Project specification DD2497
Group 2

Virtio Queue Monitor in s3k

Elias Lundgren

Erik Persson

Linus Below Blomkvist

Fredrik Gölman

Introduction

Currently the virtIO disk driver has the ability to access any memory without adhering to the rules defined by the s3k capabilities. To combat this, we want to insert a monitor on the virtIO Queue to always check that the process has enough capabilities to execute the next action in the queue.

This is important to stop an attacker from reading, writing or executing things in memory that they don't have access to. A monitor on the queue would entail some hits to performance, but like other secure microkernels, the focus is not generally on performance but reliability and security.

Attacker Perspective

Currently an attacker could use the virtIO Queue to access portions of memory without having the required capabilities. This opens up s3k to code injection and execution and in general full access to the memory.

Defender Perspective

We want to keep track of which memory ranges each process can read from and write to during runtime. Optionally we may want to attempt to mitigate code injection and execution.

Description of possible vulnerabilities countered by our project

- Unauthorized memory access (read/write)
- Code injection and execution

Requirements

Our project should at least cover a detailed explanation of the causes of the vulnerabilities and some hypothetical countermeasures. It should also cover a monitor that checks the capability. The project should not create additional security vulnerabilities. The project should also cover how the monitoring affects the performance, i.e the cost of monitoring.

Optional Requirements

The monitor should be as efficient as possible, both in memory and processing requirements. Another optional requirement could be to make this monitoring system work for virtual network devices as well, however we don’t see this as feasible seeing as there is currently no network stack implemented in the s3k architecture.