Daniel Andriesse

da.andriesse@gmail.com | https://danielandriesse.com

Professional Experience

July'19–**now** **Offensive Security Researcher**, *Intel Corporation*.
Offensive and defensive security research at the boundary between software and hardware. Current research focus on low-level CPU glitching attacks.

Jan'17–June'19 **Postdoctoral researcher**, *Vrije Universiteit Amsterdam, System and Network Security Group*.
Research on a variety of topics in systems security and network security, including reverse engineering, binary hardening, and compiler-based defenses.

Oct'16–Nov'16 **Internship (during Ph.D.)**, *Cisco Systems*, Amsterdam, Netherlands.
Developed an LLVM-based compiler pass which implements type-sensitive forward-edge Control-Flow Integrity (CFI) to harden binaries in a multi-platform operating system.

Education

2017 **Ph.D.**, *Vrije Universiteit Amsterdam, System and Network Security Group*, *cum laude* (highest honor, awarded in approx. 4% of graduations).
Research on binary-level anti-exploitation techniques, reverse engineering, and binary analysis.
Advised by prof.dr.ir. Herbert Bos and co-advised by dr. Asia Slowinska.
Thesis committee: prof.dr. Andrew S. Tanenbaum, prof.dr. Thorsten Holz, prof.dr. Frank Piessens, dr. Christian Rossow, and dr. Davide Balzarotti. **Winner of the ACM SIGSAC Doctoral Dissertation Award and the Roger Needham Ph.D. Award.**

2012 **M.Sc. Parallel and Distributed Computer Systems**, *Vrije Universiteit Amsterdam*, *cum laude* (highest honor).
Research M.Sc. (topmaster) on systems– and parallel computing.
Grade average 9.0/10.0 (ECTS grade A, top 3%).

2022–**now** **B.Sc. Psychology**, *Open University*.
Focus on neuroscience.

2010 **B.Sc. Computer Science**, *Vrije Universiteit Amsterdam*, *cum laude* (highest honor).
Grade average 8.9/10.0 (ECTS grade A, top 3%).

Ph.D. Thesis

title *Analyzing and Securing Binaries Through Static Disassembly*
advisor prof.dr.ir. Herbert Bos and dr. Asia Slowinska
description Research on safely using error-prone binary analysis to harden binaries.

M.Sc. Thesis

title *A Comparative Analysis of the Resilience of Peer-to-Peer Botnets*
advisor prof.dr.ir. Herbert Bos
grade 9.5/10 (ECTS grade A, top 1%)
description Reverse engineered several peer-to-peer botnets, assessing their resilience against enumeration and sinkholing attacks. Later published at the 2013 IEEE Symposium on Security and Privacy.

B.Sc. Thesis

title *Feasibility of the RFID Guardian as a Relay Attack Platform*
advisor dr. Melanie Rieback
grade 10/10 (ECTS grade A, top 1%)
description Designed and implemented simulated RFID relay attacks to assess their feasibility on the RFID Guardian device.

Awards and Grants

Feb'23	Intel Divisional Recognition Award
Oct'18	Winner of the 2018 ACM SIGSAC Doctoral Dissertation Award for Outstanding Ph.D. Thesis in Computer and Information Security
Apr'18	Winner of EuroSys Roger Needham Ph.D. Award for Best Ph.D. Thesis in Computer Systems in Europe
Mar'18	Nominated for Dutch Cyber Security Research Best Paper Award (top five)
Oct'17	Best Paper Award (for the paper "The Dynamics of Innocent Flesh on the Bone: Code Reuse Ten Years Later" published at CCS'17), *3rd Cyber Security Workshop in the Netherlands (CSW-NL 2017)*, (Den Haag, The Netherlands), October 2017
June'17	Awarded the distinction *cum laude* for my Ph.D. thesis, given in approximately 4% of Ph.D. graduations at Vrije Universiteit Amsterdam and requiring unanimous endorsement by my advisor, all five thesis committee members and two external readers
Apr'17	Best Paper Award (for the paper "Compiler-Agnostic Function Detection in Binaries"), *2nd IEEE European Symposium on Security and Privacy (EuroS&P'17)*, (Paris, France), April 2017
Mar'16	Nominated for Dutch Cyber Security Research Award (top five)
July'14	FBI Certificate of Recognition for outstanding efforts in the takedown of GameOver Zeus (Operation Tovar)
June'14	Winner of National Cyber Security Research Agenda (NCSRA) Ph.D. competition

Publications

[1] M. Kurth, B. Gras, D. Andriesse, C. Giuffrida, H. Bos, and K. Razavi, "NetCAT: Practical Cache Attacks from the Network," in *Proceedings of the 41st IEEE Symposium on Security and Privacy (S&P'20)*, (San Francisco, CA, USA), IEEE, May 2020.

