# Fabian N. Monrose

[A] GEORGIA INSTITUTE OF TECHNOLOGY
School of Electrical and Computer Engineering
Klaus Advanced Computing Building

*E-mail*: fabian@ece.gatech.edu
*Last update*: June 10, 2024

**[B] Education**

**Ph. D., Computer Science,** *Courant Institute of Mathematical Sciences*
New York University, New York, USA May, 1999
*Advisor*: Prof. Zvi Kedem

**M. Sc., Computer Science,** *Courant Institute of Mathematical Sciences*
New York University, New York, USA May, 1996

**B. Sc., Computer Science,** *Barry University*
Miami, Florida, USA May, 1993

**[C] Professional Experience**

JULIAN T. HIGHTOWER CHAIR, *Georgia Tech*
College of Engineering, August 2022 — present

KENAN DISTINGUISHED PROFESSOR, *University of North Carolina, Chapel Hill*
Computer Science Department, July 2017 — July 2022

CO-FOUNDER, *Zeropoint Dynamics*
Role: Chief Scientist, March 2015 — 2022

DIR., COMPUTER & INFORMATION SECURITY *Renaissance Computing Institute*
Joint appointment with UNC-CH Comp. Sci. January 2014 — 2018

PROFESSOR, *University of North Carolina, Chapel Hill*
Computer Science Department, January 2013 — present

ASSOCIATE PROFESSOR, *University of North Carolina, Chapel Hill*
Computer Science Department, July 2008 — December, 2012

ASSOCIATE PROFESSOR, *Johns Hopkins University*
Computer Science Department, July 2007 —June 2008

ASSISTANT PROFESSOR, *Johns Hopkins University*
Computer Science Department, November 2002 — June 2007

RESEARCH SCIENTIST, *Bell Laboratories, Lucent Technologies*
Secure Systems Research, July 1999 — October 2002

RESEARCH INTERN, *AT&T Labs Research*
Secure Systems Research Department, Summer 1998

RESEARCH INTERN, *Bell Communications*
High Availability and Distributed Computing Research Group, Summer 1997

RESEARCH INTERN, *Bell Communications*
Cryptography and Network Security Research Group, Summer 1996

RESEARCH ASSISTANT, *New York University*
Computer Science Department, August 1995 — 1998

RESEARCH ASSISTANT, *New York University*
Distributed Systems Group, Summer 1994

**[D] Honors**

- CIOS Honor Roll, *GT Center for Teaching and Learning*, Fall, 2023
- CSSA Graduate Teaching Award, *CS Department*, May, 2021
- Undergraduate Students Teaching Award, *CS Department*, May, 2015
- Best Student Paper Award, *IEEE Symposium on Security & Privacy* May, 2013
- Outstanding Research in *Privacy Enhancing Technologies* (PET), July, 2012
- AT&T Best Applied Security Paper Award, *NYU-Poly CSAW*, Nov, 2011
- Best Paper Award, *IEEE Symposium on Security & Privacy*, May, 2011
- Best Paper Award, *Intl. Conf. on Internet Monitoring and Protection*, April, 2011
- Faculty Research Award, *Google* May, 2011
- Faculty Research Award, *Google* March, 2009
- CAREER Award, *National Science Foundation*, February, 2006
- Best Student Paper Award, $8^{th}$ *USENIX Security Symposium* August, 1999
- Best Overall Paper Award, $8^{th}$ *USENIX Security Symposium* August, 1999
- USENIX Scholars Research Award Fall 1998
- Bell Communications Research Scholarship Fall 1997

**[E] Funding** Awarded Grants & Contracts

[G1] **PI**, DARPA (M. Antonakakis at GaTech (*lead*)), A NOVEL FRAMEWORK TO ASSESS, STATISTICALLY MODEL AND EVADE CYBER ATTACK INFRASTRUCTURE for $\$1,266,714$, October. 22 — October 2025.

[G2] **Co-PI** (with Jan-Michel Frahm), CIA, CYBER IDENTITY AND BEHAVIORAL ANALYTICS

RESEARCH CONSORTIUM (CIBAR) for $559,000, July 2017 — Dec, 2021.

[G3] **PI**, DARPA (M. Antonakakis at GaTech (*lead*)), ATTRIBUTING CYBER ACTORS THROUGH TENSOR DECOMPOSITION AND NOVEL DATA ACQUISITION for $2,019,181, Nov. 2016 — August 2021.

[G4] **PI**, NIST, KNOWLEDGE IS POWER: ASSESSING THE SECURITY AND PRIVACY OF CONSUMER IOT ARCHITECTURES AND SYSTEMS for $183,063.00, July 2017 — July, 2018.

[G5] **PI**, IEEE, ADVANCING CYBERSECURITY EDUCATION THROUGH ACTIVE, CHALLENGE-BASED, LEARNING EXERCISES for $119,999.44, Jan. 2017 — August, 2018.

[G6] **PI**, Department of Defense University Research Instrumentation Program (DURIP), NEXT GENERATION DEFENSES AGAINST WEB-BASED EXPLOITS for $116,500.00, April, 2016 — May 2017.

[G7] **Co-PI** (with Jan-Michel Frahm (*lead*)), Department of Defense University Research Instrumentation Program (DURIP), UNDERSTANDING PRIVACY RISKS OF UBIQUITOUS PERSONAL AUGMENTED REALITY HEAD-MOUNTED DISPLAYS for $95,385.00, June, 2014 — May 2015.

[G8] **PI**, NSF *Secure and Trustworthy Computing*, TWC: TTP OPTION: SMALL: SCALABLE TECHNIQUES FOR BETTER SITUATIONAL AWARENESS: ALGORITHMIC FRAMEWORKS AND LARGE SCALE EMPIRICAL ANALYSES for $667,900.00, Sept. 2014—August 2017.

[G9] **PI** Department of Homeland Security *Transition to Practice Program*, SUPPLEMENT TO NSF SDCI SEC: NEW SOFTWARE PLATFORMS FOR SUPPORTING NETWORK-WIDE DETECTION OF CODE INJECTION ATTACKS for $350,000.00, Sept. 2014—August 2015.

[G10] **PI**, Department of Defense University Research Instrumentation Program (DURIP), NEXT-GENERATION DEFENSES FOR SECURING VOIP COMMUNICATIONS for $114,345.00, June, 2013 — May 2014.

[G11] **PI**, NSF *Secure and Trustworthy Computing*, SUPPORT FOR THE 2014 USENIX SECURITY SYMPOSIUM; SAN DEIGO for $20,000.00, July 30, 2014— October 2015.

[G12] **PI**, NSF *Secure and Trustworthy Computing*, TOWARD PRONOUNCEABLE AUTHENTICATION STRINGS for $499,997.00, Aug. 2013—July 2016.

[G13] **PI**, NSF *Secure and Trustworthy Computing*, SUPPORT FOR THE 2013 USENIX SECURITY SYMPOSIUM; WASHINGTON D.C. for $10,000.00, July 30, 2013— October 2013.

[G14] **PI**, Department of Homeland Security, EFFICIENT TRACKING, LOGGING, AND BLOCKING OF ACCESSES TO DIGITAL OBJECTS (with C. Schmitt and M. Bailey) for $1,035,590. September 2012 — August 2014.

[G15] **Co-PI** (Jan-Michel Frahm (*lead*)), NSF *Division of Information & Intelligent Systems*, EAGER: AUTOMATIC RECONSTRUCTION OF TYPED INPUT FROM COMPROMISING REFLECTIONS for $151,749.00, August 2011—July 2013.

[G16] **PI**, *Verisign Labs Research Awards Program*, ON EXPLORING APPLICATIONS OF PHONETIC EDIT DISTANCE for $65,000.00, June 2011.

[G17] **PI**, *Google Faculty Research Awards Program*, SHELLOS: AN EFFICIENT RUNTIME PLATFORM FOR DETECTING CODE INJECTION ATTACKS for $61,635.00, May 2011.

[G18] **PI**, NSF *Office of Cyberinfrastructure*, SDCI SEC: NEW SOFTWARE PLATFORMS FOR SUPPORTING NETWORK-WIDE DETECTION OF CODE INJECTION ATTACKS for $800,000.00, Aug. 2011—July 2014.

