

Marios Pomonis

☎ (+1) 917-499-5228 | ✉ mariospomonis@gmail.com | 🏠 mpomonis.github.io | 🗣 mpomonis | 🌐 marios-pomonis | 🐦 @mariospomonis

Interests

I am interested in most aspects of network and systems security with a focus on OS kernel security, software exploitation and software testing.

Work Experience

Google LLC

GCP PLATFORM SECURITY

Kirkland, WA

2019 – Present

Research Experience

KERNEL SECURITY

2014 – Present

- Co-designed and developed **kr^{AX}**, a defense mechanism against Just-In-Time Code Reuse attacks.
- Modified the kernel memory layout to separate the code from data sections.
- Instrumented every memory read (through the GCC plugin interface) using range checks to prevent memory disclosure vulnerabilities from reading the code section.
- Utilized new hardware features (Intel MPX) to lower the overhead of the code instrumentation.
- Diversified the code layout to prevent attackers from using a-priori computed gadgets.
- Protected return address leaks through encryption and deception (decoys).

SOFTWARE TESTING

2013 – 2014

- Co-designed and developed **IntFlow**, a compiler extension that identifies real bugs that lead to integer errors.
- Employed Integer Overflow Checker (IOC) to detect all integer errors.
- Utilized static taint analysis to differentiate between developer-intended violations and real bugs.
- Added dynamically triggered runtime checks to pinpoint potentially exploitable errors that might be used in sensitive sinks (e.g. malloc()).

Education

Ph.D. in Computer Science

New York, USA

COLUMBIA UNIVERSITY

2012 – 2019

- Dissertation: "Preventing Code Reuse Attacks On Modern Operating Systems"
Advisors: Prof. Vasileios P. Kemerlis, Prof. Angelos D. Keromytis & Prof. Roxana Geambasu

M.Sc. in Computer Science

New York, USA

COLUMBIA UNIVERSITY

2012 – 2013

- GPA: 3.98/4

B.Sc. in Computer Science

Athens, Greece

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

2007 – 2011

- GPA: 8.13/10
- Thesis: "Implementation of the Pastry Distributed Hash Table Lookup Service over the Ns-3 Network Simulator"
Thesis Supervisor: Prof. George Xylomenos

Publications

CONFERENCE PUBLICATIONS

- "kr^{AX}: Comprehensive Kernel Protection against Just-In-Time Code Reuse"
Marios Pomonis, Theofilos Petsios, Angelos D. Keromytis, Michalis Polychronakis, Vasileios P. Kemerlis.
In Proceedings of the 12th European Conference on Computer Systems (EuroSys). April 2017, Belgrade, Serbia.
- "IntFlow: Improving the Accuracy of Arithmetic Error Detection Using Information Flow Tracking"
Marios Pomonis, Theofilos Petsios, Kangkook Jee, Michalis Polychronakis, and Angelos D. Keromytis.
In Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC). December 2014, New Orleans, LA, USA.
- "Proactive selective neighbor caching for enhancing mobility support in information-centric networks"
Xenofon Vasilakos, Vasilios A. Siris, George C. Polyzos, and **Marios Pomonis**.
In Proceedings of the 2nd Edition of the ICN Workshop on Information-centric Networking (ICN '12). ACM, New York, NY, USA.

JOURNAL PUBLICATIONS

- “Kernel Protection against Just-In-Time Code Reuse”

Marios Pomonis, Theofilos Petsios, Angelos D. Keromytis, Michalis Polychronakis, Vasileios P. Kemerlis.
ACM Transactions on Privacy and Security (TOPS) (formerly known as TISSEC), 22(1), January 2019.

Skills

Programming C/C++, x86(-64) Assembly, Python, Java, AWK, LaTeX
Technologies GCC & LLVM Internals, Operating Systems Internals, Intel PIN
Languages Greek (Native), English (Proficient), German (Elementary)

Talks & Awards

CONFERENCE TALKS

- | | | |
|------|--|----------------------------|
| 2017 | kR^X: Comprehensive Kernel Protection against Just-In-Time Code Reuse
12th European Conference on Computer Systems (EuroSys) | <i>Belgrade, Serbia</i> |
| 2014 | IntFlow: Improving the Accuracy of Arithmetic Error Detection Using Information Flow Tracking
30th Annual Computer Security Applications Conference (ACSAC) | <i>New Orleans, U.S.A.</i> |

INVITED TALKS

- | | | |
|------|---|--------------------------|
| 2017 | kR^X: Comprehensive Kernel Protection against Just-In-Time Code Reuse
20th Black Hat Briefings | <i>Las Vegas, U.S.A.</i> |
| 2017 | kR^X: Comprehensive Kernel Protection against Just-In-Time Code Reuse
NCC Group Open Forum | <i>New York, U.S.A.</i> |

AWARDS

- | | | |
|-----------|---|----------------------------|
| 2012-2017 | Fellowship
Graduate Research Assistant (GRA) | <i>Columbia University</i> |
| 2017 | Black Hat Speaker Honorarium | |

Teaching Experience

Teaching Assistant

COLUMBIA UNIVERSITY

- Spring 2015: Head Teaching Assistant (TA) for Network Security (Graduate level. Instructor Debbie Cook.)
- Spring 2014: Teaching Assistant (TA) for Network Security (Graduate level. Instructor Debbie Cook.)

New York, USA
Spring 2014 - Spring 2015

Service

EXTERNAL REVIEWER

- | | |
|----------------|--|
| USENIX | USENIX Security Symposium: 2017 |
| JCS | Journal of Computer Security: 2016 |
| ASIACCS | ACM Asia Conference on Computer and Communications Security: 2015 |
| MTD | ACM Workshop on Moving Target Defense: 2014 |
| IET | IET Information Security: 2014, 2018 |
| CCS | ACM Conference on Computer and Communications Security: 2013, 2014 |

LOCAL ARRANGEMENTS

- | | |
|-------------|--|
| ACNS | Applied Cryptography and Network Security (ACNS): 2015 |
|-------------|--|