Thomas Ristenpart

Updated August 14, 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

Awards

- Best Paper Award at ACM CHI 2018 for paper [72]
- Distinguished Student Paper Award at IEEE Symposium on Security and Privacy 2016 for paper [55]
- Sloan Foundation Research Fellow 2015
- Best Paper at USENIX Security 2014 for paper [38]

- 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 [31]
- 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] Mihir Bellare and Thomas Ristenpart. "Multi-Property-Preserving Hash Domain Extension and the EMD Transform." In: *Advances in Cryptology – Asiacrypt*. 2006.

[2] Francis Hsu, Hao Chen, Thomas Ristenpart, Jason Li, and Zhendong Su. "Back to the Future: A Framework for Automatic Malware Removal and System Repair." In: *ACSAC*. 2006.

[3] Thomas Ristenpart and Phillip Rogaway. "How to Enrich the Message Space of a Cipher." In: *Fast Software Encryption*. 2007. [Retracted February 2015].

[4] Thomas Ristenpart and Scott Yilek. "The Power of Proofs-of-Possession: Securing Multiparty Signatures against Rogue-Key Attacks." In: *Advances in Cryptology – Eurocrypt*. 2007.

[5] Mihir Bellare and Thomas Ristenpart. "Hash Functions in the Dedicated-Key Setting: Design Choices and MPP Transforms." In: *ICALP*. 2007.

[6] Thomas Ristenpart and Thomas Shrimpton. "How to Build a Hash Function from Any Collision-Resistant Function." In: *Advances in Cryptology – Asiacrypt*. 2007.

[7] Thomas Ristenpart, Gabriel Maganis, Arvind Krishnamurthy, and Tadayoshi Kohno. "Privacy-Preserving Location Tracking of Lost or Stolen Devices: Cryptographic Techniques and Replacing Trusted Third Parties with DHTs." In: *USENIX Security Symposium*. 2008.

[8] Mihir Bellare, Marc Fischlin, Adam O'Neill, and Thomas Ristenpart. "Deterministic Encryption: Definitional Equivalences and Constructions without Random Oracles." In: *Advances in Cryptology – Crypto*. 2008.

[9] Mihir Bellare and Thomas Ristenpart. "Simulation without the Artificial Abort: Simplified Proof and Improved Concrete Security for Waters' IBE Scheme." In: *Advances in Cryptology – Eurocrypt*. 2009.

[10] Yevgeniy Dodis, Thomas Ristenpart, and Thomas Shrimpton. "Salvaging Merkle-Damgård for Practical Applications." In: *Advances in Cryptology – Eurocrypt*. 2009.

[11] Mihir Bellare, Thomas Ristenpart, Phillip Rogaway, and Till Stegers. "Format-Preserving Encryption." In: *Selected Areas in Cryptography*. 2009.

[12] Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage. "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds." In: *ACM Conference on Computer and Communications Security*. 2009.

[13] Mihir Bellare, Zvika Brakerski, Moni Naor, Thomas Ristenpart, Gil Segev, Hovav Shacham, and Scott Yilek. "Hedged Public-Key Encryption: How to Protect against Bad Randomness." In: *Advances in Cryptology – Asiacrypt*. 2009.

[14] Thomas Ristenpart and Scott Yilek. "When Good Randomness Goes Bad: Virtual Machine Reset Vulnerabilities and Hedging Deployed Cryptography." In: *NDSS*. 2010.

[15] Marc Fischlin, Anja Lehmann, Thomas Ristenpart, Thomas Shrimpton, Martijn Stam, and Stefano Tessaro. "Random Oracles with(out) Programmability." In: *Advances in Cryptology – Asiacrypt*. 2010.

[16] Thomas Ristenpart, Hovav Shacham, and Thomas Shrimpton. "Careful with Composition: Limitations of the Indifferentiability Framework." In: *Advances in Cryptology – Eurocrypt*. 2011.

[17] Kenneth G. Paterson, Thomas Ristenpart, and Thomas Shrimpton. "Tag Size Does Matter: Attacks and Proofs for the TLS Record Protocol." In: *Advances in Cryptology – Asiacrypt*. 2011.

