Lucerne University of Applied Sciences and Arts

Practical De-Anonymization in the Tor Network

Timing Leaks, Traffic Correlation, and Website Fingerprinting

Bachelor Thesis

Study Program: Information & Cyber Security

Oliver TODO
Zürich (Switzerland)

Defense Date: TODO
Defense Location: Rotkreuz

Supervisor: TODO
External Expert: TODO
Industry Partner: TODO

2026

Acknowledgments

Thanks to my family, relatives, and friends for all the support given to finish this thesis.

Abstract

The content of your thesis in brief.

Contents

List of Figures

List of Tables

List of Acronyms

HSLU — Lucerne University of Applied Sciences and Arts
Tor — The Onion Router
WF — Website Fingerprinting
ISP — Internet Service Provider
NN — Neural Network
IDS — Intrusion Detection System

1 Problem Statement, Research Questions, and Vision

1.1 Problem Statement

The Tor network is widely considered secure, yet theoretical studies demonstrate that timing analyses and traffic correlation attacks can compromise user anonymity. However, practical investigations under controlled, local conditions remain scarce.

1.2 Research Questions

1. Can Website Fingerprinting attacks successfully de-anonymize Tor users in a locally simulated Shadow network?
2. To what extent do Tor's built-in circuit padding mechanisms reduce detection accuracy of such attacks?
3. What bandwidth and latency overhead do these defenses introduce?

1.3 Vision

2 State of Research

This chapter reviews existing research on Tor anonymization, website fingerprinting attacks, traffic analysis techniques, and circuit padding defenses.

3 Ideas and Concepts

4 Method(s)

4.1 Phase 1: Shadow Network Setup

Tor network simulation using Shadow/tornettools, Wikipedia mirror cloning, and wget2-based client configuration.

4.2 Phase 2: Baseline Data Collection

Packet capture and feature extraction from client nodes; training and evaluation of WF classifiers (e.g.
Deep Fingerprinting CNN).

4.3 Phase 3: Circuit Padding Activation

Configuration of Tor's built-in padding mechanisms at various levels and corresponding data collection.

4.4 Phase 4: Comparison and Analysis

Comparative analysis of detection rates with and without padding, overhead measurement, and trade-off quantification.

5 Implementation

5.1 Baseline WF Attack Results

5.2 Circuit Padding Configuration

6 Validation and Evaluation

6.1 Performance Overhead

6.2 Limitations

7 Outlook

7.1 Ethical Considerations

Reflection on ethical aspects of the research.

7.2 Future Work

A Appendices

A.1 Task Description

A.2 Project Management