes Obermaier, Florian Hauschild, Matthias Hiller, and Georg Sigl. "An Embedded Key Management System for PUF-based Security Enclosures". In: *Mediterranean Conference on Embedded Computing (MECO)*. 2018.

Obermaier et al.: The Past, Present, and Future of Physical Security Enclosures: From Battery-Backed Monitoring to PUF-Based Inherent Security and Beyond OI18

Johannes Obermaier and Vincent Immler. "The Past, Present, and Future of Physical Security Enclosures: From Battery-Backed Monitoring to PUF-Based Inherent Security and Beyond". In: *IEEE International Workshop on Physical Attacks and Inspection on Electronics*. 2018.

Obermaier et al.: The Past, Present, and Future of Physical Security Enclosures: From Battery-Backed Monitoring to PUF-Based Inherent Security and Beyond **obermaier2018securityEnclosures**

Johannes Obermaier and Vincent Immler. "The Past, Present, and Future of Physical Security Enclosures: From Battery-Backed Monitoring to PUF-Based Inherent Security and Beyond". In: *Journal of Hardware and Systems Security* 2.4 (2018), pp. 289–296. ISSN: 2509-3436. DOI: 10.1007/s41635-018-0045-2. URL: https://doi.org/10.1007/s41635-018-0045-2.

Abstract: Withstanding physical attacks in a hostile environment is of utmost importance for nowadays electronics. However, due to the long and costly development of integrated circuits (ICs), IC-level countermeasures are typically only included in varying degree and not in every chip of a device. Therefore, multiple-chip modules requiring higher levels of security are additionally protected against tampering by a physical security enclosure, e.g., by an envelope that completely encloses the device. For decades, these physical boundaries on a device-level were monitored using battery-backed mechanisms to enable detection of an attempted physical intrusion even if the underlying system is powered off. However, the battery affects the system's robustness, weight, prevents extended storage, and also leads to difficulties with the security mechanism while shipping the device. In this position paper, we present our assessment of various battery-backed tamper-respondent solutions and argue that while offering the intriguing benefit of instantaneous detection and response, the low-power nature of battery-backup contradicts a tamper-sensitive measurement, among other problems. We are therefore of the opinion that more effort should be spent towards enclosures that are based on tamper-evident physical unclonable functions (PUFs), as they are designated to provide a high level of security on the one hand and do not require a battery on the other hand. To further substantiate our argument, we summarize the work in this domain to also facilitate future research.

Obermaier et al.: A Measurement System for Capacitive PUF-based Security Enclosures **obermaier2018MeasurementSystem**

Johannes Obermaier, Vincent Immler, Matthias Hiller, and Georg Sigl. "A Measurement System for Capacitive PUF-based Security Enclosures". In: *Proceedings of the 55th Annual Design Automation Conference*. DAC '18. San Francisco, California: ACM, 2018, 64:1–64:6. ISBN: 978-1-4503-5700-5. DOI: 10.1145/3195970.3195976. URL: http://doi.acm.org/10.1145/3195970.3195976.

Obermaier et al.: A Measurement System for Capacitive PUF-Based Security Enclosures **OIHS18**

Johannes Obermaier, Vincent Immler, Matthias Hiller, and Georg Sigl. "A Measurement System for Capacitive PUF-Based Security Enclosures". In: *ACM/IEEE Design Automation Conference (DAC)*. 2018.

Plaga et al.: Adding Channel Binding for an Out-of-Band OTP Authentication Protocol in an Industrial Use-Case **Plaga2017OTPAuth**

Sven Plaga, Melanie Niethammer, Norbert Wiedermann, and Alexander Borisov. "Adding Channel Binding for an Out-of-Band OTP Authentication Protocol in an Industrial Use-Case". In: *Proceedings of the 1st International Conference on Data Intelligence and Security*. ICDIS '18. Kooperation im

Rahmen von IUNO AP4, Fraunhofer AISEC mit BOSCH Corporate Sector Research and Advance Engineering submitted to "The 1st International Conference on Data Intelligence and Security". South Padre Island, Texas, USA: IEEE, 2018. ISBN: 978-1-5386-5762-1. DOI: 10.1109/ICDIS.2018.00048.

Abstract: Abstract—One Time Passwords (OTPs) are used to increase the security of the authentication process of networked applications. Smartphone based OTP schemes already brought usable and affordable multi-factor authentication to web applications. These schemes are also a promising approach for authentication in industrial applications. This paper introduces an industrial remote maintenance use-case that uses a smartphone based OTP authentication scheme using Quick-Response (QR) codes [1]. In addition to a main communication and password authentication channel, the proposed scheme requires an out-of-band communication channel to transmit OTPs via smartphone. While baseline security for the channels can be achieved with Transport Layer Security (TLS), Out-of-Band Authentication (OOBA) remains vulnerable to Man-in-the-Middle (MitM) attacks in environments where the authenticity of the communication partner cannot be guaranteed. In order to mitigate this problem, it is crucial to establish a secure channel association. The enhancement proposed in this paper thus cryptographically binds successful out-of-band OTP authentications to the prior established data-channel with the help of TLS channel binding [2]. Recommendations include common TLS libraries that support this feature as well as further considerations for a secure implementation.

Plaga et al.: Secure your SSH Keys! – Motivation and Practical Implementation of a HSM-based Approach Securing Private SSH-Keys **PlagaECCWS18**

Sven Plaga, Norbert Wiedermann, Hansch Gerhard, and Newe Thomas. "Secure your SSH Keys! – Motivation and Practical Implementation of a HSM-based Approach Securing Private SSH-Keys". In: *Proceedings of the 17th European Conference on Cyber Warfare and Security*. ECCWS '18. University of Oslo, Norway: Academic Conferences and Publishing International (ACPI) Limited, 2018, pp. 370–379. ISBN: 978-1-911218-85-2.

Abstract: Reliable authentication of entities is the baseline for secure communications infrastructures and services. While traditional password authentication is still widely deployed, alternatives based on asymmetric cryptography are also available and provide an increased level of security. On the client-side, however, secret keys are often unprotected. Although constantly updated workstations are considered to be trusted environments, security breaches such as Spectre or Meltdown raised doubts in platform integrity. The presented work introduces realistic attack vectors which can be employed to extract cryptographic keys from workstations. Consequently, Hardware Security Modules (HSMs) are introduced which provide secure storage as well as secure utilisation of private cryptographic keys. Due to the huge amount of possible application scenarios, the paper focuses on an application scenario based on the widely used Secure Shell (SSH) protocol. Demonstrating that an improved level of security is not necessarily directly linked to costs, a rough summary of interesting Commercial-off-the-Shelf (COTS) devices is provided.

Reinbrecht et al.: Earthquake - A NoC-based optimized differential cache-collision attack for MPSoCs **ReinbrechtEtAl2018**

Cezar Reinbrecht, Bruno Forlin, Andreas Zankl, and Johanna Sepúlveda. "Earthquake - A NoC-based optimized differential cache-collision attack for MPSoCs". In: *2018 Design, Automation &*

Test in Europe Conference & Exhibition, DATE 2018, Dresden, Germany, March 19-23, 2018. IEEE, 2018, pp. 648–653. ISBN: 978-3-9819263-0-9. DOI: 10.23919/DATE.2018.8342090. URL: https://doi.org/10.23919/DATE.2018.8342090.

S. Plaga, N. Wiedermann, M. Niedermaier, A. Giehl, T. Newe: Future Proofing IoT Embedded Platforms for Cryptographic Primitives Support PlagaICST2018

S. Plaga, N. Wiedermann, M. Niedermaier, A. Giehl, T. Newe. "Future Proofing IoT Embedded Platforms for Cryptographic Primitives Support". In: *12th International Conference on Sensing Technology 2018*. ICST'18. University of Limerick, Ireland: Institute of Electrical and Electronics Engineers (IEEE), 2018, pp. 52–57. DOI: 10.1109/ICSensT.2018.8603610.

Abstract: Information security is an important property in areas with distributed and decentralized communication like the Internet of Things (IoT) or Wireless Sensor Nodes (WSNs). Secure communication realises the protection goals of confidentiality, integrity, and authenticity, which are implemented by cryptographic functions. These functions need to evolve steadily in order to catch up with new attack vectors employed by cybercriminals. This cryptographic evolution brings an increase of resource demand and consumption with it as cryptographic functions rise in complexity. The demand is difficult to satisfy by embedded platforms since they are often limited in their resources due to design efficiency. Therefore, adequate resource buffering is a crucial task in designing embedded systems that are future proof from a security point of view. In this work, we introduce a methodology for comparable resource benchmarking of cryptographic functions on embedded systems. Our approach enables designers and developers of embed- ded systems to achieve comparable results over an extended range of algorithms and implementations. This aids in the estimation of the cryptographic resource footprint. Further, we develop a measurement architecture for experimentation on different embedded platforms. We conduct a sample of reference measurements confirming well-known patterns in cryptography showing the validity of our framework. Finally, we argue for an open collaboration platform for sharing of benchmark results conducted with the framework.

Schanzenbach et al.: Practical Decentralized Attribute-Based Delegation Using Secure Name Systems schanzenbach2018abd

M. Schanzenbach, C. Banse, and J. Schütte. "Practical Decentralized Attribute-Based Delegation Using Secure Name Systems". In: *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. 2018, pp. 244–251. DOI: 10.1109/TrustCom/BigDataSE.2018.00046.

Abstract: Identity and trust in the modern Internet are centralized around an oligopoly of identity service providers consisting solely of major tech companies. The problem with centralizing trust has become evident in recent discoveries of mass surveillance and censorship programs as well as information leakage through hacking incidents. One approach to decentralizing trust is distributed, attribute-based access control via attribute-based delegation (ABD). Attribute-based delegation allows a large number of cross-domain attribute issuers to be used in making authorization decisions. Attributes are not only issued to identities, but can also be delegated to other attributes issued by different entities in the system. The resulting trust chains can then be resolved by any entity given an appropriate attribute storage and resolution system. While current proposals often fail at the

practicability, we show how attribute-based delegation can be realized on top of the secure GNU Name System (GNS) to solve an authorization problem in a real-world scenario.

Schanzenbach et al.: reclaimID: Secure, Self-Sovereign Identities Using Name Systems and Attribute-Based Encryption **schanzenbach2018reclaim**

M. Schanzenbach, G. Bramm, and J. Schütte. "reclaimID: Secure, Self-Sovereign Identities Using Name Systems and Attribute-Based Encryption". In: *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. 2018, pp. 946–957. DOI: 10.1109/TrustCom/BigDataSE.2018.00134.

Abstract: In this paper we present reclaimID: An architecture that allows users to reclaim their digital identities by securely sharing identity attributes without the need for a centralised service provider. We propose a design where user attributes are stored in and shared over a name system under user-owned namespaces. Attributes are encrypted using attribute-based encryption (ABE), allowing the user to selectively authorize and revoke access of requesting parties to subsets of his attributes. We present an implementation based on the decentralised GNU Name System (GNS) in combination with ciphertext-policy ABE using type-1 pairings. To show the practicality of our implementation, we carried out experimental evaluations of selected implementation aspects including attribute resolution performance. Finally, we show that our design can be used as a standard OpenID Connect Identity Provider allowing our implementation to be integrated into standard-compliant services.

Schneider et al.: High-Performance Unsupervised Anomaly Detection for Cyber-Physical System Networks **schneider2018anomaly**

Peter Schneider and Konstantin Böttinger. "High-Performance Unsupervised Anomaly Detection for Cyber-Physical System Networks". In: *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy*. CPS-SPC '18. Toronto, Canada: ACM, 2018, pp. 1–12. ISBN: 978-1-4503-5992-4. DOI: 10.1145/3264888.3264890. URL: http://doi.acm.org/10.1145/3264888.3264890.

Abstract: While the ever-increasing connectivity of cyber-physical systems enlarges their attack surface, existing anomaly detection frame- works often do not incorporate the rising heterogeneity of involved systems. Existing frameworks focus on a single fieldbus protocol or require more detailed knowledge of the cyber-physical system itself. Thus, we introduce a uniform method and framework for applying anomaly detection to a variety of fieldbus protocols. We use stacked denoising autoencoders to derive a feature learning and packet classification method in one step. As the approach is based on the raw byte stream of the network traffic, neither spe- cific protocols nor detailed knowledge of the application is needed. Additionally, we pay attention on creating an efficient framework which can also handle the increased amount of communication in cyber-physical systems. Our evaluation on a Secure Water Treatment dataset using Eth- erNet/IP and a Modbus dataset shows that we can acquire network packets up to 100 times faster than packet parsing based methods. However, we still achieve precision and recall metrics for longer lasting attacks of over 99%.

Schütte et al.: LUCON: Data Flow Control for Message-Based IoT-Systems schuette2018

Julian Schütte and Gerd Brost. "LUCON: Data Flow Control for Message-Based IoT-Systems". In: *Proceedings of the International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. Aug. 2018.

Selmke et al.: Locked out by Latch-up? An Empirical Study on Laser Fault Injection into Arm Cortex-M Processors Selmke18

Bodo Selmke, Kilian Zinnecker, Philipp Koppermann, Katja Miller, Johann Heyszl, and Georg Sigl. "Locked out by Latch-up? An Empirical Study on Laser Fault Injection into Arm Cortex-M Processors". In: *2018 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2018, Amsterdam, The Netherlands, September 13, 2018*. IEEE Computer Society, 2018, pp. 7–14. DOI: 10.1109/FDTC.2018.00010. URL: https://doi.org/10.1109/FDTC.2018.00010.

Seydel et al.: Safety & Security Testing of Cooperative Automotive Systems Seydel:2018

Dominique Seydel, Gereon Weiß, Daniela Pöhn, Sascha Wessel, and Franz Wenninger. "Safety & Security Testing of Cooperative Automotive Systems". In: *Embedded World Conference 2018* (2018). Ed. by WEKA Fachmedien.

Unterstein et al.: High-Resolution EM Attacks Against Leakage-Resilient PRFs Explained - And An Improved Construction Unterstein2018Improving

Florian Unterstein, Johann Heyszl, Fabrizio De Santis, Robert Specht, and Georg Sigl. "High-Resolution EM Attacks Against Leakage-Resilient PRFs Explained - And An Improved Construction". In: *Cryptographers Track RSA Conference (CT-RSA 2018)*. Springer. 2018.

Weiser et al.: DATA – Differential Address Trace Analysis: Finding Address-based Side-Channels in Binaries WeiserEtAl2018

Samuel Weiser, Andreas Zankl, Raphael Spreitzer, Katja Miller, Stefan Mangard, and Georg Sigl. "DATA – Differential Address Trace Analysis: Finding Address-based Side-Channels in Binaries". In: *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, 2018, pp. 603–620. ISBN: 978-1-931971-46-1. URL: https://www.usenix.org/conference/usenixsecurity18/presentation/weiser.

Wendland et al.: Enhancing NFV Orchestration with Security Policies wendland2018secpoltoscanfv

Florian Wendland and Christian Banse. "Enhancing NFV Orchestration with Security Policies". In: *ARES 2018: International Conference on Availability, Reliability and Security, August 27–30, 2018, Hamburg, Germany*. New York, NY, USA: ACM, 2018. ISBN: 978-1-4503-6448-5/18/08. DOI: 10.1145/3230833.3233253.

Abstract: With cloud computing and the evolution towards 5G, dynamic, self-provisioned and flexible service architectures will become even more prominent. Instead of deploying a service and its component on a single platform, components may be spread out to run at the mobile edge. At the same time, mobile edge computing requires that services move around with their consumers. In this

highly dynamic service deployment scenario, it is important to maintain technology-agnostic service descriptions. In addition, these service descriptions must carry their associated security policies with them to be able to decide whether resources are usable when upscaling or moving a service. To this end, we illustrate the definition of security policies in the technology-agnostic TOSCA service specification language. Our goal is to initiate the development of a security policy catalog for NFV services and the implementation of the necessary software tools for their enforcement.

Wiedermann et al.: Rowhammer – A Survey Assessing the Severity of this Attack Vector
Wiedermann2018Embedded

Norbert Wiedermann and Sven Plaga. "Rowhammer – A Survey Assessing the Severity of this Attack Vector". In: *Proceedings of the 2018 Embedded World Conference*. EWC '18. Nuremberg, Germany: WEKA Fachmedien, Feb. 2018. ISBN: 978-3-645-50173-6.

Abstract: Dynamic random access memory (DRAM) is a cheap manufacturable main memory architecture and widely used in consumer and professional Information Technology (IT) systems. In March 2015 Seaborn et al. presented sample code to demonstrate how an already known technical issue of this memory architecture can be exploited by making use of insights from Kim et al. This work proofed that the issue can be abused to compromise current IT systems. Using this knowledge as starting point other research teams continued the work. A JavaScript based approach was for example presented by Gruss et al. As presented exploits gained high medial attention in non-scientific press, the rowhammer bug and mitigation strategies are still object of research. In this paper, the hardware related circumstances are reviewed and analysed to provide an understanding of the technical aspects which led to this bug. Based on related work an own test setup was used to comprehend the steps of the attack. The challenges in creating this independent and functional setup based on x86 and Linux are introduced. Additionally, constraints in mounting an attack on current Linux distributions and possible mitigation strategies are presented. This paper summarises the current state of the art and provides insight to this severe though complex attack vector. With the presented results it is possible to estimate future refinements of rowhammer and identify mitigation strategies for own designs.

Zieris et al.: A Leak-Resilient Dual Stack Scheme for Backward-Edge Control-Flow Integrity
zieris2018

Philipp Zieris and Julian Horsch. "A Leak-Resilient Dual Stack Scheme for Backward-Edge Control-Flow Integrity". In: *Proceedings of the 2018 ACM Asia Conference on Computer and Communications Security*. ASIA CCS '18. Incheon, Republic of Korea: ACM, June 2018. ISBN: 978-1-4503-5576-6. DOI: 10.1145/3196494.3196531. URL: http://doi.acm.org/10.1145/3196494.3196531.

Zieris et al.: A Leak-Resilient Dual Stack Scheme for Backward-Edge Control-Flow Integrity
zieris2018Double

Philipp Zieris and Julian Horsch. "A Leak-Resilient Dual Stack Scheme for Backward-Edge Control-Flow Integrity". In: *Proceedings of the 2018 ACM on Asia Conference on Computer and Communications Security*. ASIA CCS '18. Incheon, Republic of Korea: ACM, June 2018. ISBN: 978-1-4503-5576-6. DOI: 10.1145/3196494.3196531. URL: http://doi.acm.org/10.1145/3196494.3196531.

Ahadipour et al.: A Survey on Authorization in Distributed Systems: Information Storage, Data Retrieval and Trust Evaluation **ahadipou2017**

A. Ahadipour and M. Schanzenbach. "A Survey on Authorization in Distributed Systems: Information Storage, Data Retrieval and Trust Evaluation". In: *2017 IEEE Trustcom/BigDataSE/ICESS*. 2017, pp. 1016–1023. DOI: 10.1109/Trustcom/BigDataSE/ICESS.2017.346.

Abstract: In distributed environments, entities are distributed among different security domains and they do not have prior knowledge of one another. In this setting, distributed systems and their security components such as entities, certificates, credentials, policies and trust values are dynamic and constantly changing. Thus, access control models and trust approaches are necessary to support the dynamic and distributed features of such systems and their components. The objective of this paper is to present a comprehensive survey about the security research in distributed systems. We have reviewed the dynamic and distributed nature of the components and evaluation methods of major authorization systems and access control models in existing literature. Based on this overview, we present a survey of selected trust schemes. We provide a categorization for recommendation-based and reputation-based trust models based on trust evaluation. Additionally, we use credential or certificate storage and chain discovery methods for categorizing evidence-based and policy-based trust models. This work can be used as a reference guide to understand authorization and trust management and to further research fully decentralized and distributed authorization systems.

Atienza et al.: Design, Automation & Test in Europe Conference & Exhibition, DATE 2017, Lausanne, Switzerland, March 27-31, 2017 **DBLP:conf/date/2017**

David Atienza and Giorgio Di Natale, eds. *Design, Automation & Test in Europe Conference & Exhibition, DATE 2017, Lausanne, Switzerland, March 27-31, 2017*. IEEE, 2017. ISBN: 978-3-9815370-8-6. URL: http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=7919927.

Banse et al.: A Taxonomy-based Approach for Security in Software-Defined Networking **banse2017**

Christian Banse and Julian Schuette. "A Taxonomy-based Approach for Security in Software-Defined Networking". In: *2017 IEEE International Conference on Communications, ICC 2017, Paris, France, May 21-25, 2017*. 2017.

Abstract: Software Defined Networking (SDN) promises to abstract hardware and hard-wired network topologies in favor of programmable dynamic infrastructures. However, especially features like multi-tenancy require for new ways to ensure that access to critical network resources are restricted to trusted applications and users. The challenge here is that these entities are not necessarily known at the time of planning and setup, but are rather added dynamically to the network at runtime. Controlling access to northbound interfaces of SDN controllers thus requires for new ways to express access control policies which are able to cope with this degree of complexity and abstraction. We thus introduce a taxonomy-based policy engine, which allows the definition of fine-grained security policies based on a first-order logic description of the network environment. We describe the taxonomy structure and show how it can be used in a Prolog-based policy engine to protect a secure SDN northbound interface developed in previous work. By evaluating the imple-

mentation in a virtual SDN environment, we found the performance overhead of our approach to be tolerable.

Baumann et al.: Anti-ProGuard: Towards Automated Deobfuscation of Android Apps **Baumann_2017**

Richard Baumann, Mykolai Protsenko, and Tilo Müller. "Anti-ProGuard: Towards Automated Deobfuscation of Android Apps". In: *4th Workshop on Security in highly connected IT systems*. Ed. by ACM ICPS and co-located with DISCOTEC. Neuchâtel, Switzerland, 2017.

Böttinger: Guiding a Colony of Black-box Fuzzers with Chemotaxis **boettinger_2017**

Konstantin Böttinger. "Guiding a Colony of Black-box Fuzzers with Chemotaxis". In: *38th IEEE Symposium on Security and Privacy (S&P 2017) Workshops*. 2017.

Busch et al.: A Cloud-Based Compilation and Hardening Platform for Android Apps **Busch_2017**

Marcel Busch, Mykolai Protsenko, and Tilo Müller. "A Cloud-Based Compilation and Hardening Platform for Android Apps". In: *12th International Conference on Availability, Reliability and Security*. Ed. by SBA Research. Reggio Calabria, Italy, 2017. DOI: 10.1145/3098954.3098959.

Eckert: Cyber-Sicherheit in Industrie 4.0 **eckert2017handbuch**

Claudia Eckert. "Cyber-Sicherheit in Industrie 4.0". In: *Handbuch Industrie 4.0: Geschäftsmodelle, Prozesse, Technik*. Ed. by Gunther Reinhart. München: Carl Hanser Verlag, 2017, pp. 111–135.

Eckert: Cybersicherheit Beyond 2020! **Eckert2017**

Claudia Eckert. "Cybersicherheit Beyond 2020!" In: *50 Jahre Universitäts-Informatik in München*. Ed. by Arndt Bode, Manfred Broy, Hans-Joachim Bungartz, and Florian Matthes. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017, pp. 1–10. ISBN: 978-3-662-54712-0. DOI: 10.1007/978-3-662-54712-0_1. URL: http://dx.doi.org/10.1007/978-3-662-54712-0_1.

Abstract: Mit der Zusammenführung von physischen Systemen mit virtuellen Objekten zu Cyber-Physischen Systemen (CPS) schwinden die Grenzen zwischen digitaler und physikalischer Welt und damit auch ein bisher verlässlicher Schutzwall. Dies erhöht die potentiellen Auswirkungen von erfolgreichen Angriffen und macht ein prinzipielles Umdenken beim Umgang mit diesen Gefahren notwendig. Die Gewährleistung der Integrität, Vertraulichkeit und Verfügbarkeit sind die bekannten Schutzziele, die bereits bei der klassischen IT-Sicherheit verfolgt werden. Durch die Verbindung zwischen digitaler und physischer Welt wird jedoch die Erfüllung der Ziele zunehmend schwieriger und komplexer; die IT-Sicherheitsforschung steht vor neuen Herausforderungen. Der Beitrag diskutiert wichtige derartige Herausforderungen, wie die Erforschung proaktiver Schutzverfahren, die Entwicklung resilienter System-Architekturen oder aber auch die Erforschung neuer Ansätze für eine kontrollierbare Weitergabe und Nutzung von Informationen in vernetzten Umgebungen.

