Vasileios Kemerlis

Department of Computer Science
Brown University

115 Waterman Street
P.O. Box 1910
Providence, RI 02912-1910, USA
+1 (401) 863-5787
https://cs.brown.edu/~vpk
vpk@cs.brown.edu
@vkemerlis

Research Interests

I am interested in software, hardware, and systems security, with a focus on OS kernel protection, software hardening, and information flow tracking.

Education

July 2015 — **Ph.D. in Computer Science**, *Columbia University*, Department of Computer Science, Graduate School of Arts and Sciences, New York, NY, USA.
Thesis: *Protecting Commodity Operating Systems through Strong Kernel Isolation*
Advisor: Prof. Angelos Keromytis

February 2013 — **M.Phil. in Computer Science**, *Columbia University*, Department of Computer Science, Graduate School of Arts and Sciences, New York, NY, USA.

May 2010 — **M.S. in Computer Science**, *Columbia University*, Department of Computer Science, Fu Foundation School of Engineering and Applied Science, New York, NY, USA.
GPA: 4.1/4

June 2006 — **B.S. in Computer Science**, *Athens University of Economics and Business*, Department of Informatics, Athens, Greece.
GPA: 8.76/10 (ranked 1^{st} among 177 students; top 1%)

Employment

2015–present — **Assistant Professor**, *Department of Computer Science*, Brown University.

2008–2015 — **Research Assistant (graduate)**, *Network Security Lab*, Columbia University (*advisor*: Prof. Angelos Keromytis).

Summer 2013 — **Research Assistant**, *Extreme Computing Group*, Microsoft Research (*advisor*: Dr. Marcus Peinado, Dr. Weidong Cui).

Summer 2012 — **Research Assistant**, *Autonomic Management Group*, NEC Laboratories America (*advisor*: Dr. Zhichun Li).

Spring 2007 — **Research Fellow**, *Web Information Management Group*, Athens University of Economics and Business (*advisor*: Prof. Vasilis Vassalos).

2004–2007 — **Research Assistant (undergraduate)**, *Mobile Multimedia Lab*, Athens University of Economics and Business (*advisor*: Prof. George Polyzos).

Honors and Awards

November 2018 — **Finalist** (top 10), Applied Research Paper award (for `CCR` [C.1]), Cyber Security Awareness Week (CSAW), NYU Tandon School of Engineering.

August 2015 — **Nominee**, Most Innovative Research award (for `ret2dir` [C.11]), Pwnie Awards.

November 2014 — **1st place winner**, Applied Research Paper award (for `ret2dir` [C.11]), Cyber Security Awareness Week (CSAW), NYU Tandon School of Engineering.

November 2012 — **Finalist** (top 10), AT&T Applied Research Paper award (for `kGuard` [C.17]), Cyber Security Awareness Week (CSAW), NYU Tandon School of Engineering.

June 2012 — **Scholarship** (for Ph.D. studies), Gerondelis Foundation.

July 2007 — **Ericsson Award of Excellence in Telecom.** (for B.S. thesis), Ericsson Hellas.

December 2006 — **Valedictorian**, Athens University of Economics and Business, Department of Informatics.

June 2006 — Graduated **summa cum laude**, Athens University of Economics and Business, Department of Informatics.

May 2005 — **Semifinalist**, IEEE Computer Society International Design Competition (CSIDC).

Research Activities

2015–present — **Department of Computer Science**, Brown University.

▶ Kernel Protection [C.3, J.1]. The advent of strict memory isolation mechanisms between kernel and user space, like SMEP/SMAP and PXN/PAN, has resulted in the increased use of code reuse techniques for the exploitation of memory corruption vulnerabilities in kernel code. To deal with this problem, I designed and co-developed **`kR^X`** [EuroSys '17, TOPS '18]: a kernel hardening scheme, which builds upon execute-only memory and fine-grained code diversification, for combating ROP/JOP/COP and similar code reuse attacks, including (in)direct JIT-ROP, without relying on a hypervisor or any other super-privileged component.

▶ Software Hardening [C.1, C.4, C.5, C.6, C.8]. Code reuse has been promoted to the de facto technique for exploiting memory corruption vulnerabilities. To protect binary-only software against ROP/JOP/COP, or other similar code reuse attacks, including (in)direct JIT-ROP and BROP, I co-designed **`Shuffler`** [OSDI '16]: a system that continuously re-randomizes the code of a running program, including itself, thwarting end-to-end code-reuse attacks by rapidly obsoleting leaked code layouts. In the same vein, I co-designed **`CCR`** [S&P '18]: a hybrid compiler-rewriter framework that enables fast and robust fine-grained code randomization on end-user systems, by augmenting binaries with transformation-assisting metadata. To protect C++ binaries from vtable hijacking (a prevalent C++ exploitation technique), I co-designed **`VTPin`** [ACSAC '16]: a framework for armoring C++ applications, which cannot be re-compiled or modified, against vtable hijacking through use-after-free vulnerabilities. Lastly, I designed and co-developed **`NaClDroid`** [ESORICS '16] and **`DynaGuard`** [ACSAC '15]: the former sandboxes native code in Android Apps; the latter protects applications from canary brute-force attacks.

