

Dennis Andriesse

da.andriesse@few.vu.nl | <https://mistakenot.net>

Professional Experience

- JAN'17–NOW **Postdoctoral researcher**, *Vrije Universiteit Amsterdam, System and Network Security Group*.
Research on a wide 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). Used for hardening binaries in a multi-platform operating system that runs on a variety of devices, including network switches.

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 malware 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 system and network security, and systems- and parallel programming. Grade average 9.0/10.0 (ECTS grade A, top 3%).
- 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** Thesis deals with safely using error-prone binary analysis techniques to instrument binaries with novel defenses against advanced attacks. Additionally, the thesis provides an in-depth study of the precision and challenging cases in x86/x86-64 disassembly, and discusses an improved technique for function detection in stripped binaries (the most error-prone disassembly primitive at the time of writing).

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.

Practical Binary Analysis.

Wrote the book *Practical Binary Analysis* (No Starch Press), the first book to cover the full breadth of the binary analysis field in an accessible way. Covers binary formats, disassembly, fundamental analysis and code injection techniques, binary instrumentation, taint analysis, and symbolic execution.

Newton: The Dynamics of Innocent Flesh on the Bone.

One of the main contributors to Newton, an automatic exploit generation tool based on dynamic taint analysis. Newton was the first tool to show that state-of-the-art defenses against Return-Oriented Programming at the time didn't hold up against attackers armed with dynamic binary analysis capabilities.

Nucleus: Compiler-Agnostic Function Detection in Binaries.

Main author of Nucleus, a compiler-agnostic function detector that won a best paper award at EuroS&P 2017 and was partially integrated into Binary Ninja, a well-known commercial disassembler. Nucleus can accurately perform both function start and function boundary detection in binaries, with only minimal assumptions on function or binary layout. It can naturally handle tough cases, such as non-contiguous and indirectly called functions, without any dependence on function signatures. The source is available at <https://bitbucket.org/vusec/nucleus>.

PathArmor: Practical Context-Sensitive CFI.

Major contributor to PathArmor, the first practical Context-sensitive Control-Flow Integrity (CFI) platform. Earlier CFI implementations, which track control transfers individually, have been demonstrated to leave sufficient leeway for powerful ROP attacks. Context-sensitive CFI improves security by validating control transfers to sensitive program states *within the context of preceding edges*, greatly reducing the number of exploitable program paths available to an attacker. PathArmor is available open-source at <https://github.com/dennisaa/patharmor>.

Operation Tovar: Takedown of the GameOver Zeus Botnet.

One of the main contributors to Operation Tovar, a large-scale takedown effort against GameOver Zeus (GOZ) in June 2014. At the time, GOZ was widely considered the most advanced Peer-to-Peer botnet. This was a collaboration with the FBI, CrowdStrike, Dell SecureWorks, and Saarland University (Germany). The Peer-to-Peer layer attack evolved in large part from my M.Sc. thesis work.

Parallax: Code Self-Verification Using Return-Oriented Programming.

Main author of Parallax, a novel code self-verification technique that uses Return-Oriented Programming (ROP) gadgets to protect instructions against tampering. It is the first anti-tampering system that can protect arbitrary code while being immune to attacks against traditional checksum-based tamperproofing. Parallax has grown into an ongoing research project on code self-verification for embedded devices, and has attracted dedicated funding, Ph.D. students and postdocs.

Awards and Grants

- 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
- AUG'16 Travel grant, *25th USENIX Security Symposium (USENIX Sec'16)*, (Austin, TX, USA), August 2016
- 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

Technical Skills

Binary analysis	IDA Pro, Capstone, OllyDbg, gdb, Pin, PEBIL, Dyninst, Taint analysis (libdft), Symbolic execution (Triton)
Compilers	gcc, LLVM (including LLVM passes)
Programming & scripting	C/C++, Java, Python, Ruby, Assembly, Lua, PHP, Javascript, (X)HTML/CSS, SQL, L ^A T _E X, R, Bash, Go
Operating systems	Windows, Linux, Minix
Parallel/GPU programming	MPI, CUDA, OpenCL, Hadoop, OpenGL

Publications

- [1] F. de Goër, S. Rawat, D. Andriessse, 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.
- [2] R. K. Konoth, M. Oliverio, A. Tatar, D. Andriessse, H. Bos, C. Giuffrida, and K. Razavi, "Ze-bRAM: 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.
- [3] E. van der Kouwe, D. Andriessse, H. Bos, C. Giuffrida, and G. Heiser, "Benchmarking Crimes: An Emerging Threat in Systems Security," 2018. Preprint (arXiv:1801.02381).
- [4] V. van der Veen, D. Andriessse, 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.
- [5] D. Andriessse, 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 Computer Society, April 2017. **Best Paper Award.**
- [6] D. Andriessse, 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.
- [7] D. Andriessse, 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.
- [8] D. Andriessse, 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.
- [9] D. Andriessse, C. Rossow, and H. Bos, "Distributed Crawler Detection in Peer-to-Peer Botnets," October 2015. Technical Report IR-CS-77, VU University Amsterdam.
- [10] D. Andriessse, 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.

- [11] X. Chen, A. Slowinska, D. Andriessse, 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.
- [12] D. Andriessse 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.
- [13] D. Andriessse, 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.
- [14] D. Andriessse and H. Bos, “An Analysis of the Zeus Peer-to-Peer Protocol,” May 2013. Technical Report IR-CS-74, VU University Amsterdam.
- [15] C. Rossow, D. Andriessse, T. Werner, B. Stone-Gross, D. Plohmann, C. Dietrich, and H. Bos, “P2PWED: 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. Andriessse, *Practical Binary Analysis*. No Starch Press, 2018. ISBN-13: 978-1-59327-912-7.
- [2] H. Bos and D. Andriessse, *The Red Book: A Roadmap for Systems Security Research*, ch. “The Botnet That Would Not Die”. The SysSec Consortium, August 2013.

Invited Talks

- [1] “TBD.” 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] “Hacker Russe – Wanted: Evgeny Bogachev, \$3,000,000.” Paris Match, March 2015.
- [8] “Operation Tovar Targets Gameover ZeuS Botnet, CryptoLocker Scourge.” 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 Virusedilemma.” NRC Handelsblad, November 2012.

Valorization

- Nov’17 Our function detector Nucleus was integrated into Binary Ninja, a well-known commercial disassembler
- JUNE’14 Our work on the GameOver Zeus P2P botnet was an important factor that led to the takedown of GameOver Zeus in collaboration with the FBI (Operation Tovar)

Community Service

- 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.

Languages

Dutch	Native.
English	Fluent.
Chinese (Mandarin)	Basic working proficiency.
German	Basic working proficiency.
French	Elementary proficiency.

Personal Interests

Aviation (PPL pilot, enrolled in modular CPL training at Martinair Flight Academy and working towards Aerobatics Rating)

Writing (fiction and non-fiction)

Physics

Science Fiction

Hiking/Mountaineering

References

References available upon request.