[18] Qing Zhang, Thomas Ristenpart, Stefan Savage, and Geoff Voelker. "Got Traffic? An Evaluation of Click Traffic Providers". In: *WICOM/AIRWeb Workshop on Web Quality*. 2011.

[19] Benjamin Farley, Ari Juels, Venkatanathan Varadarajan, Thomas Ristenpart, Kevin D. Bowers, and Michael M. Swift. "More for your money: exploiting performance heterogeneity in public clouds." In: *Symposium on Cloud Computing*. 2012.

[20] Yevgeniy Dodis, Thomas Ristenpart, and Salil P. Vadhan. "Randomness Condensers for Efficiently Samplable, Seed-Dependent Sources." In: *TCC*. 2012.

[21] Kevin P. Dyer, Scott E. Coull, Thomas Ristenpart, and Thomas Shrimpton. "Peek-a-Boo, I Still See You: Why Efficient Traffic Analysis Countermeasures Fail." In: *IEEE Symposium on Security and Privacy*. 2012.

[22] WesLee Frisby, Benjamin Moench, Benjamin Recht, and Thomas Ristenpart. "Security Analysis of Smartphone Point-of-Sale Systems." In: *WOOT*. 2012.

[23] Mihir Bellare, Thomas Ristenpart, and Stefano Tessaro. "Multi-instance Security and Its Application to Password-Based Cryptography." In: *Advances in Cryptology – Crypto*. 2012.

[24] Yevgeniy Dodis, Thomas Ristenpart, John P. Steinberger, and Stefano Tessaro. "To Hash or Not to Hash Again? (In)Differentiability Results for H 2 and HMAC." In: *Advances in Cryptology – Crypto*. 2012.

[25] Venkatanathan Varadarajan, Thawan Kooburat, Benjamin Farley, Thomas Ristenpart, and Michael M. Swift. "Resource-freeing attacks: improve your cloud performance (at your neighbor's expense)." In: *ACM Conference on Computer and Communications Security*. 2012.

[26] Yinqian Zhang, Ari Juels, Michael K. Reiter, and Thomas Ristenpart. "Cross-VM side channels and their use to extract private keys." In: *ACM Conference on Computer and Communications Security*. 2012.

[27] Mihir Bellare, Sriram Keelveedhi, and Thomas Ristenpart. "Message-Locked Encryption and Secure Deduplication." In: *Advances in Cryptology – Eurocrypt*. 2013.

[28] Drew Davidson, Benjamin Moench, Thomas Ristenpart, and Somesh Jha. "FIE on Firmware: Finding Vulnerabilities in Embedded Systems Using Symbolic Execution." In: *USENIX Security Symposium*. 2013.

[29] Sriram Keelveedhi, Mihir Bellare, and Thomas Ristenpart. "DupLESS: Server-Aided Encryption for Deduplicated Storage." In: *USENIX Security Symposium*. 2013.

[30] Thomas Ristenpart and Scott Yilek. "The Mix-and-Cut Shuffle: Small-Domain Encryption Secure against N Queries." In: *Advances in Cryptology – Crypto*. 2013.

[31] Kevin P. Dyer, Scott E. Coull, Thomas Ristenpart, and Thomas Shrimpton. "Protocol misidentification made easy with format-transforming encryption." In: *ACM Conference on Computer and Communications Security*. 2013.

[32] Keqiang He, Alexis Fisher, Liang Wang, Aaron Gember, Aditya Akella, and Thomas Ristenpart. "Next stop, the cloud: understanding modern web service deployment in EC2 and azure." In: *Internet Measurement Conference*. 2013.

[33] Ari Juels and Thomas Ristenpart. "Honey Encryption: Encryption beyond the Brute-Force Barrier." In: *IEEE Security & Privacy* 12.4 (2014), pp. 59–62.

[34] Ari Juels and Thomas Ristenpart. "Honey Encryption: Security Beyond the Brute-Force Bound." In: *Advances in Cryptology – Eurocrypt*. 2014.

[35] Adam Everspaugh, Yan Zhai, Robert Jellinek, Thomas Ristenpart, and Michael M. Swift. "Not-So-Random Numbers in Virtualized Linux and the Whirlwind RNG." In: *IEEE Symposium on Security and Privacy*. 2014.

