Finanziato dall'Unione europea NextGenerationEU

IMT SCUOLA ALTI STUDI LUCCA

MUR

IMT SCHOOL NATIONAL PHD PROGRAM IN "CYBERSECURITY",

CALL FOR APPLICATIONS 2023/2024
EXECUTIVE SUMMARY

PHD PROGRAM DESCRIPTION

The IMT School for Advanced Studies Lucca has launched the call for applications for the National PhD Program in "Cybersecurity" (2023/2024 academic year):

Course Description	The National Doctoral Program in Cybersecurity (Ph.D.-CySec) aims at forming a new generation of scholars, and future decision makers, who can support and increase the resilience of citizens, public institutions, and businesses to cyber-attacks, by developing and properly implementing digital processes and infrastructures that are more secure and reliable. Upon completion of their studies, Ph.D. candidates will have been trained to tackle the growing complexity of cyberattacks, exploiting holistic approaches spanning technological, economic, human, social, and legal aspects. To reach such a goal, the Ph.D.-CySec program puts forward a strong multi- and inter-disciplinary approach providing a basic exposure to all such wide-ranging spectrum of competences and focusing on four key thematic Specialization Tracks: 1. Foundational Aspects in Cybersecurity 2. Software, System, and Infrastructure Security 3. Data Governance & Protection 4. Human, Economic, and Legal Aspects in Cybersecurity Thus, Ph.D. candidates will learn how to approach cybersecurity issues from different perspectives within an inter- and multi-disciplinary team of experts from other fields. During their educational training, candidates will be given the possibility to face and tackle real-world case studies by actors and stakeholders in the field both from the private and from the public sector. In the sequel, a brief description of the main themes considered in each track is provided. **Foundational Aspects in Cybersecurity** The track will provide scientific background to further advance research in cybersecurity. Candidates will study, among the others, cryptography, Artificial Intelligence, secure programming, distributed computing, formal methods, and languages to push further the most novel contributions to cybersecurity research. Upon graduation, the Ph.D. candidate will be able to collaborate with research teams in academia and in private or public research centers. It is expected that applicants possess a strong mathematical and/or technological background that will be further refined during the course but will also be complemented by notions related to economical, legal, and social aspects.

Course Description	**Software, System, and Infrastructure Security** The track aims to provide the scientific, technological, and methodological knowledge required to face, in an appropriate and proactive way, the main problems posed by the security of systems and infrastructures of various nature and complexity, including software, hardware, and communication systems, characterized by different security and resilience requirements, depending on their specific field of application. Upon graduation, the Ph.D. candidate will be able to collaborate with multidisciplinary teams aimed at addressing, from both a technological and an operational point of view, the various security aspects of systems and infrastructures, including the critical ones. The professional outlets include, in addition to the academic career, managerial roles in the private sector and in public administration, government agencies, as well as the employment in research organizations of various types that require professionals, experts, and leaders characterized by solid scientific, technological, and methodological backgrounds in cybersecurity. **Data Governance & Protection** The huge amount of data that needs to be stored and processed effectively and efficiently today introduces the need to rely on scalable, efficient, and reliable processing platforms. For this reason, data are often handed over to third parties who offer the availability of continuous access, low costs, and elastic storage and processing services. Despite these advantages, the collection, storage, processing, and sharing of data through these services raises serious questions about the confidentiality and integrity of data and processing. Upon graduation, the Ph.D. candidate will master methods and technologies for controlling data access and usage regulation while minimising their impact on the end user and guaranteeing confidentiality, integrity, and availability of data and processing. The professional outlets include, in addition to the academic career, managerial roles in the private sector and in public administration, government agencies, and other research organizations that require professionals, experts, and leaders characterized by solid scientific, technological, and methodological backgrounds in cybersecurity. **Human, Economic, and Legal Aspects in Cybersecurity** Cybersecurity is not just technology: to prevent attacks on companies and institutions, the society needs profiles that not only possess the necessary technical knowledge and expertise on information technologies, but that are also able to understand the general socio-legal framework in which they operate and how to design operational processes in line with fundamental-rights protection standards, regulatory obligations, international policies, and economic implications. This track is primarily aimed at Ph.D. candidates with a non-STEM background, allowing them to develop a solid knowledge of the technical aspects of cybersecurity that will be used to understand and address potential or existing cybersecurity risks, and master the strategies necessary to reduce them and protect private information.

The IMT School adopts equal opportunity principles in its selection procedures and rejects any type of discrimination based on sex, gender identity, nationality, ethnicity, religious belief, sexual orientation, state of health, and any other status or quality that is not strictly relevant to the call outlined in this document.

Program official duration: 3 years.

Programs start on December 1st, 2023.

PhD Program Coordinator: Prof. Rocco De Nicola

Program official language: English.

Scholarships: 30 (distributed among the available research projects – see attachment)

The number of positions may be increased in the event that additional funding is made available after the publication of the Call.

Scholarship gross amount: 16,243.00 Euros/year (see the "Scholarships" paragraph).

Additional benefits:

- All PhD students admitted to the PhD Program are exempt from paying tuition fees, although they are still responsible for paying the yearly Regional Education Tax (currently 140.00 Euros/year);
- PhD students may be offered additional benefit (see projects descriptions).

REQUIREMENTS

Applications are open to candidates who meet the following requirements:

1. **Degree**:
   - "Laurea Magistrale" or "Specialistica" (according to DM no. 509, of November 3, 1999), or a four- or five-year degree (according to the previous rules of the Italian higher education system) obtained in Italy;
   - Foreign degrees that give access to the PhD in the Country where they have been awarded.

For the selection procedure, candidates are required to upload the documents indicated in Table 2 - Attachments to the application.

Applicants who obtain their degree by no later than **October 31st, 2023,** can also apply. These candidates will be admitted to the selection procedure "with reserve" and must provide their degree certificate by the date of enrollment, or they will be excluded from the program.

2. **Knowledge of the English language**: Applicants are required to indicate their level of English.

APPLICATION

The **application form** must be **mandatorily** filled out in **English** through the School's online procedure **by August 21st, 2023, at 1:00 p.m. (CEST)**.

Applicants must upload the **documents** in **PDF**. The **maximum size is 30MB** for each attachment.

The Selection Committee will accept **attachments** in **Italian or English only** (unless otherwise specified in the table below).

Table 1: Information		
Personal information	compulsory	In this section, applicants must enter their personal data (name, address, contact details, etc.).
English Language Level	compulsory	Applicants must indicate their level of English.
Additional information/Interview	compulsory	Applicants have to indicate the modality for the interview (IMT School campus, videoconference, or similar, or by telephone at an Italian embassy/consulate).
Additional information/Disability	optional	Applicants should indicate if they need assistance to participate in the selection procedure.
Additional information/How did you first find out about IMT?	compulsory	Applicants are required to indicate how they found out about the IMT School.
Education	compulsory	Applicants are required to indicate their university degrees. The degrees have to give access to the PhD in the Country where they have been awarded.
Additional qualifications	optional	In this section, applicants may list any other qualifications considered relevant in relation to their application.
Publications	optional	Applicants can list their own published articles, books, or any material that may be considered relevant for the PhD and research activity.

