## Gen Lu


CONTACT INFORMATION

Gould-Simpson Building 749
Department of Computer Science
The University of Arizona
Tucson, AZ 85721

Phone: 217-819-8596
Email: genlu@cs.arizona.edu
URL: http://www.cs.arizona.edu/~genlu/


RESEARCH INTERESTS

Program analysis and optimization with a focus on analysis and reverse engineering of malware code, Web security, Software security

EDUCATION

**The University of Arizona**, Tucson, AZ

Ph.D., Computer Science, GPA: 4.0 — *expected:* December, 2013

- Advisor: Saumya K. Debray, Ph.D

**University of Wisconsin-Milwaukee**, Milwaukee, WI

M.S., Computer Science, GPA: 3.89 — May 2008

**Beihang University**, Beijing, China

B.E., Computer Science, — July 2006

RESEARCH EXPERIENCE

**Research assistant** — August 2010 to present

Department of Computer Science, The University of Arizona
Supervisor: Saumya Debray Ph.D

- Designed and implemented a system for defending against environment-dependent JavaScript malware, the technique is based on data-flow analysis and program slicing, which imposes minimum performance overhead and can handle cloaking techniques implemented by various control transfer mechanisms, including cases where existing multi-path exploration techniques fail
- Designed and implemented a combination of cloaking techniques by targeting the limitations of existing malware detection and analysis systems, which can effectively hide JavaScript malware from state-of-the-art detectors
- Designed and implemented a dynamic analysis system for automatic simplification of obfuscated JavaScript code, the system is based on data-flow analysis and program slicing and consists of components for execution tracing, code analysis and JavaScript decompilation
- Developed a dynamic analysis system for deobfuscation of virtualization-obfuscated X86 programs, which is based on various program analysis and optimization techniques and automatically eliminates up to 99% of obfuscation instructions introduced by existing obfuscators

**Research assistant** — May 2009 to May 2010

Department of Computer Science, The University of Arizona
Supervisor: Chris Gniady, Ph.D

- Designed and implemented energy management techniques in virtual machine environment (Xen), which enhance the coordination and synchronization between virtual machines and virtual machine monitor, and reduce energy consumption of hard disk by 14.8% with 0.5% increase in execution time

## Publications

**Gen Lu**, Saumya K. Debray, "A Simple Client-Side Defense Against Environment-Dependent Web-Based Malware" *8th International Conference on Malicious and Unwanted Software (MALWARE'13 The Americas)* , October 2013 (to appear)

**Gen Lu**, Saumya K. Debray, "Weaknesses in Defenses against Web-Borne Malware (Short Paper)" *In the Proceedings of 10th International Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA'13)*, 139-149, July 2013.

**Gen Lu**, Saumya K. Debray, "Automatic Simplification of Obfuscated JavaScript Code: A Semantics-Based Approach" *In the Proceedings of 6th IEEE International Conference on Software Security and Reliability (SERE'12)*, 31-40, June 2012.

**Gen Lu**, Kevin Coogan, Saumya K. Debray, "Automatic Simplification of Obfuscated JavaScript Code (Extended Abstract)" *In the Proceedings of ICISTM-12 Workshop on Program Protection and Reverse Engineering (PPREW)*, 348-359, March 2012.

Kevin Coogan, **Gen Lu**, Saumya K. Debray, "Deobfuscation of virtualization-obfuscated software: a semantics-based approach" *In the Proceedings of 18th ACM Conference on Computer and Communications Security (CCS'11)*, 275-284, October 2011.

Lei Ye, **Gen Lu**, Sushanth Kumar, Chris Gniady, John H. Hartman, "Energy-efficient storage in virtual machine environments" *In the Proceedings of Proceedings of the 6th International Conference on Virtual Execution Environments (VEE'10)*, 75-84, March 2010.

## Relevant Projects

**Simulation of CPU Pipeline and Cache** Jan 2009 - May 2009

- Implemented a CPU simulator with pipelining for DLX instruction set and a CPU cache simulator

**Virtual Software Router** Jan 2009 - May 2009

- Implemented virtual router supporting ARP, ICMP, TCP/IP and OSPF protocols

**Operating System** Jan 2009 - May 2009

- Implemented the operating system functionalities of interrupt handing, device drivers, process scheduling, and memory management on top of a computer system simulator

## Invited Talks

"Weaknesses in Defenses against Web-Borne Malware", 10th International Conference on Detection of Intrusions and Malware and Vulnerability Assessment, Berlin, Germany, July, 2013

"Automatic Simplification of Obfuscated JavaScript Code: A Semantics-Based Approach", 6th IEEE International Conference on Software Security and Reliability, Washington, D.C., June 2012

"Distinct triangle areas in a planar point set", 12th Conference on Integer Programming and Combinatorial Optimization, Ithaca, NY, June 2007

## Teaching Experience

**Instructor**

Department of Computer Science, The University of Arizona

CSc345 - Analysis of Discrete Structures Summer 2011

- Designed syllabus, gave lectures, designed and graded homework, quizzes, and exams

**Teaching assistant**

Department of Computer Science, The University of Arizona

CSc422 - Introduction to Parallel and Distributed Programming Spring 2010

CSc372 - Comparative Programming Languages — Fall 2009
CSc452 - Principles of Operating Systems — Spring 2009

AWARDS

The University of Arizona, Graduate College College of Science Fellowship, 2013
University of Wisconsin-Milwaukee, Chancellor's Graduate Student Award, 2006 & 2007