Christophe Hauser, Ph.D.

Hanover, New Hampshire *Webpage*

`contact@kereoz.org`

Affiliation: Assistant Professor of Computer Science at Dartmouth College

Research interests: Software and systems security with a focus on binary program analysis and firmware analysis for vulnerability discovery, automated verification and reverse engineering, generalizing program understanding with AI, automatically retrofitting security in legacy code and supply-chain security.

Education

- **Ph.D. in computer science**—OS kernel model for intrusion detection in distributed systems
  Joint Ph.D.: CentraleSupélec, University of Paris-Saclay (French "grande école") & Queensland university of technology, Australia - October 2009/ June 2013 – Ph.D. thesis (pdf)
- **Research Master's in computing science**—Systems and network security
  University of Rennes1/CentraleSupélec/Télécom Bretagne, France - 2008/2009 – Master's thesis (pdf)
  Institute of technology, Tralee, Ireland - 2007/2008 – Erasmus (European Mobility Program)
- **Bachelor in computer science**—Algorithms, formal methods and operating systems
  University of Rennes 1, France - 2006/2007
- **University Bachelor's of Technology**—Electronics and computing engineering
  Institute of technology of the university of Rennes 1, France - 2004/2006
- **French Baccalaureate of science**—Mathematics specialty - 2003

Employment & Academic Experience

- **Dartmouth College, USA**—July 2023 - Present
  Assistant Professor of Computer Science— Faculty member and member of the Institute for Security, Technology and Society (ISTS) – I am co-leading the TRUST lab.
- **University of Southern California, USA**—September 2016 - July 2023
  Research Computer Scientist/Research Lead— Founded and co-lead the Binary Analysis and Systems Security (BASS) group at the Information Sciences Institute (ISI). Research on: binary program analysis, embedded systems security, vulnerability discovery, automated reverse engineering, software attacks and defenses. – Static analysis and symbolic execution for the verification and security analysis of embedded systems such as UAVs and FPGAs – Machine learning for program analysis.
- **University of California, Santa Barbara, USA**—January 2014 - September 2016
  Postdoctoral researcher— Binary program analysis/vulnerability discovery – design of new techniques and initial development of the `angr` binary analysis platform, as part of the "Vetting Commodity IT Software and Firmware" (VET) DARPA program.
- **INRIA/CentraleSupélec, CIDRE team, France**—October 2009 - June 2013
  PhD candidate/research assistant— Distributed intrusion detection/kernel-level security/formal models – Design and development of a formal model for information flow tracking at the operating system kernel level - Linux kernel implementation of `Blare IDS`.
- **Queensland University of Technology, Australia**—January 2011, January 2012
  Visiting PhD candidate/research assistant— Distributed intrusion detection/kernel-level security/formal models

- **University of Tokyo - Sagayama & Ono laboratory, Japan**—Summer 2009
  Research student— Prototype of combined acoustic and stochastic model for evaluation engagement as part of the Quaero European research project.
- **INRIA, METISS team, France**—Fall/Spring 2009
  Research student— Stochastic model for automatic classification of musical genre and artist recognition as part of the Quaero European research project.
- **OpenApp (Dublin, Ireland)**—June - September 2008
  Linux system administrator and web developer - Python/PostgreSQL
- **Sogeti High-Tech (Capgemini branch in Rennes, France)**—April/September 2006
  Video over IP / Embedded Linux developer - ARM/x86
- **Novelios**—Saint-Malo, France - July 2004
  Linux server prototype - System administration / shell scripting

