# Femi George Olumofin

10791 Gascoigne Drive, Cupertino, CA 95014 203-829-1604 femigolu@gmail.com

## *EXPERIENCE*

**Infoblox** 2015 – Present

Principal Software Engineer

- As the lead engineer for the flagship big-data security analytics SaaS service called Threat Insight (TI), I worked with a small team of engineers to deliver and stabilize the Amazon Web Services-based system under tight deadlines, which resulted in an Infoblox Hero Team award, and a SuperBloxer prize. TI includes a robust data collection pipeline for gathering terabytes of DNS response logs, response policy zone logs, and IP metadata logs in streaming mode from multiple on-premise and cloud sources and a handful of machine learning classifiers to detect data exfiltration/DNS tunneling, fast flux, algorithmically generated domains (aka domain generated algorithms or DGAs), dictionary DGAs, DNS Messenger malware activities, and other DNS-borne threats. In addition, TI features algorithms to tag threats on DNS traffic using multiple feed sources
- Conducted research on homograph detection for internationalized domain names using ML techniques
- Designed and architected the dnstap data collection pipeline, led data preparation for model training, built a generic detector for all classifiers and a regression-testing pipeline for the classifiers to measure detection coverage and false positives over malware packet captures and attack tools, and provided secondary research to validate classification results
- Reviewed security for the earlier SaaS product concepts and provided subject matter expertise in security, privacy and big data analytics

**Pitney Bowes** 2011 – 2015

Privacy Project Engineer

- Designed, implemented, and tested software to solve data privacy and information security problems
- Conducted research on privacy-enhancing technologies and developed intellectual property, use cases, documentation, and software prototypes to enhance the future competitiveness of Pitney Bowes, including private information retrieval (PIR), data de-identification, location authentication/verification, private matching, format-preserving encryption, and pseudo-random permutation.
- Built cryptographic protocols on traditional and embedded hardware (including a FIPS 140-2 Level 3 cryptographic module/HSM) by using C/C++, Java, and C#
- Created software prototypes to enable the deployment of multi-server PIR without replicating sensitive data, and an Android app for point and spatial private information retrieval over the database
- Provided subject matter expertise on privacy technologies to internal teams and maintained connections with the university faculties in the computer security, privacy, and applied cryptography space
- Assessed the privacy impact and developed requirements for the new global product following the privacy guidelines and laws from the US (e.g., HIPAA), Canada (e.g., PIPEDA), and 10 other markets

**University of Waterloo** 2008 – 2011

Doctoral Candidate Researcher

- Conducted research in the Cryptography, Security and Privacy Lab on computer security and privacy, especially as it relates to the private information retrieval: its computational performance, deployment of protocol to resource-constrained devices (e.g., smartphones) for location-based

services, protection of access privacy on large databases, developer-friendly data models for PIR, and concretizing the assumptions of the existing schemes to make them practical
- Wrote and presented technical papers on research findings at international conferences and workshops and reviewed technical papers for many international conferences
- Built software tools to implement technical concepts on Linux, Windows, and Android by using C, C++, and Java

**University of Manitoba** 2004 – 2008
Master's Student and Doctoral Candidate Researcher
- Conducted doctoral candidate research on software security, threat modeling, risk analysis, and how software architectural risks may be discovered through automation
- Developed techniques to assess software architectures, software product lines, or product families
- Studied architectural quality attributes, conformance, domain-specific modeling, and capturing the design knowledge for software architectures
- Wrote and presented technical papers on research findings at international conferences and workshops

**Sybase (now a subsidiary of SAP)** 1998 – 2003
Lead Software Engineer
- Built numerous software products by using HTML, CSS, JavaScript, Java, PowerBuilder, and SQL
- Led a team of six software engineers to build two award-winning products, one of which resulted in a successful mobile and Internet payment startup (now public)

**Compute-Rite Systems** 1997 – 1998
Programmer
- Built a generic access control component for a suite of products (accounting, human resources, and pension) in PowerBuilder to solve a challenging problem for the software company
- Named "Programmer of the Year" by colleagues

