

SHORT CURRICULUM VITAE

Paulo Jorge Esteves-Veríssimo

Professor

University of Luxembourg

FSTM - Faculty of Science, Technology, and Medicine - DCS

SnT - Interdisciplinary Centre for Security, Reliability and Trust

20th January 2020

Paulo Jorge Esteves-Veríssimo

Summarized Curriculum Vitae

Paulo Esteves-Veríssimo (PJV) has a PhD (1990) in Electrical and Computer Engineering from the Technical University of Lisbon IST (PT). He is Professor and FNR PEARL Chair at the University of Luxembourg Faculty of Science, Technology and Medicine (UNILU-FSTM) (http://wwwen.uni.lu/snt/people/paulo_verissimo), since fall 2014 and Head of the CritiX lab (Critical and Extreme Security and Dependability) at SnT, the Interdisciplinary Centre for Security, Reliability and Trust at the same University (<http://wwwen.uni.lu/snt>). He is adjunct Professor of the ECE Dept., Carnegie Mellon University. Previously, he has been a Professor of the Univ. of Lisbon, member of the Board of the same university, and Director of LaSIGE (<http://lasige.di.fc.ul.pt>) where he also led the Navigators research group (<http://www.navigators.di.fc.ul.pt/>).

He is the representative of UNILU-SnT in ECSO, the European Cyber Security Organisation, and member of its Scientific & Technical Committee (STC). He is also the representative of UNILU-SnT in two of the four hubs of the H2020 European Competence Network of Cybersecurity Centres of Excellence: SPARTA and CyberSec4Europe. He belongs to the Advisory Board of the National Cybersecurity Centre Observatory, Portugal. He was Chair of the IFIP WG 10.4 on Dependable Computing and Fault-Tolerance and vice-Chair of the Steering Committee of the IEEE/IFIP DSN conference. He is a member of the Portuguese Diaspora Council.

He is *Fellow* of the IEEE and *Fellow* of the ACM. He was in the finals of the Descartes European Science Prize 2004, leading a FCUL team integrated in the MAFTIA project. He is/was member of evaluation panels for a number of reputed institutions, e.g.: IEEE Computer Society Fellows Evaluation Committee (INT), European Research Council (ERC-EU). PJV is/was associate editor of several journals, e.g.: IEEE Trans. on Emerging Topics in Computing (TETC) (2019----); IEEE Trans. on Computers (TC); IEEE Trans. on Dependable and Secure Computing. He served as international PC co-chair of the IEEE/IFIP DSN 2001 conference; and international PC vice-chair of the IEEE ICDCS 2020 conference. He has also served on the programme committees of more than 170 editions of other conferences. He is often solicited as evaluator for awards, hiring, promotions and degrees in top US and European universities.

He is currently interested in architectures, middleware and algorithms for resilient modular and distributed computing, and their application for combined system security and dependability of areas like: SDN-based infrastructures; autonomous vehicles from earth to space; digital health and genomics; or blockchain and cryptocurrencies. He is author or co-author of over 200 peer-refereed publications in international scientific conferences and journals. His work is featured in known authors' books, such as, Birman, Chow, Coulouris, Kopetz, Jalote, Raynal, Tanenbaum and Kurose. His ERDÖS Number is 3. PJV is also co-author of 5 international books and has given over 200 talks in several parts of the world, more than 70 of which were keynote speeches or distinguished lectures at reputed venues. Google Scholar Citations profile: <http://scholar.google.com/citations?user=aMHx8aUAAAAJ>

Veríssimo was also involved as key lead in numerous high-level cybersecurity and dependability audit and consulting projects, as well as advanced training, for large corporations (ex., Electricidade de Portugal, Portugal Telecom, ZON, Logica), and governmental public administration bodies and agencies. Examples of the latter: the audit of the Portuguese government's computer network (CEGER), the risk assessment of the Portuguese system of telecommunications and network providers (ANACOM), or a study on Cyber Policies and cyberspace for the Brazil Federal Government. PJV also has a solid systems and engineering track record, having contributed to the design and engineering of several industrial prototypes of distributed, fault-tolerant, secure and real-time systems. He is frequently featured on national media to comment on situations related with computer security and crime.

Index

Reading Guide.....	5
PART I.....	7
1. Identification	7
2. Education.....	7
3. Appointments.....	7
4. Languages.....	9
5. Curriculum overview and discussion.....	11
6. Scientific research and leadership career	18

Reading Guide

N.B.- *In what follows, PJV denotes Paulo Esteves-Veríssimo.* Acronyms of PJV's working places: IST- Instituto Superior Técnico, from T.U. LISBON- Universidade Técnica de Lisboa (PT). FCUL- Faculdade de Ciências, from U. LISBON- Universidade de Lisboa (PT). SnT- Interdisciplinary Centre for Security, Reliability and Trust, from UNILU- University of Luxembourg (LU).

PART I

1. Identification

Name: Paulo Jorge Esteves-Veríssimo.

Birth date: 23rd August 1956.

Place: Lisboa, Portugal.

2. Education

2.1. Higher education

Place: Instituto Superior Técnico, Lisboa.

Degree: *Licenciado* 1978 Electrical Engineering.

2.2. Post-graduation (1982 - 1984)

Place: Instituto Superior Técnico, Lisboa.

Degree: *Master of Science* in Electrical and Computer Engineering (1985).

Grade: Very Good (top grade).

2.3. Post-graduation (1985 - 1990)

Place: Instituto Superior Técnico, Lisboa.

Degree: *Doctor of Philosophy* in Electrical and Computer Engineering (1990).

Grade: Unanimity, "Very honorable and with the committee's congratulations" (top grade).

2.4. Post-graduation (1994)

Place: Instituto Superior Técnico.

