Frederico Araujo

Research Scientist

website: ibm.biz/faraujo
scholar: goo.gl/Pwl3aQ

Interests & Expertise

Systems and software security, with a focus on Language-based Security and Secure Software Engineering; Compilers, Program Analysis; Formal Methods & Verification, Cloud & Mobile Computing

Education

The University of Texas at Dallas, Richardson, TX **Aug. 2016**
PhD in Software Engineering, GPA: 4.0
Dissertation: *Engineering Cyber Deceptive Software*
Advisor: Dr. Kevin W. Hamlen

The University of Texas at Dallas, Richardson, TX **Dec. 2012**
MS in Computer Science (Major: Software Engineering), GPA: 4.0
Outstanding Academic Achievement

Ecole Centrale Paris, Paris, France **Jun. 2008**
MS in Engineering, Class Rank: Top 15% among 462 students
Sept. 2004 – Jun. 2006

University of São Paulo, São Paulo, Brazil **Dec. 2007**
BS in Electrical and Computer Engineering, Class Rank: Top 1% among 645 students
Jan. 2002 – Jun. 2004, Jul. 2006 – Dec. 2007
Best Senior Thesis Award

Employment History

IBM Research, T.J. Watson Research Center, Yorktown Heights, NY **2016–present**
Research Scientist - Security Research (08/2016 – present)
Fundamental research on cyber security, leading IBM's research efforts on cyber deception defense

The University of Texas at Dallas, Richardson, TX **2010 – 2016**
Research & Teaching Assistant (09/2010 – 05/2015, 09/2015 – 08/2016)
Research on language-based security, network and system security, and honeypoting technologies; teaching and grading for SE/CS graduate and undergraduate level courses; invited lectures on software security and software verification including Model Checking, Theorem Proving, and IBM Rational Rhapsody

IBM Research, T.J. Watson Research Center, Yorktown Heights, NY **2015**
Research Intern - Security Research (06/2015 – 08/2015)
Research on cloud-based moving target defense technologies and cyber deception.

Siemens Chemtech, São Paulo, Brazil **2006 – 2010**
Software Engineer (01/2008 – 07/2010), *Engineering Intern* (07/2006 – 12/2007)
Technical lead and software architect on large-scale software projects on business logistics, supply chain integration, and manufacturing execution systems for clients such as BRFoods (world's tenth-largest food company), CSN (the second major steel-maker company in Brazil), and Transnet Pipelines South Africa. Complete list of projects available at `https://www.linkedin.com/in/fredericoaraujo`

Imaintel Systèmes de Vision, Fourquex, France **2005**
Engineering Intern (06/2005 – 08/2005)
Designed and developed the company's website and web customer services portal

University of São Paulo, São Paulo, Brazil **2003 – 2004**
Research Assistant (01/2003 – 07/2004)
Study of Artificial Neural Networks to support safety analysis and fault location on distributed systems; development of computer tools using MatLab and C++ to support network simulations

Honors, Grants & Awards

2015 *NSA CAE Cybersecurity Research Grant (primary student contributor)*, 2015–2016, $287K
2014 *NYU-Poly CSAW Best Applied Security Research Paper Award*, 2nd prize
NSF Grant to attend Oregon Programming Languages Summer School
2013 *Best Demonstration Paper Award* at AAMAS'13
2012 *Certificate of Outstanding Academic Achievement*, University of Texas at Dallas
Best Overall Paper Award at SpringSim12, Society for Modeling & Simulation
Best Paper Award at the Agent-Directed Simulation Symposium at SpringSim12
Ericsson Graduate Fellowship, Ericsson United States
2008 *Academic Excellence Award* by Accenture in recognition of senior thesis project
2007 *Best Senior Thesis Award*, University of São Paulo
Best Software Product Developed for the Industry Award, University of São Paulo
2005 *Academic Excellence Scholarship (Capes/Brafitec)*, Brazilian Ministry of Education
2004 *Academic Excellence Scholarship (Capes/Brafitec)*, Brazilian Ministry of Education

Publications

goo.gl/Pwl3aQ

[8] **Araujo, F.**, Hamlen, K.W., Embedded Honeypotting. In Cyber Deception: Building the Scientific Foundation. Springer, 2016.

