Evangelos (Vaggelis) Atlidakis

400 West 119th Street
New York, NY 10027
vatlidak@cs.columbia.edu
http://www.cs.columbia.edu/~vatlidak/

RESEARCH INTERESTS

Operating Systems, Distributed Systems, Security, Machine Learning Systems

EDUCATION

Columbia University, New York, NY — Oct. 2013 - Present
Ph.D. in Computer Science
GPA: 3.85/4
Advisors: Roxana Geambasu, Jason Nieh

University of Athens, Athens, Greece — Sep. 2005 - Aug. 2011
Bachelor of Informatics and Telecommunications
Advisors: Alex Delis, Mema Roussopoulos
GPA: 9/10

Helsinki University of Technology, Helsinki, Finland — Jan. 2009 - Jun. 2009
Exchange Student, Department of Computer Science
GPA: 10/10

EXPERIENCE

Research Intern — May 2017 - Aug 2017
Microsof Research, Microsoft, Redmond, WA, USA
Member of Microsoft Security Risk Detection Team (previously known as Project Springfield)
Supervisors: Marina Polishchuk, Patrice Godefroid

Research Associate — Sep 2012 - Sep 2013
CERN, Geneva, Switzerland
Worked on the Agile Infrastructure project; a IaaS private CERN cloud
Supervisor: Ignacio Reguero

Undergraduate Researcher — Feb 2010 - May 2011
University of Athens, Athens, Greece
Conducted research on distributed systems
Advisors: Alex Delis and Mema Roussopoulos

RESEARCH:

My research interests are in computer systems, including operating systems (OSes), distributed systems, and machine learning (ML) systems. Currently, I focus on addressing challenges inherent in the development of modern mobile, cloud, and ML applications. These applications are fundamentally different from traditional desktop applications and require renewed support from operating systems as well as new development environments. I have been running measurement studies to identify missing or mismatched abstractions for modern applications, and invent new programming abstractions and systems to support the needs of modern applications. Following are some example projects in this space.

Measurement of POSIX Abstractions in Modern OSes:
In my latest work [1, 2], I demonstrated that the abstractions offered by traditional OS standards, such as the POSIX API, are insufficient to support modern applications, such as those running on

Android, iOS, and OSX. Modern applications rely upon very different abstractions, which are currently supplied by user-space libraries implemented atop POSIX. This layering causes mismatches, inefficiencies, and even security risks. For example, I found that new abstractions typically rely on POSIX extension APIs (i.e., `ioctl`) to implement their functionality, suggesting that POSIX lacks appropriate abstractions for modern workloads. Extension APIs are problematic, because their invocations cannot be mediated by the OS, putting pressure on user-space libraries and kernel device drivers to implement correct and coherent protections of these invocations. I am now studying specific implications and identifying the new OS abstractions needed to more securely support modern applications.

Testing Tools for Data-Driven Applications:
A key aspect characterizing modern applications is their increased reliance on data and data-driven decision making. While often beneficial, this practice can have subtle detrimental consequences, such as discriminatory or racially offensive effects. I argue that such effects are bugs that should be tested for and debugged in a manner similar to functionality, reliability, and performance bugs. To this end, I developed *FairTest*, a testing toolkit for data-driven applications that identifies unwarranted association between an applications outputs and user subpopulations, including sensitive groups (e.g., defined by race or gender). Our paper [3], accepted in the second European Symposium on Security and Privacy, has attracted attention from several investigative journalists, who are considering using it to study unwarranted associations in several applications.

Security of Machine Learning Systems under Adversarial Settings:
State of the art machine learning systems, such as those using deep neural networks for classification and regression, have recently achieved unprecedented success in a variety of tasks ranging from image and speech recognition to data compression. However, recent work has made an intriguing discovery: these systems are extremely susceptible to adversarial attacks. That is, an adversary can modify correctly classified samples by adding an infinitesimal amount of carefully crafted noise that will force the model to misclassify (with high confidence) samples only marginally different from the original ones. In lieu of these vulnerabilities, I am currently working on defences to harden machine learning systems and increase their robustness against adversarial attacks. My long-term goal is to contribute solutions that will shed light into arcane ML models and will arm developers with powerful debugging primitives to help identify and address subtle security, performance, and reliability challenges.

Previous Projects:
Before joining Columbia, I worked on several projects related to distributed, peer-to-peer systems, such as BitTorrent. In one project, I enhanced BitTorrent with an optimistic unchocking policy that improves the quality of inter-connections amongst peers and increases the number of peers that are both directly connected and interested in cooperation. My evaluation showed that the approach significantly outperforms BitTorrent's original unchocking policy by (a) increasing the number of directly cooperating peers, (b) easing the load on seeders by having more peers act as data intermediaries, and (c) shortening the bootstrapping period for fresh peers [3, 4].

PUBLICATIONS

[1] V. Atlidakis, J. Andrus, R. Geambasu, D. Mitropoulos, and J. Nieh. "POSIX has become outdated." USENIX ;login: Magazine, 41(3), Fall 2016.

[2] V. Atlidakis, J. Andrus, R. Geambasu, D. Mitropoulos, and J. Nieh. "POSIX Abstractions in Modern Operating Systems: The New, the old, and the Missing." In Proceedings of the eleventh European Conference on Computer Systems (EuroSys '16), London, UK, April 2016.

[3] F. Tramer, V. Atlidakis, R. Geambasu, D. Hsu, J-P Hubaux, M. Humbert, A. Juels, and H. Lin. "Discovering Unwarranted Associations in Data-Driven Applications with the FairTest Testing Toolkit." Accepted in the second European Symposium on Security and Privacy (Euro S&P '17),

Paris, France, April 2017.

[4] V. Atlidakis, M. Roussopoulos, and A. Delis. "EnhancedBit: Unleashing the Potential of the Unchoking Policy in the BitTorrent Protocol." Journal of Parallel and Distributed Computing (JPDC), 2014.

[5] V. Atlidakis, M. Roussopoulos, and A. Delis. "Changing the Unchoking Policy for an Enhanced Bittorrent." International European Conference on Parallel and Distributed Computing (Euro-Par), 2012.

AWARDS

Recipient of Computer Science Chair's Distinguished Fellowship, Sep. 2013, Columbia University.

Recipient of IKY scholarship for entering Department of Informatics and Telecommunications with highest score, Sep. 2005, University of Athens.

TECHNICAL SKILLS

Languages: C/C++, Python, Java, Shell Scripting

Operating Systems: Ubuntu, Debian, RHEL, CentOS

Systems/Frameworks: Tensorflow, Theano, IBM CPLEX, Linux Kernel, Android

Misc: Matlab, IDA, Apache, Nagios, Puppet, Foreman, OpenStack

COURSES

Operating Systems, Advanced Operating Systems, Programming Languages, Machine Learning, Natural Language Processing, Algorithms, Cryptography.