▶ Hardware Security [C.2, P.1]. Co-designed **Polyglot** [HOST '17]: the first hardware-based instruction set randomization scheme that (a) utilizes strong encryption (AES and ECC), (b) supports code sharing, and (c) is applicable to the entire software stack (bootloader, hypervisor, OS kernel, user applications). Polyglot (naturally) protects against code injection attacks, but can also mitigate code reuse if combined with leakage-resilient code diversification.

▶ Side Channels [C.9]. Co-invented the first cache-based side channel attack that can be entirely executed in JavaScript context [CCS '15]. Proposed a set of techniques for: (a) tracking browsing activity, even when the "private browsing" mode is used; (b) constructing covert channels inside the JavaScript sandbox; and (c) detecting certain hardware events (mouse and network activity, ambient light sensor interrupts).

2008–2015 **Network Security Lab**, Columbia University.

▶ Kernel Protection [C.11, C.17, M.1]. Modern OSes employ a virtual memory model that trades strong isolation for performance. I investigated the security ramifications of weak user/kernel address space separation, and designed and implemented **kGuard** [USENIX SEC '12, `;login:` '12]: a system to protect Linux/BSD kernels from attacks that exploit the weak segregation of address spaces. In addition, I introduced **ret2dir** [USENIX SEC '14]: a new exploitation technique that enables the complete circumvention of numerous software and hardware kernel protection mechanisms, including Intel's SMEP/SMAP and ARM's PXN.

▶ Data Flow Tracking [C.12, C.19, C.20]. Dynamic data flow tracking (DFT), also referred to as information flow tracking, deals with tagging and tracking data of interest as they propagate during program execution. I designed and implemented **libdft** [VEE '12]: a dynamic DFT framework that unlike previous work is at once fast, reusable, and works with commodity software and hardware. I explored different approaches for implementing efficient instruction-level data tracking, introduced a performant and 64-bit capable shadow memory, and identified the common pitfalls responsible for the excessive run-time overhead of similar tools. In addition, I co-developed a set of techniques to further reduce the slowdown of DFT frameworks, by combining static and dynamic analysis. **TFA** [NDSS '12] separates the program logic from tracking logic, extracts the semantics of the latter, and uses traditional compiler optimizations to eliminate redundant tracking. **ShadowReplica** [CCS '13] accelerates DFT, and other shadow memory-based analyses, by decoupling analysis from execution and using spare CPU cores to run them in parallel.

▶ Software Hardening [C.16]. Applications can be logically separated to parts that face different types of threats or suffer dissimilar exposure to a particular threat. Based on this observation, I co-developed Virtual Application Partitioning (**VAP**) [CCS '12]: a technique that allows the selective and targeted application of various protection mechanisms to different software parts. Furthermore, I introduced a methodology for automatically slicing software, using a binary monitor and an intrinsic application property (user authentication), to dynamically adapt the defences being deployed by switching between protection mechanisms like dynamic taint analysis and instruction-set randomization.

▶ Anonymity Systems [C.14]. **CellFlood** [ESORICS '13] is a DoS attack that I co-developed, against Tor onion routers, which exploits a design flaw in the way Tor software builds virtual circuits. I studied the feasibility and implications of CellFlood, and demonstrated that an attacker needs only a fraction of the resources required by a network DoS attack for achieving similar damage. Furthermore, I contributed to the design and implementation of an effective solution to the problem that relies on cryptographic client puzzles.

▶ Cloud Auditing [C.15, C.13]. The risk of unauthorized access to private cloud-resident data is among the primary concerns to users of cloud services. I contributed to the design and implementation of **CloudFence** [RAID '13]: a framework that allows users to independently audit the treatment of their data, by third-party services, through the intervention of the cloud provider that hosts these services. CloudFence is built on top a fine-grained DFT framework that I developed (libdft), and besides data auditing it enables service providers to confine the use of sensitive data in well-defined domains, offering protection against inadvertent leaks and unauthorized accesses.

▶ System & Network Deception [C.22, C.23, J.2, P.3 – P.6]. **BotSwindler** [RAID '10] is a bait-injection system designed to delude and detect crimeware, by forcing it to reveal itself during the exploitation of monitored information. I contributed to the design and implementation of BotSwindler, which relies upon an out-of-host software agent that drives user-like interactions inside a virtual machine, seeking to convince malware residing within a guest OS that has captured legitimate credentials. In addition, I co-developed a novel trap-based architecture for enterprise networks that detects "silent" attackers who are eavesdropping on network traffic [WiSec '10, JCS '12].

Summer 2013 **Extreme Computing Group**, Microsoft Research.
Design and implementation of **RETracer** [C.7]: a debugging extension that leverages type information for triaging crash dumps. RETracer [ICSE '16] offers enhanced crash dump classification by utilizing static taint analysis, opportunistic reverse (concrete) execution, and a new concept that I co-developed, named backward data-flow graphs.