Degree: *Agregado* in Electrical and Computer Engineering (1994).

Grade: Unanimity (top grade).

3. Appointments

3.1. Professorships

Place/Local: Univ. of Luxembourg Faculty of Science, Techn. and Communic., FSTC, 1/9/2014.

(now called Faculty of Science, Techn. and Medicin., FSTM)

Detached to the Interdisciplinary Centre for Security, Reliability and Trust, SnT, 2014-2019.

Appointments/Nomeações:

Category/Categoria

Start/Início

Full Professor / Professeur

01.09.14

Place/Local: Faculdade de Ciências da Univ. de Lisboa, FCUL, 21/6/1995.

Appointments/Nomeações:

Category/Categoria	Start/Início
Professor / Professor Catedrático	28.09.01
Associate Professor “Agregado” / Professor Associado Agregado	21.07.95

Place/Local: Instituto Superior Técnico, Lisboa, 1/10/1979.

Appointments/Nomeações:

Category/Categoria	Start/Início
Assistant Professor “Agregado” / Professor Auxiliar Agregado	01.12.94
Assistant Professor / Professor Auxiliar	11.04.90

3.2. University service

UNILU

- **Head of the research group** CritiX at SnT-UNILU (2014----).
- Member of mockup Panels for UNILU ERC candidates’ training.

FCUL

- Member of the **Statutory Assembly** of the (unified) University of Lisbon (2013).
- **Director** of the LaSIGE Lab (<http://lasige.di.fc.ul.pt>) a research unit of the Dpt. of Computer Science and Engineering of FCUL (2006-09, 2012-14). Had been **Founding Director** (1999-2001).
- Member of the Faculty **Evaluation Committee** of FCUL, FCUL (2012-14) (responsible for regulating and supervising the periodical evaluation of faculty).
- Member (by appointment of the Rector) of the **task-group for strategic development** of the merger of the University of Lisbon and the Technical University of Lisbon (2012) (process aiming at building a future university in the Lisbon area with circa 45000 students, 3000 faculty and 300M€ state budget).
- Deputy member (2008-10) and elected **member of the Board** (2011-14) of the University of Lisbon (board defining the strategic development of the UL, and supervising its activity in the scientific, pedagogical, financial and estate grounds).
- Elected member of the FCUL **Scientific Council** (2009-14).
- Elected member of the FCUL **Statutory Assembly** (2008-09 which implemented the new juridical system of the Portuguese higher education institutions).
- **Member of the Board** of the Foundation of the FCUL (2007-14).
- **Director** of the LaSIGE (<http://lasige.di.fc.ul.pt>) DI research unit (2005-2010).
- Elected member of the **FCUL Assembly** (2005-2007).

- Coordinator of GTIC-UL, **Working Group on ICT strategy** of the University of Lisboa, which laid down for ICT in the U.L. (2004-2005).
- **Head of the Department** of Computer Science and Engineering (DI) (<http://www.di.fc.ul.pt/>) and member of the FCUL Scientific Council Coordination Committee (1999-2001).
- **Head of the research group** Navigators at IST and FCUL (1985-2014).
- Restructured and was **responsible for the Computing Service** of the DI, with more than 1000 users (1995-2004).
- Elected member of the FCUL **Pedagogical Council** (1996-1999).

IST

- A brief summary of service at IST. He was Coordinator of the Digital Systems and Computers Section of the Electrical and Computer Engineering Dpt. (DEEC) (1994-1995). He belonged to the Coordination Committee of DEEC (1984-1988 and 1994-1995). He organised and was responsible for the Computing Service of the DEEC, with circa 2000 users (1990-1995).

4. Languages

Language	Reading	Writing	Conversation
Portuguese (m.t.)	Excellent	Excellent	Excellent
English	Excellent	Excellent	Excellent
French	Excellent	Good	Excellent

5. Curriculum overview and discussion

This section contains a personal statement about the several facets of the curriculum built throughout my career: professional/academic, research, and teaching facets.

In summary, my career has focused on *distributed systems architectures, algorithms and protocols*, understood as embodying the main facets of the concepts and technologies underlying the analysis, design, configuration and integration of complex computational systems:

distribution – how processes interact, synchronise and communicate;

real-time – the timing and timeliness issues concerned with these interactions;

dependability – the reliability, availability and safety issues in face of accidental faults;

security – the integrity, confidentiality, availability and authenticity of such interactions, implying intrusion prevention in face of accidental faults;

resilience – the fusion between dependability and security --- e.g. fault and intrusion tolerance --- to fight cyber-attacks, accidental faults, design errors, or unexpected operating conditions, in a simultaneous, automatic and sustainable way.

5.1. Professional career track highlights

Selected roles amongst the **professional management or direction positions**:

Representative of UNILU-SnT in ECSO, the European Cyber Security Organisation. Representative of UNILU-SnT in two of the four hubs of the H2020 European Competence Network of Cybersecurity Centres of Excellence: SPARTA and CyberSec4Europe. Was Chair of the IFIP WG 10.4 on Dependable Computing and Fault-Tolerance. Was Vice-Chair of the Steering Committee (SC) of IEEE/IFIP DSN, International Conference on Dependable Systems and Networks.

Selected roles amongst the **academic management or direction positions**:

Principal Investigator of the IIS&D PEARL programme at SnT-UNILU (FNR – LU; 5 MEuro). Head of the CritiX research group at SnT-UNILU. Was Principal Investigator of the IISD programme (CMU-Portugal partnership, Portuguese Government; 3 MEuro). Was Founding director of LASIGE. Was Head of the Navigators research group at IST and FCUL (1985-2014). Was Elected member (2011-14) of the Board of the University of Lisbon.

