

# João Batista Corrêa Gomes Moreira

Rua Paulo de Camargo Ferraz, No. 161  
Cidade Universitária, Barão Geraldo, Campinas – SP. CEP 13083-520  
joao.moreira@lsc.ic.unicamp.br

- Education**
- Ph.D. Student in Computer Science, 2010, Campinas – SP – Brazil**  
Leveraging System Security Through Binary Modification Methods  
Advisor: Prof. Ph.D. Sandro Rigo – Computing Institute – University of Campinas – Unicamp  
Co-advisor: Prof. Ph.D. Vasileios Kemerlis – Computer Science – Brown University  
Funded by: CAPES / CNPq
- Visiting Scholar, 2014 – 2015, New York – NY – USA**  
Leveraging Compiler-Level Instrumentation Methods for Fine-Grained Control-Flow Integrity Implementation  
Project: kCFI – Kernel fine-grained Control-Flow Integrity  
Advisor: Prof. Ph.D. Angelos Keromytis – Department of Computer Science – Columbia University  
Funded by: PDSE – CAPES / Fundação Lemann
- MSc Degree in Computer Science, 2008 – 2010, Campinas – SP – Brazil**  
Power Consumption Analysis in Transactional Memory Systems  
Advisor: Prof. Ph.D. Sandro Rigo – Computing Institute – University of Campinas – Unicamp  
Funded by: CAPES / FAPESP
- Bachelor in Computer Science, 2004 – 2008, Goiânia – GO – Brazil**  
Pontifícia Universidade Católica de Goiás – PUC-GO
- Interests** Computer Architecture, Compilers, Operating Systems, Systems Security
- Research Experience**
- Ph.D. Researcher, Unicamp/Motorola Miletus IoT Group, Motorola, 2015-2016**  
Leveraging Android integration with the Internet of Things – Mentors: Prof. Ph.D. Sandro Rigo, Benício Goulart
- Research Intern, Extreme Computing Group, Microsoft Research, 2013**  
Compiler-based superdiversification for binaries – Mentor: Ph.D. Mariusz Jakubowski
- Undergrad Science Introduction Program, Computer Research Laboratory, UCG, 2007**  
Distributed algorithms and heuristics for genome projects – Advisor: Prof. Ph.D. Wellington Santos Martins
- Development Experience**
- Open Source:**  
**LLVM:** Academic research - Implementing and modifying LLVM's back-end compilation passes  
**Linux Kernel:** Academic research: Modifying/debugging core source code. Implementing new modules  
**Nmap:** Upstream patches and new scripts for NSE – Nmap's Script Engine  
**QEMU:** Academic research: Modifying QEMU's dynamic translator. Implementing new helper functions  
**ArchC:** Academic research: Integration of ArchC ARM models into MPARM cycle-accurate simulation platform
- Student, Google Summer of Code, 2008, 2009, 2010, 2012**  
**2012:** Integration of Nmap into PacketFence  
Mentor: Derek Wuelfrath – <http://packetfence.org>  
**2010:** Development of a web stamp manager for Tux Paint  
Mentor: Bruno Dilly – <http://www.tuxpaint.com>  
**2009:** Improvements on Nmap Script API, development of network security scripts  
Mentor: Gordon "Fyodor" Lyon – <http://nmap.org>  
**2008:** Development of Security layer libraries for OSSIM's Framework  
Mentor: Juan Manuel Lorenzo – <http://www.ossim.net>
- Web Developer, Redeempresarial, 2006-2007**  
Development of web applications with PHP, JavaScript, MySQL, Perl
- Teaching Experience**
- Full Courses given**  
Algorithms and Computer Programming, 1<sup>st</sup> semester 2012, IC - Unicamp  
Algorithms and Computer Programming, 1<sup>st</sup> semester 2014, IC - Unicamp  
Algorithms and Computer Programming, 2<sup>nd</sup> semester 2015, IC - Unicamp
- Teaching Assistant**  
Computer Organization and Assembly Languages, Aug 2009 – Dec 2009, IC – Unicamp  
Networks II, Jan 2007 – Jul 2007, UCG  
Networks I, Aug 2006 – Dec 2006, UCG  
Data Structures I, Aug 2005 – Jul 2006, UCG  
Calculus I, Aug 2004 – Dec 2004, UCG
- Languages** **Portuguese, English:** Reads, Writes and Speaks fluently