Summer 2012 **Autonomic Management Group**, NEC Laboratories America.
Worked on **AAPL** [C.10, P.2]. AAPL [NDSS '15] is a static analysis framework that uses data flow tracking to vet Android Apps for component hijacking vulnerabilities (permission leakage, unauthorized data access, intent spoofing). I designed and developed a novel conditional tracking scheme that leverages constant folding/propagation techniques for improving the accuracy and detection rate of the framework.

2004–2007 **Mobile Multimedia Lab**, Athens University of Economics and Business.
Worked on the Peer-to-Peer Wireless Network Confederation (**P2PWNC**) project [C.26, C.28, M.2, D.1, D.2, D.3]. P2PWNC focuses on the reciprocal provision of Internet access to mobile users through voluntary-controlled wireless access points. Implemented a Quality of Service (QoS) module [AccessNets '06] to facilitate the differentiation of the provided service, and studied the performance tradeoffs associated with various setups and architectural factors [MobiMedia '07].

Impact and Technology Transfer

XPFO [C.11] Adopted by the Linux kernel for defending against `ret2dir` attacks (*in progress*).
`https://goo.gl/4fjQaq`

RETracer [C.7] Adopted by Microsoft as the primary tool for triaging crashes; part of the Windows Error Reporting (WER) platform (since March 2015).
`https://goo.gl/t8CfHr`

"Spy in the Sandbox" [C.9]

- Apple limited the time resolution of WebKit's performance API (iOS 9 and onward). `https://goo.gl/EqCK4a`
- Mozilla reduced the resolution of `performance.now()` in Firefox (v41 and onward). `https://goo.gl/QmAqII`
- Tor decreased the time precision of JavaScript in the Tor Browser (v5.0.1 and onward). `https://goo.gl/BixTBT`
- W3C TAG finding, *Unsanctioned Web Tracking* (Finding 17, July 2015). `https://goo.gl/rKpRR9`

ret2dir [C.11]

- Linux hardened access to `/proc` for mitigating `ret2dir` attacks (v4.0 and onward). `https://goo.gl/010alY`
- OpenBSD introduced `ret2dir`-specific mitigations (v5.7 and onward). `https://goo.gl/qAmAhK`

Press and Media Coverage

○ Software Hardening [C.5]

01/17/2017 **Network World.** *7 really cool network and IT research projects.* `https://goo.gl/8wwKYj`

11/18/2016 **ACM TechNews.** *New Software Continuously Scrambles Code to Foil Cyberattacks.* `https://goo.gl/GKCvhv`

○ Side Channels [C.9]

04/21/2015 **The Register.** *JavaScript CPU cache snooper tells crooks EVERYTHING you do online.* `https://goo.gl/UhvsT8`

04/20/2015 **Forbes.** *New Browser Hack Can Spy On Eight Out Of Ten PCs.* `https://goo.gl/TX0kRq`

03/18/2015 **Hacker News.** *The Spy in the Sandbox: Practical Cache Attacks in JavaScript.* `https://goo.gl/ittVPz`

○ Kernel Protection [C.11]

01/02/2017 **Linux Journal.** *What's New in Kernel Development.* `https://goo.gl/hpcHCy`

09/14/2016 **LWN.net.** *Exclusive page-frame ownership.* `https://goo.gl/JiuOeo`

10/17/2014 **Reddit.** *ret2dir: Deconstructing Kernel Isolation.* `https://goo.gl/wslaaQ`

10/17/2014 **Hacker News.** *ret2dir: Rethinking Kernel Isolation.* `https://goo.gl/ON1wyk`

09/09/2014 **Dark Reading.** *Black Hat Europe 2014: Gullible Computers.* `https://goo.gl/DniZ7O`

Software Artifacts

CCR [C.1] https://github.com/kevinkoo001/CCR

kR^X [C.3] https://github.com/mpomonis/krx

VTPin [C.4] https://github.com/uberspot/vtpin

DynaGuard [C.8] https://github.com/nettrino/dynaguard

XPFO [C.11] https://www.cs.columbia.edu/~vpk/research/xpfo/

ret2dir [C.11] https://www.cs.columbia.edu/~vpk/research/ret2dir/

kGuard [C.17] https://www.cs.columbia.edu/~vpk/research/kguard/

libdft [C.19] https://www.cs.columbia.edu/~vpk/research/libdft/

P2PWNC [M.2] https://mm.aueb.gr/research/p2pwnc/

Teaching

Instructor

▶ All courses are new additions to the curriculum and were developed from scratch. (Numbers in parentheses indicate enrollment.)

CSCI 1650 **Software Security and Exploitation**, Brown University.
Fall 2018 (52), Fall 2017 (36), Fall 2016 (28)

CSCI 2951U **Topics in Software Security**, Brown University.
Spring 2018 (12), Spring 2017 (9), Spring 2016 (4)

Teaching Assistant

▶ Created and graded homeworks, midterms, and final exams; prepared project material and gave lectures. (Numbers in parentheses indicate enrollment.)

