Dr. Leonardo Aniello

Curriculum Vitae

(November 2023)

Personal information

Email: _____ _____

Nationality: Italian

Mother tongue: Italian **Other languages:** English (FCE: Grade A, Council of Europe Level B2)

Current positions

- Associate Professor in Cyber Security at the University of Southampton (southampton.ac.uk), Department of Electronic and Computer Science (ecs.soton.ac.uk). [Since March 2022]
- Co-founder and Chief Technology Officer (CTO) at LZero Analytics (https://www.lzeroanalytics.com/) [Since March 2023]

Activities

Visiting Researcher

- Visiting Researcher at the Cyber Security Research Group (cyber.ecs.soton.ac.uk) of the University of Southampton (September 1st – December 31st, 2017) (southampton.ac.uk)
- Visiting Researcher at Department of Computer Science at Royal Hollow University of London (May 15th - June 4th, 2013) (www.rhul.ac.uk/computerscience)
- Visiting Researcher at IBM Research Lab in Haifa (February 1st - April 30th, 2012) (www.haifa.ibm.com)

PhD Schools

- SDCI 2012 - Winter School: Hot Topics in Secure and Dependable Computing for Critical Infrastructures (Cortina d'Ampezzo, January 15th-19th 2012) (www.dis.uniroma1.it/~dotslcci/)
- METIS - CTDS'2011, How to Secure Distributed Systems? (Marrakech, April 27th-29th 2011) (www.notere-conf.org/METIS2011/)

Participation to conferences/workshops

- NCSC Workshop on Safety v Security: Challenges and Applications in the Cyber Security Era (Southampton, January 14th, 2019) (https://cyber.southampton.ac.uk/ncsc-workshop-on-safety-v-security)
- Distributed Ledger Technology Workshop (Perugia, February 1st, 2018) (dmi.unipg.it/DLTWorkshop/dlt2018.html)
- Project Final Conference "Innovation, Cybersecurity and Efficiency: a new European Platform of Securely Federated Cloud Services" (Rome, November 8th 2017) (sunfishproject.eu/sunfish-final-conference)
- NET FUTURES 2017 - Conference on internet, the economy and society in 2027 (Brussels, June 28th-29th 2017) (netfuturesconference.eu)
- ITASEC 2017 - Italian Conference on Cybersecurity (Venice, January 17th-20th 2017) (itasec17.dais.unive.it)
- NGMAST 2016 – The 10th International Conference on Next Generation Mobile Applications, Security and Technologies (Cardiff, August 24th-26th 2016) (www.ngmast.com)
- SEDA 2016 – The 5th International Conference in Software Engineering for Defense Applications (Rome, May 10th 2016) (www.sedaconference.eu/2016)
- NETYS 2014 – The 2nd International Conference on NETworked sYStems (Marrakech, May 15th-17th 2014) (www.netys.net)
- SRDS 2013 – The 32nd International Symposium on Reliable Distributed Systems (Braga, October 1st-3rd 2013) (srds.di.uminho.pt)
- ACM SAC 2013 - The 28th ACM Symposium On Applied Computing (Coimbra, March 18th-22nd 2013) (www.acm.org/conferences/sac/sac2013)
- OPODIS 2012 – The 16th International Conference On Principles Of DIstributed Systems (Rome, December 17th-20th 2012) (opodis2012.dis.uniroma1.it)
- SAFECOMP 2011 - The 30th International Conference on Computer Safety, Reliability and Security (Naples, September 19th-22nd 2011) (www.safecomp2011.unina.it)

Invited Speaker

- Cyber Workshop @University of Southampton (June 15th, 2023) – talk: "Tutorial on Blockchain"
- Blockchain 101 Course (https://github.com/soton-dsoc/blockchain-101/tree/main) @University of Southampton organised by the Decentralised Society (https://soton-dsoc.org/) – lecture on "Cryptographic Primitives & Data Structures for Blockchain" (November 23rd, 2022)
- Blockchain and Supply Chain Research Group (BSCRG) research seminar @University of Southampton (July 12th, 2022) – talk: "Towards Counterfeit Mitigation in Integrated Circuit Supply Chains using Blockchain"
- SUCSS (Southampton University Cyber Security Society) guest talk: ECS and DSoc (Southampton, November 24th, 2021) (https://www.facebook.com/events/587746212558172/) – talk: "Permissioned vs Permissionless Blockchains"
- Lecture for the British Council "Knowledge is GREAT" Lecture Series (Online, August 26th, 2021) (https://www.youtube.com/watch?v=rktcQlMPkCA&ab_channel=britishcouncilsg) – talk: "Enhancing Cyber Security via AI and BigData"
- Cyber Security Virtual Conference 2021 (Online, May 26th-27th, 2021) (https://www.ictsecuritymagazine.com/cyber-security-virtual-conference-2021/) – talk: "Consortium Blockchain to Mitigate Counterfeit in Integrated Circuit Supply Chain" (title in Italian: "Consortium blockchain per Mitigare il Rischio di Contraffazione nelle Supply Chain di Circuiti Integrati")
- Lecture for the "British Council webinar" (Online, August 4th, 2020) (https://th.registration.study-uk.britishcouncil.org/webinar-computer-sciences-degrees-specialisations-and-skills-in-ai-cyber-security-big-data) – talk: "Computer Science degrees: Specialisations and skills for careers in AI, Cyber Security, Big Data"
- Lecture for the "Computer and Network Security" MSc Course (Padua, October 31st, 2019) – talk: "An Overview on Machine Learning for Malware Analysis"
- International Summer School on "Blockchain and Cryptocurrencies Security" (Padua, June 24th-28th 2019) (https://spritz.math.unipd.it/events/2019/PIU2019/PagesOutput/BCS/) – talk: "Efficient Blockchain-based Platforms to Secure Multi-Party Systems"
- Distributed Ledger Technology Workshop (Perugia, February 1st 2018) (dmi.unipg.it/DLTWorkshop/dlt2018.html) – talk: "Blockchain-based Database for Multi-party Systems" (https://www.youtube.com/watch?v=J4DjhvgW_O0)

Publications

Awards

- ACM international conference on Distributed event-based systems (DEBS) – DEBS 10 Years Time Award 2023 for: Aniello, L., Baldoni, R. and Querzoni, L. Adaptive online scheduling in storm (DEBS 2013).

