Christophe Hauser, Ph.D.

Los Angeles, California, USA *(+1) 805 453 4703* *https://www.isi.edu/~hauser*
christophe.hauser@gmail.com

Research interests: systems/software security: binary program analysis, vulnerability discovery, embedded systems security, reverse engineering, protection of privacy

Education

- **Ph.D. in computer science**—OS kernel model for intrusion detection in distributed systems
  Joint Ph.D.: CentraleSupélec (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/Supélec/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 degree in technology**—Electronics and computing engineering
  Institute of technology of the university of Rennes 1, France - 2005/2006
- **French Baccalaureate of science**—Mathematics specialty - 2003

Employment & Academic Experience

- **University of Southern California (ISI), Los Angeles, USA**—September 2016 - Present
  —Research Computer Scientist— *I am leading the Binary Analysis and Systems Security (BASS) group. My research focuses on:* Binary program analysis, embedded systems security, vulnerability discovery, automated reverse engineering, software attacks and defenses. – Automated security protocol generation for remote software attestation (`Quasar` project/"Vetting Commodity IT Software and Firmware" (VET) DARPA program) – 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 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

- [Springer] **"Bin2vec: Learning Representations of BinaryExecutable Programs for Security Tasks"**
  [pdf] – Shushan Arakelyan, Sima Arasteh, Christophe Hauser, Erik Kline, Aram Galstyan
  Springer Cybersecurity Journal (accepted, to appear)
- [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 - acceptance rate: 38.5%
- [CESAR] **"Mise en oeuvre de politiques de protection des flux d'information dans l'environnement Android"**
  Valérie Viet Triem Tong, Radoniaina Andriatsimandefitra, Stéphane Geller, Simon Boche, Frédéric Tronel, Christophe Hauser
  C&ESAR 2011 in "Mobilité & Sécurité"

Workshop Papers and Posters

- **Nicolaas Weideman, Virginia K. Felkner, Wei-Cheng Wu, Jon May, Christophe Hauser, Luis Garcia**—PERFUME: Programmatic Extraction and Refinement For Usability of Mathematical Expression
  ACM Conference on Computer and Communications Security (CCS) workshops, CheckMate 2021
- **Shushan Arakelyan, Christophe Hauser, Erik Kline, Aram Galstyan**—Towards learning representations of binary executable files for security tasks
  AAAI Artificial Intelligence for Cybersecurity (AICS) 2020
- **Jayakrishna Menon, Christophe Hauser, Yan Shoshitaishvili, Stephen Schwab**—A binary analysis approach to retrofit security in input parsing routines
  IEEE Security and Privacy Workshops (SPW) 2018
- **Chistophe Hauser, Zhenkai Liang, Stephen Schwab**—End-to-End Service for System Security Experimentation
  (Poster) Proceedings of the IEEE symposium on Security and Privacy (SSP) 2017
- **Chistophe Hauser, Yan Shoshotaishvili, Ruoyu Wang**—Challenges and next steps in binary program analysis with angr
  (Poster) 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, 2021-2022 – $500,000
- **DARPA Artificial Intelligence Exploration (AIE)**: "Recovery of Symbolic Mathematics from Code (ReMath)" – Co-PI, jointly with Luis Garcia, 2020-2021 – $500,000
- **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
- **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
- **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
- **NSF OCI-1842703**: "DETER Research Education and Operations Mission Sustainment" – Jointly with Terry Benzel, Jelena Mirkovic and Erik Kline – $2000,000
- **Air Force Research Laboratory**: "(ISI subcontract for InferLink STTR on Autonomous Cyber Defense)" – PI – $73,500
- **ISI Internal Initiatives (IR&D)**: "Towards Automated and Principled Software Vulnerability Extrapolation" – PI – in collaboration with Aram Galstyan and Erik Kline – $200,000

Scholarships/fellowships

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

Professional Service

- **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 – (Independent)
- **Program Committee Member (conferences)**
  - USENIX Security 2022
  - EAI SecureComm 2021
  - Annual Computer Security Applications Conference (ACSAC): 2017-2020
  - Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA): 2020-2021
- **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

Students & Education

NSF REU mentor

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

Ph.D. Students

- Nicolaas Weideman, Fall 2018-present (co-advised with Jelena Mirkovic)
- Sima Arasteh, Fall 2019-present (co-advised with Jelena Mirkovic)
- Wei-Cheng Wu, Fall 2019-present (co-advised with Jelena Mirkovic)
- Shushan Arakelyan, Fall 2018-present (co-advised with Xiang Ren)

Visiting Ph.D. Students

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

Interns and Research assistants

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

Selected talks and invited presentations

- 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, 2019
- *"Binary program analysis for security"*
  INRIA Rennes, France, 2018
- *"Retrofitting security in closed-Source binary programs"*
  University of California, Riverside, 2018
- *"A Binary Analysis Approach to Retrofit Security in Input Parsing Routines"*
  IEEE Symposium on Security and Privacy Workshops, San Francisco, 2018
- *"Detecting malicious behavior and vulnerabilities in commodity software"*
  Information Sciences Institute, University of Southern California, 2016
- *"A composable binary analysis approach for vulnerabilty discovery"*
  University of Bonn, Germany, 2016
- *"Exploiting the Linux kernel"*
  University of California, Santa Barbara, 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