Amongst other events or actions in the professional and scientific sphere, it is maybe worthwhile mentioning as selected and most relevant in several topics:

Prizes and awards

Fellow of the IEEE and *Fellow* of the ACM. His team was in the finals of the Descartes European Science Prize 2004, with the project *MAFTIA*.

Evaluation activities:

Served on the IEEE Computer Society Fellows Evaluation Committee. Was Member of the European Research Council (ERC) Evaluation Panel on Computer Science and Informatics. Is/was associate editor of several journals: IEEE Trans. on Emerging Topics in Computing (TETC) (2019---); IEEE Trans. on Computers (TC); IEEE Tacs. on Dependable and Secure Computing. Served as int'l PC co-chair of the IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2001; int'l PC vice-chair of the IEEE Int'l Conference on Distributed Computing Systems, ICDCS 2020. Served on the PCs of more than 170 editions of other conferences. He is often solicited as evaluator for awards, hiring, promotions and degrees in top US and European universities.

Consulting and Auditing activities:

Member of the Scientific & Technical Committee (STC) of ECSO. Consulting on Cyber Policies for Brazil as EU expert (EU, Brazilian Government). Member of the European Security & Dependability Advisory Board, EU IST. Member of the Advisory Board of the National Cybersecurity Center Observatory (CNCS Portugal). Strategic leadership of a security and dependability audit of the complete network of telco and network providers operating in Portuguese territory (ANACOM). Team leader for the audit and security tests to the Computer Network of the Portuguese Government (CEGER).

PJV has consulted several times to the Crime Investigation Police in computer security issues. He has also made several security audits, and performed consulting and advanced training to several Portuguese companies, on computer security and dependability (ex., Electricidade de Portugal, Portugal Telecom, ZON, Logica). PJV is frequently featured on media on situations related to informatics security and crime. PJV has also contributed to the design and engineering of several industrial prototypes of distributed, fault-tolerant, secure and real-time systems, such as: post-office automation (EID); industrial manufacturing cells (Renault); dependable databases (Ferranti); home-banking (Crédit Agricole); distributed SCADA (Intracom).

Organisation of events:

General Chair of the IEEE/IFIP Dependable Systems and Networks Conference (DSN) Lisboa/Estoril-Portugal, 2009, and once again later in Luxembourg, 2018. Local Chair, IEEE RTSS 2004, Lisboa-Portugal, December 2004.

Selected keynote speech and distinguished lecture venues:

Dean's Seminar Series at Monash University, Melbourne-AUS, December 2019. KAUST CEMSE Dean's Distinguished Lecture Series, Thuwal-KSA, October 2019. IC Colloquium Series EPFL, Lausanne-CH, September 2019. TU Darmstadt, Darmstadt, DE, May 2018. ICRI-CARS Annual Workshop, Intel, Portland, US, May 2018. Science of Security series, U. Illinois Urbana-Champaign, US, April 2017. 10th Int'l Symp. on the Nat'l Info Strategy, Military Academy, Amadora-PT, April 2016. 33rd IEEE Symp. on Reliable Distributed Systems (SRDS), Nara JP, Oct, 2014. LADC'13 Rio de Janeiro, Brasil, April 2013. Safecomp 2011, September 2011, Naples, Italy. INRIA-IRISA 1994. Rennes, França, February 1994.

Selected tutorial and advanced course venues:

CPSWeek, Porto, Portugal, April 2018. 43rd Int'l Conf. on Dependable Sys and Net. (DSN 2013), Budapest, Hungary, June 2013. 26th Intl Symposium on DIStributed Computing (DISC), Salvador,

Brasil, October 2012. Info. Trust Inst.- U. Illinois, Washington St. U., Dartmouth, Cornell. Lake Geneva, US, June 2008. 12th IEEE Real-Time and Embedded Tech. and Applications Symp., S.Jose-USA, April 2006. Microsoft Research, Mountain View, USA, April 2006. IEEE/IFIP Dependable Systems and Networks (DSN) 2002, Washington-DC-USA, July 2002. **Director** 3rd edition ERSADS, European Research Seminar on Advances in Distributed Systems, Madeira-Portugal, April 1999. Pohang University, Korea, August 1995. **Organised** and lectured several modules of the LISBOA'92 International Advanced Course on Distributed Systems (1992).

5.2. Main scientific and technical achievements

I have led the Navigators research group (<http://www.navigators.di.fc.ul.pt/>) of LaSIGE-ULisboa. I currently lead the CritiX research group (Critical and Extreme Security and Dependability) at the Univ. of Luxembourg SnT, and I am currently interested in secure and dependable distributed architectures, middleware and algorithms for: resilience of large-scale systems and critical infrastructures, privacy and integrity of highly sensitive data, and adaptability and safety of real-time networked embedded systems.

I was project team leader in several National and EU projects (FNR, FCT, H2020/ESPRIT/IST): ByzRT, ThreatAdapt, SPARTA, CyberSec4Europe, CARS, IIS&D PEARL, BioBankCloud, TClouds, SecFunet, CRUTIAL, HIDENETS, MAFTIA, RESIST, SecureIST, ESFORS, CaberNet, CORTEX, TACID, DARIO, ARTIST, AJECT, RITAS, DEFEATS, COPE, Delta-4, Dinas, GODC, BROADCAST, MICRA, DEAR-COTS, Bank-92, and Elena.

Namely, I was a leader of the DELTA-4 project, whose results in the theory and practice of *distributed fault tolerance* are still cited today. His contributions to DELTA-4 include pioneering concepts on group-based distributed fault tolerance, including the AMP group communication suite supporting DELTA-4 replication schemes. I was the main architect of the DELTA-4 sister architecture XPA, which advanced the state of the art in distributed mission-critical fault-tolerant real-time systems. Some of the results of XPA include: the semi-active replication algorithm; the extremely precise, a posteriori agreement clock synchronization algorithm; and later the Cesium-Spray GPS-based large-scale global time system, which inspired later practical works.