Conference proceedings

- Thorburn, R., Sassone, V., Fathabadi, A.S., Aniello, L., Butler, M., Dghaym, D. and Hoang, T.S., 2022, October. A lightweight approach to the concurrent use and integration of SysML and formal methods in systems design. In Proceedings of the 25th International Conference on Model Driven Engineering Languages and Systems: Companion Proceedings (pp. 83-84).
- De Angelis, S., Zanfino, G., Aniello, L., Lombardi, F. and Sassone, V., 2022. Evaluating Blockchain Systems: A Comprehensive Study of Security and Dependability Attributes. Proceedings http://ceur-ws. org ISSN, 1613, p.0073.
- Dghaym, D., Hoang, T.S., Butler, M., Hu, R., Aniello, L. and Sassone, V., 2021, May. Verifying system-level security of a smart ballot box. In International Conference on Rigorous State-Based Methods (pp. 34-49). Cham: Springer International Publishing.
- Fadhel, N., Lombardi, F., Aniello, L., Margheri, A. and Sassone, V., 2019. Towards a semantic modelling for threat analysis of IoT applications: A case study on transactive energy. IET Digital Library
- Lombardi, F., Aniello, L., De Angelis, S., Margheri, A. and Sassone, V., 2018. A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids. IET Digital Library
- Aniello, L., Baldoni, R. and Lombardi, F., 2018. A blockchain-based solution for enabling log-based resolution of disputes in multi-party transactions. In Proceedings of 5th International Conference in Software Engineering for Defence Applications: SEDA 2016 5 (pp. 53-58). Springer International Publishing.
- De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A. and Sassone, V., 2018. PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain. In CEUR workshop proceedings (Vol. 2058). CEUR-WS. Second Italian Conference on Cybersecurity (ITASEC).
- Pitolli, G., Aniello, L., Laurenza, G., Querzoni, L. and Baldoni, R., 2017, October. Malware family identification with BIRCH clustering. In 2017 International Carnahan conference on security technology (ICCST) (pp. 1-6). IEEE.
- Massarelli, L., Aniello, L., Ciccotelli, C., Querzoni, L., Ucci, D. and Baldoni, R., 2017, October. Android malware family classification based on resource consumption over time. In 2017 12th International Conference on Malicious and Unwanted Software (MALWARE) (pp. 31-38). IEEE.

- Angelini, M., Aniello, L., Lenti, S., Santucci, G. and Ucci, D., 2017, October. The goods, the bads and the uglies: Supporting decisions in malware detection through visual analytics. In 2017 IEEE Symposium on Visualization for Cyber Security (VizSec) (pp. 1-8). IEEE.
- Aniello, L., Baldoni, R., Gaetani, E., Lombardi, F., Margheri, A. and Sassone, V., 2017, September. A prototype evaluation of a tamper-resistant high performance blockchain-based transaction log for a distributed database. In 2017 13th European Dependable Computing Conference (EDCC) (pp. 151-154). IEEE.
- Ucci, D., Aniello, L. and Baldoni, R., 2017, March. Share a pie? Privacy-Preserving Knowledge Base Export through Count-min Sketches. In Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy (pp. 95-106).
- Laurenza, G., Aniello, L., Lazzeretti, R. and Baldoni, R., 2017. Malware triage based on static features and public apt reports. In Cyber Security Cryptography and Machine Learning: First International Conference, CSCML 2017, Beer-Sheva, Israel, June 29-30, 2017, Proceedings 1 (pp. 288-305). Springer International Publishing.
- Gaetani, E., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A. and Sassone, V., 2017. Blockchain-based database to ensure data integrity in cloud computing environments. First Italian Conference on Cybersecurity (ITASEC)
- Shehu, Z., Ciccotelli, C., Ucci, D., Aniello, L. and Baldoni, R., 2016, August. Towards the usage of invariant-based app behavioral fingerprinting for the detection of obfuscated versions of known malware. In 2016 10th International Conference on Next Generation Mobile Applications, Security and Technologies (NGMAST) (pp. 121-126). IEEE.
- Aniello, L., Ciccotelli, C., Cinque, M., Frattini, F., Querzoni, L. and Russo, S., 2016. Automatic invariant selection for online anomaly detection. In Computer Safety, Reliability, and Security: 35th International Conference, SAFECOMP 2016, Trondheim, Norway, September 21-23, 2016, Proceedings 35 (pp. 172-183). Springer International Publishing.
- Ciccotelli, C., Aniello, L., Lombardi, F., Montanari, L., Querzoni, L. and Baldoni, R., 2015, November. Nirvana: A non-intrusive black-box monitoring framework for rack-level fault detection. In 2015 IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC) (pp. 11-20). IEEE.
- Aniello, L., Baldoni, R., Ciccotelli, C., Di Luna, G.A., Frontali, F. and Querzoni, L., 2014, May. The overlay scan attack: Inferring topologies of distributed pub/sub systems through broker saturation. In Proceedings of the 8th ACM International Conference on Distributed Event-Based Systems (pp. 107-117).
- Heinze, T., Aniello, L., Querzoni, L. and Jerzak, Z., 2014, May. Cloud-based data stream processing. In Proceedings of the 8th ACM International Conference on Distributed Event-Based Systems (pp. 238-245).
- Aniello, L., Bonomi, S., Lombardi, F., Zelli, A. and Baldoni, R., 2014. An architecture for automatic scaling of replicated services. In Networked Systems: Second International Conference, NETYS 2014, Marrakech, Morocco, May 15-17, 2014. Revised Selected Papers (pp. 122-137). Springer International Publishing.
- Aniello, L., Baldoni, R. and Querzoni, L., 2013, June. Adaptive online scheduling in storm. In Proceedings of the 7th ACM international conference on Distributed event-based systems (pp. 207-218).
- Aniello, L., Querzoni, L. and Baldoni, R., 2013, March. Input data organization for batch processing in time window based computations. In Proceedings of the 28th Annual ACM Symposium on Applied Computing (pp. 363-370).
- Aniello, L., Di Luna, G.A., Lodi, G. and Baldoni, R., 2011, September. A collaborative event processing system for protection of critical infrastructures from cyber attacks. In International Conference on Computer Safety, Reliability, and Security (pp. 310-323). Berlin, Heidelberg: Springer Berlin Heidelberg.

