Sven **Bugiel**

SYSTEMS SECURITY RESEARCHER · TENURED FACULTY

Hallesche Str. 9, 66121 Saarbrücken, Germany

☐ (+49) 176 376 067 94 | ✉ bugiel@cispa.de | 🏠 www.svenbugiel.de | in sven-bugiel | 🐦 @svebug

Experience

Faculty (Tenured), Head of Trusted Systems Research Group   since 01/2022

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY   *Saarbrücken, Germany*

- Supervised doctoral and (under-)graduate students in the area of (mobile) platform security with focus on Android, integration of hardware security components into security architectures, and usable security for authentication and access control
- Offered a graduate-level lecture *Mobile Security* and research seminar, both focused on Android security, and a core lecture *Security* covering basics of various aspects of cybersecurity

Faculty (Tenure-Track), Head of Trusted Systems Research Group   07/2018 – 12/2021

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY   *Saarbrücken, Germany*

- Supervised doctoral and (under-)graduate students in the area of (mobile) platform security with focus on Android, integration of hardware security components into security architectures, and usable security for authentication and access control
- Offered a graduate-level lecture *Mobile Security* and research seminar, both focused on Android security

Research Group Leader, Head of Trusted Systems Research Group   05/2016 – 06/2018

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY   *Saarbrücken, Germany*

- Supervised doctoral and (under-)graduate students in the area of Android platform security
- Offered a graduate-level lecture *Mobile Security*, focused on Android security, and hands-on lab for extending Android's application framework with security extensions

Research Assistant   04/2013 – 04/2016

CENTER FOR IT-SECURITY, PRIVACY, AND ACCOUNTABILITY (CISPA), SAARLAND UNIVERSITY   *Saarbrücken, Germany*

- Research on extending Android's application framework with mandatory access control, augmenting Binder IPC with message provenance information, and creating domain isolation between apps

Research Assistant   10/2010 – 03/2013

CENTER FOR ADVANCED SECURITY RESEARCH DARMSTADT (CASED), TECHNICAL UNIVERSITY DARMSTADT   *Darmstadt, Germany*

- Research on extending Android's application framework and Linux kernel with mandatory access control, creating domain isolation between apps, and leveraging hardware security components in system security architectures

Research Intern   01/2010 – 06/2010

NOKIA RESEARCH CENTER, TRUSTWORTHY MOBILE PLATFORMS GROUP   *Helsinki, Finland*

- Master thesis on implementing an application-specific credential platform using a custom software-based mobile trusted platform module in a trusted execution environment (TI M-Shield / ARM TrustZone)

Research Intern   06/2009 – 08/2009

NOKIA RESEARCH CENTER, TRUSTWORTHY MOBILE PLATFORMS GROUP   *Helsinki, Finland*

- Topic: Binding execution of secure execution environments to user-space programs by integrating authenticated boot with TCG's Dynamic Root for Trusted Measurement

Research Intern   6/2008 – 08/2008

NOKIA RESEARCH CENTER, TRUSTWORTHY MOBILE PLATFORMS GROUP   *Helsinki, Finland*

- Topic: Implementation of software-based a trusted platform module for mobile secure execution environments using ARM TrustZone

Education

Ph.D. (with highest distinction)
10/2010 – 12/2015

SAARLAND UNIVERSITY
Saarbrücken, Germany

- Thesis: *Establishing Mandatory Access Control on Android OS*
- My work demonstrated how domain isolation policies can be enforced via mandatory access control extensions to the Android application framework and underlying Linux kernel. It further proposed an extension to Android's Binder IPC to support policy enforcement with message provenance information. The thesis comprises publications at the top-tier venues NDSS, USENIX Security, and ACSAC.

M.Sc. in Security and Mobile Computing (with distinction)
10/2008 – 09/2010

TECHNICAL UNIVERSITY OF DENMARK *and* ROYAL INSTITUTE OF TECHNOLOGY
Copenhagen, Denmark and Stockholm, Sweden

- Student in the European NordSecMob Erasmus Mundus Master's Programme in Security and Mobile Computing
- Thesis: *Using TCG/DRTM for application-specific credential storage and usage* (conducted at Nokia Research Center, Helsinki, Finland)
- This thesis demonstrated how measurements by authenticated boot can be combined with *late-launch* (DRTM) by the Trusted Computing Group to bind credentials to applications