[7] **Araujo, F.**, Hamlen, K.W., Compiler-instrumented, Dynamic Secret-Redaction of Legacy Processes for Attacker Deception. In *Proceedings of the 24th USENIX Security Symposium*, Aug. 2015. [Acceptance rate: 15.7%]

[6] **Araujo, F.**, Shapouri, M., Pandey, S., Hamlen, K.W., Experiences with Honey-Patching in Active Cyber Security Education. In *Proceedings of the 8th Workshop on Cyber Security Experimentation and Test (CSET)*, 2015. [Acceptance rate: 26.7%]

[5] **Araujo, F.**, Hamlen, K.W., Bierdemann, S., and Katzenbeisser, S., From Patches to Honey-patches: Lightweight Attacker Misdirection, Deception, and Disinformation. In *Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS)*, 2014. NYU-Poli CSAW **Best Applied Security Paper Award**, 2nd prize. [Acceptance rate: 19.5%]

[4] Al-Zinati, M., **Araujo, F.**, Kuiper, D., Valente, J. and Wenkstern, R.Z., DIVAs 4.0: A Multi-Agent Based Simulation Framework. In *Proceedings of the 17th IEEE/ACM Int. Symposium on Distributed Simulation and Real Time Applications (DS-RT)*, 2013.

[3] **Araujo, F.**, Al-Zinati, M., Valente, J., Kuiper, D. and Wenkstern, R.Z., DIVAs 4.0: A Framework for the Development of Situated Multi-Agent Based Simulation Systems. In *Proceedings of the 12th International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, 2013. **Best Demonstration Paper Award**

[2] Valente, J., **Araujo, F.** and Wenkstern, R.Z., On Modeling and Verification of Agent-Based Traffic Simulation Properties in Alloy. *Journal of Agent Technologies and Systems (IJATS)*, 2012.

[1] **Araujo, F.**, Valente, J. and Wenkstern, R.Z., Modeling Agent-Based Traffic Simulation Properties in Alloy. *In Proceedings of the 2012 Symposium on Agent Directed Simulation (ADS)*, 2012. **Best Paper Award** and **Best Overall Paper Award**

Posters & Demos

Araujo, F., POSTER: From Patches to Honey-patches: Lightweight Attacker Misdirection, Deception, and Disinformation. *In 21th Cybersecurity Awareness Week Conference (CSAW)*, November, 2014. NYU-Poli, NYC.

Araujo, F., POSTER: Heartbleed Counter-attack. Poster and live demonstration presented at the Texas Security Awareness Week (TxSAW), October, 2014. UTDallas, Richardson, TX.

Araujo, F., DEMO: DIVAs 4.0: A Framework for the Development of Situated Multi-Agent Based Simulation Systems. Live demonstration presented at AAMAS'13, May, 2013. Saint Paul, MN.

Press & Media Coverage

CNBC. *World's Biggest Student Cyber Security Contests Reveal Best Young Hackers and Researchers.* Also seen in *Yahoo! News.* 11/17/2014. NYU-Poli Press Release

The Mercury *'Red Herring' turns tables on hackers.* 4/28/2014. UTD Mercury

Times of India. *New technique Red Herring fights 'Heartbleed' virus.* Also seen in *Yahoo! News.* 4/15/2014. The Economic Times – Software

CW33. *UTD Professor Creates Solution to 'Heartbleed' bug.* 4/15/2014. CW33 Dallas

CBS. *Dallas Professor Develops Stealth Program To Trap Hackers.* 4/15/2014. CBS 11 News

ScienceDaily. *Cybersecurity researchers roll out a new heartbleed solution.* 4/14/2014. Science News

Research Projects

SignaC, New Information Flow Controls for LLVM **2014 – 2016**

Supported by AFOSR, NSF, ONR, and NSA awards

Compiler instrumentation of a new taint-tracking semantics and in-memory secret redaction support into annotated C/C++ programs, yielding programs that can self-censor their address spaces in response to emerging cyber-attacks. The enhanced semantics support declarative secret annotations for legacy codes, greatly reducing the annotation burden imposed on developers, while curtailing label-creep and taint spread behavior. Work accepted at USENIX Security'15 [7]. (LLVM | Dynamic Taint Analysis)

RedHerring, Deceptive Security Patching **2013 – 2016**

Supported by AFOSR, NSF, ONR, and NSA awards

Designed and implemented a new software patching methodology, called *honey-patching*, in which elements of deception and runtime self-replication are combined to dissuade attackers from exploiting known system vulnerabilities. Honey-patches patch software security vulnerabilities in such a way that future attempted exploits of the patched vulnerabilities appear successful to attackers, while augmenting the server with an embedded honeypot that waylays, monitors, and disinforms criminals. Work accepted at CCS'14 [5] and CSET'15 [6], and awarded *best applied security paper* at CSAW'14. (Systems & Language-based Security)

