Thomas Ristenpart

Updated February 20, 2018

Associate Professor
Cornell Tech
111 Eighth Avenue #302, New York, NY 10011
email: ristenpart@cornell.edu
cell: 858-405-1740

Academic Background

University of California, San Diego. Ph.D. in Computer Science, November 2010.
Advisor: Prof. Mihir Bellare

University of California, Davis. M.S. in Computer Science, June 2005.
Advisor: Prof. Matt Bishop

University of California, Davis. B.S. in Computer Science and Engineering, June 2003.

Work History

Associate Professor (tenure track)
Cornell Tech & Department of Computer Science, Cornell University
May 2015 – present

Assistant Professor (tenure track)
Department of Computer Sciences, University of Wisconsin
January 2011 – May 2015

Visiting researcher

Microsoft Research	University of Lugano	University of Washington
June 2011	April 2008 – June 2008	June 2007 – September 2007

Graduate student researcher

UC San Diego	UC Davis
September 2005 – December 2010	July 2003 – June 2005

Software engineering intern

Center for Computing Sciences	Microsoft	Micron Technologies, Inc.
Summer 2004	Summers 2001, 2002	Summers 1999, 2000

Research Interests

Computer security: security of systems under attack; applied cryptography; privacy; cloud computing security; embedded systems security; machine learning security

Cryptography: provable security; cryptographic hash functions; encryption; key exchange; signatures; PKI; message authentication; foundations of cryptography

Awards

- Best Paper Award at ACM CHI 2018 for paper [70]
- Distinguished Student Paper Award at IEEE Symposium on Security and Privacy 2016 for paper [52]
- Sloan Foundation Research Fellow 2015
- Best Paper at USENIX Security 2014 for paper [37]
- Runner up for Award for Outstanding Research in Privacy Enhancing Technologies 2014 and New Digital Age grant from Google Executive Chairman Eric Schmidt for paper [32]
- NSF CAREER Award 2013
- Computer Science and Engineering Department Dissertation Award, University of California, San Diego, 2011
- Before graduate school: UC Regents Scholarship (2001-2003), Albert W. Bijou Scholarship (2000), Edward Frank Kraft Prize (2000), UC Davis College of Engineering Annual Fund Scholarship (2000), San Francisco Bay Area Engineering Council Scholarship (1999), Wakeman Scholarship from the UC Regents (1999), UC Davis Alumni Association Leadership Scholarship (1999)

Publications

[1] M. Bellare and T. Ristenpart. Multi-Property-Preserving Hash Domain Extension and the EMD Transform. *Advances in Cryptology – Asiacrypt*, LNCS vol. 4284, pp. 299–314. Springer, 2006

[2] F. Hsu, H. Chen, T. Ristenpart, J. Li, and Z. Su. Back to the Future: A Framework for Automatic Malware Removal and System Repair. *Annual Computer Security Applications Conference – ACSAC*, pp. 257–268. IEEE Computer Society, 2006

[3] T. Ristenpart and P. Rogaway. How to Enrich the Message Space of a Cipher. *Fast Software Encryption – FSE*, LNCS vol. 4593, pp. 101–118. Springer, 2007 [Retracted February, 2015]

[4] T. Ristenpart and S. Yilek. The Power of Proofs-of-Possession: Securing Multiparty Signatures against Rogue-Key Attacks. *Advances in Cryptology – Eurocrypt*, LNCS vol. 4515, pp. 228–245. Springer, 2007

[5] M. Bellare and T. Ristenpart. Hash Functions in the Dedicated-Key Setting: Design Choices and MPP Transforms. *International Colloquium on Automata, Languages and Programming – ICALP*, LNCS vol. 4596, pp. 399–410. Springer, 2007

[6] T. Ristenpart and T. Shrimpton. How to Build a Hash Function from Any Collision-Resistant Function. *Advances in Cryptology – Asiacrypt*, LNCS vol. 4833, pp. 147–163. Springer, 2007

