Website: www.cspensky.info **Phone:** (740) 632-6257 **E-mail:** cspensky@cs.ucsb.edu

Chad Samuel Spensky

EDUCATION

University of California, Santa Barbara Santa Barbara, CA September 2015
Doctor of Philosophy in Computer Science (**Computer Security**) Summer 2020 *(Projected)*

University of North Carolina at Chapel Hill Chapel Hill, NC August 2008
Master of Science in Computer Science (**Computer Security**) December 2010
Doctor of Philosophy in Computer Science December 2011 *(Left Program)*

University of Pittsburgh Pittsburgh, PA August 2004
University of Virginia *Semester at Sea* East and Southeast Asia *Summer 2006*
Bachelor of Science *(*GPA: 3.7, *Magna Cum Laude)* April 2008
Majors: **Computer Science (Honors) / Mathematics** Minor: **Economics**

RELATED EXPERIENCE

University of California, Santa Barbara Santa Barbara, CA *September 2015 – Present*
Ph.D. Candidate
- Currently a member of the *SecLab* and the *Shellphish* CTF team, both led by Christopher Kruegel and Giovanni Vigna.
- My current research involves novel authentication mechanisms using mobile phones, automated embedded systems analysis, hardware defenses, and low-level security evaluations (i.e., TrustZone, kernel drives).

MIT Lincoln Laboratory Lexington, MA *September 2015 – Present*
Self-Employed Consultant
- I currently consult for MIT Lincoln Laboratory on various projects, across multiple divisions on an as-needed basis.

MIT Lincoln Laboratory Lexington, MA *January 2012 – September 2015*
Associate Staff
- Worked on various projects that were focused on: web re-hosting, hardware-based introspection, semantic gap reconstruction, smart card security, communications for disaster relief, privacy on mobile devices, and novel authentication mechanisms.

University of North Carolina at Chapel Hill Chapel Hill, NC *August 2011 – December 2011*
Teaching Assistant (COMP 411: Computer Organization)
- Led weekly lab, created new assignments, graded programming and written assignments, and mentored numerous students with graduate school and employment decisions.

MIT Lincoln Laboratory Lexington, MA *May 2011 – August 2011*
Summer Intern
- Devised a novel method of creating templates of web pages using a probabilistic context-free grammar, which could be used for generating synthetic data on cyber **testbeds**.

University of North Carolina at Chapel Hill Chapel Hill, NC *August 2008 – May 2011*
Research Assistant
- Worked with Michael K. Reiter on multiple computer security related projects primarily focused on novel **authentication** schemes, networking protocols, and **machine learning**.

University of Pittsburgh Pittsburgh, PA *July 2007 – July 2008*
Lead Web Developer
- Was the lead developer of an interdisciplinary project that utilizes AJAX, PHP, Java, MySQL, CSS, and JavaScript to create a complete data exchange website for the CMPI project. *[http://db.cs.pitt.edu/group/projects/cmpi]*

CONFERENCE APPEARANCES

PeriScope: An Effective Probing and Fuzzing Framework for the Hardware-OS Boundary

Dokyung Song, Felicitas Hetzelt, Dipanjan Das, Chad Spensky, Yeoul Na, Stijn Volckaert, Giovanni Vigna, Christopher Kruegel, Jean-Pierre Seifert, Michael Franz

- Appeared at the Network and Distributed System Security Symposium (NDSS), 2019
- Developed a novel technique for both observing and **fuzzing** the interface of kernel drivers from the peripheral's perspective.

DR. CHECKER: A Soundy Analysis for Linux Kernel Drivers *(Internet Defense Prize Finalist)*

Aravind Machiry, Chad Spensky, Jacob Corina, Nick Stephens, Christopher Kruegel, Giovanni Vigna

- Appeared at the 26th USENIX Security Symposium (USENIX), 2017
- Developed a novel, *soundy*, static-analysis tool for **Linux kernel drivers**, which uncovered **158 zero-day bugs** with an overall precision of 78%.