I have also invented several concepts in fault-tolerant real-time LAN communication. The introduction of the inaccessibility predicate and mechanisms to control it, made it possible to explain and remedy short blackout phenomena observed in LANs and field-buses, which disturbed the R/T behavior and even communication correctness. His research on fault-tolerant embedded systems led to the design of CANELY, an embedded systems architecture ending a long-lasting myth that dependable real-time event- and time-triggered operation was not possible in CAN networks.

I was coordinator of, and one of the main contributors to, the CORTEX project, which as early as 2002, introduced innovative concepts and new programming models for real-time autonomous event-based systems applications, such as car-2-car communication and coordination, taken-up by other projects, such as HIDENETS and KARYON.

I was also a leader of the MAFTIA project, which made relevant contributions in concepts, architectures, and algorithms for *intrusion tolerance*. MAFTIA major innovation was a comprehensive approach for handling both accidental faults and malicious attacks in systems, including attacks by external hackers and by corrupt

insiders, by using tolerance techniques, further to classic prevention ones. I was a lead contributor to the design of the overall MAFTIA architecture. The influence and importance of MAFTIA can be measured, among other ways, by the fact that it reached the finals of the highly prestigious European Descartes Science Prize.

I have introduced the *hybrid distributed systems model* (a.k.a. “Wormholes” model) [J16], which has allowed advances in the state of the art of theory and practice of distributed algorithms in several boundary areas, where impossibility results and conflicting goals had established dead-ends for classic, that is, homogeneous, distributed systems. To cite a few advances made possible by architecturally hybrid systems: feasibility conditions for the implementation of failure detectors, in essence non-implementable in classical asynchronous models; simple but effective building blocks for some “oracle-based” theoretical solutions whose previous implementations in homogeneous models were very complex or had poor coverage; circumvention of the impossibility of exhaustion-safety in homogeneous asynchronous systems, which rendered all such systems non-resilient.

The need for hybridisation has been progressively recognised over the years, either explicitly or implicitly, both by standard manufacturers, with trusted execution environments (TEE: TPM (Trusted Platform Module), SGX (Software Guard Extensions), ARM TrustZone), or application specific hybrids coming from R&D (TTCB, A2M, USIG, CASH, TRINC, etc.). Actually, over the years more robust implementations progressively became possible in an application-specific way. Since the inception of the concept in 1999, systems have gone from software-based hybrids, e.g., using kernel separation, or hypervisor managers such as XEN Dom0, to more robust hardware-based hybrids. Here the evolution has been startling, from small PCI or USB appliances, through FPGAs, to tiles in many-core SoCs.

The model has shown its genericity, being a powerful tool to represent all these system variants enjoying the presence of hybrid components, even if conceived independently. This justifies that an increasing number of known authors have published works referring to or explicitly or implicitly following the hybrid distributed systems model in the past few years. In a recent (2019) literature survey, I have identified over 40 papers on the topic, besides the papers from my two groups Navigators and CritiX. Just exemplifying some well-know authors: Aguilera et al., Baldoni et al., Chun and Maniatis and Kubiawicz et al., Clement, Junqueira et al., Distler and Kapitza and Reiser et al., Friedman et al., Guerraoui and Vukolic et al., Kapitza and Cachin et al., Liskov and Castro, Levin, Douceur et al., Levitt and Duan et al., Liu and Asokan et al., Macedo et al., Malkhi et al., Raynal et al., Roeder and Schneider, Weisnberg and Dolev et al.

Later, I and my team formalised the notion of *Exhaustion Safety* (ES), a system safety predicate defining that a system always has enough resources to defend itself from threats. In the context of replicated systems, ES means having enough correct replicas. We later proved the *impossibility of exhaustion-safety* in homogeneous asynchronous distributed systems (e.g., BFT, BFT-PR), which obviously meant for example, that all previous designs of such fault-tolerant systems (including my own team’s) would never give resilience guarantees, in the sense of living enough to perform their mission [J27]. This despite having provisions for reactive or proactive recovery, exactly the mechanism

that had been previously invented by colleagues to safeguard the number of correct replicas above the minimum threshold. In the sequel of that work, I introduced the new concept of recovery, *proactive/reactive resilience*, for asynchronous BFT systems [P83], based on architectural hybridization, which provided a solution to this serious problem, circumventing the impossibility result. That work was one more example of the power of *hybrid distributed systems modelling*.

As a visionary, I have always been committed to fostering the sponsorship of new avenues in the s.o.t.a. of systems research, not only in Europe but also in the USA, consulting on the preparation of several research initiatives and agendas. For example, the definition of the National Research Priorities of Luxembourg, under the initiative of the FNR, 2018-2019; the European Security & Dependability Advisory Board for the FP7 IST research program, 2004-2006; NSF Grand Challenges on Distributed Systems, 2005; Co-operating Objects Research Challenges, 2005; SecurIST Advisory Board Recommendations for a Security and Dependability Research Framework in FP7; Global Computing Pro-active Initiative, ESPRIT FET, 2000.

I also have a solid *engineering track record*, besides the numerous scientific contributions, attested for example by my contribution to the design of several industrial prototypes of fault-tolerant, secure and real-time systems, such as: industrial manufacturing cells (Renault); dependable databases (Ferranti); home-banking (Crédit Agricole); distributed SCADA (Intracom).