[7] T. Ristenpart, G. Maganis, A. Krishnamurthy, and T. Kohno. Privacy-Preserving Location Tracking of Lost or Stolen Devices: Cryptographic Techniques and Replacing Trusted Third Parties with DHTs. *USENIX Security Symposium*, 2008

[8] M. Bellare, M. Fischlin, A. O'Neill, and T. Ristenpart. Deterministic Encryption: Definitional Equivalences and Constructions without Random Oracles. *Advances in Cryptology – Crypto*, LNCS vol. 5157, pp. 360–378. Springer, 2008

[9] Y. Dodis, T. Ristenpart, and T. Shrimpton. Salvaging Merkle-Damgård for Practical Applications. *Advances in Cryptology – Eurocrypt*, LNCS vol. 5479, pp. 371–388. Springer, 2009

[10] M. Bellare and T. Ristenpart. Simulation without the Artificial Abort: Simplified Proof and Improved Concrete Security for Waters' IBE Scheme. *Advances in Cryptology – Eurocrypt*, LNCS vol. 5479, pp. 407–424. Springer, 2009

[11] M. Bellare, T. Ristenpart, P. Rogaway, and T. Stegers. Format-Preserving Encryption. *Selected Areas in Cryptography – SAC*, LNCS vol. 5867, pp. 295–312. Springer, 2009

[12] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage. Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-party Compute Clouds. *ACM Computer and Communications Security – CCS*, pp. 199–212, 2009

[13] M. Bellare, Z. Brakerski, M. Naor, T. Ristenpart, G. Segev, H. Shacham, and S. Yilek. Hedged Public-key Encryption: How to Protect against Bad Randomness. *Advances in Cryptology – Asiacrypt*, LNCS vol. 5912, pp. 232–249. Springer, 2009

[14] T. Ristenpart and S. Yilek. When Good Randomness Goes Bad: Virtual Machine Reset Vulnerabilities and Hedging Deployed Cryptography. *Network and Distributed Systems Security – NDSS*, 2010

[15] M. Fischlin, A. Lehmann, T. Ristenpart, T. Shrimpton, M. Stam, and S. Tessaro. Random Oracles with(out) Programmability. *Advances in Cryptology – Asiacrypt*, LNCS vol. 6477, pp. 303–320, Springer, 2010

[16] T. Ristenpart, H. Shacham, and T. Shrimpton. Careful with Composition: Limitations of the Indifferentiability Framework. *Advances in Cryptology – Eurocrypt*, LNCS vol. 6632, pp. 487–506, Springer, 2011

[17] Q. Zhang, T. Ristenpart, S. Savage, and G. Voelker. Got Traffic? An Evaluation of Click Traffic Providers *WICOM/AIRWeb Workshop on Web Quality – WebQuality*, 2011.

[18] K. Paterson, T. Ristenpart, and T. Shrimpton. Tag Size Does Matter: Attacks and Proofs for the TLS Record Protocol. *Advances in Cryptology – Asiacrypt*, LNCS vol. 7073, pp. 372–389, Springer, 2011

[19] Y. Dodis, T. Ristenpart, and S. Vadhan. Randomness Condensers for Efficiently Samplable, Seed-Dependent Sources. *Theory of Cryptography Conference – TCC*, LNCS vol. 7194, pp. 618–635, Springer, 2012

[20] K. Dyer, S. Coull, T. Ristenpart, and T. Shrimpton. Peek-a-Boo, I Still See You: Why Efficient Traffic Analysis Countermeasures Fail. *Symposium on Security and Privacy – Oakland*, IEEE, pp. 332–346, 2012

[21] W. Frisbee, B. Moench, B. Recht, and T. Ristenpart. Security Analysis of Smartphone Point-of-Sale Devices. *Workshop On Offensive Technologies – WOOT*, USENIX, 2012

