Theofilos Petsios

(+1) 6462587246 | theofilos.pe@gmail.com | www.cs.columbia.edu/~theofilos | nettrino | @theofilospe

Research Interests

I am interested in all aspects of systems and software security, with a focus on application security, binary analysis, and privacy.

Education

Ph.D. in Computer Science *New York, USA*
Columbia University *2012 - 2018*

- Ph.D. Thesis: *“Compiler-assisted Adaptive Software Testing”*
- Academic Advisors: Angelos D. Keromytis & Steven M. Bellovin

M.Phil. in Computer Science *New York, USA*
Columbia University *2015*

M.Sc. in Computer Science (GPA 3.9 / 4) *New York, USA*
Columbia University *2012 - 2014*

B.S. in Electrical Engineering & Computer Science (GPA 8.2/10) *Athens, Greece*
National Technical University of Athens (NTUA) *2005 - 2011*

- B.S. Thesis: “Term suggestion mechanisms for Scientific Database Systems”
- Thesis Advisor: Timos Sellis

Professional Appointments

Capsule8 *New York, NY, USA*
Research Scientist *April 2018 - January 2020*

Team Overview: The research team is responsible for the design and implementation of the key detection capabilities of the Capsule8 product, the development of novel exploitation techniques, the detection of state-of-the art attacks with minimal overhead within the Capsule8 product and the support of various deployment scenarios and constraints based on customer needs.

Key Achievements:

- Designed and implemented a high-performance filter which parses user configurations into runtime constraints for telemetry processing.
- Was a core contributor to the codebase of the product, re-structured core parts of the architecture to allow scalability and performance optimizations, and wrote tools for testing, automatic synthesis of documentation, and code sanity.
- Designed and implemented utilities to automatically configure the product in new environments and minimize false positives, which was instrumental in driving new sales for the company.
- Led research projects involving systems, data science and machine learning, and developed the necessary infrastructure automation to support them.
- Established benchmarks for performance analysis of different components of the product and deployed this benchmarking as part of the continuous integration cycle.

Microsoft Research *Cambridge, UK*
Research Intern *October 2017 - December 2017*

Systems and Networking Group: Developed a framework for large-scale network traffic analysis and prediction for the Iris Project.

Trail of Bits *New York, NY, USA*
Research Intern *May 2017 - August 2017*

Worked on the Manticore symbolic execution engine, adding support for symbolic execution of Binary Ninja IL, and performed security audits.

Symantec Corporation *Herndon, VA, USA*

Research Intern *June 2015 - August 2015*

Developed an ELF binary rewriting library for ARM. Designed and implemented interfaces supporting binary rewriting, injection of anti-debugging features, injection of new modules into an existing binary, as well as detection of packers and backdoors.

Greek Army (Obligatory Service) *Athens, Greece*

IT Support & Website Administrator *August 2011 - June 2012*

Responsible for the backup & maintenance of the servers hosting the website of the Greek Ministry of National Defence.

Cybex S.A. *Athens, Greece*

System Administrator & Web Developer *January 2011 - July 2011*

Responsible for the administration of the Linux server infrastructure, as well as the hosting and domain name registration services of the company.

Talks & Media Coverage

Conference Talks

November 2017	“SlowFuzz : Automated Domain-Independent Detection of Algorithmic Complexity Vulnerabilities”	*ACM CCS, Dallas, USA*
May 2017	“Nezha : Efficient Domain - Independent Differential Testing”	*S&P, San Jose, USA*
December 2015	“DynaGuard : Armoring Canary-Based Protections against Brute-force Attacks”	*ACSAC, Los Angeles, USA*