[36] Robert Jellinek, Yan Zhai, Thomas Ristenpart, and Michael M. Swift. "A Day Late and a Dollar Short: The Case for Research on Cloud Billing Systems." In: *HotCloud*. 2014.

[37] Stephen Checkoway, Ruben Niederhagen, Adam Everspaugh, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz, Hovav Shacham, and Matthew Fredrikson. "On the Practical Exploitability of Dual EC in TLS Implementations." In: *USENIX Security Symposium*. 2014.

[38] Matthew Fredrikson, Eric Lantz, Somesh Jha, Simon Lin, David Page, and Thomas Ristenpart. "Privacy in Pharmacogenetics: An End-to-End Case Study of Personalized Warfarin Dosing." In: *USENIX Security Symposium*. 2014.

[39] Daniel Luchaup, Kevin P. Dyer, Somesh Jha, Thomas Ristenpart, and Thomas Shrimpton. "LibFTE: A Toolkit for Constructing Practical, Format-Abiding Encryption Schemes." In: *USENIX Security Symposium*. 2014.

[40] Venkatanathan Varadarajan, Thomas Ristenpart, and Michael M. Swift. "Scheduler-based Defenses against Cross-VM Side-channels." In: *USENIX Security Symposium*. 2014.

[41] Daniel Luchaup, Thomas Shrimpton, Thomas Ristenpart, and Somesh Jha. "Formatted Encryption Beyond Regular Languages." In: *ACM Conference on Computer and Communications Security*. 2014.

[42] Yinqian Zhang, Ari Juels, Michael K. Reiter, and Thomas Ristenpart. "Cross-Tenant Side-Channel Attacks in PaaS Clouds." In: *ACM Conference on Computer and Communications Security*. 2014.

[43] Liang Wang, Antonio Nappa, Juan Caballero, Thomas Ristenpart, and Aditya Akella. "WhoWas: A Platform for Measuring Web Deployments on IaaS Clouds." In: *Internet Measurement Conference*. 2014.

[44] Yevgeniy Dodis, Chaya Ganesh, Alexander Golovnev, Ari Juels, and Thomas Ristenpart. "A Formal Treatment of Backdoored Pseudorandom Generators." In: *Advances in Cryptology – Eurocrypt*. 2015.

[45] Rahul Chatterjee, Joseph Bonneau, Ari Juels, and Thomas Ristenpart. "Cracking-Resistant Password Vaults Using Natural Language Encoders." In: *IEEE Symposium on Security and Privacy*. 2015.

[46] Adam Everspaugh, Rahul Chatterjee, Samuel Scott, Ari Juels, and Thomas Ristenpart. "The Pythia PRF Service." In: *USENIX Security Symposium*. 2015.

[47] Venkatanathan Varadarajan, Yinqian Zhang, Thomas Ristenpart, and Michael M. Swift. "A Placement Vulnerability Study in Multi-Tenant Public Clouds." In: *USENIX Security Symposium*. 2015.

[48] David Cash, Paul Grubbs, Jason Perry, and Thomas Ristenpart. "Leakage-Abuse Attacks Against Searchable Encryption." In: *ACM Conference on Computer and Communications Security*. 2015.

[49] Matt Fredrikson, Somesh Jha, and Thomas Ristenpart. "Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures." In: *ACM Conference on Computer and Communications Security*. 2015.

[50] Liang Wang, Kevin P. Dyer, Aditya Akella, Thomas Ristenpart, and Thomas Shrimpton. "Seeing through Network-Protocol Obfuscation." In: *ACM Conference on Computer and Communications Security*. 2015.

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

[52] Lucas Dixon, Thomas Ristenpart, and Thomas Shrimpton. "Network Traffic Obfuscation and Automated Internet Censorship." In: *IEEE Security & Privacy* 14.6 (2016), pp. 43–53.

[53] Yan Zhai, Lichao Yin, Jeffrey S. Chase, Thomas Ristenpart, and Michael M. Swift. "CQSTR: Securing Cross-Tenant Applications with Cloud Containers." In: *Symposium on Cloud Computing*. 2016.