[2] A. Pawlowski, V. van der Veen, D. Andriesse, E. van der Kouwe, T. Holz, C. Giuffrida, and H. Bos, "VPS: Excavating High-Level C++ Constructs from Low-Level Binaries to Protect Dynamic Dispatching," in *Proceedings of the 2019 Annual Computer Security Applications Conference (ACSAC'19)*, (San Juan, Puerto Rico, USA), December 2019.

[3] E. van der Kouwe, G. Heiser, D. Andriesse, H. Bos, and C. Giuffrida, "SoK: Benchmarking Flaws in Systems Security," in *Proceedings of the 4th IEEE European Symposium on Security and Privacy (EuroS&P'19)*, (Stockholm, Sweden), IEEE, June 2019.

[4] F. de Goër, S. Rawat, D. Andriesse, H. Bos, and R. Groz, "Now You See Me: Real-time Dynamic Function Call Detection," in *Proceedings of the 2018 Annual Computer Security Applications Conference (ACSAC'18)*, (San Juan, Puerto Rico, USA), December 2018.

[5] R. K. Konoth, M. Oliverio, A. Tatar, D. Andriesse, H. Bos, C. Giuffrida, and K. Razavi, "ZebRAM: Comprehensive and Compatible Software Protection Against Rowhammer Attacks," in *Proceedings of the 13th USENIX Symposium on Operating Systems Design and Implementation (OSDI'18)*, (Carlsbad, CA, USA), USENIX, October 2018.

[6] E. van der Kouwe, D. Andriesse, H. Bos, C. Giuffrida, and G. Heiser, "Benchmarking Crimes: An Emerging Threat in Systems Security," 2018. Preprint (arXiv:1801.02381).

[7] V. van der Veen, D. Andriesse, M. Stamatogiannakis, X. Chen, H. Bos, and C. Giuffrida, "The Dynamics of Innocent Flesh on the Bone: Code Reuse Ten Years Later," in *Proceedings of the 24th Conference on Computer and Communications Security (CCS'17)*, (Dallas, TX, USA), ACM, October 2017.

[8] D. Andriesse, A. Slowinska, and H. Bos, "Compiler-Agnostic Function Detection in Binaries," in *Proceedings of the 2nd IEEE European Symposium on Security and Privacy (EuroS&P'17)*, (Paris, France), IEEE, April 2017. **Best Paper Award**.

[9] D. Andriesse, X. Chen, V. van der Veen, A. Slowinska, and H. Bos, "An In-Depth Analysis of Disassembly on Full-Scale x86/x64 Binaries," in *Proceedings of the 25th USENIX Security Symposium (USENIX Sec'16)*, (Austin, TX, USA), USENIX, August 2016.

[10] D. Andriesse, V. van der Veen, E. Göktaş, B. Gras, L. Sambuc, A. Slowinska, H. Bos, and C. Giuffrida, "Practical Context-Sensitive CFI," in *Proceedings of the 22nd Conference on Computer and Communications Security (CCS'15)*, (Denver, CO, USA), ACM, October 2015.

[11] D. Andriesse, C. Rossow, and H. Bos, "Reliable Recon in Adversarial Peer-to-Peer Botnets," in *Proceedings of the 15th Internet Measurement Conference (IMC'15)*, (Tokyo, Japan), ACM, October 2015.

[12] D. Andriesse, C. Rossow, and H. Bos, "Distributed Crawler Detection in Peer-to-Peer Botnets," October 2015. Technical Report IR-CS-77, VU University Amsterdam.

[13] D. Andriesse, H. Bos, and A. Slowinska, "Parallax: Implicit Code Integrity Verification Using Return-Oriented Programming," in *Proceedings of the 45th Conference on Dependable Systems and Networks (DSN'15)*, (Rio de Janeiro, Brazil), IEEE Computer Society, June 2015.

[14] X. Chen, A. Slowinska, D. Andriesse, H. Bos, and C. Giuffrida, "StackArmor: Comprehensive Protection from Stack-Based Memory Error Vulnerabilities for Binaries," in *Proceedings of the Network and Distributed System Security Symposium (NDSS'15)*, (San Diego, CA, USA), Internet Society, February 2015.