Conference and Journal Publications

- [SecureComm] **Street Rep: A Privacy-Preserving Reputation Aggregation System** [pdf]
  Christophe Hauser, Shirin Nilizadeh, Yan Shoshitaishvili, Ni Trieu, Srivatsan Ravi, Christophe Kruegel, Giovanni Vigna
  EAI International Conference on Security and Privacy in Communication Networks, 2023
- [RAID] **Leader: Defense Against Exploit-Based Denial-of-Service Attacks on Web Applications** [pdf]
  Rajat Tandon, Haoda Wang, Nicolaas Weideman, Shushan Arakelyan, Genevieve Bartlett, Christophe Hauser, Jelena Mirkovic
  International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2023) – Acceptance rate: 25%
- [TOSEM] **Fine-Grained Coverage-Based Fuzzing** [pdf]
  Wei-Cheng Wu, Bernard Nongpoh, Marwan Nour, Michaël Marcozzi, Sébastien Bardin, and Christophe Hauser
  ACM Transactions on Software Engineering and Methodology (2023)
- [USENIX] **Arbiter: Bridging the Static and Dynamic Divide in Vulnerability Discovery on Binary Programs** [pdf]
  Jayakrishna Menon Vadayath, Moritz Eckert, Kyle Zeng, Nicolaas Weideman, Gokulkrishna Praveen Menon, Yanick Fratantonio, Davide Balzarotti, Adam Doupé, Tiffany Bao, Ruoyu Wang, Christophe Hauser, Yan Shoshitaishvili
  USENIX Security (2022) - Acceptance rate: 18%
- [RAID] **Harm-DoS: Hash Algorithm Replacement for Mitigating Denial-of-Service Vulnerabilities in Binary Executables** [pdf]
  Nicolaas Weideman, Haoda Wang, Tyler Kann, Spencer Zahabizadeh, Wei-Cheng Wu, Rajat Tandon, Jelena Mirkovic, Christophe Hauser
  International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2022) – Acceptance rate: 25%
- [NeurIPS] **NS3: Neuro-symbolic Semantic Code Search** [pdf]
  Shushan Arakelyan, Anna Hakhverdyan, Miltiadis Allamanis, Luis Garcia, Christophe Hauser, Xiang Ren
  Conference on Neural Information Processing Systems(NeurIPS 2022) - Acceptance rate: 25.6%
- [Springer] **Bin2vec: Learning Representations of BinaryExecutable Programs for Security Tasks** [pdf]
  Shushan Arakelyan, Sima Arasteh, Christophe Hauser, Erik Kline, Aram Galstyan
  Springer Cybersecurity Journal (2021)

- [ACSAC] **Sleak: Automating Address Space Layout Derandomization** [pdf]
  Christophe Hauser, Jayakrishna Menon, Yan Shoshitaishvili, Ruoyu Wang, Christopher Kruegel, Giovanni Vigna
  In Proceedings of the Annual Computer Security Applications Conference (ACSAC) 2019 - Acceptance rate: 22.6%
- [CODASPY] **BootKeeper: Validating Software Integrity Properties on Boot Firmware Images** [pdf]
  Ronny Chevalier, Stefano Cristalli, Christophe Hauser, Yan Shoshitaishvili, Ruoyu Wang, Christopher Kruegel, Giovanni Vigna, Danilo Bruschi, Andrea Lanzi
  In Proceedings of the 9th ACM Conference on Data and Application Security and Privacy (CODASPY) 2019 - Acceptance rate: 23.5%
- [IEEE S&P] **SoK: (State of) The Art of War: Offensive Techniques in Binary Analysis** [pdf]
  Yan Shoshitaishvili, Fish Wang, Chris Salls, Nick Stephens, Mario Polino, Andrew Dutcher, John Grosen, Christophe Hauser, Christopher Kruegel, Giovanni Vigna
  Proceedings of the IEEE symposium on Security and Privacy (SSP) 2016 - Acceptance rate: 13.3%
- [NDSS] **Firmalice - Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware** [pdf]
  Yan Shoshitaishvili, Ruoyu Wang, Christophe Hauser, Christopher Kruegel, Giovanni Vigna
  Proceedings of the Network and Distributed System and Security symposium (NDSS) 2015 - Acceptance rate: 16.9%
- [IEEE ICC] **Intrusion detection in distributed systems, an approach based on taint marking** [pdf]
  Christophe Hauser, Frédéric Tronel, Colin J. Fidge, Ludovic Mé
  Proceedings of the IEEE International Conference on Computer Communications (ICC) 2013 - Acceptance rate: 39.1%
- [AISC] **A taint marking approach to confidentiality violation detection** [pdf]
  Christophe Hauser, Frederic Tronel, Jason F. Reid, and Colin J. Fidge
  10th Australasian Information Security Conference (AISC 2012) (RMIT University, Melbourne, VIC) (Josef Pieprzyk and Clark Thomborson, eds.), Conferences in Research and Practice in Information Technology, Australian Computer Society, January 2012
- [IEEE ICC] **Information flow control for intrusion detection derived from mac policy** [pdf]
  Stéphane Geller, Christophe Hauser, Frédéric Tronel, Valérie Viet Triem Tong
  Proceedings of the IEEE International Conference on Computer Communications (ICC) 2011
- [CESAR] **Mise en oeuvre depolitiques de protection des flux d'information dans l'environnement Android** [pdf]
  Valérie Viet Triem Tong, Radoniaina Andriatsimandefitra, Stéphane Geller, Simon Boche, Frédéric Tronel, Christophe Hauser
  C&ESAR 2011 in "Mobilité & Sécurité"