DIVAs 4, Multi-agent Simulation Framework **2012 – 2013**

Re-engineered and developed DIVAs 4, a real-time multi-agent simulation framework for situated virtual environments in which autonomous agents perceive their surroundings through multiple senses. Designed and developed a decentralized, self-organizing virtual environment, which significantly improved performance and scalability—30 to 3K concurrent agents per simulation node. Work accepted at AAMAS'13 [3] and DS-RT'13 [4]. (Real-time Systems Design | Framework Design)

MATISSE, Agent-based Intelligent Traffic Simulation **2011 – 2012**

Used the Alloy language and analyzer to formalize, specify and verify a simulation model for an agent-based intelligent transportation system. Work accepted at ADS'12 and IJATS'12 and awarded two *best paper awards*. (Alloy | Formal Methods)

HOPE, Mobile Assistive and Augmented Communication Android App **2011 – 2012**

Adaptive, context-aware user modeling for the HOPE (Help Our People Easily) assistive mobile application, based on captured contextual information inferred from user click patterns. Formally specified and verified the adaptation algorithm in Alloy (Android | Machine Learning)

Teaching & Mentorship

▶ **Teaching**

Penetration Testing and Active Cyber-Defense Workshop, *TxSAW* *Fall 2015*

I am helping organize this year's TxSAW (Texas Security Awareness Week) at UT Dallas, where we expect to receive over 50 high school students who will compete in a CTF exercise; as part of the two-day program, I am leading the preparation of a workshop on penetration testing and active cyber-defense with hands-on lab to be delivered to students prior to the CTF.

Active Cyber-Defense Educational Lab, *UT Dallas* *Spring 2015*

Modern cyber security educational programs that emphasize technical skills often omit or struggle to effectively teach the increasingly important science of cyber deception. In April of 2015, I led an open lab at UTD with the main goal of educating students on offensive security and active cyber-defense concepts using honey-patching as the underlying framework. The lab is documented in [6].

▶ **Teaching Assistant,** *UT Dallas*

Created and graded homeworks, midterms, and final exams; designed term projects and gave lectures.

CS6371–Advanced Programming Languages (31 students)	*Spring 2014*
CS6324–Information Security (54 students)	*Spring 2014*
CS6362–Advanced Software Architecture (36, 35, 28 students)	*Fall 2010, 2012, 2013*
CS6361–Advanced Requirements Engineering (40, 65 students)	*Spring 2013, Fall 2013*
CS6375–Machine Learning (62 students)	*Spring 2013*
CS6387–Advanced Software Engineering (15 students)	*Spring 2013*

CS6V81–Advanced Web Developement (25 students) *Spring 2012*
CS6359–Object Oriented Analysis and Design (43, 32 students) *Spring 2011, 2012*
CS3354–Software Engineering (67, 25 students) *Fall 2011, 2012*
CS3340–Computer Architecture (58, 20 students) *Fall 2010, Summer 2011*

▶ Student Mentoring

Carter Poe, (Undergraduate Student; UT Dallas)
2015–present *Comparative study of public cloud infrastructures for the suitability of deception-based defenses deployment*

Mahdi Shapouri, (M.S. Student; UT Dallas)
2014–present *Dynamic generation of IDS signatures via honey-patching*
Preparation of education lab on active defense using Shellshock

Sonakshi Pandey, (M.S. Student; UT Dallas)
Spring 2015 *Preparation of education lab on active defense using Shellshock*

Chaofan Shi, (M.S. Student; UT Dallas; now Software Engineer at eBay)
Fall 2012 *Visualization framework for distributed multi-agent simulation system*

Talks, Lectures & Presentations

▶ Invited Talks

Engineering Cyber-Deceptive Software
University of Arizona, Virginia Tech, UC Santa Cruz, University of Nebraska-Lincoln, University of Rochester, University of Connecticut, Rochester Institute of Technology, Kansas State University, University of North Carolina-Charlotte, University of North Texas, University of Colorado Denver, University of Colorado Colorado Springs, Seattle University, Miami University-Oxford, Northern Kentucky University, IBM T.J. Watson Research Center. January–March 2016.
I gave this series of talks during job hunting prior to graduation. I received 12 tenure-track Assistant Professor offers from U.S. research universities and one Research Scientist offer from IBM. `goo.gl/MyGlfR`

Compiler-instrumented, Dynamic Secret-Redaction of Legacy Processes for Attacker Deception
IBM Security "show'n'tell" Series , IBM T.J. Watson, August 2015