COMS W4180 **Network Security**, Columbia University.
Instructor: Prof. Angelos Keromytis. Fall 2012 (23), Spring 2010 (30)

COMS W4187 **Security Architecture and Engineering**, Columbia University.
Instructor: Prof. Steven Bellovin. Fall 2009 (15)

Advising and Mentoring

Doctoral Students

2018–present Maria Loukidi-Papanikoli (Dept. of Computer Science, Brown University).

2017–present Kent Williams-King (Dept. of Computer Science, Brown University).

2016–present Di Jin (Dept. of Computer Science, Brown University).

2014–present Marios Pomonis (Dept. of Computer Science, Columbia University).
Co-advisor: Prof. Angelos Keromytis

2014–2016 João Moreira (Institute of Computing, University of Campinas).
Thesis: *Protection Mechanisms Against Kernel Control-Flow Hijacking Attacks*
Co-advisor: Prof. Sandro Rigo
Post-graduation: SUSE (Software Engineer)

Master's Students

2017–2018 Sorin Vatasoiu (Dept. of Computer Science, Brown University),
`kRNG:` *Breaking and Fixing the Linux Pseudo-Random Number Generator.*
Post-graduation: Global Trading Systems (Software Engineer)

2015–2016 Pawel Sarbinowski (Dept. of Computer Science, Aalto University),
`VTPin:` *Protecting Legacy Software from VTable Hijacking.* [C.4]
Co-advisor: Prof. Elias Athanasopoulos
Post-graduation: Microsoft (Software Engineer)

2015–2016 Jordan Hendricks (Dept. of Computer Science, Brown University),
`kGuard++:` *Improving the Performance of kGuard with Low-latency Code Inflation.*
Post-graduation: Joyent (Software Engineer)

Undergraduate Students

2018–present Elisa Guerrant (Dept. of Computer Science, Brown University).

2018–present Benjamin Shteinfeld (Dept. of Computer Science, Brown University).

2017–2018 Di Yang Shi (Dept. of Computer Science, Brown University),
`AdvNN:` *An Exposition of Adversarial Examples in Neural Networks.*

Other Mentoring Activities

2014–2015 Theofilos Petsios (Ph.D. student; Columbia University),
`DynaGuard:` *Armoring Canary-based Protections against Brute-force Attacks.* [C.8]

Spring 2014 Pratyush Parimal (M.S. student; Columbia University),
`LHS:` *An Empirical Study of Exploit Mitigation Techniques in Linux Distributions.*

Spring 2013 Yibo Zhu (M.S. student; Columbia University),
Apache Tripwire: *Intrusion Recovery for Web Applications.*

2011–2013 Marco Barbera (Ph.D. student; visiting scholar from Sapienza University of Rome),
`CellFlood:` *Attacking Tor Onion Routers on the Cheap.* [C.14]

Service

Program Committee Member

`USENIX SEC` USENIX Security Symposium, 2019.

`ACSAC` Annual Computer Security Applications Conference, 2017, 2018.

DIMVA International Conference on Detection of Intrusions and Malware & Vuln. Asmt., 2017–2019.
ASIACCS ACM Asia Conference on Computer and Communications Security, 2018.
DSC IEEE Conference on Dependable and Secure Computing, 2017, 2018.
WWW International World Wide Web Conference, 2017.
ESSoS International Symposium on Engineering Secure Software and Systems, 2017.
RAID International Symposium on Research in Attacks, Intrusions and Defenses, 2016.
ISC International Information Security Conference, 2016.
WOOT USENIX Workshop on Offensive Technologies, 2018.
EuroSec European Workshop on Systems Security, 2016–2019.
CCSW ACM Cloud Computing Security Workshop, 2017.

Journal Reviewer

TDSC IEEE Transactions on Dependable and Secure Computing, 2017–2019.
TMC IEEE Transactions on Mobile Computing, 2018, 2019.
TCAD IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2017, 2018.
COSE Computers & Security, 2016, 2018.
TCC IEEE Transactions on Cloud Computing, 2016, 2017.
JSME Journal of Software: Evolution and Process, 2016.

External Reviewer

NDSS Network and Distributed System Security Symposium, 2014, 2015.
CCS ACM Conference on Computer and Communications Security, 2010–2014.
ACNS International Conference on Applied Cryptography and Network Security, 2010–2013.
USENIX ATC USENIX Annual Technical Conference, 2011.

Grant Reviewer

NSF National Science Foundation (*Panelist*), 2018.

Dissertation Committee Member

November 2018 Kanad Sinha, *Repurposing Software Defenses with Specialized Hardware*, Columbia University.
November 2018 Ioannis Agadakos, *Improving Software by Disabling Unused Code in Dynamically Linked Applications*, Stevens Institute of Technology.
March 2018 Theofilos Petsios, *Compiler-assisted Adaptive Software Testing*, Columbia University.

University Service

2017–present Concentration advising, Dept. of Computer Science, Brown University.
2015–present PhD admissions committee (*Member*), Dept. of Computer Science, Brown University.

