This is the Project Title

Andreas Ramsøy

**MInf Project (Part 2) Report**

Master of Informatics

School of Informatics

University of Edinburgh

2022

Abstract

This skeleton demonstrates how to use the infthesis style for undergraduate dissertations in the School of Informatics. It also emphasises the page limit, and that you must not deviate from the required style. The file skeleton.tex generates this document and can be used as a starting point for your thesis. The abstract should summarise your report and fit in the space on the first page

Acknowledgements

Acknowledgements go here.

Table of Contents

[Introduction 1](#_Toc85826368)

[Background 2](#_Toc85826369)

[2.X.X Operating Systems 2](#_Toc85826370)

[2.X.X Popcorn 2](#_Toc85826371)

[2.X.X Summary of MInf 1 3](#_Toc85826372)

[2.X.X Distributed Operating Systems 3](#_Toc85826373)

[2.X.X Capabilities 4](#_Toc85826374)

[2.X.X Amoeba 5](#_Toc85826375)

[2.X.X CAP 6](#_Toc85826376)

[2.X.X Plan 9 6](#_Toc85826377)

[2.X.X Kerrighed 7](#_Toc85826378)

[Bibliography 9](#_Toc85826379)

Chapter 1

# Introduction

This is the introduction

The aims of the project

Subsection of previous project summary, better in background so can explain concepts?

Short summary of last year’s work

The motivation of the research/why it’s important

Outline of how the paper is structured

Chapter 2

# Background

### 2.X.X Operating Systems

All the fundamental services of the computer’s software are provided by the operating system kernel e.g., scheduling, memory management, inter-process communication [1]. Operating systems must be exceptionally fast as to not introduce overheads to the programs that users run. They are difficult to debug and so should ideally be free from errors [1].

A so-called micro-kernel is an operating system designed to be as small as possible. As many of the services are implemented as applications as opposed to within the kernel. This is called the principle of minimality and is used to make the development of micro-kernels easier to manage [2]. This is compared to larger operating system kernels that their large size and interdependency means an error in one system can cause errors in others [2]. Developing these systems in user-space means that the operating system is better able to detect errors and better able to recover from them.

Multi-kernel operating systems are a network of independent cores that do not share resources at the lowest level [3]. Multi-kernel operating systems are better suited for heterogeneity of hardware since the use of message passing allows them to not be restricted by the differences in the hardware design of different processors [3].

### 2.X.X Popcorn

Popcorn is a multi-kernel operating system based on Linux. It provides a single system image to the user despite being split across multiple processors or groups of processors [4]. Each node, that is a processor or group of processors, run Popcorn with a single cache coherent memory linking them together [4]. Popcorn allows for heterogeneity between nodes [4].

### 2.X.X Summary of MInf 1

The first part of this project (MInf 1) worked to modify the existing Popcorn operating system to allow for multiple communication protocols to be used at the same time by nodes, and to allow nodes to be dynamically added to the system without requiring reloading the kernel module [5].

Previously, Popcorn required all connected nodes to use the same communication protocol (e.g., TCP, RDMA) between all nodes. The modifications allowed for independent protocols to be used for different nodes. This was done in such a way that only the protocols being used are loaded. They are unloaded when the nodes using it is removed so no additional resources are used.

Before last year’s project, Popcorn would only allow a list of nodes that should be connected to during the loading of the module. This was changed to load with no other nodes attached and established a joining protocol to allow other nodes to join. A proc file was used to send commands to the kernel module. Several joining protocols were considered but the final solution was chosen due to its scalability. It achieved this by forwarding messages to just two nodes each in the network, each node it passes it to forwards this message to another pair of nodes until all nodes have established a connection.

Evaluation of the implementation showed that the new features (which require some extra checks to take place) caused minimal slowdown to the system when compared to the previous version.

The goals of this project highlighted in last year’s project were: “I intend to finish providing security and authentication between nodes, add flow control to the Popcorn command messages, add functionality to remove nodes, create a command utility that allows for connection of nodes in a more user-friendly way and perform a more in-depth evaluation of Popcorn including the use of real hardware. ”

### 2.X.X Distributed Operating Systems

“The users of a true distributed system should not know (or care) on which machine (or machines) their programs are running, where their files are stored, and so on. ” [6]

There are three broad categories of distributed operating systems referred to as the “minicomputer”, “workstation”, and “processor pool” models [6]. The minicomputer model is where each device on the network has multiple users a user logs into a machine. The logged in user uses that machine but also has remote access to the others on the network [6]. The workstation model is where the user has a powerful machine that does the bulk of the work but with some distributed services like a shared file system. Finally, the processor pool model is where a group of processors are available to each user, where users can use a flexible number of processors (between them and the other users on the system [6].