[G19] **PI**, NSF *Trustworthy Computing*, SUPPORT FOR THE 2011 USENIX SECURITY SYMPOSIUM; SAN FRANCISCO for $20,000.00, July 30, 2011— October 2011.

[G20] **PI**, NSF *Trustworthy Computing*, TC: SMALL: EXPLORING PRIVACY BREACHES IN ENCRYPTED VOIP COMMUNICATIONS for $496,482.00, Aug. 2010—July 2013.

[G21] **PI**, NSF *Trustworthy Computing*, SUPPORT FOR THE 2010 USENIX SECURITY SYMPOSIUM; WASHINGTON D.C. for $20,000.00, July 30, 2010— October 2010.

[G22] **PI** (A. Stavrou at GMU (*lead*)), NSF *Trustworthy Computing*, COLLABORATIVE RESEARCH: SCALABLE MALWARE ANALYSIS USING LIGHTWEIGHT VIRTUALIZATION for $259,264.00, Sept. 2009—August 2011.

[G23] **PI**, DETECTING AND MONITORING MALFEASANCE ON THE NET, Google Faculty Research Awards Program for $90,000.00, March 2009–Feb 2010.

[G24] **Co-PI** ( W. Lee at GaTech (*lead*)), NSF *Cyber Trust*: CLEANSE:CROSS-LAYER LARGE-SCALE EFFICIENT ANALYSIS OF NETWORK ACTIVITIES TO SECURE THE INTERNET for $1,839,297.00, July 2008 — June 2012.

[G25] **PI**, Department of Homeland Security, NEW FRAMEWORKS FOR DETECTING AND MINIMIZING INFORMATION LEAKAGE IN ANONYMIZED NETWORK DATA for $962,609.00. April 2008—April 2011.

[G26] **Co-PI** (G. Masson (*lead*)), SECURITY THROUGH VIRTUALIZATION. Information Assurance Scholarship Program for $142,948.00. DoD, ANNEX II, Feb, 2008.

[G27] **Co-PI** (A. Terzis (*lead*)), NSF *Cyber Trust*: THINKING AHEAD: A PROACTIVE APPROACH FOR COUNTERING FUTURE INTERNET MALWARE for $350,000.00. September 2006 — August 2009.

[G28] **PI**, NSF *Cyber Trust*: CAREER:TOWARDS EFFECTIVE IDENTIFICATION OF APPLICATION BEHAVIORS IN ENCRYPTED TRAFFIC for $400,000.00. September 2006 — August 2011.

[G29] **PI**, NSF *Cyber Trust*: GENERATIVE MODELS FOR IMPROVING BIOMETRICALLY ENHANCED SYSTEMS for $696,553.00. December 2004 — October 2007.

[G30] **Co-PI**, NSF *STI*: TOWARDS MORE SECURE INTER-DOMAIN ROUTING (A. Rubin (*lead*)) for $616,923.00. November 2003 — June 2006.

**[F] Bib.**

**Manuscripts Under Review / Revision**

[U1] *The Guardian of Name Street: Studying Defensive Registrations for the Fortune 500*. Boladji Vinny Adjibi, Athanasios Avgetidis, Michael Bailey, Fabian Monrose and Manos Antonakakis. 2024.

[U2] *Systematically Discovering Unknown APT Infrastructure*. Athanasios Avgetidis, Boladji Vinny Adjibi, Panagiotis Kintis, Tillson Galloway, Zane Ma, Omar Alrawi, Manos Antonakakis, Roberto Perdisci, Fabian Monrose and Angelos Keromytis. 2024.

[U3] *Don't Miss Out on the Cross-Family Gossip: Using Shared Implementations of Behaviors to Uncover Relationships Within and Between Malware Families*. Kevin Valakuzhy, Miuyin Yong Wong, Omar Alrawi, Angelos D. Keromytis and Fabian Monrose. 2024.

**Refereed Conference Publications**

[P1] *Contrasting Theory to Practice: Results from Interviews with Expert Malware Analysts*. Miuyin Wong, Matthew Landen, Frank Li, Fabian Monrose and Mustaque Ahamad. In USENIX Symposium on Usable Privacy and Security, August, 2024.

[P2] *CrashTalk: Automated Generation of Precise, Human Readable, Descriptions of Software Security Bugs*. Kedrian James, Kevin Valakuzhy, Kevin Snow and Fabian Monrose. In Proceedings of the ACM Conference and Computer and Data Security, June, 2024.

[P3] *Towards Practical Fabrication Stage Attacks Using Interrupt-Resilient Hardware Trojans*. Athanasios Moschos, Fabian Monrose and Angelos Keromytis. In IEEE International Symposium on Hardware Oriented Security and Trust, May, 2024.

[P4] *Improving Security Tasks Using Compiler Provenance Information Recovered At the Binary-Level*. Yufei Du, Omar Alwari, Kevin Snow, Manos Antonakakis and Fabian Monrose. In Proceedings of ACM Conference on Computer and Communications Security, November, 2023.

[P5] *Stale TLS Certificates: Investigating Precarious Third-Party Access to Valid TLS Keys* . Zane Ma, Aaron Faulkenberry, Thomas Papastergiou, Zakir Durumeric, Michael D. Bailey, Angelos D. Keromytis, Fabian Monrose and Manos Antonakakis. In Proceedings of ACM Internet Measurement Conference, Oct, 2023.

[P6] *More Carrot or Less Stick: Organically Improving Student Time Management With Practice Tasks and Gamified Assignments*. Mac Malone and Fabian Monrose. In Proceedings of ACM Conference on Innovation and Technology In CS Education, July, 2023.

[P7] *Securely Autograding Cybersecurity Exercises Using Web Accessible Jupyter Notebooks*. Mac Malone, Yicheng Wang and Fabian Monrose. In Proceedings of ACM SIGCSE Technical Symposium, March, 2023.

[P8] *Beyond the Gates: An Empirical Analysis of HTTP-managed password stealers and operators*. Omar Alrawi, Athanasios Avgetidis, Kevin Valakuzhy, Charles Lever, Paul Burbage, Angelos Keromytis, Fabian Monrose, and Manos Antonakakis. In Proceedings of the USENIX Security Symposium, August 2023.

[P9] *View from Above: Exploring the Malware Ecosystem from the Upper DNS Hierarchy*. Aaron Faulkenberry, Athanasios Avgetidis, Zane Ma, Omar Alrawi, Charles Lever, Panagiotis Kintis, Fabian Monrose, Angelos Keromytis, and Manos Antonakakis. In Proceedings of the Annual Computer Security Applications Conference, Dec 2022.

[P10] *Automatic Recovery of Fine-grained Compiler Provenance Information at the Binary Level*. Yufei Du, Ryan Court, Kevin Z. Snow and Fabian Monrose. USENIX Annual Technical Conference, July, 2022. (Acceptance rate=16.5%)

[P11] *Disentangling Style and Content for Low Resource Video Domain Adaptation: A Case Study on Keystroke Inference Attacks*. John Lim, Jan-Michael Frahm and Fabian Monrose. In ACM Conference on Data and Application Security (CODASPY), April, 2022.

[P12] *An Online Gamified Learning Platform for Teaching Cybersecurity and More*. Mac Malone, Yicheng Wang and Fabian Monrose. ACM Annual Conference on IT Education (SIGITE), October, 2021.

[P13] *DynPTA: Combining Static and Dynamic Analysis for Practical Selective Data Protection*. Tapti Palit, Jarin Firose Moon, Fabian Monrose and Michalis Polychronakis. In Proceedings of the IEEE Symposium on Security and Privacy, May, 2021. (Acceptance rate=11.8%).

[P14] *Applicable Micropatches and Where to Find Them: Finding and Applying New Security Hot Fixes to Old Software*. Mac Malone, Yicheng Wang, Kevin Snow and Fabian Monrose. IEEE International Conference on Software Testing, Verification and Validation, April, 2021. (Acceptance rate=24.8%)

[P15] *The Circle Of Life: A Large-Scale Study of The IoT Malware Lifecycle*. Omar Alrawi, Charles Lever, Kevin Valakuzhy, Ryan Court, Kevin Snow, Fabian Monrose and Manos Antonakakis. USENIX Security Symposium, August, 2021. (Acceptance rate=18.8%).