Talks, Lectures, Presentations

Invited Talks

- **Secure Operating Systems** [C.3, C.11, C.17]

February 2018 — Wayne State University, *Host*: Prof. Fengwei Zhang
January 2018 — Athens University of Economics and Business, *Host*: Prof. George Polyzos
July 2017 — University of Athens, *Host*: Prof. Mema Roussopoulos

- **Building Trustworthy Systems** [C.2]

August 2016 — Columbia University, *Host*: Prof. Simha Sethumadhavan

- **Rethinking Kernel Isolation** [C.11]

October 2016 — Athens University of Economics and Business, *Host*: Prof. George Polyzos
November 2014 — Stevens Institute of Technology, *Host*: Prof. Georgios Portokalidis
October 2014 — VU University Amsterdam, *Host*: Prof. Herbert Bos
September 2014 — Georgia Institute of Technology, *Host*: Dr. Tielei Wang, Prof. Wenke Lee

- **Lightweight Kernel Protection against Return-to-user Attacks** [C.17]

November 2012 — AT&T Security Research Center, *Host*: Dr. Baris Coskun
July 2012 — NEC Laboratories America, *Host*: Dr. Zhichun Li

Guest Lectures

April 2016 — **The Role of the Operating System in the Era of Cyberwar**
Cybersecurity and International Relations (CSCI 1800), Brown University.
Instructor: Prof. John Savage

December 2015 — **Kernel Security (in the Embedded Word)**
Embedded and Real Time Software (CSCI 1600), Brown University.
Instructor: Prof. Steven Reiss

November 2014 — **Kernel Security: Attacks and Defenses**
Secure Systems (CS 576), Stevens Institute of Technology.
Instructor: Prof. Georgios Portokalidis

October 2014 — **Kernel Security: Building Trustworthy OSes**
Reliable Software (COMS E6121), Columbia University.
Instructor: Prof. Junfeng Yang

April 2010 — **Packet Filters: Proposed Solutions and Current Trends**
Network Systems Design and Implementation (COMS W6998), Columbia University.
Instructor: Dr. Erich Nahum

May 2009 — **Securing Networked Applications: The Role of Program Structure**
Network Security, Athens University of Economics and Business.
Instructor: Dr. Elias Efstathiou, Dr. Thanasis Papaioannou

Conference Presentations

February 2017 **The Role of Low-level Software in the Era of Cyber Conflict**
Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), San Fransisco, CA, USA.

October 2014 **`ret2dir`: Deconstructing Kernel Isolation**
Black Hat Europe (BHEU), Amsterdam, Netherlands.

August 2014 **`ret2dir`: Rethinking Kernel Isolation**
USENIX Security Symposium (USENIX SEC), San Diego, CA, USA.
[Video: `https://goo.gl/Cxdz7C`, Audio: `https://goo.gl/ab3vIJ`]

August 2012 **`kGuard`: Lightweight Kernel Protection against Return-to-user Attacks**
USENIX Security Symposium (USENIX SEC), Bellevue, WA, USA.
[Video: `https://goo.gl/y3rvHK`, Audio: `https://goo.gl/JM2cgh`]

March 2012 **`libdft`: Practical Dynamic Data Flow Tracking for Commodity Systems**
International Conference on Virtual Execution Environments (VEE), London, UK.

Industry Appointments

Summer 2014 **Software Engineer**, *Oracle America Inc.*, Santa Clara, CA, USA.
Member of the Solaris Core Kernel team. *Tasks included*: patching the kernel of Oracle Solaris to add support for full Address Space Layout Randomization (ASLR), modifying the build environment for compiling the OS/Net userland binaries as position-independent (PIE), and evaluating the performance overhead of position-independent code (PIC).

2007–2008 **Software Engineer**, *MySapient Ltd.*, Athens, Greece.
Participated in the design and development of a massively multiplayer online game (MMOG) and a social network. *Tasks included*: designing, and implementing in C++, a set of client-side networking libraries, as well as a networked game server using a distributed and scalable architecture.

2005–2007 **Student Consultant**, *Microsoft Hellas*, Athens, Greece.
Member of Developers Platform Evangelists (DPE) group. *Tasks included*: administering the departmental Microsoft Developer Network Academic Alliance (MSDNAA) subscription, organizing technical presentations (for students) involving Microsoft products, advising students entering Microsoft's worldwide "Imagine Cup" programming contest, and setting up and moderating the studentguru.gr community website. `http://www.studentguru.gr`

Funding

[F.1] Hardware-Up Security: Anti-fragility and Automation. **Co-PI**
(PI: Simha Sethumadhavan, co-PIs: Luca Carloni, Subhasish Mitra), Defense Advanced Research Projects Agency (DARPA), HR001118C0017, $5,774,181 (Brown share: **$454,099**), 12/06/2017 – 03/05/2021.

[F.2] ABIDES: Adaptive BInary Debloating and Security. **Co-PI**
(PI: Georgios Portokalidis, co-PI: Junfeng Yang),
Office of Naval Research (ONR), N00014-17-1-2788,
$3,243,244 (Brown share: **$925,930**), 09/01/2017 – 08/31/2020.

