Shaanan N. Cohney

shaanan@cohney.info, `https://cohney.info` , Updated 8 November 2018

RESEARCH INTERESTS

My current research spans applied cryptography and security as realized through design, implementation, and deployment of computer systems.

I primarily focus on improving the security of cryptographic systems through analysis of protocol standards, reverse-engineering of implementations, systems-building, and measurement of hosts on the public Internet.

My secondary research area is the impact of advances in cryptography and cyber security technologies on related areas of law, such as contract doctrine and corporate governance.

EDUCATION & WORK

PhD Computer and Information Science *2014 - (Expected 2019)*
Pseudorandom Number Generator Standardization and Security
University of Pennsylvania, Supervised by Nadia Heninger and Jonathan M. Smith

Master in Law *2017 - (Expected 2019)*
University of Pennsylvania

Cybersecurity Fellow *2018*
Senator Ron Wyden

- Drafted legislation, policy documents and advised on security concerns
- Met with stakeholders to address concerns and opportunities
- Composed press releases, issue summaries and talking points

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

Security Engineer (Intern) *2014*
Facebook Inc.

- Improved data deletion system, reducing missed data by over 90%
- Developed new internal security tooling

Bachelor of Science *2010-2014*
University of Melbourne
Computer Science (1st Class Honours)
Physics (2nd Class Honours, Div. A)
Study Abroad (Dean's List)

Diploma of Music *2010-2013*
Melbourne Conservatorium of Music
Classical Voice

AWARDS

- 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*

REFEREED PUBLICATIONS

1. Shaanan Cohney, David A. Hoffman, Jeremy Sklaroff , David A. Wishnick. *Forthcoming, Columbia Law Review, May 2019.* Coin-Operated Capitalism. SSRN Top 10% Downloads Across All Listed Fields

2. Shaanan Cohney, Nadia Heninger, Matthew D. Green. Practical state recovery attacks against legacy RNG implementations. *In ACM Conference on Computer and Communications Security (CCS), 2018* (`https://duhkattack.com`)
3. Luke Valenta, David Adrian, Antonio Sanso, Shaanan Cohney, Joshua Fried, Marcella Hastings, J. Alex Halderman, Nadia Heninger. Measuring small subgroup attacks against Diffie-Hellman. *In The Network and Distributed System Security Symposium 2017.*
4. 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. *In ACM Conference on Computer and Communications Security (CCS), 2016.* Best Paper Award, Irtf Applied Networking Research Prize
5. 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. *In 25th USENIX Security Symposium, 2016.* (`https://drownattack.com/`) Finalist Facebook Internet Defense Prize
6. Luke Valenta, Shaanan Cohney, Alex Liao, Joshua Fried, Satya Bodduluri, Nadia Heninger. Factoring as a Service. *In Financial Cryptography 2016.* (`https://seclab.upenn.edu/projects/faas/`)

INVITED PUBLICATIONS

1. Shaanan Cohney, David A. Hoffman, Jeremy Sklaroff and David A. Wishnick .The Problematic Role of Computer Code in Initial Coin Offerings *In CLS Blue Sky: Columbia Law School Blog on Corporations and Capital Markets, August 2018*
2. 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. *In Communications of the ACM, Volume 61 Issue 11, 2018*

SERVICE

External Reviewing

- IEEE Symposium on Security and Privacy 2015, 2016
- Financial Cryptography 2016
- IEEE Computer Architecture Letters 2018
- USENIX FOCI 2018

Competition Judge
PennApps Hackathon 2014-2017

ADMINISTRATIVE EXPERIENCE

Chief Risk Management Officer
Philomathean Society

- Performed financial oversight duties for a $50k annual budget
- Handled compliance and legal risk for society operations

Music Director Search Committee
University of Pennsylvania Glee Club

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

INVITED TALKS

- *Security of a Different Sort: Social Engineering*, PennApps Invited Talk, 8/2017
- *A Tour of Cryptographic Backdoors*, University of Melbourne (`https://cohney.info/backdoors`) 7/2017
- *Minds and Machines*, Philomathean Society 8/2016
- *Real World Impacts of Cryptography Policy*, University of Melbourne 7/2016

TEACHING

University of Pennsylvania

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

University of Melbourne

- Graduate Cryptography (Guest Lecturer) *∼100 students* 7/2014
- Computer Systems (Tutor, Workshop) *∼70 students* 2014
- Foundations of Computing (Tutor, Two Workshops) *∼100 students per iteration* 2013,2014
- Engineering Computation (Tutor, Workshop) *∼30 students* 2013

Graduate Associate
Riepe College House 2015-2018

- Provided counseling and support services to over 100 students
- 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, Head IT Services
Hineni Youth and Welfare Australia (Volunteering) 2008-2014

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

UNDERGRADUATE ADVISING

- Joshua Fried (now PhD Student at MIT)
- Lauren Leung (now Facebook)
- Tom Yurek (now PhD Student at University of Illinois, Urbana-Champaign)
- Joseph Cappadona
- Kevin Yim
- Henry Zhu
- Paul Lou
- Alex Liao

COMMON VULNERABILITIES AND EXPOSURES

Common Vulnerabilities and Exposures (CVEs) are identifiers assigned by a US Government agency to identify security vulnerabilities. I jointly discovered the following:

- 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

"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

OTHER ACTIVITIES

- Secretary, Melbourne University Physics Student Society 2012
- Secretary, Melbourne University Jewish Student Society 2013
- Librarian, Philomathean Society Φ 2017
- Longest serving member, Penn Glee Club 2012-2018

MISC

Australian Citizen
Penn Glee Club *Rosette* Award for Unusual Service and Dedication