CURRICULUM VITAE

Personal information

Name, Surname:	Ioana, Boureanu (married Carlson)		
Date of birth:	24.01.1985	Sex:	F
Nationality:	Romanian		
Researcher unique identifier(s) (ORCID, Researcher ID etc.):	0000-0001-5864-777X		
URL for personal website (if case):	http://people.itcarlson.com/ioana		

Education

Year	Faculty/department - University/institution - Country
2011 (dissertation defended)	Ph.D. in Computing , Imperial College London, UK *Title:* "Model checking security protocols : a multiagent system approach"

Positions - current and previous

(*Academic sector/research institutes/industrial sector/public sector/other)*

Year	Job title – Employer - Country
08/2022– Present	**Professor in Secure Systems**, Computer Science Research Centre, University of Surrey, UK
06/2023 – Present	**Director of Surrey Centre of Cyber Security (SCCS),** www.surrey.ac.uk/surrey-centre-cyber-security, recognised as an Academic Centre for Cyber Security Education (ACE-CSR) by UK's Government – the National Cyber Security Centre www.ncsc.gov.uk/
11/2017-08/2022	**Lecturer** (until 08/2019) & **Senior Lecturer in Secure Systems** (from 08/2019) Department of Computer Science, University of Surrey, UK
11/2019-present	**Visiting Senior Researcher,** Laboratoire d'Informatique, de Modélisation et d'Optimisation des Systèmes, Universite d'Auvergne, France
06/2015-06/2017	**H2020 Marie Skłodowska-Curie Fellow,** Dept. of Computing, Imperial College London + Dept. of Computer Science, University of Surrey, UK
04/2014-05/2015	**Security Architect**, Akamai Technologies Limited, London, UK
08/2013-04/2014	**Professor of Information Security**, University of Applied Sciences, Western Switzerland (HEIG-VD), Switzerland
01/2011-08/2013	**Deputy Director of Laboratory of Security & Cryptography Laboratory** (from 08/2012) & **Lecturer in Cryptography and Security** (from 08/2012) & **Research Associate in Security & Cryptography,** School of Computer and Communication Sciences, Ecole Polytechnique Federale de Lausanne (EPFL), Switzerland

Career breaks (if case)

Year	Reason

2013-2015	Worked in industry as a security and cryptography consultant for Akamai Technology Limited

Project management experience

(*Academic sector/research institutes/industrial sector/public sector/other. Please list the most relevant.)*

Year	Project title - Role – Funder – Budget – link to project webpage
06/2023 – Present	**Director of Surrey Centre of Cyber Security (SCCS),** www.surrey.ac.uk/surrey-centre-cyber-security, recognised as an Academic Centre for Cyber Security Education (ACE-CSR) by UK's Government – the National Cyber Security Centre www.ncsc.gov.uk/
06/2012-08/2013	**Deputy Director of Laboratory of Security & Cryptography Laboratory,** School of Computer and Communication Sciences, Ecole Polytechnique Federale de Lausanne (EPFL), Switzerland
2014-present in the last 10 years, Ioana has been PI (principal investigator) or Co-I (co-investigator) on **18 grants**	**[**g1] Funder – NCSC. Title: "Eskmarald: Enhanced Security of the AKMA (Authentication and Key Management for Application) Service in the context of AKMA-based Applications & Deployments " (**PI**; GBP310,000; 11/2022 – 11/2024) [g2] Funder – NCSC. Title: "TrainCyri: Gamified Training on Cyber Risk with Assessment of Cybersecurity Awareness and Psychological Fears" (**PI;** GBP60,000; 10/2022 – 04/2023) [g3] Funder – the French Government, under the "International Strategy CAP 20-25, Wide Open World" (https://cap2025.fr/ en/international/cap-20-25-international-strategy). Visiting research position in France (**PI**; the award + up to GBP 6,000 of travel expenses per year; partner: University of Auvergne; awarded five times, 2019 - 2024) [g4] Funder – the Royal Society. A Royal Society & Leverhulme Trust Senior Research Fellowship. Title: "PrivAs – Privacy Analyser Using Applied Logics" (**PI**; GBP12,150, pays for a teaching replacement for 1 semester; 10/2021 – 05/2022) [g5] Funder – EPSRC IAA (Impact acceleration account). Title: "TPM Keys in the WebAuthn Demonstrator" (**Co-I**, GBP 44,000; 02/2021 – 06/2021) [g6] Funder – EPSRC. Title: "AutoPaSS: Automatic Verification of Complex Privacy Requirements in Unbounded-Size Secure Systems" (**PI**; GBP303,000; partners: Thales, Vector; 04/2019 – 12/2022) [g7] Funder – EPSRC + NCSC (UK's National Cyber Security Centre, part of GCHQ), under UK's Research Institute for Secure Hardware and Embedded Systems (RISE). Title: "TimeTrust: Robust Timing via Hardware Roots of Trust and Non-standard Hardware" (**PI**; GBP300,000; partners: Univ. of Birmingham, Visa, Mastercard, HP Labs, 10/2010 – 02/2011, Consult Hyperion; 04/2019 – 08/2022) [g8] Funder – NCSC + BT. Title: "5GTech-Sec: Security Analysis of Systems using Emerging 5G Technologies" , a 4-year PhD studentship (**PI**; GBP145,000; partner: BT – in-kind contribution GBP298,000; 03/2019 – 12/2024) [g9] Funder – the Royal Society. A Royal Society International Exchange Award. Title: "DeCoS: Decidability and Complexity of Security Analysis for Arbitrarily-Large Secure Systems", (**PI**; GBP6,000; partner: The Institute of Mathematical Sciences (IMSc) Chennai, India, Co-I: Prof Jam Ramanujam; 03/2019 – 12/2022) [g10] Funder – Research England. An accelerator & implementation plan (**PI**; GBP10,000; 03/2019 – 08/2019)