[22] Y. Dodis, T. Ristenpart, J. Steinberger, and S. Tessaro. To Hash or Not to Hash Again? (In)Differentiability Results for H^2 and HMAC. *Advances in Cryptology – Crypto*, LNCS vol. 7417, pp. 348–366, Springer, 2012

[23] M. Bellare, T. Ristenpart, and S. Tessaro. Multi-instance Security and Its Application to Password-based Cryptography. *Advances in Cryptology – Crypto*, LNCS vol. 7417, pp. 312–329, Springer, 2012

[24] V. Varadarajan, T. Kooburat, B. Farley, T. Ristenpart, and M. Swift. Resource-freeing Attacks: Improve Your Cloud Performance (at Your Neighbor's Expense). *ACM Computer and Communications Security – CCS*, 2012

[25] Y. Zhang, A. Juels, M. Reiter, and T. Ristenpart. Cross-VM Side Channels and Their Use to Extract Private Keys. *ACM Computer and Communications Security – CCS*, 2012

[26] B. Farley, V. Varadarajan, K. Bowers, A. Juels, T. Ristenpart, and M. Swift. More for Your Money: Exploiting Performance Heterogeneity in Public Clouds. *ACM Symposium on Cloud Computing – SOCC*, 2012

[27] M. Bellare, S. Keelveedhi, and T. Ristenpart. Message-locked Encryption and Secure Deduplication. *Advances in Cryptology – Eurocrypt*, 2013

[28] D. Davidson, B. Moench, S. Jha, and T. Ristenpart. FiE on Firmware: Finding Vulnerabilities in Embedded Firmware with Symbolic Execution. *USENIX Security Symposium*, 2013

[29] M. Bellare, S. Keelveedhi, and T. Ristenpart. DupLESS: Server-aided Encryption for Deduplicated Storage. *USENIX Security Symposium*, 2013

[30] T. Ristenpart and S. Yilek. The Mix-and-Cut Shuffle: Small-domain Encryption Secure against N Queries. *Advances in Cryptology – Crypto*, 2013

[31] K. He, A. Fisher, L. Wang, A. Gembler, A. Akella, and T. Ristenpart. Next Stop, the Cloud: Understanding Modern Web Service Deployment in EC2 and Azure. *ACM Internet Measurement Conference – IMC*, 2013

[32] K. Dyer, S. Coull, T. Ristenpart, and T. Shrimpton. Protocol Misidentification Made Easy with Format-Transforming Encryption. *ACM Computer and Communications Security – CCS*, 2013

[33] A. Juels and T. Ristenpart. Honey Encryption: Security Beyond the Brute-force Bound. *Advances in Cryptology – Eurocrypt*, 2014

[34] A. Everspaugh, Y. Zhai, R. Jellinek, T. Ristenpart, and M. Swift. Not-So-Random Numbers in Virtualized Linux and the Whirlwind RNG. *IEEE Symposium on Security and Privacy – Oakland*, 2014

[35] R. Jellinek, Y. Zhai, T. Ristenpart, and M. Swift. A Day Late and a Dollar Short: The Case for Research on Cloud Billing Systems. HotCloud 2014

[36] S. Checkoway, M. Fredrikson, R. Niederhagen, A. Everspaugh, M. Green, T. Lange, T. Ristenpart, D. Bernstein, J. Maskiewicz, and H. Shacham. On the Practical Exploitability of Dual EC in TLS Implementations. *USENIX Security Symposium*, 2014

[37] M. Fredrikson, E. Lantz, S. Jha, S. Lin, D. Page, and T. Ristenpart. Privacy in Pharmacogenetics: An End-to-End Case Study of Personalized Warfarin Dosing. *USENIX Security Symposium*, 2014

[38] D. Luchaup, K. Dyer, S. Jha, T. Ristenpart, and T. Shrimpton. LibFTE: A Toolkit for Constructing Practical Format-Abiding Encryption Schemes. *USENIX Security Symposium*, 2014