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

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

[56] Drew Davidson, Hao Wu, Robert Jellinek, Vikas Singh, and Thomas Ristenpart. "Controlling UAVs with Sensor Input Spoofing Attacks." In: *WOOT*. 2016.

[57] Florian Tramèr, Fan Zhang, Ari Juels, Michael K. Reiter, and Thomas Ristenpart. "Stealing Machine Learning Models via Prediction APIs." In: *USENIX Security Symposium*. 2016.

[58] Paul Grubbs, Richard McPherson, Muhammad Naveed, Thomas Ristenpart, and Vitaly Shmatikov. "Breaking Web Applications Built On Top of Encrypted Data." In: *ACM Conference on Computer and Communications Security*. 2016.

[59] Jay Aikat, Aditya Akella, Jeffrey S. Chase, Ari Juels, Michael K. Reiter, Thomas Ristenpart, Vyas Sekar, and Michael M. Swift. "Rethinking Security in the Era of Cloud Computing." In: *IEEE Security & Privacy* 15.3 (2017), pp. 60–69.

[60] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders." In: *PACMHCI* 1.CSCW (2017), 46:1–46:22.

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

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

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

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

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

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

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

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

[69] Ivan Pustogarov, Thomas Ristenpart, and Vitaly Shmatikov. "Using Program Analysis to Synthesize Sensor Spoofing Attacks." In: *AsiaCCS*. 2017.

[70] Congzheng Song, Thomas Ristenpart, and Vitaly Shmatikov. "Machine Learning Models that Remember Too Much." In: *Computer and Communications Security*. 2017.

[71] Liang Wang, Mengyuan Li, Yinqian Zhang, Thomas Ristenpart, and Michael M. Swift. "Peeking Behind the Curtains of Serverless Platforms." In: *USENIX Annual Technical Conference*. 2018.

[72] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. ""A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology." In: *Conference on Human-Computer Interaction – CHI*. 2018.

[73] 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". In: *IEEE Symposium on Security and Privacy*. 2018.

[74] Yevgeniy Dodis, Paul Grubbs, Thomas Ristenpart, and Joanne Woodage. "Fast Message Franking: From Invisible Salamanders to Encryptment". In: *Advances in Cryptology – Crypto*. 2018.

[75] Vincent Bindschaedler, Paul Grubbs, David Cash, Thomas Ristenpart, and Vitaly Shmatikov. "The Tao of Inference in Privacy-protected Databases". In: *Proceedings of the VLDB Endowment*. 2018.

Research Impact & Media Attention

- Results from [1, 5, 10] 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. Cross-VM cryptographic side-channel attack [26] led 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 [31, 39] used by Skyhigh Networks for rapid deployment.

- TLS vulnerability found in [17] acknowledged by standardizers

- Point-of-sale vulnerabilities found in [22] acknowledged and fixed by Intuit and IDTech.[1] Bugs found by our tool Fie [28] fixed by TI.

- Format-transforming encryption [31] 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 [39].

- Discussion of issues uncovered in [35] with Linux kernel developers and Microsoft security, vulnerabilities in Microsoft patched.

- Honey encryption [34] reported on by *Technology Review*, *Business Week*, *Slashdot*, *Boston Globe*, and others.

- Study on typo tolerance in password entry [55] 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 [57] 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`).

- Paper [73] led Google to restrict advertisements on google.com and the Google Play store for search terms related to intimate-partner-violence, as well as changes to Play store policy. This work was reported on by the *New York Times*, *Le Monde*, *The Times*, and more.

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

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

- 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, 2019; 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)
- Samuel Havron (PhD, Cornell University, co-advised with Nicki Dell)
- Ian Miers (Postdoc, Cornell Tech)
- Bijeeta Pal (PhD, Cornell University)
- Nirvan Tyagi (PhD, Cornell University)
- 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

- Facebook Secure the Internet Grant, Improving Encrypted Messaging, 2018, $80,000. PI: Thomas Ristenpart. co-PI: Yevgeniy Dodis
- Google, Research Award, 2018. $40,000. PI: Nicola Dell. co-PI: Thomas Ristenpart
- 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)