Table 2: Attachments			
1	**Copy of National Identity Card or Passport**	compulsory	Applicants have to upload a copy of a valid identity document: • For Italian and EU citizens: Valid National Identity card or Passport • Non-EU applicants: National Identity card or Passport (the latter is highly recommended). The copy has to be **signed by the candidate, indicating the date and place of the signature**. In particular, the document has to contain the applicant's photograph, personal data, and document number, place and date of issue. If any of the above information is missing, the document will not be accepted.

			If the document is not in English or Italian, a translation into English or Italian should also be uploaded (an official/legal translation is not required). In the event that the copy of the document is unreadable, the Selection Committee may request a new submission.
2	**Curriculum vitae et studiorum/Resume**	compulsory	Applicants must upload their curriculum vitae et studiorum/resume **in Italian or English (the latter is highly recommended)**, indicating their university degrees, work and research experience, and publications (if any).
3	**Education**	compulsory	Candidates are required to upload one of the following documents **in Italian or English**: • for **degrees obtained in Italy** and/or in **France**, **Ireland**, **Belgium**, **Denmark** (Bruxelles Convention of May 25, 1987), and **Germany** (Italian-German Convention, ratified by the Law no. 176 of 1973): a self-declaration stating the possession of a degree, conferral date, issuing University, and final grade; • for **degrees obtained in all other EU and non-EU countries**: an official certificate indicating the possession of a degree, conferral date, issuing University, and final grade.
4	**Academic transcript/Diploma supplement**	compulsory	For each degree, the applicant has to attach one of the documents listed below **in Italian or English (English is highly recommended)**: • **Academic transcript**: an official document detailing the course, classes attended or subjects studied and results, completion date, graduation date; or alternatively, • **Diploma Supplement**: document produced by the University accompanying the diploma, providing a standardized description of the nature, level, context, content, and status of the studies completed by the applicant (https://ec.europa.eu/education/diploma-supplement_en).
5	**Research Project**	compulsory	Candidates are required to express their preference for up to four (4) research projects as referred to in Article 1 of this call for applications. The preference expressed by candidates will not be binding when assigning the projects (see "Final Ranking").
6	**Research Statement**	compulsory	To best evaluate each candidate's aptitude for the PhD Program, all candidates must upload a document (**maximum 10,000 characters, spaces included**) **mandatorily in English**, describing:

			– the candidate's competencies and experiences within the scientific or academic field relevant to the project(s) chosen and how they would use them to address the project(s); – the candidate's motivation for pursuing study at the IMT School, with particular reference to the project(s) chosen; – future projects.

If the application lacks a piece of information or an attachment referred to as "compulsory", applicants can be conditionally admitted to the selection procedure. Their application will be considered valid only if they produce the required documents by the day scheduled for the interview.

The correct completion of the online application procedure is **confirmed by an automatic email** sent to the email address indicated by each applicant while registering for the procedure; the message only confirms the receipt of the application. The School will not verify the validity and completeness of applications before the call closes.

After the submission, no changes are allowed to the entered data.

Candidates are also required to fill out a **separate section of the application form** dedicated to referees:

References	compulsory	Applicants are required to provide the **names and contact information** of **two referees**. The **referees** who are invited to submit a **reference letter in English** through the IMT School's online application system by **August 28th, 2023, at 1:00 p.m. (CEST)**, will receive an automatic notification from the School's application system. Applicants will receive an automatic notification when a letter is submitted, but they may not access any reference provided.

SELECTION COMMITTEE

The Selection Committee is nominated by decree by the Rector of the IMT School in accordance with the School regulations and comprises experts from relevant fields.

EVALUATION CRITERIA AND SELECTION PROCEDURE

Evaluation criteria

The Selection Committees will evaluate candidates'

- academic background, knowledge, skills, and scientific potential;
- general aptitude for research and potential to collaborate in the specific research activities of the project(s) selected in the application form;
- interdisciplinarity, knowledge, and skills with reference to the multidisciplinarity of the PhD Program and to the selected project(s).

Assessment of qualifications

The first phase of the selection procedure is the assessment of qualifications. This assessment is carried out in relation to the specifics of the PhD Programs and specifically to determine who is admitted to the interview.

In the assessment of qualifications phase, the evaluation of the candidates is carried out by the Committees defined in the previous paragraph "Selection Committees" and based on the candidates' application form, uploaded documents, and reference letters provided by referees.

Based on the assessment of qualifications, the Selection Committees will draw up a shortlist of candidates admitted to the interview in alphabetical order.

The shortlist of applicants admitted to the interview will be published on the School's website and Online Notice Board ("*Albo Online*").

This is the only official communication of the preliminary results to all applicants.

Interview

Candidates admitted to the interview must confirm their participation by email to phdapplications@imtlucca.it within two (2) days of the publication of the shortlist, confirming their preference to have the interview conducted in one of the methods indicated in the "Application" paragraph of this call.

During the comprehensive interview, the Selection Committees will assess the candidates' knowledge and skills with reference to the specific characteristics of the PhD Program and selected project(s).

The Selection Committee will assess all interviews by assigning a score (up to 100 points): applicants scoring at least 70 out of 100 will be eligible for the Program and, therefore, listed in the final ranking.

Final ranking

At the end of the interviews, the Selection Committee will draft the final ranking of the eligible candidates for each research project according to the scores obtained in the interview. The preference expressed by candidates in the application form is not binding: the Committee can thus assign candidates to the ranking of projects deemed most corresponding to their profile.

If multiple candidates get the same score, preference will be given to the youngest candidate.

In the event of the withdrawal or exclusion of a candidate, they shall be replaced by the next suitable candidate according to the ranking.

All rankings will be published on the School's website and Online Notice Board ("*Albo Online*").

ENROLLMENT

Once admitted to the PhD Program, candidates wishing to enroll must submit the complete enrollment form to the IMT School **no later than five (5) days from the publication of the results** on the School's Online Notice Board ("*Albo Online*") and website, using one of the following methods:

- in person or by post to:

  IMT School for Advanced Studies Lucca
  PhD and Higher Education Office
  Piazza S. Ponziano, 6
  55100 Lucca – Italy

- by certified email to imtlucca@postecert.it

Failure to submit the enrollment request by the deadline and through the above-mentioned methods will result in an automatic withdrawal of the candidate from the Program.

The enrollment request is valid only if all the requested documents have been enclosed.

If any of the documents submitted during the application procedure do not correspond to those submitted during enrollment due to an intentional false declaration, the applicant will automatically lose their right to enroll in the program.

Enrollment is effective on the first day of official classes. Unauthorized absences may nullify the enrollment procedure.

