Curriculum Vitae

Dr. Nathan S. Evans

Contact Information
+1 202-812-6882
nathan.s.evans@du.edu
https://www.linkedin.com/in/nathan-evans-30061a63

Experienced Cyber-Security Researcher and Thought Leader
Established researcher in the fields of networking and cyber security. Accomplished and resourceful professional with a knack for solving problems and delving into the details. Variegated research and engineering background including low-level networking, systems design and implementation, breaking things and fixing things. Ability to adapt and conquer new techniques.

Positions Held

- **University of Denver** (2019-Current)
  Assistant Teaching Professor (Cyber Security)
  Primarily teaching security and networking classes for the M.S. in Cyber-Security program
- **University of Denver** (2017-2019)
  Visiting Assistant Professor (Cyber Security)
  Primarily teaching security and networking classes for the Master in Cyber-Security program
- **Mt. Evans Cyber Security Services** (2017-Current)
  Sole Proprietor
  Various consulting services related to the Cyber Security field, including security auditing and advice based on industry standards
- **University of Sydney, Australia** (Summer 2017)
  Visiting Assistant Research Professor
  Research and development on the growing field of blockchain based crypto-currency and associated network protocols
- **CloudHawk** (2016-2018)
  CTO (Chief Technology Officer)
  Drive high-level technological focus and implementation choices for startup; oversee day-to-day engineering efforts.
- **Symantec Research Labs** (2011-2016)
  Sr. Principal Research Engineer
  Responsible for the research and design of next-generation security technologies, including publishing patents and peer-reviewed publications.
- **Technische Universität München** (2010-2011)
  Research Scientist
  Responsibilities included performing, publishing and presenting peer-reviewed research in the fields of networking and cyber-security, as well as assisting in student advising and teaching selected topics at the Master's level.
- **University of Denver** (2008-2010)
  Research Assistant
  Primary duty was performing novel research in systems design and network security under advisor's guidance.

- **University of Denver** (2007-2008)
  Adjunct Professor
  After successful stint as Teaching Assistant, was given the opportunity to perform duties of Adjunct Professor responsible for teaching an introduction to Computer Science course.

Technology Summary

- **Current Languages:** C, C++, Java, Perl, Python, HTML, JavaScript, Bash, Latex
- **Rusty Languages:** VB.net, C#, Prolog, Ruby, ASP, Assembly (x86/x64), VBScript, Go, R, PHP
- **Systems:** Linux, Windows, OSX, Android, Docker
- **Networking:** TCP, UDP, CAN, Ethernet, HTTP/S, SSH, FTP, MDNS, DNS...
- **Security:** OpenVAS, OSSEC, Wazuh, ELK, Kali...

Education

- **Technische Universität München** — Munich, Germany (2010-2011)
  - PhD in Computer Science (Dr. rer. nat.): August 10, 2011 (Advised by Christian Grothoff)
  - Thesis titled: “R^5N: Randomized Recursive Routing for Restricted Route Networks”
- **University of Denver** — Denver, CO (2006-2009)
  - Studied for PhD in Computer Science; departed to complete PhD at Technische Universität München
  - Master of Science in Computer Science: Thesis titled “Routing in the Dark: Pitch Black”
- **Baldwin Wallace College** — Berea, OH (2002-2006)
  - Bachelor of Science in Computer Science
  - Bachelor of Arts in Criminal Justice
  - Minor in Mathematics

Selected Presentations

- **BlackHat Europe 2016** — Amsterdam, Netherlands (November, 2015)
  - Presented “All Your Root Checks Belong to Us: The Sad State of Root Detection” work on a large scale evaluation of Android Mobile applications
- **Usenix CSET 2014** — San Diego, CA (August, 2014)
  - Presented work from MINESTRONE project, “Large-Scale Evaluation of a Vulnerability Analysis Framework” on evaluation and testing of third party vulnerability suite and framework
- **Usenix Security 2009** — Montreal, Canada (August, 2009)
  - Presented “A Practical Congestion Attack on Tor Using Long Paths”
- **Defcon 16** — Las Vegas, Nevada (August, 2008)
  - Gave presentation of research into de-anonymizing Tor users titled “De-tor-iorate Anonymity”
- **Annual Computer Security Applications Conference** — Miami Beach, Florida (December, 2007)
  - Presented “Routing in the Dark: Pitch Black”
- **Defcon 15** — Las Vegas, Nevada (August, 2007)
  - Presented practical attack on the Freenet routing algorithm titled “Routing in the Dark: Pitch Black”

Issued Patents

[1] D. M. Kienzle, M. C. Elder, and N. S. Evans, *Determining model information of devices based on network device identifiers*, US Patent 9,135,293, 2015.

[2] D. Kienzle, N. Evans, and M. Elder, *Systems and methods for discovering network topologies*, US Patent 9,219,655, 2015.

[3] N. Evans, A. Benameur, and M. Elder, *Systems and methods for obscuring network services*, US Patent 9,525,665, 2016.

[4] D. Kienzle, N. Evans, and M. Elder, *Systems and methods for estimating ages of network devices*, US Patent 9,571,372, 2017.

[5] Y. Shen, N. Evans, and A. Benameur, *Systems and methods for detecting discrepancies in automobile-network data*, US Patent 9,582,669, 2017.

[6] A. Benameur and N. Evans, *Techniques for redirecting input/output*, US Patent 9,612,852, 2017.

