Thorsten Eisenhofer

Curriculum Vitae

Profile

I am a last year doctorate student at Ruhr University Bochum working with Thorsten Holz. I am a security researcher in the DFG Cluster of Excellence "Cyber Security in the Age of Large-Scale Adversaries" (CASA). My research revolves around the intersection of machine learning and computer security. I am particularly interested in the application of machine learning for computer security and on the security properties of learning algorithms in adversarial settings.

Experiences (Excerpt)

Research Internship — *6 month* 2022
Vector Institute, Toronto, Canada
I was visiting the Cleverhans Lab at the Vector Institute in Toronto working with Nicolas Papernot on secure and trustworthy machine learning.
Advisor: Nicolas Papernot

Crossdisciplinary Internship — *6 weeks* 2021
Ruhr University Bochum, Germany
As part of the CASA Graduate School, I was doing a 6-week internship in the Cryptography group where I was working on password-authenticated key exchange.
Advisor: Eike Kiltz

Research Internship — *6 month* 2018
University of California in Santa Barbara, USA
For my Master's thesis on symbolic execution, I was interning in the SecLab at UC Santa Barbara working with Giovanni Vigna and Christopher Kruegel.
Advisors: Giovanni Vigna and Christopher Kruegel

Malware Research — *part-time* 2016 - 2018
VMRay, Bochum, Germany
I was a student worker in the malware research team of VMRay. I was working on in-depth malware analyses and investigation of new infection and evasion techniques.
Advisors: Carsten Willems and Ralf Hund

Semester Abroad — *5 month* 2015
NTNU Gjøvik, Norway
With the European Erasmus program, I spend a semester abroad at the NTNU Gjøvik in Norway during my master studies.
Main area of study: Information Security

Contact

Address
Universitätsstraße 150
44801 Bochum
Germany

Email
thorsten.eisenhofer@rub.de

Website
https://eisenhofer.me

Education

Ph.D. Student — *projected* 2019 - 2023
Ruhr University Bochum, Germany
Main area of study: ML & Computer Security
Advisor: Thorsten Holz

M. Sc. Computer Security 2016 - 2019
Ruhr University Bochum, Germany
Thesis: "Symbolic Execution of Mixed-Representation Applications"
Final grade: A (ECTS grading scale)
Award: Best student in graduating class

B. Sc. Computer Science 2012 - 2015
Paderborn University, Germany
Thesis: "Protocols for Authenticated Key Exchange"
Final grade: A (ECTS grading scale)

Teaching

ML & Computer Security 2020-2021
Ruhr University Bochum, Germany
Master · Hands-on class · Instructor

Systems Security 2021
Saarland University, Germany
Bachelor · Lecture · Teaching Assistant

Operating Systems Security 2020
Ruhr University Bochum, Germany
Master · Lecture · Teaching Assistant

Systems Security 2019
Ruhr University Bochum, Germany
Bachelor · Lecture · Teaching Assistant

Reviewing

WORMA'23 2023
Workshop · PC Member

ICML'22 2022
Conference · PC Member

USENIX Security AE'22 2022
Artifact Evaluation · PC Member

RuhrSec'20 2020
Conference · PC Member

Other

Study Advisory Board 2022-2023
Ruhr University Bochum, Germany
Faculty for Computer Science · Representative of Research Assistants

Thorsten Eisenhofer

Curriculum Vitae (Cont'd)

Publications

2023

Nico Schiller, Merlin Chlosta, Moritz Schloegel, Nils Bars, Thorsten Eisenhofer, Tobias Scharnowski, Felix Domke, Lea Schönherr, and Thorsten Holz
Drone Security and the Mysterious Case of DJI's DroneID
Network and Distributed System Security Symposium (NDSS), 2023

Hojjat Aghakhani, Lea Schönherr, Thorsten Eisenhofer, Dorothea Kolossa, Thorsten Holz, Christopher Kruegel and Giovanni Vigna
VenoMave: Clean-Label Poisoning Against Speech Recognition
Conference on Secure and Trustworthy Machine Learning (SaTML), 2023

2022

Thorsten Eisenhofer, Doreen Riepel, Varun Chandrasekaran, Esha Ghosh, Olga Ohrimenko, and Nicolas Papernot
Verifiable and Provably Secure Machine Unlearning
Computing Research Repository (CoRR), 2022

Roei Schuster, Jin Peng Zhou, Thorsten Eisenhofer, Paul Grubbs, and Nicolas Papernot
Learned Systems Security
Computing Research Repository (CoRR), 2022

Michel Abdalla, Thorsten Eisenhofer, Eike Kiltz, Sabrina Kunzweiler and Doreen Riepel
Password-Authenticated Key Exchange from Group Actions
Annual International Cryptology Conference (CRYPTO), 2022

Lea Schönherr, Maximilian Golla, Thorsten Eisenhofer, Jan Wiele, Dorothea Kolossa, and Thorsten Holz
Exploring Accidental Triggers of Smart Speakers
Computer Speech & Language (CSL), 2022

2021

Thorsten Eisenhofer, Lea Schönherr, Joel Frank, Lars Speckemeier, Dorothea Kolossa and Thorsten Holz
Dompteur: Taming Audio Adversarial Examples
USENIX Security Symposium (USENIX), 2021

2020

Joel Frank, Thorsten Eisenhofer, Lea Schönherr, Asja Fischer, Dorothea Kolossa, and Thorsten Holz
Leveraging Frequency Analysis for Deep Fake Image Recognition
International Conference on Machine Learning (ICML), 2020

Lea Schönherr, Thorsten Eisenhofer, Steffen Zeiler, Thorsten Holz, and Dorothea Kolossa
Imperio: Robust Over-the-Air Adversarial Examples for Automatic Speech Recognition Systems
Annual Computer Security Applications Conference (ACSAC), 2020