Thanassis Avgerinos

Carnegie Mellon University
Department of Electrical and
Computer Engineering
5000 Forbes Avenue,
Pittsburgh, Pennsylvania, USA

Citizenship: Greek
Office: CIC #2131A
Email: `thanassis@cmu.edu`
Homepage: `www.ece.cmu.edu/~aavgerin`

Work Experience & Education

2014-Present

Founder and Software Engineer at ForAllSecure, Inc.

2009-2014

Research Assistant, PhD in Electrical and Computer Engineering,
Carnegie Mellon University.

- *Advisor*: Prof. David Brumley.
- *Areas*: Software Security & Program Analysis.
- *Committee*: David Brumley, Virgil Gligor, André Platzer, George Candea.
- *Dissertation Title*: Exploiting Tradeoffs in Symbolic Execution for Identifying Security Bugs.

2013

Master of Science in Electrical and Computer Engineering,
Carnegie Mellon University.

- *Areas*: Software Security & Program Analysis, GPA 4.0.

2004-2009

Diploma in Electrical and Computer Engineering,
National Technical University of Athens.

- *Major*: Computer Science.
- *Minor*: Computer Networks and Telecommunications.
- *Honors*: *Summa Cum Laude*, GPA 9.86/10 (1st out of 600+ students).

Dissertation:

- *Diploma Thesis*: Automatic Refactoring of Erlang Programs.
- *Advisor*: Prof. Kostis Sagonas.
- *Committee*: Kostis Sagonas, Nikolaos Papaspyrou, Stathis Zachos

Research Interests

- Program Analysis and Verification.
- Software Security.

- Programming Language Theory, Design and Implementation.
- Compilers, compilation techniques and optimizations.
- Software Engineering.

Publications

[1] Alexandre Rebert, Sang Kil Cha, Thanassis Avgerinos, Jonathan Foote, David Warren, Gustavo Grieco, and David Brumley. Optimizing seed selection for fuzzing. In *23rd USENIX Security Symposium (USENIX Security 14)*. USENIX Association, August 2014.

[2] Thanassis Avgerinos, Alexandre Rebert, Sang Kil Cha, and David Brumley. Enhancing symbolic execution with veritesting. In *Proceedings of the 36th International Conference on Software Engineering*, June 2014.

[3] Thanassis Avgerinos, Sang Kil Cha, Alexandre Rebert, Edward J. Schwartz, Maverick Woo, and David Brumley. Automatic exploit generation. In *Communications of the ACM*, pages 74–84, February 2014.

[4] Sang Kil Cha, Thanassis Avgerinos, Alexandre Rebert, and David Brumley. Unleashing Mayhem on binary code. In *Proceedings of the 33rd IEEE Symposium on Security and Privacy*, pages 380–394, May 2012.

[5] Edward J. Schwartz, Thanassis Avgerinos, and David Brumley. Q: Exploit hardening made easy. In *Proceedings of the 19th USENIX Security Symposium (USENIX 2011)*, August 2011.

[6] David Brumley, Ivan Jager, Thanassis Avgerinos, and Edward J. Schwartz. BAP: Binary analysis platform. In *Proceedings of the 23rd International Conference on Computer Aided Verification (CAV 2011)*, July 2011.

[7] Thanassis Avgerinos, Sang Kil Cha, Brent Lim Tze Hao, and David Brumley. AEG: Automatic exploit generation. In *Proceedings of the 2011 Network and Distributed System Security Symposium*, pages 283–300. ISOC, February 2011.

[8] JongHyup Lee, Thanassis Avgerinos, and David Brumley. TIE: Principled reverse engineering of types in binary programs. In *Proceedings of the 2011 Network and Distributed System Security Symposium*, pages 251–268. ISOC, February 2011.

[9] Edward J. Schwartz, Thanassis Avgerinos, and David Brumley. All you ever wanted to know about dynamic taint analysis and forward symbolic execution (but might have been afraid to ask). In *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, pages 317–331. IEEE, May 2010.

[10] Thanassis Avgerinos and Konstantinos Sagonas. Cleaning up Erlang code is a dirty job but somebody's gotta do it. In *Proceedings of the Eighth ACM SIGPLAN Erlang Workshop*, pages 1–10, New York, NY, USA, September 2009. ACM.

[11] Konstantinos Sagonas and Thanassis Avgerinos. Automatic refactoring of Erlang programs. In *Proceedings of the Eleventh International ACM SIGPLAN Symposium on Principles and Practice of Declarative Programming*, pages 13–24, New York, NY, USA, September 2009. ACM.