A problem with distributed systems is maintaining naming consistency across different machines. E.g., two user may have the same user ID (UID) on different devices, they should not however be considered the same user, or have the same privileges when accessing resources on the other machine. As a result distributed systems either login through a centralised system or use the name of the computer that they are logged into as part of their UID (it can be thought of as user@device\_name). Another solutions are to create a user of minimum privileges (e.g., demo user), however this means users not logged on to that machine have fewer privileges than ideal. It is considered that a true distributed system should have a unique UID for each user that is used across the system [6]. But this requires a shared structure that must be kept consistent across the network.

The OSI has significant overheads so message passing is generally favoured for distributed operating systems [6]. Using message passing it must be decided whether to use blocking vs non-blocking, and reliable vs unreliable messages. This refers to code that is required to wait until a message is received vs being allowed to other things in the meantime and confirming if the message was delivered vs not confirming, respectively [6].

### 2.X.X Capabilities

A capability is a descriptor that contains a unique ID that represents a server process. This ID is cryptographically linked to the process it describes in such a way that only the server can understand which process it is for [7]. This provides protection to the process as only a user or process with the correct capability can access the protected resource (another process, memory, etc.). The rights that are granted can be specific privileges to that resource (e.g. write, read-only, execute) [8].

For a system using capabilities to remain secure it must be ensured that capabilities cannot be modified, only authorised interfaces can create them, and they are only given to processes that are authorised [9].

Capabilities can provide a secure method of granting privileges. however, they are difficult to revoke after creation. For this reason, many capability-based systems either use an access control or an intermediate system (referred to as a reference monitor in EROS) to stop revoked capabilities being used [9].

### 2.X.X Amoeba

The motivation behind Amoeba was to build a system where all resources are automatically managed by a distributed operating system [10]. As a consequence, users do not know which processor their programs run on, or how and where their files are stored in the system [10].

Amoeba provides a combination of the processor pool and workstation model where users are able to login to a particular machine but also run large jobs on a pool of processors [6].

In Amoeba users log into a terminal computer. This device does all the low latency computation whereas the group of computers known as the “processor pool” does all the larger computations [11].

Amoeba has had several iterations of file systems however, the simpler “bullet service” that stores immutable files as contiguous bytes [10].

Amoeba makes use of heterogeneity by using different machines for specialised purposes e.g., devices with large storage disks are used for file storage [10].

Amoeba’s design allows for great scalability, fault tolerance, and for processes to temporarily acquire large processing power [10].

To increase reliability new objects in a directory are replicated a set number of times and distributed across different nodes [10]. Capabilities are then stored in the directory along with the files [10].

To maintain security capabilities are used. By using a sufficiently large address space and having capabilities cryptographically linked to the resource that they are protecting, this protects the capability and therefore the resource it is protecting [10]. The use of cryptography allows capabilities to be safely used within user-space, thus following the principle of minimality and simplifying the kernel [10].

A hash of the port number that the message was sent on along with a shared secret means that an adversary cannot gain access to this [10]. This can be implemented in software or hardware but there should be no way of bypassing this function [10].

Capabilities are distributed meaning that transfers cannot be detected, this means that to allow mandatory access control a system within the kernel needs to be implemented [9].

Capabilities are not used for individual pages or memory mapped structures but instead larger structures [9].

For directories, encryption key and a random value are XORed together. The result is stored in the directory itself and the capability given to the user that owns the file. When the file is requested by the user they provide their capability along with the random value. This means only the owner is able to decrypt the directory [10].

New capabilities that have a subset of rights of the other can be created by the owner [11].

Amoeba relies on the security of the capabilities and there any messages carrying them need to be encrypted to maintain the security of the system [11]. Two different systems can provide security to the network: one is a Kerberos like authentication server, and the other uses hashes. The authentication server results in a slower system however, the second system assumes a secure network and kernel [11].

### 2.X.X CAP

The virtual address space is mapped to a physical address space used across all devices [8].

CAP can have a hierarchical structure to represent processes. The position in the hierarchy is used to regulate the resources that the process has access to [12].

Capabilities can be used to restrict memory for example, each capability lists a maximum and minimum contiguous memory range that the permissions are for. A child capability can be generated from this that gives a maximum and minimum memory value relative to its parent. This way only memory in range of the parent can be used by the child. Any number of levels parent-child capabilities can be made [12].