Patents

[P.1] S. Sethumadhavan, K. Sinha, A. D. Keromytis, V. Pappas, and **V. P. Kemerlis**. Diversified instruction set processing to enhance security (*patent pending*).

[P.2] Z. Li, Z. Wu, Z. Qian, G. Jiang, K. Lu, and **V. P. Kemerlis**. Duleak: a scalable app engine for high-impact privacy leaks.
U.S. Patent 9,245,125. Issued: Jan 26, 2016.

[P.3] B. M. Bowen, P. V. Prabhu, **V. P. Kemerlis**, S. Sidiroglou, S. J. Stolfo, and A. D. Keromytis. Methods, systems, and media for detecting covert malware.
U.S. Patent 9,971,891. Issued: May 15, 2018.

[P.4] S. J. Stolfo, A. D. Keromytis, B. M. Bowen, S. Herhskop, **V. P. Kemerlis**, P. V. Prabhu, and M. B. Salem. Methods, systems, and media for baiting inside attackers. U.S. Patent 9,501,639. Issued: Nov 22, 2016.

[P.5] S. J. Stolfo, A. D. Keromytis, B. M. Bowen, S. Herhskop, **V. P. Kemerlis**, P. V. Prabhu, and M. B. Salem. Methods, systems, and media for baiting inside attackers. U.S. Patent 9,009,829. Issued: Apr 14, 2015.

[P.6] B. M. Bowen, P. V. Prabhu, **V. P. Kemerlis**, S. Sidiroglou, S. J. Stolfo, and A. D. Keromytis. Methods, systems, and media for detecting covert malware.
U.S. Patent 8,528,091. Issued: Sep 3, 2013.

Publications

▶ Google Scholar [`https://goo.gl/DMK8AJ`] – DBLP [`https://goo.gl/dpaFrg`]
(Student advisees are underlined.)

Journal Articles (Refereed)

[J.1] M. Pomonis, T. Petsios, A. D. Keromytis, M. Polychronakis, and **V. P. Kemerlis**. Kernel Protection against Just-In-Time Code Reuse. *ACM Transactions on Privacy and Security (TOPS)*, to appear.

[J.2] B. M. Bowen, **V. P. Kemerlis**, P. Prabhu, A. D. Keromytis, and S. J. Stolfo. A System for Generating and Injecting Indistinguishable Network Decoys. *Journal of Computer Security (JCS)*, 20(2-3), January 2012.

Conference Proceedings (Refereed)

[C.1] H. Koo, Y. Chen, L. Lu, **V. P. Kemerlis**, and M. Polychronakis. Compiler-assisted Code Randomization. In *Proceedings of the 39th IEEE Symposium on Security and Privacy (S&P)*, San Fransisco, CA, USA, May 2018. [Acceptance rate: 11.5%]

[C.2] K. Sinha, **V. P. Kemerlis**, and S. Sethumadhavan. Reviving Instruction Set Randomization. In *Proceedings of the 9th IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, McLean, VA, USA, May 2017. [Acceptance rate: 24.5%]

[C.3] M. Pomonis, T. Petsios, A. D. Keromytis, M. Polychronakis, and **V. P. Kemerlis**. kR^X: Comprehensive Kernel Protection against Just-In-Time Code Reuse. In *Proceedings of the 12th European Conference on Computer Systems (EuroSys)*, Belgrade, Serbia, April 2017. [Acceptance rate: 20%]

[C.4] P. Sarbinowski, C. Giuffrida, **V. P. Kemerlis**, and E. Athanasopoulos. VTPin: Practical VTable Hijacking Protection for Binaries. In *Proceedings of the 32nd Annual Computer Security Applications Conference (ACSAC)*, Los Angeles, CA, USA, December 2016. [Acceptance rate: 22.8%]

[C.5] D. Williams-King, G. Gobieski, K. Williams-King, J. P. Blake, X. Yuan, P. Colp, M. Zheng, **V. P. Kemerlis**, J. Yang, and W. Aiello. Shuffler: Fast and Deployable Continuous Code Re-Randomization. In *Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, Savannah, GA, USA, November 2016. [Acceptance rate: 18.1%]

[C.6] E. Athanasopoulos, **V. P. Kemerlis**, G. Portokalidis, and A. D. Keromytis. NaClDroid: Native Code Isolation for Android Applications. In *Proceedings of the 21st European Symposium on Research in Computer Security (ESORICS)*, Heraklion, Greece, September 2016. [Acceptance rate: 21%]

[C.7] W. Cui, M. Peinado, S. K. Cha, Y. Fratantonio, and **V. P Kemerlis**. RETracer: Triaging Crashes by Reverse Execution from Partial Memory Dumps. In *Proceedings of the 38th International Conference on Software Engineering (ICSE)*, Austin, TX, USA, May 2016. [Acceptance rate: 19%]

[C.8] T. Petsios, **V. P. Kemerlis**, M. Polychronakis, and A. D. Keromytis. DynaGuard: Armoring Canary-based Protections against Brute-force Attacks. In *Proceedings of the 31st Annual Computer Security Applications Conference (ACSAC)*, Los Angeles, CA, USA, December 2015. [Acceptance rate: 24.4%]

