THE UNIVERSITY OF QUEENSLAND

AUSTRALIA

Title here:

Name

Candidate’s academic degrees

Candidate’s ORCID

A thesis submitted for the degree of Doctor {Master} of Philosophy at The University of Queensland in {year}

Name of the Enrolling Unit

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Topic Definition

In recent years, growth of the Internet of Things (IoT) has led to an unprecedented increase in the number of internet-connected devices, with estimates suggesting that there will be over 75 billion IoT devices by 2025 [1]. However, this growth has brought to attention the importance of network security in embedded systems, especially where sensitive data is handled. Cyber-attacks targeting IoT devices have become more sophisticated and frequent, with the number of IoT attacks increasing by 300% in 2019 alone [2]. The financial impact of these attacks is staggering, with the annual cost of data breaches speculated to reach $10.5 trillion by 2025 [3].

Trends in the IoT space such as edge computing, 5G networks, and artificial intelligence (AI) are sky-rocketing the demand for highly-performant processing solutions [4] while traditional software-based security approaches often struggle to keep up with the real-time requirements and resource constraints of IoT devices [5]. Frustaci et al. [5] highlight the limited memory, processing power, and energy resources of IoT devices make it challenging to implement strong security measures using software alone without compromising performance and battery life. This is where FPGAs can offer a solution. By leveraging the flexibility of FPGAs, it is possible to create an optomised and dedicated network security solution.

This thesis proposes the development of a RISC-V softcore processor specifically designed for network security in embedded IoT applications. The use of RISC-V has several advantages over other contemporary architectures. For one, it is an open-source instruction set architecture that is concise, modular, and extensible [6]. Its open nature allows for customization of the processor design to meet specific requirements, while its modular design enables the addition of custom instructions and extensions to emphasise security-related tasks [7]. With this, the project aims to show how a dedicated solution can mitigate potential threats at the hardware level.

1.1.1 Aims

The aims for a successful FPGA-based edge device are as follows:

1. Increase network security.
2. Minimise processing latency.
3. Maximise power efficiency.
4. Minimise Resource Utilisation.

1.1.2 Key Performance Indicators

The previous aims will then be evaluated against the following criteria:

1. **Network Security:**
   Penetration testing and vulnerability assessments will be conducted against a chosen network security method, see section 1.2. The number and severity of detected security threats will gauge the effectiveness of the security features. The subsequent key performance indicators also contribute to overall network security.

2. **Processing Latency:**
   packet processing time will be measured under various idle, average and peak network conditions. This will involve testing the system with different packet sizes and security features enabled to assess the impact on latency. The latency results will also be compared with similar security solutions to benchmark the performance of the FPGA-based processor.

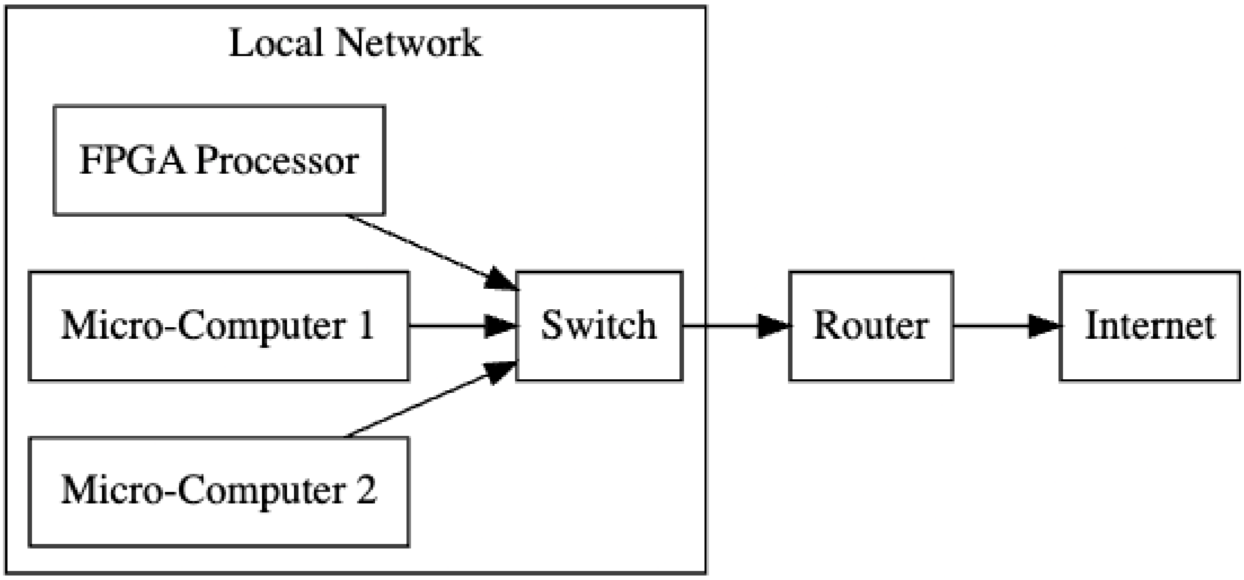
3. **Power Efficiency:**
   Power consumption will be measured during idle, average, and peak loads. The energy efficiency ratio (performance per watt) will be calculated to provide a standardized metric for comparison. The power efficiency of the system will be compared with other FPGA-based and software-based solutions to assess its relative performance. Also, a thermal camera will be used to visualise the heat radiation from the FPGA. There is also the possibility of using the integrated temperature sensor on the Arty S7 Board [8] for plots.

