

Alexandros Kaparavelos

Computer Security Lab
Department of Computer Science,
University of California, Santa Barbara,
Santa Barbara, California, 93106
☎ +18056996416
✉ kapravel@cs.ucsb.edu
🌐 www.kapravelos.com

Research Interests

My research interests span the areas of **systems and software security**. I am in particular interested in protecting the browser at all levels, from designing a secure browser architecture to measuring and understanding large-scale Internet attacks. Understanding how the web works and evolves over time and how we can make it more secure for the users is my current research focus.

Employment

Starting in **Assistant Professor**,
Jan 2016 Department of Computer Science,
North Carolina State University

Education

2010-2015 **Ph.D. in Computer Security Lab**,
Computer Science Department,
University of California, Santa Barbara, USA.

thesis *Analyzing and Defending Against Evolving Web Threats*
supervisors Professor Christopher Kruegel, Professor Giovanni Vigna

2010 **M.Sc. Candidate in Distributed Computing Systems Lab**,
Computer Science Department,
University of Crete, Greece.
GPA: 8.7 out of 10.0

thesis *Robust Prevention of Dial Attacks*
supervisor Professor Evangelos Markatos
description An extensive evaluation of the security properties that arise from making accessible telephone devices from the Internet through the use of VoIP. The term Dial stands for *Digitally Initiated Abuse of teLephones*

2007 **B.Sc. in Computer Science**,
Computer Science Department, University of Crete, Greece.
GPA: 7.43 out of 10.0

thesis *Packetloss: A Passive end-to-end Packet Loss estimation*
supervisor Professor Evangelos Markatos

description A novel idea for estimating accurately the packet loss ratio between different measuring points.

Publications

- [1] K. Thomas, E. Bursztein, C. Grier, G. Ho, N. Jagpal, **A. Kapravelos**, D. McCoy, A. Nappa, V. Paxson, P. Pearce, N. Provos, and M. Abu Rajab. Ad Injection at Scale: Assessing Deceptive Advertisement Modifications. In *Proceedings of the IEEE Symposium on Security and Privacy*. **Distinguished Practical Paper Award**, 2015.
- [2] A. Zarras, **A. Kapravelos**, G. Stringhini, T. Holz, C. Kruegel, and G. Vigna. The Dark Alleys of Madison Avenue: Understanding Malicious Advertisements. In *Proceedings of the Internet Measurement Conference (IMC)*, 2014.
- [3] **A. Kapravelos**, C. Grier, N. Chachra, C. Kruegel, G. Vigna, and V. Paxson. Hulk: Eliciting Malicious Behavior in Browser Extensions. In *Proceedings of USENIX Security Symposium*. USENIX, 2014.
- [4] G. De Maio, **A. Kapravelos**, Y. Shoshitaishvili, C. Kruegel, and G. Vigna. PEXy: The other side of Exploit Kits. In *Proceedings of the Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, 2014.
- [5] **A. Kapravelos**, Y. Shoshitaishvili, M. Cova, C. Kruegel, and G. Vigna. Revolver: An Automated Approach to the Detection of Evasive Web-based Malware. In *Proceedings of the USENIX Security Symposium*, 2013.
- [6] N. Nikiforakis, **A. Kapravelos**, W. Joosen, C. Kruegel, F. Piessens, and G. Vigna. Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2013.
- [7] N. Nikiforakis, L. Invernizzi, **A. Kapravelos**, S. Van Acker, W. Joosen, C. Kruegel, F. Piessens, and G. Vigna. You are what you include: Large-scale evaluation of remote javascript inclusions. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2012.
- [8] **A. Kapravelos**, M. Cova, C. Kruegel, and G. Vigna. Escape from Monkey Island: Evading High-Interaction Honeyclients. In *Proceedings of the Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, 2011.
- [9] **A. Kapravelos**, I. Polakis, E. Athanasopoulos, S. Ioannidis, and E.P. Markatos. D(e|i)aling with VoIP: Robust Prevention of Dial Attacks. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, 2010.
- [10] A. Friedl, S. Ubik, **A. Kapravelos**, M. Polychronakis, and E.P. Markatos. Realistic Passive Packet Loss Measurement for High-Speed Networks. In *Proceedings of the International Workshop on Traffic Monitoring and Analysis (TMA)*, 2009.
- [11] N. Armenatzoglou, Y. Marketakis, L. Kriara, E. Apostolopoulos, V. Papavasiliou, D. Kampas, **A. Kapravelos**, E. Kartsonakis, G. Linardakis, S. Nikitaki, A. Bikakis, and G. Antoniou. Flexconf: A flexible conference assistant using context-aware notification services. In *Proceedings of the IEEE Workshop on Context Aware Mobile Systems (CAMS)*, 2009.

- [12] A. Papadogiannakis, **A. Kapravelos**, M. Polychronakis, E.P. Markatos, and A. Ciuffoletti. Passive end-to-end packet loss estimation for grid traffic monitoring. In *Proceedings of the CoreGRID Integration Workshop*, 2006.