Eckert: Cybersicherheit beyond 2020! - Herausforderungen für die IT-Sicherheitsforschung **DBLP:journals/insk/Eckert17**

Claudia Eckert. "Cybersicherheit beyond 2020! - Herausforderungen für die IT-Sicherheitsforschung". In: *Informatik Spektrum* 40.2 (2017), pp. 141–146. DOI: 10.1007/s00287-017-1025-6. URL: https://doi.org/10.1007/s00287-017-1025-6.

Fischer et al.: Stack Overflow Considered Harmful? The Impact of Copy&Paste on Android Application Security **fischer2017so**

Felix Fischer, Konstantin Böttinger, Huang Xiao, Christian Stransky, Yasemin Acar, Michael Backes, and Sascha Fahl. "Stack Overflow Considered Harmful? The Impact of Copy&Paste on Android Application Security". In: *2017 IEEE Symposium on Security and Privacy (Oakland'17)*. IEEE. 2017.

Fischer et al.: Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings **DBLP:conf/ches/2017**

Wieland Fischer and Naofumi Homma, eds. *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*. Vol. 10529. Lecture Notes in Computer Science. Springer, 2017. ISBN: 978-3-319-66786-7. DOI: 10.1007/978-3-319-66787-4. URL: https://doi.org/10.1007/978-3-319-66787-4.

Green et al.: AutoLock: Why Cache Attacks on ARM Are Harder Than You Think **GreenEtAl2017**

Marc Green, Leandro Rodrigues-Lima, Andreas Zankl, Gorka Irazoqui, Johann Heyszl, and Thomas Eisenbarth. "AutoLock: Why Cache Attacks on ARM Are Harder Than You Think". In: *26th USENIX Security Symposium (USENIX Security 17)*. Vancouver, BC: USENIX Association, 2017, pp. 1075–1091. ISBN: 978-1-931971-40-9. URL: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/green.

Gulmezoglu et al.: PerfWeb: How to Violate Web Privacy with Hardware Performance Events **GulmezogluEtAl2017**

Berk Gulmezoglu, Andreas Zankl, Thomas Eisenbarth, and Berk Sunar. "PerfWeb: How to Violate Web Privacy with Hardware Performance Events". In: *Computer Security – ESORICS 2017: 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part II*. Ed. by Simon N. Foley, Dieter Gollmann, and Einar Snekkenes. Cham: Springer International Publishing, 2017, pp. 80–97. ISBN: 978-3-319-66399-9. DOI: 10.1007/978-3-319-66399-9_5. URL: https://doi.org/10.1007/978-3-319-66399-9_5.

Hansch et al.: Packet-wise Compression and Forwarding of Industrial Network Captures **hansch2017packet**

Gerhard Hansch, Peter Schneider, and Sven Plaga. "Packet-wise Compression and Forwarding of Industrial Network Captures". In: *9th IEEE International Conference on Intelligent Data Acquisi-*

tion and Advanced Computing Systems: Technology and Applications. (University "Politehnica" of Bucharest, Romania). IDAACS '17. Bucharest, Romania: IEEE, Sept. 2017, pp. 66–70. ISBN: 978-1-5386-0696-4. DOI: 10.1109/IDAACS.2017.8095051.

Abstract: Network traffic captures are necessary for a variety of security applications like identification of malicious patterns or training of intrusion detection systems. While monitoring of enterprise networks is common practice, it is rarely done for industrial production environments due to low bandwidth, confidential production data and sensitive legacy components. To address these challenges, we present methods for non-interfering recording, compression, and transmission of industrial network packet captures. Since a large portion of industrial network traffic consists of status reports that change only slightly, we replace recurring byte strings per connection to reduce the data sent, which also provides a form of concealment. We evaluate our approach by a prototypical implementation on self-generated and publicly available industrial network captures and compare our substitution algorithm to the standard zlib algorithm as well as a combination of both methods.

Hiller et al.: Hiding Secrecy Leakage in Leaky Helper Data **HO17**

Matthias Hiller and Aysun Gurur Önalan. "Hiding Secrecy Leakage in Leaky Helper Data". In: *Conference on Cryptographic Hardware and Embedded Systems*. Ed. by Wieland Fischer and Naofumi Homma. LNCS. Springer Berlin / Heidelberg, 2017, pp. 601–619.

Horsch et al.: TransCrypt: Transparent Main Memory Encryption Using a Minimal ARM Hypervisor **Horsch:2017**

Julian Horsch, Manuel Huber, and Sascha Wessel. "TransCrypt: Transparent Main Memory Encryption Using a Minimal ARM Hypervisor". In: *Proceedings of the 16th International Conference on Trust, Security and Privacy in Computing and Communications*. TrustCom '17. Sydney, Australia: IEEE, Aug. 2017, pp. 152–161. DOI: 10.1109/Trustcom/BigDataSE/ICESS.2017.232.

Huber et al.: Freeze & Crypt: Linux Kernel Support for Main Memory Encryption **secrypt17huber**

Manuel Huber, Julian Horsch, Junaid Ali, and Sascha Wessel. "Freeze & Crypt: Linux Kernel Support for Main Memory Encryption". In: *14th International Conference on Security and Cryptography*. SECRYPT 2017. Madrid, Spain: ScitePress, 2017, pp. 17–30. ISBN: 978-989-758-259-2. DOI: 10.5220/0006378400170030.

Huber et al.: Protecting Suspended Devices from Memory Attacks **Huber:2017:PSD:3065913.3065914**

Manuel Huber, Julian Horsch, and Sascha Wessel. "Protecting Suspended Devices from Memory Attacks". In: *Proceedings of the 10th European Workshop on Systems Security*. EuroSec'17. Belgrade, Serbia: ACM, 2017, 10:1–10:6. ISBN: 978-1-4503-4935-2. DOI: 10.1145/3065913.3065914. URL: http://doi.acm.org/10.1145/3065913.3065914.

Immler et al.: Variable-Length Bit Mapping and Error Correcting Codes for Higher-Order Alphabet PUFs **IHL+17**

Vincent Immler, Matthias Hiller, Qinzhi Liu, Andreas Lenz, and Antonia Wachter-Zeh. "Variable-Length Bit Mapping and Error Correcting Codes for Higher-Order Alphabet PUFs". In: *International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE)*. Ed. by Jean-Luc Danger, Sk Subidh Ali, and Thomas Eisenbarth. LNCS. Springer Berlin / Heidelberg, 2017, pp. 190–209.

Immler et al.: Take a Moment and have some t: Hypothesis testing on Raw PUF Data **IHOS17**

Vincent Immler, Matthias Hiller, Johannes Obermaier, and Georg Sigl. "Take a Moment and have some t: Hypothesis testing on Raw PUF Data". In: *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. 2017, pp. 92–97.

Immler et al.: Your Rails Cannot Hide From Localized EM: How Dual-Rail Logic Fails on FPGAs **conf:/ches/ImmlerEMVSDUALRAIL17**

Vincent Immler, Robert Specht, and Florian Unterstein. "Your Rails Cannot Hide From Localized EM: How Dual-Rail Logic Fails on FPGAs". In: *Conference on Cryptographic Hardware and Embedded Systems, CHES 2017*. 2017.

Immler et al.: Your Rails Cannot Hide from Localized EM: How Dual-Rail Logic Fails on FPGAs **ISU17**

Vincent Immler, Robert Specht, and Florian Unterstein. "Your Rails Cannot Hide from Localized EM: How Dual-Rail Logic Fails on FPGAs". In: *Conference on Cryptographic Hardware and Embedded Systems*. Ed. by Wieland Fischer and Naofumi Homma. LNCS. Springer Berlin / Heidelberg, 2017, pp. 403–424.

Jacob et al.: How to Break Secure Boot on FPGA SoCs Through Malicious Hardware **DBLP:conf/ches/JacobHZRS17**

Nisha Jacob, Johann Heyszl, Andreas Zankl, Carsten Rolfes, and Georg Sigl. "How to Break Secure Boot on FPGA SoCs Through Malicious Hardware". In: *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*. Ed. by Wieland Fischer and Naofumi Homma. Vol. 10529. Lecture Notes in Computer Science. Springer, 2017, pp. 425–442. ISBN: 978-3-319-66786-7. DOI: 10.1007/978-3-319-66787-4_21. URL: https://doi.org/10.1007/978-3-319-66787-4_21.

Jacob et al.: Compromising FPGA SoCs using malicious hardware blocks **DBLP:conf/date/JacobRZHS17**

Nisha Jacob, Carsten Rolfes, Andreas Zankl, Johann Heyszl, and Georg Sigl. "Compromising FPGA SoCs using malicious hardware blocks". In: *Design, Automation & Test in Europe Conference & Exhibition, DATE 2017, Lausanne, Switzerland, March 27-31, 2017*. Ed. by David Atienza and Gior-

gio Di Natale. IEEE, 2017, pp. 1122–1127. ISBN: 978-3-9815370-8-6. DOI: 10.23919/DATE.2017.7927157. URL: https://doi.org/10.23919/DATE.2017.7927157.

Jacob et al.: Securing FPGA SoC Configurations Independent of Their Manufacturers **conf:/ieeesocc/JacobWH17**

Nisha Jacob, Jakob Wittmann, Johann Heyszl, Robert Hesselbarth, Florian Wilde, Michael Pehl, Georg Sigl, and Kai Fisher. "Securing FPGA SoC Configurations Independent of Their Manufacturers". In: *30th IEEE International System-on-Chip Conference*. 2017.

Kirsch et al.: Combating Control Flow Linearization **kirsch2017combating**

Julian Kirsch, Clemens Jonischkeit, Thomas Kittel, Apostolis Zarras, and Claudia Eckert. "Combating Control Flow Linearization". In: *32nd International Conference on ICT Systems Security and Privacy Protection (IFIP SEC)*. May 2017. URL: https://www.sec.in.tum.de/assets/Uploads/CFL.pdf.

Kolosnjaji et al.: Empowering Convolutional Networks for Malware Classification and Analysis **kolosnjaji2017empowering**

Bojan Kolosnjaji, Ghadir Eraisha, George Webster, Apostolis Zarras, and Claudia Eckert. "Empowering Convolutional Networks for Malware Classification and Analysis". In: *30th International Joint Conference on Neural Networks (IJCNN)*. May 2017. URL: https://www.sec.in.tum.de/assets/Uploads/ConvolutionalNetworks.pdf.

Koppermann et al.: Automatic generation of high-performance modular multipliers for arbitrary mersenne primes on FPGAs **koppermann2017automatic**

P. Koppermann, F. De Santis, J. Heyszl, and G. Sigl. "Automatic generation of high-performance modular multipliers for arbitrary mersenne primes on FPGAs". In: *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. 2017, pp. 35–40. DOI: 10.1109/HST.2017.7951794.

Koppermann et al.: Low-latency X25519 hardware implementation: breaking the 100 microseconds barrier **koppermann2017x25519**

Philipp Koppermann, Fabrizio De Santis, Johann Heyszl, and Georg Sigl. "Low-latency X25519 hardware implementation: breaking the 100 microseconds barrier". In: *Microprocessors and Microsystems* (2017). ISSN: 0141-9331. DOI: http://dx.doi.org/10.1016/j.micpro.2017.07.001. URL: http://www.sciencedirect.com/science/article/pii/S0141933117300273.

Kunz et al.: A process model to support continuous certification of cloud services **stephanowProcess2017**

Immanuel Kunz and Philipp Stephanow. "A process model to support continuous certification of cloud services". In: *31th International Conference on Advanced Information Networking and Applications (AINA)*. IEEE, 2017.

Abstract: Current research on cloud service certification is working on techniques to continuously, i.e. automatically and repeatedly, assess whether cloud services satisfy certification criteria. However, traditional certifications are conducted fol- lowing static processes which are not designed to meet the requirements of continuous certification techniques. In this paper, we address this gap by redesigning the traditional certification process and adding suitable tooling to support continuous certification of cloud services. To that end, we analyze and generalize traditional certification processes and, on this basis, develop a novel, executable process model to detect ongoing changes of cloud services and adapt continuous certification techniques accordingly. We present our prototype which implements the process model and show how it allows us to automatically reconfigure continuous certification techniques according to changes observed in the target of certification as well as to continuously report certification results.

Obermaier et al.: Fuzzy-Glitch: A Practical Ring Oscillator Based Clock Glitch Attack
obermaier2017fuzzyglitch

Johannes Obermaier, Robert Specht, and Georg Sigl. "Fuzzy-Glitch: A Practical Ring Oscillator Based Clock Glitch Attack". In: *2017 International Conference on Applied Electronics (AE)*. IEEE, Sept. 2017, pp. 1–6. DOI: 10.23919/AE.2017.8053601.

Abstract: Clock glitches are useful in hardware security applications, where systems are tested for vulnerabilities emerging from fault attacks. Usually a precisely timed and controlled glitch signal is employed. However, this requires complex generators and deep knowledge about the system under attack. Therefore we present a novel approach on clock glitch fault attacks that replaces the single precise glitch by a fuzzy glitch signal. We propose a compact FPGA design for fuzzy clock glitch generation, that is based on mixing two adjustable ring oscillators of different frequencies. The combination of these oscillators creates a glitch containing random and high frequency signal components. We show on the basis of a practical implementation on a Spartan-3E, that the proposed method is able to generate the desired fuzzy clock glitch. We verified experimentally, that the fuzzy clock glitch succeeds in error injection on an STM32F030, an ARM CORTEX-M0 based microcontroller. Our results demonstrate that the fuzzy glitch is an adequate solution for fault injection.

Obermaier et al.: Shedding too much Light on a Microcontroller's Firmware Protection
obermaier2017firmwareprotection

Johannes Obermaier and Stefan Tatschner. "Shedding too much Light on a Microcontroller's Firmware Protection". In: *11th USENIX Workshop on Offensive Technologies (WOOT 17)*. Vancouver, BC: USENIX Association, 2017. URL: https://www.usenix.org/conference/woot17/workshop-program/presentation/obermaier.

Abstract: Almost every microcontroller with integrated flash features firmware readout protection. This is a form of content protection which aims at securing intellectual property (IP) as well as cryptographic keys and algorithms from an adversary. One series of microcontrollers are the STM32 which have recently gained popularity and thus are increasingly under attack. However, no practical experience and information on the resilience of STM32 microcontrollers is publicly available. The paper presents the first investigation of the STM32 security concept, especially targeting the STM32F0 sub-series. Starting with a conceptual analysis, we discover three weaknesses and develop them to vulnerabilities by demonstrating corresponding Proofs-of-Concept. At first, we discover that a common security configuration provides low protection which can be exploited using our Cold-

boot Stepping approach to extract critical data or even readout-protected firmware. Secondly, we reveal a design weakness in the security configuration storage which allows an attacker to downgrade the level of firmware protection, thereby enabling additional attacks. Thirdly, we discover and analyze a hardware flaw in the debug interface, attributed to a race condition, that allows us to directly extract read-protected firmware using an iterative approach. Each attack requires only low-priced equipment, thereby increasing the impact of each weakness and resulting in a severe threat altogether.

Pehl et al.: Secret key generation for physical unclonable functions **PHS17**

Michael Pehl, Matthias Hiller, and Georg Sigl. "Secret key generation for physical unclonable functions". In: *Information Theoretic Security and Privacy of Information Systems*. Ed. by Rafael F. Schaefer, Holger Boche, Ashish Khisti, and H. Vincent Poor. Cambridge University Press, 2017, pp. 362–389.

Philipp Stephanow: Continuous Location Validation of Cloud Service Components **Stephanow2017**

Christian Banse Philipp Stephanow Mohammad Moein. "Continuous Location Validation of Cloud Service Components". In: *Proceedings of the 9th IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. 2017.

Rakotondravony et al.: Classifying malware attacks in IaaS cloud environments **Rakotondravony:2017**

Noëlle Rakotondravony, Benjamin Taubmann, Waseem Mandarawi, Eva Weishäupl, Peng Xu, Bojan Kolosnjaji, Mykolai Protsenko, Hermann de Meer, and Hans P. Reiser. "Classifying malware attacks in IaaS cloud environments". In: *Journal of Cloud Computing* 6.1 (Dec. 2017), p. 26. DOI: 10.1186/s13677-017-0098-8. URL: http:https://doi.org/10.1186/s13677-017-0098-8.

Schanzenbach et al.: Identity and access management in a doping control use case **schanzenbachDuD2017**

Martin Schanzenbach and Sebastian Zickau. "Identity and access management in a doping control use case". In: *Datenschutz und Datensicherheit - DuD* 41.12 (2017), pp. 724–728. ISSN: 1862-2607. DOI: 10.1007/s11623-017-0867-z. URL: https://doi.org/10.1007/s11623-017-0867-z.

Abstract: The PARADISE project is in need of a solution for a very specific set of requirements regarding identity and access management (IAM), in particular for the identity and attribute delegation and the authentication of users and roles within the competitive sport setting. Additionally, athletes have to share whereabouts information with doping control officers. Due to the complex relationship between entities in the doping control use case, innovative authorization solutions regarding location and role information are required. In this article, we present our response to this challenge using decentralized attribute-based access control (ABAC) and access control based on whereabouts using geofences.

Schütte et al.: Practical Application-Level Dynamic Taint Analysis of Android Apps **schuette2017**

Julian Schütte, Alexander Küchler, and Dennis Titze. "Practical Application-Level Dynamic Taint Analysis of Android Apps". In: *Proceedings of the International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. Aug. 2017.

Abstract: Dynamic taint analysis traces data flows in applications at runtime and allows detection and consequently prevention of flow-based vulnerabilities, such as data leaks or injection attacks. While dynamic taint analysis spanning all components of the stack is potentially more precise, it requires adaptations of components across the OS stack and thus does not allow to analyze applications in their real runtime environment. In this paper, we introduce a dynamic taint analysis framework for Android applications which injects a taint analysis directly into an application's bytecode and can thus operate on any stock Android platform. Our approach is more precise than previous ones, copes with flow-aware source and sink definitions, and propagates data flows across process boundaries, including propagation over file I/O and inter process communication. We explain how our framework performs with popular apps from the Google Play Store and show that it achieves a precision which is comparable to the most precise platform-level tainting framework.

Sepulveda et al.: Efficient Security Zones Implementation through Hierarchical Group Key Management at NoC-Based MPSoCs **SFI+17**

Johanna Sepulveda, Daniel Florez, Vincent Immler, Guy Gogniat, and Georg Sigl. "Efficient Security Zones Implementation through Hierarchical Group Key Management at NoC-Based MPSoCs". In: *Microprocessors and Microsystems* 50 (2017), pp. 164–174.

Sepúlveda et al.: Exploiting Bus Communication to Improve Cache Attacks on Systems-on-Chips **SepulvedaEtAl2017a**

Johanna Sepúlveda, Mathieu Gross, Andreas Zankl, and Georg Sigl. "Exploiting Bus Communication to Improve Cache Attacks on Systems-on-Chips". In: *2017 IEEE Computer Society Annual Symposium on VLSI, ISVLSI 2017, Bochum, Germany, July 3-5, 2017*. 2017, pp. 284–289. ISBN: 978-1-5090-6762-6. DOI: 10.1109/ISVLSI.2017.57. URL: https://doi.org/10.1109/ISVLSI.2017.57.

Sepúlveda et al.: Towards trace-driven cache attacks on Systems-on-Chips - exploiting bus communication **SepulvedaEtAl2017d**

Johanna Sepúlveda, Mathieu Gross, Andreas Zankl, and Georg Sigl. "Towards trace-driven cache attacks on Systems-on-Chips - exploiting bus communication". In: *12th International Symposium on Reconfigurable Communication-centric Systems-on-Chip, ReCoSoC 2017, Madrid, Spain, July 12-14, 2017*. IEEE, 2017, pp. 1–7. ISBN: 978-1-5386-3344-1. DOI: 10.1109/ReCoSoC.2017.8016150. URL: https://doi.org/10.1109/ReCoSoC.2017.8016150.

Sepúlveda et al.: Towards Protected MPSoC Communication for Information Protection against a Malicious NoC **SepulvedaEtAl2017e**

Johanna Sepúlveda, Andreas Zankl, Daniel Flórez, and Georg Sigl. "Towards Protected MPSoC Communication for Information Protection against a Malicious NoC". In: *International Conference on Computational Science, ICCS 2017, 12-14 June 2017, Zurich, Switzerland*. Ed. by Petros Koumoutsakos, Michael Lees, Valeria V. Krzhizhanovskaya, Jack J. Dongarra, and Peter M. A. Sloot. Vol. 108. Procedia Computer Science. Elsevier, 2017, pp. 1103–1112. DOI: 10.1016/j.procs.2017.05.139. URL: https://doi.org/10.1016/j.procs.2017.05.139.

Sepúlveda et al.: Towards Protected MPSoC Communication for Information Protection against a Malicious NoC **SepulvedaEtAl2017b**

Johanna Sepúlveda, Andreas Zankl, Daniel Flórez, and Georg Sigl. "Towards Protected MPSoC Communication for Information Protection against a Malicious NoC". In: *International Conference on Computational Science, ICCS 2017, 12-14 June 2017, Zurich, Switzerland*. Vol. 108. Procedia Computer Science. Elsevier, 2017, pp. 1103 –1112. DOI: 10.1016/j.procs.2017.05.139. URL: https://doi.org/10.1016/j.procs.2017.05.139.

Sepúlveda et al.: Cache Attacks and Countermeasures for NTRUEncrypt on MPSoCs: Post-quantum Resistance for the IoT **SepulvedaEtAl2017c**

Johanna Sepúlveda, Andreas Zankl, and Oliver Mischke. "Cache Attacks and Countermeasures for NTRUEncrypt on MPSoCs: Post-quantum Resistance for the IoT". In: *30th IEEE International System-on-Chip Conference, SOCC 2017, Munich, Germany, September 5-8, 2017*. IEEE, 2017, pp. 120–125. ISBN: 978-1-5386-4034-0. DOI: 10.1109/SOCC.2017.8226020. URL: https://doi.org/10.1109/SOCC.2017.8226020.

Stephanow et al.: Evaluating the performance of continuous test-based cloud service certification **stephanowEvaluation2017**

Philipp Stephanow and Christian Banse. "Evaluating the performance of continuous test-based cloud service certification". In: *17th International Symposium on Cluster, Cloud and Grid Computing (CCGrid)*. IEEE. 2017.

Abstract: Continuous test-based cloud certification uses tests to automatically and repeatedly evaluate whether a cloud service satisfies customer requirements over time. However, inaccurate tests can decrease customers' trust in test results and can lead to providers disputing results of test-based certification techniques. In this paper, we propose an approach how to evaluate the performance of test-based cloud certification techniques. Our method allows to infer conclusions about the general performance of test-based techniques, compare alternative techniques, and compare alternative configurations of test-based techniques. We present experimental results on how we used our approach to evaluate and compare exem- plary test-based techniques which support the certification of requirements related to security, reliability and availability.

Stephanow et al.: Towards continuous security certification of Software-as-a-Service applications using web application testing **stephanowSaaS2017**

Philipp Stephanow and Koosha Khajehmoogahi. "Towards continuous security certification of Software-as-a-Service applications using web application testing". In: *31th International Conference on Advanced Information Networking and Applications (AINA)*. IEEE, 2017.

Abstract: Continuous security certification of software-as- a-service (SaaS) aims at continuously, i.e. repeatedly and automatically validating whether a SaaS application adheres to a set of security requirements. Since SaaS applications make heavy use of web application technologies, checking security requirements with the help of web application testing techniques seems evident. However, these techniques mainly focus on conducting discrete security tests, that is, mostly manually triggered tests whose results are interpreted by human experts. Thus these techniques are not per se suited to support continuous security certification of SaaS applications and have to be adapted accordingly. In this paper, we report on our current status of developing methods and tools to support test- based, continuous security certification of SaaS applications which make use of web application testing techniques. To that end, we describe major challenges to overcome and present experimental test results of using SQLMap to continuously test for SQL injection vulnerabilities.

Titze et al.: Ordol: Obfuscation-Resilient Detection of Libraries in Android Applications **titze2017**

Dennis Titze, Michael Lux, and Julian Schütte. "Ordol: Obfuscation-Resilient Detection of Libraries in Android Applications". In: *Proceedings of the International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. Aug. 2017.

