

EDUCATION & WORK

- PhD Computer and Information Science** 2014 - (Expected 2019)
 Computer and Information Security
 University of Pennsylvania, Supervised by Nadia Heninger and Jonathan M. Smith
- Cybersecurity Fellow** Summer 2018
 Senator Ron Wyden
- Master in Law** 2017 - (Expected 2019)
 University of Pennsylvania
- Master of Science in Engineering** 2014-2016
 Computer & Information Science
 University of Pennsylvania
- Intern Security Engineer** 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 (Deans List)
- Diploma of Music** 2010-2014
 Melbourne Conservatorium of Music
 Classical Voice

AWARDS

- 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

SERVICE

- External Reviewing
- IEEE Symposium on Security and Privacy 2015
 - Financial Cryptography 2016
 - IEEE Symposium on Security and Privacy 2016
 - 25th USENIX Security Symposium 2016
 - IEEE Computer Architecture Letters 2018
 - USENIX FOCI 2018

TEACHING

- University of Pennsylvania
- Guest Lecturer on Hardware Security 2016
 - Technology & Policy (Head TA) 2016
 - Operating Systems (Head TA) 2015, 2016
 - Computer Security (Head TA) 2015, 2016, 2017

• Algorithms and Data Structures	2013
University of Melbourne	
• Introduction to Quantum Cryptography, Guest Lecturer, Graduate Cryptography	July 2014
• Computer Systems (TA)	2014
• Foundations of Computing (TA)	2014
• Theoretical Research in Computer Science Presenter - Cryptography	2014
• Engineering Computation (TA)	2013
Graduate Associate Riepe College House	2015-2017
• Provided counseling and support services to over 70 freshmen	
• Organized highly attended weekly activities, including academic review sessions and study breaks	
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.	

SELECTED MEDIA COVERAGE

“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

REFEREED PUBLICATIONS

1. **Coin-Operated Capitalism** Shaanan Cohn, David A. Hoffman, Jeremy Sklaroff , David A. Wishnick. In Columbia Law Review, May 2019
2. **Practical state recovery attacks against legacy RNG implementations** Shaanan Cohn, Nadia Heninger, Matthew D. Green. In ACM Conference on Computer and Communications Security (CCS), 2018 (<https://duhkattack.com>)
3. **Measuring small subgroup attacks against Diffie-Hellman** Luke Valenta, David Adrian, Antonio Sanso, Shaanan Cohn, Joshua Fried, Marcella Hastings, J. Alex Halderman, Nadia Heninger. In The Network and Distributed System Security Symposium 2017.
4. **A Systematic Analysis of the Juniper Dual EC Incident** Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Cohn, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla, Hovav Shacham. In ACM Conference on Computer and Communications Security (CCS), 2016. **BEST PAPER AWARD**
IRTF APPLIED NETWORKING RESEARCH PRIZE
5. **DROWN: Breaking TLS using SSLv2** Nimrod Aviram, Sebastian Schinzel, Juraj Somorovsky, Nadia Heninger, Maik Dankel, Jens Steube, Luke Valenta, David Adrian, J. Alex Halderman, Viktor Dukhovni, Emilia Käsper, Shaanan Cohn, Susanne Engels, Christof Paar, and Yuval Shavitt. In 25th USENIX Security Symposium, 2016. (<https://drownattack.com/>)
FINALIST FACEBOOK INTERNET DEFENSE PRIZE
6. **Factoring as a Service** Luke Valenta, Shaanan Cohn, Alex Liao, Joshua Fried, Satya Bodduluri, Nadia Heninger. In Financial Cryptography 2016. (<https://seclab.upenn.edu/projects/faas/>)

COMMON VULNERABILITY EXPOSURES - CVE

Common Vulnerability Exposures are identifiers for the US Government maintained list of public security vulnerabilities. I was involved in the discovery of 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