	[g11] Funder – NCSC. Title: "PayPhy: Securing contactless-card payments via physical-layer measure", a 3.5-year PhD studentship (**PI**; GBP114,000; partner: Consult Hyperion, 10/2018 –03/20221) [g12] Funder – NCSC: Title: "Implementation and Performance Evaluation of Authentication Protocols and Cryptographic Algorithms in the 5GIC Testbed of the University of Surrey" (**Co-I**; GBP110,000; 03/2018 –10/2018) [g13] Funder – Industry-supported fund for the 8th International Workshop on Cryptography, Robustness, and Provably, Secure Schemes for Female Young Researchers "CrossFyre" 2018, at Univ. of Surrey (**PI**, GBP 10,000, 2018) [g14] Funder – Reseau Francilien en Sciences Informatiques (RFSI), under https://dim-rfsi.fr/projets/emergents. A collaborative research-visits' project. Title: "Collaborative Project MALEVePS", (**Co-I**; EUR 20,000; partners: Univ. de Paris 12, and Univ. Paris Evry; 2017–2018) [g15] Funder – NCSC. A grant to support the purchase of equipment for applied security research and teaching demonstration in the area of NFC (**PI**; GBP8,000; granted in 02/2017) [g16] Funder – EU Commission. A H2020 MSCA fellowship. Title: "Logic-based Verification of Privacy-Preservation in Europe's 2020 ICT", (**PI;** EUR200,000; 06/2015–06/2017) [g17] Funder – Swiss National Foundation. A grant-support to co-organise the 12th International Conference on Applied Cryptography and Network Security (ACNS 2014) (**PI**; CHF 4,000; granted in 01/2014) [g18] Funder – EU Commission. H2020 COST Action IC1403. Title "Cryptanalysis of ubiquitous computing systems" – Cryptacus (**Co-I** country-representative for Switzerland; 20 partners; full action cca. EUR 48M, 05/2014 -10/2018)

Other relevant professional experiences

Year	Description - Role
2-14-present	**PC Member in Top Venues -- Selection:** •*2024*: IEEE S&P, ACM CCS, AAMAS (senior PC); •*2023 -2019*: IEEE S&P, Usenix, IEEE Euro S&P, ACM CCS (*2023 only*), AAAI, IJCAI, Financial Crypto, ACM WiSec **Journals' Editorship:** Associate Editor of Journal of Computer Security, since 2022 **Co-Chairing-- Selection)** • IEEE S&P, Associate Chair, 2025; • General Co-Chair of ACM Conference on Security and Privacy in Wireless and Mobile Network (ACM WiSeC), 2023, UK; • General & Programme Co-Chair of International Conference on Applied Cryptography and Network Security (ACNS) 2014, Switzerland; • in the Steering Committee of the International Workshop on Cryptography, Robustness, and Provably Secure Schemes for Female Young Researchers (CrossFyre) since 2018.