[7] A. Benameur, N. Evans, and Y. Shen, *Lightweight replicas for securing cloud-based services*, US Patent 9,794,275, 2017.

[8] N. Evans, A. Benameur, and Y. Shen, *Systems and methods for detecting anomalous messages in automobile networks*, US Patent 9,843,594, 2017.

[9] A. Benameur and N. Evans, *Virtual layer rollback*, US Patent 9,898,272, 2018.

[10] N. Evans, A. Benameur, and Y. Shen, *Methods to impede common file/process hiding techniques*, US Patent 9,898,615, 2018.

[11] A. Benameur and N. Evans, *Systems and methods for enforcing secure software execution*, US Patent 9,953,158, 2018.

[12] A. Benameur, N. Evans, and Y. Shen, *Systems and methods for logging processes within containers*, US Patent 10,114,947, 2018.

Conference Publications

[13] R. Holz, D. Perino, M. Varvello, J. Amann, A. Continella, N. Evans, I. Leontiadis, C. Natoli, and Q. Scheitle, “A longitudinal study of the impact, rise, and decline of illicit cryptocurrency mining on the web,” *Under Submission* 2019.

[14] Y. Shen, N. Evans, and A. Benameur, “Insights into rooted and non-rooted android mobile devices with behavior analytics,” in *Proceedings of the 31st Annual ACM Symposium on Applied Computing*, ser. SAC ’16, Pisa, Italy: ACM, 2016, pp. 580–587, ISBN: 978-1-4503-3739-7. DOI: `10.1145/2851613.2851713`. [Online]. Available: `http://doi.acm.org/10.1145/2851613.2851713`.

[15] N. S. Evans, A. Benameur, and Y. Shen, “All your root checks are belong to us: The sad state of root detection,” in *Proceedings of the 13th ACM International Symposium on Mobility Management and Wireless Access*, ACM, 2015, pp. 81–88.

[16] N. S. Evans, A. Benameur, and M. C. Elder, “Large-scale evaluation of a vulnerability analysis framework,” in *Proceedings of the 7th USENIX conference on Cyber Security Experimentation and Test*, USENIX Association, 2014, pp. 1–8.

[17] D. M. Kienzle, N. S. Evans, and M. C. Elder, “Nice: Endpoint-based topology discovery,” in *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, ser. CISR ’14, Oak Ridge, Tennessee, USA: ACM, 2014, pp. 97–100, ISBN: 978-1-4503-2812-8. DOI: 10.1145/2602087.2602104. [Online]. Available: http://doi.acm.org/10.1145/2602087.2602104.

[18] A. Benameur, N. S. Evans, and M. C. Elder, “Minestrone: Testing the soup.,” in *Proceedings of the 6th USENIX conference on Cyber Security Experimentation and Test*, 2013.

[19] N. S. Evans, B. Polot, and C. Grothoff, “Efficient and secure decentralized network size estimation,” in *11th International IFIP TC 6 Networking Conference*, ser. LNCS, IFIP, vol. 7289, Springer Verlag, 2012, pp. 304–317.

[20] N. Evans and C. Grothoff, “Beyond simulation: Large-scale distributed emulation of p2p protocols,” in *4th Workshop on Cyber Security Experimentation and Test (CSET 2011)*, USENIX Association, 2011. [Online]. Available: http://www.usenix.org/events/cset11/tech/final_files/Evans.pdf.

[21] N. Evans and C. Grothoff, “R5n: Randomized recursive routing for restricted-route networks,” in *Network and System Security (NSS), 2011 5th International Conference on*, 2011, pp. 316–321. DOI: 10.1109/ICNSS.2011.6060022.

[22] K. C. Bader, T. Eißler, N. Evans, C. GauthierDickey, C. Grothoff, K. Grothoff, H. Meier, C. Ritzdorf, and M. J. Rutherford, “DUP: A Distributed Stream Processing Language,” in *Proceedings of the IFIP International Conference on Network and Parallel Computing (NPC 2010)*, 2010, pp. 232–246.

[23] A. Müller, N. Evans, C. Grothoff, and S. Kamkar, “Autonomous NAT Traversal,” in *10th IEEE International Conference on Peer-to-Peer Computing (IEEE P2P 2010)*, Delft, The Netherlands: IEEE, 2010. (23% Acceptance Rate), pp. 61–64.

[24] A. Fessi, N. Evans, H. Niedermayer, and R. Holz, “Pr2-P2PSIP: Privacy Preserving P2P Signaling for VoIP and IM,” in *Principles, Systems and Applications of IP Telecommunications (IPTComm), Munich*, 2010. (24% Acceptance Rate), pp. 141–152.

[25] N. Evans, C. GauthierDickey, C. Grothoff, K. Grothoff, J. Keene, and M. J. Rutherford, “Simplifying Parallel and Distributed Simulation with the DUP System,” in *Proceedings 43rd Annual Simulation Symposium (ANSS-43 2010)*, Orlando, FL, USA: Society for Modeling & Simulation International, 2010, pp. 208–215.

[26] N. S. Evans, R. Dingledine, and C. Grothoff, “A Practical Congestion Attack on Tor Using Long Paths,” in *18th USENIX Security Symposium*, USENIX, 2009. (15.1% Acceptance Rate), pp. 33–50.

[27] N. S. Evans, C. GauthierDickey, and C. Grothoff, “Routing in the dark: Pitch black,” in *ACSAC*, IEEE Computer Society, 2007. (22% Acceptance Rate), pp. 305–314.