Abstract: Android apps often include libraries supporting certain features, or allowing rapid app development. Due to Android's system design, libraries are not easily distinguishable from the app's core code. But detecting libraries in apps is needed especially in app analysis, e.g., to determine if functionality is executed in the app, or in the code of the library. Previous approaches detected libraries in ways which are susceptible to code obfuscation. For some approaches, even simple obfuscation will cause unrecognised libraries. Our approach – Ordol – builds upon approaches from plagiarism detection to detect a specific library version inside an app in an obfuscation-resilient manner. We show that Ordol can cope well with obfuscated code and can be easily applied to real life apps.

Unterstein et al.: Dissecting Leakage Resilient PRFs with Multivariate Localized EM Attacks - A Practical Security Evaluation on FPGA **Unterstein2017Dissecting**

Florian Unterstein, Johann Heyszl, Fabrizio De Santis, and Robert Specht. "Dissecting Leakage Resilient PRFs with Multivariate Localized EM Attacks - A Practical Security Evaluation on FPGA". In: *Proceedings of 8th International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2017)*. Springer. 2017.

Webster et al.: Finding the Needle: A Study of the PE32 Rich Header and Respective Malware Triage **webster2017Rich**

George Webster, Bojan Kolosnjaji, Christian von Pentz, Julian Kirsch, Zachary Hanif, Apostolis Zarras, and Claudia Eckert. "Finding the Needle: A Study of the PE32 Rich Header and Respective Mal-

ware Triage". In: *14th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*. July 2017. URL: https://www.sec.in.tum.de/assets/Uploads/RichHeader.pdf.

Zankl et al.: Automated Detection of Instruction Cache Leaks in Modular Exponentiation Software **ZanklEtAl2017**

Andreas Zankl, Johann Heyszl, and Georg Sigl. "Automated Detection of Instruction Cache Leaks in Modular Exponentiation Software". In: *Smart Card Research and Advanced Applications: 15th International Conference, CARDIS 2016, Cannes, France, November 7–9, 2016, Revised Selected Papers*. Ed. by Kerstin Lemke-Rust and Michael Tunstall. Cham: Springer International Publishing, 2017, pp. 228–244. ISBN: 978-3-319-54669-8. DOI: 10.1007/978-3-319-54669-8_14. URL: http://dx.doi.org/10.1007/978-3-319-54669-8_14.

Angermeier et al.: Risk-driven Security Engineering in the Automotive Domain **angermeier2016engineering**

Daniel Angermeier and Jörn Eichler. "Risk-driven Security Engineering in the Automotive Domain". In: 2016.

Abstract: Modern vehicles are complex systems of interlinked electronic control units with many connections to exterior devices. Consequently, security engineering for modern vehicles is a challenging task. Knowledge from several domains of expertise, especially the security domain and the automotive engineering domain, must be combined to identify and fulfill all functional and security-related requirements. We propose a risk-driven approach for security engineering, allowing well-organized cooperation between stakeholders in the security engineering process with a common method framework and distinct artifacts serving as well-defined interfaces between activities and stakeholders. At the same time, our method supports the application of established methods for individual steps, allowing for the necessary flexibility in typically very heterogeneous automotive development environments. Furthermore, our method defines supportive artifacts which help streamline the application of our method, such as catalogs and unified assessment models. Finally, we report on early experiences on the application of our method by an international OEM.

Angermeier et al.: Supporting Risk Assessment with the Systematic Identification, Merging and Validation of Security Goals **angermeier2016systematic**

Daniel Angermeier, Alexander Nieding, and Jörn Eichler. "Supporting Risk Assessment with the Systematic Identification, Merging and Validation of Security Goals". In: *Risk Assessment and Risk-Driven Testing: 4. International Workshop, RISK 2016, Revised Selected Papers*. 2016.

Abstract: Assessing security-related risks in software or systems engineering is a challenging task: often, a heterogeneous set of distributed stakeholders creates a complex system of (software) components which are highly connected to each other, consumer electronics, or Internet-based services. Changes during development are frequent and must be evaluated and handled efficiently. Consequently, risk assessment itself becomes a complex task and its results must be comprehensible by all actors in the distributed environment. Especially, systematic and repeatable identification of security goals based on a model of the system under development (SUD) is not well-supported in established methods. Thus, we demonstrate how the systematic identification, merging, and vali-

dation of security goals based on a model of the SUD in a concrete implementation of our method Modular Risk Assessment (MoRA) supports security engineers to handle this challenge.

Bilzhause et al.: Cryptographically Enforced Four-Eyes Principle **Bilzhause_et_al_SECPID16**

Arne Bilzhause, Manuel Huber, Henrich C Pöhls, and Kai Samelin. "Cryptographically Enforced Four-Eyes Principle". In: *11th International Conference on Availability, Reliability and Security (ARES)*. IEEE, 2016, pp. 760–767. DOI: 10.1109/ARES.2016.28.

Böttinger: Fuzzing Binaries with Lévy Flight Swarms **beefuzz_swarm**

Konstantin Böttinger. "Fuzzing Binaries with Lévy Flight Swarms". In: *EURASIP Journal on Information Security* (2016). DOI: doi:10.1186/s13635-016-0052-1.

Böttinger: Hunting Bugs with Lévy Flight Foraging **beefuzz**

Konstantin Böttinger. "Hunting Bugs with Lévy Flight Foraging". In: *37th IEEE Symposium on Security and Privacy (S&P 2016) Workshops*. 2016.

Böttinger et al.: DeepFuzz: Triggering Vulnerabilities Deeply Hidden in Binaries **deepfuzz**

Konstantin Böttinger and Claudia Eckert. "DeepFuzz: Triggering Vulnerabilities Deeply Hidden in Binaries". In: *13th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2016)*. 2016.

Böttinger et al.: Detecting and Correlating Supranational Threats for Critical Infrastructures **eu_ec_2016_1**

Konstantin Böttinger, Gerhard Hansch, and Bartol Filipovic. "Detecting and Correlating Supranational Threats for Critical Infrastructures". In: *15th European Conference on Cyber Warfare and Security*. ECCWS '16. Munich, Germany: Academic Conferences and Publishing International (ACPI) Limited, July 2016, pp. 34–41. ISBN: 978-1-9108-1093-4.

Abstract: As critical infrastructures have become strategic targets for advanced cyber-attacks, we face the severe challenge to provide new defense technologies for their protection. We propose a distributed supranational architecture for detection, classification, and mitigation of highly sophisticated cyber incidents targeted simultaneously at multiple critical infrastructures. We build upon a three layered architecture comprised of Security Operations Centres at organizational (O-SOC), national (N-SOC), and European (E-SOC) level using IDS and SIEM solutions. In our approach we combine machine learning and automatic ontological reasoning: First, we apply methods from the field of machine learning to analyse threat indicators of different granularity. This provides classification of very specific observables collected at compromised sites. Second, we perform ontological analysis to identify large scale correlations within an incident knowledge graph.

Böttinger et al.: Leitfaden Industrie 4.0 Security - Handlungsempfehlungen für den Mittelstand **vdma_leitfaden_i40**

Konstantin Böttinger, Martin Hutle, Bartol Filipovic, and Sebastian Rohr. *Leitfaden Industrie 4.0 Security - Handlungsempfehlungen für den Mittelstand*. VDMA Verlag, 2016.

Gall et al.: K-word Proximity Search on Encrypted Data **gall2016**

Mark Gall and Gerd" Brost. "K-word Proximity Search on Encrypted Data". In: *Proceedings of the International Conference on Advanced Information Network and Applications (AINA)*. Mar. 2016.

Hesselbarth et al.: Fast and Reliable PUF Response Evaluation from Unsettled Bistable Rings **hesselbarth2016brresponseevaluation**

Robert Hesselbarth and Georg Sigl. "Fast and Reliable PUF Response Evaluation from Unsettled Bistable Rings". en. In: *Euromicro Conference on Digital System Design (DSD 2016)*. Limassol, Cyprus, 2016. URL: http://dsd-seaa2016.cs.ucy.ac.cy/index.php?p=DSD2016;.

Abstract: Bistable ring (BR) based strong PUFs are promising candidates for lightweight authentication applications. It has been observed that a good '0'/'1'-balance of their responses correlates with longer settling times. This is problematic, since the state-of-the-art evaluation method requires the BR to be settled in order to generate a reliable PUF response. We show that settling times can easily extend beyond 100 milli seconds for 70 percent of the responses in the TBR PUF, which is a BR-based PUF with good '0'/'1'-balance characteristics. Hence, it is practically impossible to wait for all BRs to settle, which results in a reliability penalty. In order to solve this problem, we present three new methods, which allow the evaluation of unsettled BRs with increased reliability compared to the state-of-the-art method. We were able to achieve evaluation times down to 1 micro second and improve response reliability from 80 percent to up to 98.5 percent. This enables the fast and reliable use of BR-based PUFs in strong PUFs applications.

Hiller et al.: Online Reliability Testing for PUF Key Derivation **HOSB16**

Matthias Hiller, Aysun Gurur Önalan, Georg Sigl, and Martin Bossert. "Online Reliability Testing for PUF Key Derivation". In: *International Workshop on Trustworthy Embedded Devices (TrustED)*. ACM, 2016, pp. 15–22.

Hiller et al.: Algebraic Security Analysis of Key Generation with Physical Unclonable Functions **hiller_sigl2016a**

Matthias Hiller, Michael Pehl, Gerhard Kramer, and Georg Sigl. "Algebraic Security Analysis of Key Generation with Physical Unclonable Functions". In: *Security Proofs for Embedded Systems Workshop (PROOFS)*. 2016.

Horsch et al.: CoKey: Fast Token-based Cooperative Cryptography **Horsch2016**

Julian Horsch, Sascha Wessel, and Claudia Eckert. "CoKey: Fast Token-based Cooperative Cryptography". In: *Proceedings of the 32Nd Annual Conference on Computer Security Applications*. ACSAC '16. Los Angeles, California: ACM, 2016, pp. 314–323. ISBN: 978-1-4503-4771-6. DOI:

10.1145/2991079.2991117. URL: http://doi.acm.org/10.1145/2991079.2991117.

Abstract: Keys for symmetric cryptography are usually stored in RAM and therefore susceptible to various attacks, ranging from simple buffer overflows to leaks via cold boot, DMA or side channels. A common approach to mitigate such attacks is to move the keys to an external cryptographic token. For low-throughput applications like asymmetric signature generation, the performance of these tokens is sufficient. For symmetric, data-intensive use cases, like disk encryption on behalf of the host, the connecting interface to the token often is a serious bottleneck. In order to overcome this problem, we present CoKey, a novel concept for partially moving symmetric cryptography out of the host into a trusted detachable token. CoKey combines keys from both entities and securely encrypts initialization vectors on the token which are then used in the cryptographic operations on the host. This forces host and token to cooperate during the whole encryption and decryption process. Our concept strongly and efficiently binds encrypted data on the host to the specific token used for their encryption, while still allowing for fast operation. We implemented the concept using Linux hosts and the USB armory, a USB thumb drive sized ARM computer, as detachable crypto token. Our detailed performance evaluation shows that our prototype is easily fast enough even for data-intensive and performance-critical use cases like full disk encryption, thus effectively improving security for symmetric cryptography in a usable way.

Huber et al.: A Secure Architecture for Operating System-Level Virtualization on Mobile Devices **Huber:2015**

Manuel Huber, Julian Horsch, Michael Velten, Michael Weiss, and Sascha Wessel. "A Secure Architecture for Operating System-Level Virtualization on Mobile Devices". In: *Revised Selected Papers of the 11th International Conference on Information Security and Cryptology - Volume 9589*. Inscrypt 2015. Beijing, China: Springer-Verlag New York, Inc., 2016, pp. 430–450. ISBN: 978-3-319-38897-7. DOI: 10.1007/978-3-319-38898-4_25. URL: http://dx.doi.org/10.1007/978-3-319-38898-4_25.

Huber et al.: A Flexible Framework for Mobile Device Forensics Based on Cold Boot Attacks **Huber2016**

Manuel Huber, Benjamin Taubmann, Sascha Wessel, Hans P. Reiser, and Georg Sigl. "A Flexible Framework for Mobile Device Forensics Based on Cold Boot Attacks". In: *EURASIP Journal on Information Security*. Vol. 2016. 1. New York, NY, United States: Hindawi Publishing Corp., Dec. 2016, 41:1–41:13. DOI: 10.1186/s13635-016-0041-4. URL: https://doi.org/10.1186/s13635-016-0041-4.

Immler et al.: Practical Aspects of Quantization and Tamper-Sensitivity for Physically Obfuscated Keys **pepkeygen2016**

Vincent Immler, Maxim Hennig, Ludwig Kürzinger, and Georg Sigl. "Practical Aspects of Quantization and Tamper-Sensitivity for Physically Obfuscated Keys". In: *Cryptography and Security in Computing Systems*. 2016. ISBN: 978-1-4503-4065-6.

Kilic et al.: Interactive Function Identification Decreasing the Effort of Reverse Engineering
Kilic2016

Fatih Kilic, Hannes Laner, and Claudia Eckert. "Interactive Function Identification Decreasing the Effort of Reverse Engineering". In: *Proceedings of the 11th International Conference on Information Security and Cryptology (Inscrypt 2015)*. Springer International Publishing, 2016, pp. 468–487. ISBN: 978-3-319-38898-4. DOI: 10.1007/978-3-319-38898-4_27. URL: http://dx.doi.org/10.1007/978-3-319-38898-4_27.

Kolosnjaji et al.: Adaptive Semantics-Aware Malware Classification
kolosnjaji2016adaptive

Bojan Kolosnjaji, Apostolis Zarras, Tamas Lengyel, George Webster, and Claudia Eckert. "Adaptive Semantics-Aware Malware Classification". In: *13th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*. July 2016. URL: https://www.sec.in.tum.de/assets/Uploads/SemanticTopicModeling.pdf.

Kolosnjaji et al.: Deep Learning for Classification of Malware System Call Sequences
kolosnjaji2016deep

Bojan Kolosnjaji, Apostolis Zarras, George Webster, and Claudia Eckert. "Deep Learning for Classification of Malware System Call Sequences". In: *29th Australasian Joint Conference on Artificial Intelligence (AI)*. Dec. 2016. URL: https://www.sec.in.tum.de/assets/Uploads/deeplearning.pdf.

Koppermann et al.: X25519 Hardware Implementation for Low-Latency Applications
koppermann2016x25519

Philipp Koppermann, Fabrizio De Santis, Johann Heyszl, and Georg Sigl. "X25519 Hardware Implementation for Low-Latency Applications". en. In: *Euromicro Conference on Digital System Design (DSD 2016)*. Limassol, Cyprus, 2016. URL: http://dsd-seaa2016.cs.ucy.ac.cy/index.php?p=DSD2016.

Langer et al.: Analysing cyber-physical attacks to a Smart Grid: A voltage control use case
LangerSHF16

Lucie Langer, Paul Smith, Martin Hutle, and Alberto E. Schaeffer Filho. "Analysing cyber-physical attacks to a Smart Grid: A voltage control use case". In: *Power Systems Computation Conference, PSCC 2016, Genoa, Italy, June 20-24, 2016*. 2016, pp. 1–7. DOI: 10.1109/PSCC.2016.7540819. URL: http://dx.doi.org/10.1109/PSCC.2016.7540819.

Margraf et al.: Vernetzte IT-Sicherheit in Kritischen Infrastrukturen
margraf2016vernetzte

Marian Margraf, Steven Müller, Sophia Harth, and Jörn Eichler. "Vernetzte IT-Sicherheit in Kritischen Infrastrukturen". In: *DIN Mitteilungen* 6 (2016), pp. 24–28.

Muntean et al.: vTableShield: Precise Protecting of Virtual Function Dispatches in C++ Programs **448**

Paul Muntean, Peng Xu, and Claudia Eckert. "vTableShield: Precise Protecting of Virtual Function Dispatches in C++ Programs". In: *Google Ph.D. Student Summit on Compiler & Programming Technology, Munich, Germany*. Dec. 2016. URL: https://www.sec.in.tum.de/assets/staff/muntean/poster_muntean_vtable_shield.pdf.

Nyberg et al.: Enhancing Fault Emulation of Transient Faults by Separating Combinational and Sequential Fault Propagation. **conf/glvlsi/NybergHHS16**

Ralph Nyberg, Johann Heyszl, Dietmar Heinz, and Georg Sigl. "Enhancing Fault Emulation of Transient Faults by Separating Combinational and Sequential Fault Propagation." In: *ACM Great Lakes Symposium on VLSI*. Ed. by Ayse Kivilcim Coskun, Martin Margala, Laleh Behjat, and Jie Han. ACM, 2016, pp. 209–214. ISBN: 978-1-4503-4274-2. URL: http://dblp.uni-trier.de/db/conf/glvlsi/glvlsi2016.html#NybergHHS16.

Obermaier et al.: Analyzing the Security and Privacy of Cloud-based Video Surveillance Systems **obermaier2016analyzing**

Johannes Obermaier and Martin Hutle. "Analyzing the Security and Privacy of Cloud-based Video Surveillance Systems". In: *Proceedings of the 2nd ACM Workshop on IoT Privacy, Trust, and Security*. IoTPTS '16. ACM, 2016. ISBN: 978-1-4503-4283-4. DOI: 10.1145/2899007.2899008. URL: http://dx.doi.org/10.1145/2899007.2899008.

Abstract: In the area of the Internet of Things, cloud-based camera surveillance systems are ubiquitously available for industrial and private environments. However, the sensitive nature of the surveillance use case imposes high requirements on privacy/confidentiality, authenticity, and availability of such systems. In this work, we investigate how currently available mass-market camera systems comply with these requirements. Considering two attacker models, we test the cameras for weaknesses and analyze for their implications. We reverse-engineered the security implementation and discovered several vulnerabilities in every tested system. These weaknesses impair the users' privacy and, as a consequence, may also damage the camera system manufacturer's reputation. We demonstrate how an attacker can exploit these vulnerabilities to blackmail users and companies by denial-of-service attacks, injecting forged video streams, and by eavesdropping private video data — even without physical access to the device. Our analysis shows that current systems lack in practice the necessary care when implementing security for IoT devices.

Plaga et al.: Logboat – A Simulation Framework Enabling CAN Security Assessments **LogboatCAN**

Sven Plaga, Stefan Tatschner, and Thomas Newe. "Logboat – A Simulation Framework Enabling CAN Security Assessments". In: *21st International Conference on Applied Electronics*. Pilsen, Czech Republic: IEEE, 2016. ISBN: 978-80-261-0602-9. DOI: 10.1109/AE.2016.7577276.

Abstract: Traditionally, fieldbus networks are operated in closed environments, where all communication nodes are assumed to be trustworthy. Therefore, the corresponding standards do not consider any security requirements. New technology trends, such as the upcoming Internet of Things (IoT), demand an interconnection between all components of an industrial infrastructure. As a con-

sequence of this, there is a need for tools enabling security assessments and the simulation of protocol-based security improvements. In this paper we introduce Logboat, a flexible Python and Linux based simulation framework for security assessments on Controller Area Network (CAN) networks and make some architectural and technology-selection proposals. Subsequently, the different modules of Logboat and their capabilities are explained and a use case scenario is presented. The paper concludes with an outlook on upcoming research activities on CAN bus security where the presented framework can be of help.

Schanzenbach et al.: Managing and Presenting User Attributes over a Decentralized Secure Name System **schanzenbach2016**

Martin Schanzenbach and Christian Banse. "Managing and Presenting User Attributes over a Decentralized Secure Name System". In: *Data Privacy Management and Security Assurance*. Ed. by Giovanni Livraga, Vicenç Torra, Alessandro Aldini, Fabio Martinelli, and Neeraj Suri. Cham: Springer International Publishing, 2016, pp. 213–220. ISBN: 978-3-319-47072-6.

Abstract: Today, user attributes are managed at centralized identity providers. However, two centralized identity providers dominate digital identity and access management on the web. This is increasingly becoming a privacy problem in times of mass surveillance and data mining for targeted advertisement. Existing systems for attribute sharing or credential presentation either rely on a trusted third party service or require the presentation to be online and synchronous. In this paper we propose a concept that allows the user to manage and share his attributes asynchronously with a requesting party using a secure, decentralized name system.

Schütte et al.: A Data Usage Control System using Dynamic Taint Tracking **schuette2016**

Julian Schütte and Gerd" Brost. "A Data Usage Control System using Dynamic Taint Tracking". In: *Proceedings of the International Conference on Advanced Information Network and Applications (AINA)*. Mar. 2016.

Schütte et al.: Sichere Business-Apps unter Android **schuette2016sichere**

Julian Schütte, Jörn Eichler, and Dennis Titze. "Sichere Business-Apps unter Android". In: *Mobile Anwendungen in Unternehmen - Konzepte und betriebliche Einsatzszenarien*. Ed. by Thomas Barton, Christian Müller, and Christian Seel. Springer Vieweg, 2016, pp. 139–156.

Selmke et al.: Attack on a DFA protected AES by simultaneous laser fault injections **Selmke2016**

Bodo Selmke, Johann Heyszl, and Georg Sigl. "Attack on a DFA protected AES by simultaneous laser fault injections". en. In: *Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2016)*. to appear. Santa Barbara, CA, USA, 2016. URL: `http://conferenze.dei.polimi.it/FDTC16/`.

Abstract: This paper demonstrates a Fault Attack on an AES core protected by an infection type countermeasure. The redundant AES is implemented on a Xilinx Spartan-6 FPGA, with a feature size of 45 nm. By injecting exactly the same fault in both state registers of the redundant implementation using lasers, we are able to annul the protection added by the countermeasure and thus perform a successful Differential Fault Analysis. This requires a high precision double laser setup in

order to hit two different locations on the chip at the same point in time. With a priori knowledge about the location of both state registers, we were able to generate applicable faulty ciphertexts within minutes. Our results show that for applications demanding a high level of security, relying on a duplication of hardware is not sufficient.

Sepulveda et al.: Hierarchical Group-key Management for NoC-Based MPSoCs Protection **SFI+16**

Johanna Sepulveda, Daniel Flórez, Vincent Immler, Guy Gogniat, and Georg Sigl. "Hierarchical Group-key Management for NoC-Based MPSoCs Protection". In: *Journal of Integrated Circuits and Systems* 11.1 (2016), pp. 38–48.

Settanni et al.: A Collaborative Cyber Incident Management System for European Interconnected Critical Infrastructures **eu_ec_2016_2**

Giuseppe Settanni, Florian Skopik, Yegor Shovgenya, Roman Fiedler, Mark Carolan, Damien Conroy, Konstantin Böttinger, Mark Gall, Gerd Brost, Christophe Ponchel, Mirko Haustein, Helmut Kaufmann, Klaus Theuerkauf, and Pia Olli. "A Collaborative Cyber Incident Management System for European Interconnected Critical Infrastructures". In: *Journal of Information Security and Applications* Special Issue on ICS & SCADA Cyber Security (2016). accepted.

Seuschek et al.: A Cautionary Note: Side-Channel Leakage Implications of Deterministic Signature Schemes **seuschek2016cautionary**

Hermann Seuschek, Johann Heyszl, and Fabrizio De Santis. "A Cautionary Note: Side-Channel Leakage Implications of Deterministic Signature Schemes". In: *Proceedings of the Third Workshop on Cryptography and Security in Computing Systems*. ACM. 2016, pp. 7–12.

Stephanow et al.: Generating Threat Profiles for Cloud Service Certification Systems **stephanow2016generating**

Philipp Stephanow, Christian Banse, and Julian Schütte. "Generating Threat Profiles for Cloud Service Certification Systems". In: *17th IEEE High Assurance Systems Engineering Symposium (HASE)*. 2016.

Abstract: Cloud service certification aims at automatically validating whether a cloud service satisfies a predefined set of requirements. To that end, certification systems collect and evaluate sensitive data from various sources of a cloud service. At the same time, the certification system itself has to be resilient to attacks to generate trustworthy statements about the cloud service. Thus system architects are faced with the task of assessing the trustworthiness of different certification system designs. To cope with that challenge, we propose a method to model different architecture variants of cloud service certification systems and analyze threats these systems face. By applying our method to a specific cloud service certification system, we show how threats to such systems can be derived in a standardized way that allows us to evaluate different architecture configurations.

Stephanow et al.: Test-based cloud service certification of opportunistic providers
Stephanow2016test

Philipp Stephanow, Gaurav Srivastava, and Julian Schütte. "Test-based cloud service certification of opportunistic providers". In: *The 8th IEEE International Conference on Cloud Computing (CLOUD)*. July 2016.