2019-present	Active member of the Technical Committee (TC) and the Security Working Group (SWG) of the LoRa Alliance.
2021-present	Member of ISO/IEC Working group WG8, Task Force 2, and **editor of an ISO/IEC amendment**; see here: https://bit.ly/3ZyygFZ
2019-present	**Creator an international network and seminar series** on "Formal Methods for Security" (VFM-SEC); see https://fmsec.github.io or see https://uk-sps.org/
2022-present	Reviewer of Funding Policy for Cybersecurity Research for the Flemish Government, 2023
2022-present	Reviewer of Formal Proofs for Cybersecurity of the Swiss E-voting, 2022-2023, e.g., https://bit.ly/46aXzQf
2021-present	Advisory board member of a UK local-government organisation in the cyber-security sector, called **Surrey Cyber Security Cluster** (see https://surreycyber.com/)

Track record of the last 10 years

See patents, and other aspects in the narrative part.

Papers

[p1] F. Rajaona, I. Boureanu, J. Ramanujam and S. Wesemeyer, "Epistemic Model Checking for Privacy", the 2024 IEEE Computer Security Foundations Symposium (CSF), to appear in 2024

[p2] R. Miller, I. Boureanu, S. Wesemeyer, H. Zope, Z. Sun, "Systematic Improvement of Access-Stratum Security in Mobile Networks", the 8th IEEE European Symposium on Security & Privacy (EuroSnP), 2023

[p3] K. Budykho, I. Boureanu, S. Wesemeyer, F. Rajaona, D. Romero, M. Lewis, Y. Rahulan, S. Schneider, "Fine-Grained Trackability in Protocol Executions", Network and Distributed System Security Symposium (NDSS) 2023,

[p4] F. Belardinelli, I. Boureanu, V. Malvone and F. Rajaona, "Automatically Verifying Expressive Epistemic Properties of Programs", AAAI 2023, 2023

[p5] F. Rajaona, I. Boureanu, V. Malvone and F. Belardinelli, "Program Semantics and Verification Technique for AI-centred Programs", the 25th Symposium on Formal Methods (FM), 2023; **Won best-paper award.**

[p6] O. Blazy, I. Boureanu, C. Onete, P. Lafourcade, L. Robert, "How fast do you heal? A taxonomy for post-compromise security in secure-channel establishment", at the 32nd USENIX Security Symposium (USENIX Security), 2023

[p7] A. Radu, T. Chothia, C. Newton, I. Boureanu, L. Chen, "Practical EMV Relay Protection", at the 2022 IEEE Symposium on Security and Privacy (IEEE S & P), 2022)

[p8] Boureanu, C. Dragan, F. Dupressoir, D. Gerault, P. Lafourcade, "Precise and Mechanised Models and Proofs for Distance-Bounding", at the 34th IEEE Computer Security Foundations Symposium (CSF 2021)

[p9] I. Boureanu, T. Chothia, A. Debant, S. Delaune, "Security Analysis and Implementation of Relay-Resistant Contactless Payments", at the 27th ACM Conference on Computer and Communications Security (ACM CCS 2020)

[p10] I. Boureanu, P. Kouvaros , A. Lomuscio, "Verifying Security Properties in Unbounded Multiagent Systems", 15th International Conference on Autonomous Agents and Multi-Agent systems (AAMAS), 2016

[p11] I. Boureanu, M. Ohkubo, S. Vaudenay, "The Limits of Composable Crypto with Transferrable Setup Devices", the 10th ACM Symposium on Information, Computer and Communications Security (ASIACCS'15), 2015

[p12] I. Boureanu, A. Mitrokotsa, S. Vaudenay, "Practical & Provably Secure Distance-Bounding", Journal of Computer Security, volume 23, pages 229 --257, 2015

Narrative CV

1. Top Publications & Successful Grants Lead on Formal Treatments of Security & Privacy

On Formal Security for Systems with Time and Distance. Ioana Boureanu put forward the first ever cryptographically-secure designs for communication systems based on distance and time (e.g., [p12]). Formal cryptographic proofs therein were notoriously hard since physicality was not considered in security, *analogously to how socio-technicality will be tackled by DEM*. Moreover, the TimeTrust [g7] project on these topics, lead by Ioana Boureanu, published exclusively and systematically in places CORE-ranked A and A* , over the 3 years: e.g., ACM CCS, IEEE S&P.