I also have performed numerous high-level cybersecurity and dependability audit and consulting projects. I led a team that performed the audit and security tests to the Computer Network of the Portuguese Government (2001, CEGER). I also assumed the strategic leadership in a security and dependability audit of the complete network of telecommunications and network providers operating in Portuguese territory (2010, ANACOM). I have led an emblematic project about the successful, persistent and continued improvement of the security and dependability of several critical infrastructures (2008-13, EDP - Electricidade de Portugal). I also have regular collaboration with national companies and institutions, in problems related to dependability and security, and I am frequently featured on national media to comment on situations related to computer security and crime.

5.1. Projects and funding record

The scientific and technical achievements described have naturally hinged on the right research projects to serve the strategy outlined. Over my career, I have been involved in over 40 research projects, 25 of which international. But rather than the number, the quality and the purpose were always the decisive factor to launch or to join them: quality research; serving the strategic objectives of the group; quality partners. In all of them, I was an active researcher and in most, a team leader. These are detailed in Section 6.2.

Funding record, as an enabler of excellent research, was always considered strategic to me, especially if one does systems research. Over my senior career (80% of which spent

in a scarcely resourced, peripheral country like Portugal), the acquired funding for the initiatives I led or promoted, including labs I directed, exceeds 25Mio Euro.

At FCUL, the total financing budget awarded to the Navigators research group by the European Commission definitely contributed to place FCUL as one of the top four Portuguese institutions in financing captured in the IST program of the 5th Framework Program (FP5). This performance was largely maintained in the subsequent years, with a total of around 6Meuro of funding capture for the group alone.

Later, I organized and coordinated the FCUL participation in the Carnegie Mellon--Portugal international partnership (2006-11), a 56Meuro program sponsored by the Portuguese Government where FCUL led the security and dependability initiative, with a further 3MEuro financing.

From 2015 on, at the University of Luxembourg, I brought in a 5MEuro grant (PEARL-FNR), to spawn a new research lab (CritiX) and a strategic research program on Critical Information Infrastructure Security and Dependability.

Later, after consolidating the team and the research avenues, we sought to acquire more competitive funding. As of January 2020, the Lab had additionally secured more than 7MEuro from several funding sources, which for example guarantees its full sustainability to a horizon of end 2023.

5.2. Publication record

I was author or co-author of over 200 international refereed publications. Of these, 16 are books or book chapters, 8 are articles in collections, and 44 are articles in journals, all refereed. I have currently more than 11111 citations to my publications, and an H-Index of 50, computed through Google Scholar Citations. In case of interest, my ERDÖS Number is 3. GSC profile: <http://scholar.google.com/citations?user=aMHx8aUAAAAJ>

(Full list of publications in Section **Error! Reference source not found.**).

Selected publications:

1. Maria Fernandes, Jérémie Decouchant, Marcus Völp, Francisco Couto, Paulo Esteves-Veríssimo. *DNA-SeAl: Sensitivity Levels to Optimize the Performance of Privacy-Preserving DNA Alignment* (2019) IEEE Journal of Biomedical and Health Informatics CORE A. <http://hdl.handle.net/10993/40046>
2. Jiangshan Yu, David Kozhaya, Jérémie Decouchant, Paulo Esteves-Veríssimo. *RepuCoin: Your Reputation is Your Power* (2019) IEEE Transactions on Computers CORE A*. <http://hdl.handle.net/10993/38630>
3. Diego Kreutz, Jiangshan Yu, Fernando Ramos, and Paulo Verissimo (2019). *ANCHOR: logically-centralized security for Software-Defined Networks*. ACM Transactions on Privacy and Security (TOPS, previously TISSEC) . Core A.
4. Kreutz, Diego; Ramos, F.; Verissimo, Paulo; Rothenberg, C. E.; Azodolmolky, S.; Uhlig, S. "Software-Defined Networking: A Comprehensive Survey", in Procs of IEEE (2015), 103(1).
5. Miguel Correia, Nuno Ferreira Neves, Paulo Verissimo, "BFT-TO: Intrusion Tolerance with with Less Replicas", The Computer Journal, vol. 56, no. 6, pp. 693–715, Jun. 2013. Extension of: How to Tolerate Half Less One Byzantine Nodes in Practical Distributed Systems, in Proc's of the 23rd IEEE SRDS. Florianopolis, Brasil, 174-183, October 2004.

6. Giuliana Santos Veronese, Miguel Correia, Alysson Bessani, Lau Cheuk Lung, Paulo Verissimo, "Efficient Byzantine Fault-Tolerance", IEEE Transactions on Computers, vol. 62, no. 1, pp. 16–30, Jan. 2013.
7. Paulo Sousa, Alysson Bessani, Miguel Correia, Nuno Ferreira Neves, Paulo Verissimo. Highly Available Intrusion-Tolerant Services with Proactive-Reactive Recovery. IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 4, pp. 452-465, Apr. 2010. <http://doi.ieeecomputersociety.org/10.1109/TPDS.2009.83>.
8. Paulo Verissimo. Travelling through Wormholes: a new look at Distributed Systems Models. SIGACT News, vol. 37, no. 1, pages 66-81, 2006.
9. Paulo Verissimo and Nuno Ferreira Neves and Miguel Correia, "Intrusion-Tolerant Architectures: Concepts and Design", In Architecting Dependable Systems, R. Lemos, C. Gacek, A. Romanovsky (eds.), LNCS 2677, pages 3-36, Springer Verlag, 2003.
10. Verissimo, P., Casimiro, A.: The timely computing base model and architecture. IEEE Transactions on Computers, Special Issue on Asynchronous Real-Time Distr. Systems (2002).
11. D.Powell, G.Bonn, D.Seaton, P. Verissimo, F.Waeselynk. "The Delta-4 Approach to Dependability", Procs. 18th Symp. Fault-Tolerant Computing, Tokyo-Japan, June 1988.