Abstract: Through automatically checking whether cloud services satisfy customers' requirements, cloud service certifi- cation promises cloud providers competitive advantages, e.g. by attracting new customers. However, certification can increase costs of cloud providers, creating incentives for fraudulent providers to save costs by only pretending to satisfy cus- tomers' requirements. Opportunistic providers are fraudulent providers who will only cheat if they are not caught. In this paper, we propose an approach to support cloud service certi- fication of opportunistic providers. To that end, we introduce a method to model the behavior of opportunistic providers and propose a framework supporting test-based certification which builds on randomized testing and is non-invasive. We show how our framework reduces the willingness of opportunistic providers to cheat, and present experimental results of tests supporting the certification of requirements related to resource availability, resource provisioning, and quality of service.

Strobel et al.: Novel Weaknesses in IEC 62351 Protected Smart Grid Control Systems
WeaknessesIEC62351

Maximilian Strobel, Norbert Wiedermann, and Claudia Eckert. "Novel Weaknesses in IEC 62351 Protected Smart Grid Control Systems". In: *IEEE International Conference on Smart Grid Communications*. Sydney, Australia: IEEE, Nov. 2016.

Abstract: Smart Grids are characterized by a high level of interconnectedness and interdependency between their sub-components. As this increases the surface for potential cyber attacks, the control system communication needs to be protected. IEC 61850 is about to become the most prevalent communication standard in the process related parts of Smart Grid control systems, but it was not designed with security in mind. IEC 62351 extends IEC 61850 by comprehensive security measures. By analyzing the IEC 61850 and IEC 62351 specifications, three novel weaknesses in the IEC 62351 standard were discovered which will be presented in this paper. Two weaknesses allow for replay of GOOSE and Sampled Values messages and one weakness in the protocol used for time exchange (SNTP) leaves the system vulnerable to a variety of attacks.

Teichmann et al.: Agile Threat Assessment and Mitigation: An Approach for Method Selection and Tailoring
teichmann2016atam

Clemens Teichmann, Stephan Renatus, and Jörn Eichler. "Agile Threat Assessment and Mitigation: An Approach for Method Selection and Tailoring". In: *International Journal of Secure Software Engineering (IJSSE)*. Ed. by Khaled M. Khan. Vol. 7. IGI-Global, 2016.

Abstract: Security engineering and agile development are often perceived as a clash of cultures. To address this clash, several approaches have been proposed that allow for agile security engineering. Unfortunately, agile development organizations differ in their actual procedures and environmental properties resulting in varying requirements. We propose an approach to compare and select methods for agile security engineering. Furthermore, our approach addresses adaptation or construction of a tailored method taking the existing development culture into account. We demonstrate the fea-

sibility of our proposal and report early experiences from its application within a small development organization for digital solutions in the automotive domain.

Teichmann et al.: Modellgestützte Risikoanalyse der Sicherheit Kritischer Infrastrukturen für kleine und mittlere Unternehmen: Eine Übersicht **teichmann2016sotamodel**

Clemens Teichmann, Stephan Renatus, and Alexander Nieding. "Modellgestützte Risikoanalyse der Sicherheit Kritischer Infrastrukturen für kleine und mittlere Unternehmen: Eine Übersicht". In: *Multikonferenz Wirtschaftsinformatik (MKWI) 2016*. Ed. by Volker Nissen, Dirk Stelzer, Steffen Straßburger, and Daniel Fischer. Universitätsverlag Ilmenau, 2016.

Abstract: Der Einzug neuer Informations- und Kommunikationstechnologien in den Bereich der Kritischen Infrastrukturen (KI) ermöglicht eine Vielzahl neuer Angriffswege und stellt vor allem kleine und mittlere Unternehmen (KMU) vor Herausforderungen, die sie ohne speziell aus-gebildetes IT-Sicherheits-Personal sowie umfangreiche finanzielle Ressourcen nicht bewälti-gen können. Um KMU eine effiziente Durchführung von Risikoanalysen und Sicherheits-bewertungen zu ermöglichen, stellen modellgetriebene und modellbasierte Ansätze einen vielversprechenden Lösungsansatz dar. Wir untersuchen den aktuellen Publikationsstand zu modellgetriebenen Methoden und Werkzeugen der sicherheitsbezogenen Risikoanalyse Kritischer Infrastrukturen. Dabei ana-lysieren wir den Stand der Forschung anhand von Kriterien, die für den Einsatz durch KMU relevant sind. Unsere Untersuchung zeigt, dass modellbasierte Ansätze etabliert sind, aber es aktuelle Methoden und Werkzeuge kleinen und mittleren Betreibern Kritischer Infrastruktu-ren nur begrenzt ermöglichen, eine aussagekräftige Risikoanalyse und Sicherheitsbewertung durchzuführen.

Wagner et al.: Policy-Based Implicit Attestation for Microkernel-Based Virtualized Systems **Wagner2016**

Steffen Wagner and Claudia Eckert. "Policy-Based Implicit Attestation for Microkernel-Based Virtualized Systems". In: *Information Security: 19th International Conference, ISC 2016, Honolulu, HI, USA, September 3-6, 2016. Proceedings*. Ed. by Matt Bishop and A. Anderson C. Nascimento. Cham: Springer International Publishing, 2016, pp. 305–322. ISBN: 978-3-319-45871-7. DOI: 10.1007/978-3-319-45871-7_19. URL: http://dx.doi.org/10.1007/978-3-319-45871-7_19.

Abstract: We present an attestation mechanism that enables a remote verifier to implicitly evaluate the trustworthiness of the prover's system through policies. Those policies are verified and enforced by a TPM 2.0, when the attestor interacts with a virtualized hardware component of the prover's system. For instance, when the verifier reads a virtualized sensor device and requests integrity-protected sensor data, such as the average temperature, a heartbeat value, or an anomaly detection score, the prover's TPM, which acts as a trust anchor, checks and enforces the policies specified by the verifier. The prover, in turn, is also able to define policies, which can limit access to certain hardware components and are also enforced by the TPM. As a result, both parties have to cooperate for a successful attestation, which implicitly creates verifiable proof of the prover's trustworthiness using mainly symmetric instead of expensive asymmetric cryptographic operations like digital signatures.

Webster et al.: SKALD: A Scalable Architecture for Feature Extraction, Multi-User Analysis, and Real-Time Information Sharing **webster2016skald**

George Webster, Zachary Hanif, Andre Ludwig, Tamas Lengyel, Apostolis Zarras, and Claudia Eckert. "SKALD: A Scalable Architecture for Feature Extraction, Multi-User Analysis, and Real-Time Information Sharing". In: *19th International Conference on Information Security (ISC)*. Sept. 2016. URL: https://www.sec.in.tum.de/assets/Uploads/skald.pdf.

Wiedermann et al.: Poster: Smart Grid Cyber-Security Simulation Environment **wiederma2016SparksCoSimPoster**

Norbert Wiedermann and Mislav Findrik. *Poster: Smart Grid Cyber-Security Simulation Environment*. Poster at 5th D-A-CH+ Energy Informatics Conference 2016. Sept. 2016. URL: http://www.energieinformatik2016.org/wp-content/uploads/2016/10/EnInf2016_Poster_Findrik.pdf.

Wiedermann et al.: Smart Grid Cyber-Security Simulation Environment **wiederma2016SparksSmartGridCoSim**

Norbert Wiedermann and Mislav Findrik. "Smart Grid Cyber-Security Simulation Environment". In: *5th D-A-CH+ Energy Informatics Conference in conjunction with 7th Symposium on Communications for Energy Systems (ComForEn)*. Ed. by Dipl.-Ing. Dr. techn. Friederich Kupzog. ISBN: 978-3-85133-090-8. AIT Austrian Institute of Technology GmbH Giefinggasse 2 1210 Wien: Eigenverlag des Österreichischen Verbandes für Elektrotechnik, Sept. 2016, p. 96. URL: http://www.energieinformatik2016.org/wp-content/uploads/2016/09/Proceedings_DACH-Energy-Informatics_ComForEn-2016-Web.pdf.

Abstract: The current power grid is going to be extended with various field devices, which will under the control of the Distribution System Operator (DSO) be responsible to efficiently handle the demand and supply of electricity. This new system requires more interconnected ICT components than there are now, in order to collect all necessary measurement values to perform grid control operations in a fast and effective way. Before deploying new infrastructure and control functionalities it is important to understand the risk associated with potential cyber-attacks. Hence, it is very important to assess the impact cyber-attacks might have on the electrical grid and dependent infrastructure, in future smart grid scenarios. In this work, a software-software co-simulation environment for the impact assessment of cyber-attacks is presented, together with soft-ware/Hardware-in-the-loop (HIL) conceptual realization of a testbed environment dedicated for development and evaluation of security countermeasures.

Wolf et al.: Adaptive Modelling for Security Analysis of Networked Control Systems **WolfWSHWH16**

Jan Wolf, Felix Wieczorek, Frank Schiller, Gerhard Hansch, Norbert Wiedermann, and Martin Hutle. "Adaptive Modelling for Security Analysis of Networked Control Systems". In: *4th International Symposium for ICS & SCADA Cyber Security Research 2016, ICS-CSR 2016, 23 - 25 August 2016, Queen's Belfast University, UK*. 2016. URL: http://ewic.bcs.org/content/ConWebDoc/56479.

Zankl et al.: Towards Efficient Evaluation of a Time-Driven Cache Attack on Modern Processors **ZanklEtAl2016**

Andreas Zankl, Katja Miller, Johann Heyszl, and Georg Sigl. "Towards Efficient Evaluation of a Time-Driven Cache Attack on Modern Processors". In: *Computer Security – ESORICS 2016: 21st European Symposium on Research in Computer Security, Heraklion, Greece, September 26-30, 2016, Proceedings, Part II*. Ed. by Ioannis Askoxylakis, Sotiris Ioannidis, Sokratis Katsikas, and Catherine Meadows. Cham: Springer International Publishing, 2016, pp. 3–19. ISBN: 978-3-319-45741-3. DOI: 10.1007/978-3-319-45741-3_1. URL: http://dx.doi.org/10.1007/978-3-319-45741-3_1.

Adam et al.: Two Architecture Approaches for MILS Systems in Mobility Domains (Automobile, Railway and Avionik) **Adam2015**

D. Adam, S. Tverdyshev, C. Rolfes, T. Sandmann, S. Baehr, O. Sander, J. Becker, and U. Baumgarten. "Two Architecture Approaches for MILS Systems in Mobility Domains (Automobile, Railway and Avionik)". In: *International Workshop on MILS: Architecture and Assurance for Secure Systems (MILS 2015)*. 2015. URL: http://mils-workshop.euromils.eu/downloads/hipeac_literature/03-mils15_submission_5.pdf.

Banse et al.: A Secure Northbound Interface for SDN Applications **Banse:2015**

Christian Banse and Sathyanarayanan Rangarajan. "A Secure Northbound Interface for SDN Applications". In: *The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. 2015.

Abstract: Software-Defined Networking (SDN) promises to introduce flexibility and programmability into networks by offering a northbound interface (NBI) for developers to create SDN applications. However, current designs and implementations have several drawbacks, including the lack of extended security features. In this paper, we present a secure northbound interface, through which an SDN controller can offer network resources, such as statistics, flow information or topology data, via a REST-like API to registered SDN applications. A trust manager ensures that only authenticated and trusted applications can utilize the interface. Furthermore, a permission system allows for fine-grained authorization and access control to the aforementioned resources. We present a prototypical implementation of our interface and developed example applications using our interface, including an SDN management dashboard.

Böttinger et al.: Detecting Fingerprinted Data in TLS Traffic **boettinger2015detecting**

Konstantin Böttinger, Dieter Schuster, and Claudia Eckert. "Detecting Fingerprinted Data in TLS Traffic". In: *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*. ASIA CCS '15. Singapore, Republic of Singapore: ACM, 2015, pp. 633–638. ISBN: 978-1-4503-3245-3. DOI: 10.1145/2714576.2714595. URL: http://doi.acm.org/10.1145/2714576.2714595.

Brost et al.: Identifying Security Requirements and Privacy Concerns in Digital Health Applications **brost2015**

Gerd Stefan Brost and Mario Hoffmann. "Identifying Security Requirements and Privacy Concerns in Digital Health Applications". English. In: *Requirements Engineering for Digital Health*. Ed. by Samuel A. Fricker, Christoph Thümmler, and Anastasius Gavras. Springer International Publishing, 2015, pp. 133–154. ISBN: 978-3-319-09797-8. DOI: 10.1007/978-3-319-09798-5_7. URL: http://dx.doi.org/10.1007/978-3-319-09798-5_7.

Eckert et al.: Industrie 4.0 meets IT-Sicherheit: eine Herausforderung! **fallenbeck_eckert2015**

Claudia Eckert and Niels Fallenbeck. "Industrie 4.0 meets IT-Sicherheit: eine Herausforderung!" In: *Informatik-Spektrum*. Springer, Mar. 2015.

Eichler et al.: Modular risk assessment for the development of secure automotive systems **eichler2015modular**

Jörn Eichler and Daniel Angermeier. "Modular risk assessment for the development of secure automotive systems". In: *Tagungsband der 31. VDI/VW-Gemeinschaftstagung Automotive Security*. 2015.

Abstract: Methods for the assessment of security risks often follow an inflexible "one size fits all" approach. Consequently, these methods might get too superficial for complex vehicular functions, systems, or ECUs and too heavy-weight for quick risk assessments. We propose a risk assessment method for the development of automotive systems which features a modular structure and supports hierarchical decomposition of the target of evaluation to achieve improved scalability. Thus, the effort and level of detail for each assessment can be adjusted to the potential damage and to the current state of the development process. Our approach also offers guidance and catalogues for practical application in industry. We report on early experiences from the application of our approach for the development of electronic control units by an international OEM.

Heyszl et al.: Geldspielgeräte in Zukunft mit geprüfter Sicherheit **heyszl2015geldspielgerate**

Johann Heyszl and Florian Thiel. "Geldspielgeräte in Zukunft mit geprüfter Sicherheit". In: *Datenschutz und Datensicherheit-DuD* 39.4 (2015), pp. 234–239.

Hiller et al.: Low-Area Reed Decoding in a Generalized Concatenated Code Construction for PUF **hiller2015lowearea**

Matthias Hiller, Ludwig Kürzinger, Georg Sigl, Sven Müelich, Sven Puchinger, and Martin Bossert. "Low-Area Reed Decoding in a Generalized Concatenated Code Construction for PUF". In: *Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. To appear. 2015.

Horsch et al.: Transparent Page-based Kernel and User Space Execution Tracing from a Custom Minimal ARM Hypervisor **Horsch:2015**

Julian Horsch and Sascha Wessel. "Transparent Page-based Kernel and User Space Execution Tracing

from a Custom Minimal ARM Hypervisor". In: *The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. 2015.

Abstract: In this paper, we present a framework for trans- parent kernel and user execution tracing from a minimal ARM hypervisor. The framework utilizes hardware-supported virtualization on modern ARM CPUs to restrict the number of executable pages in the system without interfering with the traced guest. The resulting page faults give the framework access to page-granular control flow information. The framework is transparent and agnostic to kernel and user space software not requiring any changes or additional components in the traced guest. The application scenarios for the framework include malware analysis, malware detection and runtime integrity protection. We furthermore present a detailed example application for the framework which uses the provided trace data to enforce a particular page-granular control flow to defend the guest against control flow hijacking attacks like return-oriented programming. The detailed performance analysis of our prototype implementation running on a Cortex-A15 development board with Android shows that the framework and the example application perform well even in adverse benchmarking scenarios. Therefore, the framework not only can be useful for realizing virtualization-based security mechanisms known and researched on x86 platforms for ARM, but also shows that the very lightweight ARM hardware virtualization support allows for new mechanisms relying on very frequent interaction with the hypervisor.

Hutle et al.: Vulnerability analysis of digital instrumentation and control systems important to safety – a methodical approach **hutle2015vulnerability**

Martin Hutle and Freddy Seidel. "Vulnerability analysis of digital instrumentation and control systems important to safety – a methodical approach". In: *IAEA International Conference on Computer Security in a Nuclear World*. to appear. 2015.

Muntean et al.: Automated Generation of Buffer Overflows Quick Fixes using Symbolic Execution and SMT **muntean_eckert2015a**

P. Muntean, V. K. Kommanapalli, A. Ibing, and Eckert C. "Automated Generation of Buffer Overflows Quick Fixes using Symbolic Execution and SMT". In: *International Conference on Computer Safety, Reliability & Security (SAFECOMP'15)*. LNCS, 2015.

Muntean et al.: Automated Detection of Information Flow Vulnerabilities in UML State Charts and C Code **muntean_eckert2015b**

P. Muntean, A. Rabbi, A. Ibing, and Eckert C. "Automated Detection of Information Flow Vulnerabilities in UML State Charts and C Code". In: *IEEE International Workshop on Model-Based Verification & Validation (MVV'15)*. IEEE, 2015.

Muntean et al.: SMT-Constrained Symbolic Execution Engine for Integer Overflow Detection in C Code **muntean_eckert2015c**

P. Muntean, M. Rahman, A. Ibing, and Eckert C. "SMT-Constrained Symbolic Execution Engine for Integer Overflow Detection in C Code". In: *14th International Information Security South Africa Conference, (ISSA'15)*. IEEE, 2015.

Nyberg et al.: Closing the gap between speed and configurability of multi-bit fault emulation environments for security and safety-critical designs

DBLP:journals/mam/NybergHRS15

Ralph Nyberg, Johann Heyszl, Dirk Rabe, and Georg Sigl. "Closing the gap between speed and configurability of multi-bit fault emulation environments for security and safety-critical designs". In: *Microprocessors and Microsystems - Embedded Hardware Design* 39.8 (2015), pp. 1119–1129. DOI: 10.1016/j.micpro.2015.05.015. URL: http://dx.doi.org/10.1016/j.micpro.2015.05.015.

Nyberg et al.: Efficient Fault Emulation through Splitting Combinational and Sequential Fault Propagation

Nyberg2015a

Ralph Nyberg, Johann Heyszl, and Georg Sigl. "Efficient Fault Emulation through Splitting Combinational and Sequential Fault Propagation". In: *1st International Workshop on Resiliency in Embedded Electronic*. 2015.

Proskurin et al.: Retrospective Protection utilizing Binary Rewriting

proskurin_kilic_eckert2015

Sergej Proskurin, Fatih Kilic, and Claudia Eckert. "Retrospective Protection utilizing Binary Rewriting". In: *14. Deutscher IT-Sicherheitskongress*. May 2015. URL: https://www.sec.in.tum.de/assets/Uploads/BinProtect2.pdf.

Proskurin et al.: seTPM: Towards Flexible Trusted Computing on Mobile Devices based on GlobalPlatform Secure Elements

Proskurin:2015

Sergej Proskurin, Michael Weiß, and Georg Sigl. "seTPM: Towards Flexible Trusted Computing on Mobile Devices based on GlobalPlatform Secure Elements". In: *Smart Card Research and Advanced Application, 14th International Conference, CARDIS 2015, Bochum, Germany, November 4-6, 2015. Proceedings*. 2015.

Abstract: Insufficiently protected mobile devices present an ubiquitous threat. Due to severe hardware constraints, such as limited printed circuit board area, hardware-based security as proposed by the Trusted Computing Group is usually not part of mobile devices, yet. We present the design and implementation of seTPM, a secure element based TPM, utilizing Java Card technology. seTPM establishes trust in mobile devices by enabling Trusted Computing based integrity measurement services, such as IMA for Linux. Our prototype emulates TPM functionality on a GlobalPlatform secure element which allows seamless integration into the Trusted Software Stack of Linux-based mobile operating systems like Android. With our work, we provide a solution to run Trusted Computing based security protocols while supplying a similar security level as provided by hardware TPM chips. In addition, due to the flexible design of the seTPM, we further increase the security level as we are able to selectively replace the outdated SHA-1 hash algorithm of TPM 1.2 specification by the present Keccak algorithm. Further, our architecture comprises hybrid support for the TPM 1.2 and TPM 2.0 specifications to simplify the transition towards the TPM 2.0 standard.

Renatus et al.: Improving prioritization of software weaknesses using security models with AVUS **renatus2015improving**

Stephan Renatus, Corrie Bartelheimer, and Jörn Eichler. "Improving prioritization of software weaknesses using security models with AVUS". In: *Proceedings of the 15th IEEE International Working Conference on Source Code Analysis and Manipulation*. 2015.

Abstract: Testing tools for application security have become an integral part of secure development life-cycles. Despite their ability to spot important software weaknesses, the high number of findings require rigorous prioritization in many environments. Most testing tools provide generic ratings to support prioritization. Unfortunately, ratings from established tools lack context information especially with regard to the security requirements of respective components or source code. Thus experts often spend a great deal of time re-assessing the prioritization provided by these tools. This paper introduces our lightweight tool AVUS that adjusts context-free ratings of software weaknesses according to a user-defined security model. We also present a first evaluation applying AVUS to a well-known open source project and the findings of a popular, commercially available application security testing tool.

Renatus et al.: Method Selection and Tailoring for Agile Threat Assessment and Mitigation **renatus2015method**

Stephan Renatus, Clemens Teichmann, and Jörn Eichler. "Method Selection and Tailoring for Agile Threat Assessment and Mitigation". In: *Proceedings of the First International Workshop on Agile Secure Software Development (ASSD)*. 2015.

Abstract: Security engineering and agile development are often perceived as a clash of cultures. To address this clash, several approaches have been proposed that allow for agile security engineering. Unfortunately, agile development organization differ in their actual procedures and environmental properties resulting in varying requirements. We propose an approach to compare and select methods for agile security engineering. Furthermore, our approach addresses adaptation or construction of a tailored method taking the existing development culture into account. We demonstrate the feasibility of our proposal and report early experiences from its application within a small development organization for digital solutions in the automotive domain.

Salfer et al.: Attack Surface and Vulnerability Assessment of Automotive Electronic Control Units **salfer_eckert**

Martin Salfer and Claudia Eckert. "Attack Surface and Vulnerability Assessment of Automotive Electronic Control Units". In: *Proceedings of the 12th International Conference on Security and Cryptography (SECRYPT 2015)*. Colmar, France, July 2015.

Schütte et al.: ConDroid: Targeted Dynamic Analysis of Android Applications **Schuette2015**

Julian Schütte, Rafael Fedler, and Dennis Titze. "ConDroid: Targeted Dynamic Analysis of Android Applications". In: *Proceedings of the International Conference on Advanced Information Networking and Applications (AINA)*. 2015.

Abstract: Recent years have seen the development of a multitude of tools for the security analysis of Android applications. A major deficit of current fully automated security analyses, however, is their inability to drive execution to interesting parts, such as where code is dynamically loaded or certain data is decrypted. In fact, security-critical or downright offensive code may not be reached at all by such analyses when dynamically checked conditions are not met by the analysis environment. Harmful code may thus remain completely invisible to the analysis software and subsequently not be analyzed altogether. To tackle this unsolved problem, we propose a tool combining static call path analysis with bytecode instrumentation and a heuristic partial symbolic execution, which aims at executing interesting calls paths. It can systematically locate potentially security-critical code sections and instrument applications such that execution of these sections can be observed in a dynamic analysis. Among other use cases, this can be leveraged to force applications into revealing dynamically loaded code, a simple yet effective way to circumvent detection by security analysis software such as the Google Play Store's Bouncer. We illustrate the functionality of our tool by means of a simple logic bomb example and a real-life security vulnerability which is present in hunderd of apps and can still be actively exploited at this time.

Selmke et al.: Precise Laser Fault Injections into 90 nm and 45 nm SRAM-cells

Selmke2015a

Bodo Selmke, Stefan Brummer, Johann Heyszl, and Georg Sigl. "Precise Laser Fault Injections into 90 nm and 45 nm SRAM-cells". In: *Smart Card Research and Advanced Applications - 14th International Conference, CARDIS 2015, Bochum, Germany, November 4-6, 2015. Revised Selected Papers*. 2015, pp. 193–205. doi: 10.1007/978-3-319-31271-2_12. url: http://dx.doi.org/10.1007/978-3-319-31271-2_12.

Abstract: Fault injection into integrated circuits by exposure to laser light is a common method to break cryptographic devices. The specific requirements of sophisticated fault attacks as well as the presence of countermeasures ask for precise control of the generated faults. However, the feature-sizes of integrated circuits are decreasing while the physical dimensions of laser spots are lower bounded by the used wavelength. We investigate laser-based fault injection into SRAM cells of two popular FPGAs with different feature-sizes, i.e. 90 nm and 45 nm, which are interesting in the context of current security chips. We describe our setup and methods for precise calibration of all important parameters. Our practical experiments confirm that single bit faults are achievable on 90 nm feature size SRAM cells. The precision is lower in the 45 nm technology, because adjacent SRAM cells are affected in many cases. However, depending on the location of an SRAM cell within a hard macro and the previous values of adjacent cells, an attacker can still achieve precise single-bit manipulations. This should be a design criteria for choosing storage locations of variables and for efficient error correction codes for secure implementations.

