Maria Mushtaq

PhD Researcher in Computer Science

Side Channel Attacks, Detection and Countermeasures - System Security - Operating Systems

Personal Information

Adress: Lab-STICC, CNRS UMR 6285 Université Bretagne Sud, BP 92116 - 56321 56100, Lorient, France

Date of Birth: 22-02-1991

Nationality: Pakistani

E-mail: maria.mushtaq@univ-ubs.fr

Web Page: www-labsticc.univ-ubs.fr/~mushtaq

Education and Qualifications

2016–2019 **3rd-year PhD Researcher**, *Lab-STICC, Université de Bretagne Sud*, France, *Thesis Title: Consideration of side-channel attacks in the allocation of resources within MPSoC*.

2012–2014 **Masters in Computer Science**, *COMSATS University Islamabad*, Lahore Campus, Pakistan.
CGPA 3.17/4

2008–2012 **Bachelors in Computer Science**, *The Islamia University of Bahawalpur*, Bahawalpur, Pakistan.
CGPA 3.12/4

Professional Experience

08–12/2014 **Visiting Lecturer**, *Dpt. of Computer Science*, The Government Sadiq Women University , Bhawalpur.
Pakistan

2015–2016 **Lecturer**, *Dpt. of Computer Science*, COMSATS University Islamabad, Lahore Campus.
Pakistan

02–08/2016 **Research Officer**, *Dpt. of Electrical Engineering*, Information Technology University, Pakistan.

Skills

Programming Languages	C, C++, HTML, Python, LaTeX
Operating Systems	Windows, Linux
Office	MS Office, Open Office, Beamer
Multiprocessors	Multi and Many-core systems
Security	Cryptosystems, Side Channel Attacks, Detection and Countermeasures

Teaching & Lecturing Experience

2019

Logical Side Channel Attacks, *Lab Sessions for 2nd-year of Masters in Cyber Security (M2 Cyber-Sécurité des Systemes Embarques)*, Sciences et Sciences de l'ingénieur, Université de Bretagne Sud, France.

2016–2015

Human Computer Interaction, *Lectures and Lab Sessions for 4th-year of Bachelor in Computer Sciences*, Dpt. of Computer Science, COMSATS University Islamabad, Lahore Campus, Pakistan.

2016–2015

Research Ethics, *Lectures and Lab Sessions for 4th-year of Bachelor in Computer Sciences*, Dpt. of Computer Science, COMSATS University Islamabad, Lahore Campus, Pakistan.

2016–2015

Introduction to Computers, *Lectures and Lab Sessions for 2nd-year of Bachelor in Psychology*, Dpt. of Psychology, COMSATS University Islamabad, Lahore Campus, Pakistan.

08–12/2014

Computer Architecture, *Lectures and Lab Sessions for 2nd-year of Bachelor in Computer Sciences*, Dpt. of Computer Science, The Government Sadiq Women University, Bahawalpur, Pakistan.

08–12/2014

Introduction to Algorithms, *Lectures and Lab Sessions for 3rd-year of Bachelor in Computer Sciences*, Dpt. of Computer Science, The Government Sadiq Women University, Bhawalpur, Pakistan.

08–12/2014

Assembly Language, *Lectures and Lab Sessions for 3rd-year of Bachelor in Computer Sciences*, Dpt. of Computer Science, The Government Sadiq Women University, Bhawalpur, Pakistan.

Internship Supervisions

2018

Jeremy Bricq, *Implementation of cache-based timing side-Channel attacks in multi- & many-core systems (3 Months)*, Masters in CyberSecurity, Dpt. of Computer Science, Université Libre de Bruxelles, Brussels, Belgium.

2018

Samy Rida, *Implementation of countermeasure techniques for cache-based timing side-channel attacks in multi- & many-core systems (3 Months)*, Masters in Cybersecurity of Embedded Systems, Faculty of sciences and sciences for Engineering, Université Bretagne Sud, Lorient, France.

2018 **Usman Ali**, *Implementation of cache-based timing side-Channel attacks in multi- & many-core systems (3 Months)*, Masters in Electrical Engineering, Dpt. of Electrical Engineering, Information Technology University, Lahore, Pakistan.

Publications

Invited Talks

2019 **Side-channel Information Leakage –Attacks, Detection & Mitigation**, *22nd March 2019*, LIRMM, Université de Montpellier, France.

International Conferences

2019 **Sherlock Holmes of Cache Side-Channel Attacks in Intel's x86 Architecture**,
M. Mushtaq, A. Akram, M. K. Bhatti, C. Maham, V. Lapotre, G. Gogniat, Accepted at IEEE Conference on Communications and Network Security (CNS), Washington, USA, 2019.

2018 **NIGHTs-WATCH: A Cache-Based Side-Channel Intrusion Detector using Hardware Performance Counters**,
M. Mushtaq, A. Akram, M. K. Bhatti, A. Usman, V. Lapotre, G. Gogniat, Published at ISCA-HASP, Los Angeles, USA, 2018.

2018 **Run-time Detection of Prime+Probe Side-Channel Attack on AES Encryption Algorithm**,
M. Mushtaq, A. Akram, M. K. Bhatti, R. N. Raees, V. Lapotre, G. Gogniat, Published at Global Information Infrastructure and Networking Symposium (GIIS), Thessaloniki, Greece, 2018.