BOOMERANG: Exploiting the Semantic Gap in Trusted Execution Environments

Aravind Machiry, Eric Gustafson, Chad Spensky, Chris Salls, Nick Stephens, Ruoyu Wang, Antonio Bianchi, Yung Ryn Choe, Christopher Kruegel, Giovanni Vigna

- Appeared at the Network and Distributed System Security Symposium (NDSS), 2017
- Highlighted a **critical bug** resulting from the semantic-gap between the trusted and untrusted worlds on TrustZone-enabled **mobile phones**, as well as a **novel defense**.

SoK: Privacy on Mobile Devices – It's Complicated

Chad Spensky, Jeffrey Stewart, Arkady Yerukhimovich, Richard Shay, Ari Trachtenberg, Rick Housley, and Robert K Cunningham

- Appeared at the Privacy Enhancing Technologies Symposium (PETS), 2016
- Analyzed the state-of-**privacy** for **mobile devices**, providing insights and suggestions for the development of future privacy-enhancing technologies.

Towards Transparent Introspection

Kevin Leach, Chad Spensky, Westly Weimer, and Fengwei Zhang

- Appeared at the 23rd IEEE Conference on Software Analysis, Evolution, and Reengineering (SANER), 2016
- Introduced the concept of **process-based introspection** and described the potential capabilities and limitations of such a system (e.g., information retrieval vs. polling interval).

LO-PHI: Low-Observable Physical Host Instrumentation for Malware Analysis

Chad Spensky, Hongyi Hu, and Kevin Leach

- Appeared at the Network and Distributed System Security Symposium (NDSS), 2016
- Demonstrated the ability to analyze **highly-sophisticated malware** with the same fidelity as existing systems, using both **hardware** and **software introspection** mechanisms coupled with novel **semantic-gap** reconstruction techniques.

Using Open-source Hardware to Support Disadvantaged Communications

Andrew Weinert, Hongyi Hu, Chad Spensky, and Benjamin Bullough

- Appeared at the Global Humanitarian Technology Conference (GHTC), 2015
- Developed, deployed, and tested a ad-hoc communications network to be used in **disaster-relief** scenarios.

Live Disk Forensics on Bare Metal

Chad Spensky and Hongyi Hu

- Appeared at the Open Source Digital Forensics Conference (OSDFCon), 2014
- Developed an **FPGA** to **passively monitor SATA traffic** of physical machines and developed the necessary components, e.g. SATA protocol reconstruction, to bridge the **semantic gap** to high-level file system operations in realtime.

Discovering Access-control Misconfigurations: New approaches and Evaluation Methodologies *(Primary Author)*

Lujo Bauer, Yuan Liang, Michael K. Reiter, and Chad Spensky

- Appeared at the Second ACM Conference on Data and Application Security and Privacy (CODASPY), 2012
- Proposed a **machine learning** approach for efficiently identifying accesses that are wrongfully denied in **access-control** environments, i.e. misconfigurations, and evaluated its usefulness in multiple scenarios.

Making Peer-Assisted Content Distribution Robust to Collusion Using Bandwidth Puzzles

Michael K. Reiter, Vyas Sekar, Chad Spensky, and Zhenghao Zhang

- Appeared at Fifth International Conference on Information Security Systems (ICISS), 2009.
- Proposed and demonstrated the use of **cryptographic puzzles** to enforce bandwidth usage in contribution-aware systems.

COMPUTER SKILLS

Operating Systems: **Ubuntu, OSX**

Software Experience: ***Python, C, Ethernet/Wireless Networking, PHP, JavaScript, HTML, CSS, LaTeX, Git, Java, C++, IDA Pro,*** *Debian Packages, Perl, SQL, Tcl, ARM/MIPS/x86 Assembly, GDB, OllyDbg, Matlab, SolidWorks*

Hardware Experience: Soldering, Multimeter, Oscilloscope, Logical Analyzer, *U-boot, Xilinx Tools, PICKit, DSTREAM, SATA, UART, JTAG, SPI, I²C, PCI, CAN*

PATENTS

SYSTEMS AND METHODS FOR SINGLE DEVICE AUTHENTICATION US Patent 10182040

- Ubiquitous authentication with smartphones using trusted execution environments.

