

Scott E. Coull

<http://www.scottcoull.com/>

EDUCATION

Johns Hopkins University, Baltimore, MD

Ph.D., Computer Science, May 2009

- Thesis: Methods for Evaluating the Privacy of Anonymized Network Data
- Advisor: Professor Fabian Monrose

Rensselaer Polytechnic Institute, Troy, NY

M.S., Computer Science, June 2005

- Thesis: Sequence Alignment for Masquerade Detection
- Advisor: Professor Boleslaw K. Szymanski

B.S., Computer Science, December 2003

- *magna cum laude*
- Minor in Information Technology

PROFESSIONAL EXPERIENCE

Mandiant, Reston, VA

Director, Data Science Research

Sr. Manager, Data Science

Principal Data Scientist

Senior Staff Data Scientist

April 2021 to Present

January 2019 to March 2021

January 2018 to December 2018

January 2017 to December 2017

- Led an international team of ten machine learning researchers to develop solutions for security problems across the entire range of products and services
- Led research and development of MalwareGuard, a next-generation anti-virus system using machine learning
 - Deployed to more than 2M customer endpoints
 - Responsible for more than \$25M in additional revenue
 - Won several industry/government awards
- Initiated FireEye's university sponsored research program and on-boarded first university research group
- Created a top-tier research program focusing on adversarial machine learning and novel uses of machine learning for security problems
- Created the Data Science 101 curriculum for FireEye and taught the course to more than two hundred students internationally
- Developed innovative internal initiatives for sharing data science resources, managing research projects, and expanding the reach of the FireEye Data Science group

RedJack, LLC., Silver Spring, MD

Senior Research Scientist

Research Scientist

October 2015 to December 2016

June 2010 to September 2015

- Captured and managed more than \$1.2M of new research funding as PI, additional \$16M as key personnel
- Developed new cryptographic primitives and network traffic generation techniques to enable censorship circumvention
- Analyzed information leakage from encrypted mobile messaging applications, including iMessage and WhatsApp
- Applied NLP methods to find indicators of child exploitation within Tor hidden services and characterize communication patterns
- Lead effort to develop privacy guidelines to safely share computer network data for DHS PREDICT and FCC Measuring Mobile Broadband
- Mentored graduate students and junior researchers

University of North Carolina, Chapel Hill, NC

Postdoctoral Research Associate

May 2009 to August 2010

- Investigated role of semantics and temporal information in the development of robust similarity metrics for network behaviors with applications to traffic analysis and privacy measurement
- Designed a malleable digital signature scheme for efficiently signing sets and intervals with applications to non-interactive agreement protocols distributed systems
- Mentored and supervised graduate students on research projects

Johns Hopkins University, Baltimore, MD

Research Assistant

January 2008 to May 2009

- Evaluated channels of information leakage in sanitized network data using machine learning techniques
- Developed information-theoretic tools for analyzing the privacy and utility of sanitized network data
- Studied information leakage in encrypted Voice over IP (VoIP) protocols, as well as efficient countermeasures

Teaching Assistant

August 2005 to December 2007

- Lead Teaching Assistant for: Data Structures, Automata Theory, Programming Languages, Computer Forensics, and Network Security
- Prepared and presented lectures, provided supplemental instruction to students
- Supervised grading of and provided solutions to tests, projects, and homework

Sandia National Laboratories, Livermore, CA

Summer Research Intern

June 2006 to August 2006

- Developed a multi-scale anomaly detection system to detect data exfiltration and stealthy scans using unsupervised clustering methods
- Performed red team exercises on collaboration and network security devices

Rensselaer Polytechnic Institute, Troy, NY

Teaching Assistant

January 2004 to May 2005

- Teaching Assistant for: Operating Systems, and The Human-Computer Interface
- Provided supplemental instruction to students
- Supervised grading of and provided solutions to tests, projects, and homework

FX Technologies, LLC, Troy, NY

Consultant

October 2000 to December 2018

- Designed and implemented security and disaster recovery systems for clients
- Provided project proposals and designed networks based on client needs
- Performed security audits to assess client network security needs

Travelers Insurance, Hartford, CT

Summer Intern - Information Systems Security

May 2001 to August 2001

Summer Intern - Mainframe Operations Group

June 2000 to August 2000

AWARDS &
CERTIFICATIONS

International Information Systems Security Certification Consortium (ISC²)

- Certified Information Systems Security Professional (CISSP), 2012-2024

Privacy Enhancing Technologies (PET) Award

- Outstanding Research in Privacy Enhancing Technologies, Runner-up, 2014

Computing Research Association

- Computing Innovation Fellowship (Award Rate: 11.4%), 2009-2010

Rensselaer Polytechnic Institute

- Stanley I. Landgraf Prize for Outstanding Academic Achievement, 2004
- Founder's Award of Excellence, 2003
- Upsilon Pi Epsilon Computer Science Honor Society, 2002
 - Chapter Secretary, 2002-2004

