

IPC Side-channel Attacks

Advisor: **Roland Czerny**

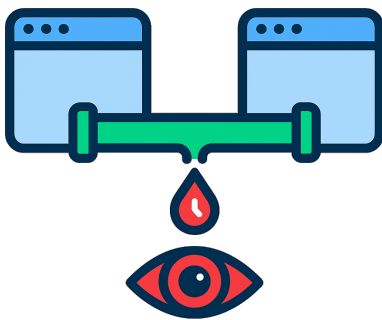
Motivation

Inter-process communication (IPC) on Unix/Linux systems happens through sockets and message buses such as D-Bus. These channels are essential for programs to work together, but they also create side effects in timing and queues. Even if the content of messages is hidden, such effects may still reveal information. The question is: can an attacker learn something simply by observing IPC behavior?

The topic is open — you can look at different IPC mechanisms and decide the direction together with your advisor.

Goals and Tasks

-  Learn about IPC on Unix/Linux and read related research.
-  Come up with simple experiments to test if timing or queue effects leak information.
-  Write small test programs to measure and analyze possible leaks.



Literature

- > [A. Silberschatz, P. B. Galvin, and G. Gagne](#)
Operating System Concepts, Chapter 20.9 Interprocess Communication
2018
- > [L. Maar et al.](#)
KernelSnitch: Side-Channel Attacks on Kernel Data Structures
[NDSS](#)

Courses & Deliverables

☒ Master Project

Project code
Report
Presentation

– OR –

☒ Master's Thesis

Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☒ CS ☒ ICE ☒ SEM

Prerequisites

- > Basic operating system knowledge (processes, IPC)
- > Some programming experience (Python or C)
- > Interest in system security

Advisor Contact

roland.czerny@tugraz.at