Jorden Whitefield

Secure Systems Group, Department of Computer Science, Aalto University, Espoo, Finland

(+358) 41 703 9066 | jorden.whitefield@googlemail.com | jwhitefield.co.uk | jorden.whitefield

Research Interests

Security Protocol Analysis, Trusted Computing, Security and Privacy Architectures, Automotive Security, Formal Verification Tools.

Education

PhD in Computer Science (Funded EPSRC iCASE with Thales UK) *University of Surrey*

Surrey Centre for Cyber Security, Department of Computer Science *October. 2015 - February. 2019*

- Thesis title: Formal Analysis and Applications of Direct Anonymous Attestation
- Supervised by Liqun Chen, Steve Schneider and Helen Treharne.

Graduate Certificate in Learning and Teaching *University of Surrey*

Department of Higher Education *Jan. 2016 - Jun. 2017*

- Fellow of the Higher Education Academy, Reference: PR137274
- The course explored the theory and practice of teaching, curriculum design and implementation, and pedagogy research.

BSc (Hons) in Computer Science (Result: 1:1) *University of Surrey*

Department of Computer Science *Sep. 2011 - Jul. 2015*

- Dissertation Project: Linking ProB and LTSmin
- EDF Best Digital Project Prize: Awarded for achieving the highest mark for the Final Year project.
- University of Surrey Scholarship Award: awarded for performance in my studies.
- Modules studied include: Computer Security, Information Security Management, Software Engineering Project

Research Experience

Secure Systems Group *Aalto University*

Post Doctoral Researcher *Jan. 2019 - Present*

- Research themes: Attestation, Android Security, Blockchain and Consensus

Thales UK Research and Technology *Reading, UK*

iCASE Placement *Jul. 2017 - Oct. 2017*

- Thales indicated a strong interest in Trusted Platform Modules (TPM) and Trusted Execution Environments (TEE) and how these technologies can be used within security protocols, *e.g.*, investigating how Direct Anonymous Attestation could be applied in the vehicular domain.
- Secondment to Thales eSecurity – Defined scope of work in collaboration with Thales aligned to trusted computing agenda. Developed a demonstrator of the O-Token protocol defined in the STM 2017 paper. Responsible for leading the project, defined an initial requirements specification, supervised a graduate student in the development of the demonstrator and presented outcomes for internal review.

EPSRC Impact Acceleration Account, Privacy-enhanced capabilities for VANETs using Direct Anonymous Attestation (£35k) *University of Surrey*

Co-Investigator *Jan. 2018 - Jul. 2018*

- Defined the architecture to be used within the proposal to build a demonstrator for privacy-preserving Vehicle-2-Anything (V2X) communications by employing Direct Anonymous Attestation that is standardized in ISO/IEC 20008-2 & 11889.
- Co-wrote the work packages within the proposal.
- Project in partnership with two industrial partners: Pervasive Intelligence and Thales UK. The demonstrator is implemented in a relevant lab environment using automotive boxes, communication interfaces and message standards.

EPSRC Vacation Bursary, Integration of ProB and LTSmin *University of Surrey*

Research Student *Jun. 2014 - Aug. 2014*

- Collaborated with research groups at the University of Twente and the University of Düsseldorf.
- Developed prototype as a basis for a new tool integration between the two model checkers.

Industry

Associate Software Engineer *London, UK*

Accenture UK *Jul. 2013 - Jul. 2014*

- Developed hybrid mobile applications for Android and iOS.
- Extended legacy government software systems with a RESTful API layer to integrate with modern systems.
- Software Quality Assurance Engineer for HMRC digital services.

Service

Contributed Talks

- Real World Crypto (RWC) 2019 – "Direct Anonymous Attestation in the Wild", [YouTube], [Slides]
- 1st UK Research Institute in Secure Hardware and Embedded Systems (RISE) Annual Conference 2018 – "Formal Analysis and Applications of Direct Anonymous Attestation" [Slides]

Reviewer

- European Symposium on Research in Computer Security – 23rd Symposium (ESORICS 18), Integrated Formal Methods – 14th International Conference (iFM 18)
- IEEE Transactions on Dependable and Secure Computing (TDSC)

Other

- Founder and lead organiser of Surrey Secure Systems Reading Group. Involved coordinating weekly meetings.
- PhD Student Representative, provided support for new PhD students and represented students in the doctoral college committee.

Teaching

CS-E4310: Mobile Systems Security

Aalto University

Department of Computer Science *2019*

- Graded student exercises, and I was responsible for organising the student presentation portion of the course.

CS-E4000: Seminar in Computer Science

Aalto University

Department of Computer Science *2019*

- Supervised an MSc student to produce a report for the state-of-the-art and limitations of Android app collusion attacks.

COM3009: Computer Security

University of Surrey

Department of Computer Science *2016/17*

- Lab demonstrator for practical sessions for a class of 40 final year students.
- Supported student learning in cryptography, application of CrypTool for lab exercises and symbolic security protocol verification in Scyther.

COM2039: Parallel Computing

University of Surrey

Department of Computer Science *2016/17*

- Lab demonstrator for practical sessions for a class of 60 second year students.
- Supported student learning in labs for basics of programming NVIDIA CUDA in C.

COM1032: Mobile Computing

University of Surrey

Department of Computer Science *2015/16*

- Provided support in lab on Android, Java and Android Studio.
- Marking lead for two courseworks for over 100 students, which required evaluation of Java code and testing on tablets. Experienced in using grade descriptors and automated feedback and personalised formative feedback.

COM1028: Programming Fundamentals

University of Surrey

Department of Computer Science *2015/16 & 2016/17*

- Lead lab demonstrator for practical sessions in the lab sessions for class of 60 first year students.
- Mentored students to become lab demonstrators for this module.
- Lead tutorial sessions for students who required extra support in groups of 20 or more.
- Module aim was to deliver fundamentals of programming using Java in Eclipse IDE.

Publications

Published

- J. Whitefield, L. Chen, R. Sasse, H. T. Steve Schneider, and S. Wesemeyer, "A Symbolic Analysis of ECC-based Direct Anonymous Attestation," in *2019 IEEE European Symposium on Security and Privacy, EuroSP 2019, Stockholm, Sweden, June 17-19, 2019*, 2019

- J. Whitefield, L. Chen, T. Giannetsos, S. Schneider, and H. Treharne, "Privacy-enhanced capabilities for VANETs using Direct Anonymous Attestation," in *2017 IEEE Vehicular Networking Conference, VNC 2017, Torino, Italy, November 27-29, 2017*, 2017, pp. 123–130

- J. Whitefield, L. Chen, F. Kargl, A. Paverd, S. Schneider, H. Treharne, and S. Wesemeyer, "Formal analysis of V2X revocation protocols," in *Security and Trust Management - 13th International Workshop, STM 2017, Oslo, Norway, September 14-15, 2017, Proceedings*, 2017, pp. 147–163

- J. Bendisposto, P. Körner, M. Leuschel, J. Meijer, J. van de Pol, H. Treharne, and J. Whitefield, "Symbolic Reachability Analysis of B Through ProB and LTSmin," in *Integrated Formal Methods - 12th International Conference, IFM 2016, Reykjavik, Iceland, June 1-5, 2016, Proceedings*, 2016, pp. 275–291

Skills

Programming	Java, Python, C++, JavaScript
Formal tools	Tamarin Prover, Scyther
Misc.	Git, SVN, Linux, LaTeX

Basic Information

Date of Birth: 19/05/1992 **Nationality:** British **Languages:** English (native)