europass Curriculum vitae

PERSONAL INFORMATION

Enkeleda Bardhi

RESEARCH EXPERIENCE

August 2023–November 2023

Visiting PhD Scholar in Computer Science

Purdue University, Indiana, USA

During my visit to Purdue University, I have been working with Purdue University's Networking and Systems Lab (PurNET) on the integration of Machine Learning (ML)-based security mechanisms on the programmable network devices. I had the chance to meet and work with extremely motivated PhD students and professors. Our collaboration is still ongoing.

October 2022–February 2023

Visiting PhD Scholar in Computer Science

Delft University of Technology, Delft, The Netherlands

During my visit to TU Delft, I have been working with the Embedded and Networked Systems (ENS) group on security mechanisms on the programmable network devices topic. I had the chance to work with extremely motivated PhD students and professors. Our collaboration is concluded with a scientific paper currently submitted for peer review at an international conference.

November 2020–January 2024

PhD in Computer Engineering

Sapienza University of Rome, Rome, Italy

My research is mainly focused on the network security and privacy area. In particular, I am interested in studying Future Internet Architectures, mostly Information-Centric Networking (ICN) and emerging technologies, including Software Defined Networking (SDN) and Programmable Networks. I am an enthusiast of applying Machine Learning (ML) and Artificial Intelligence (AI) as tools to model my research projects, thus delivering security and privacy issues.

Articles and Projects

Published **Future Generation Computer Systems**

Anonymous Federated Learning via Named-Data Networking [1]. Federated Learning (FL) represents the de facto approach for distributed training of machine learning models. Nevertheless, researchers have identified several security and privacy FL issues. Among these, the lack of anonymity exposes FL to linkability attacks, representing a risk for model alteration and worker impersonation, where adversaries can explicitly select the attack target, knowing its identity. Named-Data Networking (NDN) is a novel networking paradigm that decouples the data from its location, anonymising the users. NDN embodies a suitable solution to ensure workers' privacy in FL, thus fixing the abovementioned issues. However, several issues must be addressed to fit FL logic in NDN semantics, such as missing push-based communication in NDN and anonymous NDN naming convention. To this end, this paper contributes a novel anonymous-by-design FL framework with a customised communication protocol leveraging NDN. The proposed communication scheme encompasses an ad-hoc FL-oriented naming convention and anonymity-driven forwarding and enrollment procedures. The anonymity and privacy requirements considered during the framework definition are fully satisfied through a detailed analysis of the framework's robustness. Moreover, we compare the proposed mechanism and state-of-the-art anonymity solutions, focusing on the communication efficiency perspective. The simulation results show latency and training time improvements up to $\sim$30%, especially when dealing with large models, numerous federations, and complex networks.

Published **The 8th IEEE European Symposium on Security and Privacy, 3-7 July 2023**

GNN4IFA: Interest Flooding Attack Detection with Graph Neural Networks [2]. In the context of Information-Centric Networking, Interest Flooding Attacks (IFAs) represent a new and dangerous sort of distributed denial of service. Since existing proposals targeting IFAs mainly focus on local information, in this paper, we propose GNN4IFA as the first mechanism exploiting complex non-local knowledge for IFA detection by leveraging Graph Neural Networks (GNNs) handling the overall network topology. In order to test GNN4IFA, we collect SPOTIFAI, a novel dataset filling the current lack of available IFA datasets by covering a variety of IFA setups, including $\sim$40 heterogeneous scenarios over three network topologies. We show that GNN4IFA performs well on all tested topologies and setups, reaching over 99% detection rate along with a negligible false positive rate and small computational costs. Overall, GNN4IFA overcomes state-of-the-art detection mechanisms both in terms of raw detection and flexibility and – unlike all previous solutions in the literature – also enables the transfer of its detection on network topologies different from the one used in its design phase.

