Stelios Sidiroglou-Douskos

Stelios Sidiroglou-Douskos

Research Scientist
MIT, Computer Science and Artificial Intelligence Laboratory

Ph.D. 2008, Columbia University
M.Phil. 2006, Columbia University
M.Sc. 2003, Columbia University

The Stata Center, Building 32-G728
32 Vassar St, Cambridge, MA 02139
stelios at csail dot mit dot edu

About

Stelios is a research scientist in the Computer Science and Artificial Intelligence Laboratory at MIT in Cambridge, MA. He is also a member of the Center for Reliable Software CRS. His technical interests are in systems security, software reliability, software engineering and "unsound" computation.
He is also a co-founder of Locu, Inc. (Acquired by GoDaddy)

Link to Google Scholar page.

News

- Our paper "Control Jujutsu: On the Weaknesses of Fine-Grained Control Flow Integrity" was accepted at CCS 2015
- Our paper "Automatic Error Elimination by Multi-Application Code Transfer" was accepted at PLDI 2015 [MIT NEWS]
- Our paper "Missing the Point: On the Effectiveness of Code Pointer Integrity"was accepted at Oakland 2015
- Our paper "Automatic Integer Overflow Discovery Using Goal-Directed Conditional Branch Enforcement" was accepted at ASPLOS 2015
- Our paper "Principled Sampling for Anomaly Detection" was accepted at NDSS 2015

Research

My research interests span the areas of systems, security and programming languages. In particular, I investigate ways in which software can be pushed to operate beyond its prescribed use to provide

conscious computing. The motivation for this research is that today's software systems are exploding in size and complexity, resulting in security vulnerabilities and pathological performance characteristics. Fortunately, complexity has a significant fringe benefit that can be used to combat these problems: software elasticity or the ability of a program to operate outside its intended use. Software elasticity is founded on the observation that as software grows in complexity so does its ability to tolerate unexpected events such as induced errors or reduced accuracy. In previous work, I used the concept of software elasticity to develop systems that can automatically heal themselves from a variety of faults. Recently, I have used software elasticity to create systems that can dynamically trade off accuracy for reliability, performance and power. In the future, the focus of my research will be on solving traditionally hard problems by challenging conventional assumptions.

Secure Cloud Computing Systems

Modern cloud computing systems offer unprecedented computational resources and flexibility in allocating those resources to a variety of users and tasks. But cloud computing systems also provide attackers with new opportunities and can amplify the ability of the attacker to compromise the computing infrastructure.

The Cloud Intrusion Detection and Repair project is developing a system that observes normal interactions during the secure operation of the cloud to derive properties that characterize this secure operation. If any part of the cloud subsequently attempts to violate these properties, the system intervenes and changes the interaction (by, for example, adding or removing operations or changing the parameters that appear in operations) to ensure that the cloud executes securely and survives the attack while continuing to provide uninterrupted service to legitimate users.

This project is currently funded under the DARPA Mission-Oriented Resilient Clouds (MRC) program. MIT is the sole performer.

Input Rectification

Applications are typically able to process the vast majority of inputs securely. Attacks usually succeed because they contain an atypical feature that the application does not process correctly. Our input rectification research observes inputs that the application processes correctly to derive a model (in the form of constraints over input fields) of the "comfort zone" of the application (the set of inputs that the application can process successfully). When it encounters an input that is outside the comfort zone, the rectifier uses the model to change the input to move the input into the comfort zone of the application. Our results show that this technique eliminates security vulnerabilities in a range of applications, leaves the overwhelming majority of safe inputs unchanged, and preserves much of the useful information in modified atypical inputs.

Code Perforation

Many modern computations (such as video and audio encoders, Monte Carlo simulations, and machine learning algorithms) are designed to trade off accuracy in return for increased performance.

To date, such computations typically use ad-hoc, domain-specific techniques developed specifically for the computation at hand. Our research explores a new general technique, Code Perforation, for automatically augmenting existing computations with the capability of trading off accuracy in return for performance. In contrast to existing approaches, which typically require the manual development of new algorithms, our implemented SpeedPress compiler can automatically apply code perforation to existing computations with no developer intervention whatsoever. The result is a transformed computation that can respond almost immediately to a range of increased performance demands while keeping any resulting output distortion within acceptable user-defined bounds.