[15] D. Andriesse and H. Bos, "Instruction-Level Steganography for Covert Trigger-Based Malware," in *Proceedings of the 11th Conference on Detection of Intrusions and Malware & Vulnerability Assessment*, DIMVA'14, (London, United Kingdom), Springer-Verlag, July 2014.

[16] D. Andriesse, C. Rossow, B. Stone-Gross, D. Plohmann, and H. Bos, "Highly Resilient Peer-to-Peer Botnets Are Here: An Analysis of Gameover Zeus," in *Proceedings of the 8th IEEE International Conference on Malicious and Unwanted Software*, MALWARE'13, (Fajardo, Puerto Rico), IEEE Computer Society, October 2013.

[17] D. Andriesse and H. Bos, "An Analysis of the Zeus Peer-to-Peer Protocol," May 2013. Technical Report IR-CS-74, VU University Amsterdam.

[18] C. Rossow, D. Andriesse, T. Werner, B. Stone-Gross, D. Plohmann, C. Dietrich, and H. Bos, "P2PWNED: Modeling and Evaluating the Resilience of Peer-to-Peer Botnets," in *Proceedings of the 34th IEEE Symposium on Security and Privacy*, S&P'13, (San Francisco, CA, USA), IEEE Computer Society, May 2013.

Books and Book Chapters

[1] D. Andriesse, *Practical Binary Analysis*. No Starch Press, 2018. ISBN-13: 978-1-59327-912-7. Translations in Polish, Korean, Japanese, and Chinese (Mandarin).

Patents

[1] R. K. Konoth, A. Tatar, M. Oliverio, D. Andriesse, H. Bos, C. Giuffrida, and K. Razavi, "Computing Device with Increased Resistance Against Rowhammer Attacks." U.S. Patent Application (pending) US 2020/0012600 A1, January 2020.

Invited Talks

[1] "Exploiting and Mitigating the Rowhammer Vulnerability." Summer Research Institute (SuRI) 2019, June 2019. Annual event at EPFL, Switzerland.

[2] "Binary Instrumentation and Dynamic Taint Analysis." SURF Security & Privacy, February 2019. Workshop (2 hours).

[3] "Practical Binary Analysis." Finse Winter School, (Finse, Norway), May 2018. Invited lecturer for two $1\frac{1}{2}$ hour lectures.

[4] "Anatomy of a Massive Peer-to-Peer Botnet Takedown." Awesome IT: The Civilization of Bytes, (Amsterdam, The Netherlands), April 2016.

[5] "Stealthy Reconnaissance in Peer-to-Peer Botnets." National Cyber Security Center (NCSC) Conference, (The Hague, The Netherlands), June 2014. Winner of NCSRA 2014 Ph.D. competition.

[6] "Neutralizing Peer-to-Peer Botnets." Open Web Application Security Project (OWASP) Netherlands Chapter, ('s-Hertogenbosch, The Netherlands), May 2013.

[7] "Deliberately Destroying Drones: A P2P Botnet Takeover Case Study." National Cyber Security Center (NCSC) Conference, (The Hague, The Netherlands), January 2013.

Media Coverage

[1] "Bad benchmarks bedevil boffins' infosec efforts." The Register, January 2018.

[2] "The dynamics of innocent flesh on the bone: code reuse ten years later." The Morning Paper, December 2017.

[3] "Hoe een opmerkelijke coalitie een Russische crimineel bestreed." De Correspondent, February 2016.

[4] "Zo haal je een botnet uit de lucht." De Correspondent, February 2016.

[5] "Dit is de meest gevreesde cybercrimineel ter wereld: Slavik." Vrij Nederland, February 2016.

[6] "How the FBI Took Down the Botnet Designed to Be 'Impossible' to Take Down." Vice Motherboard, August 2015.

[7] "Hackeur Russe – Wanted: Evgeny Bogachev, $3,000,000." Paris Match, March 2015.

[8] "Operation Tovar Targets Gameover ZeuS Botnet." Krebs on Security, June 2014.

[9] "Altijd Wat: Cybercrime." Dutch Public Broadcasting (NPO), July 2013.

[10] "P2P Botnets Much Larger Than They Seemed." heise.de, May 2013.

[11] "Het Virusdilemma." NRC Handelsblad, November 2012.