[39] V. Varadarajan, T. Ristenpart, and M. Swift. Scheduler-based Defenses against Cross-VM Side-channels. *USENIX Security Symposium*, 2014

[40] L. Wang, A. Nappa, J. Caballero, T. Ristenpart, and A. Akella. WhoWas: A Platform for Measuring Web Deployments on IaaS Clouds. *ACM Internet Measurement Conference – IMC*, 2014

[41] D. Luchaup, T. Shrimpton, T. Ristenpart, S. Jha. Formatted Encryption Beyond Regular Languages. *ACM Computer and Communications Security – CCS*, 2014

[42] Y. Zhang, A. Juels, M. Reiter, and T. Ristenpart. Cross-tenant Side-channel Attacks in PaaS Clouds. *ACM Computer and Communications Security – CCS*, 2014

[43] Bruce Schneier, Matthew Fredrikson, Tadayoshi Kohno, and Thomas Ristenpart. Surreptitiously Weakening Cryptographic Systems. Non-peer-reviewed survey article, 2015

[44] Y. Dodis, C. Ganesh, A. Golovnev, A. Juels, and T. Ristenpart. A Formal Treatment of Backdoored Pseudorandom Generators. *Advances in Cryptology – Eurocrypt*, 2015

[45] R. Chatterjee, J. Bonneau, A. Juels, T. Ristenpart. Cracking-Resistant Password Vaults using Natural Language Encoders. *IEEE Symposium on Security and Privacy – Oakland*, 2015

[46] V. Varadarajan, Y. Zhang, T. Ristenpart, and M. Swift. A Placement Vulnerability Study in Multi-tenant Public Clouds. *USENIX Security Symposium*, 2015

[47] Adam Everspaugh, Rahul Chatterjee, Sam Scott, Ari Juels, and Thomas Ristenpart. The Pythia PRF Service. *USENIX Security Symposium*, 2015

[48] Liang Wang, Kevin Dyer, Aditya Akella, Thomas Ristenpart, and Thomas Shrimpton. Seeing through Network Protocol Obfuscation. *ACM Computer and Communications Security – CCS*, 2015

[49] Matthew Fredrikson, Somesh Jha, and Thomas Ristenpart. Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures. *ACM Computer and Communications Security – CCS*, 2015

[50] David Cash, Paul Grubbs, Jason Perry, and Thomas Ristenpart. Leakage-abuse Attacks against Searchable Encryption. *ACM Computer and Communications Security – CCS*, 2015

[51] Joseph Jaeger, Thomas Ristenpart, and Qiang Tang. Honey Encryption Security Beyond Message Recovery. *Advances in Cryptology – Eurocrypt*, 2016

[52] Rahul Chatterjee, Anish Athayle, Devdatta Akhawe, Ari Juels, and Thomas Ristenpart. pASSWORD tYPOS and How to Correct Them Securely. *IEEE Symposium on Security and Privacy – Oakland*, 2016

[53] Drew Davidson, Hao Wu, Rob Jellinek, Vikas Singh, and Thomas Ristenpart. Controlling UAVs with Sensor Input Spoofing Attacks. *Workshop on Offensive Technologies – WOOT*, 2016

[54] Florian Tramer, Fan Zhang, Ari Juels, Michael Reiter, and Thomas Ristenpart. Stealing Machine Learning Models via Prediction APIs. *USENIX Security Symposium*, 2016

[55] Yan Zhai, Lichao Yin, Jeffrey Chase, Thomas Ristenpart, and Michael Swift. CQSTR: Securing Cross-tenant Applications with Cloud Containers *ACM Symposium on Cloud Computing – SOCC*, 2016

[56] Paul Grubbs, Richard McPherson, Muhammad Naveed, Thomas Ristenpart, and Vitaly Shmatikov. Breaking web applications built on top of encrypted data. *ACM Computer and Communications Security – CCS*, 2016

[57] Lucas Dixon, Thomas Ristenpart, and Thomas Shrimpton. Network Protocol Obfuscation and Automated Internet Censorship. *IEEE Security and Privacy Magazine*, 2016