CAP restricts users from procedures using a capability. to restrict who can run it, this is opposed to the conventional way operating systems determine each of the things done are allowed (and throws error when this happens) [12].

### 2.X.X Plan 9

Plan 9 allows for heterogeneity; different processor architectures are able to join the network running Plan 9 [13]. Messages are transferred between nodes in a high-level way, e.g. text, when possible as this simplifies the kernel when dealing with different processor architectures (however, binary can still be used for large transfers of data) [13].

Plan 9 interacts with services as if they are files and uses file operations as such. This means one simple, well understood protocol can be used to access almost all services [13].

Authentication between nodes is conducted by solving encrypting/decrypting challenge messages with some key [13]. Following both of the nodes success on the challenge messages one of the nodes sends a message to the authentication server. The authentication server then sends a message to both nodes containing a conversation key. The message that the authentication server is encrypted such that only that node can get the conversation key. The conversation key is then used to encrypt the conversation from then on [13].

This method does not rely on a synchronized clock, unlike Kerberos [13].

In Plan 9 the use of the same secured protocol to represent services rather than the use of firewalls means security is implemented in any Plan 9 service from the start [13].

There is no superuser, each individual server must ensure security (physical access to the server does give special permissions) [13].

### 2.X.X Kerrighed

Kerrighed is an operating system for clusters [14]. It provides a single system image to the end user [14]. Kerrighed is built from Linux with some kernel modules added [14]. This has the advantage of existing programs being able to be recompiled to work on a cluster and do not require any further modification [14]. Kerrighed allows for memory sharing and message passing between nodes on a cluster [14].

