Sami Zhioua

INRIA Saclay
1 Rue Honoré d'Estienne d'Orves, Batiment Alan Turing
Campus de l'École Polytechnique, 91940, Palaiseau, France
zhioua@lix.polytechnique.fr

RESEARCH INTEREST

Fairness in Machine Learning, Causality, Reinforcement Learning, Planning and Learning in uncertain environments.
Privacy Enhancing Technologies, Anonymity Protocols, Malware Analysis and Detection, SCADA Security.

JOB EXPERIENCE

INRIA, LIX, École Polytechnique, Paris-Saclay, France
Advanced Researcher — September 2021 - ..

Higher Colleges of Technology (HCT), Dubai, UAE
Assistant Professor — August 2019 - July 2021

King Fahd University of Petroleum and Minerals (KFUPM), KSA
Assistant Professor — September 2009 - August 2019

McGill University, Canada
Postdoctoral research and teaching fellow — January 2008 - August 2009

Université Laval, Canada
Course Lecturer
Teaching and Research Assistant — January 2002 - August 2009

EDUCATION

Université Laval, Canada — February 2008
Ph.D. in Computer Science
Dissertation: *Stoachastic Systems Divergence through Reinforcement Learning*
Advisor: Josée Desharnais
Co-advisor: François Laviolette
External 1 : Martha Kwiatkowska (Oxford University)
External 2 : Doina Precup (McGill University)

Université Laval, Canada — July 2003
M.Sc. in Computer Science, GPA 4.17/4.33

Université de Tunis, Tunisia — July 2000
Institut Supérieur de Gestion (ISG), Tunis
B.Sc. in Computer Science.

TEACHING EXPERIENCE

Undergraduate Courses

- *CIS-2103: Principles of Information Security and Privacy (HCT)*
- *CSF-4613: Security Intelligence (HCT)*
- *CSF-4203: Telecommunications and WAN Security (HCT)*
- *CIS-2003: Statistics and Probabilities (HCT)*
- *CIS-2903: Operating Systems (HCT)*
- *CIN-2103: Fundamentals of Networking (HCT)*
- *CIS-1003: Information Systems in Organizations and Society (HCT)*
- *ICT-2013: Computational Thinking and Coding (HCT)*
- *ICS-444: Computer and Network Security (KFUPM)*
- *ICS-343 : Fundamentals of Computer Networks (KFUPM)*
- *ICS-202 : Data Structures (KFUPM)*
- *ICS-102 : Introduction to Computing I - Java I (KFUPM)*
- *ICS-201 : Introduction to Computing II - Java II (KFUPM)*
- *GLO-3004 : Formal Spec. and Software Verif. (Université Laval)*
- *COMP-322 : Introduction to C++ (McGill University)*

Graduate Courses

- *SEC-511 : Principles of Information Assurance and Security (KFUPM)*
- *SEC-595 : Malware Analysis (KFUPM)*
- *SEC-536 : Web Application Security (KFUPM)*
- *SEC-531 : Secure Software (KFUPM)*

Online Courses

- *IT-500 : Business and Information Technology (SEU, Colorado State Univ)*
- *CS-507 : Introduction to Cyber Security and Digital Crime (SEU, CSU)*
- *IT-575 : Innovative Solutions in Complex Organizations (SEU, CSU)*
- *CS-562 : Enterprise Cyber Security (SEU, CSU)*
- *CS-699 : Capstone Information Security Project (SEU)*
- *CS-683 : Ethical Hacking and Penetration Testing (SEU, CSU)*
- *CS-663 : Digital Forensics and Investigation (SEU, CSU)*

Specialized Trainings (Short Courses)

- *OC1107-105 : Ethical Hacking (KFUPM)(**offered 3 times**)*
- *OC1107-106 : Hands-On Penetration Testing (KFUPM)(**offered 4 times**)*
- *OC127-195 : Malware Analysis (KFUPM)(**offered 3 times**)*
- *OC1306-103 : Web Hacking and Security (KFUPM)(**offered 2 times**)*
- *OC1508-102 : Exploit Reverse-Engineering (KFUPM)(**offered 1 time**)*