Published **The 8th IEEE European Symposium on Security and Privacy, 3-7 July 2023**

Security and Privacy of IP-ICN Coexistence: A Comprehensive Survey [3] Today's Internet is experiencing a massive number of users with a continuously increasing need for data, which is the leading cause of introduced limitations among security and privacy issues. To overcome these limitations, a shift from host-centric to data-centric is proposed, and in this context, Information-Centric Networking (ICN) represents a promising solution. Nevertheless, unsettling the current Internet's network layer – i.e., Internet Protocol (IP) – with ICN is a challenging, expensive task since it requires worldwide coordination among Internet Service Providers (ISPs), backbone, and Autonomous Services (AS). Therefore, researchers foresee that the replacement process of the current Internet will transition through the coexistence of IP and ICN. In this perspective, novel architectures combine IP and ICN protocols. However, only a few of the proposed architectures place the security-by-design feature. Therefore, this article provides the first comprehensive Security and Privacy (SP) analysis of the state-of-the-art IP-ICN coexistence architectures by horizontally comparing the SP features among three deployment approaches – i.e., overlay, underlay, and hybrid – and vertically comparing among the ten considered SP features. Lastly, the article sheds light on the open issues and possible future directions for IP-ICN coexistence. Our analysis shows that most architectures fail to provide several SP features, including data and traffic flow confidentiality, availability, and communication anonymity. Thus, this article shows the secure combination of current and future protocol stacks during the coexistence phase that the Internet will definitely walk across.

Published **The 17th International Conference on Availability, Reliability and Security (ARES22), 23-26 August 2022**

Sim2Testbed Transfer: NDN Performance Evaluation [4]. The Internet model has changed from its first design, rolling from host-centric to information-centric. Consequently, researchers foresee the urge for a new network paradigm that will be more suitable for the needs of nowadays users. Named-data Networking (NDN) adheres to the Information-Centric Networking (ICN) paradigms that have been proposed as possible current Internet substitutes. New proposals concerning NDN-related challenges are released regularly. However, most of these proposals are evaluated using network simulations or theoretical analysis due to lacking a full-stack NDN testbed. Although valid, research has shown that simulation environments or proposed overlay testbeds disturb the experiments and introduce performance mismatches. Motivated by the shreds of evidence mentioned above, we propose a setup of an NDN testbed composed of Raspberry Pi devices. After that, we conduct performance analysis for crucial NDN features such as name-based forwarding, in-network caching, and data packet signing. Our experiments confirm the benefits of enabling caches in intermediate nodes. Furthermore, we compare different signing algorithms based on the producer's goodput and processing time. Indeed, SHA-256 is confirmed as the most lightweight with 103 Mpbs goodput and 130 μs processing time. Nevertheless, a security and performance trade-off must be met. On the other hand, as research has demonstrated, such features can be exploited to compromise users' privacy and degrade the network's performance. Additionally, the attack performance might change while implemented in a real deployment. To validate such effects, we transfer two state-of-the-art privacy attacks from a simulation domain to a physical environment, i.e., our testbed. While one of the transferred attacks preserves the preciseness on the testbed, the other demonstrates result mismatches.

Published **IEEE Conference on Local Computer Networks (LCN), 4 October - 7 October 2021**

ICN PATTA: ICN Privacy Attack Through Traffic Analysis [5]. PATTA is the first privacy attack based on network traffic analysis in Information-Centric Networking. PATTA aims to automatically identify the category of requested content by sniffing the communication towards the first hop router. PATTA applies text processing and machine learning techniques to content names in content-oriented architectures. We evaluate PATTA in a simulated network, achieving an accuracy in determining a real-time content category equal to 96%.

Accepted for publication at USENIX OSDI 2024	Caravan: Practical Online Learning of In-Network ML Models with Labeling Agents
Major Revision submitted at IEEE Network Magazine	Is AI a Trick or T(h)reat for Securing Programmable Data Planes?
Submitted at ACM CoNext 2024	Fully Distributed In-Network DDoS Detection with ML
Ongoing	Symbolic Knowledge Extraction for Lightweight AI-based IN-Network Intrusion Detection Systems
Ongoing	NetEye: Extending the Capabilities of a Programmable Switch using Time-Shifted Streams

