Shaanan N. Cohney PhD

shaanan@cohney.info, https://cohney.info , Updated 22 November, 2022

WORK

Lecturer (U.S. Assistant Professor equivalent) *2021-*
University of Melbourne

Postdoctoral Associate *2020*
Center for Information Technology Policy
Princeton University

Visiting Fellow *2020*
Center for Technology, Innovation, & Competition
Penn Law

Geller Fellow *2019*
Placement at Federal Trade Commission, Office of Policy Planning

Cybersecurity Fellow *2018*
U.S. Senator Ron Wyden

Security Engineer (Intern) *2014*
Facebook Inc.

EDUCATION

Graduate Certificate in University Education *Expected 2022*
University of Melbourne

PhD Computer and Information Science *2014 - 2020*
Pseudorandom Number Generator Standardization and Security
University of Pennsylvania

Master in Law *2017 - 2019*
University of Pennsylvania

Master of Science in Engineering *2014-2016*
Computer & Information Science
University of Pennsylvania

Bachelor of Science *2011-2014*
University of Melbourne
Study Abroad, University of Pennsylvania (DEAN'S LIST)

Diploma of Music *2011-2013*
Melbourne Conservatorium of Music
Classical Voice

ACADEMIC AWARDS

- Winner, Top Tech Trends, *State Government of Victoria Digital Innovation Festival*, 2022
- Nominee, Teacher of the Year, *Faculty of Engineering and Information Technology*, 2021, 2022
- Geller Fellow, *Wharton Public Policy Initiative, 2019*
- Pwnie Award, Best Cryptographic Attack, *Black Hat, 2016*
- Best Paper, *ACM Conference on Computer and Communications Security (CCS) 2016*
- Finalist, Facebook Internet Defense Prize, *USENIX Security, 2016*
- Dean's Award for Excellence in Tutoring, *University of Melbourne, 2014*
- Computer Science Research Prize, *University of Melbourne, 2013*

CONFERENCE PUBLICATIONS

1. Lianglu Pan, Shaanan Cohney, Toby Murray, Thuan Pham. *Detecting Excessive Data Exposures in Web Server Responses with Metamorphic Fuzzing.* IN SUBMISSION, 2022.
2. Shaanan Cohney, Mark Cheong. *COVID Down Under: where did Australia's pandemic apps go wrong?.* PREPRINT, IN SUBMISSION, 2022.
3. Ben Burgess, Avi Ginsberg, Edward W. Felten, Shaanan Cohney. *Watching the Watchers: Bias and vulnerability in remote proctoring software.* USENIX SECURITY SYMPOSIUM, 2022. **220K tweet impressions!**
4. Shaanan Cohney, Ross Teixeira, Anne Kohlbrenner, Mihir Kshirsagar, Yan Shvartzshnaider, Madeline Sanfilippo. *Virtual Classrooms and Real Harms.* SYMPOSIUM ON USABLE PRIVACY AND SECURITY, 2021. **Front Page NYTimes**
5. Shaanan Cohney, Andrew Kwong, Shachar Paz, Daniel Genkin, Nadia Heninger, Eyal Ronen, Yuval Yarom. *Pseudorandom Black Swans: Cache Attacks on CTR_DRBG.* IEEE SECURITY AND PRIVACY, 2020.
6. Shaanan Cohney, Nadia Heninger, Matthew D. Green. *Practical state recovery attacks against legacy RNG implementations.* ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY (CCS), 2018. (https://duhkattack.com)
7. Luke Valenta, David Adrian, Antonio Sanso, Shaanan Cohney, Joshua Fried, Marcella Hastings, J. Alex Halderman, Nadia Heninger. *Measuring small subgroup attacks against Diffie-Hellman.* THE NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM 2017.
8. Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Cohney, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla, Hovav Shacham. *A Systematic Analysis of the Juniper Dual EC Incident.* ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY (CCS), 2016. **Best Paper Award, IRTF Applied Networking Research Prize**
9. Nimrod Aviram, Sebastian Schinzel, Juraj Somorovsky, Nadia Heninger, Maik Dankel, Jens Steube, Luke Valenta, David Adrian, J. Alex Halderman, Viktor Dukhovni, Emilia Käsper, Shaanan Cohney, Susanne Engels, Christof Paar, and Yuval Shavitt. *DROWN: Breaking TLS using SSLv2..* 25TH USENIX SECURITY SYMPOSIUM, 2016. **Finalist Facebook Internet Defense Prize** (https://drownattack.com/)
10. Luke Valenta, Shaanan Cohney, Alex Liao, Joshua Fried, Satya Bodduluri, Nadia Heninger. *Factoring as a Service.* FINANCIAL CRYPTOGRAPHY 2016.

