Jonas Haglund

jonas_87@msn.com • • • • • • • R⁶

Expertise

Languages:
C, **Standard ML**, **ARM assembly**, **Java**; also familiar with **Verilog** and **VHDL**.

Formal Methods:
Modeling hardware, formalizing properties, and formal proofs in interactive theorem proving (**HOL4, higer-order logic**). I also have experience in with model checking (**NuSMV, temporal logic**) and deductive verification (**Frama-C, Hoare logic**).

Systems Software:
Hypervisors and operating systems, mainly exception handling, memory management and device drivers in **Linux**.

Interests and Future Learning

Hardware:
CPUs/Computer architecture, I/O and devices, 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.

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 worked 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.

My future interests concern both **hardware** and **software**. Regarding **hardware**, 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. I am also interested in formally verifying timing properties. Regarding **software**, I am interested in learning about and formally verifying operating systems and hypervisors, for instance, interrupt management, process/task scheduling, memory allocation, network stack, power management, etc.

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.

This work involved modeling a DMA controller of a NIC of an SoC, including initialization, memory accesses, and teardown, and defining and verifying an invariant that implies that the DMA controller can access only certain memory regions. I also wrote an isolation monitor inside a hypervisor (a research hypervisor called PROSPER) whose purpose is to ensure that Linux, on top of the hypervisor, cannot reconfigure the DMA controller to access non-Linux memory (i.e., hypervisor or other guest memory). These results are a continuation of my master's thesis, and were generalized in the form of a general model of DMA controllers with verified memory isolation.

All this was demonstrated in the form of a CCTV system, where I paravirtualized Linux 5.15.13 to run on top of the hypervisor, on ARMv7, alongside an isolated camera driver guest. The camera driver guest takes and encrypts pictures and hands them over to Linux (via the hypervisor) when Linux requests so. The result is that the CCTV system can send encrypted pictures over the Internet, avoiding trusting all the complex Linux software involved to not leak plain pictures.

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 - 2025-02

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.