SCHOLARSHIPS

The scholarship amount is 16,243.00 Euros/year and shall be disbursed in monthly installments.

For any research or training activities at universities or research centers abroad, the scholarship amount is increased by 50% for up to twelve (12) months.

Scholarships are subject to the payment of social security contributions (INPS) managed separately under Article 2, paragraph 26 of Law no. 335 of August 8, 1995, as amended, with two-thirds paid by the Administration and one-third by the scholarship recipient.

Admitted candidates who have already benefited from a PhD scholarship in Italy cannot be assigned another one.

The scholarship has a maximum duration of three (3) years and is subject to annual confirmation: according to articles 15 and 16 of the IMT School PhD Regulations, students must complete all the activities provided for each academic year.

If a student withdraws or is excluded within 45 days from the beginning of the Program, they are not entitled to the scholarship. The scholarship will be awarded to the next eligible candidate according to the final ranking. For this reason, the first scholarship payment will be made only after the successful completion of the first 45 days of the program.

If a student registers after 45 days from the beginning of the Program, he/she is entitled to the scholarship starting from the actual date of enrollment.

TREATMENT OF PERSONAL DATA

The IMT School will use the personal data provided by applicants solely for selection procedures and institutional aims in accordance with the provisions of the current European and Italian legislation (EU Regulation 2016/679 and Italian D. Lgs. 196/03 - *Italian Privacy Code*, as modified by the D. Lgs. 101/2018) and the relevant School Regulations.

Applicants are granted all the rights established by art. 15, sections 2, 3, and 4 of Chapter III, and art. 77 of the EU Regulation 2016/679.

For further information regarding the call and the selection procedure, please contact the PhD and Higher Education Office by email at phdapplications@imtlucca.it or by phone at +39 0583 4326530.

Further information regarding the PhD Programs and the IMT School is available at www.imtlucca.it.

FINAL PROVISIONS

Relevant laws and the IMT School PhD Regulations shall be applied to any issue or item not covered by the present call for applications.

NATIONAL PHD PROGRAM IN "CYBERSECURITY" - RESEARCH PROJECTS

1. Keeping Systems, Data, and Your Identity Secure

Curriculum: Software, System, and Infrastructure Security

University: Università della Calabria

Funds: DM MUR 118/2023

Additional benefits: University canteen

Website: https://angelo.furfaro.dimes.unical.it, https://people.dimes.unical.it/andreapugliese

Contact persons: Angelo Furfaro, Andrea Pugliese

Description

The project aims at studying various problems related to different aspects of cybersecurity,

with the aim of (i) identifying methodological and technological approaches and solutions to the issues that currently present the greatest interest, also through the study of real cases proposed by public and private actors and stakeholders) and (ii) defining and developing more secure and reliable processes and infrastructures. The main topics of the project include (i) methods, techniques and tools for the protection of systems, infrastructure and data and (ii) methods, techniques and tools for digital identity and accountability. The student will study and identify, in the above areas, appropriate solutions for the benefit of individual citizens, public institutions and other complex organizations. The student will also develop knowledge and skills that will allow him/her a wide range of professional possibilities, in the public sector (including the National Cybersecurity Agency), research laboratories, centers of study and expertise, private

sectors, and other complex organizations, including through collaboration with inter- and multi-disciplinary teams in cybersecurity - in general, in those settings that require professionals with solid scientific, methodological, and technological skills in cybersecurity.

2. Cross-Layer Design of Secure Systems

Curriculum: Software, System, and Infrastructure Security

University: Alma Mater Studiorum - Università di Bologna

Funds: DM MUR 118/2023

Additional benefits: -

Website: https://disi.unibo.it/en/research/research-areas/computer-security-biometric-systems-and-legal-issues

Contact person: Marco Prandini

Description

The research project will investigate the interplay between the different layers and methodologies involved in the design of secure systems. Security is an intrinsically interdisciplinary field, and the proposed challenge is to take into account aspects that are traditionally independent such as hardware design (e.g. trusted cores, reference monitors), software architectures (e.g. novel virtualization approaches), networking models (e.g. interplay between network programmability and security), formal methods (e.g. analysis, automatic generation of code from provably secure design descriptions), and the human element (e.g. sensitivity to attack vectors).

3. Machine Learning for Threat Detection

Curriculum: Software, System, and Infrastructure Security

University: Università di Palermo

Funds: DM MUR 118/2023Università di Palermo

Additional benefits: -

Website: https://www.unipa.it/persone/docenti/d/alessandra.depaola

Contact person: Alessandra De Paola

Description

In many cybersecurity contexts, it is crucial to timely recognize ongoing events by analyzing

information provided by different sensing nodes. Intrusion detection and malware recognition, for instance, are two common scenarios in which heterogeneous data/features are evaluated together to extract the peculiarities of different attacks. Most approaches exploit supervised classifiers to identify known attacks; however, these are not effective in the case of new threats, i.e., zero-day attacks, where unforeseen patterns may occur. The research activity aims to address this challenge by proposing new solutions that conjugate anomaly detection algorithms with the most recent artificial intelligence methods in order to identify potential cybersecurity breaches at an early stage. To this aim, the candidate should exploit a combination of various techniques, such as statistical analysis, unsupervised learning, classification algorithms and other artificial intelligence methods, to overcome the limitations of single approaches. The research activity should address several challenges, such as the need to perform detection of anomalies and potential threats in real time, also minimizing resource consumption, especially in those scenarios where resource-limited devices are used.

4. Usable and Secure Authentication Mechanisms

Curriculum: Software, System, and Infrastructure Security

University: Università Ca' Foscari, Venezia

Funds: DM MUR 118/2023

Additional benefits: Access to extensive research funds for participation to conferences and schools.

Website: https://www.unive.it/data/people/5590985

Contact person: Flaminia Luccio

Description

Authentication is preliminary to access control and authorization since it allows for identifying users and programs into a system. Authentication is often based on multi-factor approaches, such as passwords, OTPs and biometrics, and typically tend to reduce usability. It is thus important to explore trade-offs between usability and security in order to make users accept the proposed mechanism and prevent abuses such as the selection of weak passwords, the sharing of OTP devices, etc. The PhD student will analyze existing authentication solutions and classify them based on their security, usability and compliance to existing regulations. Then, the student will investigate innovative solutions that balance usability and security with respect to various threat models and regulatory/administrative domains, also considering real case studies.

5. Formal Analysis of Trusted Execution Environments

Curriculum: Foundational Aspects of Cybersecurity

University: Università Ca' Foscari, Venezia

Funds: DM MUR 118/2023

Additional benefits: Access to extensive research funds for participation to conferences and schools.

Website: https://www.unive.it/data/people/5590470

Contact person: Riccardo Focardi

Description

Hardware and software systems drive the digital transformation. They are a pervasive aspect of our daily lives and we rely upon them for a growing number of critical tasks. The ever-growing complexity of these system raises concerns about their security. This project aims at rigorously studying which are the security guarantees that some of these emerging systems provide to their users. The PhD student will use the techniques and methodologies provided by the field of language-based security to study the design and implementation of trusted execution environments (TEEs) in different contexts. The student will investigate innovative solutions to formally prove the security of a system based on the properties of the underlying TEEs. These solutions might be implemented directly in hardware or as IDE/compiler plugins helping the programmer to develop secure-by-design software.

