Dr. Saša Radomirović

Personal Data

	Senior Lecturer in Secure Systems Director of Cyber Security MSc Programme
Address	Computer Science Research Centre, University of Surrey GU2 7XH, Guildford, Surrey
Email	`s.radomirovic@surrey.ac.uk`
Web site	`https://www.surrey.ac.uk/people/sasa-radomirovic`

Research Interests

Formal methods for information security, design and verification of cryptographic protocols, analysis of human factors in security critical systems, and threat modeling.

Academic Employment

2022–	Senior Lecturer, University of Surrey, Guildford, UK
2020–2022	Associate Professor, Heriot-Watt University, Edinburgh, UK
2016–2019	Senior Lecturer, University of Dundee, UK
2014–2016	Lecturer, ETH Zürich, Switzerland
2012–2014	Senior Scientist, ETH Zürich, Switzerland
2007–2012	Post-doc, University of Luxembourg, Luxembourg
2006–2007	Postdoctoral Fellow, Centre de Recerca Matemàtica, Barcelona
2005–2006	ERCIM Postdoctoral Fellow, NTNU, Trondheim, Norway

Education

2005 Ph.D. Mathematics, Rutgers University, New Brunswick, NJ, USA
Thesis: Cusp Forms Over Function Fields and Modular Symbols
Adviser: Jerrold Tunnell

1998 Dipl. Math. ETH, ETH Zürich, Zürich, Switzerland
Thesis: Investigations Into Span Programs With Multiplication
Adviser: Ueli Maurer, Ronald Cramer

Professional Services (partial listing)

- Commissioned by Swiss Federal Chancellery (2022, 2023) to review security proofs of Swiss Post E-Voting protocol used in Swiss federal elections 2023.
- Associate editor of IEEE Transactions on Dependable and Secure Computing (since 2022).
- Co-chair of the Security Track of the 37th and 38th ACM Symposium on Applied Computing (SAC 2022, 2023).
- Program committee member of 30+ conferences.
- External examiner of PhD dissertations at University of Luxembourg, ETH Zürich, IRISA Rennes, University of Newcastle.

Selected Publications

1. Sven Hammann, Michael Crabb, Saša Radomirović, Ralf Sasse, and David Basin. "I'm Surprised So Much Is Connected": A Study on Users' Online Accounts. In *ACM CHI 2022*.
2. David Basin, Jannik Dreier, Sofia Giampietro, and Saša Radomirović. Verifying Table-Based Elections. In *ACM CCS 2021*.
3. Sven Hammann, Saša Radomirović, Ralf Sasse, and David Basin. User Account Access Graphs. In *ACM CCS 2019*.
4. David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirović, Ralf Sasse, and Vincent Stettler. A Formal Analysis of 5G Authentication. In *ACM CCS 2018*.
5. Barbara Kordy, Sjouke Mauw, Saša Radomirović, and Patrick Schweitzer, "Attack–defense trees," *Journal of Logic and Computation*, vol. 24, no. 1, 2014.
6. Ton van Deursen, Sjouke Mauw, and Saša Radomirović, "mCarve: Carving attributed dump sets," in *20th USENIX Security Symposium*, 2011.