[P16] *To Gamify or Not? On Leaderboard Effects, Student Engagement, and Learning outcomes in a Cybersecurity Intervention*. Mac Malone, Yicheng Wang, Kedrian James, Murray Anderegg, Jan Werner and Fabian Monrose. ACM SIGCSE Technical Symposium, 2021. (Acceptance rate=31%).

[P17] *A Flexible Framework for Expediting Bug Findings by Leveraging Past (Mis-)Behavior to Discover New Bugs*. Sanjeev Das, Kedrian James, Jan Werner, Manos Antonakakis, Michalis Polychronakis and Fabian Monrose. ACM Annual Computer Security Applications Conference (ACSAC), December 2020. (Acceptance rate=23.1%).

[P18] *Methodologies for Quantifying (Re-)randomization Security and Timing under JIT-ROP*. Md Salman Ahmed, Ya Xiao, Kevin Z. Snow, Gang Tan, Fabian Monrose and Danfeng Yao. In Proceedings of the ACM Conference on Computer and Communications Security, October, 2020. (Acceptance rate=17%).

[P19] *Mitigating Data Leakage by Protecting Memory-resident Sensitive Data*. Tapti Palit, Fabian Monrose and Michalis Polychronakis. In Proceedings of the Annual Computer Security Application Conference, December 2019. (Acceptance rate=22.6%).

[P20] *The SEVerESt Of Them All: Inference Attacks Against Secure Virtual Enclaves*. Jan Werner, Joshua Mason, Manos Antonakakis, Michalis Polychronakis and Fabian Monrose. In

Proceedings of the ACM Asia Conference on Computer and Communication Security, July 2019. (Acceptance rate=21.4%).

[P21] *SoK: The Challenges, Pitfalls, and Perils of Using Hardware Performance Counters for Security*. S. Das, J. Werner, M. Antonakakis, M. Polychronakis and F. Monrose. In Proceedings of the IEEE Symposium on Security and Privacy, May, 2019. (Acceptance rate=13.6%).

[P22] *SoK: Security Evaluation of Home-Based IoT Deployments*. O. Alrawi, C. Lever, M. Antonakakis and F. Monrose. In Proceedings of the IEEE Symposium on Security and Privacy, May, 2019. (Acceptance rate=13.6%).

[P23] *Security Concerns in Asynchronous Web Server Architectures: When Performance Optimizations Empower Data-oriented Attacks*. M. Morton, J. Werner, K. Z. Snow, M. Antonakakis, M. Polychronakis and F. Monrose. In Proceedings of the IEEE European Symposium on Security and Privacy, April, 2018. (Acceptance rate=22%).

[P24] *Practical Attacks Against Graph-based Clustering*. Y. Chen, Y. Nadji, A. Kountouras, F. Monrose, R. Perdisci, M. Antonakakis, N. Vasiloglou. In Proceedings of the ACM Conference on Computer and Communications Security, October, 2017. (Acceptance rate=18%).

[P25] *Keeping Zombie Gadgets at Bay by Re-randomizing after Disclosure*. Micah Morton, Forrest Li, Kevin Snow, Michalis Polychronakis and Fabian Monrose. In Proceedings of Engineering Secure Systems and Software conference (ESSoS), July, 2017.

[P26] *Revisiting Browser Security in the Modern Era: New Data-only Attacks and Defenses*. Roman Rogowski, Micah Morton, Forrest Li, Kevin Z. Snow, Fabian Monrose and Michalis Polychronakis. In Proceedings of the IEEE European Symposium on Security and Privacy, March 2017. (Acceptance rate=17.5%).

[P27] *Virtual U: Defeating Face Liveness Detection by Building Virtual Models From Your Public Photos*. Yi Xu, True Price, Jan-Michael Frahm and Fabian Monrose. In Proceedings of the USENIX Security Symposium, August 2016. (Acceptance rate=15.5%).

[P28] *Return to the Zombie Gadgets: Undermining Destructive Code Reads via Code-Inference Attacks*. Kevin Z. Snow, Roman Rogowski, Jan Werner, Hyungjoon Koo, Fabian Monrose and Michalis Polychronakis. In Proceedings of the IEEE Symposium on Security and Privacy, May, 2016. (Acceptance rate=14%).

[P29] *No-Execute-After-Read: Preventing Code Disclosures in Commodity Software*. Jan Werner, George Baltas, Rob Dallara, Nathan Otterness, Kevin Snow, Fabian Monrose and Michalis Polychronakis. In Proceedings of the ACM Asia Conference on Computer and Communication Security, May 2016. (Acceptance rate=21%).

[P30] *Detecting Malicious Exploit Kits using Tree-based Similarity Searches*. Teryl Taylor, Xin Hu, Ting Wang, Jiyong Jang, Marc Stoeckin, Fabian Monrose and Reiner Sailer. In Proceedings of the ACM Conference on Data and Application Security and Privacy, pages 255-266, March, 2016. (Acceptance rate=19%).

[P31] *Cache, Trigger, Impersonate: Enabling Context-Sensitive Honeyclient Analysis On-the-Wire*. Teryl Taylor, Kevin Snow, Nathan Otterness and Fabian Monrose. In Proceedings of

the $23^{nd}$ ISOC Network and Distributed Systems Security Symposium (NDSS), Feb., 2016. (Acceptance rate=15.4%).

[P32] *Isomeron: Code Randomization Resilient to (Just-in-Time) Return-Oriented Programming*. Luca Davi, Christopher Liebchen, Ahmad-Reza Sadeghi, Kevin Z. Snow, and Fabian Monrose. In Proceedings of the $22^{nd}$ ISOC Network and Distributed Systems Security Symposium (NDSS), Feb., 2015. (Acceptance rate=21%).

[P33] *Watching the Watchers: Inferring TV Content from Outdoor Light Effusions*. Yi Xu, Jan-Michael Frahm and Fabian Monrose. In Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS), November, 2014. (Acceptance rate=19%).

[P34] *Emergent Faithfulness to Morphological and Semantic Heads in Lexical Blends*. Katherine Shaw, Elliott Moreton, Andrew White and Fabian Monrose. In Proceedings of the Annual Meeting on Phonology, February, 2014.

[P35] *Seeing Double: Reconstructing Obscured Typed Input from Repeated Compromising Reflections*. Yi Xu, Jared Heinly, Andrew M. White, Fabian Monrose and Jan-Michael Frahm. In Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS), November, 2013. (Acceptance rate=20%)

[P36] *Check my profile: Leverage static analysis for fast and accurate detection of ROP gadgets*. Blaine Stancill, Kevin Snow, Nathan Otterness, Fabian Monrose, Lucas Davi, and Ahmad-Reza Sadeghi. In Proceedings of the 16th International Symposium on Research in Attacks, Intrusions, and Defenses, October, 2013.

[P37] *Crossing the Threshold: Detecting Network Malfeasance via Sequential Hypothesis Testing*. Srinivas Krishnan, Teryl Taylor, Fabian Monrose and John McHugh. In Proceedings of the $42^{nd}$ Annual IEEE/IFIP International Conferences on Dependable Systems and Networks; Performance and Dependability Symposium, June, 2013.