[C.9] Y. Oren, **V. P. Kemerlis**, S. Sethumadhavan, and A. D. Keromytis. The Spy in the Sandbox: Practical Cache Attacks in JavaScript and their Implications. In *Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS)*, Denver, CO, USA, October 2015. [Acceptance rate: 19.8%]

[C.10] K. Lu, Z. Li, **V. P. Kemerlis**, Z. Wu, L. Lu, C. Zheng, Z. Qian, W. Lee, and G. Jiang. Checking More and Alerting Less: Detecting Privacy Leakages via Enhanced Data-flow Analysis and Peer Voting. In *Proceedings of the 22nd Network and Distributed System Security (NDSS) Symposium*, San Diego, CA, USA, February 2015. [Acceptance rate: 16.9%]

[C.11] **V. P. Kemerlis**, M. Polychronakis, and A. D. Keromytis. ret2dir: Rethinking Kernel Isolation. In *Proceedings of the 23rd USENIX Security Symposium (USENIX SEC)*, San Diego, CA, USA, August 2014. [Acceptance rate: 19%]

[C.12] K. Jee, **V. P. Kemerlis**, A. D. Keromytis, and G. Portokalidis. ShadowReplica: Efficient Parallelization of Dynamic Data Flow Tracking. In *Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS)*, Berlin, Germany, October 2013. [Acceptance rate: 19.8%]

[C.13] V. Pappas, **V. P. Kemerlis**, A. Zavou, M. Polychronakis, and A. D. Keromytis. CloudFence: Data Flow Tracking as a Cloud Service. In *Proceedings of the 16th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, Saint Lucia, October 2013. [Acceptance rate: 23.1%]

[C.14] M. V. Barbera, **V. P. Kemerlis**, V. Pappas, and A. D. Keromytis. CellFlood: Attacking Tor Onion Routers on the Cheap. In *Proceedings of the 18th European Symposium on Research in Computer Security (ESORICS)*, Egham, UK, September 2013. [Acceptance rate: 17.8%]

[C.15] A. Zavou, V. Pappas, **V. P. Kemerlis**, M. Polychronakis, G. Portokalidis, and A. D. Keromytis. Cloudopsy: an Autopsy of Data Flows in the Cloud. In *Proceedings of the 15th International Conference on Human-Computer Interaction (HCI)*, Las Vegas, NV, USA, July 2013.

[C.16] D. Geneiatakis, G. Portokalidis, **V. P. Kemerlis**, and A. D. Keromytis. Adaptive Defenses for Commodity Software through Virtual Application Partitioning. In *Proceedings of the 19th ACM Conference on Computer and Communications Security (CCS)*, Raleigh, NC, USA, October 2012. [Acceptance rate: 18.9%]

[C.17] **V. P. Kemerlis**, G. Portokalidis, and A. D. Keromytis. kGuard: Lightweight Kernel Protection against Return-to-user Attacks. In *Proceedings of the 21st USENIX Security Symposium (USENIX SEC)*, Bellevue, WA, USA, August 2012. [Acceptance rate: 19.4%]

[C.18] E. Athanasopoulos, **V. P. Kemerlis**, M. Polychronakis, and E. P. Markatos. ARC: Protecting against HTTP Parameter Pollution Attacks Using Application Request Caches. In *Proceedings of the 10th International Conference on Applied Cryptography and Network Security (ACNS)*, Singapore, June 2012. [Acceptance rate: 17.2%]

[C.19] **V. P. Kemerlis**, G. Portokalidis, K. Jee, and A. D. Keromytis. libdft: Practical Dynamic Data Flow Tracking for Commodity Systems. In *Proceedings of the 8th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments (VEE)*, London, UK, March 2012.

[C.20] K. Jee, G. Portokalidis, **V. P. Kemerlis**, S. Ghosh, D. I. August, and A. D. Keromytis. A General Approach for Efficiently Accelerating Software-based Dynamic Data Flow Tracking on Commodity Hardware. In *Proceedings of the 19th Network and Distributed System Security (NDSS) Symposium*, San Diego, CA, USA, February 2012. [Acceptance rate: 18%]

[C.21] **V. P. Kemerlis**, V. Pappas, G. Portokalidis, and A. D. Keromytis. iLeak: A Lightweight System for Detecting Inadvertent Information Leaks. In *Proceedings of the 6th European Conference on Computer Network Defense (EC2ND)*, Berlin, Germany, October 2010.

[C.22] B. M. Bowen, P. Prabhu, **V. P. Kemerlis**, S. Sidiroglou, A. D. Keromytis, and S. J. Stolfo. BotSwindler: Tamper Resistant Injection of Believable Decoys in VM-Based Hosts for Crimeware Detection. In *Proceedings of the 13th International Symposium on Recent Advances in Intrusion Detection (RAID)*, Ottawa, Canada, September 2010. [Acceptance rate: 23%]

[C.23] B. M. Bowen, **V. P. Kemerlis**, P. Prabhu, A. D. Keromytis, and S. J. Stolfo. Automating the Injection of Believable Decoys to Detect Snooping. In *Proceedings of the 3rd ACM Conference on Wireless Network Security (WiSec)*, Hoboken, NJ, USA, March 2010 (*short paper*). [Acceptance rate: 21.2%]

[C.24] K. Katsaros, **V. P. Kemerlis**, C. Stais, and G. Xylomenos. A BitTorrent Module for the OMNeT++ Simulator. In *Proceedings of the 17th IEEE/ACM International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS)*, London, UK, September 2009.