LAW REVIEW PUBLICATIONS

1. Shaanan Cohney, David A. Hoffman. *Transactional Scripts.* MINNESOTA LAW REVIEW, NOVEMBER 2020.
2. Shaanan Cohney, David A. Hoffman, Jeremy Sklaroff, David A. Wishnick. *Coin-Operated Capitalism.* COLUMBIA LAW REVIEW, APRIL 2019. **SSRN Top 10% Downloads Across All Listed Fields**

JOURNAL ARTICLES

Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Cohney, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla, Hovav Shacham. *Where did I leave my keys?: lessons from the Juniper Dual EC incident.* COMMUNICATIONS OF THE ACM, VOLUME 61 ISSUE 11, 2018.

REGULATORY FILINGS

1. Nia Brazzell, Jordan Bresinger, Shaanan Cohney, Sayash Kapoor, Mhir Kshirsagar, Jonathan Mayer, Arvind Narayanan. *Submission to ANPR R111004 Commercial Surveillance.* 2022.
2. Jeannie Paterson, Shaanan Cohney, Gabby Bush, Liam Harding, Alex Paterson. *Submission to the ACCC's Digital Platform Services Inquiry Discussion Paper.* 2022.
3. Jeannie Paterson, Shaanan Cohney, Lars Kulik, Liam Harding. *Response to the Review of the Privacy Act.* 2022.
4. Amit Achrekar, Atif Ahmad, Shanton Chang, Shaanan Cohney*, Suelette Dreyfus, Chris Leckie*, Toby Murray, Jeannie Paterson*, Thuan Pham, Liz Sonenberg. *Strengthening Australia's cybersecurity regulations and incentives, Response to the Department of Home Affairs Discussion Paper .* 2021 * LEAD DRAFTERS.
5. Marshini Chetty, Shaanan Cohney, Mihir Kshirsagar, Arunesh Mathur, Jonathan Mayer, Arvind Narayanan, Ross Teixeira, Ari Ezra Waldman. *Comments on Revised Proposed Regulations Implementing the California Consumer Privacy Act.* 2020.

PATENTS

- Toby Murray, Thuan Pham, Lianglu Pan, Shaanan Cohney. *SYSTEM AND METHOD FOR DETECTING EXCESSIVE DATA EXPOSURES.* AUSTRALIAN PROVISIONAL PATENT 2022903182. **2022**, *Equal Contributions*

OTHER WRITINGS

1. Simon Coghlan, Jeannie Patterson, Shaanan Cohney, Tim Miller. *Unis are using artificial intelligence to keep students sitting exams honest. But this creates its own problems.* THE CONVERSATION, 2021.
2. Shaanan Cohney, David A. Hoffman, Jeremy Sklaroff and David A. Wishnick. *The Problematic Role of Computer Code in Initial Coin Offerings.* CLS BLUE SKY: COLUMBIA LAW SCHOOL BLOG ON CORPORATIONS AND CAPITAL MARKETS, AUGUST 2018.

SERVICE

Internal Roles

- Lead, Programming Fundamentals Curriculum (University of Melbourne) 2022-

Program Chair

- Workshop on Attacks on Cryptography 2022
- Transactional Scripts and Legal Order, Workshop 2019

Program Committee

- Privacy Enhancing Technologies Symposium 2023
- IEEE Workshop on Technology and Consumer Protection 2021, 2022
- USENIX Security 2021 (Session Chair), 2022 (Session Chair), 2023
- Financial Cryptography 2020, 2021

External Reviewing

- The Hawaii International Conference on System Sciences (HICSS) 2022
- USENIX Security 2017-2020
- USENIX FOCI 2018
- IEEE Computer Architecture Letters 2018
- IEEE Symposium on Security and Privacy 2015-2016
- Financial Cryptography 2015-2016

Law Article Peer Review

- Article published in Stanford Journal of Blockchain Law and Policy 2021
- Article published in Kansas Law Review 2021

Strategic Workshops

- Privacy Enhancing Technology in the Public Interest (Boston University) 2022
- Bridging the Law-CS Gap (Georgetown/Boston University) 2020
- Reviving the OTA (Georgetown Law) 2018