[58] Ivan Pustogarov, Thomas Ristenpart, and Vitaly Shmatikov. Using Program Analysis to Synthesize Sensor Spoofing Attacks. *Asia CCS*, 2017

[59] Paul Grubbs, Thomas Ristenpart, and Yuval Yarom. Modifying an Enciphering Scheme After Deployment. *Advances in Cryptology – Eurocrypt*, 2017

[60] Liang Wang, Paul Grubbs, Jiahui Lu, Vincent Bindschaedler, David Cash, and Thomas Ristenpart. Side-Channel Attacks on Shared Search Indexes *IEEE Symposium on Security and Privacy – Oakland*, 2017

[61] Paul Grubbs, Kevin Sekniqi, Vincent Bindschaedler, Muhammad Naveed, and Thomas Ristenpart. Leakage-Abuse Attacks against Order-Revealing Encryption. *IEEE Symposium on Security and Privacy – Oakland*, 2017

[62] Paul Grubbs, Thomas Ristenpart, and Vitaly Shmatikov. Why Your Encrypted Database Is Not Secure. *HotOS* 2017

[63] Jay Aikat, Aditya Akella, Jeffrey Chase, Ari Juels, Michael Reiter, Thomas Ristenpart, Vyas Shekar, and Michael Swift. Rethinking Security in the Era of Cloud Computing *IEEE Security & Privacy* 2017

[64] Joanne Woodage, Rahul Chatterjee, Yevgeniy Dodis, Ari Juels, and Thomas Ristenpart. A New Distribution-Sensitive Secure Sketch and Popularity-Proportional Hashing *Advances in Cryptology – Crypto*, 2017

[65] Paul Grubbs, Jiahui Lu, and Thomas Ristenpart. Message Franking via Committing Authenticated Encryption *Advances in Cryptology – Crypto*, 2017

[66] Adam Everspaugh, Kenneth G. Paterson, Thomas Ristenpart, and Sam Scott. Key Rotation for Authenticated Encryption. *Advances in Cryptology – Crypto*, 2017

[67] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders *PACM: Human-Computer Interaction: Computer-Supported Cooperative Work and Social Computing (CSCW)*, 2017

[68] Rahul Chatterjee, Joanne Woodage, Yuval Pnueli, Anusha Chowdhury, and Thomas Ristenpart. The TypTop System: Personalized Typo-tolerant Password Checking *ACM Computer and Communications Security – CCS*, 2017

[69] Congzheng Song, Thomas Ristenpart, and Vitaly Shmatikov. Machine Learning Models that Remember Too Much *ACM Computer and Communications Security – CCS*, 2017

[70] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "A Stalker's Paradise": How Intimate Partners Abuse Technology *ACM Conference on Human Factors in Computing Systems (CHI)*, 2018

[71] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The Spyware Used in Intimate Partner Violence. *IEEE Symposium on Security and Privacy – Oakland*, 2018