Journals

- De Angelis, S., Lombardi, F., Zanfino, G., Aniello, L. and Sassone, V., 2023. Security and dependability analysis of blockchain systems in partially synchronous networks with Byzantine faults. International Journal of Parallel, Emergent and Distributed Systems, pp.1-21.
- Amri, S.A., Aniello, L. and Sassone, V., 2023. A Review of Upgradeable Smart Contract Patterns based on OpenZeppelin Technique. The Journal of The British Blockchain Association.
- Aniello, L., Halak, B., Chai, P., Dhall, R., Mihalea, M. and Wilczynski, A., 2021. Anti-BlUFf: towards counterfeit mitigation in IC supply chains using blockchain and PUF. International Journal of Information Security, 20, pp.445-460.
- Pitolli, G., Laurenza, G., Aniello, L., Querzoni, L. and Baldoni, R., 2021. MalFamAware: automatic family identification and malware classification through online clustering. International Journal of information security, 20, pp.371-386.
- Yilmaz, Y., Aniello, L. and Halak, B., 2021. ASSURE: A hardware-based security protocol for resource-constrained IoT systems. Journal of Hardware and Systems Security, 5(1), pp.1-18.
- O'Sullivan, M., Aniello, L. and Sassone, V., 2020. A methodology to select topology generators for ad hoc mesh network simulations. Journal of Communications, 15(10).
- Grigorescu, S., Cocias, T., Trasnea, B., Margheri, A., Lombardi, F. and Aniello, L., 2020. Cloud2edge elastic AI framework for prototyping and deployment of AI inference engines in autonomous vehicles. Sensors, 20(19), p.5450.
- Massarelli, L., Aniello, L., Ciccotelli, C., Querzoni, L., Ucci, D. and Baldoni, R., 2020. Androdfa: android malware classification based on resource consumption. Information, 11(6), p.326.

- Lombardi, F., Muti, A., Aniello, L., Baldoni, R., Bonomi, S. and Querzoni, L., 2019. Pascal: An architecture for proactive auto-scaling of distributed services. Future Generation Computer Systems, 98, pp.342-361.
- Ucci, D., Aniello, L. and Baldoni, R., 2019. Survey of machine learning techniques for malware analysis. Computers & Security, 81, pp.123-147.
- Elingiusti, M., Aniello, L., Querzoni, L. and Baldoni, R., 2018. Malware detection: A survey and taxonomy of current techniques. Cyber threat intelligence, pp.169-191.
- Lombardi, F., Aniello, L., Bonomi, S. and Querzoni, L., 2017. Elastic symbiotic scaling of operators and resources in stream processing systems. IEEE Transactions on Parallel and Distributed Systems, 29(3), pp.572-585.
- Aniello, L., Querzoni, L. and Baldoni, R., 2015. High frequency batch-oriented computations over large sliding time windows. Future Generation Computer Systems, 43, pp.1-11.
- Lodi, G., Aniello, L., Di Luna, G.A. and Baldoni, R., 2014. An event-based platform for collaborative threats detection and monitoring. Information Systems, 39, pp.175-195.

Workshops

- Gokkaya, B., Aniello, L., Karafili, E. and Halak, B., 2023. A methodology for cybersecurity risk assessment in supply chains. The 4th International Workshop on Cyber-Physical Security for Critical Infrastructures Protecstion, , The Hague, Netherlands. 28 Sep - 29 Oct 2023.
- De Angelis, S., Zanfino, G., Aniello, L., Lombardi, F. and Sassone, V., 2019, October. Blockchain and cybersecurity: a taxonomic approach. In Workshop. EU Blockchain Observatory.
- Laurenza, G., Ucci, D., Aniello, L. and Baldoni, R., 2016, June. An architecture for semi-automatic collaborative malware analysis for CIs. In 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W) (pp. 137-142). IEEE.
- Aniello, L., Bonomi, S., Breno, M. and Baldoni, R., 2013, September. Assessing data availability of Cassandra in the presence of non-accurate membership. In Proceedings of the 2nd International Workshop on Dependability Issues in Cloud Computing (pp. 1-6).
- Aniello, L., Lodi, G. and Baldoni, R., 2011, May. Inter-domain stealthy port scan detection through complex event processing. In Proceedings of the 13th European Workshop on Dependable Computing (pp. 67-72).

Book chapters

- Massarelli, L., Aniello, L., Ciccotelli, C., Querzoni, L., Ucci, D. and Baldoni, R., 2022. Machine Learning for Malware Analysis in Embedded Systems. In Machine Learning for Embedded System Security (pp. 127-153). Cham: Springer International Publishing.
- Aniello, L., Halak, B., Chai, P., Dhall, R., Mihalea, M. and Wilczynski, A., 2021. Securing hardware supply chain using PUF. Authentication of Embedded Devices: Technologies, Protocols and Emerging Applications, pp.115-144.
- Yilmaz, Y., Aniello, L. and Halak, B., 2021. ASSURE: A hardware-based security protocol for internet of things devices. Authentication of Embedded Devices: Technologies, Protocols and Emerging Applications, pp.55-87.
- Baldoni, R., De Nicola, R., Prinetto, P., Anglano, C., Aniello, L., Antinori, A., Armando, A., Aversa, R., Baldi, M., Barili, A. and Bartoletti, M., 2018. The future of Cybersecurity in Italy: Strategic focus area.
- Aniello, L., Armenia, S., Baldoni, R., D'Amore, F., Annachiara, D.P., Franchina, L., Montanari, L., Panetta, I.C., Querzoni, L., Giovanni, R.L. and Vincenzo, V.N., 2014. 2014 Italian Cyber Security Report. Consapevolezza della minaccia e capacità difensiva della Pubblica Amministrazione italiana.
- Aniello, L., Baldoni, R., Chockler, G., Laventman, G., Lodi, G. and Vigfusson, Y., 2012. Distributed attack detection using Agilis. Collaborative Financial Infrastructure Protection: Tools, Abstractions, and Middleware, pp.157-174.
- Marchetti, M., Colajanni, M., Messori, M., Aniello, L. and Vigfusson, Y., 2012. Cyber attacks on financial critical infrastructures. Collaborative Financial Infrastructure Protection: Tools, Abstractions, and Middleware, pp.53-82.
- Aniello, L., Di Luna, G.A., Lodi, G. and Baldoni, R., 2012. Collaborative inter-domain stealthy port scan detection using esper complex event processing. Collaborative Financial Infrastructure Protection: Tools, Abstractions, and Middleware, pp.139-156.