5.3. Teaching career Highlights

In what is today an extensive teaching career, I have taught and/or been responsible for several **courses** on several **domains** of systems and algorithms: *distributed systems and algorithms, real-time and embedded systems, fault tolerance, security and resilience*. Earlier on, I have also taught *system management, computer architecture, digital systems and microprocessors, electronics*.

Since the beginning of my senior career, I have lectured more than 80 graduation and post-graduation regular **course editions** in the matters above, at IST, FCUL, and UNILU, totalling an average of over 2 courses per semester (full list in Section **Error! Reference source not found.**). I was more than 20 times **Invited Professor** at several national and international universities (EPFL, UFBA, UFSC, ISCTEM, IST, UMINHO, FCTUC, ISEG, U. Roma, CUSO, TU Vienna). Additionally, I have taught over 20 advanced courses and **tutorials** in several venues.

Being fascinated by teaching as "transmission of knowledge", I take great pleasure in lecturing, and I have always invested in **textbooks** that could guide the students in further after-lecture study, especially in emerging subjects. With colleagues, I wrote several of those in a number of innovative subjects in their time, such as '*distributed systems*' [L6-8,L12], '*intrusion tolerance*' [L13], '*resilient computing systems*' [L15], or '*software-defined networking*' (SDN) [J35]. One of these [L6-L8], directed to graduate studies, was largely adopted in several countries, with over 12.000 copies sold today. The latter [J35], had over 3200 citations (GSC) in January 2020, and is extensively quoted by Kurose and Ross in the latest edition (7th) of their famous textbook *Computer Networking: A Top-Down Approach*. I find it also quite rewarding that my own research work is featured in known authors' textbooks, such as, K. Birman, R. Chow, G. Coulouris, H. Kopetz, P. Jalote, M. Raynal, A. Tanenbaum and J. Kurose.

Whenever called for, I have served in **academic evaluation**. I was part of 20 **habilitation** juries, and also 40 national and 22 international **PhD** jurys. I also served in numerous

MSc theses juries, overall more than 60. I have successfully **supervised** over 20 MSc theses and 8 PhD theses. I **currently supervise** 8 PhD students, half of whom are in the final leg of their PhD. Most of the students and researchers I have mentored have had very successful careers in academia or industry.

Full elements about my teaching and mentoring career can be found in Section **Error! Reference source not found.**

6. Scientific research and leadership career

Facts are described in chronological order, to retain the causal nexus in the career trajectory.

6.1. Main career chapters

IST – T.U. LISBON - INESC

The career of Paulo Esteves-Veríssimo (PJV) has started within the universe of the Technical University of Lisbon IST and of INESC. He was with the IST from 1979 to 1995. He got a PhD (1990) and “Agregação” (1994) in Electrical and Computer Engineering from the Technical University of Lisbon IST. As a young researcher, he helped found and was a researcher at INESC (Systems and Computer Engineering Institute) since its creation in 1980, a laboratory initially affiliated with IST.

He was a key element in the successful application of INESC to the programs Ciência (FCT- national research funding agency) and PEDIP (Ministry of Industry), in 1990/91, and in the restructuration of INESC that followed. The programmes brought circa 10 Mio euro to INESC. In the nineties, he devotes significant attention to the INESC effort in technology transfer and start-up creation in industrial automation, CIM/SCADA sectors.

Navigators

He founded the Navigators research group at INESC in 1985, which devoted their attention initially to distributed and embedded real-time systems and large-scale distributed systems. The group acquired an extensive experience in several domains of distributed systems, fault/intrusion tolerance, real-time and security. The group has pursued two research lines--- Fault and Intrusion Tolerance in Open Distributed Systems; Timeliness and Adaptation in Dependable Systems--- where it published extensively, thanks to intense activity spawned by the acquisition of funding from a significant number of projects.

Incidentally, he had the honour of signing, as leader of the local team in the DELTA-4 project, the first Portuguese participation ever in a European Research Project (Esprit, 1986). DELTA-4 was to become one of the most successful european systems research projects to date. All these events significantly helped to put INESC (and Portugal) on the map of international computer science and engineering research.

FCUL – U. LISBON

At FCUL, the University of Lisboa Faculty of Sciences, since 1995, he started another chapter, where he has led strategically the [Navigators research group](#) --- which he transferred to FCUL (<http://www.navigators.di.fc.ul.pt>) --- to a significant development, counting 7 senior PhD elements (faculty and research associates) and several students and temporary researchers, in a total of 35+ people. The group was quite successful in acquiring research funding that allowed increasing activity, qualitatively and quantitatively, having scaled-up to 50+ members, and running dozens of projects.

Over the years since his arrival, as senior member of faculty, member of the Scientific Council of FCUL, and Head of Department, he was a key person in the development of the Computer Science and Engineering Dpt. of FCUL from a 5-faculty to a 45-faculty large high-quality department with 1500 students, ranked one of the best in Portugal (<https://ciencias.ulisboa.pt/en/informatics>).

During his period at FCUL, he was heavily involved in the creation, promotion and development of a new research lab, with a cooperative-competitive model and philosophy of management. The lab was LaSIGE, the research laboratory where the Navigators were later located.

LaSIGE

The Laboratory for Large-Scale Informatics Systems, LaSIGE (<http://lasige.di.fc.ul.pt>), a research unit of the Dpt. of Informatics of FCUL, was created in 1998, and PJV was founding Director. PJV has chaired the Scientific Council of LaSIGE by inherence of the Director role. As founder, senior researcher, group leader, and Director on several occasions, he helped develop the lab to a leading institution in Portugal and internationally, with considerable visibility and reputation, gathering at a point more than three quarters of the Dpt. faculty.

LaSIGE was systematically very highly ranked in the national research unit evaluations (between Very Good and Excellent), systematically ranked in the top 5 national units in competitive research funding capture, and has gotten very favourable reports from its International Advisory Board.