Research Impact & Media Attention

- Results from [1, 5, 9] used during NIST SHA-3 competition to analyze new cryptographic hash function standard
- Adeona privacy-preserving device tracking software [7] covered by *The New York Times*, *Technology Review*, *ABC News*, and many others. Adeona downloaded >113,000 times since July 2008.
- Mozilla, Google developers acknowledge security vulnerabilities found in [14]
- Cloud computing attacks [12] featured in *Technology Review*, *PC World*, and others. European Network and Information Security Agency cites our work [12] in report on best practices for cloud computing security. More recent cross-VM side-channel attacks [25] lead to discussions with industry vendors regarding implications, and has been covered by *Hackernews*, *Threatpost*, *Technology Review*, *DarkReading*, and others.
- Proposed standard FFX for encryption methods for credit cards, SSNs, healthcare records based on [11]. Companies now deploy FFX widely to protect credit card data and other sensitive information. Algorithms for FPE and FTE with regular expression formats [32, 38] used by Skyhigh Networks for rapid deployment.
- TLS vulnerability found in [18] acknowledged by standardizers
- Point-of-sale vulnerabilities found in [21] acknowledged and fixed by Intuit and IDTech.[1] Bugs found by our tool Fie [28] fixed by TI.
- Format-transforming encryption [32] deployed with Tor, and currently being integrated into other censorship circumvention tools such as Lantern and uProxy. Our regular language tools for building FPE and FTE schemes used in industry [38].
- Ongoing discussion of issues uncovered in [34] with Linux kernel developers and Microsoft security.
- Honey encryption [33] reported on by *Technology Review*, *Business Week*, *Slashdot*, *Boston Globe*, and others.
- Study on typo tolerance in password entry [52] spawned changes in production Dropbox password login system (added a caps lock indicator). Typo tolerance reported on by *Technology Review*, *Threatpost*, *Slashdot*, and others. TypTop [68] released as public, open source software (`https://typtop.info/`).
- Results on machine learning model confidentiality [54] reported on by *Quartz*, *Wired*, *Medium.com*, *ACM.org*, *The Register*.
- Collaboration between Cornell Tech (led primarily by Nicola Dell, with some help from me) and the New York City's Office to Combat Domestic Violence lead to NYC Hope web portal (`https://www1.nyc.gov/nychope/site/page/home`).

[1] `https://security.intuit.com/index.php/home/alerts/95-security-update-for-gray-gopayment-card-reader`

Invited Talks (selected)

- Princeton University, *Tech Privacy and Safety in Intimate Partner Violence*, February 2018
- Facebook, *Tech Privacy and Safety in Intimate Partner Violence*, October 2017
- Google, *Tech Privacy and Safety in Intimate Partner Violence*, October 2017
- University of Chicago, *Making Password Checking Systems Better*, November 2016
- DIMACS Workshop on Cryptography and its Interactions: Learning Theory, Coding Theory, and Data Structures, *Stealing Machine Learning Models and Using Them to Violate Privacy*, July 2016
- DIMACS/MACS Workshop on Cryptography for the RAM Model of Computation, *Making Password Checking Systems Better*, June 2016
- Carnegie Mellon University, *Making Password Systems Better*, March 2016
- Crypto for Big Data Workshop at Columbia University, *Exploiting Leakage in Searchable Encryption and Machine Learning*, December 2015
- EPFL, *Model Inversion and other Threats in Machine Learning*, September 2015
- ETH Zurich, *Honey Encryption: Security Beyond the Brute-force Bound*, September 2015
- Fast Software Encryption 2014, *New Encryption Primitives for Uncertain Times*, March 2014
- DIMACS Workshop on Current Trends in Cryptography, *Message-locked Encryption and Secure Deduplication*, April 2013
- Royal Holloway University of London, *Message-locked Encryption and Secure Deduplication*, April 2013
- Real World Cryptography, *Message-locked Encryption and Secure Deduplication*, January 2013
- Microsoft Research, *Practice-driven Cryptographic Theory*, August 2012
- Stanford University, *Practice-driven Cryptographic Theory*, June 2012
- Qualcomm, *Practice-driven Cryptographic Theory*, June 2012
- NSF Workshop for Security of Cloud Computing, *New Problems in Security for Cloud Computing*, February 2012
- Isaac Newton Institute for Mathematical Sciences, *Practice-driven Cryptographic Theory*, January 2012
- Dagstuhl Workshop on Public-key Cryptography, *Careful with Composition: Limitations of the Indifferentiability Framework*, September 2011
- Microsoft Research, *Tag Size Does Matter: Attacks and Proofs for the TLS Record Protocol*, June 2011
- Microsoft Research, *Careful with Composition: Limitations of the Indifferentiability Framework*, June 2011