Technical reports

- L. Aniello, R. Baldoni, G. Chockler, G. Laventman, G. Lodi and Y. Vigfusson: *Agilis: An Internet-Scale Distributed Event Processing System for Collaborative Detection of Cyber Attacks* (MIDLAB TR 04/2011)

Appointments as Editor

- In February 2020, I've been appointed as an Associate Editor for the journal IET Cyber-Physical Systems: Theory & Applications.

Steering Committees

- 5th Distributed Ledger Technology Workshop (DLT 2023) (https://dltgroup.dmi.unipg.it/DLTWorkshop/dlt2023.html)
- 4th Distributed Ledger Technology Workshop (DLT 2022) (https://dlt2022.github.io/)
- Trends in Distributed Ledger Technologies (Trends in DLT 2021) (https://dltgroup.dmi.unipg.it/DLTWorkshop/dlt2021.html)
- 3rd Distributed Ledger Technology Workshop (DLT 2020) (http://www.dmi.unipg.it/DLTWorkshop/dlt2020.html)
- Second Distributed Ledger Technology Workshop (DLT 2019) (http://www.dmi.unipg.it/DLTWorkshop/dlt2019.html)
- Distributed Ledger Technology Workshop (DLT 2018) (https://www.dmi.unipg.it/DLTWorkshop/dlt2018.html)

Program Committees

- 5th Distributed Ledger Technology Workshop (DLT 2023) (https://dltgroup.dmi.unipg.it/DLTWorkshop/dlt2023.html)
- 5th Workshop on Machine Learning for Cybersecurity (MLCS2023) (https://mlcs.lasige.di.fc.ul.pt/)
- 4th Distributed Ledger Technology Workshop (DLT 2022) (https://dlt2022.github.io/)
- 4th Workshop on Machine Learning for Cybersecurity (MLCS2022) (https://mlcs.lasige.di.fc.ul.pt/2022/)
- 3rd Workshop on Machine Learning for Cybersecurity (MLCS2021) (https://mlcs.lasige.di.fc.ul.pt/2021/)
- 2nd Workshop on Machine Learning for Cybersecurity (MLCS2020) (https://mlcs.lasige.di.fc.ul.pt/2020/)
- WebSci'20 Workshop: Socio-technical AI systems for defence, cybercrime and cybersecurity (STAIDCC20) (https://www.southampton.ac.uk/~sem03/STAIDCC20.html)
- 3rd Distributed Ledger Technology Workshop (DLT 2020) (http://www.dmi.unipg.it/DLTWorkshop/dlt2020.html)
- Second Distributed Ledger Technology Workshop (DLT 2019) (http://www.dmi.unipg.it/DLTWorkshop/dlt2019.html)
- 21st International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2019) (https://sss2019.lip6.fr/symp/sss2019/)
- Workshop on Machine Learning for Cyber Security (MLCS 2019) (http://mlcs.lasige.di.fc.ul.pt/)
- First Workshop on Foundations and Applications of Distributed Ledgers (FADL 2018) (http://2018.discotec.org/cfp_w_fadl.html)
- Distributed Ledger Technology Workshop (DLT 2018) (https://www.dmi.unipg.it/DLTWorkshop/dlt2018.html)

Reviewer activities

Journals: IEEE Transactions on Parallel and Distributed Systems (TPDS), IEEE Transactions on Emerging Topics in Computing (TETC), Journal of Network and Computer Applications (JNCA), ACM Transactions on Modeling and Performance Evaluation of Computing Systems (TOMPSEC), IEEE Transactions on Dependable and Secure Computing (TDSC), IEEE Transactions on Computers (TC), Applied Soft Computing (WFSC), Future Generation Computer Systems (FGCS), Transactions on Information Forensics & Security (TIFS), Pervasive and Mobile Computing (PMC), Computer & Security (COSE), Distributed and Parallel Databases (DAPD), Transactions on Cyber-Physical Systems (TCPS), Transactions on Services Computing (TSC), IEEE Network Magazine, IEEE Network, Journal of Computer and System Sciences (JCSS)

Conferences: IEEE International Conference on Distributed Computing Systems (ICDCS), International Conference on Computer Safety, Reliability and Security (Safecomp), International Conference on Distributed Computing and Networking (ICDCN), ACM Symposium on Principles of Distributed Computing (PODC), ACM/IFIP/USENIX Middleware Conference (Middleware), ACM International Conference on Distributed Event-Based Systems (DEBS), Symposium on Reliable Distributed Systems (SRDS), International Information Security and Privacy Conference (IFIP SEC), International Carnahan Conference on Security Technology (ICSST), IEEE European Symposium on Security and Privacy (EuroS&P), International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS)

Workshops: Hot Topics in Cloud Data Processing (HotCDP), International Workshop on Big Data Analytics for Security (DASec), Distributed Ledger Technology Workshop (DLT), Workshop on Machine Learning for Cyber Security (MLCS)