## *EDUCATION*

**Ph.D. in Computer Science** University of Waterloo, Waterloo, ON 2011
- Dissertation: *Practical Private Information Retrieval:* Constructs for querying a database while keeping the queries and responses hidden from the database holder
- Advisor: Ian Goldberg

**M.Sc. in Computer Science** University of Manitoba, Winnipeg, MB 2006
- Thesis: *Holistic Assessment of Software Product Line Architectures: The HoPLAA approach*

**B.Sc. in Computer Science (First Class)** University of Benin, Benin City, Edo 1995

## *PUBLICATIONS*

**Refereed Conferences and Workshops**

Bin Yu, Les Smith, Mark Threefoot, and Femi Olumofin, "Behavior Analysis Based DNS Tunneling Detection and Classification with Big Data Technologies," *International Conference on Internet of Things and Big Data (IoTBD, 2016)*, Rome, Italy, April 2016

Ryan Henry, Femi Olumofin, and Ian Goldberg, "Practical PIR for Electronic Commerce," *18th ACM Conference on Computer and Communications Security*," Chicago, IL, October 2011

Prateek Mittal, Femi Olumofin, Carmela Troncoso, Nikita Borisov, and Ian Goldberg, "PIR-Tor: Scalable Anonymous Communication Using Private Information Retrieval," *12th USENIX Security Symposium*, San Francisco, CA, August 2011

Femi Olumofin and Ian Goldberg, "Revisiting the Computational Practicality of Private Information Retrieval," *15th International Conference on Financial Cryptography and Data Security*, Saint Lucia, February 2011

Femi Olumofin and Ian Goldberg, "Privacy-preserving Queries over Relational Databases," *10th Privacy Enhancing Technologies Symposium*, Berlin, Germany, July 2010

Femi Olumofin, Piotr K. Tysowski, Ian Goldberg, and Urs Hengartner, "Achieving Efficient Query Privacy for Location Based Services," *12th Privacy Enhancing Technologies Symposium,* Berlin, Germany, July 2010

Femi Olumofin and Vojislav B. Mišić, "Preserving Architectural Knowledge through Domain-Specific Modeling," *6th Object-Oriented Programming, Systems, Languages & Applications Workshop on Domain-Specific Modeling*, Portland, Oregon, USA, October 2006

Femi Olumofin and Vojislav B. Mišić, "Extending the ATAM Architecture Evaluation to Product Line Architectures," *5th Working IEEE/IFIP Conference on Software Architecture*, pp. 45–56, Pittsburgh, PA, USA, November 2005

Femi Olumofin and Vojislav B. Mišić, "Quality-Driven Conformance Checking in Product Line Architectures," *Workshop on Reengineering towards Product Lines (R2PL, 2005)*, Pittsburgh, PA, November 2005.

Len Bass, Mari Matinlassi, and Femi Olumofin, "Quality Session Report," *5th Working IEEE/IFIP Conference on Software Architecture (WICSA, 2005)*, pp. 191–192, Pittsburgh, PA, November 2005.

John A. Akinyemi, Sylvanus A. Ehikioya, Femi Olumofin, and Chima Adiele, "An Ontology and Knowledge Representation of a Financial Audit System," *Proceedings of the International Association of Science and Technology for Development International Conference on Knowledge Sharing and Collaborative Engineering (KSCE 2004)*, Saint Thomas, U.S. Virgin Islands, November 2004.

**Refereed Journals**

Femi Olumofin and Vojislav B. Mišić, "A Holistic Architecture Assessment Method for Software Product Lines," *Information and Software Technology*, Volume 49, Issue 4, pp. 309–323, April 2007

**Patents/Patent Applications**

"Method and System for Privacy-Friendly Location-Based Advertising," Application 14/872199, filed 01-Oct-2015 (with John Desmond, Qiuju Gu, and Michael Swenson)

"Secure Perfect Hash," Application 14/733000, filed 08-Jun-2015 (with Yassir Nawaz and Shi Hao Yuan)