[P38] *Just-In-Time Code Reuse: On the Effectiveness of Fine-Grained Address Space Layout Randomization*. Kevin Snow, Lucas Davi, Alexandra Dmitrienko, Christopher Liebchen, Fabian Monrose and Ahmad-Reza Sadeghi. In Proceedings of $34^{th}$ IEEE Symposium on Security and Privacy, May, 2013. (**Best Student Paper Award**). (Acceptance rate=12%)

[P39] *Clear and Present Data: Opaque Traffic and its Security Implications for the Future*. Andrew White, Srinivas Krishnan, Michael Bailey, Fabian Monrose and Phil Porras. In Proceedings of the $20^{th}$ ISOC Network and Distributed Systems Security Symposium, Feb., 2013. (Acceptance rate=18.8%)

[P40] *Security and Usability Challenges of Moving-Object CAPTCHAs: Decoding Codewords in Motion*. Yi Xu, Gerardo Reynaga, Sonia Chiasson, Jan-Michael Frahm, Fabian Monrose and Paul van Oorschot. In Proceedings of the $21^{th}$ USENIX Security Symposium, August, 2012. (Acceptance rate=19%)

[P41] *Toward Efficient Querying of Compressed Network Payloads*. Teryl Taylor, Scott E. Coull, Fabian Monrose and John McHugh. In USENIX Annual Technical Conference, June, 2012. (Acceptance rate=18%)

[P42] *iSpy: Automatic Reconstruction of Typed Input from Compromising Reflections*. Rahul Raguram, Andrew White, Dibyendusekhar Goswami, Fabian Monrose and Jan-Michael Frahm. In Proceedings of the $18^{th}$ ACM Conference on Computer and Communications Security (CCS), November, 2011. (Acceptance rate=14%)

[P43] *ShellOS: Enabling Fast Detection and Forensic Analysis of Code Injection Attacks*. Kevin Snow, Srinivas Krishnan, Fabian Monrose and Niels Provos. In Proceedings of the $20^{th}$ USENIX Security Symposium, August, 2011. (Acceptance rate=17%)

[P44] *An Empirical Study of the Performance, Security and Privacy Implications of Domain Name Prefetching*. Srinivas Krishnan and Fabian Monrose. In Proceedings of the $41^{st}$ Annual IEEE/IFIP International Conferences on Dependable Systems and Networks; Dependable Computing and Communications Symposium, June, 2011. (Acceptance rate=17.6%)

[P45] *Amplifying Limited Expert Input to Sanitize Large Network Traces*. Xin Huang, Fabian Monrose, and Michael K. Reiter. In Proceedings of the $41^{st}$ Annual IEEE/IFIP International Conferences on Dependable Systems and Networks; Performance and Dependability Symposium, June, 2011.

[P46] *Phonotactic Reconstruction of Encrypted VoIP Conversations*. Andrew White, Kevin Snow, Austin Matthews and Fabian Monrose. In Proceedings of $32^{nd}$ IEEE Symposium on Security and Privacy, May, 2011. (**Best Paper Award**). (Acceptance rate=11.1%)

[P47] *Towards Optimized Probe Scheduling for Active Measurement Studies*. Daniel Kumar, Fabian Monrose and Michael K. Reiter. In Proceedings of the $6^{th}$ International Conference on Internet Monitoring and Protection (ICIMP), March, 2011 (**Best Paper Award**).

[P48] *On Measuring the Similarity of Network Hosts: Pitfalls, New Metrics, and Empirical Analyses*. Scott Coull, Micheal Bailey and Fabian Monrose. In Proceedings of the $18^{th}$ Annual Network and Distributed Systems Security Symposium, February, 2011. (Acceptance rate=20%)

[P49] *Trail of Bytes: Efficient Support for Forensic Analysis*. Srinivas Krishnan, Kevin Snow, and Fabian Monrose. In Proceedings of the $17^{th}$ ACM Conference on Computer and Communications Security (CCS), November, 2010. (Acceptance rate=17.2%)

[P50] *The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis*. Yinqian Zhang, Fabian Monrose, and Michael K. Reiter. In Proceedings of the $17^{th}$ ACM Conference on Computer and Communications Security (CCS), November, 2010. (Acceptance rate=17.2%)

[P51] *Traffic Classification using Visual Motifs: An Empirical Evaluation*. Wilson Lian, Fabian Monrose and John McHugh. In Proceedings of the $7^{th}$ International Symposium on Visualization for Cyber Security (VizSec), September, 2010.

[P52] *Understanding Domain Registration Abuses*. Scott Coull, Andrew White, Ting-Fang Yen, Fabian Monrose and Michael K. Reiter. In Proceedings of the International Information Security Conference, September, 2010.

[P53] *English Shellcode*. Josh Mason, Sam Small, Greg McManus and Fabian Monrose. In Proceedings of the $16^{th}$ ACM Conference on Computer and Communications Security (CCS), pages 524-533, November, 2009. (Acceptance rate=18.4%)

[P54] *Browser Fingerprinting from Coarse Traffic Summaries: Techniques and Implications*. Ting-Fang Yen, Xin Huang, Fabian Monrose and Michael K. Reiter. In Proceedings of $6^{th}$ Conference on Detection of Intrusions and Malware and Vulnerability Assessment, pages 157-175, July, 2009.

[P55] *Toward Resisting Forgery Attacks via Pseudo-Signatures*. Jin Chen, Dan Lopresti and Fabian Monrose. In Proceedings of $10^{th}$ International Conference on Document Anaalysis and Recognition (ICDAR), July, 2009.

[P56] *The Challenges of Effectively Anonymizing Network Data*. Scott Coull, Fabian Monrose, Michael K. Reiter and Michael Bailey. In Proceedings of the DHS Cybersecurity Applications and Technology Conference for Homeland Security (CATCH), pages 230-236, 2009.

[P57] *Efficient Defenses Against Statistical Traffic Analysis*. Charles Wright, Scott Coull and Fabian Monrose. In Proceedings of Network and Distributed Systems Security, pages 237-250 Feb, 2009. (Acceptance rate=11.7%).

[P58] *Towards Practical Biometric Key Generation with Randomized Biometric Templates*. Lucas Ballard, Seny Kamara, Fabian Monrose, and Michael K. Reiter. In Proceedings of the $15^{th}$ ACM Conference on Computer and Communications Security, pages 235-244. Oct, 2008. (Acceptance rate=$18.2\%$).

[P59] *All Your iFrames point to us: Characterizing the new malware frontier*. Niels Provos, Panayiotis Mavrommatis, Moheeb Rajab, and Fabian Monrose. In Proceedings of the $17^{th}$ USENIX Security Symposium, pages 1-15, July, 2008. (Acceptance rate=$15.9\%$).

[P60] *To Catch a Predator: A Natural Language Approach for Eliciting Protocol Interaction*. Sam Small, Josh Mason, Fabian Monrose, Niels Provos and Adam Stubblefield. In Proceedings of the $17^{th}$ USENIX Security Symposium, pages 171-183, July, 2008. (Acceptance rate=$15.9\%$).

[P61] *Peeking Through the Cloud: DNS-based client estimation techniques and its applications*. Moheeb Rajab, Niels Provos, Fabian Monrose and Andreas Terzis. In Proceedings of the $6^{th}$ Applied Cryptography and Network Security conference (ACNS), pages 21-38, June, 2008.

[P62] *Spot Me If You Can: recovering spoken phrases in encrypted VOIP conversations*. Charles Wright, Lucas Ballard, Scout Coull and Fabian Monrose. In Proceedings of $29^{th}$ IEEE Symposium on Security and Privacy, May, 2008 (17 pages).(Acceptance rate=$11.2\%$).

[P63] *Taming the Devil: Techniques for Evaluating Anonymized Network Data*. Scott Coull, Charles Wright, Angelos Keromytis, Fabian Monrose, and Michael Reiter. In Proceedings of the $15^{th}$ Annual Network and Distributed Systems Security Symposium, pages 125-146, Feb., 2008 (Acceptance rate=$18\%$).

[P64] *On Web Browsing Privacy in Anonymized NetFlows*. Scott Coull, Michael Collins, Charles Wright, Fabian Monrose, and Michael Reiter. In Proceedings of the $16^{th}$ USENIX Security Symposium, pages 339-352, August, 2007. (Acceptance rate=$12.29\%$).

[P65] *Language Identification of Encrypted VoIP Traffic: Alejandra y Roberto or Alice and Bob?* Charles Wright, Lucas Ballard, Fabian Monrose and Gerald Masson. In Proceedings

of the $16^{th}$ USENIX Security Symposium, pages 43-54, August, 2007. (Acceptance rate=12.29%).

[P66] *Towards Valley-free Inter-domain Routing*. Sophie Qiu, Patrick McDaniel and Fabian Monrose. In Proceedings of the IEEE International Conference on Communications, June, 2007. (8 pages)

[P67] *Playing Devil's Advocate: Inferring Sensitive Information from Anonymized Traces*. Scott Coull, Charles Wright, Fabian Monrose, Michael Collins and Michael Reiter. In Proceedings of the $14^{th}$ Annual Network and Distributed Systems Security Symposium (NDSS), pages 35-47, February 2007. (Acceptance rate=15%).