Competition Judge
PennApps Hackathon 2014-2019

Book Proposal Reviewer
Manning Publications 2021

FUNDING

1. University of Melbourne Teaching and Learning Grant
   Automated Feedback Tools for CS, $20,000 AUD — 2022
2. Atomos Inc. Teaching Equipment $1,000 AUD — 2022
3. Blackmagic Design Teaching Equipment $3,000 AUD — 2021
4. Algorand Foundation RFF Grant, $400,000 AUD — 2021
5. "Enabling Internet-Scale Measurement of Digital Platform Competition",
   Early Career Grant, $39,494 AUD — 2021
6. Ripple Fund Research Grant, $10,000 USD — 2019
7. NSF Travel Award for Real World Crypto, $700 USD — 2019
8. Wharton Public Policy Institute Summer Fellowship (×2), $20,000 USD — 2018-2019

TEACHING

University of Melbourne

- Information Security and Privacy (INFO30006), *~200 students* — 2021S1, 2022S1
- Foundations of Algorithms (COMP10002), *~500 students* — 2021S2, 2022S2
- Graduate Cryptography (Guest Lectures) *~100 students* — 2014, 2016, 2022
- Computer Systems (Tutor) *~70 students* — 2014S1
- Foundations of Computing (Tutor) *~100 students per iteration* — 2013S2,2014S1
- Engineering Computation (Tutor) *~30 students* — 2013S2

Princeton University

- Scientists Against Time: History of Cryptography (Guest Lectures) — 2020, 2021, 2022

University of Pennsylvania

- Computer Security (Head TA) *~100 students per iteration* — 2015sf, 2016sf, 2017sf
- Guest Lectures on Hardware Security, Social Engineering — 2016
- Technology & Policy (Head TA) *~50 students* — 2016s
- Operating Systems (Head TA) *~150 students per iteration* — 2015f, 2016f
- Algorithms and Data Structures *~200 students* — 2013s

Graduate Associate
Riepe College House — 2015-2019

- Provided counseling and support services to over 150 students over four years
- Organized highly attended weekly activities, including academic review sessions and study breaks
- Led crisis management in situations ranging from psychological distress to fire/flooding

Education Officer, CTO
Hineni Youth and Welfare Australia (Volunteering) — 2008-2014

- Board member managing curriculum and teaching performance of counselors for youth 12-18

ADMINISTRATIVE ROLES

Lead, Programming Fundamentals Curriculum 2022-
Computing and Information Systems (Unimelb)

Comptroller
Philomathean Society Φ

- Oversaw audit and compliance for a $50k USD annual budget
- Handled legal and operational risk

Music Director Search Committee
University of Pennsylvania Glee Club

- Served on committee with University Staff and Alumni to hire new director
- Reviewed and edited position description and hiring materials

DOCTORAL ADVISING

- Faxing Wang, University of Melbourne, CIS 2022-
- Lianglu Pan, University of Melbourne, CIS 2021-
- Elisa Shioji, Melbourne Law School 2020-
- Ben Burgess, Princeton University (Project Supervision) 2020-2022
- Kartikeya Kandula, Princeton University (Project Supervision) 2020-

MASTERS ADVISING

- Joshua Fried, University of Pennsylvania (now PhD Student at MIT) 2016-2018

UNDERGRADUATE ADVISING

- Joseph Surin, University of Melbourne (now Security at elttam) 2022
- Lauren Leung, University of Pennsylvania (now Facebook) 2017
- Tom Yurek, University of Pennsylvania (now PhD at University of Illinois, Urbana-Champaign) 2017
- Joseph Cappadona, University of Pennsylvania 2017
- Henry Zhu, University of Pennsylvania (now PhD Student at UIUC) 2017
- Kevin Yim, University of Pennsylvania 2016
- Paul Lou, University of Pennsylvania (now PhD Student at UCLA) 2016
- Alex Liao, (now stealth startup) 2015

THESIS COMMITTEES

- Jaiden Fairoze (Masters, now PhD student at UC Berkeley) 2021

TALKS & PANELS

(excludes presentations accompanying publications at archival venues)

- *Investing in Vapor*, George Washington Univeristy 10/2022
- *Artifical Intelligence in Healthcare*, Melbourne Connect, Public Debate 6/2022
- *Hack Like The Movies*, Splendour in the Grass, Panel 7/2022
- *Exam Software Security*, American Association of Law Schools Annual Meeting, Panel 1/2022
- *Privacy in EdTech*, Federal Trade Commission 7/2021
- *Why public sector professionals need to be cybersecurity leaders*, Digital Government Festival, Panel 6/2022
- *The Exploit Bazzar*, Gandel-Besen House, Invited Public Talk 7/2021
- *On Psuedoranom Generators*, Harari Institute of Computing, BU 5/2021
- *Public Interest Technology Panel*, PIT-UN 3/2021
- *Privacy and Educational Technology*, Networking and Information Technology Research and Development (NITRD) 1/2021