Talks

November 2023	Poster (Second Runner-Up): "One Model is Not Enough: A Fully Distributed DDoS Detection Mechanism for Programmable Data Planes."; Venue: ACE Center for Evolvable Computing at the University of Illinois Urbana-Champaign [6].
October 2023	Seminar: "In the Intersection of Current and Future Internet Security and Privacy"; Venue: PurNET Group Meeting, Purdue University [7].
October 2023	Seminar: "Some of the Network Security Principles"; Venue: Computer Network Fall 2023, Purdue University [8].
May 2023	Seminar: "The Journey of the Internet: From the Present to the Future"; Course: Advanced Information Systems Security and Blockchain; Venue: Sapienza University of Rome
January 2023	Seminar: "The Future of the Internet: Security and Privacy of Current and Future Networking Paradigm"; Venue: Cybersecurity Group at Delft University of Technology, The Netherlands [9].
March 2022	Seminar: "Security and Privacy Aspects of Future Internet Architectures"; Course: Advanced Information Systems Security and Blockchain; Venue: Sapienza University of Rome
November 2021	Seminar: "The Road Ahead Future Internet: From IP to ICN"; Course: Computer Network Security; Venue: University of Padua [10].
November 2021	Seminar: "Future Internet Architectures"; Course: Sistemi di Calcolo 2; Venue: Sapienza University of Rome [11].
December 2020	Seminar: "Future Internet Architectures"; Course: Sistemi di Calcolo 2; Venue: Sapienza University of Rome [12].

Fundings

2022-2023	"The-old-meets-the-new: Securing the IoT Networks through Artificial Intelligence Solutions and Emerging Technologie"; Progetti per Avvio alla Ricerca, Tipo 1, Sapienza University of Rome; Total: 1000€
2023-2024	"The Trick and T(h)reat of Artificial Intelligence in Programmable Network"; Progetti per Avvio alla Ricerca, Tipo 2, Sapienza University of Rome; Total: 2000€

Teaching Assistant

February 2022-October 2022	Faculty of Law - Digitisation for Human Resources Course

WORK EXPERIENCE

November 2018 – August 2020

Data Entry

Giuseppe Mengotti SNC
Piazza Libertà 38, 36061 Bassano del Grappa (VI)

I took care of the data entry of all the new products in the database application of the company. Furthermore, I was responsible for preparing different statistics on data provided by the database, according to the objectives to be achieved.

May 2017 – September 2017

Helpdesk Support

Digicom Sh.a
Tirana, Albania

Part of the help-desk support team at Digicom, an Internet Service Provider, the first one offering fiber optics technology. This position also gave me the possibility to deal with problem-solving in an efficient way and create some practical background in this field.

June 2016 – December 2016

Operator

Intercom Data Service (IDS), Tirana, Albania

Operator for 180 Vodafone, activation office for ADSL, fiber optics, and telephony.

June 2015 – December 2015

Operator

Intercom Data Service (IDS), Tirana, Albania

Operator for Mediaset Premium, activation office, and client care operator.

EDUCATION AND TRAINING

August 2019–December 2019

Erasmus Exchange in Computer Science

Universitetet i Oslo, Oslo, Norway

An experience that gave me an advanced definition of security since I attended the Ethical Hacking course. Furthermore, the courses on Advanced Big Data Systems and The Future Internet Protocols gave me a better knowledge of the fields of data processing and management, and also telecommunication.

September 2018–Present

M.Sc. in ICT for Internet and Multimedia

Università degli Studi di Padova, Padova, Italy

During this master's program, I have attended a wide catalog of courses, including security, telecommunications, and computer science, with a GPA of 28.3/30. I completed this cycle of studies with a master thesis entitled Traffic Analysis for Named Data Networking, in collaboration with the Spritz Security and Privacy Research Group, University of Padua.

September 2014–October 2017

B.S. in Telecommunication Engineering

Polytechnic University of Tirana, Tirana, Albania

Successfully completed the three years of study and a thesis on image processing using segmentation techniques with Matlab evaluated with 9/10.