- VMWare, *Virtual Security: Data Leakage in Third-Party Clouds and VM Reset Vulnerabilities*, September 2010
- U. of Washington, *Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Clouds*, November 2009
- U. of Washington, *Virtual Machine Reset Vulnerabilities and Hedged Cryptography*, November 2009
- Microsoft Research, *Virtual Security: Data Leakage in Third-Party Clouds and VM Reset Vulnerabilities*, November 2009
- Dagstuhl Workshop on Symmetric Cryptography, *Salvaging Merkle-Damgård for Practical Applications*, January 2009
- Lorentz Center Workshop on Hash Functions, *Design Paradigms for Building Multi-Property Hash Functions*, June 2008
- Ecole Polytechnique Fédérale de Lausanne, *Privacy-Preserving Location Tracking of Lost or Stolen Devices*, May 2008
- Echternach Symmetric Cryptography Seminar, *Design Paradigms for Building Multi-Property Hash Functions*, January 2008
- Microsoft Research, *New Approaches for Building Cryptographic Hash Functions*, August 2007
- U. of Bristol, *New Approaches for Building Cryptographic Hash Functions*, May 2007
- U. of California, Davis, *New Approaches for Building Cryptographic Hash Functions*, March 2007

Professional Activities

- *Steering committee*: USENIX Security 2017–present; Real-World Cryptography Symposium 2013–present; DIMACS Workshop on Secure Cloud Computing 2014
- *Program co-Chair*: Cloud Computing Security Workshop 2011, USENIX Security Symposium 2017
- *Program committee*: Fast Software Encryption 2009, 2010; Cloud Computing Security Workshop 2010, 2012, 2013, 2014; Selected Areas in Cryptology 2010; Financial Cryptography and Data Security 2011; HotCloud 2011, 2012; Computer and Communications Security 2011, 2012; Eurocrypt 2012, 2014, 2016, 2018; Symposium on Security and Privacy (Oakland) 2012, 2013, 2015; Network and Distributed Security Symposium 2013, 2014, 2015, 2016; Crypto 2013; HotDep 2013; Dependable Systems and Networks 2014; USENIX Security Symposium 2014, 2015, 2016, 2018; FOCI 2014, 2016; Symposium on Cloud Computing 2014
- *Journal reviewer*: Journal of Computer Security; Journal of Cryptology; Designs, Codes and Cryptography
- *Invited panelist*: "How to Choose SHA-3", Lorentz Center Workshop on Hash Functions, June 2008; Electronic Transactions Association
- *Invited participant*: DARPA ISAT Future Ideas Symposium, June 2010; NSF Workshop on the Security of Cloud Computing 2012; DARPA ISAT Workshop 2013

Teaching Experience

- Cornell Tech, masters "Cryptography", Spring 2016, Spring 2017, Spring 2018
- Cornell Tech, graduate "Computer Security", Fall 2015, Fall 2016, Spring 2018
- Cornell Tech, masters "Building Startup Systems", Fall 2015, Fall 2016 (academic coordinator for class)
- University of Wisconsin–Madison, graduate "Information Security", Fall 2013
- University of Wisconsin–Madison, "Information Security", Fall 2011, 2012, Spring 2014
- University of Wisconsin–Madison, graduate "Applied Cryptography", Spring 2011,2012
- *Teaching Assistant*, UC San Diego, undergraduate "Modern Cryptography", 2006, 2008, 2010
- *Teaching Assistant*, UC San Diego, graduate "Modern Cryptography", 2008
- *Teaching Assistant*, UC Davis, undergraduate "Intro. to Programming and Problem Solving", 2001.