2018 **Machine Learning for Security: The case of Side-Channel Attack Detection at Run-time**,
M. Mushtaq, A. Akram, M. K. Bhatti, C. Maham, Y. Muneeb, F. Umer, V. Lapotre, G. Gogniat, Published at IEEE- International Conference on Electronics Circuits and Systems (ICECS), Bordeaux, France, 2018.

2017 **Improving Confidentiality Against Cache-based SCAs**,
M. Mushtaq, M. A. Mukhtar, V. Lapotre, M. K. Bhatti, G. Gogniat, Published at Conference of ACM WomENcourage, Barcelona, Spain, 2017.

International Journals

2019 **WHISPER: A Tool for Run-time Detection of Cache Side-Channel Attacks**,
M. Mushtaq, J. Bricq, M. K. Bhatti, A. Akram, V. Lapotre, G. Gogniat, Under Review at ACM Transactions on Embedded Computing Systems (TECS) since February 2019.

2019 **A Decade of Cache-based Software Side-Channel Attacks & Mitigation Techniques**,
M. Mushtaq, V. Lapotre, M. K. Bhatti, M. A. Mukhtar, G. Gogniat, Under Review at Elsevier Information Systems since February, 2019.

2018 **Meet the Sherlock Holmes of Information Security: Survey of cache SCA Detection Techniques**,
A. Akram, M. Mushtaq, M. K. Bhatti, V. Lapotre, G. Gogniat, Under Review at EURASIP Journal on Information Security (JINS) since August 2018.

2018 **Smart Flush: A Timing Countermeasure against FLUSH+RELOAD Cache-based Side-Channel Attack on RSA**,
M. A. Mukhtar, M. Mushtaq, M. K. Bhatti, V. Lapotre, G. Gogniat, Under Review at Elsevier Journal of Systems Architecture since March, 2019.

2017 **Locality-Aware Task Scheduling of Homogenous Parallel Computing Systems**,
M. K. Bhatti, I. OZ, S. Amin, M. Mushtaq, P. Konstantin, B. Mats, Published at Springer Computing, 2017.

Books

2015 **Developing Trust in Ride Sharing System**,
Mushtaq, M., Ahmad, A., Mirza, H. T, Lambert Academic Publishing, ISBN: 978-3-659-66303-1, 2015.

National Workshops & Presentations

2018 **Cache-Based Side Channel Intrusion Detection using Hardware Performance Counters**,
M. Mushtaq, A. Akram, M. K. Bhatti, V. Lapotre, G. Gogniat, Presented at 16th International Workshops on Cryptographic Architectures Embedded in Logic Devices (CryptArchi), 2018.

2015 **Cache based Side Channels–Attacks & Mitigation**, *Workshop on Cyber Security, Université de Bretagne Sud, Lorient, France*, 2015.

Reviews in International Conferences

2019 **IEEE L-CCS**, *IEEE Control Systems Letters*, 2019.

2019 **IEEE-CCODE**, *IEEE International Conference on Communication, Computing and Digital Systems*, 2019.

2018 **IEEE-FIT**, *IEEE- 17th International Conference on Frontiers of Information Technology*, 2018.

2018 **IEEE-ISVLSI**, *IEEE Symposium on VLSI*, 2018.

Certificates and Appreciations

2019 **Certificate of participation in NeCS Cyber Security Winter school**, *held on 18-22 February*, Fei della Paganella, Trento, Italy, 2019.

2017 **Certificate of participation in 17th International Summer School on Information Security and Protection**, *held on 17-21 July*, Gif-sur-Yvette, Paris, France, 2017.

2012 **Certificate of Participation in 10th International Conference on Frontiers of Information Technology**, *held on 14-16 Dec*, Serena Hotel, Islamabad, Pakistan, 2012.

International Mobility

05–08/2018

Embedded Computing Lab, *Information Technology University, Lahore, Pakistan, Invited PhD Research Stay*,
Extension of detection mechanism to scheduling-based protection mechanism against cache-based side channel attacks.

Honours and Scholarships

2019
2016

Secured PhD Grant by Ministry of Defense and Bretagne Region , *France*.

2018

Secured travel grant for international mobility and research , *Université de Bretagne Sud*, Lorient, France.

2018

Secured travel grant for international mobility and research, *Université de Bretagne Loire*, France.

Trainings

2019

Participation in NeCS Cyber Security Winter school, *held on 18-22 February*, Fei della Paganella, Trento, Italy, 2019.

2017

Participation in 17th International Summer School on Information Security and Protection, *held on 17-21 July*, Gif-sur-Yvette, Paris, France, 2017.

International Collaborations

Dpt. of Elctrical Engineering	ECLab, Information Technology University, Lahore, Pakistan
Dpt. of Computer Engineering	University of California, USA
Dpt. of Computer Engineering	Ajman University, UAE
Dpt. of Electrical and Computer Engineering	Dhofar University, UAE

References

Guy Gogniat
Professor
Lab-STICC
Université Bretagne Sud,
Lorient, France
✉ guy.gogniat@univ-ubs.fr

Vianney Lapotre
Associate Professor
Lab-STICC
Université Bretagne Sud,
Lorient, France
✉ Vianney.lapotre@univ-ubs.fr

Muhammad Khurram Bhatti
Assistant Professor
ECLab
Information Technology University,
Lahore, Pakistan
✉ khurram.bhatti@itu.edu.pk

Languages

Urdu — Native Speaker

English — Professional Profeciency

French — B1 Level Certificate

Personal Interests

- Reading Literature,
- Watching Films,
- Jogging.