Alexandros Kapravelos

+1 805-699-6416
akaprav@ncsu.edu
kapravelos.com
@kapravel

Research Interests

My research interests span the areas of **systems and web 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

Jan 2016-now **Assistant Professor**
Department of Computer Science
North Carolina State University

Grants and Contracts

Total funding: $1,591,426

ONR XS-Shredder: A Cross-Layer Framework for Removing Code Bloat in Web Applications
Total Award: $1,230,547; NCSU amount: **$300,000**
Duration: 2 years (July 2017 - June 30, 2019)
NCSU PI: Alexandros Kapravelos; PI: Adam Doupé; CoPIs: Manuel Egele, Nick Nikiforakis

NSF SaTC: CORE: Medium: Collaborative: Taming Web Content Through Automated Reduction in Browser Functionality
Total Award: $1,199,787; NCSU amount: **$406,609**
Duration: 4 years (September 1, 2017 - August 31, 2021)
NCSU PI: Alexandros Kapravelos; PI: Adam Doupé; CoPI: Engin Kirda

DARPA CHECRS: Cognitive Human Enhancements for Cyber Reasoning Systems
Total award: $11,730,557; NCSU Amount: **$884,817**
Duration: 3,5 years
PI: Ruoyu (Fish) Wang (ASU)
CoPIs (ASU): Yan Shoshitaishvili, Tiffany Bao, Adam Doupé, Chitta Baral, Stephanie Forrest
CoPIs (NCSU): Alexandros Kapravelos
CoPIs (EURECOM): Davide Balzarotti, Yanick Fratantonio
CoPIs (UCSB): Giovanni Vigna, Christopher Kruegel
CoPIs (UIowa): Antonio Bianchi

Awards

2015 Distinguished Practical Paper Award from IEEE Symposium on Security and Privacy

2015 UC Santa Barbara - Outstanding Dissertation Award

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] Quan Chen and **A. Kapravelos**. Mystique: Uncovering information leakage from browser extensions. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2018.

[2] L. Invernizzi, K. Thomas, **A. Kapravelos**, O. Comanescu, Jean-Michel Picod, and E. Bursztein. Cloak of Visibility: Detecting When Machines Browse A Different Web. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2016.

[3] K. Thomas, E. Bursztein, C. Grier, G. Go, 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.

[4] 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.

[5] **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.

[6] 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.

[7] **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.

[8] 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.

[9] 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.

[10] **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.

[11] **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.

[12] 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.

[13] 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.

[14] 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

NCSU

Spring 2019 CSC-405 Computer Security
Spring 2019 CSC-705 Operating Systems Security
Spring 2018 CSC-405 Computer Security
Fall 2017 CSC-591 Systems Attacks and Defenses
Spring 2017 CSC-405 Introduction to Computer Security
Fall 2016 CSC-574 Computer and Network Security
Spring 2016 CSC-705 Operating Systems Security

UCSB

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

University of Crete

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

Previous Research Experience

2010 – 2015 — As a Research Assistant in the Computer Security Lab at the University of California, Santa Barbara I was the lead developer of Wepawet, a public platform for the analysis of web-based threats. I also 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 was 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 (ICSI) 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.

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.

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).

Service

Workshops & Conferences

co-Chair — Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb): 2019

co-Chair — International Conference on Parallel and Distributed Systems - Security Session (ICPADS): 2016

TPC member	USENIX Security Symposium: 2017, 2018
TPC member	IEEE Symposium on Security and Privacy: 2019
TPC member	ACM Conference on Computer and Communications Security (CCS): 2018, 2019
TPC member	World Wide Web Conference (WWW) - Security Track: 2018
TPC member	ACM Conference on Data and Application Security and Privacy (CODASPY): 2017, 2018, 2019
TPC member	Annual Computer Security Applications Conference (ACSAC): 2016, 2017, 2018
TPC member	European Workshop on Systems Security (EuroSec): 2018, 2019
TPC member	Workshop on Offensive Technologies (WOOT): 2016, 2017, 2018
TPC member	Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA): 2017, 2018
TPC member	Symposium on Electronic Crime Research (eCrime): 2016, 2017, 2018
TPC member	ACM Symposium on Applied Computing (SAC) - Security Track: 2018
TPC member	NSF SaTC panel: 2016, 2018

Capture-The-Flag Competitions

Organizer	DEF CON CTF - I am part of the 'Order of the Overflow' team that organizes the largest, oldest and most prestigious hacking competition co-located with the DEF CON Hacking Conference.
Organizer	HackPack CTF - I have been organizing yearly since 2016 a Capture The Flag (CTF) competition at NCSU together with the security student club named HackPack that I mentor.
Organizer	International Capture the Flag (iCTF) - I was one of the organizing members for the worlds' largest educational hacking competition for 4 years (2010-2014)

Press

2015	Interview with BBC regarding malicious browser extensions `http://goo.gl/FiHzLU`
2015	Official blogpost by Google for our IEEE S&P paper `https://goo.gl/XAU3qm`
2015	Official blogpost by Google with part of the work we did during my internship `http://goo.gl/3FKIuU`
2014	News article at InfoWorld for our malicious advertisement measurement study presented at IMC'14 `http://goo.gl/Fs0aVU`
2014	News article at PCWorld regarding Hulk and malicious browser extensions `http://goo.gl/RyNjNm`
2014	News article at IEEE Spectrum magazine article about browser fingerprinting `http://goo.gl/trS3th`
2013	News article at DARKReading for *Revolver* `http://goo.gl/191J5S`

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.

PhD Students

2018-now Nikolaos Pantelaios - Extension takeover
2017-now Kyle Martin - Browser Exploitation framework
2017-now Shaown Sarker - JavaScript Obfuscation
2017-now Jordan Jueckstock - Browser functionality reduction
2017-now Igibek Koishybayev - Web application attack-surface reduction
2016-now Quan Chen - Browser tainting for privacy leaks [1]
2014 Suqi Liu - Identifying malicious browser extensions with machine learning

Master's Students

2018-now Shantanu Chandorkar - Threat-intelligence framework
2018 Chinmay Rudrapatna - Threat-intelligence feeds
2018 Alex Shevtsov - visiting student - DOMQuery project
2017 Georgios Tsirantonakis - visiting student - DOMQuery project
2014 Giacomo Vecere - In-browser website analysis
2014 Vasilios Mavroudis - Non-determinism in JavaScript
2014 Apostolis Zarras - Malicious Advertisements [4]
2013 Giancarlo De Maio - Analysis of Exploit kits [6]
2013 Luca Montecchi and Aldo Vaccari - Profiling JavaScript in the browser
2012 Sahin Koc - DNS reputation in conjunction with dynamic analysis systems

Undergraduate Students

2018-now Aidan Beggs - Extensions in the wild
2018-now Will Rabb - Form-leaking on the web
2018-now Tyler Nielsen - Browser extensions code dependencies
2018-now Apostolos Karampelas - DOM protections from extensions
2017-2018 Robert Reichel - Browser extensions analysis
2014 Abhinav Gupta - Improving detection of Java-based drive-by download attacks in Wepawet

Other Mentoring Activities

2016-now HackPack student club at NCSU - Mentoring the security student club and guide them to learn practical security skills and participate in CTF competitions

Updated

November, 2018