Settanni et al.: A Blueprint for a Pan-European Cyber Incident Analysis System

eu_ec_2015

Giuseppe Settanni, Florian Skopik, Helmut Kaufmann, Tobias Gebhardt, Klaus Theuerkauf, Konstantin Böttinger, Mark Carolan, Damien Conroy, and Pia Olli. "A Blueprint for a Pan-European Cyber Incident Analysis System". In: *3rd International Symposium for ICS & SCADA Cyber Security Research 2015, ICS-CSR 2015*. 2015.

Specht et al.: Improving Non-profiled Attacks on Exponentiations Based on Clustering and Extracting Leakage from Multi-channel High-Resolution EM Measurements
DBLP:conf/cosade/SpechtHKS15

Robert Specht, Johann Heyszl, Martin Kleinsteuber, and Georg Sigl. "Improving Non-profiled Attacks on Exponentiations Based on Clustering and Extracting Leakage from Multi-channel High-Resolution EM Measurements". In: *Constructive Side-Channel Analysis and Secure Design - 6th International Workshop, COSADE 2015, Berlin, Germany, April 13-14, 2015. Revised Selected Papers*. 2015, pp. 3–19. doi: 10.1007/978-3-319-21476-4_1. url: http://dx.doi.org/10.1007/978-3-319-21476-4_1.

Stephanow et al.: Towards continuous certification of Infrastructure-as-a-Service using low-level metrics. **stephanow2015continuous**

Philipp Stephanow and Niels Fallenbeck. "Towards continuous certification of Infrastructure-as-a-Service using low-level metrics." In: *12th IEEE International Conference on Advanced and Trusted Computing (ATC)*. IEEE. 2015.

Abstract: Continuous cloud service certification describes the process of continuously validating whether a service adheres to a set of requirements. However, most requirements derived from existing standards such as ISO-27001:2013 are generic, often times inherently ambiguous and thus cannot be validated automatically. In this paper, we address this gap by presenting a bottom-up approach using low-level metrics available through widely deployed implementations of infrastructure-as-a-service (IaaS) components. We further present examples how these lowlevel metrics can serve to construct complex metrics to support validation of generic requirements.

Stephanow et al.: Language Classes for Cloud Service Certification Systems
stephanow2015language

Philipp Stephanow and Mark Gall. "Language Classes for Cloud Service Certification Systems". In: *2015 IEEE 11th World Congress on Services (SERVICES)*. IEEE. 2015.

Abstract: Certification of cloud services aims at increasing the trust of customers towards cloud services and providing comparability between cloud services. Applying the concept of certification to cloud services requires systems which continuously detect ongoing changes of the service and assess their impact on customer requirements. In this paper, we propose eight language classes for cloud service certification systems to facilitate research in design and implementation of these systems. To that end, we draw on language classes developed for signature-based intrusion detection systems and apply them to cloud service certification systems.

Taubmann et al.: A Lightweight Framework for Cold Boot Based Forensics on Mobile Devices **Taubmann:2015**

Benjamin Taubmann, Manuel Huber, Sascha Wessel, Lukas Heim, Hans Peter Reiser, and Georg Sigl. "A Lightweight Framework for Cold Boot Based Forensics on Mobile Devices". In: *Proceedings of the 2015 10th International Conference on Availability, Reliability and Security*. ARES '15. Washington, DC, USA: IEEE Computer Society, 2015, pp. 120–128. isbn: 978-1-4673-6590-1. doi: 10.1109/ARES.2015.47. url: https://doi.org/10.1109/ARES.2015.47.

Titze et al.: Apparecium: Revealing Data Flows in Android Applications **Titze2015**

Dennis Titze and Julian Schütte. "Apparecium: Revealing Data Flows in Android Applications". In: *Proceedings of the International Conference on Advanced Information Networking and Applications (AINA)*. 2015.

Abstract: With Android applications processing not only personal but also business-critical data, efficient and precise data flow analysis has become a major technique to detect apps handling critical data in unwanted ways. Although data flow analysis in general is a thoroughly researched topic, the event-driven lifecycle model of Android has its own challenges and practical application requires for reliable and efficient analysis techniques. In this paper we present Apparecium, a tool to reveal data flows in Android applications. Apparecium has conceptual differences to other techniques, and can be used to find arbitrary data flows inside Android applications. Details about the used techniques and the differences to existing data flow analysis tools are presented, as well as an evaluation against the data flow analysis framework FlowDroid.

Titze et al.: Preventing Library Spoofing on Android **Titze2015a**

Dennis Titze and Julian Schütte. "Preventing Library Spoofing on Android". In: *Proceedings of IEEE International Workshop on Trustworthy Software Systems*. Helsinki, Finland, 2015.

Abstract: Dynamic loading of libraries is a widely used technique in Android applications. But including and executing external library code does not only have benefits, it can have severe detrimental security implications for the application and the user.
In this paper we explain the mechanisms of loading external library code into an Android application and discuss resulting security implications. Since an attacker can easily impersonate libraries if the application does not perform the necessary verification, loading such code can introduce severe security problems. As a remedy, we present how external code can be verified and since currently available application often do not perform such verification, we introduce a novel way to enforce this verification. A prototype of this system has been published as open-source which can be easily integrated into existing apps and libraries.

Velten et al.: User Identity Verification Based on Touchscreen Interaction Analysis in Web Contexts **Velten:2015**

Michael Velten, Peter Schneider, Sascha Wessel, and Claudia Eckert. "User Identity Verification Based on Touchscreen Interaction Analysis in Web Contexts". In: *Information Security Practice and Experience*. Ed. by Javier Lopez and Yongdong Wu. Vol. 9065. Lecture Notes in Computer Science. Springer International Publishing, 2015, pp. 268–282. isbn: 978-3-319-17532-4. doi: 10.1007/978-3-319-17533-1_19.

Abstract: The ever-increasing popularity of smartphones amplifies the risk of loss or theft, thus increasing the threat of attackers hijacking critical user accounts. In this paper, we present a framework to secure accounts by continuously verifying user identities based on user interaction behavior with smartphone touchscreens. This enables us to protect user accounts by disabling critical functionality and enforcing a reauthentication in case of suspicious behavior. We take advantage of standard mobile web browser capabilities to remotely capture and analyze touchscreen interactions. This approach is completely transparent for the user and works on everyday smartphones without requiring any special software or privileges on the user's device. We show how to successfully clas-

sify users even on the basis of limited and imprecise touch interaction data as is prevalent in web contexts. We evaluate the performance of our framework and show that the user identification accuracy is higher than 99% after collecting about a dozen touch interactions.

Wessel et al.: Improving Mobile Device Security with Operating System-level Virtualization **Wessel:2015**

Sascha Wessel, Manuel Huber, Frederic Stumpf, and Claudia Eckert. "Improving Mobile Device Security with Operating System-level Virtualization". In: *Computers & Security*. Vol. 52. C. Oxford, UK: Elsevier Advanced Technology Publications, July 2015, pp. 207–220. doi: 10.1016/j.cose.2015.02.005. url: https://doi.org/10.1016/j.cose.2015.02.005.

Xiao et al.: Is Feature Selection Secure against Training Data Poisoning? **huang_eckert15**

Huang Xiao, Battista Biggio, Gavin Brown, Giorgio Fumera, Claudia Eckert, and Fabio Roli. "Is Feature Selection Secure against Training Data Poisoning?" In: *Proceedings of The 32nd International Conference on Machine Learning (ICML'15)*. Lille, France, July 2015, p. 16891698. url: https://www.sec.in.tum.de/assets/Uploads/main-camera-ready.pdf.

Belaïd et al.: Towards fresh re-keying with leakage-resilient PRFs: cipher design principles and analysis **DBLP:journals/jce/BelaidSHMMSST14**

Sonia Belaïd, Fabrizio De Santis, Johann Heyszl, Stefan Mangard, Marcel Medwed, Jörn-Marc Schmidt, François-Xavier Standaert, and Stefan Tillich. "Towards fresh re-keying with leakage-resilient PRFs: cipher design principles and analysis". In: *J. Cryptographic Engineering* 4.3 (2014), pp. 157–171. doi: 10.1007/s13389-014-0079-5. url: http://dx.doi.org/10.1007/s13389-014-0079-5.

Fallenbeck et al.: IT-Sicherheit und Cloud Computing **fallenbeck_eckert**

Niels Fallenbeck and Claudia Eckert. "IT-Sicherheit und Cloud Computing". In: ed. by Thomas Bauernhansl, Michael ten Hompel, and Birgit Vogel-Heuser. Springer Vieweg, 2014, pp. 397–431.

Filipovic: Firmware protection is already half way **filipovic2014firmwareprotection**

Bartol Filipovic. "Firmware protection is already half way". In: *Product and Know-how Protection (Brochure)* 1 (2014), pp. 28–29.

Filipovic: Firmware-Schutz ist die halbe Miete **filipovic2014firmwareschutz**

Bartol Filipovic. "Firmware-Schutz ist die halbe Miete". In: *Produkt- und Know-how-Schutz (Broschüre)* 1 (2014), pp. 28–29.

Filipovic: Maschine mit Kopierschutz **filipovic2014maschine**

Bartol Filipovic. "Maschine mit Kopierschutz". In: *Konstruktion - Zeitschrift für Produktentwicklung und Ingenieur-Werkstoffe (Zeitschrift)* 11-12 (2014), p. 6.

Filipovic: Security aufbauen und pflegen **filipovic2014security**

Bartol Filipovic. "Security aufbauen und pflegen". In: *Mechatronik (Zeitschrift)* 11 (2014). 122. Jahrgang, pp. 52–53.

Gebert et al.: Demonstrating the Optimal Placement of Virtualized Cellular Network Functions in Case of Large Crowd Events **Banse2014**

Steffen Gebert, David Hock, Thomas Zinner, Phuoc Tran-Gia, Marco Hoffmann, Michael Jarschel, Ernst-Dieter Schmidt, Ralf-Peter Braun, Christian Banse, and Andreas Köpsel. "Demonstrating the Optimal Placement of Virtualized Cellular Network Functions in Case of Large Crowd Events". In: *Proceedings of the 2014 ACM Conference on SIGCOMM*. SIGCOMM '14. Chicago, Illinois, USA: ACM, 2014, pp. 359–360. isbn: 978-1-4503-2836-4. doi: 10.1145/2619239.2631428. url: http://doi.acm.org/10.1145/2619239.2631428.

Gonz´alez-Manzano et al.: An Architecture for Trusted PaaS Cloud Computing for Personal Data **aumueller2014**

Lorena Gonz´alez-Manzano, Gerd Brost, and Matthias Aumueller. "An Architecture for Trusted PaaS Cloud Computing for Personal Data". English. In: *Trusted Cloud Computing*. Ed. by Helmut Krcmar, Ralf Reussner, and Bernhard Rumpe. Springer International Publishing, 2014, pp. 239–258. isbn: 978-3-319-12717-0. doi: 10.1007/978-3-319-12718-7_15. url: http://dx.doi.org/10.1007/978-3-319-12718-7_15.

Heinz et al.: Side-Channel Analysis of a High-Throughput AES Peripheral with Countermeasures **Heinz2014**

Benedikt Heinz, Johann Heyszl, and Frederik Stumpf. "Side-Channel Analysis of a High-Throughput AES Peripheral with Countermeasures". In: *2014 Internation Symposium on Integrated Circuits (ISIC)*. 2014.

Hennig et al.: Vorrichtung und Verfahren mit einem Träger mit Schaltungsstrukturen **hennig2014vorrichtung**

Maxim Hennig, Oliver Schimmel, Philipp Zieris, and Bartol Filipovic. *Vorrichtung und Verfahren mit einem Träger mit Schaltungsstrukturen*. WO Patent App. PCT/EP2014/055,123. Oct. 2014. url: https://www.google.com/patents/WO2014154504A2?cl=de.

Hoffmann et al.: Wireless-enabled smart societies in the 2020s: An overview of the 31st meeting of wireless world research forum [From the guest editors] **Hoffmann2014c**

M.D. Hoffmann, N. Jefferies, and L.H. Woo. "Wireless-enabled smart societies in the 2020s: An overview of the 31st meeting of wireless world research forum [From the guest editors]". In: *IEEE Vehicular Technology Magazine* 9.1 (2014). cited By 0, pp. 26–27. doi: 10.1109/MVT.2014.2306531. url: http://www.scopus.com/inward/record.url?eid=2-s2.0-84898462551&partnerID=40&md5=72e2185e4da7885a8552160f9ad7b03e.

Horsch et al.: TrustID: Trustworthy Identities for Untrusted Mobile Devices Horsch:2014b

Julian Horsch, Konstantin Böttinger, Michael Weiß, Sascha Wessel, and Frederic Stumpf. "TrustID: Trustworthy Identities for Untrusted Mobile Devices". In: *Proceedings of the 4th ACM Conference on Data and Application Security and Privacy*. CODASPY 2014. San Antonio, Texas, USA: ACM, 2014, pp. 281–288. isbn: 978-1-4503-2278-2. doi: 10.1145/2557547.2557593.

Abstract: Identity theft has deep impacts in today's mobile ubiquitous environments. At the same time, digital identities are usually still protected by simple passwords or other insufficient security mechanisms. In this paper, we present the TrustID architecture and protocols to improve this situation. Our architecture utilizes a Secure Element (SE) to store multiple context-specific identities securely in a mobile device, e.g., a smartphone. We introduce protocols for securely deriving identities from a strong root identity into the SE inside the smartphone as well as for using the newly derived IDs. Both protocols do not require a trustworthy smartphone operating system or a Trusted Execution Environment. In order to achieve this, our concept includes a secure combined PIN entry mechanism for user authentication, which prevents attacks even on a malicious device. To show the feasibility of our approach, we implemented a prototype running on a Samsung Galaxy SIII smartphone utilizing a microSD card SE. The German identity card nPA is used as root identity to derive context-specific identities.

Horsch et al.: SobTrA: A Software-based Trust Anchor for ARM Cortex Application Processors Horsch:2014a

Julian Horsch, Sascha Wessel, Frederic Stumpf, and Claudia Eckert. "SobTrA: A Software-based Trust Anchor for ARM Cortex Application Processors". In: *Proceedings of the 4th ACM Conference on Data and Application Security and Privacy*. CODASPY 2014. San Antonio, Texas, USA: ACM, 2014, pp. 273–280. isbn: 978-1-4503-2278-2. doi: 10.1145/2557547.2557569.

Abstract: In this paper, we present SobTrA, a Software-based Trust Anchor for ARM Cortex-A processors to protect systems against software-based attacks. SobTrA enables the implementation of a software-based secure boot controlled by a third party independent from the manufacturer. Compared to hardware-based trust anchors, our concept provides some other advantages like being updateable and also usable on legacy hardware. The presented software-based trust anchor involves a trusted third party device, the verifier, locally connected to the untrusted device, e.g., via the microSD card slot of a smartphone. The verifier is verifying the integrity of the untrusted device by making sure that a piece of code is executed untampered on it using a timing-based approach. This code can then act as an anchor for a chain of trust similar to a hardware-based secure boot. Tests on our prototype showed that tampered and untampered execution of SobTrA can be clearly and reliably distinguished.

Jacob et al.: Hardware Trojans: current challenges and approaches DBLP:journals/iet-cdt/JacobMHS14

N. Jacob, Dominik Merli, Johann Heyszl, and Georg Sigl. "Hardware Trojans: current challenges and approaches". In: *IET Computers & Digital Techniques* 8.6 (2014), pp. 264–273. doi: 10.1049/iet-cdt.2014.0039. url: http://dx.doi.org/10.1049/iet-cdt.2014.0039.

Kilic et al.: Blind Format String Attacks **Kilic_eckert2014**

Fatih Kilic, Thomas Kittel, and Claudia Eckert. "Blind Format String Attacks". In: *Proceedings of the International Workshop on Data Protection in Mobile and Pervasive Computing (DAPRO)*. Lecture Notes in Computer Science. Springer, Sept. 2014. url: https://www.sec.in.tum.de/assets/Uploads/formatstring.pdf.

Kittel et al.: Code Validation for Modern OS Kernels **kittel_eckert2014**

Thomas Kittel, Sebastian Vogl, Tamas K. Lengyel, Jonas Pfoh, and Claudia Eckert. "Code Validation for Modern OS Kernels". In: *Workshop on Malware Memory Forensics (MMF)*. Dec. 2014. url: https://www.sec.in.tum.de/assets/Uploads/acsacmmfkittel.pdf.

Lengyel et al.: Multi-tiered Security Architecture for ARM via the Virtualization and Security Extensions **lengyel_eckert2014**

Tamas K. Lengyel, Thomas Kittel, and Claudia Eckert. "Multi-tiered Security Architecture for ARM via the Virtualization and Security Extensions". In: *1st Workshop on Security in highly connected IT systems*. Sept. 2014. url: https://www.sec.in.tum.de/assets/Uploads/lengyelshcis2.pdf.

Merli: Attacking and Protecting Ring Oscillator Physical Unclonable Functions and Code-Offset Fuzzy Extractors **Merli2014**

Dominik Merli. "Attacking and Protecting Ring Oscillator Physical Unclonable Functions and Code-Offset Fuzzy Extractors". PhD thesis. Technische Universität München, 2014.

Milosevic et al.: Tolerating permanent and transient value faults **milosevic2014tolerating**

Zarko Milosevic, Martin Hutle, and André Schiper. "Tolerating permanent and transient value faults". In: *Distributed Computing* 27.1 (2014), pp. 55–77. doi: 10.1007/s00446-013-0199-7. url: http://dx.doi.org/10.1007/s00446-013-0199-7.

Moradi et al.: Early Propagation and Imbalanced Routing, How to Diminish in FPGAs **moradi2014early**

Amir Moradi and Vincent Immler. "Early Propagation and Imbalanced Routing, How to Diminish in FPGAs". In: *Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings*. 2014, pp. 598–615. doi: 10.1007/978-3-662-44709-3_33. url: http://dx.doi.org/10.1007/978-3-662-44709-3_33.

Muntean et al.: Context-sensitive detection of information exposure bugs with symbolic execution **muntean_eckert2014**

P. Muntean, C. Eckert, and A Ibing. "Context-sensitive detection of information exposure bugs with symbolic execution". In: *International Workshop on Innovative Software Development Methodologies and Practices (InnoSWDev'14)*. ACM, Nov. 2014. url: https://www.sec.in.tum.de/assets/Uploads/PMInnoSWDev14.pdf.

Nyberg et al.: Closing the Gap between Speed and Configurability of Multi-bit Fault Emulation Environments for Security and Safety-Critical Designs
DBLP:conf/dsd/NybergNHRS14

Ralph Nyberg, Jurgen Nolles, Johann Heyszl, Dirk Rabe, and Georg Sigl. "Closing the Gap between Speed and Configurability of Multi-bit Fault Emulation Environments for Security and Safety-Critical Designs". In: *17th Euromicro Conference on Digital System Design, DSD 2014, Verona, Italy, August 27-29, 2014*. 2014, pp. 114–121. doi: 10.1109/DSD.2014.39. url: http://dx.doi.org/10.1109/DSD.2014.39.

Rieke et al.: Monitoring Security Compliance of Critical Processes rieke2014monitoring

Roland Rieke, Jürgen Repp, Maria Zhdanova, and Jörn Eichler. "Monitoring Security Compliance of Critical Processes". In: *Proceedings of the 22nd Euromicro International Conference on Parallel, Distributed, and Network-based Processing*. IEEE, 2014.

Abstract: Enforcing security in process-aware information systems at runtime requires the monitoring of systems' operation using process information. Analysis of this information with respect to security and compliance aspects is growing in complexity with the increase in functionality, connectivity, and dynamics of process evolution. To tackle this complexity, the application of models is becoming standard practice. Considering today's frequent changes to processes, model-based support for security and compliance analysis is not only needed in pre-operational phases but also at runtime. This paper presents an approach to support evaluation of the security status of processes at runtime. The approach is based on operational formal models derived from process specifications and security policies comprising technical, organizational, regulatory and cross-layer aspects. A process behavior model is synchronized by events from the running process and utilizes prediction of expected close-future states to find possible security violations and allow early decisions on countermeasures. The applicability of the approach is exemplified by a scenario from a hydroelectric power plant.

Salfer et al.: Efficient Attack Forest Construction for Automotive On-board Networks
salfer_eckert2014a

Martin Salfer, Hendrik Schweppe, and Claudia Eckert. "Efficient Attack Forest Construction for Automotive On-board Networks". In: *Lecture Notes in Computer Science*. Vol. 8783. Springer, 2014, pp. 442–453.

Schuster et al.: Evaluation of Bistable Ring PUFs Using Single Layer Neural Networks
schuster2014evaluation

Dieter Schuster and Robert Hesselbarth. "Evaluation of Bistable Ring PUFs Using Single Layer Neural Networks". In: *Trust and Trustworthy Computing*. Springer, 2014, pp. 101–109.

Schuster et al.: Evaluation of Bistable Ring PUFs Using Single Layer Neural Networks
DBLP:conf/trust/SchusterH14

Dieter Schuster and Robert Hesselbarth. "Evaluation of Bistable Ring PUFs Using Single Layer Neural Networks". In: *Trust and Trustworthy Computing - 7th International Conference, TRUST 2014, Her-*

aklion, Crete, Greece, June 30 - July 2, 2014. Proceedings. 2014, pp. 101–109. doi: 10.1007/978-3-319-08593-7_7. url: http://dx.doi.org/10.1007/978-3-319-08593-7_7.

Schütte: NFC? Aber sicher. **Schuette2014a**

Julian Schütte. "NFC? Aber sicher." In: *Datenschutz und Datensicherheit (DuD)* 38 (1 2014), pp. 20–24.

Abstract: Mit Ausnahme von Apples iPhone zählt NFC mittlerweile zur Grundausstattung jedes High-End-Smartphone und neue Anwendungen wie Mobile Payment halten derzeit Einzug. Doch das so praktische Bezahlen mit dem Smartphone hat auch Tücken. NFC bietet keinerlei Sicherheitsmechanismen und Apps sind leicht anzugreifen. Schon zeichnet sich eine ganze Reihe neuer Angriffsszenarien ab. Verschiedene Sicherheitsmechanismen können Abhilfe schaffen, doch ihr Einsatz hat sowohl technische, als auch organisatorische Hürden.

Schütte et al.: AppCaulk: Data Leak Prevention by Injecting Targeted Taint Tracking Into Android Apps **Schuette2014**

Julian Schütte, Dennis Titze, and J. M. de Fuentes. "AppCaulk: Data Leak Prevention by Injecting Targeted Taint Tracking Into Android Apps". In: *Proceedings of the International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. 2014.

Abstract: As Android is entering the business domain, leaks of business-critical and personal information through apps become major threats. Due to the context- insensitive nature of the Android permission model, information flow policies cannot be enforced by on- board mechanisms. We therefore propose AppCaulk, an approach to harden any existing Android app by in- jecting a targeted dynamic taint analysis, which tracks and blocks unwanted information flows at runtime. Critical data flows are first discovered using a static taint analysis and the relevant data propagation paths are instrumented by a taint tracking code at register level. At runtime the dynamic taint analysis woven into the app detects and blocks data leaks as they are about to occur. In contrast to existing taint analysis approaches like Taintdroid, AppCaulk does not require modification of the Android middleware and can thus be applied to any stock Android installation. In this paper, we explain the design of AppCaulk, describe the evaluation of its prototype, and compare its effectiveness with Taintdroid.

Specht et al.: Investigating Measurement Methods for High-Resolution Electromagentic Field Side-Channel Analysis **Specht2014**

Robert Specht, Johann Heyszl, and Georg Sigl. "Investigating Measurement Methods for High-Resolution Electromagentic Field Side-Channel Analysis". In: *2014 Internation Symposium on Integrated Circuits (ISIC)*. 2014.

Titze et al.: App-Ray: User-driven and fully automated Android app security assessment **appray2014**

Dennis Titze, Philipp Stephanow, and Julian Schütte. *App-Ray: User-driven and fully automated Android app security assessment*. Tech. rep. 2014.