Media Coverage

Press on CodePhage

- MIT News
- Slashdot
- Hacker News
- The Register
- Gizmodo
- Fortune
- Gizmag
- ComputerWorld

Locu acquired by GoDaddy:

- Acquired by GoDaddy

Press on our Secure Cloud Computing Systems work:

- Agence France-Press(AFP)

Some press on our software self-healing work:

- MIT News
- MIT Technology Review
- Slashdot

Some press on our Code Perforation work:

- MIT News

Papers

2015

1. **[CCS] "Control Jujutsu: On the Weaknesses of Fine-Grained Control Flow Integrity"**
   Isaac Evans, Fan Long, Ulziibayar Otgonbaatar, Howard Shrobe, Martin Rinard, Hamed Okhravi, **Stelios Sidiroglou-Douskos** . CCS 2015

2. **[HPEC]** ***"Program Fracture and Recombination for Efficient Automatic Code Reuse"***
   Peter Amidon, Eli Davis, **Stelios Sidiroglou-Douskos** , Martin Rinard. HPEC 2015

3. **[PLDI] "Automatic Error Elimination by Multi-Application Code Transfer"**

4. **[Oakland] "Missing the Point: On the Effectiveness of Code Pointer Integrity"**
   Isaac Evans, Samuel Fingeret, Julian Gonzalez, Ulziibayar Otgonbaatar, Tiffany Tang, Howard Shrobe, **Stelios Sidiroglou-Douskos** , Martin Rinard, Hamed Okhravi. Oakland 2015

5. **[ASPLOS] "Automatic Integer Overflow Discovery Using Goal-Directed Conditional Branch Enforcement"**
   Stelios Sidiroglou , Eric Lahtinen, Nathan Rittenhouse, Paolo Piselli, Fan Long, Doekhwan Kim, Martin Rinard. ASPLOS 2015

6. **[NDSS] "Principled Sampling for Anomaly Detection"**
   Brendan Juba, Christopher Musco, Fan Long, **Stelios Sidiroglou** , Martin Rinard. NDSS 2014.

2014

7. **[USPTO]** ***"Automatic Correction of Program Logic"***
   Jeff Perkins, **Stelios Sidiroglou** , Martin Rinard, et al. . U.S. Patent Number 8788884. Issued on June 7th, 2012.

8. **[PLDI]** ***"Automatic Runtime Error Repair and Containment via Recovery Shepherding"***
   Fan Long, **Stelios Sidiroglou** , Martin Rinard. PLDI 2014.

9. **[POPL]** ***"Sound Input Filter Generation for Integer Overflow Errors"***
   Fan Long, **Stelios Sidiroglou** , Deokhwan Kim, Martin Rinard. POPL 2014.

2013

10. **[CASCON] "A Source-to-Source Transformation Tool for Error Fixing"**
    Your Khmelevsky, Martin Rinard, Stelios Sidiroglou. CASCON 2013 Toronto, Canada, November 2013

11. **[USPTO]** ***"Methods, systems, and media for detecting covert malware"***
    Brian M. Bowen, Pratap V. Prabhu, Vasileios P. Kemerlis, **Stelios Sidiroglou** , Salvatore J. Stolfo, and Angelos D. Keromytis. U.S. Patent Number 8,528,091. Issued on September 3rd, 2013.

12. **[USPTO]** ***"Systems, methods, and media protecting a digital data processing device from attack"***
    Stelios Sidiroglou , Angelos D. Keromytis, and Salvatore J. Stolfo U.S. Patent Number 8,407,785. Issued on March 26th, 2013.

2012

13. **[RACES'12]** ***"Dancing with Uncertainty"***
    Sasa Misailovic, **Stelios Sidiroglou** and Martin Rinard
    In the Proceedings of the SPLASH 2012 Workshop on Relaxing Synchronization for Multicore and Manycore Scalability
    June 2012, Zurich, Switzerland.