6. Towards Effective Strategies for Monitoring, Analyzing, and Mitigating Information Disorder

Curriculum: Foundational Aspects in Cybersecurity

University: Istituto di Informatica e Telematica -CNR di Pisa

Funds: Istituto di Informatica e Telematica

Additional benefits: -

Website: https://cyb.iit.cnr.it/

Contact person: Maurizio Tesconi

Description

This project focuses on the development of techniques for monitoring, analysing and mitigating Information Disorder. Information disorder refers to the dissemination of false or misleading information that can cause confusion, harm or even social and political destabilization. The project aims to identify and develop effective methods to detect and address two specific problems: coordinated behavior and the use of manipulated content such as DeepFake. Coordinated Behaviour refers to groups of users performing synergic actions in pursuit of a common intent. One objective will be to identify and characterize this type of behavior on social networks by identifying indices to measure it. The use of manipulated content is another major problem of information disorder. The project will focus on identifying and developing effective methods to detect and mitigate the use of DeepFake content. To achieve these objectives, the project will use a combination of qualitative and quantitative research methods with a multidisciplinary approach, ranging from computer science to social sciences. The expected results of this project are the development of effective techniques and strategies to detect and mitigate the coordinated behavior and use of DeepFake content in online information ecosystems. The results of the project will contribute to the broader effort to combat information disorder and its impact on society and democracy.

7. Study of Secure Off-Chain Protocols for Controlling IoT Devices

Curriculum: Software, Systems and Infrastructure Security

University: Università di Camerino

Funds: FFO Ateneo

Additional benefits: -

Website: https://computerscience.unicam.it/

Contact person: Leonardo Mostarda, Michele Loreti

Description

The main goal of this research project is to advance the off-chain protocol state of the art by building a novel approach that can run-on battery-operated sensor and actuator IoT devices. Off-chain solutions are second layer approaches that can be used in the context of Distributed Ledger Technology (DLT) in order to improve scalability. This research project aims at conceiving secure protocols that allow the implementation of a novel off-chain system that is scalable and energy efficient. In particular, this off-chain system must be conceived to be executed on IoT devices that are battery powered, have low computation capabilities (in terms of memory and CPU power) and have limited communication range. These limitations pose the main challenges in order to devise off-chain secure protocols. The goal is to investigate security provable techniques that can guarantee off-chain system security. This will be done by adapting the existing modelling and formal analysis approaches. More precisely, the project aims at developing tools and methodologies that support the specification and verification of security properties. These tools must allow the formalization of security requirements that can be verified at design time and monitored during the system execution. The tools and methodologies developed in the project will be applied to smart city scenarios.

8. Cryptographic Tools and Protocols for Quantum-Safe Networks

Curriculum: Foundational Aspects in Cybersecurity

University: Università Politecnica delle Marche

Funds: DM MUR 118/2023

Additional benefits: -

Website: https://www.univpm.it

Contact person: Marco Baldi

Description

The availability of the first quantum computers motivates the need to study, design, analyze, implement, integrate, validate, and test new cryptographic tools and primitives capable of withstanding both attacks performed with classical computers and future quantum computer-based attacks. The hosting research group has already been active for many years in designing and implementing post-quantum cryptographic primitives and participating in their standardization process coordinated by NIST. The research project is aimed at investigating, designing, and validating new approaches for finding new solutions to major open problems in

this research area, such as: devising new efficient and secure post-quantum digital signature schemes, integrating post-quantum cryptographic into existing applications (such as Internet security protocols, space communications, etc.), identify new cryptographic protocols to perform advanced functions and for use in decentralized cryptography-based infrastructures, such as those leveraging blockchain and distributed ledger technology.

9. AI-based Botnet Classification and Categorization Through Behavior Analysis

Curriculum: Software, System, and Infrastructure Security

University: IIT-CNR

Funds: Altro

Additional benefits: -

Website: https://ccn.iit.cnr.it/en/

Contact persons: Abraham Gebrehiwot and Filippo Lauria

Description

Botnets represent one of the most serious cybersecurity threats faced by organizations today. While a significant amount of research has been accomplished on botnet analysis and detection, several challenges remain unaddressed, such as the ability to design detectors which can cope with new forms of botnets. The goal of the project is to use artificial intelligence-based techniques to classify and categorize botnets by analyzing the commands executed and the malware used to infect devices. A network infrastructure implementing honeypots will be used to interact with bots and collect useful data. Using artificial intelligence-based behavior analysis of bots attempting to infect new victim devices, the project aims to identify patterns and signatures that can be used to classify and categorize botnets. The ultimate goal of the project is to use this information to prevent future botnet attacks.

10. Cybersecurity of RISC-V-based Cyber-Physical Systems in Embedded Scenarios

Curriculum: Software, System, and Infrastructure Security

University: Politecnico di Torino

Funds: DM MUR 118/2023

Additional benefits: -

Website: -

Contact person: Alessandro Savino

Description

Embedded computing systems (ECS) at the base of several application domains (CPS, IoT, transportation, autonomous driving, etc.) must be designed with security in mind from their design phase in a measurable manner.

Security must be considered at all layers of an ECS design, including:

- Embedded hardware vulnerabilities
- Memory Access Protection (MMU & MPU)
- Secure Debugging (HSM and Host)
- Runtime Manipulation Detection
- Secure Feature Activation (Switch Over)

In particular, the hardware is the root of trust of a full ECS; with jeopardized hardware, the whole system is at stake. Thus, it is imperative to enhance the control and trust of hardware across the supply chain and during its operation, and this is the global objective of this Ph.D. project.

This Ph.D. project aims to investigate new RISC-V-based CPU-centric architectures protected against the significant hardware security threats observed across different computing domains: from low-end embedded to High-Performance Computing (HPC) systems. Such an investigation should also exploit security features from external accelerators, either implemented with standard CMOS or with emerging technologies.

The research aims to create an all-encompassing analysis framework and implementation strategy to ensure security in the hardware supply chain and system operation. This involves integrating dedicated monitoring and countermeasure hardware and software to mitigate the effects of attacks that can compromise information or disrupt services.

Solutions will be considered at all stages of the system design process, including simulation, architectural design, and Register Transfer Level (RTL) design, working mainly on open hardware architectures such as RISC-V.

11. Detection and Characterization of Fake Media Content

Curriculum: Data Governance and protection

University: University of Siena

Funds: ex DM 118 co-funded with research funds available at the Department

Additional benefits:

Website: -

Contact person: Mauro Barni

Description

The diffusion of fake media and the ease with which end-users can create fake media is raising increasing concern, due to the impact that the diffusion of fake media can have on our society. It is essential that public entities develop tools to detect fake media, monitor their diffusion on social media and within our society, and investigate the reason behind the creation and diffusion of fake media.