Research projects

- As LZero Analytics CTO
  - *LZero - SSV Integration* (2023-24, $40k) (https://forum.ssv.network/t/ssv-x-lzero-analytics-grant-proposal-lzero-ssv-integration/1053) Grant funded by the SSV Network Governance (https://forum.ssv.network/) to develop a prototype that integrates the LZero technology with the SSV network.
- As Principal Investigator (PI)
  - *Leaping PANDA* (2021-2022, £60k), in partnership with Bristol-based company Riskaware and London-based CACI. This project aimed at integrating the PANDA technology with system developed under the OCCAM-RT and CyPrIAAn projects described below.
  - OCCAM-RT *Operational CyberspaCe Attack Modelling – Real-Time* (2020, £181k), in partnership with Bristol-based company Riskaware. OCCAM-RT aims to predict the next steps of evolving complex cyber-attacks in enterprise and military networks. It contributes to enhancing the UK's competitiveness in the defense field by proactively reacting to sophisticated cyber-attacks.
- As Co-Investigator (Co-I)
  - HD-Sec Holistic Design of Secure Systems on Capability Hardware (2020-2025, £1030k). This project aims to create formal methods to guide software design which will speed up the process and reduce errors and security vulnerabilities that could have been exploited by hackers. The University's research will be guided and validated by a range of security-critical industrial case studies with support from industrial partners Airbus, Arm, Altran, AWE, Galois, L3Harris, Northrop Grumman and Thales.
  - The Dragon Awakens: China's Rise in Artificial intelligence and Its National and International Security Implications (2019-2020, £7k). Grant provided by the University of Southampton (UoS) Web Science Institute (WSI) Research Stimulus Fund.
  - CyPrIAAn *Cyber Predictive Intelligence for Asset-based Analytics* (2019, £96k). This project proposes an approach to Cyber Predictive Intelligence for Asset-based Analytics (CyPrIAAn). It first creates Cyber Situational Awareness on a managed cyber infrastructure by integrating available Cyber Threat Intelligence with live security events. Then, building on a graph-based knowledge, CyPrIAAn prediction engine reasons on sequence-based adversary models and asset threats to generate predictions on possible next steps of the attacker, including what their target assets might be. Finally, it proactively proposes corresponding adjustments to cyber defences.
  - BlockIT *Blockchain-empowered Infrastructure for IoT* (2018-2019, £157k) (www.petrashub.org/portfolio-item/blockchain-empowered-infrastructure-for-iot-blockit). This project looks how blockchain, the technology behind decentralised systems such as Bitcoin, can be exploited to make the Infrastructure of IoT more resilient. This project will use blockchain to connect and coordinate IoT devices, enabling them to share their data with guarantees that their integrity will be preserved, and privacy protected.
- As Researcher
  - ATENA *Advanced Tools to assEss and mitigate the criticality of ICT compoNents and their dependencies over Critical InfrAstructure* (2016 - 2018) (www.atena-h2020.eu). EU project funded by Horizon2020 under the call dedicated to Digital Security. It aims at leveraging the outcomes from previous European Research activities, particularly from CockpitCI and MICIE EU projects and pushes at innovating them by exploiting advanced features of ICT and Cyber Security, to be tailored and validated in selected Use Cases (electricity, gas, water domains), in order to be adopted at operational industrial maturity level.
  - SUNFISH *SecUre iNFormatIon SHaring in federated heterogeneous private clouds* (2015 - 2017) (www.sunfishproject.eu). EU project funded by Horizon2020 under the call dedicated to ICT, particularly to Advanced Cloud Infrastructure and Services. SUNFISH will develop and integrate software enabling secure cloud federation as required by the Public Sector. The project will achieve this by meeting the specific challenges faced by the Maltese and Italian Ministries of Finance, as well as by the UK Regional Cyber Crime Units. Solutions developed will be exploited so as to be usable by other Public, and potentially also Private Sector, Players.
  - MYSE *Make Your System Elastic (2014)*. AWS Research Award worth $5k in AWS credits to carry out experiments on a framework for automatic scaling of replicated services.
  - TENACE *Protecting National Critical Infrastructures from Cyber Threats* (2013 - 2016) (www.dis.uniroma1.it/~tenace). Italian project funded by the Italian Ministry of Education, University and Research under the PRIN program. The overall goal is the protection of national Critical Infrastructures (CI) from cyber threats following a collaborative approach.
  - DOTS-LCCI *Dependable Off-The-Shelf based middleware systems for Large-scale Complex Critical Infrastructures* (2010 - 2012) (dots-lcci.prin.dis.unina.it). The project aims to define novel methods and techniques to assure and assess the resiliency level of current and future OTS-based LCCIs.
  - CoMiFin *Communication Middleware for Monitoring Financial Critical Infrastructure* (2008 - 2011) (www.comifin.eu). EU project funded by the Seventh Framework Programme (FP7). The research area is Critical Infrastructure Protection (CIP), focusing on the Critical Financial Infrastructure (CFI).

Research interests

Malware Analysis. Recent years have shown a dramatic increase in both number and sophistication of cyber-attacks. One of the main drivers of such trend is the appearance of more and more complex types of malware. I'm currently involved in the study of advanced techniques for malware analysis, specifically aimed at identifying similarities among malware to understand their genealogy and how they are likely to evolve over time.

Blockchain and Smart Contracts. Thanks to the success of Bitcoin and the promising emergence of Ethereum, novel technologies of blockchain and smart contracts are having a great momentum. Their fascinating properties about availability, integrity and decentralisation are stimulating the interest of main businesses, such as financial institutions and supply chains. I'm investigating blockchain-based systems with the aim of overcoming one the main drawbacks of these technologies, namely their performance in terms of transaction latency and throughput, while keeping their disrupting strengths, so that they could be used in many other practical scenarios.

IoT Security. Internet of Things (IoT) is a skyrocketing trend and is becoming more and more pervasive in everyone's daily life and in many diverse enterprise environments as well. Security of IoT devices and networks is one the major concerns on IoT evolution and spread. Within this wide research area, my specific topics of interest are vulnerability assessment and firmware analysis. Fingerprinting aims at discovering and recognising what devices, or what types of devices, are part a given network. From one hand, this can help network administrator to figure out the devices connected to her network, and, from the other hand, it sheds light on what information can be gathered by a malicious actor during a stealthy reconnaissance. Firmware analysis aims at simulating device execution to carry out dynamic analysis of its firmware. This enables key operations for the enhancement of IoT security, such as debugging, discovering bugs and errors, or runtime analysis of a suspicious appliance, without the need for running the firmware on the device itself. The huge variety of devices in terms of hardware, memory mapping and operating system makes it almost impossible to automate the setup of a virtual environment where to accurately simulate a specific device. This is commonly done manually and requires significant effort and expertise. The principal goal of this research activity is automating as much as possible the process of firmware extraction, memory mapping identification and consequent setup of the virtual environment where to simulate the device.

Privacy-preserving Data Sharing. Sharing data has become fundamental to have at disposal larger datasets to process and possibly mine more valuable information. Some of these data might be confidential, and proper privacy-preserving methods should be applied to enable their sharing. At the moment, I'm involved in researching how to use probabilistic data structures, specifically count-min sketches, to share data in such a way to add a controlled amount of noise to preserve the privacy of specific information.