[P68] *A Multifaceted Approach to Understanding the Botnet Phenomenon*. Jay Zarfoss, Moheeb Rajab, Fabian Monrose, and Andreas Terzis. In Proceedings of the ACM SIGCOMM/-USENIX Internet Measurement Conference (IMC), pages 41-52, October, 2006. (Acceptance rate=15.25%).

[P69] *Fast and Evasive Attacks: Highlighting the Challenges Ahead*. Moheeb Rajab, Fabian Monrose, and Andreas Terzis. In Proceedings of the $9^{th}$ International Symposium on Recent Advances in Intrusion Detection (RAID), pages 206-225, September, 2006 (Acceptance rate=17.2%).

[P70] *Biometric Authentication Revisited: Understanding the Impact of Wolves in Sheep's Clothing*. Lucas Ballard, Fabian Monrose, and Daniel Lopresti. In Proceedings of the USENIX Security Symposium, pages 29-41, August 2006 (Acceptance rate=12.3%).

[P71] *On Origin Stability in Inter-Domain Routing*. Sophie Qui, Patrick McDaniel, Fabian Monrose and Aviel D. Rubin. In Proceedings of IEEE International Symposium on Computers and Communications (ISCC), pages 489-496, July, 2006.

[P72] *Memory Bound Puzzles: A Heuristic Approach*. Sujata Doshi, Fabian Monrose and Aviel D. Rubin. In Proceedings of the International Conference on Applied Cryptography and Network Security (ACNS), pages 98-113, June 2006 (Acceptance rate=15.13%).

[P73] *Achieving Efficient Conjunctive Searches on Encrypted Data*. Lucas Ballard, Seny Kamara and Fabian Monrose. In Proceedings of $7^{th}$ International Conference on Information and Communications Security (ICICS), pages 414-426, December, 2005. (Acceptance rate=18%)

[P74] *On the Effectiveness of Distributed Worm Monitoring*. Moheeb Rajab, Fabian Monrose and Andreas Terzis. In Proceedings of $14^{th}$ USENIX Security Symposium, pages 225-237, August, 2005. (Acceptance rate=14.8%)

[P75] *Scalable VPNs for the Global Information Grid*. Bharat Doshi, Antonio De Simone, Fabian Monrose, Samuel Small, and Andreas Terzis. In Proceedings of IEEE MILCOM, May, 2005. (7 pages)

[P76] *An Extensible Platform for Evaluating Security Protocols*. Seny Kamara, Darren Davis, Ryan Caudy and Fabian Monrose. In Proceedings of the $38^{th}$ Annual IEEE Simulation Symposium (ANSS), pages 204-213, April, 2005.

[P77] *Efficient Time Scoped Searches on Encrypted Audit Logs*. Darren Davis, Fabian Monrose, and Michael Reiter. In Proceedings of the $5^{th}$ International Conference on Information and Communications Security (ICICS), pages 532-545, October, 2004. (Acceptance rate=17%)

[P78] *On User-Choice in Graphical Password Systems*. Darren Davis, Fabian Monrose, and Michael Reiter. In Proceedings of the $13^{th}$ USENIX Security Symposium, pages 151-164, August, 2004. (Acceptance rate=12%)

[P79] *Toward Speech-Generated Cryptographic Keys on Resource Constrained Devices*. Fabian Monrose, Micheal Reiter, Daniel Lopresti, Chilin Shih, and Peter Li. In Proceedings of the $11^{th}$ USENIX Security Symposium, pages 283–296, August, 2002. (Acceptance rate=16%)

[P80] *Using Voice to Generate Cryptographic Keys: A Position Paper*. Fabian Monrose, Michael Reiter, Peter Li and Susanne Wetzel. In Proceedings of the 2001: A Speaker Odyssey workshop, pages 237-242, 2001.

[P81] *Cryptographic Key Generation from Voice*. Fabian Monrose, Michael Reiter, Peter Li and Susanne Wetzel. In Proceedings of the $21^{st}$ Annual IEEE Symposium on Security & Privacy, pages 202-212, May 2001. (Acceptance rate=17.75%)

[P82] *Privacy-Preserving Global Customization*. Bob Arlein, Ben Jai, Markus Jakobsson, Fabian Monrose, and Michael Reiter. In Proceedings of the $2^{nd}$ ACM Conference on Electronic Commerce, pages 176-184. April 2000. (Acceptance rate=18%)

[P83] *Password Hardening using Keystroke Dynamics*. Fabian Monrose, Michael K. Reiter and Susanne Wetzel. In Proceedings of the $6^{th}$ ACM Conference on Computer and Communications Security, pages 73-82, November 1999. (Acceptance rate=19.3%)

[P84] *The Design and Analysis of Graphical Passwords*. Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter and Aviel D. Rubin. In Proceedings for the $8^{th}$ USENIX Security Symposium, pages 1-14, August 1999. (**Best Paper Award**). (Acceptance rate=26%)

[P85] *Distributed Execution with Remote Audit*. Fabian Monrose, Peter Wyckoff and Aviel D. Rubin. In Proceedings of the ISOC Network and Distributed Systems Security Symposium (NDSS), pages 103-113, February 1999. (Acceptance rate=24%)

[P86] *Third Party Validation for Java Applications*. Ian Jermyn, Fabian Monrose, and Peter Wyckoff. In Proceedings of the International Conference on Computers and their Applications, March 1998.

[P87] *Authentication via Keystroke Dynamics*. Fabian Monrose and Aviel D. Rubin. In Proceedings of the $4^{th}$ ACM Conference on Computer and Communications Security, pages 48-56, April 1997. (Acceptance rate=26.6%)

**Refereed**
**Journal**
**Publications**

[P88] *Security and Usability Challenges of Moving-Object CAPTCHAs: Decoding Codewords in Motion*. Yi Xu, Gerardo Reynaga, Sonia Chiasson, Jan-Michael Frahm and Fabian Monrose. IEEE Transactions on Dependable and Secure Computing, February, 2014.

[P89] *On the Privacy Risks of Virtual Keyboards: Automatic Reconstruction of Typed Input from Compromising Reflections*. Rahul Raguram, Andrew White, Yi Xu, Jan-Michel Frahm, Pierre Georgel, and Fabian Monrose. IEEE Transactions on Dependable and Secure Computing, Volume 10, Issue 3, pages 154-167, May-June, 2013.

[P90] *Trail of Bytes: New Techniques for Supporting Data Provenance and Limiting Privacy Breaches*. Srinivas Krishnan, Kevin Snow, and Fabian Monrose. IEEE Transactions on Information Forensics and Security, pages 1876-1889, Issue 6, Volume 7, 2012.

[P91] *Understanding Domain Registration Abuses (Invited Paper)*. Scott Coull, Andrew White, Ting-Fang Yen, Fabian Monrose and Michael K. Reiter. Special Issue of Computers & Security (COSE), pages 806-815, Volume 31, Number 7, October, 2012.

[P92] *Uncovering Spoken Phrases in Encrypted Conversations*. Charles Wright, Lucas Ballard, Scott Coull, Fabian Monrose, and Gerald Masson. ACM Transactions on Information and Systems Security (TISSEC), Volume 13, Number 4, pages 1 - 30, December, 2010.

[P93] *Peeking Through the Cloud: Client Density Estimation via DNS Cache Probing*. Moheeb Abu Rajab, Fabian Monrose and Niels Provos. ACM Transactions on Internet Technologies (TOIT), Volume 10, Number 3, October, 2010.

[P94] *Forgery Quality for Behavioral Biometric Security*. Lucas Ballard, Daniel Lopresti and Fabian Monrose. IEEE Transactions on System, Man and Cybernetics, (Special Issue on Biometric Security), pages 1107-1118, December, 2006. (Acceptance rate=18.75%).