# Bibliography

|  |  |
| --- | --- |
| [1] | E. Novikov and I. Zakharov, “Verification of Operating System Monolithic Kernels Without Extensions,” 30 October 2018. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-03427-6\_19. [Accessed 6 November 2020]. |
| [2] | B. Roch, “Monolithic kernel vs. Microkernel,” 2004. [Online]. Available: http://web.cs.wpi.edu/~cs3013/c12/Papers/Roch\_Microkernels.pdf. [Accessed 2 November 2020]. |
| [3] | A. Baumann, P. Barham, P.-E. Dagand, T. Harris, R. Isaacs, S. Peter, T. Roscoe, A. Schüpbach and A. Singhania, “The Multikernel: A New OS Architecture for Scalable Multicore Systems,” October 2009. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1629575.1629579?casa\_token=I7\_hNx4wHdsAAAAA:0SVwWy0PBIxp-ZjoK3g9NLYR0uT1tJUHc29C2HBgPjo\_VysRDtqGmfp1-3Swdqh6lng4qYOkTf3vKg. [Accessed 8 November 2020]. |
| [4] | M. Sadini, A. Barbalace, B. Ravindran and F. Quaglia, “A Page Coherency Protocol for Popcorn Replicated-kernel Operating System,” 2013. [Online]. Available: http://www.popcornlinux.org/images/publications/marc2013\_camera\_ready\_fixed.pdf. [Accessed 21 October 2020]. |
| [5] | A. Ramsøy, “A Scalable Node Management Structure and Joining Protocol,” 25 April 2020. [Online]. Available: https://drive.google.com/file/d/1g8kiPErOtCLB8Fy-v3gVgQo5qDO3VJSe/view?usp=sharing. [Accessed 22 October 2021]. |
| [6] | A. S. Tanenbaum and R. V. Renesse, “Distributed Operating Systems,” December 1985. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/6041.6074. [Accessed 17 June 2021]. |
| [7] | J. S. Shapiro, “The EROS System Structure,” 11 January 2007. [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.108.5173&rep=rep1&type=pdf. [Accessed 15 October 2021]. |
| [8] | R. Achermann, D. Cock, R. Haecki, N. Hossle, L. Humbel, T. Roscoe and D. Schwyn, “mmapx: Uniform memory protection in a heterogeneous world,” 1 June 2021. [Online]. Available: https://sigops.org/s/conferences/hotos/2021/papers/hotos21-s08-achermann.pdf. [Accessed 23 September 2021]. |
| [9] | J. S. Shapiro, J. M. Smith and D. J. Farber, “EROS: a fast capability system,” 12 December 1999. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/319151.319163. [Accessed 14 October 2021]. |
| [10] | S. Mullender, G. v. Rossum, A. Tananbaum, R. v. Renesse and H. v. Staveren, “Amoeba: a distributed operating system for the 1990s,” May 1990. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/53354. [Accessed 28 May 2021]. |
| [11] | A. S. Tanenbaum, R. v. Renesse, H. v. Staveren, G. J. Sharp and S. J. Mullender, “Experiences with the Amoeba distributed operating system,” 1 December 1990. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/96267.96281. [Accessed 10 June 2021]. |
| [12] | R. Needham and R. Walker, “The Cambridge CAP Computer and its protection system,” November 1997. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/1067625.806541. [Accessed 27 September 2021]. |
| [13] | R. Pike, D. Presotto, S. Dorward, B. Flandrena, K. Thompson, H. Trickey and P. Winterbottom, “Plan 9 from Bell Labs,” no date. [Online]. Available: http://9p.io/sys/doc/9.html. [Accessed 2 September 2021]. |
| [14] | C. Morin, R. Lottiaux, G. Vallée, P. Gallard, G. Utard, R. Badrinath and L. Rilling, “Kerrighed: A Single System Image Cluster Operating System for High Performance Computing,” 1 June 2004. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-45209-6\_175. [Accessed 13 October 2021]. |
| [15] | M. Accetta, R. Baron, W. Bolosky, D. Golub, R. Rashid, A. Tevanian and M. Young, “Mach: A New Kernel Foundation For UNIX Development,” 1986. [Online]. Available: http://cseweb.ucsd.edu/classes/wi11/cse221/papers/accetta86.pdf. [Accessed 8 November 2020]. |
| [16] | A. Barbalace, A. Murray, R. Lyerly and B. Ravindran, “Towards Operating System Support for Heterogeneous-ISA Platforms,” April 2014. [Online]. Available: http://www.popcornlinux.org/images/publications/sfma14.pdf. [Accessed 21 October 2020]. |
| [17] | D. L. Black, D. B. Golub, D. P. Julin, R. F. Rashid, R. P. Draves, R. W. Dean, A. Forin, J. Barrera, H. Tokuda, G. Malan and D. Bohman, “Microkernel Operating System Architecture and Mach,” 30 April 1992. [Online]. Available: https://courses.cs.washington.edu/courses/cse451/15wi/lectures/extra/Black92.pdf. [Accessed 8 November 2020]. |
| [18] | J. Corbet, “Popcorn Linux pops up on linux-kernel,” 5 May 2020. [Online]. Available: https://lwn.net/Articles/819237/. [Accessed 25 October 2020]. |
| [19] | R. Krten, “Getting Started with QNX Neutrino: A Guide for Realtime Programmers,” 2008. [Online]. Available: http://jedrzej.ulasiewicz.staff.iiar.pwr.wroc.pl/Neutrino/getting\_started.pdf. [Accessed 8 November 2020]. |
| [20] | S. Peter, A. Schüpbach, D. Menzi and T. Roscoe, “Early experience with the Barrelfish OS and the Single-Chip Cloud Computer,” 2011. [Online]. Available: https://people.inf.ethz.ch/troscoe/pubs/marc11-barrelfish.pdf. [Accessed 8 November 2020]. |
| [21] | R.F.Rashid and H.Tokuda, “Mach: A system software kernel,” 15 June 1990. [Online]. Available: https://www.sciencedirect.com/science/article/pii/0956052190900045. [Accessed 20 October 2020]. |
| [22] | A. Barbalace, B. Ravindran and D. Katz, “Popcorn: a replicated-kernel OS based on Linux,” 2014. [Online]. Available: https://www.linuxsecrets.com/kdocs/ols/2014/ols2014-barbalace.pdf. [Accessed 10 April 2021]. |
| [23] | “Openmach Git Repository,” [Online]. Available: https://github.com/openmach/openmach/blob/master/include/mach/message.h. [Accessed 8 November 2020]. |
| [24] | “Structure of monolithic kernel, microkernel and hybrid kernel-based operating systems,” 17 July 2008. [Online]. Available: https://en.wikipedia.org/wiki/Monolithic\_kernel#/media/File:OS-structure2.svg. [Accessed 8 November 2020]. |
| [25] | Shubham, “What is kernel - monolithic and microkernel,” 29 January 2018. [Online]. Available: https://medium.com/@shrimantshubham/what-is-kernel-microkernel-and-monolithic-kernel-66c6de358b43. [Accessed 18 April 2021]. |
| [26] | A. Barbalace, B. Ravindran and D. Katz, “Popcorn: a replicated-kernel OS based on Linux,” 2014. [Online]. Available: https://www.linuxsecrets.com/kdocs/ols/2014/ols2014-barbalace.pdf. [Accessed 19 April 2021]. |
| [27] | B. Ravindran, “Replicated-kernel Linux,” [Online]. Available: http://popcornlinux.org/index.php/replicated-kernel-linux. [Accessed 19 April 2021]. |