[C.25] A. Kosmopoulos, I. Karamichali, **V. P. Kemerlis**, and G. C. Polyzos. Fueling Game Development in Mobile P2P Environments. In *Proceedings of the 18th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Athens, Greece, September 2007.

[C.26] P. A. Frangoudis, **V. P. Kemerlis**, D. C. Paraskevaidis, E. C. Efstathiou, and G. C. Polyzos. Experimental Evaluation of Community-Based WLAN Voice and Data Services. In *Proceedings of the 3rd International Mobile Multimedia Communications Conference (MobiMedia)*, Nafpaktos, Greece, August 2007.

[C.27] E. G. Giannopoulou, **V. P. Kemerlis**, M. Polemis, J. Papaparaskevas, A. C. Vatopoulos, and M. Vazirgiannis. A Large Scale Data Mining Approach to Antibiotic Resistance Surveillance. In *Proceedings of the 20th IEEE International Symposium on Computer-Based Medical Systems (CBMS)*, Maribor, Slovenia, June 2007.

[C.28] E. C. Efstathiou, F. A. Elianos, P. A. Frangoudis, **V. P. Kemerlis**, D. C. Paraskevaidis, E. C. Stefanis, and G. C. Polyzos. Public Infrastructures for Internet Access in Metropolitan Areas. In *Proceedings of the 1st International Conference on Access Networks (AccessNets)*, Athens, Greece, September 2006.

[C.29] **V. P. Kemerlis**, E. C. Stefanis, G. Xylomenos, and G. C. Polyzos. Throughput Unfairness in TCP over WiFi. In *Proceedings of the 3rd IFIP Conference on Wireless On Demand Network Systems and Services (WONS)*, Les Mènuires, France, January 2006.

Workshop Proceedings (Refereed)

[W.1] G. Xylomenos, K. Katsaros, and **V. P. Kemerlis**. Peer Assisted Content Distribution over Router Assisted Overlay Multicast. In *Proc. of the 1st Euro-NF Workshop on Future Internet Architecture (FIA)*, Paris, France, November 2008.

Magazine Articles (Edited)

[M.1] **V. P. Kemerlis**, G. Portokalidis, E. Athanasopoulos, and A. D. Keromytis. kGuard: Lightweight Kernel Protection. *USENIX ;`login:` Magazine*, 37(6), December 2012.

[M.2] P. A. Frangoudis, G. C. Polyzos, and **V. P. Kemerlis**. Wireless Community Networks: An Alternative Approach for Broadband Nomadic Network Access. *IEEE Communications Magazine*, 49(5), May 2011.

Demo

[D.1] E. C. Efstathiou, F. A. Elianos, P. A. Frangoudis, **V. P. Kemerlis**, D. C. Paraskevaidis, G. C. Polyzos, and E. C. Stefanis. Practical Incentive Techniques for Wireless Community Networks. In *International Conference on Mobile Systems, Applications, and Services (MobiSys)*, Uppsala, Sweden, June 2006.

[D.2] E. C. Efstathiou, F. A. Elianos, P. A. Frangoudis, **V. P. Kemerlis**, D. C. Paraskevaidis, G. C. Polyzos, and E. C. Stefanis. The Peer-to-Peer Wireless Network Confederation Scheme. In *International Conference on Computer Communications (INFOCOM)*, Barcelona, Spain, April 2006.

[D.3] E. C. Efstathiou, F. A. Elianos, P. A. Frangoudis, **V. P. Kemerlis**, D. C. Paraskevaidis, G. C. Polyzos, and E. C. Stefanis. The Peer-to-Peer Wireless Network Confederation Scheme: Protocols, Algorithms, and Services. In *International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (TridentCom)*, Barcelona, Spain, March 2006.

Non-academic Papers

[Z.1] M. Pomonis, T. Petsios, A. D. Keromytis, M. Polychronakis, and **V. P. Kemerlis**. kR^X: Comprehensive Kernel Protection against Just-In-Time Code Reuse. In *Black Hat USA (BHUSA)*, Las Vegas, NV, USA, July 2017.

[Z.2] J. Moreira, S. Rigo, M. Polychronakis, and **V. P. Kemerlis**. Drop the ROP: Fine-Grained Control-Flow Integrity for the Linux Kernel. In *Black Hat Asia (BHASIA)*, Singapore, March 2017.

[Z.3] **V. P. Kemerlis**, M. Polychronakis, and A. D. Keromytis. ret2dir: Deconstructing Kernel Isolation. In *Black Hat Europe (BHEU)*, Amsterdam, Netherlands, October 2014.