OPEN SOURCE PROJECTS

Communication Assistive Technology over Ad-hoc Networks (CATAN) https://github.com/mit-ll/CATAN

- A low-cost, scalable system that creates a wide-area, best-effort, ad-hoc wireless network for disaster relief.

LL-Smartcard https://github.com/mit-ll/LL-Smartcard

- A Python module for interacting with smart cards.

LL-Fuzzer https://github.com/mit-ll/LL-Fuzzer

- An automated NFC fuzzing framework for Android devices.

LO-PHI https://github.com/mit-ll/LO-PHI

- A framework for low-level introspection and semantic gap reconstruction for both physical and virtual machines.

TEACHING / MENTORING

- Co-lead reading seminar on Secure Computer Architectures / UCSB (Winter Quarter 2019)
- Instructor for Master Robotics course (Grades 4-6) / TerrificScientifc (2017-2018) [*http://terrificscientific.org/*]
- Currently mentoring multiple undergraduate researchers / UCSB (2016-Present)
- Mentored 3 students with the U.S. Navy through the PIPELINES program / UCSB (2017) *[http://pipelines-csep.cnsi.ucsb.edu/]*
- Guest lecturer for CSC 6991 Topics in Computer Security / Wayne University (2016)
- Taught CS 16: Problem Solving with Computers / UCSB (Summer 2016) *[http://cs.ucsb.edu/~cspensky/cs16.html]*
- Mentored various interns at MIT-LL: two Ph.D. students and one Masters student / MIT-LL (2013,2014,2015)
- Mentored two high-school students in the building of a Turing machine / MIT-LL (2015) *[http://www.ll.mit.edu/news/]*
- Presented authentication concepts to K-12 children / MIT-LL (2014) *[https://www.ll.mit.edu/outreach/ScienceOnSaturday.html]*

RECOGNITIONS / POSITIONS

- IBM PhD Fellowship Award Recipient (2 year) / IBM (2018-2020) *[link]*
- Computer Science Department Treasurer / UCSB (2018-2019) *[http://www.cs.ucsb.edu/~greps/who-we-are/]*
- Featured in Pushing the Boundaries Graduate Division Publication / UCSB (2018) *[*link*]*
- Faculty Recruiting Committee Member / UCSB (2017-2018)
- Vice President of Academic Affairs (Graduate Student Association) / UCSB (2017-2018) *[http://www.gsa.ucsb.edu/]*
- Facebook Internet Defense Prize Finalist for DR. CHECKER at USENIX '17 / UCSB (2017) *[https://internetdefenseprize.org/]*
- Computer Science Graduate Student Distinguished Lecture Finalist / UCSB (2017) *[http://www.ucsb-cs-summit.com/]*
- Presented research at UCSB IT Summit / UCSB (2017)
- Semi-finalist in New Venture Competition / UCSB (2016) *[https://tmp.ucsb.edu/nvc/new-venture-competition]*
- Semi-finalist in Grad Slam Competition / UCSB (2016) *[http://www.gradpost.ucsb.edu/grad-slam/2016]*
- Computer Science Supplemental Stipend Recipient / UCSB (2015-2017)
- Work presented at International Conference of Crisis Mappers / MIT-LL (2014) *[Video]*
- Presenter at Cyber and Netcentric Workshop / MIT-LL (2013, 2014, 2015) *[https://conferences.ll.mit.edu/cnw/]*
- Technology Office Challenge Winner / MIT-LL (2014)
- Merit-based Bonus / MIT-LL (2013)
- President of Computer Science Students Association / UNC-CH (2010 - 2011) *[http://www.cs.unc.edu/~cssa/]*
- Graduate and Professional Student Federation Senator / UNC-CH (2010 - 2011) *[http://gpsf.unc.edu/]*
- Departmental Facilities and Web Committee Member / UNC-CH (2011) *[http://www.cs.unc.edu/Admin/Committees/]*
- Systems Tea Czar / UNC-CH (2010) *[http://www.cs.unc.edu/~jeffay/dirt/systea/]*
- Club Football / UNC-CH (2008-2011) *[http://campusrec.unc.edu/program/football/]*
- Dean's List Recipient / Pitt (7 of 8 semesters)
- Ham Radio Operator (Call sign: KC1CNW)