

Mr. Craig S. Miles

CONTACT INFORMATION

Doctoral Fellow / Graduate Research Assistant
Software Research Laboratory
The Center for Advanced Computer Studies
University of Louisiana at Lafayette

117 Templeton Dr.
Lafayette, LA 70508-5625 USA
Mobile: +1-503-621-8249
E-mail: craig@craigmil.es
WWW: <http://craigmil.es>

RESEARCH INTERESTS

Cyber security and malware defense: reverse engineering, malware analysis, malware detection, malware classification, machine learning, dynamic analysis, static analysis, compilers, optimization, unpacking, and steganography

EDUCATION

University of Louisiana at Lafayette, Lafayette, LA

Ph.D. (**In Progress**), Computer Science, Expected Spring 2014

- Status: ABD
- Gained Candidacy: September, 2012
- Comprehensives: Programming Languages and Compilers, Operating Systems
- Adviser: Professor Arun Lakhotia
- Area of Study: Malware Analysis, Detection, and Classification

The University of Montana, Missoula, MT

M.S., Computer Science, May 2010

- Thesis Topic: *Modern Steganography: An Overview*
- Adviser: Professor Joel Henry

Oregon State University, Corvallis, OR

B.S., Mathematical Sciences, June 2007

- Computer Science option

PROFESSIONAL EXPERIENCE

University of Louisiana at Lafayette, Lafayette, LA

Graduate Research Assistant

August 2010 to present

- Supervisor: Professor Arun Lakhotia
- Project: Malware Analysis and Attribution using Genetic Information (MAAGI) under DARPA I2O Cyber Genome effort.
- Development of new theories and technologies for countering threats relating to malware.
- Development of methodologies for identifying, extracting, comparing, and re-using the functional components of compiled executables.
- Supervision of undergraduate students in computer science in tasks related to malware analysis.

The University of Montana, Missoula, MT

Graduate Research Assistant

April 2009 to October 2009

- Supervisor: Professor Joel Henry
- Project: Distributed Simulation Network under Air Force SBIR AF071-070 (Timely Decision-Making for Logistics Support)
- Summary: A system of discrete simulations running on servers across the internet. Each simulation is representative of a critical component of the global transportation infrastructure such as an airport, seaport, barge terminal, etc. Used to support disaster response planning and exercises for both civil and military organizations.

- Development of a configurable airport simulation built in Arena®.
- Implementation of backing store for simulations.
- Constructed airport simulation validation process.

Translations.com, Corvallis, OR

Localization Engineer

January 2008 to August 2008

- Analysis of web sites/software for localization potential and time/material requirements
- Automation of analysis, file parsing, and filtering
- Re-engineering of translated components
- Ensured compliance with clients requirements and integrity of data
- Interfaced and coordinated with project management, art-graphics personnel, sales and customers
- Provided quotes on new projects for marketing/sales departments

HARDWARE AND SOFTWARE SKILLS

Computer Programming:

- X86 Assembly, C, C++, C#, Java, Perl, PHP, Python, Scheme, UNIX shell scripting, GNU make, SQL, and others

Reverse Engineering:

- IDA Pro, OllyDbg, PEiD, hex editors, Cuckoo Sandbox, Bochs Emulator, unpackers

Dynamic Instrumentation:

- Pin, ParadyN/Dyninst

Numerical Analysis:

- R, Maple, Mathematica

Version Control and Software Configuration Management:

- DVCS (Mercurial, Git), VCS (CVS, SVN)

Information/Internet Technology:

- Networking (TCP/IP, DNS), Services (Apache, SQL, MediaWiki)

Localization and Internationalization Technology:

- SDL Trados, Alchemy Catalyst

Desktop Editing and Productivity Software:

- Vim, Eclipse, Visual Studio
- T_EX (L^AT_EX, B_IB_TE_X),
- Microsoft Office, OpenOffice.org, LibreOffice, Google Drive

Operating Systems:

- Microsoft Windows family, Apple OS X, Linux and other UNIX variants

CERTIFICATIONS

The 2012 International Summer School on Information Security and Protection

- Awarded May 2012

Hex-Rays IDA Pro Advanced Reverse Engineering Course

- Awarded April 2012

Hex-Rays IDA Pro Standard Reverse Engineering Course

- Awarded April 2012

AWARDS

University of Louisiana at Lafayette

- University Fellowship - Tuition and Stipend, 2010–2013

REFEREED
JOURNAL
PUBLICATIONS

- [1] Lakhotia, A., A. Walenstein, C. Miles, and A. Singh. VILO: A Rapid Learning Nearest-Neighbor Classifier for Malware Triage. In: *Journal in Computer Virology*, 2013. doi:10.1007/s11416-013-0178-3
- [2] Miles, C., A. Lakhotia, and A. Walenstein. In Situ Reuse of Logically Extracted Functional Components. *Journal in Computer Virology*. 8(3):73–84. 2012. doi:10.1007/s11416-012-0167-y

CONFERENCE
PUBLICATIONS

- [3] Miles, C., A. Lakhotia, and A. Walenstein. In Situ Reuse of Logically Extracted Functional Components. In: *Proceedings of the 21st Annual EICAR Conference*, May 7–8, 2012. Best Paper Award.
- [4] LeDoux, C., M. Sharkey, B. Primeaux, and C. Miles. Instruction Embedding for Improved Obfuscation. In: *Proceedings of the 50th Annual ACM Southeast Conference (ACM-SE 12)*, March 29–31, 2012.

OTHER
PUBLICATIONS

- [5] Miles, C. *Modern Steganography: An Overview*. Master’s thesis, The University of Montana, Missoula, MT, 2010.

TEACHING
EXPERIENCE

The University of Montana, Missoula, MT

Instructor

Autumn 2009

- Instructor for CS 172: Computer Modeling
 - Problem solving with spreadsheets and databases using the computer to analyze a set of data
 - Presentation of results of analysis

Instructor

Spring 2009

- Instructor for CS 101: Object Oriented Programming
 - Introduction to object-oriented programming using a visual programming environment.
 - Students create programs using drag-and-drop and these programs control animated on-screen characters and objects.

Instructor

Autumn 2008

- Instructor for CS 102: Object Oriented Programming
 - Elementary programming techniques using the Visual BASIC programming language.
 - Students write a wide range of primarily nonmathematical programs.

PROFESSIONAL
SERVICE

Referee Service

- *Software: Practice and Experience*
- *Brazilian Symposium on Information and Computer System Security*

PROFESSIONAL
MEMBERSHIPS

Association for Computing Machinery (ACM), Student Member, 2010–present

REFERENCES
AVAILABLE TO
CONTACT

Removed from online version due to privacy considerations; available upon request.