Erasmus Programme of the European Union
09/2007 – 08/2008

HELSINKI UNIVERSITY OF TECHNOLOGY (*now* AALTO UNIVERSITY)
Helsinki, Finland

- Exchange student for two semesters

Pre-Diploma in Security in Information Science
10/2004 – 08/2008

HORST GÖRTZ INSTITUTE FOR IT SECURITY, RUHR-UNIVERSITY
Bochum, Germany

- Pre-Diploma is comparable to a B.Sc. degree

Relevant Awards

2024, Apr 15   Best teaching award for *Mobile Security (Winter Term 2023/2024)* at Computer Science Department of Saarland University

2019, Oct 14   Best teaching award for *Selected Topics in Mobile Security (Summer Term 2019)* at Computer Science Department of Saarland University

2015, Apr 20   Best teaching award for *Foundations of Cybersecurity (Winter Term 2014/2015)* at Computer Science Department of Saarland University

2015, Mar 25   Saarland award for outstanding university education 2014 ("Landespreis Hochschullehre 2014") for *Proseminar Hacking (Summer Term 2014)*

2014, Oct 20   Best teaching award for *Proseminar Hacking (Summer Term 2014)* at Computer Science Department of Saarland University

Selected Lectures

Mobile Security
since Winter Term 2016/17

ADVANCED LECTURE FOR GRADUATE STUDENTS (EVERY WINTER TERM)

- Lecture covers fundamental aspects of mobile operating systems and application security at the example of Android and its ecosystem
- Content includes Android's security architecture, issues of third party libraries and UI deception, network and web security aspects, and trusted execution environments.
- Lecture content of last iteration: `https://cms.cispa.saarland/mobsec2122/2/Lecture_schedule`
- The lecture is accompanied by practical exercises and a course project to extend Android with a custom security feature

Selected Topics in Mobile Security
since Summer Term 2018

SEMINAR (EVERY SUMMER TERM)

- Discussion of recent research results in the area of mobile security with a strong focus on Android
- Course page of last iteration: `https://cms.cispa.saarland/stims21/`

Security
Winter Term 2022/23

CORE LECTURE

- Lecture covers fundamental aspects of cybersecurity, ranging from basics of cryptography and cryptographic protocols, network security, authentication and access control, system security, to usable security, distributed systems, and anonymity.
- Course page of last iteration: `https://cms.cispa.saarland/sec2223/`
- The lecture is accompanied by a mixture of practical and theoretical exercises

Scientific Publications

Online profiles

𝒢	Google Scholar:	`http://scholar.google.de/citations?user=sPrlusAAAAAJ`
	DBLP:	`https://dblp.org/pid/31/7561.html`
ⓘD	ORCID:	`https://orcid.org/0000-0002-7151-9614`

Conference Proceedings

[1] Y. Elbitar, A. Hart, and S. Bugiel, "**The power of words: A comprehensive analysis of rationales and their effects on users' permission decisions**," in *32nd Annual Network & Distributed System Security Symposium (NDSS'25)*, The Internet Society, 2025.

[2] E. Ackermann, N. Mauthe, and S. Bugiel, "**Work-in-progress: Northcape: Embedded real-time capability-based addressing**," in *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE Computer Society, 2024.

[3] A. Jallow, M. Schilling, M. Backes, and S. Bugiel, "**Measuring the effects of stack overflow code snippet evolution on open-source software security**," in *45th IEEE Symposium on Security and Privacy (SP'24)*, IEEE, 2024.

[4] D. Chakraborty, M. Schwarz, and S. Bugiel, "**Talus: Reinforcing TEE confidentiality with cryptographic coprocessors**," in *27th International Conference on Financial Cryptography and Data Security (FC'23*, 2023.

[5] S. Ghorbani Lyastani, M. Backes, and S. Bugiel, "**A systematic study of the consistency of two-factor authentication user journeys on top-ranked websites**," in *30th Annual Network & Distributed System Security Symposium (NDSS '23)*, The Internet Society, 2023.

[6] A. Dawoud and S. Bugiel, "**Bringing balance to the force: Dynamic analysis of the Android application framework**," in *28th Annual Network & Distributed System Security Symposium (NDSS '21)*, ISOC, 2021.

[7] Y. Elbitar, M. Schilling, T. Nguyen, M. Backes, and S. Bugiel, "**What really matters: The effect of timing & rationales on users' runtime permission decisions**," in *31st USENIX Security Symposium (SEC '21)*, USENIX, 2021.

[8] J. Huang, M. Backes, and S. Bugiel, "**A11y and privacy don't have to be mutually exclusive: Constraining accessibility service misuse on Android**," in *31st USENIX Security Symposium (SEC '21)*, USENIX, 2021.

[9] S. Ghorbani Lyastani, M. Schilling, M. Neumayr, M. Backes, and S. Bugiel, "**Is FIDO2 the kingslayer of user authentication? A comparative usability study of FIDO2 passwordless authentication**," in *41st IEEE Symposium on Security and Privacy (SP '20)*, IEEE, 2020.