14. **[ICSE'12]** ***"Automatic Input Rectification"***
    Fan Long, Vijay Ganesh, Michael Carbin, **Stelios Sidiroglou** and Martin Rinard
    In the Proceedings of the *34th International Conference on Software Engineering.*
    June 2012, Zurich, Switzerland.

15. **[USPTO]** ***"Methods, media and systems for detecting anomalous program executions"***
    Salvatore J. Stolfo, Angelos D. Keromytis and **Stelios Sidiroglou** , . U.S. Patent Number 8,074,115. Issued on January 7th, 2012.

2011

Stelios Sidiroglou, Sasa Misailovic, Henry Hoffman, Martin Rinard
In the ACM SIGSOFT Symposium on the Foundations of Software Engineering.
September 2011, Szeged, Hungary.

17. **[ASPLOS'11]** ***"Dynamic Knobs for Power-Aware Computing"***
Stelios Sidiroglou, Henry Hoffman, Stelios Sidiroglou, Michael Carbin, Sasa Misailovic, Anant Agarwal and Martin Rinard
In the Proceedings of the *15th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS).*
March 2011, Newport beach, CA, USA

18. **[USPTO]** ***"Methods, systems and media for software self-healing"***
Michael E. Locasto, Angelos D. Keromytis, Salvatore J. Stolfo, Angelos Stavrou, Gabriela Cretu, **Stelios Sidiroglou**, Jason Nieh, and Oren Laadan. U.S. Patent Number 7,962,798. Issued on June 14th, 2011.

19. **[USPTO]** ***"Systems and methods for detecting and inhibiting attacks using honeypots"***
Stelios Sidiroglou , Angelos D. Keromytis, and Kostas G. Anagnostakis. U.S. Patent Number 7,904,959. Issued on March 8th, 2011.

2010

20. **[ICISC'10]** ***"An Adversarial Evaluation of Network Signaling and Control Mechanisms"***
Kangkook Jee, **Stelios Sidiroglou**, Angelos Stavrou, Angelos D. Keromytis
In the Proceedings of the *13th International Conference on Information Security and Cryptology (ICISC).*
December 2010, Seoul,Korea

21. **[ONWARD'10]** ***Patterns and Statistical Analysis for Understanding Reduced Resource Computing***
Martin Rinard, Sasa Misailovic, Hank Hoffman and **Stelios Sidiroglou**,
In the Proceedings of the Onward! 2010 Conference
October 2010, Reno-Tahoe, Nevada, USA.

22. **[RAID '10]** ***"BotSwindler: Tamper Resistant Injection of Believable Decoys in VM-Based Hosts for Crimeware Detection"***
Brian M. Bower, Pratap Prabhu, Vasileios P. Kemerlis, **Stelios Sidiroglou**, Angelos D. Keromytis and Salvatore J. Stolfo
In the Proceedings of the *13th International Symposium on Recent Advances in Intrusion Detection.*
September 2010. Ottawa, Canada

23. **[ICSE '10]** ***"Quality of Service Profiling"***
Sasa Misailovic, **Stelios Sidiroglou**, Hank Hoffman and Martin Rinard
In the Proceedings of the *32nd International Conference on Software Engineering.*
May 2010, Cape Town, South Africa.

24. **[IJCNS '10]** ***"Shadow Honeypots"***
Michalis Polychronakis, Periklis Akritidis, **Stelios Sidiroglou** , Kostas G. Anagnostakis, Angelos D. Keromytis, and Evangelos Markatos.
In the *International Journal of Computer and Network Security (IJCNS),* vol. 2, no. 7, July 2010.

2009

25. **[SOSP '09]** ***"Automatically Patching Errors in Deployed Software"***
Jeff H. Perkins (MIT), Sunghun Kim (HKUST), Sam Larsen (VMware), Saman Amarasinghe (MIT), Jonathan Bachrach (MIT), Michael Carbin (MIT), Carlos Pacheco (BCG), Frank Sherwood, **Stelios Sidiroglou** (MIT), Greg Sullivan (BAE

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.