[P95] *On Inferring Application Protocol Behaviors in Encrypted Network Traffic*. Charles Wright, Fabian Monrose, and Gerald Masson. Journal of Machine Learning Research (Special Issue on Machine Learning for Computer Security), Volume 7, pages 2745-2769, December, 2006. (Acceptance rate=20%)

[P96] *Password Hardening using Keystroke Dynamics*. Fabian Monrose, Micheal Reiter, and Susanne Wetzel. In Journal of Information Security (IJCS), Volume 1, Number 2, pages 69-83, February 2002.

[P97] *Keystroke Dynamics as a Biometric for Authentication*. Fabian Monrose and Aviel D. Rubin. Future Generation Computing Systems Journal: Security on the Web (Special Issue), pages 351-359, volume 16, March 2000.

**Refereed**
**Workshop**
**Publications**

[P98] *Revisiting the Threat Space for Vision-based Keystroke Inference Attacks*. John Lim, True Price, Fabian Monrose and Jan-Michael Frahm. IEEE Computer Vision and Pattern Recognition Workshops (CVPRW), 2020.

[P99] *Caught Red Handed: Video-based subsequence matching under real-world transformations*. Yi Xu, Jan-Michael Frahm, and Fabian Monrose. IEEE Computer Vision and Pattern Recognition Workshops (CVPRW), 2017.

[P100] *Isn't that Fantabulous: Security, Linguistic and Usability Challenges of Pronounceable Tokens*. Andrew White, Katherine Shaw, Fabian Monrose and Elliott Moreton. In Proceedings of the New Security Paradigms Workshop (NSPW), September, 2014. (Acceptance rate=32%).

[P101] *Automatic Hooking for Forensic Analysis of Document-based Code Injection Attacks: Techniques and Empirical Analyses*. Kevin Snow and Fabian Monrose. In Proceedings of the European Workshop on System Security (EuroSec), April, 2012. (6 pages).

[P102] *DNS Prefetching and Its Privacy Implications*. Srinivas Krishnan and Fabian Monrose. In Proceedings of the 3rd USENIX Workshop on Large-Scale Exploits and Emergent Threats, April, 2010. (9 pages)

[P103] *Secure Recording of Accesses to a Protected Datastore*. Srinivas Krishnan and Fabian Monrose. In Proceedings of the 2nd ACM Workshop on Virtual Machine Security (VMSec), pages 23-32, November, 2009.

[P104] *My Botnet is Bigger than Yours (Maybe, Better than Yours): Why size estimates remain challenging*. Moheeb Rajab, Jay Zarfoss, Fabian Monrose and Andreas Terzis. In Proceedings of USENIX Workshop on Hot Topics in Understanding Botnets, April, 2007 (Acceptance rate=$32.4\%$) (8 pages).

[P105] *Using Visual Motifs to Classify Encrypted Traffic*. Charles Wright, Fabian Monrose and Gerald Masson. In Proceedings of the ACM Workshop of Visualization for Computer Security (VizSEC), November, 2006 (Acceptance rate=$34\%$) (8 pages).

[P106] *On the Impact of Dynamic Addressing on Malware Propagation*. Moheeb Rajab, Fabian Monrose, and Andreas Terzis. In Proceedings of the $4^{th}$ ACM Workshop of Recurring Malcode (WORM), November, 2006 (Acceptance rate=$29\%$) (8 pages)

[P107] *Efficient Techniques for Detecting False Origin Advertisements in Inter-domain Routing*. Sophie Qui, Patrick McDaniel, Fabian Monrose, and Andreas Terzis. In Proceedings of the $2^{nd}$ Workshop on Secure Network Protocols, pages 12-19, November 2006. (Acceptance rate=$40\%$).

[P108] *Evaluating the Security of Handwriting Biometrics*. Lucas Ballard, Daniel Lopresti and Fabian Monrose. In Proceedings of the $10^{th}$ International Workshop on Frontiers in Handwriting Recognition, pages 461-466, October, 2006 (Acceptance rate=$28.5\%$).

[P109] *Worm Evolution Tracking via Timing Analysis*. Moheeb Rajab, Fabian Monrose and Andreas Terzis. In Proceedings of the $3^{rd}$ ACM Workshop on Recurring Malware (WORM), pages 52-59, November, 2005 (Acceptance rate=$25\%$).

[P110] *HMM Profiles for Network Traffic Classification (extended Abstract)*. Charles Wright, Fabian Monrose and Gerald Masson. In Proceedings of ACM Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC), pages 9-15, October, 2004.

**Book Chapters**

[B1] *Graphical Passwords (revisited)*. Fabian Monrose and Micheal Reiter. *Security and Usability: Designing Security Systems That People Can Use*. Editors: Lorrie Cranor and Simson Garfinkel. OReilly & Associates, 2005.

**Other Manuscripts**

[M111] *Towards Stronger User Authentication*, Ph.D. Thesis. Fabian Monrose. Courant Institute of Mathematical Sciences, New York University, May 1999.

[M112] *Correlation Resistant Storage*. Lucas Ballard, Mathew Green, Breno *de* Medeiros and Fabian Monrose. Cryptology ePrint Archive Report 2005/417.

[M113] *Evaluating Biometric Security (Invited Paper)*. Daniel Lopresti, Lucas Ballard and Fabian Monrose. In Proceedings of the $1^{st}$ Korea-Japan Workshop on Pattern Recognition, November 2006. (6 pages)

[M114] *Biometric Key Generation using Pseudo-Signatures* (Poster Presentation). Lucas Ballard, Jin Chen, Daniel Lopresti and Fabian Monrose. In International Conference on Frontiers of Handwriting Recognition, Feb. 2008 (8 pages).

[M115] *Masquerade: Simulating a Thousand Victims* Sam Small, Josh Mason, Ryan MacArthur. In ;login: The USENIX Magazine, December 2008.

**[G]: Teaching Activities**

- *Advanced Computer Security*, Fall 2023, 16 students.
- *Introduction to Computer Security*, Spring 2022, 59 students.
- *Computer and Network Forensics*, Spring 2021, 13 students.
- *Technical Communications and Writing in Computer Science*, Spring 2021, 14 students.
- *Introduction to Computer Security*, Fall 2020, 19 students.
- *Technical Communications and Writing in Computer Science*, Spring 2020, 18 students.
- *Introduction to Computer Security*, Spring 2019, 34 students.
- *Introduction to Computer Security*, Spring 2017, 48 students.
- *Computer Forensics*, Fall 2016, 14 students.
- *Introduction to Computer Security*, Spring 2016, 43 students.
- *Introduction to Computer Security*, Spring 2015, 30 students.
- *Introduction to Computer Security*, Spring 2012, 26 students.
- *Network Security*, Fall 2008, 21 students.

- *Special Topics in Computer Science*, Spring 2009, 7 students.
- *Network Security*, Fall 2009, 16 students.
- *Introduction to Computer Security*, Spring 2010, 17 students.
- *Network Security*, Fall 2010, 11 students.
- *Introduction to Computer Security*, Spring 2012, 25 students.

**Ph.D. Students**

- Sophie Qui (co-advised with G. Mason), Ph.D., Spring 2007, (*Cisco Systems*)
- Charles Wright, Spring 2008, Ph.D., (*Portland State University*)
- Seny Kamara, Spring 2008, Ph.D., (*Brown University*)
- Moheeb Abu Rajab (co-advised with A. Terzis), Ph.D., Spring 2008, (*Google Inc.*)
- Lucas Ballard, Spring 2008, Ph.D., (*Google Inc.*)
- Scott Coull, Fall 2009, Ph.D., (*RedJack*)
- Josh Mason, Fall 2009, Ph.D., (*Research Professor, UIUC*)
- Kevin Snow, Spring 2014, Ph.D., *Zeropoint Dynamics*
- Andrew White, Fall 2015, Ph.D., *Netflix*
- Teryl Taylor, Summer 2016, Ph.D., *IBM TJ Watson*
- Srinivas Krishnan (co-advised with K. Jeffay; deferred), *Google*
- Yi Xu (co-advised with Jan-Michael Frahm), *Snapchat*
- John Lim (co-advised with Jan-Michael Frahm) *Salesforce*
- Mac Malone (*Lean*)
- Kedrian James
- Yufei Du
- Kevin Valakuzhy (co-advised with M. Antonakakis)
- James Fullwood
- Vinny Adjibi (co-advised with M. Antonakakis)

