

GEORGIOS SYROS

Email: syros.g@northeastern.edu ♦ Website: georgios.wiki
LinkedIn: linkedin.com/in/gsiros

Education

Northeastern University, Boston, MA, United States Fall 2023 - Present
Ph.D. in Computer Science, **GPA: 4.0**
Advisors: *Prof. Alina Oprea, Prof. Cristina Nita-Rotaru*

Athens University of Economics and Business, Athens, Greece 2019 - 2023
B.Sc. in Computer Science, **GPA: 9.35/10**

Research Experience

Cybersecurity & Privacy Institute, Northeastern University, Boston 2023 - Present
Graduate Research Assistant
Research in security for systems that employ machine learning and AI.

Maryland Cybersecurity Center, University of Maryland, College Park 2022
Undergraduate Research Assistant
Research Internship in security for machine learning in database management systems.

Mobile Multimedia Lab, Athens University of Economics and Business 2021 - 2023
Undergraduate Research Assistant
Research on distributed ledger technologies and decentralized storage networks.

Publications

SAGA: A Security Architecture for Governing AI Agentic Systems, NDSS, 2026
Georgios Syros, Anshuman Suri, Jacob Ginesin, Cristina Nita-Rotaru, Alina Oprea,
A secure architectural framework to control communication and capabilities of AI agents.

DROP: Poison Dilution via Knowledge Distillation for Federated Learning, preprint, 2025
Georgios Syros*, Anshuman Suri*, Farinaz Koushanfar, Cristina Nita-Rotaru, Alina Oprea,
A defense that mitigates backdoor attacks in FL by distilling clean knowledge from poisoned models.

Backdoor Attacks in Peer-to-Peer Federated Learning, ACM Transactions on Privacy and Security (TOPS), 2024
Georgios Syros*, Gokberk Yar*, Simona Boboila, Cristina Nita-Rotaru, Alina Oprea,
Analyzes and demonstrates novel backdoor attacks in decentralized federated learning settings.

Decentralized NFT-based Evolvable Games, 4th Conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS), 2022
Christos Karapapas, **Georgios Syros**, Iakovos Pittaras, George C. Polyzos,
Proposes a blockchain-based framework designed to support artist sustainability in digital games, enabling the use of NFTs as dynamic, evolvable assets that respond to player actions.

Talks

From Autonomy to Accountability: Securing Agentic AI Systems with SAGA

@ *Khoury Security Day '25*,

May 2025

DROP: Poison Dilution via Knowledge Distillation for Federated Learning

@ *New England Systems Day '25*,

Feb 2025

Teaching Experience

Northeastern University

Assisted students with their projects and graded assignments for the following courses:

- CS3650 Computer Systems
- CS6620 Fundamentals of Cloud Computing

Fall 2025

Summer 2025

Awards and Honors

- Financial Scholarship for Academic Excellence, *Huawei Hellas Enterprise*
- Honor for High Academic Performance, *Athens University of Economics and Business*
- Selected for Greek delegation, *Huawei Seeds for the Future 2021*

Academic Service

Reviewed submissions for the following venues:

- ACM Transactions on Privacy and Security (TOPS) Journal
- ACM Conference on Computer and Communications Security (CCS)

Software

- COOKMATE: developing an enhanced microwave interface with accessibility features [[PDF](#)] [[GitHub](#)]
- STRABO.IO; a real time NLP-backed Greeklish-to-Greek translation keyboard for Android [[GitHub](#)]
- VÇOOM; developing a fast, lightweight video calling web app using WebRTC [[GitHub](#)]
- SIMPLEGRAM; A simple Pub/Sub distributed messenger app [[GitHub¹](#)] [[GitHub²](#)]

Technical Skills

Programming: Python, C, C++, Java, PostgreSQL

Machine Learning: TensorFlow, PyTorch, Adversarial ML, Federated Learning

Security: Network monitoring (Wireshark), Cryptographic protocols

Tools: Docker, Git, LaTeX