"Improving Fraud Risk Score Using Location Information while Preserving Privacy of the Location Information," Application 14/831902, filed 21-Aug-2015 (with Jun Zhang)

"Dynamic Database Update in Multi-Server Private Information Retrieval Scheme," Grant No. US9141824B2, 2014

"System and Method for Matching Data Sets While Maintaining Privacy of Each Set," Grant No. US 9443092, 2016 and EU Application 15191414.0-1870, filed 2014 (with Yassir Nawaz)

"Fully Private Marketing Campaign System," Application US20150348087, filed 2014 (with Robert Cordery)

"Method and System for Obtaining Offers from Sellers Using Privacy-Preserving Verifiable Statements," Application US20140337239A1 and Application US20140337239, filed 2013 (with Yassir Nawaz)

"System and Method for Electronic and Physical Delivery of Mail," Application US20140189018, filed 2013 (with Rick Ryan and Yassir Nawaz)

"Method and System for Negotiating Group Offers while Maintaining Privacy of Consumers," Application US20140108134, filed 2012 (with John Desmond, Richard Heiden, Alla Tsipenyuk, Venkat Ghatti, John Merola, and Andrei Obrea)

**Invited Talks**

| | |
|---|---|
| "Practical Private Information Retrieval," Microsoft Research Redmond Cryptography Colloquium, Redmond, WA | Apr 2018 |
| Private Information Retrieval," Pitney Bowes Strategic Technology & Innovation Centre Seminar, Shelton, CT | Mar 2015 |

**Other Selected Talks**

| | |
|---|---|
| "Threat Insight: ATC Big Data Analytics Platform," Infoblox HQ TAD (Technology, Architecture, & Design) Talk, Santa Clara, CA | Apr 2018 |
| "A Primer on Private Information Retrieval," Oracle HQ, Redwood City, CA | Mar 2015 |
| "A Primer on Data De-Identification," Pitney Bowes Algorithms Talk, Shelton, CT | Jul 2014 |
| "Making Cryptography Usage Evident in Applications," short talk at Real World Cryptography Workshop 2014, New York City | Jan 2014 |
| "Private Information Retrieval," Centre for Applied Cryptographic Research (CACR), University of Waterloo | Dec 2010 |
| "Revisiting the Computational Practicality of Private Information Retrieval," Financial Cryptography and Data Security, Saint Lucia | Mar 2011 |
| A rump at the Nineteenth USENIX Security Symposium (Security'10), Washington DC | Aug 2010 |
| "Preserving Access Privacy Over Large Databases," Centre for Applied Cryptographic Research (CACR), University of Waterloo | Dec 2010 |
| "Privacy-preserving Queries over Relational Databases," Privacy Enhancing Technologies Symposium, Berlin, Germany | Jul 2010 |
| "Achieving Efficient Query Privacy in Location-Based Services," Cryptography, Security, and Privacy Group Seminar, University of Waterloo | Mar 2009 |
| Extending the ATAM Architecture Evaluation to Product Line Architectures," Working IEEE/IFIP Conference on Software Architecture (WICSA 2005), Pittsburgh, Pennsylvania | Nov 2005 |
| "Quality-Driven Conformance Checking in Product Line Architectures," International Workshop on Reengineering towards Product Lines (R2PL, 2005), Pittsburgh, Pennsylvania | Nov 2005 |

**Selected Conferences and Workshops**

| | |
|---|---|
| 39th IEEE Symposium on Security and Privacy, San Francisco, CA | May-18 |
| 38th IEEE Symposium on Security and Privacy, San Jose, CA | May-17 |
| 37th IEEE Symposium on Security and Privacy, San Jose, CA | May-16 |
| Real World Cryptography Conference 2016, Stanford, CA | Jan-16 |
| 36th IEEE Symposium on Security and Privacy, San Jose, CA | May-15 |
| 21st ACM Conference on Computer and Communications Security, Scottsdale, AZ | Nov-14 |
| Workshop on Privacy in the Electronic Society (WPES, 2014), Scottsdale, AZ | Nov-14 |
| The ACM Cloud Computing Security Workshop (CCSW, 2014), Scottsdale, AZ | Nov-14 |

| | |
|---|---|
| Real World Cryptography Workshop 2014, New York City | Jan-14 |
| Privacy Enhancing Technologies Symposium 2013, Bloomington, IA | Jul 2013 |
| PETools: Workshop on Privacy Enhancing Tools, Bloomington, IA | Jul 2013 |
| USENIX Security '13 Symposium, Washington, DC | Aug 2013 |
| 2013 USENIX Summit on Hot Topics in Security, Washington, DC | Aug 2013 |