Distributed Event Processing. The distribution of the computation allows parallelising the load to both achieve better performance and support the elaboration of massive data volumes, which is becoming a common requirement for today's BigData applications. My research activities in this field regard adaptive scheduling and scaling for frameworks supporting continuous queries, such as Apache Storm.

Intrusion Detection/Prevention Systems. As more and more systems are connected to the Internet, many security threats arise that would compromise both the operation of provided services and the reputation of service providers, as well as undermine finances and privacy of service customers. Such worrying situation requires the development of proper solutions for detecting, preventing and mitigating present cyber attacks.

Collaborative Environments. A collaborative environment is aimed to support interactions among distinct parties interested in achieving a common goal. A typical form of collaboration is the sharing of information, which entails relevant issues to address like interoperability and privacy. An interesting case study I have investigated regards the collaboration of different financial institutions for improving their own defenses against cyber attacks.

PhD Students

I'm currently supervising (as primary supervisor) or co-supervising (as secondary) the following PhD students:

- Asma Almosa (Ensuring decentralisation of layer 2 blockchains)
- Xinrui Liu (Efficient and secure blockchain-based databases)
- George Giamouridis (Blockchain-based DNS resolver)
- Xiaomeng Feng (Zero-trust architectures for Cyber-Physical Power Systems)
- Charles Hutchins (Protection of wireless sensor networks based on game theory)
- Betul Gokkaya (supply chai threat analysis)
- Gilberto Zanfino (blockchain privacy and scalability)
- Tadani Alyahya (IoT Fingerprinting)
- Thomas Albert John Murray (firmware security analysis)
- Michael O'Sullivan (network routing protocol inference)
- Jordan Charlie Luxton (blockchain scalability)

Past PhD students I supervised:

- Shaima Amur Mohamed Al Amri (smart contract life cycle)

Past PhD students I co-supervised:

- Christopher John Maidens (privacy-preserving data sharing for cyber threat intelligence analysis)
- Stefano De Angelis (performance and security of permissioned blockchain)
- Luca Massarelli (machine learning techniques for malware analysis)
- Giuseppe Laurenza (machine learning techniques for malware analysis)
- Federico Lombardi (automatic scaling of distributed systems)
- Daniele Ucci (privacy preserving techniques for data sharing)

Students' Theses

I've been the supervisor for the Third Year Individual Project of the following undergraduate students at the University of Southampton:

- Thomas Smith: Using Blockchain for Video Game Distribution (2023)
- Rubel Miah: Developing a cyber exposure assessment in supply chains (2023)
- Phillip Rucci: Motivating Password Best Practice Through Interactive Tools (2023)
- John-Martin Adams: Gamification to improve young adult's understanding of cyber security (2023)
- Jack Roberts: AndroBase: Customisable Android Malware Dataset Generation (2023)
- Til Jordan: Evaluation of speed, scalability and security of IOTA (2022)
- Tudor-Andrei Mavrodin: Detection and Isolation of rogue devices in a home network (2022)
- Robin Jones: Blockchain-based Electronic Healthcare Records Management (2022)
- Oscar McAuley: Combining Deep Transfer Learning and Image Synthesis Using GANs to Produce a More Robust Static Malware Classifier (2022)
- Nathan Dimond: Assessing the scalability of consensus protocols used in permissioned blockchain (2022)
- Justin Rauh: Detection of Malicious Ultrasonic Communication Through Neural Networks (2022)
- Joshua Wardle: Anonymous, End-to-End Encrypted Secure Messaging over the Ethereum Blockchain (2022)
- Benjamin Boyce: Using Generative Adversarial Networks To Create More Realistic Malware Instances (2022)
- Andreea Nechita: *The Machine is not Fooled Twice: Using Generative Adversarial Networks for Android Malware Detection* (2021)
- Jonathan Bartlett: *Malware detection using cloud-based online machine learning* (2021)
- Jeremy Westhead: *Application of machine learning techniques and symbolic execution for malware identification* (2021)
- Luke Washak: *Trust Based IoT Intrusion Detection System Using Machine Learning* (2021)
- Matthew Taylor: *Using Machine Learning to predict the future evolution of malware variants* (2021)
- Martin Kanev: *Android Ransomware Detection Using API Calls* (2021)
- Syed Fathir: *IoT Malware Detection based on Machine Learning and Network Traffic Analysis* (2020)
- Florence Marshall: *Evaluating Visibility and Privacy within a Blockchain Supply Chain Management System* (2020)
- Gabriel Airey: *Device Categorisation using Network Fingerprinting* (2020)
- Ruwaydah Widaad Raymode: *Extracting attack patterns from malware using Machine Learning techniques* (2020)
- Ori Lazar: *False Alarms removal in Video Motion and Changes Detection applied in live surveillance cameras* (2019)
- Ashley Lavery: *Electricity trading using Blockchain* (2019)
- Jack Bunce: *Evaluation of permissioned-blockchain security and performance when Byzantine nodes are introduced* (2019)
- Kirtan Amin: *Authenticating IoT Devices with Physically Unclonable Functions using a Blockchain Architecture* (2019)
- James Town: *Comparing various machine learning approaches for malware attribution of Advanced Persistent Threats* (2019)
- Spas Zahariev: *Blockchain for optimising food delivery services* (2019)
- Samuel Wild: *Smart home cybersecurity, an exploration of vulnerabilities in 'Internet-of-Things' (IOT) devices used in home networks* (2018)
- Jamie Sian: *The development of a layered Network Intrusion Detection and Prevention System for Industrial Control Systems* (2018)

I've been the supervisor for the Individual Project of the following Master students at the University of Southampton:

- Shivani Subramanian: Cyber Security in the Cosmos - An LSTM-driven intrusion detection system (2023)
- Jash Rele: Intrusion detection to detect grey hole attacks in network of drones (2023)
- Xinyi Zhang: Future malware variants prediction based on Generative Adversarial Network (2023)
- Mansour Alshehri: Blockchain Based Open Education Platform (2023)