4. **Resource Utilisation:**
   Resource utilization will be evaluated by measuring the counts of FPGA resources in the FPGA design software, such as look-up tables (LUTs), flip-flops and block RAM (BRAM). Memory and CPU utilization on the target IoT devices will also be observed to ensure the system does not overburden the limited resources available.

1.2 Project Overview

This section will now pertain to the complete hardware and software stack of of the proposed solution. A high-level overview of which can be seen in figure 1.1.

Figure 1.1: High-Level Network Overview



Here, the local network refers to the arrangement of the edge devices in the network (left-hand side). It consists of the project's primary focus, the RISC-V softcore processor as well as two microcomputers which will be implemented as Raspberry Pis, (RPis). On the right hand side is the router which will interface the local network with the external internet structure, allowing packets to be received externally.

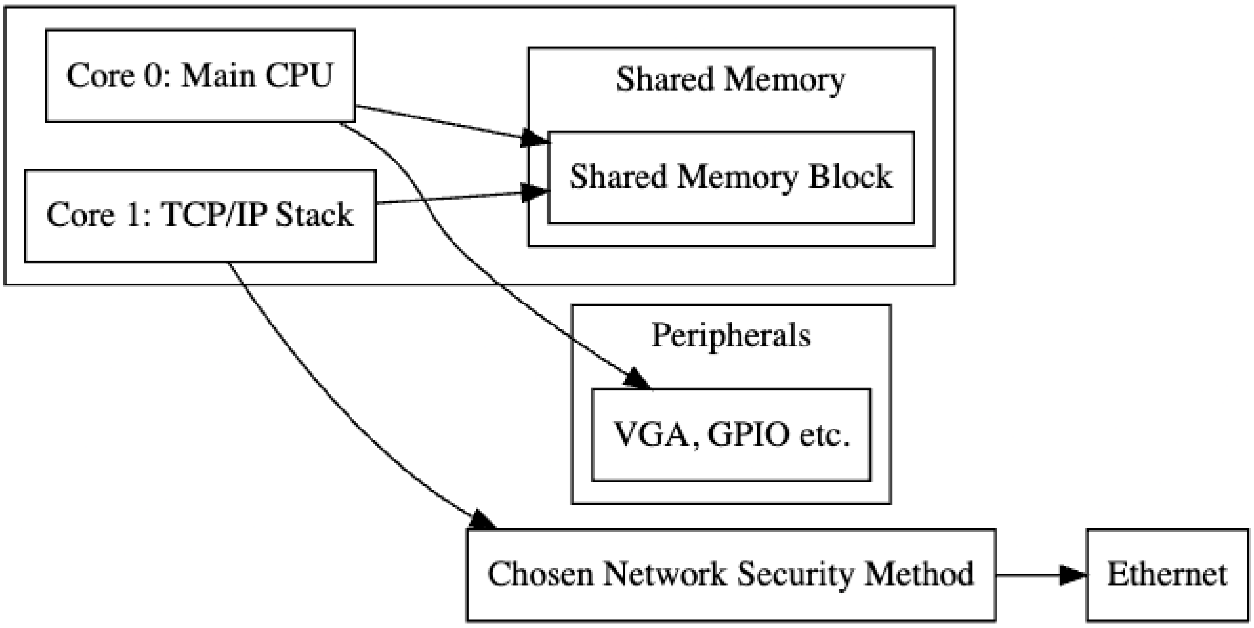
1.2.1 FPGA Processor

The FPGA will be running a real-time operating system, Zephyr. Zephyr has support for multicore designs as well as support for many types of peripherals and networking services. Functionality will be split across two cores as seen in figure 1.2. Core 0, will be the main core which will handle task-dispatching as well as peripheral interfacing (VGA, GPIO *etc.*). Like Core 1, which will handle the networking stack, it has access to a unified, shared memory block allowing it to subsequently access the processed packets. As the project progresses, the resource allocation for each core will be adjusted exclusively to their requirements.

1.2.2 Microcomputers

Basic software containers, deployed via Kubernetes, will run on the Microcomputers. These images will contain established libraries that provide TCP/IP stack interfacing as well as the ability to send/receive packets.

Figure 1.2: High-Level FPGA Architecture Overview



1.2.3 Switch

It has not been decided yet which switch will be used. Furthermore, communication protocols for the chosen commercial switch will need to be researched.

1.2.4 Router

Same as the switch, it has not been decided yet which router will be used.

1.2.5 Chosen Network Security Method

To emphasise the network security aspect of the project, an additional layer of network security will be designed and implemented. It has not yet been decided which network security method will be used. Here, a custom hardware component will be designed that implements a typical network security method such as an accelerated cryptographic processor or a firewall that filters packets. The possible options are elaborated on in 2.2.1

