Evaluating the Efficacy of Gaussian Padding on Website Fingerprinting Attacks

Master thesis by Johannes Leupold
Date of submission: 01.09.2021

1. Review: Jean-Paul Degabriele
2. Review: Some Other Guy
Darmstadt

TECHNISCHE UNIVERSITÄT DARMSTADT

Computer Science Department

IT Security

Cryptography and Network Security

Erklärung zur Abschlussarbeit gemäß §22 Abs. 7 APB TU Darmstadt

Hiermit versichere ich, Johannes Leupold, die vorliegende Masterarbeit gemäß §22 Abs. 7 APB der TU Darmstadt ohne Hilfe Dritter und nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die Quellen entnommen wurden, sind als solche kenntlich gemacht worden. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Mir ist bekannt, dass im Falle eines Plagiats (§38 Abs. 2 APB) ein Täuschungsversuch vorliegt, der dazu führt, dass die Arbeit mit 5,0 bewertet und damit ein Prüfungsversuch verbraucht wird. Abschlussarbeiten dürfen nur einmal wiederholt werden.

Bei einer Thesis des Fachbereichs Architektur entspricht die eingereichte elektronische Fassung dem vorgestellten Modell und den vorgelegten Plänen.

Darmstadt, 01.09.2021

J. Leupold

Abstract

Abstract

Contents

1 Introduction

This is the introduction.

2 Background Material

2.1 Theoretical Setting

2.1.1 Threat Model

2.1.2 Attacks and Defenses

2.2 Gaussian Padding

2.3 Security Bound Estimation according to Cherubin [1]

3 Prior Work

4 Experimental Methodology

4.1 Trace Data

4.2 Evaluating Attack Performance

4.3 Error Bound Estimation

5 Results

5.1 Empirical Performance of Gaussian Padding

5.2 Estimated Security Bounds

6 Discussion

7 Conclusion

Bibliography

[1] Giovanni Cherubin. “Bayes, not Naïve: Security Bounds on Website Fingerprinting Defenses”. In: *Proceedings on Privacy Enhancing Technologies* 2017.4 (Oct. 2017), pp. 215–231. DOI: 10.1515/popets-2017-0046. URL: https://petsymposium.org/2017/papers/issue4/paper50-2017-4-source.pdf.

List of Figures

List of Tables