THESIS SUPERVISION

- Master Thesis. *Muhammad Aliyu Sulaiman.* ***Attacking Anonymous Communication Networks Through Port Redirection***. Defended May 2012.
- Master Thesis. *Taher Al-Shehari.* ***Web Browsers Resistance to Traffic Analysis Attacks***. Defended November 2014.
- Master Thesis. *Majdi Bin Salman.* ***Fingerprinting Tor Protocol Network Traffic***. Defended December 2014.
- Master Thesis. *Asem Ghaleb.* ***SCADA Security Simulation Testbed Design and Implementation***. Defended December 2015.
- Master Thesis. *Haroon Wardak.* ***SCADA Security Access Control Attacks: Network Detection***. Defended January 2017.
- Master Thesis. *Abdullah Qasem.* ***Network Traffic Analysis Using Approximate Hash Matching***. Defended May 2017.
- Master Thesis. *Yasir Al-Agl.* ***Security Analysis of Tor Protocol Multiplexing Algorithms***. Defended May 2017.
- Master Thesis. *Abdullah Al-Qahtani.* ***Empirical Analysis of Censorship Resistance Systems***. Defended December 2017.

BOOKS

Stochastic Systems Divergence through Reinforcement Learning.
S. Zhioua. Paperback, First Edition, ISBN: 978-3-8473-3971-7, February 2012, LAP Publishing.

A Dynamic Compiler for an Embedded Java Virtual Machine.
S. Zhioua. 96 pages, Paperback, First Edition, ISBN: 3639095065, October 2008, VDM Verlag.

Embedded Java Security: Security for Mobile Devices.
M. Debbabi, M. Saleh, C. Talhi, S. Zhioua. 270 pages, 38 illus., Hardcover, First Edition, ISBN: 978-1-84628-590-5 , November 2006, Springer Verlag.

JOURNAL PAPERS

K. Makhlouf, S. Zhioua, and C. Palamidessi. Machine learning fairness notions: Bridging the gap with real-world applications. *Information Processing Management* Volume 58 Issue 5 (2021)

K. Makhlouf, S. Zhioua, and C. Palamidessi. On the Applicability of ML Fairness Notions. *ACM SIGKDD Explorations Newsletter* Volume 23 Issue 1 June 2021 pp 14–23 (2021)

A. Ghaleb, S. Zhioua, and A. Almulhem. On PLC network security. *International Journal of Criticial Infrastructure Protection (IJCIP)* Volume 22 (2018): Pages 62-69.

T. Al-Shehari and S. Zhioua. An empirical study of web browsers' resistance to traffic analysis and website fingerprinting attacks. *Cluster Computing* Volume 21 Issue 4 (2018): pages 1917-1931.

S. Zhioua. Analyzing anonymity attacks through noisy channels. *Information and Computation Journal*, Volume 244, Pages 76-112, Elsevier, October 2015.

S. Zhioua. The web browser factor in traffic analysis attacks. *Journal of Security and Communication Networks*. Volume 8, Issue 18, Pages 4227-4241. John Wiley & Sons, September 2015.

J. Desharnais, F. Laviolette, and S. Zhioua. Testing Probabilistic Equivalence through Reinforcement Learning. *Information and Computation Journal*, Volume 227, Pages 21-57, Elsevier, June 2013.

S. Zhioua. Tor Traffic Analysis using Hidden Markov Models. *Journal of Security and Communication Networks*, Volume 6, Issue 9, pages 1075-1086, John Wiley & Sons, September 2013.

H. Yahyaoui, S. Zhioua. Boostrapping Trust of Web Services based on Trust Patterns and Hidden Markov Models. *International Journal of Knowledge and Information Systems*. Volume 37, Issue 2, Page 389-416, Springer, 2013.

M. Debbabi, M. Saleh, C. Talhi, and S. Zhioua. Security Evaluation of J2ME CLDC Embedded Java Platform. *Journal of Object Technology*, Vol 5, Nb 2, P 125-154, March-April 2006.