19th Annual Computer Security Application Conference

- Best Student Paper Award, 2003

PROFESSIONAL
SERVICE

Program Committees:

International Conference on Information Systems Security (2009); ISOC Network and Distributed Systems Security Symposium (2010); International Symposium on Stabilization, Safety, and Security of Distributed Systems (2010); ACM Workshop on Information Sharing and Collaborative Security (2014, 2015, 2016); USENIX Workshop on Offensive Technologies (2016, 2017); ACM Conference on Computer and Communications Security (2017); Privacy Enhancing Technologies Symposium (2018, 2019, 2020, 2022); ACM Workshop on Artificial Intelligence and Security (2019, 2020, 2021, 2022); USENIX Security Symposium (2017,2021); ESORICS (2021, 2022); IEEE Deep Learning & Security (2022)

External Reviewer – Conferences:

ISOC Network and Distributed Systems Security Symposium; IEEE Symposium on Security and Privacy; USENIX Security Symposium, Information Security Conference; IACR CRYPTO; ACM Conference on Computer and Communications Security; IACR Pairings; International Conference on Cryptology and Network Security; IACR Theory of Cryptography Conference; Privacy Enhancing Technologies Symposium

External Reviewer – Journals:

ACM Transactions on Information and Systems Security; ACM Transactions on Internet Technology; IEEE Transactions on Systems, Man, and Cybernetics; SIGCOMM Computer Communications Review; ACM/IEEE Transactions on Networking; IEEE Transactions on Dependable and Secure Computing; IEEE Transactions on Wireless Communications; IEEE Transactions on Mobile Computing; Communications of the ACM

BOOK CHAPTERS

[B1] S. Coull. “*Traffic Analysis.*” In H. van Tilborg and S. Jajodia (Eds.) *Encyclopedia of Cryptography and Security.* Springer Publishing. 2011. pp. 1311-1313.

JOURNAL
PUBLICATIONS

[J7] L. Demetrio, S. Coull, B. Bigio, G. Lagorio, A. Armando, and F. Roli. “*Adversarial EXEMples: A Survey and Experimental Evaluation of Practical Attacks on Machine Learning for Windows Malware Detection.*” *ACM Transactions on Privacy and Security (TOPS)*, 24(4), September, 2021.

[J6] S. Coull and K. Dyer. “*Traffic Analysis of Encrypted Messaging Services: Apple iMessage and Beyond.*” *ACM SIGCOMM Computer Communications Review*, 44(4), October, 2014.

[J5] S. Coull, A. White, T. F. Yen, F. Monrose, and M. Reiter. “*Understanding Domain Registration Abuses.*” *Computers & Security*, 31(7), October, 2012. pp. 806-815. (Invited Paper)

[J4] S. Coull, M. Green, and S. Hohenberger. “*Access Controls for Oblivious and Anonymous Systems.*” *ACM Transactions on Information and Systems Security*, 14(1), May, 2011. pp. 1-28.

[J3] C. Wright, L. Ballard, S. Coull, F. Monrose, and G. Masson. “*Uncovering Spoken Phrases in Encrypted Voice over IP Conversations.*” *ACM Transactions on Information and Systems Security*, 13(4), December, 2010. pp. 1-30.

[J2] S. Coull and B. Szymanski. “*On the Development of an Internet-Centric Defense for Scanning Worms.*” *Computers & Security*, 28(7), October, 2009. pp. 637-647.