Advising

Current:

- Rahul Chatterjee (PhD, Cornell University)
- Paul Grubbs (PhD, Cornell University)
- Diana Freed (PhD, Cornell University, co-advised with Nicki Dell)
- Nirvan Tyagi (PhD, Cornell University)
- Julien Vanegue (PhD, Cornell University, co-advised with Vitaly Shmatikov)
- Liang Wang (PhD, Wisconsin)

Alumni:

- Ivan Pustogarov (Postdoc, 2017). First employment: University of Toronto (postdoc)
- Adam Everspaugh (PhD, 2017). First employment: Uptake.
- Venkatanathan Varadarajan (PhD, 2015). First employment: Oracle Labs.
- Robert Jellinek (MS, 2014). First employment: Amazon
- Benjamin Moench (BS, 2014). First employment: Symantec
- Alexis Fisher (MS, 2013). Project title: *EC2 Analysis Methods*. First employment: Sandia National Laboratories
- Benjamin Farley (MS, 2012). Thesis title: *Cloud Gaming: Taking Advantage of Performance Variability on EC2*. First employment: Amazon AWS
- WesLee Frisby (MS, 2012). First employment: Sandia National Laboratories

- Thawan Kooberat (MS, 2012). First employment: Facebook
- Adam Vail (BS, 2012). First employment: Graduate school at University of Wisconsin

Funding

- NSF SaTC: CORE: Large: Collaborative: Accountable Information Use: Privacy and Fairness in Decision-Making Systems, May 18, 2017 – May 17, 2022, $899,999. PI: Helen Nissenbaum. co-PI: Thomas Ristenpart
- NSF SaTC: CORE: Medium: Collaborative: Cryptographic Data Protection in Modern Systems, May 31, 2017 – May 30, 2021, $800,000. PI: Vitaly Shmatikov. co-PI: Thomas Ristenpart
- Schmidt Sciences. Apr. 25, 2017 – Apr. 25, 2019, $200,000. PI: Vitaly Shmatikov. co-PI: Thomas Ristenpart.
- ARO Toward Principled Foundations for Honey Objects in Information Security, Apr. 1, 2016 – Mar. 31, 2019, $388,795. PI: Ari Juels. co-PI: Thomas Ristenpart.
- TTP: Medium: Democratizing Secure Password Management, Aug. 11, 2011 – Aug. 31, 2019, $1,197,699. PI: Ari Juels. co-PI: Thomas Ristenpart
- Google, Gift, 2016, $20,000
- Google, Research Award, 2016, $56,500
- TWC: Medium: Collaborative: Distribution-Sensitive Cryptography, Nov. 16, 2015 – Aug. 31, 2019, $399,833 (to Cornell). PI: Ari Juels. co-PIs: Thomas Ristenpart, Thomas Shrimpton
- Microsoft, Gift, 2015, $60,000
- Sloan Fellow, Gift, 2015, $50,000
- Microsoft, Gift, 2014, $50,000
- NSF TWC: Frontier: Collaborative: Rethinking Security in the Era of Cloud Computing, Sept. 1, 2013 – Aug. 31, 2018, $1,995,068 (to Wisconsin). PI: Michael Reiter. co-PIs: Srinivasa Akella, Jay Aikat, Jeffrey Chase, Peng Ning, Thomas Ristenpart, Vyas Sekar, Michael Swift
- DoD Air Force: Mathematical Foundations of Secure Computing Clouds, Mar. 25, 2013 – Mar. 14, 2018, $338,443 ($56,925 to Cornell). PI: Benjamin Recht. Co-PIs: Stark Draper, Jordan Ellenberg, Robert Nowak, Christopher Re, Thomas Ristenpart, Steven Wright
- NSF CAREER: Infrastructure for Secure Cloud Computing, 2013 – 2017, $480,620. PI: Thomas Ristenpart
- Microsoft, Gift, 2013, $50,000 (to Wisconsin)
- Microsoft, Gift, 2012, $50,000 (to Wisconsin)
- NSF TC: Medium: Collaborative Research: Random Number Generation and Use in Virtualized Environments, Sept. 1, 2011 – Aug. 31, 2015, $749,149 (to Wisconsin). PI: Thomas Ristenpart. Co-PIs: Yevgeniy Dodis, Michael Swift
- RSA Laboratories, Gift, 2011, $20,000 (to Wisconsin)