Invited Talks

April 2019	“Using Linux Tracing to Detect Attacks at Scale”	*OSIRIS Lab, NYU, USA*
March 2018	Guest Lecture on “Fuzz Testing” for Graduate-Level Course “Reliable Software”	*Columbia University, USA*
August 2017	Empire Hacking NYC: “Extending Manticore with Binary Ninja”	*MongoDB, New York, USA*
March 2017	Guest Lecture on “Fuzz Testing” for Graduate-Level Course “Reliable Software”	*Columbia University, USA*
October 2016	Empire Hacking NYC: “Differential Fuzzing with LLVM’s LibFuzzer”	*TwoSigma, New York, USA*

Media Coverage

March 2019	“Millions of Binaries Later: a Look Into Linux Hardening in the Wild”	*Hacker News Front Page*
November 2017	“Found: Our Best Future Cyber Protectors in World’s Biggest Student-Led Cybersecurity Games”	*Morning Star*
August 2014	NYT Bits: “XRay: A New Tool for Tracking the Use of Personal Data on the Web”	*The New York Times*

Skills

Programming	C/C++, Python, Go, Bash, LaTeX, HTML, CSS, Javascript, SQL, PHP, Java, Vimscript
Technologies	LLVM & GCC internals, Intel PIN, Kubernetes, Docker, Buildkite, Pandas, Bokeh, Flask
Languages	Greek (*Native*) English (*Proficient*) French, Spanish (*Elementary proficiency - ILR scale 1+*)

Honors & Awards

2012-2018	**Fellowship**, Graduate Research Assistantship (GRA), Columbia University	*New York, USA*
2017	**2nd Place at NYU-CSAW Applied Research Competition**, New York University (NYU)	*New York, USA*
2017	**Finalist Travel Grant for NYU-CSAW**, New York University (NYU)	*New York, USA*
2014	**Bug Bounty Grant**, Facebook	*New York, USA*
2014	**Scholarship (for Ph.D. studies)**, Gerondelis Foundation	*New York, USA*
2005	**Scholarship (for B.S. studies)**, Eurobank EFG	*Athens, Greece*

Service

Reviewer

CSAW	CSAW Research Competition: 2018, 2019
TOSEM	ACM Transactions on Software Engineering and Methodology (TOSEM): 2018

External Reviewer

USENIX	USENIX Security Symposium: 2017
CCS	ACM Conference on Computer and Communications Security: 2013, 2014
IWSEC	International Workshop on Security: 2014
MTD	ACM Workshop on Moving Target Defense: 2015
IET	IET Information Security: 2014

Other

Columbia University	Reviewer of applications for the Master's Program in Computer Science : 2015, 2016

Open-Source Software

BibTeX entry from URL	A Chrome extension that produces BibTeX entries from the active URL (Users > 10k, Rating: 5 stars).
LBSProximityAuditor	An auditing framework for Location Based Services.
NEZHA	A differential fuzzing framework built on top of libFuzzer.
SQLRand	A compiler pass that guards against SQL injections.
INTFLOW	An LLVM pass to detect integer errors with low false positives.
DYNAGUARD	A set of protections of canary-based defenses against brute-force attacks.

Teaching and Mentorship

Instructor, Introduction to Programming in C *New York, USA*

COLUMBIA UNIVERSITY *Summer 2014*

- Designed and taught a three week summer intensive course for the School of Continuing Education at Columbia University (Students: 16)

Teaching Assistant *New York, USA*

COLUMBIA UNIVERSITY *Summer 2013 - Fall 2016*

- Fall 2016: Head Teaching Assistant (TA) for Network Security (Graduate level. Instr. Debbie Cook. Students: 34)
- Spring 2015: TA for Network Security (Graduate level. Instr. Debbie Cook. Students: 33)
- Fall 2013: Head TA for Data Structures & Algorithms (Undergraduate level. Instr.: Shlomo Hershkop. Students: 70)
- Spring 2013: Head TA for Advanced Programming (Undergraduate level. Instr.: Shlomo Hershkop. Students: 14)

Student Mentor *New York, USA*

COLUMBIA UNIVERSITY *2016*

- Fall 2016: Jason Zhao (undergraduate student). Project: Guided fuzzing for resource exhaustion bugs.
- Spring 2016: Benjamin Low (undergraduate student). Project: Towards a taxonomy of the security properties of major OSes.