Workshop Papers and Posters

- **AutoCPS: Control Software Dataset Generation for Semantic Reverse Engineering**—Haoda Wang, Christophe Hauser and Luis Garcia
  IEEE Security and Privacy Workshops 2022, SafeThings
- **PERFUME: Programmatic Extraction and Refinement For Usability of Mathematical Expression**—Nicolaas Weideman, Virginia K. Felkner, Wei-Cheng Wu, Jon May, Christophe Hauser, Luis Garcia
  ACM Conference on Computer and Communications Security (CCS) workshops, CheckMate 2021
- **Towards learning representations of binary executable files for security tasks**—Shushan Arakelyan, Christophe Hauser, Erik Kline, Aram Galstyan
  AAAI Artificial Intelligence for Cybersecurity (AICS) 2020

- **A binary analysis approach to retrofit security in input parsing routines**—Jayakrishna Menon, Christophe Hauser, Yan Shoshitaishvili, Stephen Schwab
  IEEE Security and Privacy Workshops (SPW) 2018
- **End-to-End Service for System Security Experimentation (Poster)**—Chistophe Hauser, Zhenkai Liang, Stephen Schwab
  Proceedings of the IEEE symposium on Security and Privacy (SSP) 2017
- **Challenges and next steps in binary program analysis with angr (Poster)**—Chistophe Hauser, Yan Shoshotaishvili, Ruoyu Wang
  Proceedings of the IEEE symposium on Security and Privacy (SSP) 2017

Funding Awards and Distinctions

- **DARPA Artificial Intelligence Exploration (AIE)**: "Hybrid AI to Protect Integrity of Open Source Code (SocialCyber)" – Co-PI, jointly with Jim Blythe, 2021-2023 – $1M
- **DARPA Artificial Intelligence Exploration (AIE)**: "Recovery of Symbolic Mathematics from Code (ReMath)" – Co-PI, jointly with Luis Garcia, 2020-2021 – $1M
- **Department of Energy/Honeywell Federal Manufacturing & Technologies LLC**: "Replacing Aging Programmable Electronics Rapidly (REAPER)-Phase 3" – Co-PI, jointly with Andrew Schmidt, 2021 – $300,000
- **Department of Energy/Honeywell Federal Manufacturing & Technologies LLC**—Replacing Aging Programmable Electronics Rapidly (REAPER)-Phase 2
  Jointly with Matthew French, Andrew Schmidt, Stephen Schwab and Joshua Monson, 2020 $225,000
- **Air Force Research Lab**: "STTR on Autonomous Cyber Defense" – PI, 2019-2020 – $73,000
- **NSF CNS-1815495 SaTC: CORE: Small:**: "Hardening Systems Against Low-Rate DDoS Attacks" – Co-PI, jointly with Jelena Mirkovic, 2018-2021 – $500,000
- **NSF CNS-1659886**: "Research Experiences for Undergraduates (REU)" – Co-PI, jointly with Jelena Mirkovic, 2017-2020 – $360,000
- **Department of Energy/Honeywell Federal Manufacturing & Technologies LLC**: "Replacing Aging Programmable Electronics Rapidly (REAPER)" – Jointly with Matthew French, Andrew Schmidt and Travas Haraldsen, 2019 – $250,000
- **Air Force Research Laboratory**: "(ISI subcontract for InferLink STTR on Autonomous Cyber Defense)" – PI, 2019 – $73,500
- **AFOSR FA9550-18-1-0306, Secretary of Air Force (SECAF) 2030 Science and Technology Study**: "The future of autonomous decision making in safety-critical cyber environments" – Co-PI, Jointly with Srivatsan Ravi, 2018 – $190,000
- **NSF OCI-1842703**: "DETER Research Education and Operations Mission Sustainment" – Jointly with Terry Benzel, Jelena Mirkovic and Erik Kline, 2018 – $2000,000
- **ISI Internal Initiatives (IR&D)**: "Towards Automated and Principled Software Vulnerability Extrapolation" – PI – in collaboration with Aram Galstyan and Erik Kline, 2018 – $200,000

Scholarships/fellowships

- **French Ministry of Education and Research Ph.D. fellowship**—2009-2013
- **ERASMUS Scholarship**—2008

