Babak Yadegari

1040 E. 4th St., Tucson, AZ
Office: Room 846
☎ *(520) 243 0433*
✉ *babaky@cs.arizona.edu*

Education

2016 **Post-Doctoral Research Associate**, *University of Arizona*, Tucson, AZ.

2011–2016 **PhD, Computer Science**, *University of Arizona*, Tucson, AZ.

Advisor: Professor Saumya Debray

2005–2010 **BS, Computer Science and Engineering**, *Shiraz University*, Shiraz, Iran.

Experience

2011–present **Research Associate**, *Lynx Research Group, University of Arizona*, Tucson, AZ.
Focused on development of algorithms and tools to automate the process of penetrating various anti-analysis defenses erected by malware. The Approaches are semantics-based meaning they are not based on superficial syntactic characteristics that can be easily changed, and generic so they are not specific to any particular techniques used by the malware authors.

Summer and Fall 2009 **Research Assistant**, *APA Research Group, Shiraz University*, Shiraz, Iran.
Worked on a number of projects trying to apply data mining algorithms and techniques to identify malicious code based on windows API calls, either by extracting calls from the executable image (static) or by running the executable and monitor the system calls (dynamic).

Fall 2010 **Workshop**, *Shiraz University*, Shiraz, Iran.
Held one session workshop on penetration testing and SQL injection mostly based on Certified Ethical Hacking (CEH) trainings.

Fall 2008, 2007 **Teaching Assistant**, *Shiraz University*, Shiraz, Iran.
Operating Systems Concepts, Assembly and Machine Languages Programming.

Technical Experience

Proficient With

languages C/C++, Python, X86 Assembler, C#, Matlab

technologies Ollydbg, MySQL, SQLite, LaTeX, Bash Scripting, CVS, SVN

Familiar With

languages Java, PHP, Perl, Erlang, J2EE (under Tomcat), ASP.NET (under IIS)

technologies Django, Apache

Certificates

Network+, Redhat Certified Engineer (RHCE)

Achievements and Awards

Spring 2016 Received Graduate Assistant Fellowship, Computer Science Department, University of Arizona

Fall 2015 My paper ”A Generic Approach to Automatic Deobfuscation of Executable Code” was selected among ten finalists in Cyber Security Awareness Week (CSAW’15)

Spring 2015 Outstanding Research Assistant, Computer Science Department, University of Arizona

Spring 2015 Outstanding Research Assistant Award, Graduate and Professional Students Council, Graduate College, University of Arizona

Spring 2015 Received Galileo Circle Scholars Fellowship, University of Arizona

Spring 2015 Received Graduate Assistant Fellowship, Computer Science Department, University of Arizona

Fall 2008 First place in Shiraz University hacking contest to identify and repair vulnerabilities in the university network, Shiraz University

Selected Coursework Projects

University of Arizona, Tucson

Cloud Computing Adopted Swift distributed object store (originally implemented for use in open-stack) to planet-lab with automatic scaling and tenant/user based authentication.

Advanced Operating Systems Implemented a log-structured file system using FUSE user space file-system library featuring crash recovery and garbage collection.

Computer Networking Implemented a simple network router to route network packets between other routers and application servers with inter-domain routing to update routing tables dynamically.

Selected Publications

[1] Yadegari, Babak ; Debray, Saumya: Symbolic Execution of Obfuscated Code. In: *22nd ACM Conference on Computer and Communications Security (CCS)*, 2015

[2] Yadegari, Babak ; Johanesmayer, Brian ; Whitely, Benjamin ; Debray, Saumya: A Generic Approach to Automatic Deobfuscation of Executable Code. In: *IEEE Symposium on Security and Privacy (OAKLAND)*, 2015

[3] Qiu, Jing ; Yadegari, Babak ; Johanesmayer, Brian ; Whitely, Benjamin ; Debray, Saumya: Identifying and Understanding Self-Checksumming Defenses in Software. In: *Fifth ACM Conference on Data and Application Security and Privacy*, 2015

[4] Yadegari, Babak ; Debray, Saumya: Bit-Level Taint Analysis. In: *14th IEEE International Working Conference on Source Code Analysis and Manipulation (SCAM)*, 2014

[5] Ahmadi, Mansour ; Sami, Ashkan ; Rahimi, Hossein ; Yadegari, Babak: Malware detection by behavioural sequential patterns. In: *Computer Fraud and Security* 2013 (2013), Nr. 8, S. 11–19

[6] Ahmadi, Mansour ; Sami, Ashkan ; Rahimi, Hossein ; Yadegari, Babak: Iterative System Call Patterns Blow the Malware Cover. In: *Security for The Next Generation (Best Paper Award)*, 2011

[7] Sami, Ashkan ; Yadegari, Babak ; Rahimi, Hossein ; Peiravian, Naser ; Hashemi, Sattar ; Hamze, Ali: Malware detection based on mining API calls. In: *Proceedings of the 2010 ACM Symposium on Applied Computing* ACM, 2010, S. 1020–1025

[8] Sami, Ashkan ; Peiravian, Naser ; Yadegari, Babak ; Rahimi, Hossein: Data Mining for CRM on massive and unbalance data Of telecommunication companies. In: *Third International Conference on Data Mining*, 2010