## Conference Publications

### **SBSeg 2016**

João Moreira, Sandro Rigo. Go With the FLOW: Fine-Grained Control-Flow Integrity for the Kernel. In XVI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais 2016.

### **SBACPAD 2014**

João Moreira, Lucas Teixeira, Edson Borin, Sandro Rigo. Leveraging Optimization Methods for Dynamically Assisted Control-Flow Integrity Mechanisms. In 26<sup>th</sup> International Symposium on Computer Architecture and High Performance Computing 2014.

### **AMAS-BT 2012**

João Moreira, Divino Lucas, Guido Araujo, Edson Borin, Sandro Rigo. Asynchronous Program Flow Verification Through Binary Instrumentation in QEMU. In Workshop on Architectural and Microarchitectural Support for Binary Translation 2012.

### **RSP 2011**

João Moreira, Felipe Klein, Alexandro Baldassin, Paulo Centoducatte, Rodolfo Azevedo, Sandro Rigo. Using Multiple Abstraction Levels to Speed up an MPSoC Virtual Platform Simulator. In Rapid System Prototyping 2011.

### **ISLPED'10**

Felipe Klein, Alexandro Baldassin, João Moreira, Rodolfo Azevedo, Sandro Rigo. STM versus Lock-based Systems: An Energy Consumption Perspective. In International Symposium on Low Power Electronics and Design 2010.

## Skills

### **Programming Languages:**

- Object oriented: C++, Python, Java
- Script: Lua, Python, Perl, Bash
- Web oriented: PHP, Javascript
- Structured: C
- Database: SQL Language
- Assembly: x86, ARM, AVR

### **System Administration:**

- Installation, configuration, security and maintenance of Linux environments running multiple services

### **Other:**

- Experience with version control systems, IDEs and compiler toolchains
- Knowledge about secure programming and code auditing, including reverse engineering and fuzzing
- Knowledge about network security, TCP/IP and penetration testing

## Talks

### **Conference Presentations:**

#### **Asynchronous Program Flow Verification Through Binary Instrumentation in QEMU, 2012**

- Workshop on Architectural and Microarchitectural Support for Binary Translation. Portland, OR, USA.

#### **Using Multiple Abstraction Levels to Speed up an MPSoC Virtual Platform Simulator, 2011**

- Rapid System Prototyping. Karlsruhe, Germany.

### **Invited Talks:**

#### **Asynchronous Program Flow Verification Through Binary Instrumentation in QEMU**

- AMD Tech Talk. Austin, TX, USA - 2012. *Host:* Mauricio Breternitz

#### **Low Level Playground** - On the implementation of rootkits in PCI devices

- H2HC, Hackers to Hackers Conference. São Paulo, SP, Brazil - 2008. *Host:* Rodrigo Branco

#### **Uso de BioPerl em projetos Genoma** - Development of tools using the BioPerl library

- FISL, Fórum Internacional de Software Livre. Porto Alegre, RS, Brazil - 2008.

#### **Hacking the Big Brother** - How to improve personal privacy

- H2HC, Hackers to Hackers Conference. Brasília, DF, Brazil - 2007. *Host:* Rodrigo Branco

- Ekoparty Hacking Conference. Buenos Aires, Argentina - 2007. *Host:* Federico Kirschbaum

#### **World Wild Worms - XSS-based malware principles**

- H2HC, Hackers to Hackers Conference. Brasília, DF, Brazil - 2007. *Host:* Rodrigo Branco