In the last years, multimedia forensic researchers have developed several tools to distinguish genuine media from fake ones and to identify several forms of media manipulations. Yet, detecting fake media and media manipulations is not enough to combat the use of manipulated media for disinformation campaigns; it is necessary that the malevolent use of the manipulations is identified. At the same time, the integrity of a media asset does not ensure that the use of the asset is a benign one: the inclusion of a pristine image in a wrong context may lead to user disinformation as much as the use of a manipulated image.

The next challenge in media forensics, then, is to characterize media manipulation within the context and discourse wherein the media is used and link the manipulation to the intended goal of the counterfeiter.

The goal of this research is twofold:

1. to build suitable, multimodal, models to study the contextual impact of media manipulations;
2. to develop a pool of automatic techniques working under different modalities (images, videos, text), linking the manipulations of a media asset to the intended meaning of the manipulation.

The expected research is a truly multidisciplinary one, touching both the cognitive and technological aspects of the addressed problem.

12. Cryptographic Algorithms and Protocols for Satellite Telecommunication Applications

Curriculum: Software, System, and Infrastructure Security

Institution: Istituto di Calcolo e Reti ad Alte Prestazioni (Cnr-ICAR)

Funds: CNR-ICAR

Additional benefits: -

Website: www.icar.cnr.it

Contact person: Giovanni Schmid

Description

The emergence of quantum computers has triggered the development of new solutions for future secured communications by major security agencies and standardization bodies. This project aims to identify, investigate, and trade off the best candidate quantum cryptography (QC) and post-quantum cryptography (PQC) algorithms and protocols for secure satellite telecommunication missions. The project will focus on the following three main activities:

1. Identification of satellite telecommunication scenarios requiring protection from quantum computers, with the definition of a complete set of functional and security requirements for each scenario;
2. Selection of QC and PQC algorithms and their implementation in networking protocols compliant with the functional and security requirements previously identified;
3. Development of a testbed to evaluate in a laboratory environment the usability and performance of the above protocols within their use cases.

The above-selected algorithms and protocols will comply with open cryptography and satellite communications standards.

13. Assessing and Improving Security of AI Code Generators

Curriculum: Foundational Aspects of Cybersecurity

University: Federico II University of Naples

Funds: University

Additional benefits: -

Website: http://www.dessert.unina.it/

Contact person: Domenico Cotroneo

Description

Nowadays, AI code generators are a valuable solution to help programmers and developers automate coding tasks and reduce the time and effort needed to create software applications. Since they are founded on deep neural networks, AI-based code generators are inevitably exposed to adversarial inputs, i.e., inputs with subtle perturbations that can mislead the models. This issue has several implications also in security applications. Poisoning of AI code

generators refers to the malicious act of intentionally feeding the generator with malicious code or data with the intent of causing it to generate flawed or vulnerable code. These vulnerabilities can be exploited by attackers to gain unauthorized access to systems, steal sensitive data, or cause other types of damage.

This project will focus on the assessment of the data used to feed the AI code generators to ensure that only high-quality code (i.e., free from biases, errors, or vulnerabilities) can be used as a source of information for the models. To fulfill this goal, the Ph.D. candidate will develop solutions based on ML, or that leverage static and dynamic analysis, to assess the code correctness and vulnerabilities. More specifically, the candidate will adopt these solutions to:

1. assess whether the AI code generators are poisoned, i.e., whether the code generated by the models adheres to best practices and industry standards for security, reliability, maintainability, and other quality metrics; and
2. heal the poisoned models by fine-tuning them on data free from vulnerability, i.e., to let the generator learn from examples of code that have already been tested and verified to meet certain standards.

14. Malware Detection for Edge-based Computing and Edge-AI

Curriculum: Software, System, and Infrastructure Security

University: Università degli Studi dell'Insubria (Varese)

Funds: DM MUR 118/2023

Additional benefits: -

Website: -

Contact person: Elena Ferrari

Description

Edge computing allows faster computation and better support for real-time applications than pure cloud-based architectures. However, the rapid increase in the size of edge computing networks and their heterogeneity raise new security issues and challenges. This project aims to address some of the most relevant ones, that is, those related to malware detection, with a focus on the challenging use case of edge-AI. The Ph.D. student will work on the definition of innovative lightweight decentralized solutions for early-stage malware detection at the edge. Learning approaches, such as deep learning, will be investigated, where edge devices are responsible for the learning process without any central observer or coordinator. The challenge is to achieve good accuracy and competitive efficiency even if participating devices lack a global view of the network to feed their learning process.

One of the reference scenarios of the Ph.D. research activity is the challenging Edge-AI use case. Edge-AI services can run under different architectures (e.g., federated learning, decentralized, federated learning, or hybrid solutions), characterized by various advantages and drawbacks, and different security threats. Part of the Ph.D. activity will be devoted to understanding and analyzing the rapidly evolving threat class represented by malware for edge-AI under the most challenging attack scenarios and learning architectures. Detection techniques will be designed, able to cope with different kinds of poisoning attacks, either performed individually or collaboratively (i.e., Sybil attacks).

15. Assessing Risks and Mitigating Harm in AI Systems: Towards the Development of a Trustworthy and Secure AI

Curriculum: Software, System, and Infrastructure Security

University: University of Bari

Funds: DM MUR 118/2023

Additional benefits: -

Website: https://serlab.di.uniba.it/people/danilo-caivano/

Contact person: Danilo Caivano

Description

The proliferation of intelligent systems in our society has revolutionized various fields. At the same time, the widespread adoption of such systems has led to a corresponding increase in risks associated with cybersecurity.

Intelligent systems must be built with reference to "trust by design" and "security by design" principles to ensure that they are trustworthy and generate results that do not cause harm or unnecessary risk. The advent of Generative AI has further enhanced these risks that must be addressed to ensure that these systems are designed with the appropriate safeguards from cyberattacks.

Cybersecurity and trustworthiness are interlinked as the principles of trustworthiness complement and sometimes overlap the ones of AI cybersecurity.

Trustworthiness features such as robustness, accuracy, traceability, explainability, data quality, and fairness inherently complement cybersecurity.

The objective of this Ph.D. project is to investigate such issues and propose novel solutions for a Trustworthy and Secure AI, identify potential risks and vulnerabilities of AI models and algorithms, and provide actions for remediation. Proposed solutions and approaches should help organizations develop and validate their intelligent systems and ensure they meet the necessary standards for safety, security, robustness, and privacy protection while also promoting transparency, accountability, and ethical behavior. Finally, intelligent systems should be validated to make them compatible with current regulations.

16. Protection of Data in Use via Trusted Execution Environment (Tee) Technology

Curriculum: Software, System, and Infrastructure Security

University: University of Naples "Parthenope"

Funds: Research funds of the FITNESS research group.