Professional Service

- **Oganizing comittee**
  - ACM Conference on Computer and Communications Security (CCS) 2022 - Workshop Co-chair, workshop selection and organization committee.
- **Workshop Chair**
  - CheckMate: Research on offensive and defensive techniques in the context of Man At The End (MATE) attack – (ACM CCS 2021)
  - Machine Learning for Program Analysis (MLPA) workshop 2020
- **Program Committee Member (conferences)**
  - Network and Distributed System Security (NDSS) Symposium 2024
  - The ACM Conference on Computer and Communications Security (CCS) 2022, 2023
  - USENIX Security 2022
  - Annual Computer Security Applications Conference (ACSAC): 2017-2023
  - Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA): 2020-2023
  - IEEE Secure Development Conference 2023
  - EAI SecureComm 2021
- **Journal Reviewer**
  - ACM Transactions On Privacy and Security (TOPS, formerly TISSEC), 2016
- **External Reviewer**
  - USENIX Security Symposium 2016
  - Network and Distributed Systems Security Symposium (NDSS) 2016
- **Program Committee Member (workshops)**
  - USENIX Workshop on Offensive Technologies (WOOT '19, '20,'21)
  - NDSS Workshop on Binary Analysis Research (BAR) 2019, 2021
  - ACSAC DYnamic and Novel Advances in Machine Learning and Intelligent Cyber Security (DYNAMICS) Workshop 2020
  - IEEE Euro S&P Workshop on Software Attacks and Defenses SAD 2020
  - ACSAC Software Security, Protection, and Reverse Engineering Workshop (SSPREW) 2019

Mentoring & Supervision

Ph.D. Students

- Wei-Cheng Wu, Fall 2019-present
- Nicolaas Weideman, Fall 2018-present (co-advised with Jelena Mirkovic)

- Sima Arasteh, Fall 2019-present (co-advised with Mukund Raghothaman)
- Shushan Arakelyan, 2018-2022 (co-advised with Aram Galstyan and Xiang Ren)

Visiting Ph.D. Students

- Afsah Anwar, University of Central Florida, Summer 2019.
- Lesly-Ann Daniel , CEA (France), Fall 2019.
- Kasra Koorehdavoudi (Summer 2018), co-advised with Srivatsan Ravi

NSF REU students

- Summer 2021: Rene Reyes
- Summer 2020: Tyler Kann
- Summer 2019: Claire Cannatti
- Summer 2018: Kai Walberg

Interns and Research assistants

- Peifeng Ye (Spring 2019)
- Marton Demeter (Summer 2018), co-advised with Srivatsan Ravi
- Jayakrishna Menon, Jan-Oct 2018
- Ashitha Bettadapura (Fall 2017)

Selected talks, guest lectures and invited presentations

- *"Mitigating (a class of) algorithmic complexity vulnerabilities in Binary Programs"*
  University of Utah, 2022
- *"Vulnerability discovery on binary programs: current approaches and perspectives"*
  INRIA Rennes, France, 2022
- *"Security: a journey of data-flow problems"*
  GrammaTech, USA, 2022
- Dagstuhl Seminar 19331 on Software Protection Decision Support and Evaluation Methodologies, Dagstuhl, Germany, August 2019
- *"BootKeeper: Validating Software Integrity Properties on Boot Firmware Images"*
  ACM Conference on Data and Application Security and Privacy (CODASPY), Dallas, USA, 2019
- *"Binary program analysis for security"*
  INRIA Rennes, France, 2018
- *"Retrofitting security in closed-Source binary programs"*
  University of California, Riverside, USA, 2018
- *"A Binary Analysis Approach to Retrofit Security in Input Parsing Routines"*
  IEEE Symposium on Security and Privacy Workshops, San Francisco, USA, 2018
- *"Detecting malicious behavior and vulnerabilities in commodity software"*
  Information Sciences Institute, University of Southern California, USA, 2016

- *"A composable binary analysis approach for vulnerabilty discovery"*
  University of Bonn, Germany, 2016
- *"Exploiting the Linux kernel"*
  University of California, Santa Barbara, USA, 2014
- *"Intrusion detection in distributed systems, an approach based on taint marking"*
  IEEE International Conference on Computer Communications (ICC), Budapest, Hungary, 2013
- *"Distributing security labels over the network in [D]Blare"*
  Technicolor Research & Innovation labs, France, 2013
- *"Leveraging LSM kernel hooks for intrusion detection"*
  INRIA Rennes, France, 2010