LaSIGE developed initially activities in a number of relevant areas of computer science and engineering (CSE), including: human-computer interaction and multimedia; information management, net-centric, parallel and distributed computing; software engineering; and security and dependability. Later, as Director again, he has restructured the modus-operandi and the research lines, to considerably improve its ability to promote new lines, to reinforce its competitiveness and secure external R&D project funding. That philosophy bore fruit and kept LaSIGE a very dynamic and adaptive institution, which kept improving its breadth in scientific areas.

Under his leadership, LaSIGE reached a sustained activity of high-level research and a critical mass of researchers, as measured by several objective indicators: around 30 PhD-level researchers, in a total of 140+ researchers including post-grad students, many of which foreigners; an average of 20 on-going, and over 60 finished projects (of which a third on average are international).

CMU-Portugal partnership

PJV helped develop the Carnegie Mellon | Portugal international partnership (2006-12), sponsored by the Portuguese Government. He organized the University of Lisboa Faculty of Sciences (FCUL) participation in the initiative, gaining a significant insight into the key factors of success for the organisation of dual PhD and MSc programmes in alliance with cooperative research. The partnership was materialized by a joint "Information and Communication Technologies Institute", ICTI, with poles in CMU and in Portugal.

Veríssimo has set up the program at FCUL and was the coordinator of the FCUL pole during the programme (<http://cmuportugal.di.fc.ul.pt/>). FCUL has had a leading role in one of the initiatives of the partnership --- *Information and Infrastructure Security and Dependability* --- through faculty from the Department of Computer Science and Engineering, and researchers from LaSIGE.

Two graduate **dual programs** were organized in this initiative, providing respectively Master (MSc) and Doctoral (PhD) degrees. Either program confers a dual degree to the successful candidates, both from the Carnegie Mellon University and from the University of Lisbon.

As a result of this partnership, the CSE area of FCUL gained significant international visibility and drastically improved its ability of international recruitment, both of students and faculty. On the other hand, the Master program on Information Security, which he founded and led in the first years (<http://msi.di.fc.ul.pt>) in narrow cooperation with CMU, continues working successfully, now in solo under FCUL responsibility, still training top-level technical decision makers, its alumni occupying important positions in the market and academia.

SnT – UNILU – FSTM

At the University of Luxembourg since 2014, where PJV is a Professor of the Faculty of Science, Technology and Medicine (FSTM), and member of the Department of Computer Sciences (DCS), his research is organized at SnT, the Interdisciplinary Centre for Security, Reliability and Trust (<http://www.en.uni.lu/snt>), where he is a member of the Management Committee.

PJV is the Representative of UNILU-SnT in ECSO, the European Cyber Security Organisation (<https://www.ecs-org.eu/>) and member of its Scientific & Technical Committee. He is as well representative of UNILU-SnT in two of the four hubs of the H2020 European Competence Network of Cybersecurity Centres of Excellence (<https://cybercompetencenetwork.eu/>) launched in 2019: SPARTA and CyberSec4Europe.

The participation of SnT as founding member of the EU ECSO cPPP public-private partnership in cybersecurity was pivoted by PJV in 2016. This activity helped the position of Luxembourg, given the size of the country, in the call for Cybersecurity Competence Networks in H2020, which PJV mentored, in coordination with several colleagues. SnT was invited to six proposals, participating to three of the approved four Networks, in a very competitive selection. CritiX is involved in two of them, and SnT is the only institution to be part of three networks. The importance of these successes for SnT and

Luxembourg cannot be overstated: R&D programs of several thousand Mio euros are envisaged in this area for Horizon Europe (HE), the sequel of H2020.

During his period at SnT, he has heavily involved in the creation, promotion and development of a new research lab, with a non-typical objective: state-of-the-art research in a problem area that may be described as one of the facets of extreme computing -- withstanding extreme levels of threat, like advanced persistent threats, considering critical information infrastructures. That lab was CritiX.

CritiX

The CritiX lab (Critical and Extreme Security and Dependability - <http://www.en.uni.lu/snt/research/critix>) was built from scratch in September 2014 at SnT. In cruise speed, CritiX has counted on average 15-20 people, amongst which 3 senior PhD elements, and several post-docs, PhD students and engineers.

The objective from the onset was for the lab to be internationally recognised in time as having a unique expertise in Resilient Modular and Distributed Computing, as a crucial paradigm to counter advanced persistent threats against valuable targets, and thus defeat extreme failures or adversary power and sustain perpetual and unattended operation of critical information infrastructures (CII).

In order to set up a coherent development momentum for the young lab, both in acquiring critical mass and producing quality and quantity research outputs, a concrete strategic plan was devised, anchored on a generous grant received from the National Science foundation of Luxembourg (FNR). This was the 5-year, 5MEuro strategic research PEARL programme described below.

With this baseline support, PJV led the lab through an ambitious research strategy along four focal points: resilience of cyber-physical system infrastructures and control; internet and cloud infrastructures resilience; security and dependability of embedded components; data privacy and integrity in highly sensitive sectors.

The evolution of the lab since 2015 was significant, achieving reputation and successes on several fronts: e-Health systems, featuring critical biomedical data processing and storage needs; financial operations featuring blockchain-based infrastructures; autonomous and cooperative vehicles and other CPS featuring SCADA/DCS; cloud data center architectures featuring critical hypervisor and SDN operation needs. More detail can be found [here](#). After consolidating the team and the research avenues, effort was directed to consolidate the lab economically, through competitive funding. As of January 2020, the Lab had additionally secured more than 7MEuro from several funding sources, which for example guarantee its full sustainability to a horizon of end 2023.