Introduction to Cyber-Deception Defense
TCEA Statewide Programming Contest Workshop, UT Dallas. May 2015

From Patches to Honey-patches
CS Department "Let's Talk" Series, UT Dallas, December 2014

▶ Selected Guest Lectures

Dynamic Secret Redaction for Attacker Deception
CS6301–Language-based Security, UT Dallas (Fall 2015)
Instructor: Prof. Kevin Hamlen

Introduction to Honeypots and Honey-patching
CS6301–Language-based Security, UT Dallas (Fall 2014, Fall 2015)
Instructor: Prof. Kevin Hamlen

Using Honeypots for Attack Detection and Analysis
CS4398–Digital Forensics, UT Dallas (Fall 2014)
Instructor: Prof. Bhavani Thuraisingham

An Introduction to Model Checking
CS6362–Advanced Requirements Engineering, UT Dallas (Spring 2013)
Instructor: Prof. Lawrence Chung

Formal Methods and a Tutorial on the Alloy Model Finder
CS6362–Advanced Requirements Engineering, UT Dallas (Spring 2013)
Instructor: Prof. Lawrence Chung

Model-driven Design with IBM Rhapsody
Executive Master in Software Engineering, UT Dallas (Spring 2012)
Instructor: Prof. Rym Wenkstern

Scenario-based Verification
CS6362–Advanced Software Architecture, UT Dallas (Fall 2010)
Instructor: Prof. Kendra Cooper

Automated Theorem Proving for the Verification of Software Systems
CS6362–Advanced Software Architecture, UT Dallas (Fall 2010)
Instructor: Prof. Kendra Cooper

Model Checking, a tutorial on SPIN model checker
CS6362–Advanced Software Architecture, UT Dallas (Fall 2010)
Instructor: Prof. Kendra Cooper

▶ **Conference Presentations**

Compiler-instrumented, Dynamic Secret-Redaction of Legacy Processes for Attacker Deception [presentation video]
USENIX Security Symposium (USENIX Sec), Washington D.C., Aug 2015

Experiences with Honey-Patching in Active Cyber Security Education
Work. Computer Experimentation and Test (CSET), Washington D.C., Aug 2015

From Patches to Honey-patches: Lightweight Attacker Misdirection, Deception, and Disinformation
ACM Conf. on Computer and Communications Security (CCS), Scottsdale, AZ, Nov 2014

Modeling agent-based traffic simulation properties in Alloy
Symposium on Agent Directed Simulation (ADS), Orlando, FL, Mar 2012

Open Source Contribution

Clang Quala `https://github.com/sampsyo/clang-quala`
Quala adds overlay type systems to LLVM and Clang, inspired by Java 8's JSR-308 and the Checker Framework, enabling user-customizable type systems on legacy C/C++ and making it possible to add optional checks to a language without hacking the compiler. I ported Quala to version 3.7 of LLVM and Clang as part of my research work on SignaC to implement declarative secret annotations.

AIMA `https://github.com/aima-java/aima-java/wiki/AIMA3e-Overview`
AIMA (Artificial Intelligence: A Modern Approach) is the leading textbook in Artificial Intelligence, being used in over 1300 universities in over 110 countries. During my graduate-level Artificial Intelligence class at UT Dallas, I discovered a bug in one of the book's Java-implemented algorithms for uninformed search. I submitted the bug report with the suggested patch, which has been accepted and applied to the online code base.

Service

External reviewer for SEDE 2011, SEDE 2012, and IEEE ACSEAC 2012.

Technical Skills

Programming	C, C++, Java, .Net (C#, Asp.Net, Asp.MVC), Python, OCaml
Web & Mobile Development	Android, HTML, CSS, JavaScript, JQuery, Ajax, Node.js
Databases	SQL Server, Oracle, MySQL
Software Engineering	UML, RUP, Test-Driven Development, IBM Rational Rhapsody, System Architecture, Enterprise Integration Patterns, Design Patterns, Refactoring, Reverse Engineering
Software Configuration Mgt	SVN, GIT, Darcs, Maven, Jenkins, Apache Archiva, Trac
Formal Modeling	Model Checking, Theorem Proving, Alloy, Coq
Program Analysis	Information-flow Analysis, Type Theory
Compiler Development	LLVM, Clang
Virtualization	VMWare ESXi, Linux Containers (LXC)
Intrusion Detection	Snort, Bro, Honeypots (mhn)

Languages

English (Fluent), *Portuguese* (Native), *French* (Fluent)