Patents

1. Automated Exploit Generation.
2. Code Base Partitioning System.
3. Detecting Exploitable Bugs in Binary Code.

Invited Talks

1. Enhancing Symbolic Execution with Veritesting. *11th Annual Programming Language Seminar*, NTUA, December 2013.

2. Unleashing Mayhem on Binary Code. *10th Annual Programming Language Seminar*, NTUA, December 2012.

3. AEG: Automatic Exploit Generation. *9th Annual Programming Language Seminar*, NTUA, December 2011.

4. All You Ever Wanted to Know About Dynamic Taint Analysis and Forward Symbolic Execution (but Might Have Been Afraid to Ask).
   - *Workshop on Offensive Technologies, WOOT*, Washington DC, August 2010.
   - *8th Annual Programming Language Seminar*, NTUA, December 2010.

Fellowships & Awards

Year	Award	Requirements
2012	Technical Chamber of Greece	Top ECE student in Greece
2011	Thomaideio Award	Top student graduating from ECE
2010	Kondoulis Award	Top student graduating from NTUA
2010	Chrysovergis Award	Top student graduating from ECE
2010	Sfaellou Award	Top student during the first 8 semesters
2009	Dean's Tuition Fellowship	Carnegie Mellon University – PhD Scholarship
2009	Paris Kanellakis Award	Top student with a CS major in NTUA
2004-2008	State Scholarships Foundation	Awarded each year to the top 3 students of the department
2006	C. Papakyriakopoulos Award	Awarded for excellence in Mathematics
2006, 2009	KARY Award	Awarded to the top students of every NTUA department
2004	State Scholarships Foundation	Awarded to the first 5 students matriculating at ECE

Research & Teaching Experience

Sep. 2009 — Present	Research Assistant in Computer Security.
Fall 2010	Teaching Assistant for 18-487: Introduction to Software Security, Network Security and Applied Cryptography, taught by David Brumley.
Spring 2011	Teaching Assistant for 18-733: Applied Cryptography, taught by Virgil Gligor.
Summer 2011	Research Intern at Microsoft Research, working with Mariusz Jakubowski, Marcus Peinado and the eXtreme Computing Group (XCG).
Spring 2012	Teaching Assistant for 18-732: Secure Software Systems, taught by David Brumley.

Past Projects

Tidier	I am the main developer of Tidier, a tool for automatic refactoring of Erlang programs. The tool has a freely available web interface.

Services

I have served as an external reviewer or a program committee member for the following conferences:

- Oakland 2010, 2011, 2012, 2013
- CCS 2013
- USENIX 2012, 2014
- WOOT 2012
- AsiaCCS 2010, 2011
- NDSS 2010

Course Work

Fall 2009	• 18-730: Introduction to Computer Security, taught by Virgil Gligor. • 18-732: Secure Software Systems, taught by David Brumley.
Spring 2010	• 18-731: Network Security, taught by Adrian Perrig. • 18-733: Applied Cryptography, taught by Virgil Gligor.
Spring 2011	• 18-739c: Special Topics in Security: Vulnerabilities, Defense and Malware Analysis, taught by David Brumley.
Spring 2012	• 15-780: Graduate Artificial Intelligence, taught by Martial Hebert and Ariel Procaccia.
Fall 2012	• 15-857: Analytical Performance Modeling & Design of Computer Systems, taught by Mor Harchol-Balter.
Spring 2013	• 15-745: Optimizing Compilers for Modern Architectures, taught by Todd C. Mowry.

Miscellaneous

Programming Languages

- Extensive Knowledge: C, C++, Java, Pascal, SML, OCaml, F#, Erlang, Prolog, Datalog, Python, Ruby, x86 assembly, bash, LaTeX.
- Experience in: Haskell, PHP, SQL, AVR Assembly, Matlab, Mathematica, Javascript, Perl.

Platforms

- Linux, Mac, Windows.

Language Skills

- Greek: Mother tongue.
- English: Certificate of Proficiency in English, Michigan University and
  Certificate of Proficiency in English, Cambridge University.
- German: Zentrale Mittelstüfenprüfung, Goethe Institut München.
- French: Diplôme d' Études de Langue Française, Institut Français d' Athènes.

Hobbies

- Basketball, Racquetball, Chess, Squash, Swimming.
- Moral & Political Philosophy, History, Popular Economics.