[10] D. C. Nguyen, E. Derr, M. Backes, and S. Bugiel, "**Fixdep: Android tool support to fix insecure code dependencies**," in *36th Annual Computer Security Applications Conference (ACSAC '20)*, ACM, 2020.

[11] D. Chakraborty, C. Hammer, and S. Bugiel, "**Secure multi-execution in Android**," in *34th Symposium on Applied Computing (SAC '19)*, ACM, 2019.

[12] D. Chakraborty, L. Hanzlik, and S. Bugiel, "**SimTPM: User-centric tpm for mobile devices**," in *29th USENIX Security Symposium (SEC '19)*, USENIX, 2019.

[13] A. Dawoud and S. Bugiel, "**Droidcap: OS support for capability-based permissions in Android**," in *26th Annual Network & Distributed System Security Symposium (NDSS '19)*, ISOC, 2019.

[14] J. Huang, N. Borges, S. Bugiel, and M. Backes, "**Up-to-crash: Evaluating third-party library updatability on Android**," in *4th IEEE European Symposium on Security and Privacy (EuroSP '19)*, IEEE, 2019.

[15] D. C. Nguyen, E. Derr, M. Backes, and S. Bugiel, "**Short text, large effect: Measuring the impact of user reviews on Android app security & privacy**," in *40th IEEE Symposium on Security and Privacy (SP '19)*, IEEE, 2019.

[16] S. G. Lyastani, M. Schilling, S. Fahl, M. Backes, and S. Bugiel, "**Better managed than memorized? studying the impact of managers on password strength and reuse**," in *28th USENIX Security Symposium (SEC '18)*, USENIX, 2018.

[17] M. Oltrogge, E. Derr, C. Stransky, Y. Acar, S. Fahl, C. Rossow, G. Pellegrino, S. Bugiel, and M. Backes, "**The Rise of the Citizen Developer: Assessing the Security Impact of Online App Generators**," in *39th IEEE Symposium on Security and Privacy (SP '18)*, IEEE, 2018.

[18] M. Backes, S. Bugiel, O. Schranz, P. von Styp-Rekowsky, and S. Weisgerber, "**ARTist: The Android runtime instrumentation and security toolkit**," in *2nd IEEE European Symposium on Security and Privacy (EuroSP'17)*, IEEE, 2017.

[19] M. Backes, S. Bugiel, P. von Styp-Rekowsky, and M. Wißfeld, "**Seamless in-app ad blocking on stock Android**," in *Mobile Security Technologies (MOST) 2017 Workshop*, IEEE, 2017.

[20] E. Derr, S. Bugiel, S. Fahl, Y. Acar, and M. Backes, "**Keep me Updated: An Empirical Study of Third-Party Library Updatability on Android**," in *24th ACM Conference on Computer and Communication Security (CCS '17)*, ACM, 2017.

[21] J. Huang, O. Schranz, S. Bugiel, and M. Backes, "**The ART of App Compartmentalization: Compiler-based Library Privilege Separation on Stock Android**," in *24th ACM Conference on Computer and Communication Security (CCS '17)*, ACM, 2017.

[22] Y. Acar, M. Backes, S. Bugiel, S. Fahl, P. McDaniel, and M. Smith, "**SoK: Lessons Learned From Android Security Research For Appified Software Platforms**," in *37th IEEE Symposium on Security and Privacy (SP '16)*, IEEE, 2016.

[23] M. Backes, S. Bugiel, and E. Derr, "**Reliable Third-Party Library Detection in Android and its Security Applications**," in *23rd ACM Conference on Computer and Communications Security (CCS '16)*, ACM, 2016.

[24] M. Backes, S. Bugiel, E. Derr, S. Gerling, and C. Hammer, "**R-Droid: Leveraging Android App Analysis with Static Slice Optimization**," in *11th ACM Asia Conference on Computer and Communications Security (ASIACCS '16)*, Invited paper, ACM, 2016.

[25] M. Backes, S. Bugiel, E. Derr, P. McDaniel, D. Octeau, and S. Weisgerber, "**On Demystifying the Android Application Framework: Re-Visiting Android Permission Specification Analysis**," in *26th USENIX Security Symposium (SEC '16)*, USENIX, 2016.

[26] M. Backes, S. Bugiel, C. Hammer, O. Schranz, and P. von Styp-Rekowsky, "**Boxify: Full-fledged app sandboxing for stock Android**," in *24th USENIX Security Symposium (SEC '15)*, USENIX, 2015.