Chapter 2

Literature Review

2.1 Internet of Things (IoT)

2.2 Network Stacks

2.2.1 Network Security Methods

Packet Filtering

Cryptographic Acceleration

2.3 Operating Systems

2.3.1 Real-Time Operating Systems (RTOSs)

2.3.2 Kubernetes Clusters

2.4 Instruction Set Architectures (ISAs)

2.4.1 RISC-V

2.5 Field Programmable Gate Arrays (FPGAs)

Chapter 3

Project Plan

3.1 Milestones and Timeline

Below is the full outline and expected completion for each milestone:

Table 3.1: Proposed Milestone Timeline

Task	Description	Due (by end of week)
Proposal*	Project proposal	Sem 1, Week 8
Program Microcomputers	Deploy Kubernetes cluster to microcomputers	Sem1, Week 9
Interface Microcomputers	Have the local area network completely set up and RPis interfaced to switch	Sem1, Week 10
Seminar*	Present Seminar	Week 11
Design the RISC-V softcore Processor	Implement proposed FPGA design	Break, Week 1
Run Zephyr	Flash and run Zephyr on the softcore processor.	Break Week 2
Interface TCP/IP stack core	Get the FPGA interfaced in the LAN	Break, Week 3
Create Network Security Component	Create and implement the chosen network security method	Break Week, 3-4
Experimentation	Start taking measurements	Sem 2, Week 1
Measure and Compare	Compare measurements to preexisting solutions	Sem 2, Week 2
Poster & Demonstration*	Thesis project demonstration	Sem 2, Week 11
Thesis*	Thesis Write-up	Sem 2, Week 14

Bibliography

[1] T. Alam, “A reliable communication framework and its use in internet of things (iot),” *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 3, 05 2018.

[2] M. Michael, “Attack landscape h1 2019: Iot, smb traffic abound,” 09 2019. Accessed: 2023-03-20.

[3] S. Morgan, “Cybercrime to cost the world $10.5 trillion annually by 2025,” 11 2020. Accessed: 2023-05-27.

[4] N. Nuttall, “Top strategic iot trends and technologies through 2023,” September 2018. Accessed: 2023-05-27.

[5] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, “Evaluating critical security issues of the iot world: Present and future challenges,” *IEEE Internet of Things Journal*, vol. 5, pp. 2483–2495, October 2017.

[6] D. A. Patterson and A. Waterman, “The risc-v revolution,” in *2017 IEEE International Conference on Computer Design (ICCD)*, pp. 1–5, 2017.

[7] A. Waterman, Y. Lee, R. Avizienis, D. A. Patterson, and K. Asanović, “The risc-v instruction set manual volume ii: Privileged architecture version 1.9.1,” Tech. Rep. UCB/EECS-2016-161, EECS Department, University of California, Berkeley, Nov 2016.

[8] Digilent, *Arty S7 Reference Manual*, October 2019.