Jorden Whitefield
Computer Security Researcher

✉ jorden.whitefield@googlemail.com | ⑤ jorden.whitefield | ⊕ jwhitefield.co.uk

Employment

2019 -   **Aalto University** Post Doctoral Researcher.

2013 - 2014   **Accenture UK** Associate Software Engineer.

I developed hybrid mobile applications for Android and Apple iOS. I extended legacy UK government software systems with a RESTful API layer to integrate with modern systems.

Education

2015 - 2019   **University of Surrey** Computer Security PhD (Funded EPSRC iCASE with Thales UK)

PhD supervisors: Liqun Chen, Steve Schneider, and Helen Treharne.

My thesis was titled: Formal Analysis and Applications of Direct Anonymous Attestation.

2016 - 2017   **University of Surrey** Graduate Certificate in Learning and Teaching.

I am a fellow of the Higher Education Academy UK (Reference #: R137274). The course explored the theory and practice of teaching, curriculum design and implementation, and pedagogy research.

2011 - 2015   **University of Surrey** BSc Computer Science (First class honours)

Dissertation Project: Linking ProB and LTSmin.

I was awarded the EDF Best Digital Project Prize for achieving the highest mark for the dissertation project.

I received a scholarship from the University of Surrey for performance in my studies.

Modules I studied include: Computer Security, Information Security Management, Software Engineering Project.

Placements

2017   **Thales eSecurity UK** (Cambridge, UK)

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.

I also defined a scope of work in collaboration with Thales aligned to their trusted computing agenda. I developed a demonstrator of the O-Token protocol defined in my STM 2017 paper. I was responsible for leading the project, defined an initial software requirements specification, supervised a graduate student in the development of the demonstrator and presented outcomes for internal review.

Awards

EPSRC UK Impact Acceleration Account, Privacy-enhanced capabilities for VANETs using Direct Anonymous Attestation (£47k)

Co-Investigator: January 2018 - December 2018

Project partners: University of Surrey, Pervasive Intelligence UK, Thales Research and Technology UK

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.

The demonstrator is implemented in a relevant lab environment using NexCom automotive boxes, TPM developer modules, various communication interfaces and message standards.

Service

Contributed Talks   **2019**   Real World Crypto (RWC) 2019 – Direct Anonymous Attestation in the Wild.

📄 Slides | ▶ YouTube

2018   1st UK Research Institute in Secure Hardware and Embedded Systems (RISE) Annual

Conference 2018 – Formal Analysis and Applications of Direct Anonymous Attestation.
📄 Slides

Reviewer 2018 European Symposium on Research in Computer Security (ESORICS) – 23rd Symposium

Integrated Formal Methods (iFM) – 14th International Conference

IEEE Transactions on Dependable and Secure Computing (TDSC)

Teaching

2019 **CS-E4310: Mobile Systems Security**, Aalto University

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

CS-E4000: Seminar in Computer Science, Aalto University

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

2017 **COM3009: Computer Security**, University of Surrey

I was a lab demonstrator for lab sessions for a class of 40 final year students.

I supported student learning in cryptography, application of CrypTool for lab exercises and symbolic security protocol verification in Scyther.

COM2039: Parallel Computing, University of Surrey

I was a lab demonstrator for lab sessions for a class of 60 second year students.

Supported student learning in labs for basics of programming NVIDIA CUDA in C.

2016 **COM1032: Mobile Computing**, University of Surrey

I provided support in lab sessions on Android, Java and Android Studio.

I was the marking lead for two assignments 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.

2015 **COM1028: Programming Fundamentals**, University of Surrey

I was the lead lab demonstrator for practical sessions in the lab sessions for class of 60 first year students.

I mentored students to become lab demonstrators for this module.

I lead tutorial sessions for students who required extra support in groups of 20 or more.

The module aim was to deliver fundamentals of programming using Java in Eclipse IDE.

Publications

2019 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. **Jorden, Whitefield**, Liqun Chen, Ralf Sasse, Steve Schneider, Helen Treharne and Stephan Wesemeyer.

🌐 To appear | 🔗 ETH Preprint

2017 Privacy-Enhanced Capabilities for VANETS Using Direct Anonymous Attestation.

In 2017 IEEE Vehicular Networking Conference, VNC 2017, Torino, Italy, November 27-29, 2017, 123–30. **Jorden, Whitefield**, Liqun Chen, Thanassis Giannetsos, Steve Schneider, and Helen Treharne. 2017.

🌐 10.1109/VNC.2017.8275615 | 🔗 Surrey ePubs

Formal Analysis of V2X Revocation Protocols

In Security and Trust Management - 13th International Workshop, STM 2017, Oslo, Norway, September 14-15, 2017, Proceedings, 147–63. **Jorden Whitefield**, Liqun Chen, Frank Kargl, Andrew Paverd, Steve Schneider, Helen Treharne, and Stephan Wesemeyer. 2017.

🌐 10.1007/978-3-319-68063-7_10 | 🗒 1704.07216

2016 Symbolic Reachability Analysis of B Through ProB and LTSmin

In Integrated Formal Methods - 12th International Conference, IFM 2016, Reykjavik, Iceland, June 1-5, 2016, 275-91. Bendisposto, Jens, Philipp Körner, Michael Leuschel, Jeroen Meijer, Jaco van de Pol, Helen Treharne, and **Jorden Whitefield**. 2016.

🌐 10.1007/978-3-319-33693-0_18 | 🗒 1603.04401

Technical skills

Programming	Java (incl Android) Python C++ Javascript HTML and CSS
Formal tools	Tamarin Prover Scyther
Other	LaTeX Bash Git Linux
Areas of expertise	Security Protocol Analysis Trusted Computing V2X Security Security and Privacy Software Development
References	Available on request.