Jonas Haglund

1991 Kraft Dr. SW, Suite 2001, Blacksburg, Virginia 24061, Virginia Tech, USA.

jonas_87@msn.com • • • • • • R[6]

Research Interests

My research interest involves the development of reliable computer systems. This includes work on low-level software such as operating systems that configure hardware, the hardware itself, including input/output devices, and formal verification using interactive theorem provers. Currently, my focus is on creating formally verified and synthesized device driver software for configuring direct memory access controllers (DMACs).

Previously, I concentrated on formally modeling DMACs and proving (using an interactive theorem prover) the conditions under which the DMACs can access specific memory regions. This involved examining an Ethernet DMAC as a case study and generalizing the results for most DMACs by identifying common DMAC features.

I am very interested in extending my research in the future to encompass functional properties, such as transmitted packets, instead of just memory isolation, but also other hardware components than DMACs. These components may include bus and network-on-chip interfaces and protocols, as well as the functional parts of I/O devices, such as the control logic in a USB controller and CPUs.

Education

KTH/EECS, Lindstedtsvägen 5, 114 28 Stockholm, Sweden 2016-10 – 2023-06
PhD in computer science with focus on formal verification of memory isolation in the context of DMA.

KTH/CSC, Lindstedtsvägen 5, 114 28 Stockholm, Sweden 2012-08 – 2016-10
Master in computer engineering with focus on general problem solving, formal methods, systems software and hardware.

KTH/CSC, Lindstedtsvägen 5, 114 28 Stockholm, Sweden 2010-08 – 2012-06
Continuation of bachelor in computer engineering with focus on computer science.

KTH/STH, Hälsovägen 11C, 141 57 Huddinge, Sweden 2007-08 - 2010-08
Start of bachelor in computer engineering with focus on computer networks.

Research Experience

ECE, Virginia Tech, 1991 Kraft Dr. SW, Blacksburg, Virginia 24061, United States 2023-08 - present

As a postdoctoral research associate I am working on formal verification of that device drivers configure I/O devices to respect memory isolation, and synthesis of such drivers.

Arm Ltd, 110 Fulbourn Road, Cambridge, CB1 9NJ, United Kingdom 2021-01 – 2021-02

A seven week internship where I worked on modeling and formalizing security properties of an ARM architecture.

RISE Research Institutes of Sweden, Isafjordsgatan 22, 164 40 Kista, Sweden 2016-03 – 2016-09

Worked on a research project (PROSPER) where I programmed parts of a hypervisor and extended a port of Linux to run on top of the hypervisor.

Teaching and Other Experiences

ECE, Virginia Tech, 1991 Kraft Dr. SW, Blacksburg, Virginia 24061, United States 2023-08 – 2024-05

I supervised Aditya Gawali's and Robbie Platt's master's thesis projects, about modeling and verifying DMA device drivers:

- Modeling and Synthesis of Linux DMA Device Drivers using HOL4. Aditya Gawali. May 7, 2024.
- Verification of DMAC Device Driver Operations in HOL4. Robert D. Platt. May 7, 2024.

KTH/EECS, Lindstedtsvägen 5, 114 28 Stockholm, Sweden 2016-10 – 2021-12

Teaching Assistance: I have been a teaching assistant during my PhD thesis research for the following courses (corresponding to one year of full-time work): Computer Security, Logic in Computer Science, Formal Methods and Algorithms, Data Structures and Complexity. I contributed with: planning tutorials, helping students with labs and graded labs, making assignments, and making and correcting exams. I have also developed lab assignments for the formal methods course involving C program verification and model checking.

Other: I was a member of the PhD computer science program council. I organized retreats for the PhD students, participated in a program evaluation, documented the program, attended Council meetings, announced PhD courses, and responded to PhD course requests. I have also reviewed three papers in the area of security and formal methods.

Publications

Haglund, Jonas. Formal Verification of Peripheral Memory Isolation. 2023-06

PhD thesis about formal verification (with interactive theorem proving) of memory isolation of I/O devices, that can be used to formally verify that device drivers configure their associated devices to access only certain memory regions.

Haglund, J., & Guanciale, R. Formally Verified Isolation of DMA. In A. Griggio & N. Rungta (Eds.), Proceedings of the 22nd Conference on Formal Methods in Computer-Aided Design – FMCAD 2022 (pp. 118–128). TU Wien Academic Press. DOI: https://doi.org/10.34727/2022/isbn.978-3-85448-053-2_18 2022-10

This paper describes a general model of DMA controllers which is formalized and verified with respect to memory isolation.

Haglund, J., Guanciale, R. Trustworthy isolation of DMA devices. J BANK FINANC TECHNOL 4, 75–94 (2020). DOI: https://doi.org/10.1007/s42786-020-00018-x 2020-05

A journal article that is an extension of the following article. Describes a monitor that checks that an Ethernet interface is isolated, with the monitor being a part of a hypervisor with Linux on top.

Haglund, J., Guanciale, R. (2019). Trustworthy Isolation of DMA Enabled Devices. In: Garg, D., Kumar, N., Shyamasundar, R. (eds) Information Systems Security. ICISS 2019. DOI: https://doi.org/10.1007/978-3-030-36945-3_3 2019-12

A case study of formally verifying the conditions under which an Ethernet interface controller can access only certain memory regions.

Professional Presentations

Paper at FMCAD 2022. 2022-10

Research Group Retreat. Described a formal model of a USB DMA controller. 2022-06

Seminar at KTH/EECS. Described a formal analysis tool of DMA controllers including a USB DMA controller. 2022-03

Seminar at KTH/EECS. Presentation of 80% of my PhD studies. 2021-11

Seminar at ARM. Described a formal analysis of memory isolation of an Ethernet controller, with a runtime monitor configuring the Ethernet controller to respect isolation. 2021-02

Seminar at KTH/EECS. Presentation of 50% of my PhD studies. 2020-06

Paper at International Conference in Information Systems Security (ICISS). 2019-12

Seminar at KTH/EECS. Presentation of 30% of my PhD studies. 2019-11

Poster presentation at Euro S&P. Described formal verification of memory isolation of an Ethernet DMA controller. 2019-06

Research Group Retreat. Described a formal model and a memory isolation proof of an Ethernet DMA controller. 2019-05

Expertise

Languages:
ARM assembly, C, Java, but also familiar with Verilog and VHDL.

Formal Methods:
Modeling hardware, formalization of properties, and formal proofs (interactive theorem proving; I have some experience with model checking, NuSMV, and deductive verification, Frama-C).

Systems Software:
Hypervisors and operating systems (mainly memory management and peripherals).

Interests and Future Learning

Hardware:
CPUs/Computer architecture, I/O and peripherals, and network-on-chips.

Systems software:
Operating systems and device drivers, hypervisors, and compilers.

Logic and formal verification:
Modeling and proofs in interactive theorem proving (mainly HOL4), including using it for development (synthesis) of hardware and software.

Personality

I like to have a deep understanding of concepts with details, and to achieve results with high quality. I also try to have a long-term perspective.