Additional benefits: Additional research contract within the context of the active project(s), to be negotiated on an individual basis.

Websites: http://www.fitnesslab.eu/, https://certify-project.eu/, https://encrypt-project.eu/, https://cyberseas.eu/, https://incisive-project.eu/

Contact person: Luigi Romano

Description

Even the most secure algorithm is vulnerable, if the computing environment where it is executed is not adequately protected (ENISA Annual Report on Cybersecurity Research and Innovation Needs and Priorities). Effective protection is needed not only when data is "in transfer" (e.g. exchanged over a network connection) or "at rest" (e.g. stored on a disk) but also when it is "in use" (e.g. loaded in the RAM or in the CPU). While the protection of data in transfer and at rest is relatively easy to achieve, protection of data in use is still - to a large extent - an open issue. The main challenge is that data must be protected even from attacks by privileged users (e.g. system administrators or cloud providers) and software (e.g. the OS or the hypervisor). The availability of effective mechanisms for the protection of data in use is a key enabler of a number of application domains, such as Industrial Control Systems, Smart Grids, eHealth, and more. Also importantly, it is the prerequisite for the real take-up of cloud computing. Some of the big players in the cloud market already offer solutions (e.g. Microsoft ACC) which provide protection of data in use via TEE. The PhD program will focus on techniques for the protection of data in use via TEE, and apply them to challenging use cases in realistic setups, within the context of research projects funded by the European Commission, including CERTIFY, ENCRYPT, CyberSEAS, and INCISIVE.

17. Software and Infrastructure Security: Analysis and Verification of Properties

Curriculum: Software, System, and Infrastructure Security

University: University of Pisa

Funds: DM MUR 118/2023

Additional benefits: -

Websites: https://di.unipi.it/

Contact person: Gian-Luigi Ferrari

Description

The overall aim of the PhD project is concerned with defining methodologies and tools to govern the design, development, and maintenance of secure ICT infrastructures. The project involves the design of innovative solutions to govern both the management process and the development of secure ICT infrastructure, through the use of a variety of techniques ranging from static analysis to dynamic analysis, from probabilistic to symbolic methods, to the adoption of digital twin and distributed ledger with the goal of detecting possible malicious activities, preventing or limiting their impact, according to a self-defence and autonomic paradigm. The PhD project aims to significantly extend the power and scalability of currently available techniques to make them applicable to real-world infrastructure in several application fields.

18. Unsupervised and Continuous Learning for Intrusion Detection Systems

Curriculum: Software, System and Infrastructure Security

University: University of Udine

Funds: University

Additional benefits: -

Website: -

Contact persons: Gian Luca Foresti, Marino Miculan

Description

Nowadays, Intrusion Detection Systems represent a fundamental research subject in the field of cyber security. To overcome the problem of recognizing new types of attacks, increasingly frequent in recent years, it is important to design and develop new unsupervised machine learning models capable of detecting anomalies in computer networks. Among other issues, a problem is that most attacks to computer networks are rare events, with respect to the whole (legit) traffic; moreover, attackers constantly change the pattern of their actions, in order to hide from IDSs. The PhD research activities will be focalized on new unsupervised approaches with continuous learning capabilities for anomaly detection; in particular, the proposed study should consider recent neural network architectures such as SF-SOINN for efficient continuous learning. The proposed systems must be tested on important benchmark datasets (e.g., NSL-KDD, etc.) in order to demonstrate its ability in detecting new attacks, learning them and imtevolving its knowledge to increase system robustness to multiple attacks.

19. Methods and Tools for the Security Assessment of Critical Information Infrastructures

Curriculum: Software, System and Infrastructure Security

University: IMT School for Advanced Studies Lucca

Funds: DM MUR 118/2023

Additional benefits: Students are offered free on-campus housing and free meals at the IMT canteen for three years

Website: https://sysma.imtlucca.it/

Contact persons: Letterio Galletta

Description

Information and communications technologies (ICT) form a vital part of our society, providing essential goods and services. Critical information infrastructures (CIIs) are ICT platforms that enable other critical infrastructures whose disruption may affect the safety of citizens. Security engineering for CIIs is a multidisciplinary field involving various topics, from secure software development and cryptography to embedded systems and network security. Formal modelling and verification techniques have the potential to provide strong security guarantees and support vulnerability detection. However, developing effective formal methods-based tools for CIIs is still open. This project aims to provide new methodologies and tools for the security assessment of CIIs that could support Macro-regional CSIRT in their activities. The research could focus on different aspects, such as network security, protocol security, and application security, and can consider different verification techniques.

20. Tools and Techniques for Scalable and Usable Cyber Ranges

Curriculum: Software, System and Infrastructure Security

University: IMT School for Advanced Studies Lucca

Funds: DM MUR 118/2023

Additional benefits: Students are offered free on-campus housing and free meals at the IMT canteen for three years

Website: https://sysma.imtlucca.it/

Contact persons: Gabriele Costa

Description

Cyber ranges are highly sophisticated infrastructures that serve as battlegrounds for cybersecurity activities including, e.g., training, testing, and incident simulation. Although modern virtualization and simulation technologies provide the building blocks for cyber ranges, scalability, re-usability, and affordability are still open issues. As a matter of fact, the access to cyber ranges is today limited and the benefit for the society at large is only marginal.

The goal of this project is to investigate state-of-the-art technologies and methodologies for making cyber ranges accessible to a wider class of users. The candidate will have access to cyber range technologies currently available and will have to investigate innovative approaches to improve their usability and scalability. These approaches include (but are not limited to): infrastructure design languages, orchestration, vulnerability testing, red team automation, exploitability, gamification techniques, attack strategies generation and execution.

21. Machine Learning Models for the Analysis and Detection of Stealth Threats and Latent Vulnerabilities

Curriculum: Foundational Aspects in Cybersecurity

University: University of Cagliari

Funds: DM MUR 118/2023

Additional benefits: -

Website: www.unica.it, www.pralab.diee.unica.it

Contact person: Giorgio Giacinto

Description

The trend in the development of cyber threats is characterised by the exploitation of latent vulnerabilities and by the stealthiness of the techniques used to attack systems and sensors, designed to evade sensing and detection tools. This research project is aimed at devising effective machine learning models based on the recent advances in other fields such as image and natural language understanding. The goal is to spot even small signals of suspicious activities while keeping the rate of false alarms small. Recent advances in deep learning models, as well as the use of ensemble methods, will be leveraged to build a novel framework. In particular, a huge effort will be spent in investigating different models to represent either source code or binaries that can reveal potential vulnerabilities or malicious actions. To this end, recent advances in machine learning models for language modelling and multimedia processing will be analysed and tailored to the computing environment.