Publications

Conference Publications

C1 **Theofilos Petsios**, Jason Zhao, Angelos D. Keromytis, and Suman Jana. *"SlowFuzz : Automated Domain-Independent Detection of Algorithmic Complexity Vulnerabilities. "*. In Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS), Dallas, TX, November 2017.

C2 **Theofilos Petsios**, Adrian Tang, Salvatore Stolfo, Angelos D. Keromytis, and Suman Jana. "Nezha *: Efficient Domain - Independent Differential Testing"*. In 38th IEEE Symposium on Security and Privacy (S&P), San Jose, CA, May 2017.

C3 Marios Pomonis,**Theofilos Petsios**, Angelos D. Keromytis, Michalis Polychronakis, Vasileios P. Kemerlis. *"kR^X : Comprehensive Kernel Protection against Just-In-Time Code Reuse"*. In Proceedings of the 12th European Conference on Computer Systems (EuroSys), April 2017.

C4 **Theofilos Petsios**, Vasileios P. Kemerlis, Michalis Polychronakis, Angelos D. Keromytis. *"DynaGuard: Armoring Canary-based Protections against Brute-force Attacks"*. In Proceedings of the 31th Annual Computer Security Applications Conference (ACSAC), December 2015.

C5 Iasonas Polakis, George Argyros, **Theofilos Petsios**, Suphannee Sivakorn, Angelos D. Keromytis. *"Where's Wally? Precise User Discovery Attacks in Location Proximity Services"*. In Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS), October 2015.

C6 Marios Pomonis, **Theofilos Petsios**, Kangkook Jee, Michalis Polychronakis, and Angelos D. Keromytis. *"IntFlow: Improving the Accuracy of Arithmetic Error Detection Using Information Flow Tracking"*. In Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC), December 2014.

C7 M. Lecuyer, G. Ducoffe, F. Lan, A. Papancea, **T. Petsios**, R. Spahn, A. Chaintreau, and R. Geambasu. *"XRay: Enhancing the Web's Transparency with Differential Correlation."*, in Proceedings of the USENIX Security Symposium, August 2014.

Journal Publications

J1 George Argyros, **Theofilos Petsios**, Suphannee Sivakorn, Angelos D. Keromytis, and Jason Polakis. *"Evaluating the Privacy Guarantees of Location Proximity Services"*. In ACM Transactions on Privacy and Security (TOPS) (formerly known as TISSEC).

J2 Marios Pomonis,**Theofilos Petsios**, Angelos D. Keromytis, Michalis Polychronakis, Vasileios P. Kemerlis.*"Kernel Protection against Just-In-Time Code Reuse"*. In ACM Transactions on Privacy and Security (TOPS) (formerly known as TISSEC).

Other Publications

O1 **Theofilos Petsios**, *"Compiler-assisted Adaptive Software Testing"*, PhD Thesis, April 2018.

O2 **Theofilos Petsios**, Adrian Tang, Dimitris Mitropoulos, Salvatore Stolfo, Angelos D Keromytis, Suman Jana. *"Tug-of-War: Observations on Unified Content Handling"*, arXiv preprint arXiv:1708.09334, August 2017.

O3 Marios Pomonis,**Theofilos Petsios**, Angelos D. Keromytis, Michalis Polychronakis, Vasileios P. Kemerlis. *"kR^X : Comprehensive Kernel Protection against Just-In-Time Code Reuse"*. Black Hat USA Conference, July 2017.

O4 George Argyros, **Theofilos Petsios**, Dimitris Mitropoulos, Yunhui Zheng, Angelos D. Keromytis, and Junfeng Yang. *"Towards Scalable Symbolic Execution in Interpreted Languages"*, in RSAC Security Scholar Poster Exhibition, RSA Conference, February 2017.