- [J1] S. Coull, and B. Szymanski. “*Sequence Alignment for Masquerade Detection.*” Computational Statistics and Data Analysis, 52(8), April, 2008. pp. 4116-4131.
- [C19] S. Rahman, S. Coull, M. Wright. “*On the Limitations of Continual Learning for Malware Classification.*” In Proceedings of the 1st Conference on Lifelong Learning Agents, August 2022.
- [C18] G. Severi, J. Meyer, S. Coull, and A. Oprea. “*Explanation-Guided Backdoor Poisoning Attacks Against Malware Classifiers.*” In Proceedings of the 30th USENIX Security Symposium, August 2021. (Acceptance rate: 18.7%)
- [C17] K. Dyer, S. Coull, and T. Shrimpton. “*Marionette: A Programmable Network-Traffic Obfuscation System.*” In Proceedings of the 24th USENIX Security Symposium, August, 2015. (Acceptance rate: 15.7%)
- [C16] S. Coull and E. Kenneally. “*Toward a Comprehensive Disclosure Control Framework for Shared Data.*” In Proceedings of the IEEE International Conference on Technologies for Homeland Security, November, 2013.
- [C15] K. Dyer, S. Coull, T. Ristenpart, and T. Shrimpton. “*Protocol Misidentification Made Easy with Format-Transforming Encryption.*” In Proceedings of the 20th ACM Conference on Computer and Communications Security, November, 2013. (Acceptance rate: 19.8%, 2014 PET Award Runner-up)
- [C14] T. Taylor, S. Coull, F. Monrose, and J. McHugh. “*Toward Efficient Querying of Compressed Network Payloads.*” In Proceedings of the USENIX Annual Technical Conference, June, 2012. (Acceptance rate: 14.1%)
- [C13] K. Dyer, S. Coull, T. Ristenpart, and T. Shrimpton. “*Peek-a-boo, I Still See You: Why Efficient Traffic Analysis Countermeasures Fail.*” In Proceedings of the 33rd IEEE Symposium on Security and Privacy, May, 2012. (Acceptance rate: 13%)
- [C12] L. Wei, S. Coull, and M. Reiter. “*Bounded Vector Signatures and their Applications.*” In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS '11), March, 2011. pp. 277-285. (Acceptance rate: 16.1%)
- [C11] S. Coull, F. Monrose, and M. Bailey. “*On Measuring the Similarity of Network Hosts: Pitfalls, New Metrics, and Empirical Analyses.*” In Proceedings of the 18th Annual Network and Distributed Systems Security Symposium, February, 2011. (Acceptance rate: 20.1%)
- [C10] S. Coull, A. White, T. F. Yen, F. Monrose, and M. Reiter. “*Understanding Domain Registration Abuses.*” In Proceedings of the 25th IFIP International Information Security Conference, September, 2010. pp. 68-79. (Acceptance rate: 24.5%)
- [C9] S. Coull, M. Green, and S. Hohenberger. “*Controlling Access to an Oblivious Database using Stateful Anonymous Credentials.*” In Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography (PKC), March, 2009. pp. 501-520. (Acceptance rate: 25%)
- [C8] S. Coull, F. Monrose, M. Reiter, and M. Bailey. “*The Challenges of Effectively Anonymizing Network Data.*” In Proceedings of the DHS Cybersecurity Applications and Technology Conference for Homeland Security (CATCH), March, 2009. pp. 230-236.

[C7] C. Wright, S. Coull, and F. Monroe. “*Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis.*” In Proceedings of the 16th Annual Network and Distributed Systems Security Symposium, February, 2009. pp. 237-250. (Acceptance rate: 11.7%)

[C6] C. Wright, L. Ballard, S. Coull, F. Monroe, and G. Masson. “*Spot Me If You Can: Uncovering Spoken Phrases in Encrypted VoIP Conversations.*” In Proceedings of the 29th IEEE Symposium on Security and Privacy, May, 2008. pp. 35-49. (Acceptance rate: 11.2%)

[C5] S. Coull, C. Wright, A. Keromytis, F. Monroe, and M. Reiter. “*Taming the Devil: Techniques for Evaluating Anonymized Network Data.*” In Proceedings of the 15th Annual Network and Distributed Systems Security Symposium, February, 2008. pp. 125-135. (Acceptance rate: 17.8%)

[C4] S. Coull, M. Collins, C. Wright, F. Monroe, and M. Reiter. “*On Web Browsing Privacy in Anonymized NetFlows.*” In Proceedings of the 16th USENIX Security Symposium, August, 2007. pp. 339-352. (Acceptance rate: 12.3%)

[C3] S. Coull, C. Wright, F. Monroe, M. Collins, and M. Reiter. “*Playing Devil’s Advocate: Inferring Sensitive Information from Anonymized Network Traces.*” In Proceedings of the 14th Annual Network and Distributed Systems Security Symposium, February, 2007. pp. 35-47. (Acceptance rate: 15%)

[C2] S. Coull and B. Szymanski. “*On the Development of an Internetwork-Centric Defense for Scanning Worms.*” In Proceedings of the 40th Annual Hawaiian International Conference on System Sciences, Waikoloa, HI, January, 2007.

[C1] S. Coull, J. Branch, B. Szymanski and E. Breimer. “*Intrusion Detection: A Bioinformatics Approach.*” In Proceedings of the 19th Annual Computer Security Applications Conference, Las Vegas, NV, December, 2003. pp. 24-33. (Best Student Paper Award)

WORKSHOP
PAPERS

[W3] S. Coull and C. Gardner. “*Activation Analysis of a Byte-Based Deep Neural Network for Malware Classification.*” In Proceedings of the 2nd Deep Learning and Security Workshop (DLS), San Francisco, CA, May 2019.