PERSONAL SKILLS

Mother tongue: Albanian

Other languages

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	C1	C1	C1	C1	C1
	TOEFL iTP, B2				
Italian	C1	C1	C1	C1	B2
	CELI 3, B2				
German	A1	A1	A1	A1	A1

Levels: A1 and A2: Basic user – B1 and B2: Independent user – C1 and C2: Proficient user
Common European Framework of Reference for Languages

Skills

- Cybersecurity: is one of my main research interests. I am attracted by both the study of defence mechanisms and also doing research in the attacker's point of view.
- Programmable network devices: lately my research focus includes security mechanisms that are embedded into programmable network devices – e.g., Tofino switches – to provide scalable and lightweight intrusion detection mechanisms.
- Networking: the world of networking is one of my main interests including IoT networks, Information-Centric Networking and recently I am focusing on Software Defined Networking (SDN). The challenges that the world of networking is facing, especially for the future of the internet, make me feel really enthusiastic in working in this direction.
- Artificial intelligence: using AI and Machine Learning algorithms for automatizing the detection and mitigation mechanisms in networking has been the my research interest. Lately, my focus has been using xAI techniques to extract lightweight logic rules from the ML models that can be used in constrained environments.

Other skills

- Coding: High intermediate skills of programming languages such as: Python, C, C++, MySQL, Matlab, OpenCV. Also a good knowledge of HTML and Java, used during some courses in my Bachelor studies.
- Other: hard-working, decision making, analytical thinking, problem solving, self-organised and team working.

PUBLICATIONS

[1] Andrea Agiollo, Enkeleda Bardhi, Mauro Conti, Nicolò Dal Fabbro, and Riccardo Lazzeretti. "Anonymous Federated Learning via Named-Data Networking". In: *Future Generation Computer Systems* 152 (2024), pp. 288–303. URL: https://doi.org/10.1016/j.future.2023.11.009.

[2] Andrea Agiollo, Enkeleda Bardhi, Mauro Conti, Riccardo Lazzeretti, Eleonora Losiouk, and Andrea Omicini. "GNN4IFA: Interest Flooding Attack Detection With Graph Neural Networks". In: *8th IEEE European Symposium on Security and Privacy, EuroS&P 2023, Delft, Netherlands, July 3-7, 2023*. IEEE, 2023, pp. 615–630. URL: https://doi.org/10.1109/EuroSP57164.2023.00043.

[3] Enkeleda Bardhi, Mauro Conti, Riccardo Lazzeretti, and Eleonora Losiouk. "Security and Privacy of IP-ICN Coexistence: A Comprehensive Survey". In: *IEEE Commun. Surv. Tutorials* 25.4 (2023), pp. 2427–2455. URL: https://doi.org/10.1109/COMST.2023.3295182.

[4] Enkeleda Bardhi, Mauro Conti, Riccardo Lazzeretti, Eleonora Losiouk, and Ahmed Taffal. "Sim2Testbed Transfer: NDN Performance Evaluation". In: *ARES 2022: The 17th International Conference on Availability, Reliability and Security, Vienna,Austria, August 23 - 26, 2022*. ACM, 2022, 63:1–63:9. URL: https://doi.org/10.1145/3538969.3544447.

[5] Enkeleda Bardhi, Mauro Conti, Riccardo Lazzeretti, and Eleonora Losiouk. "ICN PATTA: ICN Privacy Attack Through Traffic Analysis". In: *46th IEEE Conference on Local Computer Networks, LCN 2021, Edmonton, AB, Canada, October 4-7, 2021*. IEEE, 2021, pp. 443–446. URL: https://doi.org/10.1109/LCN52139.2021.9525013.

[6] Enkeleda Bardhi. *(Second Poster Runner-UP!)One Model is Not Enough: A Fully Distributed DDoS Detection Mechanism for Programmable Data Planes*. http://tinyurl.com/ysv8jzsk. 2023.

[7] Enkeleda Bardhi. *In the Intersection of Current and Future Internet Security and Privacy*. http://tinyurl.com/bdhsedm5. 2023.

[8] Enkeleda Bardhi. *Some of the Network Security Principles*. http://tinyurl.com/3p3uytf5. 2023.

[9] Enkeleda Bardhi. *The Future of the Internet: Security and Privacy of Current and Future Networking Paradigms*. http://tinyurl.com/mrfa4h3x. 2023.

[10] Enkeleda Bardhi. *The Road Ahead Future Internet: from IP to ICN*. https://tinyurl.com/2jjknms3. 2021.

[11] Enkeleda Bardhi. *The Road Ahead Future Internet: from IP to ICN*. https://tinyurl.com/yvfs7sd8. 2021.

[12] Enkeleda Bardhi. *Future Internet Architectures*. https://tinyurl.com/mtp9xrzz. 2020.