Christopher Hicks

— Security and Privacy Research Student —

chrishicks@mailbox.org
(+44)7938875365
chrishicks.io
github.com/hkscy

Education

University of Birmingham, UK 2010 - 2019
Academic Centre of Excellence in Cyber Security Research (ACE-CSR)

- PhD Computer Science (3.5 year research period), graduation July 2020
  I developed novel, standards-focussed techniques for privacy and trust that are suitable for national scale, distributed systems. In particular I proposed several new methods for securing vehicle-to-everything (V2X) architectures, I contextualised secure hardware and attestation protocols for this application, and I also discovered new cryptographic, key management and implementation vulnerabilities in an existing vehicle immobiliser system.
- **MEng Electronic and Software Engineering with Industrial Placement Year, 80% Overall**
  I studied a broad range of curriculum from both electronic engineering and computer science during my joint-honours degree. Modules include *Software Engineering*, *Networks and Distributed Systems*, *Operating Systems with C/C++*, *Digital Logic and Microprocessor Systems*, *Small Embedded Systems, Data Mining* and *Cryptography*.

Peer-Reviewed Publications

- Christopher Hicks and Flavio D. Garcia. VDAA: A Vehicular DAA scheme for Unlinkable ECDSA Pseudonyms in V2X. Under Submission to Euro S&P 2020.
- Eric Verheul, **Christopher Hicks**, and Flavio D. Garcia. IFAL: Issue First Activate Later Certificates for V2X. *In IEEE European Symposium on Security and Privacy (Euro S&P)* 2019.
- **Christopher Hicks**, Flavio Garcia, and David Oswald. Dismantling the AUT64 Automotive Cipher. *In IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES)* 2018.

Teaching and Peer Review

- Reviewed manuscripts for ESORICS 2019, Africacrypt 2019 and IEEE Transactions on Information Forensics & Security 2020. 2019
- Postgraduate Teaching Assistant (PGTA) for the masters-level *Cryptography* course at the University of Birmingham. I presented weekly tutorial lectures and marked the corresponding homework tasks. 2016 - 2019
- Additional PGTA experience in *Mathematical Techniques for Computer Science* and *Introduction to Computer Security*. 2015 - 2016

Awards and Scholarships

- Competitive L3-TRL 3.5 year PhD scholarship at an ACE-CSR university.
- Student with the highest overall marks in both third and fourth years of MEng degree.

Selected Talks

- Presented "Issue First Activate Later (IFAL) certificates for V2X" at Euro S&P 2019. 2019
- Presented "Dismantling the AUT64 automotive cipher" to an audience of 600 at CHES 2018. 2018

Key Research Interests

- Security and Privacy
- Machine Learning
- Authentication
- Key Management
- Reverse Engineering
- Cryptanalysis

Research Experience

PhD Computer Science, University of Birmingham 2015-2019

Thesis: *Cryptographic key management for the vehicles of tomorrow.*

- Based on the latest European standards for Vehicle-to-Everything (V2X) communication and in collaboration with Radboud University Nijmegen, I proposed a novel certificate issuance mechanism that improves trust for vehicles with limited connectivity. Our scheme, which both allows for pseudonym pre-issuance and removes the need for conventional revocation lists, is evidenced by both a proof in the formal setting and a benchmark implementation written in C++.
- To address the issue of ensuring privacy despite colluding certificate authorities in V2X, I proposed a new security architecture and formalisation that reconciles the strong privacy guarantees of Direct Anonymous Attestation (DAA) based on secure hardware with the efficiency, standards-compliance and centralised revocation necessary for safety-critical inter-vehicle messaging.
- Reverse engineered a previously unstudied vehicle immobiliser system and discovered several flaws in the proprietary cryptography, protocol and implementation. I developed new attacks based on integral cryptanalysis that enable, in certain configurations, the full 120 bit secret key to be recovered in milliseconds using a standard laptop.

Master's Project, University of Birmingham 2015

Thesis: *Gaining insight into virtualised-host disk activity.*

- I developed a tool for introspecting the NTFS storage behaviour of virtualised-hosts running on the Xen hypervisor. My tool was able to identify when sensitive financial information was written to disk by a host, notifying the hypervisor of alarming activity.

International Summer School Attendance

- Research Institute for Secure Hardware and Embedded Systems (RISE) School*, UK*, 2018.
- School on the Computer Aided Analysis of Cryptographic Protocols*, Romania*, 2016.
- 15th International School on Foundations of Security Analysis and Design (FOSAD)*, Italy*, 2015.

Additonal Interests

- **Coursera:** *Cryptography I* and *Machine Learning* by Stanford University, *Neural Networks and Deep Learning* and *Improving Deep Neural Networks* by deeplearning.ai
- **CTFs:** AFNOM hacking club member, Hack The Box (HTB), OverTheWire.

Key Technologies and Languages

- **Programming languages:** Python, C, C++, Bash, Java, MATLAB, LabVIEW, VHDL and SQL.
- **Libraries:** NumPy, OpenSSL, Crypto++, matplotlib and TensorFlow.
- **Technologies:** Authentication, protocols, key management, embedded systems, distributed systems, Linux, virtualisation, TPM and SGX secure hardware, exploitation, penetration testing, reverse engineering using IDA Pro, Wireshark packet inspection, software profiling, source code control and LaTeX.

Referees

- **Professor Flavio D. Garcia**, PhD Supervisor, School of Computer Science, University of Birmingham, f.garcia@bham.ac.uk, 0121 414 4794.
- **Professor Mark Ryan**, Internal examiner, Lead for the Centre of Security and Privacy, School of Computer Science, University of Birmingham, m.d.ryan@cs.bham.ac.uk, 0121 414 7361.