Reviewing

May'24 Program committee member, *27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID'24)*, (Padua, Italy), October 2024

Feb'23 Program committee member, *17th IEEE Workshop on Offensive Technologies (WOOT'23)*, (San Francisco, CA, USA), May 2023

May'21 Reviewer, *ACM Transactions on Programming Languages and Systems*

Dec'19–Jan'20 Program committee member, *Workshop on Binary Analysis Research 2020 (BAR'20)*

Oct'19 Reviewer, *IEEE Security & Privacy Magazine*

Nov'18–Feb'19 Program committee member, *4th IEEE European Symposium on Security and Privacy (EuroS&P'19)*, (Stockholm, Sweden), June 2019

May'18–July'18 Program committee member, *25th ACM Conference on Computer and Communications Security (CCS'18)*, (Toronto, Canada), October 2018

May'18–June'18 Program committee member, *12th USENIX Workshop on Offensive Technologies (WOOT'18)*, (Baltimore, MD, USA), August 2018

July'18 Reviewer, *ACM Computing Surveys (CSUR)*

Feb'18–Mar'18 Program committee member (short track), *38th IEEE International Conference on Distributed Computing Systems (ICDCS'18)*, (Vienna, Austria), July 2018

Nov'17–Jan'18 Shadow program committee member, *Eurosys 2018*, (Porto, Portugal), April 2018

Oct'17 Ph.D. evaluation committee member, "Selected x86 Low-level Attacks and Mitigations" by Christian Otterstad, University of Bergen, Norway

Aug'17 Reviewer, *IEEE Security & Privacy Magazine*, special issue "Hacking Without Humans"

May'17 Reviewer, *Journal of Computer Security*

Sep'16 Reviewer, *22nd ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS'17)*, (Xi'an, China), April 2017

July'16 Reviewer, *11th International Conference on Malicious and Unwanted Software (MALCON'16)*, (Fajardo, Puerto Rico), October 2016

Nov'15 Session chair "Hardening", *18th International Symposium on Research in Attacks, Intrusions, and Defenses (RAID'15)*, (Kyoto, Japan), Springer, November 2015

Teaching

Course Organization

2018 **Secure Programming**, *VU University*, Amsterdam, (B.Sc.).
Lecturer and course organizer

2017 **Computer and Network Security**, *VU University*, Amsterdam, (M.Sc.).
Co-organized two-month course (together with prof.dr.ir. Herbert Bos), taught 50% of lectures, created challenges and exam questions.

2014–2016 **Computer Networks Excellence Track**, *VU University*, Amsterdam, (B.Sc.).
Organized "excellence track" for excellent students in computer networks. Designed, introduced and supervised the assignments that comprise the excellence track.

Advising/Project Work

2017 **Master's Thesis**, *VU University*, Amsterdam, (M.Sc.).
Co-supervised Master's thesis on using hardware branch tracking to implement a shadow stack for the Linux kernel.

2017 **Literature Study**, *VU University*, Amsterdam, (M.Sc.).
Co-supervised individual literature study on the dark web.

2016 **Excellence Track Programming Project**, *VU University*, Amsterdam, (B.Sc.).
Co-supervised five excellence track students programming a large-scale malware analysis system.

2016 **Literature Study**, *VU University*, Amsterdam, (M.Sc.).
Co-supervised individual literature study on botnet C2 channels.

2011 **Advanced Programming**, *VU University*, Amsterdam, (B.Sc.).
Supervised course work for individual students.

Course Work

2012–2017 **Computer and Network Security**, *VU University*, Amsterdam, (M.Sc.).
Taught lectures, created challenges and exam questions.

2013–2017 **Binary and Malware Analysis**, *VU University*, Amsterdam, (M.Sc.).
Created botnet sinkholing challenge, taught guest lectures.

2011–2016 **Computer Networks**, *VU University*, Amsterdam, (B.Sc.).
Designed and graded assignments, organized excellence track.

2014–2014 **Security**, *VU University*, Amsterdam, (B.Sc.).
Taught guest lectures.

2011–2014 **Computer Systems**, *VU University*, Amsterdam, (B.Sc.).
Supervised practicals.

2012 **Internet Programming**, *VU University*, Amsterdam, (M.Sc.).
Graded assignments.

2009–2011 **Data Structures and Algorithms**, *VU University*, Amsterdam, (B.Sc.).
Taught tutorials.

2008–2011 **Introduction to Programming**, *VU University*, Amsterdam, (B.Sc.).
Supervised practicals.

2010 **Online Information Systems**, *VU University*, Amsterdam, (B.Sc.).
Supervised practicals.

2009–2010 **Logical Structures**, *VU University*, Amsterdam, (B.Sc.).
Taught tutorials.

2009 **C**/**C**++, *VU University*, Amsterdam, (B.Sc.).
Graded assignments.