- Lusine Tumoyan: Blockchain Integration with Internet of Vehicles for Long-Distance Inter-Vehicular Communication (2023)
- Rahul Ravi: Blockchain Based System Design Patterns (2022)
- Nasser Al-Aamri: Consortium Blockchain for Privacy-preserving in E-government (2022)
- Krishna Kumar Sharma: A Zero-Knowledge Proof based Blockchain System for University Consortium (2022)
- Keyi Zhu: Threat analysis in the smart home system (2022)
- Jomin Madassery Jacob: IoT Communication Middleware: a comparison between MQTT and Blockchain (2022)
- Daniel James Griffiths: Detecting Cybersquatting-Based Business Email Compromise (2022)
- Abel Kurian Oommen: Cyber Attack Generation in Virtual IoT Networks (2022)
- Pouria Toopchi: Machine-Driven Social Bot Identification (2021)
- George Giamouridis: BlockDom: A Blockchain Based DNS Protocol Based on Sharding Architecture (2021)
- Anastasios Dasyras: Malware Detection Using Memory Forensicsand Machine Learning (2021)
- Yang Li: *Blockchain-based System Design Patterns* (2020)
- Tinthid Jaikla: *A Blockchain-based Secure Communication Middleware for Microservices* (2020)
- Rishabh Saini: *Evading automated malware analysis by identifying real user systems & detecting human presence* (2020)
- Rhys Lockley: *Cyber security training in SMEs through cyber attack generation in virtualised environments* (2020)
- Petros Soutzis: *A system for predicting future malware variants* (2020)
- Mutaz Alajlan: *Cyber Attack Generation in Virtual Environments: A design to automate reconnaissance and penetration testing by using a CVE dictionary* (2020)
- Alexander Newton: *Future Malware Prediction Through Generative Modelling* (2020)
- Akin Eker: *Recognising and Detecting Activities in ADL Datasets* (2019)
- Oguz Kurt: *Machine Learning-based Attack Detection in IoT Environments* (2019)
- Dawid Malyszko: *An Advanced Face Analysis: The Development of the Kinship Verification Method and Model-Based Approach for Kin Face Generator* (2019)
- Zijian Wu: *Machine Learning-based Attack Detection in Enterprise Environments* (2019)
- Sandeep Mistry: *Malware Analysis Economics – Investigating optimal techniques with limited resources* (2019)

I've been the principal advisor for the theses of the following master students at "La Sapienza" University of Rome:

- Dr. Gabriele Vecchia: *Design and Implementation of a Blockchain-based e-Voting Mechanism for Democratic Governance in Cloud Federations* (2018)
- Dr. Stefano De Angelis: *Assessing Security and Performances of Consensus algorithms for Permissioned Blockchains* (2018)
- Dr. Danilo Agosto: *APT28's Trojan Xagent: Reverse Engineering and Controlling* (2017)
- Dr. Luca Massarelli: *Android Malware Family Classification based on DFA and SVM* (2017)
- Dr. Gregorio Pitolli: *Malware Analysis through Machine Learning: an Experimental Evaluation* (2017)
- Dr. Edoardo Gaetani: *Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments* (2017)
- Dr. Zigrid Sheu: *Towards the Usage of Invariant-based App Fingerprinting for Malware Detection in Android* (2016)
- Dr. Stefano Rosini: *Network Traffic Analysis In Android For Malware Detection* (2016)
- Dr. Matteo Pomilia: *A study on obfuscation techniques for Android malware* (2016)
- Dr. Michele Marra: *Securing Android: a review of isolation techniques* (2016)
- Dr. Andrea Fantaccione: *Malware detection for PDF documents using Machine Learning techniques* (2016)
- Dr. Donato Dell'Atti: *Reverse Engineering For Malware Analysis: Dissecting The Novel Banking Trojan ZeusVM* (2016)
- Dr. Luca Di Vincenzo: *Design, Development and Performance Analysis of a Distributed Stream Processing Application in the Apache Spark Framework* (2015)
- Dr. Vincenzo Deriu: *Count-min sketches for privacy preserving data sharing: a case study on malware detection* (2015)
- Dr. Emilio Faonio: *Comparazione di performance e fault tolerance di motori di event processing distribuiti e centralizzati: Storm vs Esper* (2012)

Teaching

2023/2024

- COMP6224: Foundations of Cyber Security (https://www.southampton.ac.uk/courses/modules/comp6224.page)
- COMP2207: Distributed Systems and Networks (https://www.southampton.ac.uk/courses/modules/comp2207.page)
- COMP2216: Principles of Cyber Security (https://www.southampton.ac.uk/courses/modules/comp2216.page)

2022/2023

- COMP6224: Foundations of Cyber Security (https://www.southampton.ac.uk/courses/modules/comp6224.page)
- COMP2207: Distributed Systems and Networks (https://www.southampton.ac.uk/courses/modules/comp2207.page)

- COMP2216: Principles of Cyber Security (https://www.southampton.ac.uk/courses/modules/comp2216.page)

2021/2022

- COMP6224: Foundations of Cyber Security (https://www.southampton.ac.uk/courses/modules/comp6224.page)
- COMP2207: Distributed Systems and Networks (https://www.southampton.ac.uk/courses/modules/comp2207.page)
- COMP2216: Principles of Cyber Security (https://www.southampton.ac.uk/courses/modules/comp2216.page)

2020/2021

- COMP6224: Foundations of Cyber Security (https://www.southampton.ac.uk/courses/modules/comp6224.page)
- COMP2207: Distributed Systems and Networks (https://www.southampton.ac.uk/courses/modules/comp2207.page)
- COMP2216: Principles of Cyber Security (https://www.southampton.ac.uk/courses/modules/comp2216.page)

2019/2020

- COMP6224: Foundations of Cyber Security (https://www.southampton.ac.uk/courses/modules/comp6224.page)
- COMP2207: Distributed Systems and Networks (https://www.southampton.ac.uk/courses/modules/comp2207.page)
- COMP2216: Principles of Cyber Security (https://www.southampton.ac.uk/courses/modules/comp2216.page)

2018/2019

- COMP6224: Foundations of Cyber Security (https://www.southampton.ac.uk/courses/modules/comp6224.page)
- COMP2207: Distributed Systems and Networks (https://www.southampton.ac.uk/courses/modules/comp2207.page)
- COMP2216: Principles of Cyber Security (https://www.southampton.ac.uk/courses/modules/comp2216.page)

2017/2018

- COMP2216: Principles of Cyber Security (southampton.ac.uk/courses/modules/comp2216.page)

