LUKE T. VALENTA

CONTACT INFORMATION

luke.valenta@gmail.com (704) 207-5358
http://lukevalenta.com Philadelphia, PA

EDUCATION

Ph.D. Computer Science, **University of Pennsylvania**, advised by Nadia Heninger — Sep 2014 - present
M.S. computer science, **University of Pennsylvania**, GPA 3.93 — Sep 2014 - May 2016
B.S. computer science, B.S. mathematics, **University of Maryland**, GPA 4.0 — Sep 2011 - May 2014
Double major physics and mathematics, **Frostburg State University**, G.P.A 4.0 — Sep 2009 - May 2011

RESEARCH INTERESTS

Computer Security, Privacy, Applied Cryptography, Elliptic Curve Cryptography, Distributed Systems

INDUSTRY EXPERIENCE

Ph.D. Intern, Advanced Security Research Group, Cisco Systems — Jun 2017 - Aug 2017

HONORS AND AWARDS

Facebook Internet Defense Prize Finalist — Oct 2016
Pwnie Award - Best Cryptographic Attack, Black Hat — Aug 2016
Best Paper Award, ACM CCS — Oct 2015
Pwnie Award - Most Innovative Research, Black Hat — Aug 2015
Philip Merrill Presidential Scholar — Sep 2013
John D. Gannon Scholarship — Sep 2013
University of Maryland Computer Science Departmental Honors — Sep 2012 - May 2013
Jeffrey C. and Sandra W. Huskamp Computer Science Scholarship — Sep 2012
Honor Society of Phi Kappa Phi, College Park Chapter — Sep 2012
Kappa Mu Epsilon Mathematics Honor Society — Sep 2010
Dean's List at University of Maryland — Sep 2011 - May 2014
Dean's List at Frostburg State University — Sep 2009 - May 2011

PUBLICATIONS

- May the Fourth Be With You: A Microarchitectural Side Channel Attack on Several Real-World Applications of Curve25519. Daniel Genkin, Luke Valenta, Yuval Yarom. *2017 ACM Conference on Computer and Communications Security (CCS, 2017).*
- Post-quantum RSA. Daniel J. Bernstein, Nadia Heninger, Paul Lou, Luke Valenta. *Post-Quantum Cryptography 2017 (PQCrypto 2017).*
- Measuring small subgroup attacks against Diffie-Hellman. Luke Valenta, David Adrian, Antonio Sanso, Shaanan Cohney, Joshua Fried, Marcella Hastings, J. Alex Halderman, Nadia Heninger. *Network and Distributed Systems Symposium 2017 (NDSS 2017).*
- 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 Cohney, Susanne Engels, Christof Paar, Yuval Shavitt. *25th USENIX Security Symposium (USENIX Security 2016).*
- Factoring as a Service. Luke Valenta, Shaanan Cohney, Joshua Fried, Satya Boddulari, Nadia Heninger. *Financial Cryptography and Data Security 2016 (FC 2016)*
- Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann. *2015 ACM Conference on Computer and Communications Security (CCS, 2015).* **Best paper award**.
- Alibi Routing. Dave Levin, Youndo Lee, Luke Valenta, Zhihao Li, Victoria Lai, Cristian Lumezanu, Neil Spring, Bobby Bhattacharjee. *ACM SIGCOMM Computer Communication Review. Vol. 45. No. 4. ACM, 2015. (SIGCOMM 2015).*
- Blindcoin: Blinded, Accountable Mixes for Bitcoin. Luke Valenta, Brendan Rowan. *Proceedings of the 2nd Workshop on Bitcoin Research, in Association with Financial Cryptography and Data Security 2015. (BITCOIN 2015).*

TEACHING EXPERIENCE

CIS551: Computer and Network Security, University of Pennsylvania, TA — Sep 2017
CIS551: Computer and Network Security, University of Pennsylvania, TA — Sep 2016
CIS331: Computer Security, University of Pennsylvania, TA — May 2016
CIS556: Cryptography, University of Pennsylvania, TA — Sep 2015
CMSC216: Introduction to Computer Systems, University of Maryland, TA — Sep 2013
MATH237: Calculus II, Frostburg State University, Tutor — Sep 2010 - May 2011
MATH236: Calculus I, Frostburg State University, Tutor — Sep 2010 - May 2011

TALKS

Measuring small subgroup attacks against Diffie-Hellman
Network and Distributed Systems Symposium — Feb 2017
Factoring as a Service
Boston University Security Group — Nov 2016
Financial Cryptography — Feb 2016
How Bitcoin Works
Net Tuesday Philly Meetup — Mar 2015

SERVICES

Program committees
Workshop on Bitcoin and Blockchain Research, program committee — Jan 2017
Privacy Enhancing Technologies, external reviewer — Jan 2017
Student government
Graduate Student Engineering Group, University of Pennsylvania, president — May 2016 - May 2017
Graduate Student Engineering Group, University of Pennsylvania, vice president — May 2015 - May 2016
Miscellaneous
Security Reading Group, Univeristy of Pennsylvania, organizer — Sep 2014 - present

TECHNICAL SKILLS

Languages: Go, Python, C, C++, Java, Ruby, MatLab, OCaml, LaTex, HTML
Operating Systems: UNIX, Linux, Android

RELATED COURSEWORK

Computer Networks, Algorithms, Programming Handheld Devices, Network Security, Programming Languages, Cryptography, Computer Architecture, Discrete Structures, Computer Systems, Object Oriented Programming, Machine Learning

ACTIVITIES

Mr. and Mrs. Penn Bodybuilding Competition, participant — Nov 2014, Nov 2016
UMD Gymkana Troupe (gymnastics), member — Sep 2011 - May 2014
PennApps Hackathon, participant — Sep 2013
ACM Mid-Atlantic Regional Programming Contest, placed ninth — Nov 2012
UMD Mobile Applications Developers Club, member — Sep 2012 - May 2014