On Provably Security of Homogenous Systems. LoRaWAN is the de-facto technology behind IoT (Internet of Things) networks. The thorny problems in formal security for IoT was linked to replication and homogeneity in these systems; grant [g6], lead by Ioana Boureanu, dealt with this. In [p2], published at the top NDSS conference and a precursor of this paper published at IEEE Euro S&P 2020, we produced what the Lora Alliance recognises as the most faithful formal modelling of the security protocol used by their devices to (re)join the LoRa network. Not only did we find insecurities and worked with the LoRa Alliance towards patches, but **these formally-found security improvements have been adopted in the 1.1 and 1.2 versions of the LoRA specifications.**

On Security-Verification with MAS-inspired Methods. In her PhD, Ioana Boureanu pioneered *automatic* verification of security protocols using multi-agent systems logics. She continued to be active in this area via top-tier publications (e.g., [p10]). During her fellowship [g4], this was extended towards privacy analysis, leading to **recent, top papers [p4,p5], with [p5] wining best-paper award.**

2. Media Coverages. An **attack against ApplePay and Visa, found in TimeTrust [g7], made the front pages of all major media outlets** over several days, with multiple interviews on radio and TV, in total of over 900 coverages in 10 days; see e.g., https://www.bbc.co.uk/news/technology-58719891. One can find more about this attack in [p7] or here: https://practical_emv.gitlab.io/ , including **Ioana Boureanu demo-ing live on stage this attack.**

3. Patents & Standardisation. Ioana Boureanu's work in secure constructions for time and distance resulted in the first patent on authenticated relay-protection (US Patent number: 9930523), in 2015.

- TimeTrust [g7] proposed a version **ISO/IEC14443 provably secure against relays**; this is now under standardisation at ISO/IEC, and Ioana Boureanu is the project editor for this ISO amendment; see here: https://bit.ly/3ZyygFZ

4. Top Industrial Partners & Impact. Both EPSRC/ GCHQ-funded projects lead by Ioana Boureanu (see below) are in collaboration with top industrial players: Mastercard, Visa, HP Labs, Consult Hyperion, Thales, Vector, BT, etc.

– For a version of the aforesaid "**ApplePay-Visa attack" found also with formal methods, Google paid us a $10,000 bounty**. The ApplePay-Visa attack also lead to SumUp terminals no longer take over-the-limit contactless payments from their readers. With Consult Hyperion, we also implemented provably more-secure, backwards-compatible versions of Mastercard's contactless protocol in [p9]; Mastercard is considering both, for different reasons. Indeed, a **senior director from Visa says**: " [...] **I highly rate Ioana Boureanu and her team's delivery from the TimeTrust initiative,** *the team has identified and demonstrated the practicality of [...] man-in-the-middle attacks in modern EMV contactless card and mobile payment systems, .. created a very positive push forward to the industry on improving the technology in EMV contactless... "* ; full statement here: https://bit.ly/3JHHkiS .

- On LoRa, Ioana Boureanu worked with a company called NCC Group to extend one of their tools, used for the analysis of LoRaWAN traffic, w.r.t. our aforesaid privacy-related attacks [p2]. NCC Group uses this tool for their customers and it is now also released open source.

Peer recognition

(1) Prizes, Awards, Fellowships

- Co-receiver of a **SquareUP Bounty** for finding security flaws in Square Terminal, $20000, 2024
- Univ. of Surrey's Faculty of Engineering and Physical Sciences, **Vice-chancellor Excellence Award - Teacher of the Year**, 2023
- **Royal Society Leverhulme Trust Senior Research Fellow,** 10/2021 -- **31/05/2022**
- Co-receiver of a **Google Bounty** for finding security flaws in Google Pay, $10000, 2021
- **Recognised IEEE Services** by the IEEE (Institute of Electrical and Electronics Engineers), incl. free membership, 2021
- **Fellow of UK's Higher Education Academy,** 2019
- **Horizon 2020 Marie Skłodowska-Curie (MSCA) Fellow**, 2015 -2017
- Best Akamai EMEA Cybersecurity Consultant and **Akamai University Cybersecurity Trainer**, Akamai, 2015
- **Dean's Prize for Research**, by the Dean for School of Engineering, EPFL, Switzerland, 2013

(2) Invited Speaker --*Selection.* Full details at http://people.itcarlson.com/ioana/researchInterests.html

[i1] Invited Speaker at Seminar Series of the Institute of Mathematical Science Chennai (IMSc), Talk: "Symbolic Verification of Epistemic Properties in Programs", Chennai, India, October 2022

[i2] Invited Speaker at NCSC's Conference on Safety, Security, and Verification, Talk: "Proximity-centred Security and Safety with Corrupted Verifiers and Mobile Parties", UK, September 2021

[i3] Invited Speaker at the UK-SPS series, Talk: "Practical and Formal Analysis Security of Contactless Mobile Payments", (see https://www.youtube.com/watch?v=3wzkd07A5ZU), December 2021

[i4] Invited Speaker at "Romanian Cryptology Days" (RCD), Talk: "Better Security with Hardware Roots of Trust", Bucharest, Romania, September 2019

Ioana, Boureanu (married Carlson)