22. Harnessing Societal Infrastructures. Formally

Curriculum: Foundational Aspects of Cybersecurity

University: Gran Sasso Science Institute

Funds: DM MUR 118/2023

Additional benefits: -

Website: https://cs.gssi.it

Contact person: Emilio Tuosto

Description

Modern societies rely on infrastructures that are more and more connected through digital networks. This creates complex cyber-physical ecosystems that are vulnerable to many different types of attacks. A source of weakness is that this integration possibly involves systems that were originally designed to operate in (closed) trustworthy settings. In fact, some systems may not provide strong security guarantees (or satisfy only basic security requirements) because they are conceived to operate in non-hostile environments. Therefore, their integration with other systems, nowadays hardly negotiable, could easily introduce security breaches if done naively. This could possibly compromise sub-systems, including those designed to guarantee strong security requirements. This project aims to develop formal approaches to harness existing systems with security guarantees. The main idea is to analyse existing systems and identify weaknesses that could expose them to attacks. The project considers a case study involving a platform developed at Actyx (https://developer.actyx.com/) to support the coordination of factory production. The platform has been designed and implemented assuming a non-adversarial context. A crucial part of the project is to develop approaches to enforce security in systems that rely on the Actyx platform, whose formal modelling and analysis have been initiated in a recent publication.

23. Methodologies and Techniques for Countering and Mitigating the Impact of GenAI and LLM on Information Disorder

Curriculum: Software, System, and Infrastructure Security

University: Università degli Studi di Salerno

Funds: DM MUR 118/2023 - M4C1-PNRR

Additional benefits: -

Website: https://www.unisa.it/

Contact person: Vincenzo Loia

Description

Generative Artificial Intelligence (GenAI) is a branch of Artificial Intelligence aimed at creating complex data, such as images, videos, audio, text, etc., from scratch, mimicking human creativity. The capabilities of emulating human language and interaction skills of Open AI ChatGPT and Bing Sydney are particularly impressive examples. The Large Language Models (LLMs) are revolutionizing the writing approach of journalists, writers, and researchers. However, LLMs are affected by two different issues: (1) biased data adopted for the training task can lead to demographic stereotypes and imprecise information; (2) the generated results can arbitrarily be true or not. As a consequence, the risk of spreading imprecise or false information is high with unchecked generated text. Moreover, presented weaknesses can be easily adopted in disinformation campaigns or political propaganda by, for example, fake persona creation, AI-generated imagery, deep fake for discrediting adversaries, etc.

This project aims to find methodologies able to identify and monitor disinformation phenomena nourished by LLMs. The objective is to let users use and exploit advantages associated with the employment of such innovative technologies, and work for their optimization in order to study solutions that could mitigate the negative effects of LLMs. Moreover, solutions to unmask voluntary or involuntarily generated disinformation content without censorship will be approached.

24. XAI Methodologies and Techniques for Countering Information Disorder

Curriculum: Software, System, and Infrastructure Security

University: Università degli Studi di Salerno

Funds: DM MUR 118/2023 - M4C1-PNRR

Additional benefits: -

Website: https://www.unisa.it/

Contact person: Giuseppe Fenza

Description

Explainable AI (xAI) refers to strategies and procedures employing Artificial Intelligence technology (AI) that allow human experts to gain insight into the AI model outcomes. xAI is a powerful approach for spotting model defects and data biases, contributing to an increase in user trust. The interpretability achieved through xAI models can be exploited for generalization independently from training data issues, such as limited availability of labeled data and lack of domain-specific or multi-language information. In addition, the application of xAI can be a double-edged sword. It substantially improves cybersecurity practices but leaves, at the same time, the system vulnerable to adversary attacks. In this regard, xAI can be adopted to study the vulnerabilities of a system and, consequently, guide its strength or protection. Insights from cybersecurity can be studied to approach threats of the infodemic era, where disinformation attempts can undermine the role of institutions, national security, and democracy itself.

This project aims at studying xAI methodologies that support the definition of more powerful, robust, and generalizable models (in terms of propaganda, fake news, hate speech detection, etc.). The objective is to identify information disorder counterfeiting solutions where models

must be capable of dealing with ever-new challenges due to continuous technological evolution.

25. Automating Risk Assessment of Infrastructure with AI/ML Components

Curriculum: Software, System, and Infrastructure Security

University: Universita' degli studi di Trento

Funds: DM 118/2023 - M4C1- Inv. 3.4

Additional benefits: The students will be trained in the industrial methodologies used by the industry partners and spend 6 months at Vrije Universiteit Amsterdam

Website: https://securitylab.disi.unitn.it

Contact persons: Fabio Massacci, Marco Rocchetto

Description

Several methodologies exist for cybersecurity risk assessment of IT/OT infrastructures (such as ISO 27001, ISO 27002, ISO 27005, NIST SP 800-53, CIS Control v8). However, they are hardly automated and even less account for the presence of artificial intelligence or machine learning components. To date, risk analysis is done by exploiting the experience of technical personnel and is based on beliefs and opinions rather than scientific theories. The result is that risk analysis, which should be a central activity of IT/OT infrastructures management, is found on the margins of corporate GRC (Governance, Risk, Compliance), being almost always evaluated as not very informative. The purpose of the research is the definition of an automatic or semi-automatic process for risk assessment (which includes the identification of threats with a relative estimate of impact and probability). The project will be in cooperation with an innovative start-up company (https://www.v-research.it/) that will support the student in the concrete case studies and the activities for the technological transfer of the results of the project.

26. Countering fake contents and malicious activities

Curriculum: Software, System and Infrastructure Security

University: Università degli Studi di Catania

Funds: DM MUR 118/2023

Additional benefits:

Website: https://web.dmi.unict.it/it/content/dottorato-informatica

Contact persons: Giampaolo Bella, Sebastiano Battiato

Description

Common media such as digital images, audio and video clips could be fake, namely generated by computer programs to resemble genuine ones, with the aim of offering altered contents to unaware users. At an extreme, such contents and the services delivering them could become fully malicious, so as to actively engage with other computer programs as well as with the users to craft cunning attack vectors. Even whole devices could be malicious, including modern Voice Personal Assistants and, more in general, widespread IoT devices – and the role itself of the user could be exploited, for example by mounting a self-issue attack on a voice channel.

The overarching goal of this research is to liberate the IoT from fake contents as well as from malicious activity. The technical objectives are: to promote a precise understanding of the scope and aims of fake contents and malicious activity in the IoT; to devise scalable approaches to thwart fake contents and malicious activity at all architectural layers of the IoT; to define algorithms to detect fake media and deep fakes in the context of the IoT; to implement such algorithms as viable and practical tools that are applicable to real-world scenarios; to tailor the novel algorithms and tools to the particular problem of user privacy preservation so as to make them fully compliant with the General Data Protection Regulation.

27. Explainable and robust AI solutions for malware detection and analysis

Curriculum: Software, system and infrastructure security

University: CNR

Funds: CNR

Additional benefits: -

Contact person: Fabio Martinelli

Description

Design and implementation of techniques for detecting intrusions on mobile devices and IoT, through the use of federated machine learning techniques. Particular importance will be given to the explainability of the proposed models, in order to integrate the techniques developed in a real context, where they can be of support to the malware analyst. Solutions will also be designed for assessing the risk of being attacked by malware, also providing ad-hoc best practices to protect mobile/IoT devices from cyberattacks.