Vogl et al.: Dynamic Hooks: Hiding Control Flow Changes within Non-Control Data **vogl_eckert2014**

Sebastian Vogl, Robert Gawlik, Behrad Garmany, Thomas Kittel, Jonas Pfoh, Claudia Eckert, and Thorsten Holz. "Dynamic Hooks: Hiding Control Flow Changes within Non-Control Data". In: *Proceedings of the 23rd USENIX Security Symposium*. USENIX, Aug. 2014. url: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/vogl#.pdf.

Vogl et al.: Persistent Data-only Malware: Function Hooks without Code **vogl_pfoh_eckert2014**

Sebastian Vogl, Jonas Pfoh, Thomas Kittel, and Claudia Eckert. "Persistent Data-only Malware: Function Hooks without Code". In: *Proceedings of the 21th Annual Network & Distributed System Security Symposium (NDSS)*. Feb. 2014. url: http://www.internetsociety.org/doc/persistent-data-only-malware-function-hooks-without-code#.pdf.

Weiss et al.: Integrity Verification and Secure Loading of Remote Binaries for Microkernel-Based Runtime Environments **Weiss:2014a**

Michael Weiss, Steffen Wagner, Roland Hellman, and Sascha Wessel. "Integrity Verification and Secure Loading of Remote Binaries for Microkernel-Based Runtime Environments". In: *Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on*. 2014, pp. 544–551. doi: 10.1109/TrustCom.2014.69.

Abstract: While most microkernel-based systems implement non-essential software components as user space tasks and strictly separate those tasks during runtime, they often rely on a static configuration and composition of their software components to ensure safety and security. In this paper, we extend a microkernel-based system architecture with a Trusted Platform Module (TPM) and propose a verification mechanism for a microkernel runtime environment, which calculates integrity measurements before allowing to load (remote) binaries. As a result, our approach is the first to adopt the main ideas of the Integrity Measurement Architecture (IMA), which has been proposed for Linux-based systems, to a microkernel. In comparison, however, it significantly reduces the Trusted Computing Base (TCB) and allows for a strict separation of the integrity verification component from any rich operating system, such as GNU/Linux or Android, running in parallel. In our implementation, which is based on L4/Fiasco. OC with L4Re as runtime environment, we present our extension of the existing L4Re loader service that calculates integrity measurements for each binary. We also evaluate our implementation on two ARM-based developer boards and discuss code size, security, and performance of our proposed integrity verification mechanism.

Weiß et al.: On Cache Timing Attacks Considering Multi-Core Aspects in Virtualized Embedded Systems **Weiss2014b**

Michael Weiß, Benjamin Weggenmann, Moritz August, and Georg Sigl. "On Cache Timing Attacks Considering Multi-Core Aspects in Virtualized Embedded Systems". In: *The 6th International Conference on Trustworthy Systems (InTrust 2014)*. Beijing, China, 2014. url: http://crypto.fudan.edu.cn/intrust2014/.

Abstract: Virtualization has become one of the most important security enhancing techniques for embedded systems during the last years, both for mobile devices and cyber-physical system (CPS). One of the major security threats in this context is posed by side channel attacks. In this work, Bernstein's time-driven cache-based attack against AES is revisited in a virtualization scenario based on an actual CPS using the PikeOS microkernel virtualization framework. The attack is conducted in the context of the implemented virtualization scenario using different scheduler configurations. We provide experimental results which show that using dedicated cores for crypto routines will have a high impact on the vulnerability of such systems. We also compare the results to previous work in that field and our visualization directly shows the differences between cache architectures of the ARM Cortex-A8 and Cortex-A9. Further, a non-invasive countermeasure against timing attacks based on the scheduler of PikeOS is devised, which in fact increases the system's security against cache timing attacks.

Xiao et al.: Support Vector Machines under Adversarial Label Contamination **huang_eckert2014**

Huang Xiao, Battista Biggio, Blaine Nelson, Han Xiao, Claudia Eckert, and Fabio Roli. "Support Vector Machines under Adversarial Label Contamination". In: *Journal of Neurocomputing, Special Issue on Advances in Learning with Label Noise* (Aug. 2014). In press. url: https://www.sec.in.tum.de/assets/Uploads/main-revision.pdf.

Android Malware Recognition: Rafael Fedler and Marcel Kulicke and Julian Schütte **Fedler2013a**

An Antivirus API for Android Malware Recognition. "Rafael Fedler and Marcel Kulicke and Julian Schütte". In: *Proceedings of the 8th International Conference on Malicious and Unwanted Software (MALWARE), Puerto Rico, 2013*. 2013.

Angermeier et al.: PAL-privacy augmented LTE: A privacy-preserving scheme for vehicular LTE communication **angermeier2013pal**

Daniel Angermeier, Alexander Kiening, and Frederic Stumpf. "PAL-privacy augmented LTE: A privacy-preserving scheme for vehicular LTE communication". In: *Proceeding of the tenth ACM international workshop on Vehicular inter-networking, systems, and applications*. ACM. 2013, pp. 1–10.

Dhungana et al.: Identity management framework for cloud networking infrastructure **Dhungana2013e**

R.D. Dhungana, A. Mohammad, S. Rangarajan, A. Sharma, and I. Schoen. "Identity management framework for cloud networking infrastructure". In: cited By 3. 2013, pp. 13–17. doi: 10.1109/Innovations.2013.6544386. url: http://www.scopus.com/inward/record.url?eid=2-s2.0-84881096342&partnerID=40&md5=1ba77534e721c98febf4a7364213c

Eichler: Voll ausgereift – Sichere Software mit OpenSAMM, BSIMM und SSE-CMM **eichler2013voll**

Jörn Eichler. "Voll ausgereift – Sichere Software mit OpenSAMM, BSIMM und SSE-CMM". In: *iX* 11 (2013), pp. 112–118.

Abstract: Dass Software sensible Daten sicher verarbeiten sollte, dürfte Konsens sein. Doch das Messen und Vergleichen der relevanten Parameter ist keineswegs einfach. Reifegradmodelle sollen dabei helfen, Sicherheitslücken im Entwicklungsprozess zu schließen.

Fallenbeck et al.: Sicheres Cloud Computing **Fallenbeck2013**

Niels Fallenbeck and Iryna Windhorst. "Sicheres Cloud Computing". In: *Computerwoche* (2013).

Fedler et al.: Native Code Execution Control for Attack Mitigation on Android **Fedler2013**

Rafael Fedler, Marcel Kulicke, and Julian Schütte. "Native Code Execution Control for Attack Mitigation on Android". In: *Proceedings of the 3rd Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), Berlin, 2013*. 2013.

Abstract: On the Android platform, antivirus software suffers from significant deficiencies. Due to platform limitations, it cannot access or monitor an Android device's file system, or dynamic behavior of installed apps. This includes the downloading of malicious files after installation, and other file system alterations. That has grave consequences for device security, as any app – even without openly malicious code in its package file – can still download and execute malicious files without any danger of being detected by antivirus software. In this paper, we present a proposal for an antivirus interface to be added to the Android API. It allows for three primary operations: (1) on-demand file system scanning and traversal, (2) on-change file system monitoring, (3) a set of basic operations that allow for scanning of arbitrary file system objects without disclosing their contents. This interface can enable Android antivirus software to deploy techniques for malware recognition similar to those of desktop antivirus systems. The proposed measures comply with Android's security architecture and user data privacy is maintained. Through our approach, antivirus software on the Android platform would reach a level of effectiveness significantly higher than currently, and comparable to that of desktop antivirus software.

Fedler et al.: On the Effectiveness of Malware Protection on Android. An Evaluation of Android Antivirus Apps **techreport2013**

Rafael Fedler, Marcel Kulicke, and Julian Schütte. *On the Effectiveness of Malware Protection on Android. An Evaluation of Android Antivirus Apps*. Fraunhofer AISEC TechReport. 2013.

Filipovic et al.: Leitfaden "Produkt- und Know-how-Schutz" **filipovic2013leitfaden**

Bartol Filipovic, Rolf Simons, Alexandra Schulz, Benno Scholze, Harald Liese, Thomas Meiwald, Peter Mnich, and Oliver Winzenried. *Leitfaden "Produkt- und Know-how-Schutz"*. VDMA. 2013.

Haustein et al.: Collaboratively Exchanging Warning Messages between Peers While under Attack **DBLP:conf/IEEEares/HausteinSTS13**

Mirko Haustein, Herbert Sighart, Dennis Titze, and Peter Schoo. "Collaboratively Exchanging Warning Messages between Peers While under Attack". In: *ARES*. IEEE Computer Society, 2013, pp. 726–731.

Henning et al.: Manipulationssensible Kopierschutzfolie **hennig2013manipulationssensible**

Maxim Henning, Oliver Schimmel, Philipp Zieris, and Georg Sigl. "Manipulationssensible Kopierschutzfolie". In: *D-A-CH security 2013 : Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven*. Ed. by P. Schartner. 2013, pp. 344–355.

Herrmann et al.: Behavior-based tracking: Exploiting characteristic patterns in DNS traffic **HerrmannBF13**

Dominik Herrmann, Christian Banse, and Hannes Federrath. "Behavior-based tracking: Exploiting characteristic patterns in DNS traffic". In: *Computers & Security* 39 (2013), pp. 17–33. doi: 10.1016/j.cose.2013.03.012. url: http://dx.doi.org/10.1016/j.cose.2013.03.012.

Abstract: We review and evaluate three techniques that allow a passive adversary to track users who have dynamic IP addresses based on characteristic behavioral patterns, i.e., without cookies or similar techniques. For this purpose we consider 1-Nearest-Neighbor classifiers, a Multinomial Naïve Bayes classifier and pattern mining techniques based on the criteria support and lift. For evaluation we focus on the case of a curious DNS resolver. Therefore, we analyze the effectiveness of the techniques using a common, large-scale dataset that contains the DNS queries issued by more than 3600 users over the course of two months. We find that behavior-based tracking is feasible: The best technique can link up to 85.4% of the surfing sessions of all users on a day-to-day basis. Moreover, for tracking to be effective only the most significant features or the most popular hostnames have to be considered. Our results indicate that users can degrade accuracy by changing their IP addresses more frequently, e.g., every few minutes. On the other hand, we find that the previously proposed DNS "range query" obfuscation techniques cannot prevent tracking reliably. Our findings are not limited to DNS traffic. Behavior-based tracking can be implemented by any adversary that has access to the web requests issued by users or their machines.

Heyszl: Impact of Localized Electromagnetic Field Measurements on Implementations of Asymmetric Cryptography **Heyszl2013**

Johann Heyszl. "Impact of Localized Electromagnetic Field Measurements on Implementations of Asymmetric Cryptography". PhD thesis. Technische Universität München, 2013.

Heyszl et al.: Clustering Algorithms for Non-profiled Single-Execution Attacks on Exponentiations **DBLP:conf/cardis/HeyszlIMSS13**

Johann Heyszl, Andreas Ibing, Stefan Mangard, Fabrizio De Santis, and Georg Sigl. "Clustering Algorithms for Non-profiled Single-Execution Attacks on Exponentiations". In: *Smart Card Research and Advanced Applications - 12th International Conference, CARDIS 2013, Berlin, Germany, November 27-29, 2013. Revised Selected Papers*. 2013, pp. 79–93. doi: 10.1007/978-3-319-08302-5_6. url: http://dx.doi.org/10.1007/978-3-319-08302-5_6.

Hoffmann et al.: Introducing Life Management Platforms and Collaborative Service Fusion to Contextual Environments **Hoffmann2013d**

M. Hoffmann and P. Jäppinen. "Introducing Life Management Platforms and Collaborative Service Fusion to Contextual Environments". In: *Communications in Computer and Information Science* 182 CCIS (2013). cited By 0, pp. 41–52. doi: 10.1007/978-3-642-41205-9_4. url: http://www.scopus.com/inward/record.url?eid=2-s2.0-84904885644&partnerID=40&md5=228663e67571ca879a55950d59b803d3.

Hoffmann: An App Approach Towards User Empowerment in Personalized Service Environments **DBLP:conf/esocc/Hoffmann13**

Mario Hoffmann. "An App Approach Towards User Empowerment in Personalized Service Environments". In: *ESOCC*. Vol. 8135. Lecture Notes in Computer Science. Springer, 2013, pp. 149–163.

Khalid et al.: On implementing trusted boot for embedded systems **DBLP:conf/host/KhalidRI13**

Obaid Khalid, Carsten Rolfes, and Andreas Ibing. "On implementing trusted boot for embedded systems". In: *2013 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2013, Austin, TX, USA, June 2-3, 2013*. 2013, pp. 75–80. doi: 10.1109/HST.2013.6581569. url: http://dx.doi.org/10.1109/HST.2013.6581569.

Kiening et al.: Trust assurance levels of cybercars in v2x communication **kiening2013trust**

Alexander Kiening, Daniel Angermeier, Herve Seudie, Tyrone Stodart, and Marko Wolf. "Trust assurance levels of cybercars in v2x communication". In: *Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles*. ACM. 2013, pp. 49–60.

Kiening et al.: Verifiable Trust between Electronic Control Units based on a single Trust Anchor **kiening2013verifiable**

Alexander Kiening, Christoph Krauß, and Claudia Eckert. "Verifiable Trust between Electronic Control Units based on a single Trust Anchor". In: *11th escar* (2013).

Krauß et al.: Using Trusted Platform Modules for Location Assurance in Cloud Networking **krauss2013**

Christoph Krauß and Volker Fusenig. "Using Trusted Platform Modules for Location Assurance in Cloud Networking". In: *Proceedings of the 7th International Conference on Network and System Security (NSS 2013)*. Lecture Notes in Computer Science. Springer, June 2013.

Mark Gall et al.: An Architecture for Community Clouds Using Concepts from the Intercloud **Gall2013**

Angelika Schneider Mark Gall and Niels Fallenbeck. "An Architecture for Community Clouds Using Concepts from the Intercloud". In: *Proc. the 27th IEEE International Conf. Advanced Information Networking and Applications (AINA)*. 2013.

Merli et al.: Localized electromagnetic analysis of RO PUFs
DBLP:conf/host/MerliHHSSS13

Dominik Merli, Johann Heyszl, Benedikt Heinz, Dieter Schuster, Frederic Stumpf, and Georg Sigl. "Localized electromagnetic analysis of RO PUFs". In: *2013 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2013, Austin, TX, USA, June 2-3, 2013*. 2013, pp. 19–24. doi: 10.1109/HST.2013.6581559. url: http://dx.doi.org/10.1109/HST.2013.6581559.

Merli et al.: Identities for Embedded Systems Enabled by Physical Unclonable Functions
Merli13Identities

Dominik Merli, Georg Sigl, and Claudia Eckert. "Identities for Embedded Systems Enabled by Physical Unclonable Functions". In: *Number Theory and Cryptography - Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday*. 2013, pp. 125–138. doi: 10.1007/978-3-642-42001-6_10. url: http://dx.doi.org/10.1007/978-3-642-42001-6_10.

Merli et al.: Protecting PUF Error Correction by Codeword Masking **Merli2013Protecting**

Dominik Merli, Frederic Stumpf, and Georg Sigl. *Protecting PUF Error Correction by Codeword Masking*. Cryptology ePrint Archive, Report 2013/334. http://eprint.iacr.org/. 2013.

Rottondi et al.: A Decisional Attack to Privace-friendly Data Aggregation in Smart Grids
krauss2013a

C. Rottondi, D. Marco Savi, G. Polenghi, and C Krauss. "A Decisional Attack to Privace-friendly Data Aggregation in Smart Grids". In: *IEEE Globecon 2013 - Symposium on Selected Areas in Communications (GC13)*. IEEE, 2013.

Rottondi et al.: Distributed Privacy-Preserving Aggregation of Metering Data in Smart Grids **rottondi2013a**

Cristina Rottondi, Giacomo Verticale, and Christoph Krauß. "Distributed Privacy-Preserving Aggregation of Metering Data in Smart Grids". In: *IEEE Journal on Selected Areas in Communication (JSAC) - JSAC Smart Grid Communications Series* (2013).

Rottondi et al.: Secure Distributed Data Aggregation in the Automatic Metering Infrastructure of Smart Grids **rottondi2013**

Cristina Rottondi, Giacomo Verticale, and Christoph Krauß. "Secure Distributed Data Aggregation in the Automatic Metering Infrastructure of Smart Grids". In: *IEEE International Conference on Communications (ICC) - Selected Areas in Communications Symposium (ICC SAC)*. IEEE, June 2013.

Schoo et al.: Threat model based security evaluation of open connectivity services
Schoo2013e

P. Schoo and R. Marx. "Threat model based security evaluation of open connectivity services". In: *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications*

Engineering, LNICST 58 (2013). cited By 0, pp. 313–322. doi: 10.1007/978-3-642-37935-2_24. url: http://www.scopus.com/inward/record.url?eid=2-s2.0-84883129450&partnerID=40&md5=085a2bc8a7c5bdc78dfd75693483f384.

Schütte et al.: Blick unter die Haube – Werkzeuge und Verfahren zur Sicherheitsanalyse von Android-Apps **Schuette2013a**

Julian Schütte and Dennis Titze. "Blick unter die Haube – Werkzeuge und Verfahren zur Sicherheitsanalyse von Android-Apps". In: *iX* (11/2013 2013).

Stumpf et al.: When the lights go out - Attacks and security solutions for smart metering **stumpf2013when**

Frederic Stumpf and Konstantin Böttinger. "When the lights go out - Attacks and security solutions for smart metering". In: *23. SmartCard Workshop 2013. Tagungsband : Darmstadt, 6./7. Februar 2013*. Fraunhofer Verlag, 2013, 2013, pp. 158–169. isbn: 978-3-8396-0500-4.

Theißing et al.: Comprehensive analysis of software countermeasures against fault attacks **DBLP:conf/date/TheissingMSSS13**

Nikolaus Theißing, Dominik Merli, Michael Smola, Frederic Stumpf, and Georg Sigl. "Comprehensive analysis of software countermeasures against fault attacks". In: *Design, Automation and Test in Europe, DATE 13, Grenoble, France, March 18-22, 2013*. 2013, pp. 404–409. url: http://dl.acm.org/citation.cfm?id=2485386.

Titze et al.: A Configurable and Extensible Security Service Architecture for Smartphones **Titze2013**

Dennis Titze, Philipp Stephanow, and Julian Schütte. "A Configurable and Extensible Security Service Architecture for Smartphones". In: *Proceedings of the Seventh International Symposium on Frontiers in Networking with Applications (FINA 2013)*. 2013.

Velten et al.: Secure and Privacy-Aware Multiplexing of Hardware-Protected TPM Integrity Measurements among Virtual Machines **Velten:2012**

Michael Velten and Frederic Stumpf. "Secure and Privacy-Aware Multiplexing of Hardware-Protected TPM Integrity Measurements among Virtual Machines". In: *Information Security and Cryptology – ICISC 2012*. Ed. by Taekyoung Kwon, Mun-Kyu Lee, and Daesung Kwon. Vol. 7839. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2013, pp. 324–336. isbn: 978-3-642-37681-8. doi: 10.1007/978-3-642-37682-5_23. url: http://dx.doi.org/10.1007/978-3-642-37682-5_23.

Abstract: Measuring the integrity of critical operating system components and securely storing these measurements in a hardware-protected Trusted Platform Module (TPM) is a well-known approach for improving system security. However, currently it is not possible to securely extend this approach to TPMs used in virtualized environments. In this paper, we show how to multiplex integrity measurements of arbitrarily many Virtual Machines (VMs) with just a single standard TPM. In contrast to existing approaches such as vTPM, our approach achieves a higher level of security since measure-

ments will never be held in software but are fully hardware-protected by the TPM at all times. We establish an integrity-protected mapping between each measurement and its respective VM such that it is not possible for an attacker to alter this mapping during remote attestation without being detected. Furthermore, all measurements will be stored in the TPM in a concealed manner in order to prevent information leakage of other VMs during remote attestation. The experimental results of our proof of concept implementation show the feasibility of our approach.

Velten et al.: Active File Integrity Monitoring Using Paravirtualized Filesystems **Velten:2013**

Michael Velten, Sascha Wessel, Frederic Stumpf, and Claudia Eckert. "Active File Integrity Monitoring Using Paravirtualized Filesystems". In: *Trusted Systems*. Ed. by Roderick Bloem and Peter Lipp. Vol. 8292. Lecture Notes in Computer Science. Springer International Publishing, 2013, pp. 53–69. isbn: 978-3-319-03490-4. doi: 10.1007/978-3-319-03491-1_4.

Abstract: Monitoring file integrity and preventing illegal modifications is a crucial part of improving system security. Unfortunately, current research focusing on isolating monitoring components from supervised systems can often still be thwarted by tampering with the hooks placed inside of Virtual Machines (VMs), thus resulting in critical file operations not being noticed. In this paper, we present an approach of relocating a supervised VM's entire filesystem into the isolated realm of the host. This way, we can enforce that all file operations originating from a VM (e.g., read and write operations) must necessarily be routed through the hypervisor, and thus can be tracked and even be prevented. Disabling hooks in the VM then becomes pointless as this would render a VM incapable of accessing or manipulating its own filesystem. This guarantees secure and complete active file integrity monitoring of VMs. The experimental results of our prototype implementation show the feasibility of our approach.

Wagner et al.: Lightweight Attestation & Secure Code Update for Multiple Separated Microkernel Tasks **Wagner:2013**

Steffen Wagner, Christoph Krauss, and Claudia Eckert. "Lightweight Attestation & Secure Code Update for Multiple Separated Microkernel Tasks". In: *Proceedings of the ISC 2013: The 16th Information Security Conference*. LNCS. Dallas, Texas, USA: Springer, Nov. 2013.

Abstract: By implementing all non-essential operating system services as user space tasks and strictly separating those tasks, a microkernel can effectively increase system security. However, the isolation of tasks does not necessarily imply their trustworthiness. In this paper, we propose a microkernel-based system architecture enhanced with a multi-context hardware security module (HSM) that enables an integrity verification, anomaly detection, and efficient lightweight attestation of multiple separated tasks. Our attestation protocol, which we formally verified using the automated reasoning tool ProVerif, implicitly proves the integrity of multiple tasks, efficiently communicates the result to a remote verifier, and enables a secure update protocol without the need for digital signatures that require computationally expensive operations.

Wessel et al.: Improving Mobile Device Security with Operating System-Level Virtualization **Wessel:2013**

Sascha Wessel, Frederic Stumpf, Ilja Herdt, and Claudia Eckert. "Improving Mobile Device Secu-

rity with Operating System-Level Virtualization". In: *Security and Privacy Protection in Information Processing Systems*. Ed. by Lech J. Janczewski, Henry B. Wolfe, and Sujeet Shenoi. Vol. 405. IFIP Advances in Information and Communication Technology. Springer Berlin Heidelberg, 2013, pp. 148–161. isbn: 978-3-642-39217-7. doi: 10.1007/978-3-642-39218-4_12.

Abstract: In this paper, we propose a lightweight mechanism to isolate one or more Android userland instances from a trustworthy and secure entity. This entity controls and manages the Android instances and provides an interface for remote administration and management of the device and its software. Our approach includes several security extensions for secure network access, integrity protection of data on storage devices, and secure access to the touchscreen. Our implementation requires only minimal modification to the software stack of a typical Android-based smartphone, which allows easy porting to other devices when compared to other virtualization techniques. Practical tests show the feasibility of our approach regarding runtime overhead and battery lifetime impact.

Windhorst et al.: Dynamic Certification of Cloud Services **DBLP:conf/IEEEares/WindhorstS13**

Iryna Windhorst and Ali Sunyaev. "Dynamic Certification of Cloud Services". In: *ARES*. IEEE Computer Society, 2013, pp. 412–417.

Angermeier et al.: A Secure Architecture for Smart Meter Systems **angermeier2012secure**

Daniel Angermeier, Konstantin Böttinger, Andreas Ibing, Dieter Schuster, Frederic Stumpf, and Dirk Wacker. "A Secure Architecture for Smart Meter Systems". English. In: *Cyberspace Safety and Security*. Ed. by Yang Xiang, Javier Lopez, C.-C.Jay Kuo, and Wanlei Zhou. Vol. 7672. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2012, pp. 108–122. isbn: 978-3-642-35361-1. doi: 10.1007/978-3-642-35362-8_10. url: http://dx.doi.org/10.1007/978-3-642-35362-8_10.

