Daniel Gibert Llauradó

Technology Centre:	CeADAR
Academic Mentor:	Dr. Quan Le
Company Partner:	IBM Ireland
Company Mentor:	Dr. Giulio Zizzo.

Dr. Gibert has completed his PhD (2020) in Engineering and Information Technologies at the University of Lleida (Spain), MSc (2016) in Artificial Intelligence at the Polytechnic University of Catalonia, and a BSc (2014) in Computer Engineering at the University of Lleida, Spain. His doctoral work titled "Going Deep into the Cat and the Mouse Game: Deep Learning for Malware Classification" explored the application of machine learning and deep learning to tackle the problem of malware detection and classification.

Dr. Quan Le

Quan is a Research Fellow and a senior member of the Applied Research Group within CeADAR at UCD. Quan completed his PhD in protein structure classification, using neural networks and kernel methods. After his PhD, he completed a postdoc in bioinformatics, working on the application of profile Hidden Markov Models in sequence alignments. He has been leading multiple industry-focused machine learning projects, and developed two deep learning libraries. His research interests include the application of machine learning in bioinformatics, healthcare, geospatial data, cybersecurity, and AI Ethics.

Dr. Giulio Zizzo

Giulio is a Research Staff Member at IBM Research. He is part of the Security and Privacy team researching secure and robust machine learning systems. Giulio obtained his PhD from Imperial College London focusing on adversarial machine learning. During his PhD he worked with FeedForward AI, a startup developing AI solutions for the music industry. Prior he worked at BAE Systems and obtained his master's degree from the University of Manchester.

CeADAR

CeADAR is Ireland's national centre for Applied Artificial Intelligence. CeADAR is a market-focused technology centre that drives the accelerated research, development, and deployment of AI and data analytics technology and innovation into businesses. The Centre is the bridge between the worlds of applied research in AI and data analytics and their commercial deployment. CeADAR is funded by Enterprise Ireland and IDA Ireland, is headquartered in University College Dublin and is a partnership with the Technological University Dublin (formerly DIT). The Centre's work focuses on developing tools, techniques and technologies that enable more people, organisations and industries to use analytics and AI for better decision making, unlocking hidden insights and sustained competitive advantage. It provides a vibrant research community with vast experience and expertise in the development and dissemination of scientific research including industry-applied data analytics. The centre is the designated EU AI Digital Innovation Hub in Ireland and is one of 30 across the EU.

IBM Ireland Limited

IBM Research is one of the world's largest industrial research and development organizations employing more than 3,000 scientists and engineers in 12 labs around the world. Since the first lab opened in 1945, IBM Research has hosted six Nobel Prize winners and six Turing award winners. The Dublin research lab hosts one of the Security and Privacy research teams with a wide range of research including robust machine learning, differential privacy, federated learning as well as major contributions to open-source projects including the Adversarial Robustness Toolbox (ART) and Diffprivlib.

University College Dublin (UCD)

UCD is one of Europe's leading research-intensive universities; an environment where undergraduate education, masters and PhD training, research, innovation and community engagement form a dynamic spectrum of activity. The international standing of UCD has grown in recent years; it is currently ranked within the top 1% of higher education institutions worldwide. UCD is also Ireland's most globally engaged university with over 33,000 students drawn from 144 countries, including almost 4,000 students based at locations outside of Ireland. As Ireland's largest university, with its great strength and diversity of disciplines, UCD embraces its role to contribute to the flourishing of Ireland through the study of people, society, business, economy, culture, languages and the creative arts, as well as through research and innovation.

Daniel's project

"Development of a Robust, Scalable, and Explainable AI-based System for Malware Detection"

The fight against malware has turned out to be a never-ending and cyclical arms race: as security analysts and researchers improve their defenses, malware developers continue to innovate, find new infection vectors and enhance their obfuscation techniques. At the dawn of the antivirus industry, signature-based methods and heuristic-based methods were sufficient to identify malware files. These methods require the manual creation of these rules and heuristics, via the careful selection of a representative sequence of bytes or other features indicating the presence of malicious code. However, the use of obfuscation techniques such as polymorphism and metamorphism resulted in a flow of hundreds of thousands of malicious samples being discovered every day. Consequently, previous approaches became ineffective because (1) the manual creation of rules couldn't keep up with the huge flows of malware, and (2) they couldn't detect new malware until analysts manually created a detection rule.

Under these circumstances, machine learning (ML) has become an appealing signature-less approach to detect malware because of its ability to handle large volumes of data and to generalize to never-before-seen malware. The proposed research will develop novel machine learning methods for the task of malware detection and classification. Traditionally, machine learning approaches extract a set of features that provide an abstract view of the executable. Afterwards, the features are used to train a model to solve the task at hand. However, the feature engineering process is time-consuming and requires human resources to determine which features to extract and use for the classification process. Recently, the feature engineering process has started to be replaced by deep learning. Deep learning replaces the feature engineering process by an underlying system which typically consists of a neural network with multiple layers, that performs both feature learning and classification. Nevertheless, deep learning approaches take as input raw data and in consequence, a lot of useful information is overlooked like the API imports and exports table, the usage of the registers, characteristics extracted from the PE header and sections, etc. To deal with this problem, we will design and implement a multimodal framework so that malware characteristics are effectively represented. In addition, special emphasis will be put on designing models that are able to defend and withstand adversarial attacks and obfuscation techniques employed by malware authors to obfuscate the executables and avoid detection. Last but not least, we will develop tools and techniques to address the "black-box problem". That is, the inability of ML models to give an explanation of why they have reached a particular conclusion. Thus, we will focus on developing methods and techniques that enable an understanding of why the AI/ML models developed are giving specific results.