2016/2017

- *Sistemi di Calcolo (*www.dis.uniroma1.it/~sc*)*
- Seminars in Advanced Topics in Computer Science Engineering (https://piazza.com/uniroma1.it/spring2017/...): *Machine Learning for Malware Detection*
- Distributed Systems (www.dis.uniroma1.it/~baldoni/...): *Amazon's Dynamo, Google's BigTable*
- Systems and Enterprise Security (www.dis.uniroma1.it/~querzoni/teaching/...): *Malware Analysis*
- Percorsi formativi in materia di cyber threat - Modulo Tecnici Avanzato, erogato dalla Presidenza del Consiglio dei Ministri: *Malware Detection Methods, Malware Reverse Engineering*
- Corso di Formazione per Amministratori di Sistemi Informatici per le Intercettazioni: *Le Misure Minime di Sicurezza ed il loro Audit*

2015/2016

- Distributed Systems (www.dis.uniroma1.it/~baldoni/...): *Amazon's Dynamo, Google's BigTable*
- Systems and Enterprise Security (www.dis.uniroma1.it/~querzoni/teaching/...): *Penetration Testing*
- Mobile Applications and Cloud Computing (www.dis.uniroma1.it/~beraldi/MACC_16/index.html): *Security aspects in Mobile Applications and Cloud Computing*
- Seminars in Distributed Systems (www.dis.uniroma1.it/~baldoni/semsd2014.php): *Machine Learning for Malware Detection, Blockchain and Smart Contracts*
- Percorsi formativi in materia di cyber threat - Modulo Tecnici Avanzato, erogato dalla Presidenza del Consiglio dei Ministri: *Esercitazione su Apache Storm, Malware Detection e Penetration Testing, Reverse Engineering per Malware Analysis*

2014/2015

- Distributed Systems (www.dis.uniroma1.it/~baldoni/...): *Amazon's Dynamo, Google's BigTable*
- *Sistemi di Calcolo (*www.dis.uniroma1.it/~sc*)*: *Tutoring*

2013/2014

- Distributed Systems (www.dis.uniroma1.it/~baldoni/...): *Amazon's Dynamo, Google's BigTable*
- Distributed Systems Seminars (www.dis.uniroma1.it/~baldoni/semsd2014.php?lang=ita): *Storage management in Hadoop for time window computations*
- Elective in Computer Networks (www.dis.uniroma1.it/~becchett/Elective/elective.html): *Privacy in collaborative environments*
- Corso su Cyber Threat erogato dalla Presidenza del Consiglio dei Ministri: *Distributed Processing and Distributed Storage*

2012/2013

- Distributed Systems (www.dis.uniroma1.it/~baldoni/...): *Amazon's Dynamo, Google's BigTable*
- Elective in Architecture and Distributed Systems (www.dis.uniroma1.it/~querzoni/teaching/...): *Amazon's Dynamo, Google's BigTable*
- Distributed Systems Seminars (www.dis.uniroma1.it/~baldoni/3ff32a3dd753664.php): *Storage management in Hadoop for time window computations*

2011/2012

- Elective in Architecture and Distributed Systems (www.dis.uniroma1.it/~querzoni/teaching/...): *Port scan detection techniques*
- Distributed Systems Seminars (www.dis.uniroma1.it/~baldoni/SemSD2012.htm): *Storage management in Hadoop for time window computations*

2010/2011

- Distributed Systems Seminars (www.dis.uniroma1.it/~baldoni/...): *Port scan detection techniques*

Administrative activities

- Since January 2020, I have served as the PGR Senior Admissions Tutor for ECS. In this role, I lead the process of allocating funding for PhD scholarships within ECS. My responsibilities include overseeing the advertising of available scholarships, collecting applications, conducting preliminary rankings, and presenting the applications to the PGR funding allocation panel. To ensure a robust pool of applications, I periodically encourage academic staff to identify suitable students and remind them of upcoming deadlines. Additionally, I enhance awareness among ECS students about PhD opportunities by sending targeted emails to eligible individuals. Furthermore, I organize an annual PhD information event featuring talks from academics and current PhD students. This event aims to provide undergraduate and postgraduate students with a comprehensive understanding of what pursuing a PhD entails.
- Since September 2019, I have served as a reviewer for grant applications within the ECS internal review process.

Education and training

Ph.D. Student at "La Sapienza" University of Rome (November 2010 – October 2013). Dissertation title: "Timely Processing of Big Data in Collaborative Large-Scale Distributed Systems". Advisor: Prof. Roberto Baldoni.

Master's Degree in Computer Engineering at "La Sapienza" University of Rome (October 2010). Dissertation title: "A contract-based event-driven model for cooperative environments: the case of collaborative security". Supervisor: Prof. Roberto Baldoni. Final grade: 110/110 cum laude.

Bachelor's Degree in Computer Engineering at "La Sapienza" University of Rome (December 2003). Dissertation title: "A System for Automatic Project Assignment". Supervisor: Prof. Fabrizio d'Amore. Final grade: 110/110 cum laude.

Past work experiences

Lecturer in Cyber Security at the University of Southampton (https://www.southampton.ac.uk/), Department of Electronic and Computer Science (https://www.southampton.ac.uk/about/faculties-schools-departments/school-of-electronics-and-computer-science)

- January 2018 – February 2022

Temporary Research Fellow at Research Center of Cyber Intelligence and Information Security (www.cis.uniroma1.it), Department of Computer and System Sciences "Antonio Ruberti", via Ariosto 25, 00185, Rome, Italy (www.dis.uniroma1.it), "La Sapienza" University of Rome (www.uniroma1.it)

- January 2014 – December 2017

Sistematica S.p.A., via Bramante 43, 05100, Terni (TR), Italy (www.grupposistematica.it)

- February 2004 – July 2005: design and development of the client side of a system for storing and managing data received by satellite, in the context of Cosmo SkyMed project (www.cosmo-skymed.it)
- April 2007 – December 2007: analysis, design and development of a distributed system for the management of both lift maintenance and spot display inside lifts
- January 2008 – March 2009: analysis, design and development of a monitoring system of Italian dams (www.registroitalianodighe.it)

E-VOLVING Business Integration, via del Maglio 6, 05100, Terni (TR), Italy (www.e-volving.it)

- July 2006 – December 2006: analysis, design and development of a web application for invoices management for a well-known Italian company