One considerable success was the launch of a partnership with Intel (2017), in the context of the Intel Collaborative Research Institute on Collaborative Autonomous and Resilient Systems (ICRI-CARS), focused on vehicles, and autonomous driving safety-security concerns, through hardware assisted resilience mechanisms. This was the first SnT partnership with an international company not established in Luxembourg, which is an excellent sign of the contribution of CritiX to the international relevance of SnT.

PEARL Programme IIS&D

PJV was granted an Excellence Award for Research in Luxembourg (PEARL) Chair from the National Science foundation of Luxembourg (FNR), for his proposed 5MEuro strategic research programme on Information Infrastructure Security and Dependability at the University of Luxembourg (2015-2021). PEARL is a competitive grant reserved to public institutions inside Luxembourg.

IIS&D was crucial to enable the research strategy and successes of CritiX in the first 5 years, catalysing: team building; student recruiting; ramping activity up in the focal topics; attracting partners and European grants; attaining visibility of the lab as one of the international poles in the area; making the subjects relevant to partner companies and organisations.

Letting the international Scientific Advisory Board speak, upon the PEARL 4th year review (Feb 2019), quoting e.g.: «... *In terms of the main goal of the Pearl program, to create a world-class center of excellence in an area crucial to society at Luxembourg, the board finds that this goal is being achieved with extraordinary success...*» or «... *The depth and breadth of the projects being pursued is outstanding, especially when considering the short amount of time the group has been in operation... Very few groups worldwide can boast such breadth...*»

6.2. Research projects

In the course, and as enabling factors of, the research career and outputs described above, he is/was involved in several dozens of research projects and activities as an active researcher and team leader *except where noted otherwise*. Project data and funding record are listed below, only for the ongoing projects.

Ongoing / Presentes:

SnT - UNILU

- **ByzRT - Intrusion resilient real-time communication and computation in autonomous systems.** Sponsoring body: FNR Luxembourg (CORE Inter). Project /UniLux funding: 1.240.000€ / 980.000,00€. **Coordinator:** University of Luxembourg (LU). Start Date: June 2020. Duration: 3 years.
- **Admorph: Towards Adaptively Morphing Embedded Systems.** Sponsoring body: European Commission – H2020. Project / UniLux funding: 4.500.000 € / 690.000,00 €. **Coordinator:** Universiteit van Amsterdam. **Start date:** Jan 2020. Duration 3 years. Team member.
- **ThreatAdapt - Adaptive Byzantine Fault and Intrusion Tolerance.** Sponsoring body: FNR Luxembourg (CORE Inter). Project /UniLux funding: 967.000,00€. **Coordinator:** University of Luxembourg (LU). Start Date: Feb 2019. Duration: 3 years.

- **SPARTA hub --- European Competence Network of Cybersecurity Centres of Excellence ---** Strategic Programs for Advanced Research and Technology in Europe (<https://www.sparta.eu/>). Sponsoring body: European Commission (H2020). Project / SnT funding: 16.000.000,00 € / 365.000,00 €. Coordinator: LIST-CEA (FR). Start Date: Feb 2019. Duration: 3 years.
- **CyberSec4Europe hub ---- European Competence Network of Cybersecurity Centres of Excellence ----** Cyber Security for Europe (<https://cybersec4europe.eu/>). Sponsoring body: European Commission (H2020). Project / SnT funding: 15.000.000,00 € / 155.000,00 €. Coordinator: Goethe Univ. Frankfurt (DE). Start Date: Feb 2019. Duration: 3 years.
- **GenoMask - PoC - Early stage read filtering and masking of genomic information.** Sponsoring body: FNR Luxembourg (JUMP Proof-of-Concept). Project /UniLux funding: 232.240,00 €. Coordinator: University of Luxembourg (LU). Start Date: Feb 2019. Duration: 2 years. Team member.
- **HyLIT - Architectural Support for Intrusion Tolerant Operating-System Kernels.** Sponsoring body: FNR Luxembourg (CORE). Project /UniLux funding: 858.000,00 €. Coordinator: University of Luxembourg (LU). Start Date: Nov 2018. Duration: 3 years. Team member.
- **CARS - Architectural Support for Automatic Resilience of Autonomous Cooperative Systems.** Sponsoring body: Intel Corporation. Project /UniLux funding: 600.000,00 €. Coordinator: Intel Collaborative Research Institute for Collaborative Autonomous & Resilient Systems (ICRI-CARS). Start date: Oct 2017. Duration 3 years.
- **IIS&D PEARL - Information Infrastructure Security and Dependability.** Sponsoring body: FNR Luxembourg (PEARL grant). Project /UniLux funding: 4.750.000,00 €. Coordinator: University of Luxembourg (LU). Start Date: Jan 2015. Duration: 5+2 years.

From the above-mentioned projects, IIS&D has offered the baseline umbrella to: (i) kick-start the CritiX lab; (ii) and set in motion the strategy defined with the senior members, right in the first months of operation.

CARS prefigures the success in attracting global industrial players, and together with HyLIT covered important scientific results and their applicability to one relevant vertical: Autonomous Vehicles – ADAS (Autonomous Driving Assistance Systems), V2X (vehicle-to-vehicle|infrastructure) communication.

GenoMask is a proof-of-concept project destined to validate some important scientific results in data privacy and integrity of critical data, in this case for eHealth – Biomedical information, genomics.

SPARTA and CyberSec4Europe hubs of the European Competence Network of Cybersecurity Centres of Excellence constitute, as mentioned, a vantage point for community R&D developments, as well as for networking and project mounting in the future.

ThreatAdapt and Admorph, the latest projects to be launched, feature, not surprisingly, the very top of the s.o.t.a. in resilient computing systems, in this case, the dynamic adaptability and morphing capacity of computing systems of diverse scales, in the face of a changing threat surface.