M. Debbabi, A. Gherbi, L. Ketari, C. Talhi, N. Tawbi, H. Yahyaoui, and S. Zhioua. E-Bunny: A Dynamic Compiler for Embedded Java Virtual Machines. *Journal of Object Technology*, Vol 4, Nb 1, P 83-108, January-February 2005.

CONFERENCE PAPERS

A. Qasem, S. Zhioua, and K. Makhlouf. Finding a Needle in a Haystack: The Traffic Analysis Version. Proceedings on Privacy Enhancing Technologies 2019.2 (2019)

A. Amro, S. Almuhammadi, and S. Zhioua. NetInfoMiner: High-level Information Extraction From Network Traffic, IEEE International Conference on Big Data and Smart Computing (IEEE BigComp 2017) Jeju, Korea (February 13-16, 2017).

A. Ghaleb, S. Zhioua, A. Almulhem. SCADA-SST: A SCADA Security Testbed. World Congress on Industrial Control Systems Security (WCICSS-2016). December 12-14, 2016, London, UK.

H. Wardak, S. Zhioua, A. Almulhem. PLC Access Control: A Security Analysis. World Congress on Industrial Control Systems Security (WCICSS-2016). December 12-14, 2016, London, UK.

S. Zhioua, A. Ben Jabeur, M. Langar and W. Ilahi. Detecting Malicious Sessions through Traffic Fingerprinting using Hidden Markov Models. 10th International Conference on Security and Privacy in Communication Networks. Sept 24-26, 2014, China.

S. Zhioua, M. Langar. Traffic Analysis of Web Browsers. Formal Methods in Security (FMS) @ Petri Nets 2014: 20-33.

S. Zhioua. The Middle East under Malware Attack: Dissecting Cyber Weapons. IEEE ICDCS Workshop on Network Forensics, Security and Privacy (NFSP 2013). Philadelphia, USA, July 8, 2013.

M. Sulaiman, S. Zhioua. Attacking Tor through Unpopular Ports. IEEE ICDCS Workshop on Network Forensics, Security and Privacy (NFSP 2013). Philadelphia, USA, July 8, 2013.

S. Zhioua. Anonymity Attacks on Mix Systems: A Formal Analysis. *13th Information Hiding Conference*, Prague, Czech Republic. *Lecture Notes in Computer Science 6958*, Pages 133-147. 2011.

H. Yahyaoui and S. Zhioua. Bootstrapping Trust of Web Services through Behavior Observation. In Proceedings of the *11th International Conference on Web Engineering (ICWE 2011)*, LNCS 6757, Pages 319-330, Paphos, Cyprus, June 2011.

S. Zhioua. A New Information Leakage Measure for Anonymity Protocols. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Volume 50 (Security and Privacy in Communication Networks), Part 8, pages 398-414. Springer, 2010.

S. Zhioua. A Geometric View of Mutual Information: Application to Anonymity Protocols. *In proceedings of the International Symposium on Information Theory and its Applications (ISITA)*. Pages 60-65. October, 2010.

S. Zhioua, J. Desharnais, F. Laviolette, and D. Precup. Learning the Difference between Partially Observable Dynamical Systems. In *Lecture Notes in Artificial Intelligence* (Proceedings of the 20th European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases, ECML-PKDD), 2009.

F. Laviolette, S. Zhioua. Testing Stochastic Processes through Reinforcement Learning. In *NIPS'06 Workshop on Testing of Deployable Learning and Decision Systems*, Kiri Wagstaff, Chris Drummond and Dragos Margineantu (Eds), 8 pages, 2006.

J. Desharnais, F. Laviolette, and S. Zhioua. Testing Probabilistic Equivalence through Reinforcement Learning. In *Lecture Notes in Computer Science*(Proceedings of the 26th Conference on Foundations of Software Technology and Theoretical Computer Science), Vol 4337, P 236-247, Springer, 2006.

J. Desharnais, F. Laviolette, K. Darsini Moturu, and S. Zhioua. Trace Equivalence Characterization through Reinforcement Learning. In *Advances in Artificial Intelligence* (Proceedings of the 19th Canadian Conference on Artificial Intelligence), Vol 4013, P 371-382, Springer, 2006.