Teaching Experience

- 2010-2014 International Capture the Flag (iCTF) - I was one of the organizing members for the worlds' largest educational hacking competition for the past 4 years
- November 2012 Guest Lecture titled "Web Application Security" at UCSB's CS177 class "Computer Security and Privacy"
- April 2012 "Into the Mind of the Hacker" - Three hour hands-on workshop at UC Santa Barbara by request of Web Standard Group
- Spring 2009 Teaching Assistant, CS459 - Internet Measurements, University of Crete
- Spring 2008 Teaching Assistant, CS118 - Discrete Mathematics, University of Crete
- Fall 2007, Fall 2008 Teaching Assistant, CS345 - Operating Systems, University of Crete

Work Experience

- 2016 – future I am joining the Department of Computer Science at North Carolina State University as an Assistant Professor in January 2016.
- 2010 – 2015 As a Research Assistant in the Computer Security Lab at the University of California, Santa Barbara I am the lead developer of Wepawet, a public platform for the analysis of web-based threats. More recently, I have deployed a new public platform to track the evolution of malicious JavaScript attacks based on the work that I did for the Revolver paper. I am also part of the core team organizing the UCSB International Capture the Flag (iCTF) hacking competition, the largest live security exercise with more than 900 participating students and a proud member of the Shellphish hacking group.
- Sept – Dec 2014 I did an internship at Google at the anti-abuse research group under the supervision of Elie Bursztein and worked on a project with the goal to understand in depth ad injection from malicious browser extensions.
- June – Sept 2014 I visited the Security Group at UC San Diego for 3 months and worked with Stefan Savage and Geoff Voelker on a machine learning project regarding malicious browser extensions.
- Oct – Dec 2013 I consulted at Lastline Inc. for 3 months regarding advanced web security problems based on my experience from Wepawet.
- June – Sept 2013 For the summer of 2013 I visited the International Computer Science Institute at Berkeley to work as an intern with Chris Grier and Vern Paxson. My project there was to understand and develop methods to detect malicious extensions for the Chrome browser.
- 2005 – 2010 I worked as a Research Assistant at Distributed Computing Systems Lab of FORTH-ICS in Heraklion. I participated in two EU-funded programs: LOBSTER (Large-scale Monitoring of Broadband Internet Infrastructures) and MOMENT (Monitoring and Measurement in the Next Generation Technologies).

Sep - Nov 2009 I visited Prof. Christopher Kruegel and Giovanni Vigna for 3 months at the University of California, Santa Barbara and worked in the Computer Security Lab as Junior Research Assistant.

Awards

- 2011 IEEE Symposium on Security and Privacy Travel Grant
- 2011 USENIX Security Symposium Student Travel Grant
- 2012 IEEE Symposium on Security and Privacy Travel Grant
- 2012 USENIX Security Symposium Student Travel Grant
- 2013 ACM CCS Student Travel Grant
- 2014 USENIX Security Symposium Student Travel Grant
- 2015 Distinguished Practical Paper Award from IEEE Symposium on Security and Privacy

Press

- 2013 News article at DARKReading for *Revolver*
<http://goo.gl/l91J5S>
- 2014 News article at IEEE Spectrum magazine about browser fingerprinting
<http://goo.gl/trS3th>
- 2014 News article at PCWorld regarding Hulk and malicious browser extensions
<http://goo.gl/RyNjNm>
- 2014 News article at InfoWorld for our malicious advertisement measurement study presented at IMC'14
<http://goo.gl/Fs0aVU>
- 2015 Official blogpost by Google with part of the work we did during my internship there
<http://goo.gl/3FKluU>
- 2015 Interview with BBC regarding malicious browser extensions
<http://goo.gl/FiHzLU>

Mentoring

Over the years I had the fantastic opportunity to work with undergraduate and graduate students on some of the research projects that I envisioned at the time.

- 2014 Giacomo Vecere - In-browser website analysis
- 2014 Suqi Liu - Identifying malicious browser extensions with machine learning
- 2014 Vasilios Mavroudis - Non-determinism in JavaScript
- 2014 Abhinav Gupta - Improving detection of Java-based drive-by download attacks in Wepawet
- 2014 Apostolis Zarras - Malicious Advertisements [2]
- 2013 Giancarlo De Maio - Analysis of Exploit kits [4]
- 2013 Luca Montecchi and Aldo Vaccari - Profiling JavaScript in the browser
- 2012 Sahin Koc - DNS reputation in conjunction with dynamic analysis systems

References

Giovanni Vigna

Department of Computer Science
University of California, Santa Barbara
Santa Barbara, CA 93106
✉ vigna@cs.ucsb.edu

Christopher Kruegel

Department of Computer Science
University of California, Santa Barbara
Santa Barbara, CA 93106
✉ chris@cs.ucsb.edu

Stefan Savage

Department of Computer Science and
Engineering
University of California, San Diego
La Jolla, CA, 92093-0404
✉ savage@cs.ucsd.edu

Updated

September, 2015