- *Leaving Randomness To Chance*, Princeton Seminar 9/2020
- *Cache Attacks on CTR_DRBG*, Workshop on Attacks in Cryptography 8/2020
- *Side Channel Attacks on PRGs*, Real World Cryptography 1/2020
- *Technology Platforms for the Global Crypto-Economy (Panel)*, Columbia Business School 12/2019
- *Complexity Taxes & Blockchains*, Transactional Scripts & Legal Order 10/2019
- *Cryptographers and Congress*, Real World Cryptography 1/2019
- *Too Important to be Left to Chance*, University of Melbourne 12/2018
- *Coin Operated Capitalism*, Penn Law Board of Overseers 11/2018
- *Cryptocurrencies & the Law*, University of Pennsylvania School of Arts & Sciences 10/2018
- *Practical state recovery attacks against legacy RNG implementations*, Kangacrypt 12/2018
- *Security of a Different Sort: Social Engineering*, PennApps Keynote 8/2017
- *A Tour of Cryptographic Backdoors*, University of Melbourne (https://cohney.info/backdoors) 7/2017
- *Real World Impacts of Cryptography Policy*, University of Melbourne 7/2016
- *Introduction to Cryptography*, Theoretical Research in Computer Science Seminar, University of Melbourne 2014

COMMON VULNERABILITIES AND EXPOSURES (CVEs)

CVEs are identifiers assigned by the U.S. government to identify security vulnerabilities. I jointly discovered the following:

- CVE-2019-15703 - CTR_DRBG Flaw
- CVE-2016-8492, CVE-2017-14187 - DUHK Attack
- CVE-2016-0701 - Small Subgroup Attacks
- CVE-2016-0800 - General DROWN Attack
- CVE-2015-3197, CVE-2016-0703 - Special DROWN Attack

SELECTED MEDIA COVERAGE & MENTIONS

"Fun run facial recognition prompts concern" *Australian Associated Press* 8/2022
"Spyware Sales Explosion Powers Attacks" *Australian Associated Press* 8/2022
"Been Getting *Those* Sugar Daddy DMs On Insta? Here's How To Spot A Scammer From A Mile Away", *ELLE Magazine* 6/2022
"Fake Check-Ins And False Vaccine Certificates Are On The Rise In Australia", *Junkee* 08/2021
"Victoria's QR codes badly made, developers say", *The Age, Top Story* 6/2021
Appearance: Interview on Privacy of Apple Devices, *ABC National News* 5/2021
"Online Cheating Charges Upend Dartmouth Medical School" *NYTimes Front Page, Quoted* 5/2021
"Universities urged to review remote learning software", *Port Swigger* 12/2020
"Cryptocoin computer code fails on promoter claims", *Financial Times* 6/2019
"New Research Finds Backdoor 'Centralized Control' in many ICOs", *Bitcoinist* 7/2018
"Most ICOs Retain Centralized Control, Break Whitepaper Promises, Academic Report Shows" *Coin Telegraph* 7/2018
"Holy DUHK! Boffins name bug that could crack crypto wide open", *The Register* 10/2017
"DUHK Crypto Attack Recovers Encryption Keys, Exposes VPN Connections, More", *Bleeping Computer* 10/2017
"PRNG Weakness Reflects Poorly on Government Crypto Certification", *Security Boulevard* 10/2017
"Thousands of popular sites at risk of Drown hack attacks", *BBC News* 3/2016
"Drown attack: How weakened encryption jeopardizes 'secure' sites", *The Guardian* 3/2016
"Juniper promises to fix ScreenOS cryptography … eventually", *Info World* 1/2016
"Breaking 512-bit RSA with Amazon EC2 is a cinch. So why all the weak keys?", *Ars Technica* 10/2015

MISC

Bruce Montgomery Prize, Lifetime Service, *University of Pennsylvania Glee Club, 2019*
ROSETTE Award for Unusual Service and Dedication, *University of Pennsylvania Glee Club, 2018*
U.S. Permanent Resident (EB-2 with National Interest Waiver)

REFERENCES

Matt Blaze
McDevitt Professor of Computer Science and Law
Georgetown University
mab497@georgetown.edu

Jonathan Mayer
Assistant Professor
Center for IT Policy
Princeton University
jonathan.mayer@princeton.edu

Nadia Heninger
Associate Professor
University of San Diego
nadiah@cs.ucsd.edu

Matthew D. Green
Associate Professor
Johns Hopkins University
mgreen@cs.jhu.edu

David A. Hoffman
William A. Schnader Professor of Law, Deputy Dean
Universiy of Pennsylvania Carey Law School
dhoffman@law.upenn.edu