[W2] O. Suci, S. Coull, and J. Johns. “*Exploring Adversarial Examples in Malware Detection.*” In Proceedings of the In Proceedings of the 2nd Deep Learning and Security Workshop (DLS), San Francisco, CA, May, 2019.

[W1] O. Suci, S. Coull, and J. Johns. “*Exploring Adversarial Examples in Malware Detection.*” In Proceedings of the AAAI Fall 2018 Symposium on Adversary-Aware Learning Techniques and Trends in Cybersecurity, Arlington, VA, October, 2018.

MANUSCRIPTS

[M4] K. Dyer, S. Coull, T. Ristenpart, and T. Shrimpton. “*Protocol Misidentification Made Easy with Format-Transforming Encryption.*” Cryptology ePrint Archive 2012/494.

[M3] S. Coull, J. Branch, B. Szymanski, and E. Breimer. “*Sequence Alignment for Masquerade Detection.*” Rensselaer Polytechnic Institute Computer Science Technical Report 06-14.

[M2] S. Coull and B. Szymanski. “*A Reputation-based System for the Quarantine of Random Scanning Worms.*” Rensselaer Polytechnic Institute Computer Science Technical Report 05-01.

[M1] S. Coull and B. Szymanski. “*Reputation-based Security in Routed Networks.*” In Supplemental Proceedings of the International Conference on Dependable Systems and Networks (DSN), Florence, Italy, June, 2004.

INVITED AND
MISC. TALKS

[I8] S. Coull. “*Promises and challenges of Security in Trustworthy AI.*” Presented at the 5th Deep Learning and Security Workshop (DLS), San Francisco, CA, May 2022.

[I7] S. Coull. “*Activation Analysis of a Byte-based Deep Neural Network for Malware Classification.*” Presented at Conference on Applied Machine Learning for Information Security (CAMLIS), Washington, DC. October 12, 2018.

[I6] S. Coull. “*Privacy vs. Security.*” Presented at the NIST Cloud Computing Forum, Gaithersburg, MD. July 8, 2015.

[I5] S. Coull. “*How (Not) to Apply Differential Privacy to Anonymity Networks.*” Presented at the DIMACS Working Group on Measuring Anonymity. Rutgers University, New Brunswick, NJ. May 30, 2013.

[I4] S. Coull and E. Kenneally. “*A Qualitative Risk Assessment Framework for Sharing Computer Network Data.*” Presented at the 40th Research Conference on Communication, Information, and Internet Policy (TPRC). Arlington, VA. September 23, 2012.

[I3] S. Coull. “*Information Leakage in Encrypted Network Traffic: Attacks and Countermeasures.*” Presented at University of Maryland Computer Science Colloquium. College Park, MD. September 20, 2011.

[I2] S. Coull. “*Network Data Anonymization.*” Presented at Pennsylvania State University Computer Science and Engineering Colloquium. State College, PA. March 25, 2010.

[I1] S. Coull. “*Toward Privacy Definitions for Anonymized Network Data.*” Presented at the 23rd Annual IEEE Computer Communications Workshop. Lenox, MA. October 18-21, 2009.

POSTERS

[Po2] O. Suci, S. Coull, and J. Johns. “*Exploring Adversarial Examples in Malware Detection.*” Presented at the 40th IEEE Symposium on Security and Privacy, May 2019.

[Po1] S. Coull, F. Monrose, and M. Reiter. “*Network Data Privacy.*” Presented at IPAM Workshop on Statistical and Learning-Theoretic Challenges in Data Privacy. Los Angeles, CA. February 22-26, 2010.

PATENTS

[Pa6] S. Coull, J. Johns. “*Cyber-Threat Analyses Using Machine Learning and Prior Observations.*”

[Pa4] D. Krisiloff, S. Coull. “*Churn-Aware Machine Learning for Cybersecurity Threat Detection.*” U.S. Patent Application 16/842,568. April, 2020.

[Pa3] S. Coull, D. Krisiloff, and G. Severi. “*System and Method for Heterogeneous Transferred Learning for Enhanced Cybersecurity Threat Detection.*” U.S. Patent Application 16/542,739. August, 2019.

[Pa2] S. Coull and J. Johns. “*System and Method for Adaptive Graphical Depiction and Selective Remediation of Cybersecurity Threats.*” U.S. Patent 11,201,890. Filed March, 2019. Issued December, 2021.

[Pa1] J. Johns, B. Jones, and S. Coull. “*System and Method for Analyzing Binary Code for Malware Classification Using Artificial Neural Network Techniques.*” U.S. Patent 11,108,809. Filed October, 2017. Issued August, 2021.