Banse et al.: Tracking Users on the Internet with Behavioral Patterns: Evaluation of Its Practical Feasibility **BanseHF12**

Christian Banse, Dominik Herrmann, and Hannes Federrath. "Tracking Users on the Internet with Behavioral Patterns: Evaluation of Its Practical Feasibility". In: *Information Security and Privacy Research - 27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012, Heraklion, Crete, Greece, June 4-6, 2012. Proceedings*. 2012, pp. 235–248. doi: 10.1007/978-3-642-30436-1_20. url: http://dx.doi.org/10.1007/978-3-642-30436-1_20.

Abstract: Traditionally, service providers, who want to track the activities of Internet users, rely on explicit tracking techniques like HTTP cookies. From a privacy perspective behavior-based tracking is even more dangerous, because it allows service providers to track users passively, i. e., without cookies. In this case multiple sessions of a user are linked by exploiting characteristic patterns mined from network traffic. In this paper we study the feasibility of behavior-based tracking in a real-world setting, which is unknown so far. In principle, behavior-based tracking can be carried out by any attacker that can observe the activities of users on the Internet. We design and implement a behavior-based tracking technique that consists of a Naive Bayes classifier supported by a cosine similarity decision engine. We evaluate our technique using a large-scale dataset that contains all

queries received by a DNS resolver that is used by more than 2100 concurrent users on average per day. Our technique is able to correctly link 88.2 % of the surfing sessions on a day-to-day basis. We also discuss various countermeasures that reduce the effectiveness of our technique.

Borran et al.: Quantitative Analysis of Consensus Algorithms **borran2012quantitative**

Fatemeh Borran, Martin Hutle, Nuno Santos, and André Schiper. "Quantitative Analysis of Consensus Algorithms". In: *IEEE Trans. Dependable Sec. Comput.* 9.2 (2012), pp. 236–249. doi: 10.1109/TDSC.2011.48. url: http://doi.ieeecomputersociety.org/10.1109/TDSC.2011.48.

Borran et al.: Timing analysis of leader-based and decentralized Byzantine consensus algorithms **borran2012timing**

Fatemeh Borran, Martin Hutle, and André Schiper. "Timing analysis of leader-based and decentralized Byzantine consensus algorithms". In: *J. Braz. Comp. Soc.* 18.1 (2012), pp. 29–42. doi: 10.1007/s13173-012-0058-6. url: http://dx.doi.org/10.1007/s13173-012-0058-6.

Bouard et al.: Driving automotive middleware towards a secure ip-based future **bouard2012driving**

Alexandre Bouard, Benjamin Glas, Anke Jentzsch, Alexander Kiening, Thomas Kittel, and B Weyl. "Driving automotive middleware towards a secure ip-based future". In: *10th escar* (2012).

Brunner et al.: AWESOME - Automated web emulation for secure operation of a malware-analysis environment **Brunner2012c**

M. Brunner, C.M. Fuchs, and S. Todt. "AWESOME - Automated web emulation for secure operation of a malware-analysis environment". In: cited By 0. 2012, pp. 68–71. url: http://www.scopus.com/inward/record.url?eid=2-s2.0-84881398063&partnerID=40&md5=4001ff875853bb58d5924be3c5aa2c15.

Brunner et al.: AWESOME - Automated Web Emulation for Secure Operation of a Malware-Analysis Environment **bft2012**

Martin Brunner, Christian M. Fuchs, and Sascha Todt. "AWESOME - Automated Web Emulation for Secure Operation of a Malware-Analysis Environment". In: *Proceedings of the Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2012)*. ISBN: 978-1-61208-209-7. Best Paper Award. International Academy, Research, and Industry Association (IARIA). Rome, Italy: XPS, Aug. 2012, pp. 68–71. url: http://www.thinkmind.org/index.php?view=article&articleid=securware_2012_3_20_30016.

Dehning et al.: Sichere Nutzung von Cloud-Anwendungen am Beispiel des TeleTrusT Bundesverband IT-Sicherheit e.V. als Praxisleitfaden für Verbände und KMU. **Dehning2012**

Oliver Dehning, Karsten U. Bartels, Axel Borchers, Michael Gröne, Thorsten Humberg, Dr. Holger Mühlbauer, Christian Senk, Dr. Thomas Störtkuhl, and Iryna Tsvihun. *Sichere Nutzung von Cloud-*

Anwendungen am Beispiel des TeleTrusT Bundesverband IT-Sicherheit e.V. als Praxisleitfaden für Verbände und KMU. Herausgeber: TeleTrusT – Bundesverband IT-Sicherheit e.V. 2012.

Eckert et al.: Sicherheit im Smart Grid - Sicherheitsarchitekturen für die Domänen Privatkunde und Verteilnetz unter Berücksichtigung der Elektromobilität **eckert2012**

Claudia Eckert and Christoph Krauß. *Sicherheit im Smart Grid - Sicherheitsarchitekturen für die Domänen Privatkunde und Verteilnetz unter Berücksichtigung der Elektromobilität*. Alcatel-Lucent Stiftung, Stiftungsreihe 96. 2012. url: http://www.stiftungaktuell.de/files/sr96_sicherheit_im_smart_grid.pdf.

Filipovic: Maschine mit Kopierschutz **filipovic2012maschine**

Bartol Filipovic. "Maschine mit Kopierschutz". In: *Forschung Kompakt* 12 (2012), pp. 15–17.

Filipovic: Schutz durch Firmware-Verschlüsselung **filipovic2012schutz**

Bartol Filipovic. "Schutz durch Firmware-Verschlüsselung". In: *VDMA-Nachrichten (Zeitschrift)* 3 (Mar. 2012), pp. 26–27.

Fusenig et al.: Security architecture for cloud networking **Fusenig20124c**

V. Fusenig and A. Sharma. "Security architecture for cloud networking". In: cited By 2. 2012, pp. 45–49. doi: 10.1109/ICCNC.2012.6167464. url: http://www.scopus.com/inward/record.url?eid=2-s2.0-84859920491&partnerID=40&md5=76b10f4dce317007b8e035bd93f6546e.

Heyszl et al.: Localized Electromagnetic Analysis of Cryptographic Implementations **DBLP:conf/ctrsa/HeyszlMHSS12**

Johann Heyszl, Stefan Mangard, Benedikt Heinz, Frederic Stumpf, and Georg Sigl. "Localized Electromagnetic Analysis of Cryptographic Implementations". In: *Topics in Cryptology - CT-RSA 2012 - The Cryptographers' Track at the RSA Conference 2012, San Francisco, CA, USA, February 27 - March 2, 2012. Proceedings*. 2012, pp. 231–244. doi: 10.1007/978-3-642-27954-6_15. url: http://dx.doi.org/10.1007/978-3-642-27954-6_15.

Heyszl et al.: Strengths and Limitations of High-Resolution Electromagnetic Field Measurements for Side-Channel Analysis **DBLP:conf/cardis/HeyszlMHSS12**

Johann Heyszl, Dominik Merli, Benedikt Heinz, Fabrizio De Santis, and Georg Sigl. "Strengths and Limitations of High-Resolution Electromagnetic Field Measurements for Side-Channel Analysis". In: *Smart Card Research and Advanced Applications - 11th International Conference, CARDIS 2012, Graz, Austria, November 28-30, 2012, Revised Selected Papers*. 2012, pp. 248–262. doi: 10.1007/978-3-642-37288-9_17. url: http://dx.doi.org/10.1007/978-3-642-37288-9_17.

Heyszl et al.: Vorrichtung und Verfahren zur effizienten einseitigen Authentifizierung **Heyszl2011a**

Johann Heyszl and Frederic Stumpf. "Vorrichtung und Verfahren zur effizienten einseitigen Authentifizierung". Pat. DE102010002241. 2012.

Hiller et al.: Reliability bound and channel capacity of IBS-based fuzzy embedders **Hiller2012Adaptive**

M. Hiller, F. De Santis, D. Merli, and G. Sigl. "Reliability bound and channel capacity of IBS-based fuzzy embedders". In: *Adaptive Hardware and Systems (AHS), 2012 NASA/ESA Conference on*. 2012, pp. 213–220. doi: 10.1109/AHS.2012.6268652.

Hiller et al.: Complementary IBS: Application specific error correction for PUFs **DBLP:conf/host/HillerMSS12**

Matthias Hiller, Dominik Merli, Frederic Stumpf, and Georg Sigl. "Complementary IBS: Application specific error correction for PUFs". In: *2012 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2012, San Francisco, CA, USA, June 3-4, 2012*. 2012, pp. 1–6. doi: 10.1109/HST.2012.6224310. url: http://dx.doi.org/10.1109/HST.2012.6224310.

Hoffmann et al.: Context-based distribution of points of interest **Hoffmann20123f**

M. Hoffmann, A. Mohammad, and S. Khan. "Context-based distribution of points of interest". In: cited By 0. 2012, pp. 37–39. doi: 10.1145/2348676.2348686. url: http://www.scopus.com/inward/record.url?eid=2-s2.0-84866660172&partnerID=40&md5=379f13df1f84b6631dad8ee90e05d1ca.

Hofinger et al.: When browsing leaves footprints: automatically detect privacy violations **hofinger2012browsing**

Hans Hofinger, Alexander Kiening, and Peter Schoo. "When browsing leaves footprints: automatically detect privacy violations". In: *Proceedings of the First Workshop on Measurement, Privacy, and Mobility*. ACM. 2012, p. 9.

Kannan et al.: Genetic algorithm based feature selection algorithm for effective intrusion detection in cloud networks **Kannan2012e**

A. Kannan, G.Q. Maguire Jr., A. Sharma, and P. Schoo. "Genetic algorithm based feature selection algorithm for effective intrusion detection in cloud networks". In: cited By 6. 2012, pp. 416–423. doi: 10.1109/ICDMW.2012.56. url: http://www.scopus.com/inward/record.url?eid=2-s2.0-84873161461&partnerID=40&md5=c07ed0f11b4a3b5118b1fd8e6c73a

Kannan et al.: N-ary tree based key distribution in a network as a service provisioning model **Kannan2012c**

A. Kannan, Q.G. Maguire Jr., A. Sharma, V. Fusenig, and P. Schoo. "N-ary tree based key distribution in a network as a service provisioning model". In: cited By 0. 2012, pp. 952–960. doi: 10.1145/

2345396.2345550. url: http://www.scopus.com/inward/record.url?eid=2-s2.0-84866115096&partnerID=40&md5=e890443ce20192f8c5ebbbf9a74400f3.

Merli et al.: Physical Unclonable Functions - CMOS-Implementierungen und Hardware-Attacken **Merli2012Physical**

Dominik Merli and Georg Sigl. "Physical Unclonable Functions - CMOS-Implementierungen und Hardware-Attacken". In: *Physical Unclonable Functions - CMOS-Implementierungen und Hardware-Attacken* Datenschutz und Datensicherheit (2012), pp. 876 –880. doi: 10.1007/s11623-012-0294-0.

Milosevic et al.: Brief announcement: tolerating permanent and transient value faults **milosevic2012ba**

Zarko Milosevic, Martin Hutle, and André Schiper. "Brief announcement: tolerating permanent and transient value faults". In: *ACM Symposium on Principles of Distributed Computing, PODC '12, Funchal, Madeira, Portugal, July 16-18, 2012*. 2012, pp. 333–334. doi: 10.1145/2332432.2332496. url: http://doi.acm.org/10.1145/2332432.2332496.

Murray et al.: Cloud networking: An infrastructure service architecture for the wide area **Murray2012**

P. Murray, A. Sefidcon, R. Steinert, V. Fusenig, and J. Carapinha. "Cloud networking: An infrastructure service architecture for the wide area". In: *HP Laboratories Technical Report* 111 (2012). cited By 0. url: http://www.scopus.com/inward/record.url?eid=2-s2.0-84861642437&partnerID=40&md5=3ea4d226a88998947b9d07536b95df1f.

Rangarajan et al.: V2C: A secure vehicle to cloud framework for virtualized and on-demand service provisioning **Rangarajan2012c**

S. Rangarajan, M. Verma, A. Kannan, A. Sharma, and I. Schoen. "V2C: A secure vehicle to cloud framework for virtualized and on-demand service provisioning". In: cited By 0. 2012, pp. 148–154. doi: 10.1145/2345396.2345422. url: http://www.scopus.com/inward/record.url?eid=2-s2.0-84866126705&partnerID=40&md5=f3ccc81b11c7847ace62e3

Rieke et al.: Architecting an Security Strategy Measurement and Management System **Rieke2012**

Roland Rieke, Julian Schütte, and Andrew Hutchison. "Architecting an Security Strategy Measurement and Management System". In: *Proceedings of the Model Driven Security Workshop (MDSec) at the ACM/IEEE 15th International Conference on Model Driven Engineering Languages & Systems (MODELS)*. 2012.

Rottondi et al.: Implementation of a Protocol for Secure Distributed Aggregation of Smart Metering Data **rottondi2012**

Cristina Rottondi, Giacomo Verticale, and Christoph Krauß. "Implementation of a Protocol for Secure Distributed Aggregation of Smart Metering Data". In: *International Conference on Smart Grid Technology, Economics and Policies (SG-TEP 2012)*. IEEE, Nov. 2012.

Schoo et al.: Collaboration between Competing Mobile Network Operators to Improve CIIP **Schoo:2012**

Peter Schoo, Manfred Schäfer, André Egners, Hans Hofinger, Sascha Wessel, Marian Kuehnel, Sascha Todt, and Michael Montag. "Collaboration between Competing Mobile Network Operators to Improve CIIP". In: *Critical Information Infrastructures Security*. Ed. by Bernhard M. Hämmerli, Nils Kalstad Svendsen, and Javier Lopez. Vol. 7722. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2012, pp. 215–227. isbn: 978-3-642-41484-8. doi: 10.1007/978-3-642-41485-5_19.

Abstract: Mobile Network Operators (MNOs) deploy a vital part of today's Critical Information Infrastructures (CII). Protection of these CIIs shall ensure operational continuity despite of the potential loss of system integrity and malware attacks. Sharing information about security related incidents allows MNOs to better react to attacks and anomalies, and to mitigate the impact of the observed phenomena. The fear to risk its reputation may hinder an MNO to share information that could help other MNOs to improve their protection and assure operational continuity. The contributions of this paper are technical solutions for collaboration between competing MNOs, which prevent loss of reputation and thus improve the acceptance to share information.

Schütte: Goal-based Policies for Self-Protecting Systems **Schuette2012**

Julian Schütte. "Goal-based Policies for Self-Protecting Systems". In: *Proc. the 26th IEEE International Conf. Advanced Information Networking and Applications (AINA)*. Fukuoka, Japan: IEEE Computer Society Press, Mar. 2012.

Schütte et al.: Security Policies in Dynamic Service Compositions **Schuette2012b**

Julian Schütte, Mark Gall, and Hervais Simo Fhom. "Security Policies in Dynamic Service Compositions". In: *Proceedings of the International Conference on Security and Cryptography (SECRYPT 2012), Rome*. 2012.

Schütte et al.: Model-based Security Event Management **Schuette2012a**

Julian Schütte, Roland Rieke, and Timo Winkelvos. "Model-based Security Event Management". In: *Proceedings of the Sixth International Conference Mathematical Methods, Models, and Architectures for Computer Network Security (MMM-ACNS-2012), St. Petersburg*. 2012.

Segura: tapndrop. Secure information sharing in the cloud. **Segura2012**

Xavier Segura. "tapndrop. Secure information sharing in the cloud." In: Droidcon Berlin. 2012. url: https://prezi.com/iigifztlkaon/tapndrop-secure-information-sharing-in-the-cloud/.

Sharma et al.: Bridging the security drawbacks of virtualized network resource provisioning model **Sharma2012d**

A. Sharma, V. Fusenig, I. Schoen, and A. Kannan. "Bridging the security drawbacks of virtualized network resource provisioning model". In: cited By 0. 2012. doi: 10.1145/2365316.2365318. url: http://www.scopus.com/inward/record.url?eid=2-s2.0-84867505253&partnerID=40&md5=c9737f60f033c2265a4c154e7c468bc8.

Stephanow et al.: Secure cloud based file exchange through Near Field Communication (NFC) enabled endpoints **Stephanow2012**

Philipp Stephanow, Xavier Segura, and Julian Schütte. *Secure cloud based file exchange through Near Field Communication (NFC) enabled endpoints*. Tech. rep. Fraunhofer AISEC, 2012. url: http://www.cloud-competence-center.com/wp-content/uploads/2012/05/tapndrop.pdf.

Tsvihun et al.: Cloud-Leitstand: Die Schaltzentrale für die Cloud **Tsvihun2012**

Iryna Tsvihun and Niels Fallenbeck. "Cloud-Leitstand: Die Schaltzentrale für die Cloud". In: *ISIS Cloud & SaaS Report* 1 (2012).

Wagner et al.: T-CUP: A TPM-Based Code Update Protocol Enabling Attestations for Sensor Networks **Wagner:2012a**

Steffen Wagner, Christoph Krauß, and Claudia Eckert. "T-CUP: A TPM-Based Code Update Protocol Enabling Attestations for Sensor Networks". English. In: *Security and Privacy in Communication Networks*. Ed. by Muttukrishnan Rajarajan, Fred Piper, Haining Wang, and George Kesidis. Vol. 96. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer Berlin Heidelberg, 2012, pp. 511–521. isbn: 978-3-642-31908-2. doi: 10.1007/978-3-642-31909-9_32. url: http://dx.doi.org/10.1007/978-3-642-31909-9_32.

Abstract: In this paper, we propose a secure code update protocol for TPM-equipped sensor nodes, which enables these nodes to prove their trustworthiness to other nodes using efficient attestation protocols. As main contribution, the protocol provides mechanisms to maintain the ability of performing efficient attestation protocols after a code update, although these protocols assume a trusted system state which never changes. We also present a proof of concept implementation on IRIS sensor nodes, which we have equipped with Atmel TPMs, and discuss the security of our protocol.

Wagner et al.: Attestation of Mobile Baseband Stacks **Wagner:2012b**

Steffen Wagner, Sascha Wessel, and Frederic Stumpf. "Attestation of Mobile Baseband Stacks". In: *Network and System Security*. Ed. by Li Xu, Elisa Bertino, and Yi Mu. Vol. 7645. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2012, pp. 29–43. isbn: 978-3-642-34600-2. doi: 10.1007/978-3-642-34601-9_3.

Abstract: Distributed denial of service (DDoS) attacks from a large number of compromised mobile devices are a major threat to mobile networks. In this paper, we present a concept, an architecture,

and a protocol for a hardware-based attestation which enables mobile devices to efficiently prove that their baseband stack is still trustworthy. Our attestation mechanism enables verification of the baseband stack without using expensive asymmetric cryptographic operations, maintains the ability to update (or recover) the baseband binary, and allows the network to enforce a certain version, state, or configuration of the baseband at network connect. Our approach represents an efficient method to block devices with a compromised baseband stack and thus prevents distributed denial of service attacks to mobile networks.

Weiß et al.: A Cache Timing Attack on AES in Virtualization Environments **Weiss:2012**

Michael Weiß, Benedikt Heinz, and Frederic Stumpf. "A Cache Timing Attack on AES in Virtualization Environments". English. In: *Financial Cryptography and Data Security*. Ed. by AngelosD. Keromytis. Vol. 7397. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2012, pp. 314–328. isbn: 978-3-642-32945-6. doi: 10.1007/978-3-642-32946-3_23. url: http://dx.doi.org/10.1007/978-3-642-32946-3_23.

Abstract: We show in this paper that the isolation characteristic of system virtualization can be bypassed by the use of a cache timing attack. Using Bernstein's correlation in this attack, an adversary is able to extract sensitive keying material from an isolated trusted execution domain. We demonstrate this cache timing attack on an embedded ARM-based platform running an L4 microkernel as virtualization layer. An attacker who gained access to the untrusted domain can extract the key of an AES-based authentication protocol used for a financial transaction. We provide measurements for different public domain AES implementations. Our results indicate that cache timing attacks are highly relevant in virtualization-based security architectures, such as trusted execution environments.

Wessel et al.: Page-Based Runtime Integrity Protection of User and Kernel Code **Wessel:2012**

Sascha Wessel and Frederic Stumpf. "Page-Based Runtime Integrity Protection of User and Kernel Code". In: *Proceedings of the Fifth European Workshop on Systems Security*. EuroSec 2012. Bern, Switzerland: ACM, 2012.

Abstract: In this contribution, we propose a mechanism to verify the integrity of user and kernel code at runtime. To this end, all executable content is verified before execution using a cryptographic hash function and a precomputed whitelist of hashes. The verification is enforced by restricting page access rights. In particular, virtualization techniques are used to ensure that all pages are either marked executable or writeable and that the page content is verified before execution. We show that even for an unmodified Linux-based operating system all executable content can be precomputed and therefore per-page hashes can be calculated to generate the whitelist for the verification. We implemented our concept to show that our approach is feasible.

Wieczorek et al.: Towards secure fieldbus communication **Wieczorek2012d**

F. Wieczorek, C. Krauß, F. Schiller, and C. Eckert. "Towards secure fieldbus communication". In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 7612 LNCS (2012). cited By 0, pp. 149–160. doi: 10.1007/978-3-

642-33678-2_13. url: http://www.scopus.com/inward/record.url?eid=2-s2.0-84867593322&partnerID=40&md5=b6472716366838ed01a6d37b66b00316.

Wieczorek et al.: Towards Secure Fieldbus Communication **wieczorek2012**

Felix Wieczorek, Christoph Krauß, Frank Schiller, and Claudia Eckert. "Towards Secure Fieldbus Communication". In: *31st International Conference on Computer Safety, Reliability and Security (SAFECOMP)*. Springer, Sept. 2012.

Windhorst: Cloud Migration **Windhorst2012a**

Iryna Windhorst. "Cloud Migration". In: ed. by Dr. Tobias Höllwarth. 2nd Edition. ISBN 978-3-8266-9177-5. mitp, 2012. Chap. The Risks of Cloud computing, pp. 79–85.

Windhorst: Der Weg in die Cloud **Windhorst2012**

Iryna Windhorst. "Der Weg in die Cloud". In: ed. by Dr. Tobias Höllwarth. 2. Auflage. mitp, 2012. Chap. Risiken beim Einsatz von Cloud-Computing, Maßnahmen zur Reduktion der Cloud-Sicherheitsrisiken, pp. 91–97.

Windhorst et al.: Managementsysteme für Informationssicherheit: Marktübersicht. Vorgehensmodell. Handlungsempfehlungen **Windhorst2012b**

Iryna Windhorst and Benedikt Pirzer. *Managementsysteme für Informationssicherheit: Marktübersicht. Vorgehensmodell. Handlungsempfehlungen*. Tech. rep. Fraunhofer AISEC, 2012. url: https://www.aisec.fraunhofer.de/content/dam/aisec/Dokumente/Publikationen/Studien_TechReports/deutsch/ISMS_Softwaresysteme_ISO27001.pdf.

Wüpper et al.: Informationssicherheitsmanagement – Praxisleitfaden für Manager **Wuepper2012**

Werner Wüpper, Christian Aust, Dr. Joachim Gerber, Daniel Hecker, Dr. Mathias Herrmann, Peter Herrmann, Dr. Holger Mühlbauer, Christian Schmitz, Harald Wacker, Hilde von Waldenfels, Jochen Wildner, Iryna Windhorst, and Ellen Wüpper. *Informationssicherheitsmanagement – Praxisleitfaden für Manager*. TeleTrusT – Bundesverband IT-Sicherheit e.V. 2012.

Wüpper et al.: Information Security Management – Best Practice Guidelines for Managers **Wuepper2012a**

Werner Wüpper and Iryna Windhorst. "Information Security Management – Best Practice Guidelines for Managers". In: *ISSE 2012 Securing Electronic Business Processes. Highlights of theInformation Security Solutions Europe 2012 Conference*. Ed. by Helmut Reimer, Norbert Pohlmann, and Wolfgang Schneider. 2012, pp. 21–36.

Attiya et al.: Structured Derivation of Semi-Synchronous Algorithms **attiya2011structured**

Hagit Attiya, Fatemeh Borran, Martin Hutle, Zarko Milosevic, and André Schiper. "Structured Derivation of Semi-Synchronous Algorithms". In: *Distributed Computing - 25th International Symposium,*

DISC 2011, Rome, Italy, September 20-22, 2011. Proceedings. 2011, pp. 374–388. doi: 10.1007/978-3-642-24100-0_37. url: http://dx.doi.org/10.1007/978-3-642-24100-0_37.