[27] M. Backes, S. Bugiel, and S. Gerling, "**Scippa: System-centric IPC provenance on Android**," in *30th Annual Computer Security Applications Conference (ACSAC '14)*, ACM, 2014.

[28] M. Backes, S. Bugiel, S. Gerling, and P. von Styp-Rekowsky, "**Android Security Framework: Extensible multi-layered access control on Android**," in *30th Annual Computer Security Applications Conference (ACSAC '14)*, ACM, 2014.

[29] S. Bleikertz, S. Bugiel, H. Ideler, S. Nürnberger, and A.-R. Sadeghi, "**Client-controlled Cryptography-as-a-Service in the Cloud**," in *11th International Conference on Applied Cryptography and Network Security (ACNS'13)*, Springer, 2013.

[30] S. Bugiel, S. Heuser, and A.-R. Sadeghi, "**Flexible and fine-grained mandatory access control on Android for diverse security and privacy policies**," in *22nd USENIX Security Symposium (SEC '13)*, USENIX, 2013.

[31] F. F. Brasser, S. Bugiel, A. Filyanov, A.-R. Sadeghi, and S. Schulz, "**Softer smartcards: Usable cryptographic tokens with secure execution**," in *Financial Cryptography and Data Security (FC'12)*, ser. LNCS, Springer, 2012.

[32] S. Bugiel, L. Davi, A. Dmitrienko, T. Fischer, A.-R. Sadeghi, and B. Shastry, "**Towards taming privilege-escalation attacks on Android**," in *19th Annual Network & Distributed System Security Symposium (NDSS'12)*, ISOC, 2012.

[33] S. Bugiel, L. Davi, A. Dmitrienko, S. Heuser, A.-R. Sadeghi, and B. Shastry, "**Practical and lightweight domain isolation on Android**," in *1st ACM CCS Workshop on Security and Privacy in Mobile Devices (SPSM'11)*, ACM, 2011.

[34] S. Bugiel, L. Davi, and S. Schulz, "**Scalable trust establishment with software reputation**," in *6th Annual Workshop on Scalable Trusted Computing (STC'11)*, ACM, 2011.

[35] S. Bugiel, S. Nürnberger, A.-R. Sadeghi, and T. Schneider, "**Twin clouds: Secure cloud computing with low latency**," in *Communications and Multimedia Security Conference (CMS'11)*, (Best Paper Award), Springer, 2011.

[36] S. Bugiel, T. Pöppelmann, S. Nürnberger, A.-R. Sadeghi, and T. Schneider, "**AmazonIA: When elasticity snaps back**," in *18th ACM Conference on Computer and Communications Security (CCS'11)*, ACM, 2011.

[37] S. Bugiel, A.-R. Sadeghi, T. Schneider, and S. Nürnberger, "**Twin clouds: An architecture for secure cloud computing (extended abstract)**," in *Workshop on Cryptography and Security in Clouds (CSC'11)*, 2011.

[38] S. Bugiel, A. Dmitrienko, K. Kostiainen, A.-R. Sadeghi, and M. Winandy, "**TruWalletM: Secure web authentication on mobile platforms**," in *2nd Conference on Trusted Systems (INTRUST'10)*, 2010.

[39] S. Bugiel and J.-E. Ekberg, "**Implementing an application-specific credential platform using late-launched mobile trusted module**," in *5th Annual Workshop on Scalable Trusted Computing (STC'10)*, ACM, 2010.

[40] J.-E. Ekberg and S. Bugiel, "**Trust in a small package: Minimized MRTM software implementation for mobile secure environments**," in *4th Annual Workshop on Scalable Trusted Computing (STC'09)*, ACM, 2009.

Technical Reports

[TR-1] M. Backes, S. Bugiel, S. Gerling, and P. von Styp-Rekowsky, "Android security framework: Enabling generic and extensible access control on Android," Saarland University, Tech. Rep. A/01/2014, Apr. 2014.

[TR-2] S. Bugiel, S. Heuser, and A.-R. Sadeghi, "myTunes: Semantically Linked and User-Centric Fine-Grained Privacy Control on Android," Center for Advanced Security Research Darmstadt, Technical Report TUD-CS-2012-0226, 2012.

[TR-3] ——, "Towards a Framework for Android Security Modules: Extending SE Android Type Enforcement to Android Middleware," Center for Advanced Security Research Darmstadt, Tech. Rep. TUD-CS-2012-0231, 2012.

[TR-4] S. Bugiel, L. Davi, A. Dmitrienko, T. Fischer, and A.-R. Sadeghi, "XManDroid: A new Android evolution to mitigate privilege escalation attacks," Technische Universität Darmstadt, Technical Report TR-2011-04, 2011.