**Doctoral Committees**

- (**Reader**) Breno de Medeiros, *New Cryptographic Primitives and Applications*, Ph.D., Johns Hopkins University, May 2004

- (**Reader**) Kendall Giles, *Knowledge Discovery in Computer Network Data: A Security Perspective*, Ph.D., Johns Hopkins University, October, 2006
- (**Advisor**) Sophie Qui, *Towards Stable, Reliable and Policy-Compliant Inter-domain Routing*, Ph.D., Johns Hopkins University, May, 2007
- (**Reader, external examiner**) Julie Thorpe, *On the Predictability and Security of User Choice in Passwords*, Ph.D., Carleton University, Fall, 2007
- (**Reader**) Sujata Doshi, *New Techniques to Defend Against Computer Security Attacks*, Ph.D., Johns Hopkins University, October, 2008
- (**Advisor**) Charles Wright, *On Information Leakage Attacks in Encrypted Network Traffic*, Ph.D., Johns Hopkins University, 2008
- (**Advisor**) Seny Kamara, *Improved Definitions and Efficient Constructions for Secure Obfuscation*, Ph.D., Johns Hopkins University, 2008
- (**Advisor**) Lucas Ballard, *Robust Techniques for Evaluating Biometric Cryptographic Key Generators*, Ph.D., Johns Hopkins University, 2008
- (**Co-Advisor**) Moheeb Abu Rajab, *Towards a Better Understanding of Internet-Scale Threats*, Ph.D., Johns Hopkins University, 2008
- (**Advisor**) Joshua Mason, *Towards Stronger Adversarial Threat Models in Systems Security*, Ph.D., Johns Hopkins University, June, 2009
- (**Advisor**) Scott Coull, *Methods for Evaluating the Privacy of Anonymized Network Data*, Ph.D., Johns Hopkins University, 2009
- (**Reader, external examiner**) Lu Liming, *Traffic Monitoring and Analysis for Source Identification*, Ph.D., Singapore University, Spring, 2011
- (**Reader, external examiner**) M. Antonakakis, *Improving Internet Security via Large-Scale Passive and Active DNS Monitoring*, Ph.D., Georgia Institute of Technology, Spring, 2012
- (**Reader**) Y. Song, *A Behavior-based Approach Towards Statistics-Preserving Network Trace Anonymization*, Ph.D., Columbia University, Spring, 2012
- (**Reader**) V. Pappas, *Defending Against Return-Oriented Programming*, Ph.D., Columbia University, Spring, 2014
- (**Advisor**) Kevin Z. Snow, *Identifying Code Injection and Code Reuse Payloads in Memory Error Exploits*, Ph.D., University of North Carolina at Chapel Hill, Fall, 2014.
- (**Advisor**) Andrew M. White, *Practical Analysis of Encrypted Network Traffic*, Ph.D., University of North Carolina at Chapel Hill, Fall, 2015.
- (**Co-Advisor**) Yi Xu, *Toward Robust Video Event Detection and Retrieval Under Adversarial Constraints*, Ph.D., University of North Carolina at Chapel Hill, Spring, 2016.
- (**Advisor**) Teryl Taylor, *Using Context to Improve Network-based Malware Detection*, Ph.D., University of North Carolina at Chapel Hill, Summer, 2016.

- (**Reader**) Dennis Bueno, *Automated Software Security Analysis Using Control and Data Abstractions*, Ph.D., University of Michigan, 2017.
- (**Reader**) Tracey John, *Virtual Career Advisor System*, MPhil., University of the West Indies, Barbados, 2017.
- (**Reader**) Louis Soleyn, *Software Techniques for Implementing Dynamic, Network-Aware, Energy-Efficient Mobile Applications*, MPhil., University of the West Indies, Barbados, 2018.
- (**Reader**) Chaz Lever, *Empirical Analysis of Existing and Emerging Threats at Scale Using DNS*, Georgia Institute of Technology, Fall, 2017.
- (**Reader, external examiner**) Adrian Tang, *Security Engineering of Hardware-Software Interfaces*, Columbia University, Spring, 2018.
- **(Reader) Calvin Deutschbein,** *Mining Secure Behavior of Hardware Designs*, **UNC Chapel Hill, July, 2021.**
- **(Reader) Tapti Palit,** *Sensitive Data Encryption: A Scalable Defense against Sensitive Data Leakage*, **Stony Brook University, October, 2021.**
- **(Reader, external examiner) Salman Ahmed,** *Quantitative Metrics and Measurement Methodologies for System Security Assurance*, **Virginia Tech, Dec, 2021.**
- **(Reader) Omar Alrawi,** *Security and Threat Evaluation of Smart Home Technology*, **Georgia Institute of Technology, July, 2022.**
- **(Advisor) Mac Malone,** *Improving Student Engagement and Learning Outcomes with a Gamified Learning Platform*, **Ph.D., University of North Carolina at Chapel Hill, May, 2023.**
- **(Reader) Evan Downing,** *Improving the Understanding of Malware Using Machine Learning*, **Georgia Institute of Technology, December 2023.**
- **(Advisor) Kedrian James,** *Improving Software Security Triage and Remediation*, **Ph.D., University of North Carolina at Chapel Hill, May, 2024.**
- **(Reader) Kevin Hutto,** *Remote Sensor Security Through Encoded Computation and Cryptographic Signatures*, **Ph.D., Georgia Institute of Technology, May, 2024.**
- **(Reader) Matthew Pruett,** *A Framework for Analyzing Undefined Behavior in C Software*, **Georgia Institute of Technology, 2025 (expected)**
- **(Reader) Miuyin M. Wong,** *Narrowing the Gap between Research and Practice through the Understanding of Malware Analysis Workflows*, **Georgia Institute of Technology, 2024 (expected)**

**BS/MS**
**Advisees**

- Wilson Lian, *Traffic Classification using Visual Motifs*, University of North Carolina at Chapel Hill, Honors Thesis, 2010.
- Austin Matthews, *Phonetic Edit Distance: New Techniques and Empirical Analyses*, University of North Carolina at Chapel Hill, Honors Thesis, 2011.

- Chris Allen, *WarFlying: Creating Aerial WiFi-maps using Custom Drones*, University of North Carolina at Chapel Hill, Honors Thesis, 2013.
- Rob Dallara, *On the (In)effectiveness of Execute-no-Read (XNR) as a Defense against Just-in-Time Code Reuse Attacks.* University of North Carolina at Chapel Hill, Comprehensive paper, 2015.
- Micah Moreton, *Detecting Potential for Server-side Data-oriented Attacks*, University of North Carolina at Chapel Hill, 2017
- Roman Rogowski, *Revisiting Browser Security in the Modern Era*. University of North Carolina at Chapel Hill, Comprehensive paper, 2017.
- Boo Fullwood, *Revisiting Charger-based Side Channel Password Inference Attacks*. University of North Carolina at Chapel Hill, Comprehensive paper, 2022.
- Kevin Lane, *Cloud-based Architectures for Detecting VoIP Scams*. University of North Carolina at Chapel Hill, Comprehensive paper, 2022.