M. Debbabi, M. Saleh, C. Talhi, and S. Zhioua. Security Analysis of Mobile Java. In *Proceedings of the 16th International Conference on Database and Expert Systems Applications (DEXA 2005)*, P 231-235, IEEE Computer Society, 2005.

M. Debbabi, M. Saleh, C. Talhi, and S. Zhioua. Java for Mobile Devices: A Security Study. In *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005)*, P 235-244, IEEE Computer Society, 2005.

M. Debbabi, A Gherbi, L. Ketari, C. Talhi, H. Yahyaoui, and S. Zhioua. A Synergy between Efficient Interpretation and Fast Selective Dynamic Compilation for the Acceleration of Embedded Java Virtual Machines. In *Proceedings of the 3rd International Conference on the Principles and Practice of Programming in Java (ACM PPPJ'04)*, P 100-107, ACM Press, 2004.

M. Debbabi, A. Gherbi, L. Ketari, C. Talhi, N. Tawbi, H. Yahyaoui, and S. Zhioua. E-Bunny: A Dynamic Compiler for Embedded Java Virtual Machines. In *Proceedings*

of the 3rd International Conference on the Principles and Practice of Programming in Java (ACM PPPJ'04), P 108-115, ACM Press, 2004.

M. Debbabi, M. Erhioui, L. Ketari, N. Tawbi, H. Yahyaoui, and S. Zhioua. Method Call Acceleration in Java Virtual Machines. In *Lecture Notes in Computer Science* (Proceedings of the International Conference on Computational Science 2003), Vol 2659, P 750-759, Springer, 2003.

PATENTS

Method Call Acceleration in Java Virtual Machines.
M. Debbabi, N. Tawbi, S. Zhioua, M. Erhioui, L. Ketari, H. Yahyaoui.
Patent disclosure filed at:

- US Patent Office: US20020405266P 20020822.
- European Patent Office: EP1394675.
- Japan Patent Office: JP2004086869.
- Chinese Patent Office: CN1251076.

RESEARCH PROJECTS

National Science, Technology and Innovation Plan (NSTIP) Mar 2014 - Mar 2016
Industrial Control Systems (SCADA) Security.

Deanship of Scientific Research (KFUPM) April 2013 – April 2014
Fast-Track Research Grant FT121-011 Traffic Fingerprinting of Tor Anonymity System.

Deanship of Scientific Research (KFUPM) Jan 2012 – Jan 2013
Fast-Track Research Grant SF111-CCSE-17. Investigation of Two New Attacks on Tor Protocol.

Deanship of Scientific Research (KFUPM) Mar 2010 – Jan 2011
Junior Faculty Research Grant JF10007. Towards A new Approach to Analyze Anonymity Protocols.

Concordia University - Alcatel Canada May 2004 - December 2004
Security Analysis of Java Micro Edition (J2ME).

Laval University - Panasonic New York (PINTL) Jan 2002 - March 2003
Acceleration of Java Micro Edition (J2ME).

AWARDS

Merit posdoctoral scholarship from Quebec Government (FQRNT)
$30,000 per year. 2008-2010

Merit Ph.D. scholarship from Quebec Government (FQRNT)
$20,000 per year. 2005-2006

Merit Ph.D. scholarship form Tunisian Government
$12,000 per year. 2003-2006

Merit scholarship form Laval University (Bourse de la fondation)
$12,000 per year (declined for unallowed combination) 2005

Winner of the OCTAS competition.
Acceleration and security of wireless mobile Java platforms. 2006

COMMUNITY SERVICE

Main responsible for the M.Sc. in Information Security program at KFUPM (first master in security program in Saudi Arabia) January 2013 -

Chairman of the Computer Science Curriculum Committee Sept 2011 - Jan 2015

1. Leading a team of 12 faculty members in curriculum activities
2. Leading a major revision of the B.S. in Computer Science program according to the ACM/IEEE Standard

President of the Computer Science Graduate Students Association at Laval University (elected position) Oct 2005 - Oct 2006

1. Represents the graduate students in computer science (more than 100 students),
2. Defends their rights,
3. Organizes academic and social activities. October 2005 - October 2006