NIKOLAOS GALANIS

LinkedIn/nikos-galanis | GitHub/nikosgalanis • +44 07521205965 • nick.galanis@canonical.com

EDUCATION

UNIVERSITY COLLEGE LONDON | London, UK
MSc Information Security *2022 - 2023*
School of Engineering, Department of Computer Science

- Overall GPA: 76.2 % | First-Class Honours, Distinction
- Dissertation*: Detecting and Defending Against Targeted Data Poisoning Attacks in Federated Learning Models.* Supervisor: Prof. Emiliano de Cristofaro (Grade: 82%)
- Modules Include: Privacy Enhancing Technologies (95%), Malware (70%), Introduction to Cryptography (75%), Research in Information Security (72%), Computer Security I & II (75%), Cryptocurrencies (70%)

NATIONAL & KAPODISTRIAN UNIVERSITY OF ATHENS | Athens, GR
BSc Computer Science *2017 - 2021*
Department of Informatics and Telecommunications

- Overall GPA: 85.8% | First-Class Honours | top 9%
- Major GPA: 92%
- Dissertation: *Protection of Sensitive Data: Creating, Analysing and Testing Protocols of Differential Privacy*. Supervisor: Assoc. Prof. Konstantinos Chatzikokolakis (Grade: 100%, Inclusion in the journal for best dissertations of the Department in 2021).
- Modules Include: Computer Security (100%), Artificial Intelligence II (100%), Data Mining Techniques (100%), Network Management (100%), Software Design for Algorithmic Problems (100%), Algorithmic Operations Research (100%), Object-Oriented Programming (100%), Implementation of Database Systems (90%)

PROFESSIONAL EXPERIENCE

CANONICAL | UBUNTU London, UK
Security Software Engineer I (Established) *March 2024 - present*

- Proactively identifying and patching vulnerabilities in Ubuntu (Debian) and Python packages, ensuring the security and integrity of the software ecosystem.
- Implementing the generation of OpenVEX documents for Canonical's CVEs and Security Notices.
- Utilizing Machine Learning to implement automation for the pipelines of the Security Team.
- Contributing to Malware scanning of the Ubuntu Archive.

Associate Security Software Engineer *September 2023 – March 2024*

- Proactively identifying and patching vulnerabilities in Ubuntu (Debian) and Python packages, ensuring the security and integrity of the software ecosystem.
- Conducting code reviews for Ubuntu Main Inclusion Reviews (MIRs), ensuring security and quality of packages.
- Implementing the generation of an OVAL library for the purposes of communicating Canonical's Security Notices.

RESEARCH EXPERIENCE

UNIVERSITY OF ATHENS, DEPARTMENT OF INFORMATICS Athens, GR
Research Assistant *July 2020 - July 2022*

- Demonstrated applications of Differential Privacy to real-world problems, such as large datasets for queries and Machine Learning algorithms, operating on various programming languages such as Python and Java.
- Co-supervised a BSc Dissertation about Membership Inference Attacks Against ML Models.
- Designed and developed a Local D.P. protocol aiming to deal with extreme accuracy errors caused by limited data, leveraging probability theory, written in Python.

PUBLICATIONS

- Galanis, Nick. "Defending against Data Poisoning Attacks in Federated Learning via User Elimination." arXiv preprint arXiv:2404.12778 (2024).

RESEARCH INTERESTS

Data Privacy, Information Security, Data Mining, Anonymous Communication, Federated Learning

CYBER SECURITY RELATED PROJECTS

DATA POISONING ATTACKS IN FEDERATED LEARNING University College London (UCL)
Machine Learning Security (Python) ***(link)*** *December 2022 – September 2023*

- Exploring the emergence of Data Poisoning Attacks as a significant threat to FL models, outlining their methodology and impact on model functionality.
- Introducing a novel defense approach against Data Poisoning Attacks, including algorithmic solutions aimed at predicting and mitigating malicious contributions to FL models while safeguarding user privacy and model utility.

LOCAL DIFFERENTIAL PRIVACY RESEARCH University of Athens
Data Privacy (Python, Java) ***(link)*** *January 2021 - June 2021*

- Testing the accuracy and the privacy protection offered by multiple DP libraries. Specifically, several queries were run on the IBM's diffprivlib, Google's DP library, and ARX tool, operating on Python and Java.
- Designing a new local D.P. protocol and tested in comparison with pre-existing ones, to eliminate the problem of large accuracy errors when limited users are participating in a survey. Implemented using Python.

FLOW CORRELATION ATTACKS AGAINST MIXING NETWORKS University College London (UCL)
Network Anonymity (Python) ***(link)*** *March 2023 - April 2023*

- Implementation of attacks on Mix networks with the goal of de-anonymizing users' traffic by analyzing traffic patterns and message timing.
- The attack involves monitoring and analyzing the timing of messages in the network to establish correlations between senders and receivers without accessing message contents.
- The attack results in a 100% detection rate, posing a significant threat to Mix networks, and the project discusses defenses outlined in related research.

TECHNICAL SKILLS

- Programming Languages: C, C++, Python, C#, Java, Solidity, Bash, PHP, JavaScript, MATLAB, Prolog, Haskell
- Programming Paradigms: Procedural, Object Oriented, Logic, Functional
- Parallel Programming: Threads (POSIX), MPI, OpenMP, CUDA
- ML Frameworks: PyTorch, Keras
- Version Control: Git, GitHub
- Typesetting: LaTeX, Markdown

TEACHING EXPERIENCE

UNIVERSITY OF ATHENS, DATA STRUCTURES Athens, GR
Teaching Assistant *March 2019 - June 2021*

- Engaged in the conduction of labs, creation of homework exercises in C and slides, resulting in re-designing the course, under Assoc. Prof. Konstantinos Chatzikokolakis.

UNIVERSITY OF ATHENS, INTRODUCTION TO PROGRAMMING COURSE Athens, GR
Teaching Assistant *September 2019 - February 2020*

- Engaged in the conduction of labs in C, under Assoc. Prof. Panagiotis Stamatopoulos.

HONOURS AND AWARDS

REPUBLIQUE FRANCAISE Paris, France
Accepted in France Excellence Europa Scholarship Programme *March 2022*

MUNICIPALITY OF FILOTHEI Filothei, Greece
Award for Excellence in University Entrance exams *July 2017*

HELLENIC NAVY Piraeus, Greece
Students' award of Excellence *January 2016, January 2017*