**[H]:**
**Service**

- **ECE PhD Admissions committee (Chair for Software & Systems TIG),** **2024**
- $14^{th}$ **ACM Conference on Data and Application Security and Privacy,** **2024**
- **ECE PhD Admissions committee (Chair for Software & Systems TIG),** **2023**
- **Faculty Recruiting Committee member, School of Cybersecurity & Privacy,** **2023**
- $13^{th}$ **ACM Conference on Data and Application Security and Privacy,** **2023**
- $29^{th}$ **Annual Computer Security Applications Conference,** **2021**
- $41^{st}$ IEEE Symposium on Security and Privacy, 2020
- $40^{th}$ IEEE Symposium on Security and Privacy, 2019
- $20^{th}$ Symposium on Research in Attacks and Defenses, 2018
- CVPR Workshop on Computer Vision and Computer Security, 2017
- $18^{th}$ Symposium on Research in Attacks and Defenses, (**Chair**), 2016
- $1^{st}$ IEEE APWG Symposium on Electronic Crime Research (eCrime), 2016
- ACM Workshop on Information Sharing and Collaborative Security, 2015
- $17^{th}$ Symposium on Research in Attacks and Defenses, (**Co-Chair**), 2015
- DARPA Information Science and Technology (ISAT) advisory group 2014
- $9^{th}$ USENIX Workshop on Hot Topics in Security (**Co-Chair**) 2014
- $16^{th}$ Symposium on Research in Attacks and Defenses, 2014

- $15^{th}$ Symposium on Research in Attacks and Defenses, (**General Chair**), 2013
- $22^{nd}$ USENIX Security Symposium, 2013
- $20^{th}$ ACM Conference on Computer and Communications Security, 2013
- $11^{th}$ International Conference on Cryptography and Network Security 2012
- NSF Secure and Trustworthy Cyberspace Panelist, 2012
- $15^{th}$ International Symposium on Recent Advances in Intrusion Detection 2012
- $12^{th}$ Annual Digital Forensics Research Conference 2012
- $16^{th}$ Financial Cryptography and Data Security 2012
- $6^{th}$ USENIX Workshop on Hot Topics in Security 2011
- NSF Cyber Trust panelist, 2006—2009, 2011
- $11^{th}$ Annual Digital Forensics Research Conference 2011
- $18^{th}$ ACM Conference on Computer and Communications Security 2011
- $17^{th}$ ACM Conference on Computer and Communications Security 2010
- $14^{th}$ Financial Cryptography and Data Security 2010
- $30^{th}$ International Conference on Distributed Computing Systems 2010
- $16^{th}$ ACM Conference on Computer and Communications Security 2009
- $18^{th}$ USENIX Security Symposium, (**Program Chair**) 2009
- $16^{th}$ Annual Network and Distributed Systems Security Symposium 2009
- $29^{th}$ International Conference on Distributed Computing Systems 2008
- $17^{th}$ USENIX Security Symposium 2008
- $29^{th}$ Annual IEEE Symposium on Security and Privacy 2008
- $15^{th}$ Annual Network and Distributed Systems Security Symposium 2008
- $1^{st}$ USENIX Workshop on Large-scale Exploits & Emergent Threats, (**Program Chair**) 2008
- $6^{th}$ IEEE Biometrics Symposium 2008
- $14^{th}$ Annual Network and Distributed Systems Security Symposium 2007
- $2^{nd}$ USENIX Workshop on Hot Topics in Security 2007
- $10^{th}$ Information Security Conference 2007
- $1^{st}$ USENIX Workshop on Hot Topics in Understanding Botnets 2007
- $16^{th}$ USENIX Security Symposium 2007

- $28^{th}$ Annual IEEE Symposium on Security and Privacy 2007
- NSF Exploratory Research panelist, 2006–2007
- $15^{th}$ USENIX Security Symposium 2006
- $4^{th}$ ACM Workshop of Recurring Malware 2006
- $13^{th}$ Annual Network and Distributed Systems Security Symposium 2006

**Editorial/Advisory Boards**

- Johns Hopkins Information Security Institute Advisory Board 2016–*present*
- ACM Transactions of Information and System Security 2006 — *2009*

**Organizing & Steering Committees**

- *Steering Committee*, Research in Attacks, Intrusions and Defenses (RAID) 2016 - 2019
- *General and Local Chair*, Research in Attacks, Intrusions and Defenses (RAID) 2013
- *Local Arrangements Chair*, Financial Cryptography and Data Security 2011
- *Steering Committee*, USENIX Security Symposium 2012-2015
- *Steering Committee*, Network & Distributed Systems Security Symposium 2007-10
- *Steering Committee*, USENIX Wksh. on Large-scale Exploits & Emergent Threats 2009-2014
- *Publicity Chair*, ACM Workshop on Rapid Malcode, Arlington 2006
- *Co-organizer,* DIMACS Workshop on Security and Usability, Rutgers 2004

**Patents / Provisional Filings**

[F1] Jan Werner, Rob Dallara, George Baltas, Michalis Polychronakis, Kevin Snow and Fabian Monrose. *Methods, Systems, and Computer Readable Media for Preventing Code Reuse Attacks.* U.S. Patent No. 10,628,589, April, 2020.

[F2] Xin Hu, Jiyong Jang, Fabian Monrose, Marc Philippe Stoecklin, Teryl Taylor and Ting Wang. *Detecting Web Exploit Kits by Tree-based Structural Similarity Search*. U.S. Patent 10,560,471, Feb, 2020.

[F3] T. Taylor, K. Snow, N. Otterness, and F. Monrose. *Methods, systems, and computer readable media for detecting malicious network traffic*, U.S. Patent No. 9,992,217, June 2018.

[F4] Srinivas Krishnan, Fabian Monrose, Michael Bailey, Phillip Porras, and Andrew White. *Methods, Systems, and Computer Readable Media for Rapid Filtering of Opaque Data Traffic*, U.S. Patent No. 9,973,473, May 2018.

[F5] S. Krishnan, T. Taylor, F. Monrose and J. McHugh. *Methods, Systems, and Computer Readable Media for Detecting Compromised Computing Hosts*. U.S. Patent No. 9,934,379, April 2018.

[F6] S. Krishnan, K. Snow, and F. Monrose. *Methods, Systems, and Computer Readable Media for Efficient Computer Forensic Analysis and Data Access Control*. U.S. Patent No. 9,721,089, August 2017.

[F7] Keven Z. Snow, Fabian Monrose and Srinivas Krishnan. *Methods, Systems, and Computer Readable Media for Detecting Injected Machine Code*. U.S. Patent 9,305,165, April 5, 2016.

[F8] Fabian Monrose, Teryl Taylor, Srinivas Krishnan and John McHugh. United States Patent Application Serial No. 14/773,660 for *Methods, Systems, and Computer Readable Media for Detecting a Compromised Computing Host*, March, 2015.

[F9] Robert Arlein, Ben Jai, Markus Jakobsson, Fabian Monrose and Michael Reiter. *Method & Apparatus for Providing Privacy-preserving Global Customization*. U.S. Patent No. 7,107,269, September, 2006.

[F10] Phil L. Bohannon, Markus Jakobsson, Fabian Monrose, Michael K. Reiter and Susanne Wetzel. *Generation of Repeatable Cryptographic Keys Based on Varying Parameters.* U.S. Patent No. 6,901,145, May 31, 2005.

[F11] Markus Jakobbson and Fabian Monrose. *System & Apparatus for Incorporating Advertising into Printed Images*. U.S. Patent No. 6,873,424, March, 2005.

**Expert Testimony**

[G1] Apple Inc. v. VirnetX Inc., Case IPR2014-00237/238, Patent 8,504,697, Expert Testimony at Deposition, October, 2014, Washington D.C.

[G2] Apple Inc. v. VirnetXInc., Case IPR2014-00403/404, Patent 7,987,274 B2, Expert Testimony at Deposition, February, 2015, Washington D.C.

[G3] Apple Inc. v. VirnetX Inc., Case IPR2015-00871, IPR2014-00482/483 Patent 7,987,274 Expert Testimony at Deposition, March, 2015, Washington D.C.

[G4] Apple Inc. v. VirnetX Inc., Case IPR2015-01009, Patent 8,843,643, Expert Testimony at Deposition, April, 2015, Washington D.C.

[G5] Apple Inc. v. VirnetX Inc., Case IPR2016-00331/332, Patent 8,504,696 B2 Expert Testimony at Deposition, December, 2015, Washington D.C.

[G6] Apple Inc. v. VirnetX Inc., Case IPR2016-01585, Patent 8,904,516 Expert Testimony at Deposition, August, 2016, Washington D.C.

[G7] Apple Inc. v. VirnetX Inc., Case IPR2015-1046, Patent 6,502,135 Expert Testimony at Deposition, September, 2016, Washington D.C.

[G8] Apple Inc. v. VirnetX Inc., Case IPR2017-00337, Patent 9,038,163 Expert Testimony at Deposition, November, 2016, Washington D.C.

[G9] Google Inc. v. Uniloc 2017 LLC., Patent 8,949,954, Declaration, January, 2020, Washington D.C.