## *AWARDS AND DISTINCTIONS*

- NSERC Postgraduate Scholarship D2 — 2008 – 2010
- President's Graduate Scholarship — 2008 – 2010
- University of Manitoba Graduate Fellowship — 2007 – 2008
- Manitoba Graduate Scholarship — 2007 – 2008
- University of Manitoba UMSU Award — 2007
- Faculty of Science Award — 2005

## *ACADEMIC/PROFESSIONAL SERVICE*

- Session Chair, Location, Mobility, and Privacy Track at WPES — 2014

Reviewer: IEEE SMC 2015, PETS 2013, JBI 2013, CCSW 2012, BJMCS 2012, ESORICS 2011, Eurocrypt 2011, ACM WPES 2011, and ICITST 2011

- Organizer, Pitney Bowes Privacy & Security Conference — 2012 & 2013
- Seminar Organizer, Centre For Applied Cryptographic Research (CACR), University of Waterloo — Jul 2010 - 2011
- Summarizer, login: The USENIX Magazine. Using Humans Session, USENIX Security Symposium 2010 (Security'10) and Networks and Communications Session, Fifth USENIX Workshop on Hot Topics in Security (HotSec, 2010), Washington DC — Aug 2010

## *TEACHING AND SUPERVISING*

**Courses Taught**

- Data Structures & Algorithms (second year), University of Manitoba — Wint. 07 – Sum. 07/08

**Interns Supervised (Infoblox)**

- Athanasios Kountouras, PhD Student in Computer Science, Georgia Institute of Technology — Jun – Aug, 2016

**Interns Supervised (Pitney Bowes)**

- Zhao Chen, 3B Computer Science, University of Waterloo — Jan – Apr, 2014
- Brandon Ma, 3B Mechatronics Engineering, University of Waterloo — Aug – Dec, 2013
- Niles Nelson, 4A Computer Science, University of Waterloo — May – Aug, 2013
- Suchintan Singh, 3B Systems Design Engineering, University of Waterloo — Jan – Apr, 2013

## *AFFILIATIONS*

- Association for Computing Machinery, and IEEE Computer Society
- Past: USENIX, and International Financial Cryptography Association

## *PROFICIENCY*

- Languages: C, C++, Java, Scala, Python, JavaScript, Go, x86 Assembly
- Cloud/Big Data/Tools: Apache Spark, Cassandra, Redis, Jenkins
- Amazon Web Services: EMR, EC2, S3, ELB, VPC, RDS, DynamoDB, DataPipeline, IAM, ElastiCache, Athena and so on
- Operating Systems: Mac, Linux, and Windows

## *VOLUNTEERING*

- Home construction work for a local Mexican family in Ensenada, Mexico — June 2018
- Quality control, Second Harvest Food Bank — Nov 2017
- Home construction work for a local Mexican family in Ensenada, Mexico — June 2017
- Home construction work for a local Mexican family in Ensenada, Mexico — June 2016
- Judge & Sponsor Judge, Connecticut Invention Convention — 2013 – 2014
- Volunteer, Grad Open House, University of Waterloo — Feb 2010
- Volunteer, CS4U, University of Waterloo — Nov 2008
- Graduate Student Representative, CS Dept. Council, University of Manitoba — 2006 – 2007
- Volunteer, University 1 “Meet Your Future Symposium,” University of Manitoba — Oct 2006
- Computer Science Representative, “Evening of Excellence,” University of Manitoba — Jan 2005