Baums et al.: Cloud Computing – Leitfaden für mittelständische Unternehmen **Baums2011**

Ansgar Baums, Hans-Dieter Becker, Alexander Raubold, Stefanie Schmitt, Iryna Tsvihun, Mark Vasic, and Andrea Wlcek. *Cloud Computing – Leitfaden für mittelständische Unternehmen*. Bundesministerium für Wirtschaft und und Technologie. Nov. 2011. url: http://www.bmwi.de/cloudcomputing/data/pdf/file.pdf.

Biely et al.: Consensus when all processes may be Byzantine for some time **biely2011consensus**

Martin Biely and Martin Hutle. "Consensus when all processes may be Byzantine for some time". In: *Theor. Comput. Sci.* 412.33 (2011), pp. 4260–4272. doi: 10.1016/j.tcs.2010.11.012. url: http://dx.doi.org/10.1016/j.tcs.2010.11.012.

Borran et al.: Timing Analysis of Leader-Based and Decentralized Byzantine Consensus Algorithms **borran2011timing**

Fatemeh Borran, Martin Hutle, and André Schiper. "Timing Analysis of Leader-Based and Decentralized Byzantine Consensus Algorithms". In: *5th Latin-American Symposium on Dependable Computing, LADC 2011, São José dos Campos, Brazil, 25-29 April 2011*. 2011, pp. 166–175. doi: 10.1109/LADC.2011.12. url: http://dx.doi.org/10.1109/LADC.2011.12.

Eckert et al.: Sicherheit im Smart Grid - Herausforderungen und Handlungsempfehlungen **eckert2011b**

Claudia Eckert and Christoph Krauß. "Sicherheit im Smart Grid - Herausforderungen und Handlungsempfehlungen". In: *Datenschutz und Datensicherheit* 8 (2011), pp. 535–541.

Eckert et al.: Sicherheit im Smart Grid - Eckpunkte für ein Energieinformationsnetz **eckert2011**

Claudia Eckert, Christoph Krauß, and Peter Schoo. *Sicherheit im Smart Grid - Eckpunkte für ein Energieinformationsnetz*. Stiftung-Verbundkolleg / Projekt Newise Nr. 90. 2011. url: http://www.stiftungaktuell.de/files/sr90_sicherheit_im_energieinformationsnetz_gesamt_1.pdf.

Filipovic: Protection against counterfeit products **filipovic2011protection**

Bartol Filipovic. "Protection against counterfeit products". In: *Researching: Security (Broschure)* (Sept. 2011), p. 17.

Filipovic: Schutz vor Produktfälschungen **filipovic2011schutz**

Bartol Filipovic. "Schutz vor Produktfälschungen". In: *Wir erforschen: Sicherheit (Broschüre)* (Sept. 2011), p. 17.

Filipovic et al.: Schutz eingebetteter Systeme vor Produktpiraterie – Technologischer Hintergrund und Vorbeugemaßnahmen **filipovic2011schutzeingebetter**

Bartol Filipovic and Oliver Schimmel. *Schutz eingebetteter Systeme vor Produktpiraterie – Technologischer Hintergrund und Vorbeugemaßnahmen*. Tech. rep. Fraunhofer AISEC, 2011.

Janning et al.: A Cost-Effective FPGA-based Fault Simulation Environment **DBLP:conf/fdtc/JanningHSS11**

Angelika Janning, Johann Heyszl, Frederic Stumpf, and Georg Sigl. "A Cost-Effective FPGA-based Fault Simulation Environment". In: *2011 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2011, Tokyo, Japan, September 29, 2011*. 2011, pp. 21–31. doi: 10.1109/FDTC.2011.19. url: http://dx.doi.org/10.1109/FDTC.2011.19.

Krauß et al.: Sicherheit im Smart Grid - Sicherheitsarchitekturen für die Domäne Privatkunde **krauss2011**

Christoph Krauß and Claudia Eckert. *Sicherheit im Smart Grid - Sicherheitsarchitekturen für die Domäne Privatkunde*. Alcatel-Lucent Stiftung, Stiftungsreihe 94, Gestaltungslinien für Sicherheit und Datenschutz im Energieinformationsnetz. 2011.

Merli et al.: Side-Channel Analysis of PUFs and Fuzzy Extractors **DBLP:conf/trust/MerliSSS11**

Dominik Merli, Dieter Schuster, Frederic Stumpf, and Georg Sigl. "Side-Channel Analysis of PUFs and Fuzzy Extractors". In: *Trust and Trustworthy Computing - 4th International Conference, TRUST 2011, Pittsburgh, PA, USA, June 22-24, 2011. Proceedings*. 2011, pp. 33–47. doi: 10.1007/978-3-642-21599-5_3. url: http://dx.doi.org/10.1007/978-3-642-21599-5_3.

Milosevic et al.: On the Reduction of Atomic Broadcast to Consensus with Byzantine Faults **milosevic2011reduction**

Zarko Milosevic, Martin Hutle, and André Schiper. "On the Reduction of Atomic Broadcast to Consensus with Byzantine Faults". In: *30th IEEE Symposium on Reliable Distributed Systems (SRDS 2011), Madrid, Spain, October 4-7, 2011*. 2011, pp. 235–244. doi: 10.1109/SRDS.2011.36. url: http://dx.doi.org/10.1109/SRDS.2011.36.

Mohammad et al.: Information Sharing with User Managed Access **Alam2011**

Alam Mohammad and Mario Hoffmann. "Information Sharing with User Managed Access". In: EEMA: The eID Interoperability Conference. 2011. url: https://www.eema.org/Events/Presentations/?eventId=784be67a-b2a7-45d3-8f00-1c1c3cee7976.

Abstract: Managing of sharing information in social networks is a difficult task for users and can violate the user's privacy. The UMA protocol enables the "Authorizing User" to control access to his/her own resources, i.e. identities, preferences, data, through an "Authorization Manager" (AM). Based on user's policies the AM may grant access to third parties that request for those information. When a "Requester" attempts access to a protected resource owned and protected by the authorizing user stored at some "Host", he is told where to go (the location of the AM) in order to request an access token. When he gets to the AM, he might be asked to convey claims about the requesting party, e.g. a web user or corporation, that satisfy the user's policy. After obtaining the right access token the requester is then able to receive the information he originally asked for. In our presentation the protocol and current prototype development will be introduced in detail.

Ries et al.: Verification of data location in cloud networking **Ries2011439**

T. Ries, V. Fusenig, C. Vilbois, and T. Engel. "Verification of data location in cloud networking". In: cited By 3. 2011, pp. 439–444. doi: 10.1109/UCC.2011.72. url: http://www.scopus.com/inward/record.url?eid=2-s2.0-84856349455&partnerID=40&md5=dde2a7cdb5911c28dd6ff5eba9fd1bd9.

Schütte: Apollon: Towards a Semantically Extensible Policy Framework **Schuette2011b**

Julian Schütte. "Apollon: Towards a Semantically Extensible Policy Framework". In: *Proceedings of the International Conference on Security and Cryptography (SECRYPT)*. 2011.

Schütte et al.: Auctions for Secure Multi-Party Policy Negotiation in Ambient Intelligence **Schuette2011a**

Julian Schütte and Stephan Heuser. "Auctions for Secure Multi-Party Policy Negotiation in Ambient Intelligence". In: *Proceedings of the Seventh International Symposium on Frontiers in Networking with Applications (FINA)*. 2011.

Stephanow et al.: Maturity Of Cloud Computing Technology Components Within Infrastructure-as-a-Service: A Practical Approach **stephanow2011c**

P. Stephanow, M. Kulicke, and M. Aumüller. *Maturity Of Cloud Computing Technology Components Within Infrastructure-as-a-Service: A Practical Approach*. Tech. rep. Fraunhofer AISEC, 2011.

Stephanow et al.: Anforderungserhebung in der öffentlichen Verwaltung - Ein Vorschlag für einen strukturierten Erhebungsprozess und die resultierende Anforderungsdokumentation **stephanow2011d**

Philipp Stephanow and Sebastian Hudert. "Anforderungserhebung in der öffentlichen Verwaltung - Ein Vorschlag für einen strukturierten Erhebungsprozess und die resultierende Anforderungsdokumentation". In: *Wirtschaftinformatik Proceedings*. 2011.

Subramanian et al.: An Architecture To Provide Cloud Based Security Services For Smartphones **stephanow2011**

Stephanow P. Subramanian L. and Maquire G. "An Architecture To Provide Cloud Based Security Services For Smartphones". In: *27th Meeting of the Wireless World Research Forum (WWRF)*. 2011.

Subramanian et al.: Towards Cloud Based Smartphone Security **stephanow2011b**

Stephanow P. Subramanian L. and T. Wahl. "Towards Cloud Based Smartphone Security". In: *4. Workshop Grid- und Cloud-Technologie für den Entwurf technischer Systeme (grid4ts)*. 2011.

Tsvihun et al.: Cloud Security – Sicherheit in der Wolke **Tsvihun2011**

Iryna Tsvihun and Gerd Stefan Brost. "Cloud Security – Sicherheit in der Wolke". In: *ISIS Cloud & SaaS Report* (2011), pp. 10–11.

Tsvihun et al.: Security Analysis of the IaaS Offering "Fujitsu Cloud in Central Europe" **Tsvihun2011a**

Iryna Tsvihun and Marcel Kulicke. *Security Analysis of the IaaS Offering "Fujitsu Cloud in Central Europe"*. Tech. rep. Fraunhofer AISEC, 2011.

Bless et al.: A Security Model for Future Vehicular Electronic Infrastructures **bless2010model**

Roland Bless, Gerrit Grotewold, Christian Haas, Boris Hackstein, Stefan Hofmann, Anke Jentzsch, Alexander Kiening, Christoph Krauß, Julian Lamberty, Michael Müter, Peter Schoo, Lars Völker, and Christoph Werle. "A Security Model for Future Vehicular Electronic Infrastructures". In: *8th escar* (2010).

Brunner et al.: The Fraunhofer SIT malware analysis laboratory - establishing a secured, honeynet-based cyber threat analysis and research environment **Brunner2010**

Martin Brunner, Michael Epah, Hans Hofinger, Christopher Roblee, Peter Schoo, and Sascha Todt. *The Fraunhofer SIT malware analysis laboratory - establishing a secured, honeynet-based cyber threat analysis and research environment*. Fraunhofer SIT, Darmstadt. Sept. 2010. url: `http://publica.fraunhofer.de/documents/N-141410.html`.

Brunner et al.: Infiltrating critical infrastructures with next-generation attacks: W32.Stuxnet as a showcase threat **N-151330**

Martin Brunner, Hans Hofinger, Christoph Krauß, Christopher Roblee, Peter Schoo, and Sascha Todt. *Infiltrating critical infrastructures with next-generation attacks: W32.Stuxnet as a showcase threat*. Fraunhofer SIT, Darmstadt. Dec. 2010. url: `http://publica.fraunhofer.de/documents/N-151330.html`.

Brunner et al.: Anonymity and Privacy in Distributed Early Warning Systems Critis2010

Martin Brunner, Hans Hofinger, Christopher Roblee, Peter Schoo, and Sascha Todt. "Anonymity and Privacy in Distributed Early Warning Systems". In: *Proceedings of the 5th International Conference on Critical Information Infrastructures Security (CRITIS 2010)*. Athens, Greece: Springer, Sept. 2010, pp. 82–93.

Gonz´alez-Tablas et al.: An architecture for user-managed location sharing in the Future Internet of Services Gonzalez-Tablas2010

Ana I. Gonz´alez-Tablas, Alam Mohammad, and Mario Hoffmann. "An architecture for user-managed location sharing in the Future Internet of Services". In: *The 4th International Workshop on Trustworthy Internet of People, Things & Services*. Tokyo 103-8520, Japan, 2010, p. 8. url: http://www.companionable.net/index.php?option=com_content&view=category&layout=blog&id=18&Itemid=27.

Heyszl et al.: Efficient One-pass Entity Authentication based on ECC for Constrained Devices DBLP:conf/host/HeyszlS10

Johann Heyszl and Frederic Stumpf. "Efficient One-pass Entity Authentication based on ECC for Constrained Devices". In: *HOST 2010, Proceedings of the 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 13-14 June 2010, Anaheim Convention Center, California, USA*. 2010, pp. 88–93. doi: 10.1109/HST.2010.5513107. url: http://dx.doi.org/10.1109/HST.2010.5513107.

Krauß: Detecting Compromised Nodes in Wireless Sensor Networks: Misbehavior-based Detection versus Attestation-based Detection krauss2010c

Christoph Krauß. "Detecting Compromised Nodes in Wireless Sensor Networks: Misbehavior-based Detection versus Attestation-based Detection". In: *it-Information Technology* 52.6 (2010), pp. 325–330. doi: 10.1524/itit.2010.0610.

Merli et al.: Improving the quality of ring oscillator PUFs on FPGAs DBLP:conf/cases/MerliSE10

Dominik Merli, Frederic Stumpf, and Claudia Eckert. "Improving the quality of ring oscillator PUFs on FPGAs". In: *Proceedings of the 5th Workshop on Embedded Systems Security, WESS 2010, Scottsdale, AZ, USA, October 24, 2010*. 2010, p. 9. doi: 10.1145/1873548.1873557. url: http://doi.acm.org/10.1145/1873548.1873557.

Muehlbach et al.: MalCoBox: Designing a 10 Gb/s Malware Collection Honeypot Using Reconfigurable Technology Muehlbach2010

Sascha Muehlbach, Martin Brunner, Christopher Roblee, and Andreas Koch. "MalCoBox: Designing a 10 Gb/s Malware Collection Honeypot Using Reconfigurable Technology". In: *Field Programmable Logic and Applications (FPL), 2010 International Conference on*. Milan, Italy: IEEE Computer Society, Aug. 2010, pp. 592 –595. doi: 10.1109/FPL.2010.116. url: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5694317&isnumber=5694025.

Schütte et al.: Authentic Refinement of Semantically Enhanced Policies in Pervasive Systems **Schuette2010**

Julian Schütte, Nicolai Kuntze, Andreas Fuchs, and Atta Badii. "Authentic Refinement of Semantically Enhanced Policies in Pervasive Systems". In: *Proceedings of the 25th International Information Security Conference (IFIP SEC)*. 2010.

Schütte et al.: Description Logics-based Handling of Inter-Domain Policy Conflicts **Schuette2010b**

Julian Schütte and Tobias Wahl. "Description Logics-based Handling of Inter-Domain Policy Conflicts". In: *IEEE Vehicular Technology Magazine* 5.4 (2010), pp. 68–78.

Stephanow et al.: Opportunities Of Security-as-a-Service On Smart Phones **Stephanow2010**

Philipp Stephanow and Iryna Tsvihun. "Opportunities Of Security-as-a-Service On Smart Phones". In: *25th Meeting of the Wireless World Research Forum (WWRF)* (2010).

Stephanow et al.: Technische Aspekte der Informationssicherheit in Cloud Computing Systemen **Stephanow2010a**

Philipp Stephanow, Iryna Tsvihun, and Angelika Ruppel. *Technische Aspekte der Informationssicherheit in Cloud Computing Systemen*. BITKOM Leitfaden: Cloud Computing – was Entscheider wissen müssen. 2010.

Streitberger et al.: Cloud Computing Security - Protection Goals. Taxonomy. Market Review. **Streitberger2010**

Werner Streitberger and Angelika Ruppel. *Cloud Computing Security - Protection Goals. Taxonomy. Market Review.* Fraunhofer SIT, 2010.

Stumpf: Leveraging Attestation Techniques for Trust-Establishment in Distributed Systems **Stumpf2010**

Frederic Stumpf. "Leveraging Attestation Techniques for Trust-Establishment in Distributed Systems". PhD thesis. Darmstadt University of Technology, 2010.

Tsvihun et al.: Vergleich der Sicherheit traditioneller IT-Systeme und Public Cloud Computing Systeme **Tsvihun2010**

Iryna Tsvihun, Philipp Stephanow, and Dr. Werner Streitberger. *Vergleich der Sicherheit traditioneller IT-Systeme und Public Cloud Computing Systeme*. Tech. rep. Fraunhofer AISEC, 2010.

Zhang et al.: QoS-Aware Self-adaptation of Communication Protocols in a Pervasive Service Middleware **Zhang2010**

Weishan Zhang, Klaus Marius Hansen, Joao Fernandes, Julian Schütte, and Francisco Milagro Lardies. "QoS-Aware Self-adaptation of Communication Protocols in a Pervasive Service Middleware". In:

Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing. GREENCOM-CPSCOM '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 17–26. isbn: 978-0-7695-4331-4. doi: http://dx.doi.org/10.1109/GreenCom-CPSCom.2010.132.

Akram et al.: Identity Metasystem in Location Based Persistent Authentication **EuroCAT2009**

Hasan Ibne Akram, Christian Damsgaard Jensen, and Mario Hoffmann. "Identity Metasystem in Location Based Persistent Authentication". In: *In Proceedings of the 3rd European Workshop on Combining Context with Trust, Security and Privacy (EuroCAT09)*. Pisa, Italy, Sept. 2009.

Bißmeyer et al.: simTD Security Architecture: Deployment of a Security and Privacy Architecture in Field Operational Tests **Bissmeyer2009**

Norbert Bißmeyer, Hagen Stuebing, Manuel Mattheß, Jan Peter Stotz, Julian Schütte, Matthias Gerlach, and Florian Friederici. "simTD Security Architecture: Deployment of a Security and Privacy Architecture in Field Operational Tests". In: *Proceedings of the 7th ESCAR Embedded Security in Cars Conference, Düsseldorf*. 2009.

Dahmen et al.: Short Hash-based Signatures for Wireless Sensor Networks **DahmenKrauss2009**

Erik Dahmen and Christoph Krauß. "Short Hash-based Signatures for Wireless Sensor Networks". In: *Proceedings of the 8th International Conference on Cryptology and Network Security (CANS 2009)*. Lecture Notes in Computer Science. Springer, Dec. 2009.

Eckert et al.: On Controlled Sharing of Virtual Goods **Eckert2009**

Claudia Eckert, Frederic Stumpf, and Omid Tafreschi. "On Controlled Sharing of Virtual Goods". In: *Proceedings of the 7th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods*. Nancy, France, Sept. 2009.

Stumpf et al.: A Security Architecture for Multipurpose ECUs in Vehicles **Stumpf2009a**

Frederic Stumpf, Christian Meves, Benjamin Weyl, and Marko Wolf. "A Security Architecture for Multipurpose ECUs in Vehicles". In: *25. VDI/VW-Gemeinschaftstagung: Automotive Security*. Ingolstadt, Germany, Oct. 2009.

Velikova et al.: Towards security in decentralized workflows **Velikova2009**

Zaharina Velikova, Julian Schütte, and Nicolai Kuntze. "Towards security in decentralized workflows". In: *Proceedings of the International Conference on Ultra Modern Telecommunications (ICUMT)*. 2009, pp. 1–6.

Wahl et al.: Security Mechanisms for an Ambient Environment Middleware **Wahl2009**

Tobias Wahl and Julian Schütte. "Security Mechanisms for an Ambient Environment Middleware". In: *Proceedings of International Workshop on Distributed Computing in Ambient Environments (DiComAe), Annual Conference on Artificial Intelligence (KI)*. 2009.

Zhang et al.: A Genetic Algorithms-based approach for Optimized Self-protection in a Pervasive Service Middleware **Zhang2009a**

Weishan Zhang, Julian Schütte, Mads Ingstrup, and Klaus M. Hansen. "A Genetic Algorithms-based approach for Optimized Self-protection in a Pervasive Service Middleware". In: *Proceedings of the 7th International Joint Conference on Service Oriented Computing (ICSoC)*. ICSOC-ServiceWave '09. Springer-Verlag, 2009.

Abstract: Pervasive computing is characterized by heterogeneous devices that usually have scarce resources requiring op- timized usage. These devices may use different commu- nication protocols which can be switched at runtime. As different communication protocols have different quality of service (QoS) properties, this motivates optimized self- adaption of protocols for devices, e.g., considering power consumption and other QoS requirements, e.g. round trip time (RTT) for service invocations, throughput, and reliabil- ity. In this paper, we present an extensible approach for self-adaptation of communication protocols for pervasive web services, where protocols are designed as reusable connec- tors and our middleware infrastructure can hide the com- plexity of using different communication protocols to upper layers. We also propose to use Genetic Algorithms (GAs) to find optimized configurations at runtime to achieve self- adaption of web service transport protocols (TCP, UDP and Bluetooth), taking into consideration QoS requirements. Our tests show that protocol switching involves little per- formance overhead and runs efficiently. Our evaluations also show that the proposed approach for achieving self- adaptation for communication protocols is effective where optimized configurations of protocols can be obtained with acceptable performance and quality by GAs.

Kuntze et al.: Securing Decentralized Workflows in Ambient Environments **Kuntze2008**

Nicolai Kuntze and Julian Schütte. "Securing Decentralized Workflows in Ambient Environments". In: *Proceedings of the 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC)*. EUC '08. Washington, DC, USA: IEEE Computer Society, 2008, pp. 361–366. isbn: 978-0-7695-3492-3. doi: http://dx.doi.org/10.1109/EUC.2008.86. url: http://dx.doi.org/10.1109/EUC.2008.86.

Schütte: Sichere Bluetooth-Kommunikation in Ad-hoc-Situationen **Schuette2008**

Julian Schütte. *Sichere Bluetooth-Kommunikation in Ad-hoc-Situationen*. ISBN: 9783639044362. VDM Verlag, 2008.

Heider et al.: On Path-Centric Navigation and Search Techniques for Personal Knowledge Stored in Topic Maps **Heider2007a**

Jens Heider and Julian Schütte. "On Path-Centric Navigation and Search Techniques for Personal Knowledge Stored in Topic Maps". In: *Topic Maps Research and Applications (TMRA)*. 2007.

Hoffmann et al.: Towards Semantic Resolution of Security in Ambient Environments **Hoffmann2007**

Mario Hoffmann, Atta Badii, Stephan Engberg, Renjith Nair, Daniel Thiemert, Manuel Matthess, and Julian Schütte. "Towards Semantic Resolution of Security in Ambient Environments". In: *Proceedings of the second International Conference on Ambient Intelligence Developments, AmI.d '07*. Ed. by Antonio Maña and Carsten Rudolph. Springer, 2007, pp. 13–22.

Schütte et al.: Security made easy: Achieving user-friendly communication protection in ad-hoc situations **Schuette2007**

Julian Schütte and Jens Heider. "Security made easy: Achieving user-friendly communication protection in ad-hoc situations". In: *International Conferene on Emerging Security Information, Systems, and Technologies (SECURWARE)*. Vol. 0. Los Alamitos, CA, USA: IEEE Computer Society, 2007, pp. 139–144. isbn: 0-7695-2989-5. doi: http://doi.ieeecomputersociety.org/10.1109/SECUREWARE.2007.32.

Eckert: Cybersicherheit beyond 2020! - Herausforderungen für die IT-Sicherheitsforschung **eckert2017forschungsfokus**

Claudia Eckert. "Cybersicherheit beyond 2020! - Herausforderungen für die IT-Sicherheitsforschung". In: *Fraunhofer-Forschungsfokus: Digitalisierung*. Ed. by tba. Springer Verlag, to be published, tba.

Esbach et al.: A New Security Architecture for Smartcards Utilizing PUFs **Esbach2012**

T. Esbach, W. Fumy, O. Kulikovska, D. Merli, D. Schuster, and F. Stumpf. "A New Security Architecture for Smartcards Utilizing PUFs". In: *ISSE 2012* ().

Heyszl et al.: Asymmetric Cryptography in Automotive Access and Immobilizers **Heyszl2011**

Johann Heyszl and Frederic Stumpf. "Asymmetric Cryptography in Automotive Access and Immobilizers". In: *ESCAR 2011* ().

Merli et al.: Semi-invasive EM Attack on FPGA RO PUFs and Countermeasures **Merli2011**

Dominik Merli, Dieter Schuster, Frederic Stumpf, and Georg Sigl. "Semi-invasive EM Attack on FPGA RO PUFs and Countermeasures". In: *WESS 2011* ().

Unterstein et al.: SCA Secure and Updatable Crypto Engines for FPGA SoC Bitstream Decryption– Extended version **DBLP:journal/jcen/UntersteinJHGH19**

Florian Unterstein, Nisha Jacob, Neil Hanley, Chongyan Gu, and Johann Heyszl. "SCA Secure and Updatable Crypto Engines for FPGA SoC Bitstream Decryption– Extended version". In: *Journal of Computational Engineering*. Springer, to appear.