Cyprus University of Technology
Faculty of Engineering and Technology

**Bachelor's Thesis**

# Exploring the fingerprintability of honeypot systems, based on observed discrepancies, and designing and proposing techniques for preventing detection

**Stylianos Kyriakou**

**Limassol, May 2025**

Τεχνολογικό Πανεπιστήμιο Κύπρου

**ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ**

## ΗΜΠ 412 -Διπλωματική Εργασία Ακαδημαϊκό έτος 2024-2025

**Όνομα Φοιτητή / ΑΦΤ :** Στυλιανός Κυριάκου / 22603

Βαθμός: 9.0

**Τίτλος:** Study the fingerprintability of honeypot systems, based on observed discrepancies and designing and proposing techniques for prevention

**Επιβλέπων Καθηγητής:**

| Όνομα | Υπογραφή | Ημερ. |
|---|---|---|
| Παναγιώτης Ηλία | | 3/6/2025 |

**Εξεταστής 1:**

| Όνομα | Υπογραφή | Ημερ. |
|---|---|---|
| Αντρέας Δημοσθένους | | 3/6/2025 |

**Εξεταστής 2:**

| Όνομα | Υπογραφή | Ημερ. |
|---|---|---|
| Χρίστος Λοΐζου | | 3/6/2025 |

CYPRUS UNIVERSITY OF TECHNOLOGY

FACULTY OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER ENGINEERING AND INFORMATICS

Bachelor's Thesis

# Exploring the fingerprintability of honeypot systems, based on observed discrepancies, and designing and proposing techniques for preventing detection

**Stylianos Kyriakou**

Supervisor

Faculty of Engineering and Technology

Dr. Panagiotis Ilia

Lecturer in the Department of Electrical Engineering,

Computer Engineering and Informatics

Limassol, May 2025

## Copyrights

Copyright© 2025 Stylianos Kyriakou

All rights reserved.

The approval of the thesis by the Department of Electrical Engineering, Computer Engineering and Informatics does not imply necessarily the approval by the Department of the views of the writer.

I would like to thank my professors for helping me achieve my goals and complete this thesis. This wouldn’t have been possible without my supervisor Dr. Panagiotis Ilia. I am very grateful for the support that my friends and family have given me throughout my academic journey.

# ABSTRACT

Cybersecurity is a crucial aspect of today's highly interconnected world. Nowadays, everything is connected to the internet, exposing a potentially broad surface to attacks, since everything is susceptible. From personal computers, to servers, cloud infrastructure, mobile devices, sensors, and even electrical appliances - almost every device we use in our daily life - is potentially vulnerable and susceptible to attacks, and is being attacked daily. One technology that has been designed and deployed to help us better understand how attackers and malicious actors act, is honeypots. Honeypots are decoy systems that aim to entrap attackers into thinking that they managed to gain access to a system but in reality, they are in a separate environment aimed at monitoring their behavior and letting the administrators know how an attacker is carrying out their attack, what vulnerabilities they might go after, and what tools or techniques they are using. This in the end can help the developers improve their system’s security. The problem arises when an attacker figures out that they are interacting with a honeypot - a process known as fingerprinting - and, as a result, they either avoid carrying out their attack or, in some cases, even turn the honeypot against its owner. This thesis aims to help make honeypots undetectable so they can spy on the attackers and let the developers know their system’s weakest links. By analyzing headers, banners, and service behaviors, and comparing them to those of real-world machines, I aim to suggest practical techniques that enhance the stealth and effectiveness of honeypots.