28. Security policy management for digital sovereignty

Curriculum: Data governance and protection

University: CNR

Funds: CNR

Additional benefits: -

Contact person: Fabio Martinelli

Description

The project focuses on the management of policies for digital sovereignty starting from regulations and laws till producing machine understandable, enforceable and verifiable policies. This entails the adoption of methodologies for automated policy generation from natural language, also including large language models. Such security policies will be used for data usage control and data sovereignty solutions that are main instruments of digital sovereignty. The policy management framework could be also adopted in several contexts from compliance to standards to fine grained and continuous control of data and systems in accordance to regulations, usage control policies and privacy preferences. Policy models may include

obligation management frameworks.

29. Preventing, investigating and fighting cybercrimes: substantial and procedural issues

Curriculum: Human, Economic, and Legal Aspects in Cybersecurity

University: Sant'Anna School of Advanced Studies - Pisa

Funds: DIRPOLIS INSTITUTE and prof. Gaetana Morgante

Additional benefits: Additional research contract within the context of the active project(s), to be negotiated on an individual basis.

Websites: https://www.santannapisa.it/en/istituto/dirpolis-institute

Contact person: Gaetana Morgante

Description

Investigating, preventing and fighting cybercrimes is challenging the traditional categories of criminal law and procedure. The building of an efficient legal framework at a domestic, European and international level needs a strong multidisciplinary approach to the juridical, ethical, economical, political, social and human profiles of cybersecurity. The PhD program will concern the different forms of cybervictimization (individual and collective, public and private up to the CyberWar) and take into account the studies on Digital Criminology. The different models of prevention and repression of cybercrimes will also be studied in the light of the international obligations and cooperation (so-called Cyber-Diplomacy). The PhD program will also cover the procedural issues of Cybersecurity from the analysis of the multileveled legal framework up to the collection of the best investigative practices to balance cybersecurity and protection of the fundamental rights in cyberspace (so-called Digital forensics), and the questions related to the jurisdiction on crimes committed in the cyber- and transnational dimension.

30. Advanced solutions for data security and privacy in emerging scenarios

Curriculum: Data Governance and Protection

University: Università degli Studi di Milano

Funds: DM MUR 118/2023

Additional benefits: -

Websites: https://samarati.di.unimi.it/

Contact person: Pierangela Samarati

Description

Data are the central resource for any modern society. Also, the availability of highly performing systems and services (e.g., cloud/fog/edge/IoT) for gathering, storing, and processing data, as well as of efficient machine learning and AI-based solutions operating on large data collections, brings great benefits on a personal, business, economic and social level. On the other hand, data may be sensitive or company-confidential and cannot be shared openly, and their confidentiality, as well as their integrity, should be guaranteed even when non fully trusted parties are involved in data storage or processing. The goal of the project is to contribute to the development of advanced scientific and technological solutions enabling the different actors (e.g., individuals, companies, institutions) with control over their data in the various data release, sharing, and analysis scenarios. The research is in the area of computer science and can entail investigation of different scientific and technological issues contributing to solving the problem of protecting data in emerging scenarios. Technological aspects that can be investigated include: data modeling for enforcing security and privacy restrictions; access control languages and models; data protection in release, storage, or computation by untrusted parties; data integrity; data security and privacy in artificial intelligence scenarios; and AI-based security and privacy solutions.

31. Methodologies and Methods for Quantitative Risk Assessment with reference to European and Domestic Regulations and Frameworks

Curriculum: Software, system and infrastructure security

University: CINI Cybersecurity National Lab

Funds: DM 117/2023

Additional benefits: -

Websites: https://cybersecnatlab.it/

Contact person: Paolo Prinetto

Description

A few years after the first European cybersecurity directive came into operation, a new directive (NIS 2) was published in January 2023, effectively replacing the first one. NIS 2 was the result of a major improvement process of the previous directive, with the goal of strengthening the security measures required and necessary for the protection of critical infrastructure. In fact, new application areas were added, in addition to those previously identified as critical, and the risk management measures to be taken by operators and providers of essential services were better detailed.

In the Italian context the "*Framework Nazionale per la Cybersecurity e la Data Protection*", which outlines guidelines for the proper and effective cybersecurity management of systems. Accompanying this document is also the identification of a set of "*essential controls*", that is, minimum security measures that are easily implemented that refer to the guidelines expressed within the Italian Cybersecurity Framework.

In both contexts, it becomes crucial to be able to provide tools that can enable a rigorous, objective, and quantitative approach to the assessment process that can be applicable not only by large organizations but also by small and medium-sized enterprises.

32. Implementation of acoustic jammers for privacy protection - technical, ethical, and legal issues

Curriculum: Software, system and infrastructure security

University: CINI Cybersecurity National Lab

Funds: DM 117/2023

Additional benefits: -

Websites: https://cybersecnatlab.it/

Contact person: Paolo Prinetto

Description

Microphones are commonly installed in many devices, not just phones but also IoT and wearable devices. Most microphones are today based on MEMS sensors.

Several cases have been reported in which microphones are used to violate privacy in order to fraudulently record private conversations.

Many papers have been published about attack techniques that resort to ultrasonic waves to prevent these attacks by creating a DoS on a microphone (i.e., the microphone cannot record any sound at all or the sound is extremely distorted and not intelligible).

In addition, other attack techniques exploit ultrasonic waves to activate voice commands on smart devices (e.g., SIRI, Google, Alexa): these commands cannot be heard by humans but can still be picked up by common microphones.

During the proposed thesis, we want to deeply analyze DoS attacks against microphones, from both red-teaming and blue-teaming perspectives, in different thread scenarios. In addition, we need to deeply investigate how different sound frequencies might affect electronic devices (i.e., disturbing them and creating unwanted DoS) and people (i.e., possible Impacts on health and safety).

33. Evaluation of Resilient and Secure Cyber-Physical and Distributed Systems

Curriculum: Software, System, and Infrastructure Security

University: Università degli Studi di Firenze

Funds: DM MUR 118/2023

Additional benefits: -

Website: http://rcl.dimai.unifi.it/, https://www.unifi.it/p-doc2-0-0-A-3f2b342f372e2b.html

Contact person: Andrea Ceccarelli

Description

As systems are becoming massively distributed, interconnected, and evolutionary, the complexity of threats and attack paths is increasing. Models for the security and dependability assessment must take into consideration the multiplicity of components, which often share similarities, but at the same time exhibit variations due to different configurations or roles. Further, due to dynamicity and evolution, changes to configurations are introduced over time, and system models need to be updated to reflect such changes.

The proposed research focuses on selected aspects of the design and especially the evaluation of resilient and secure cyber-physical systems, with a particular preference for the security of critical infrastructures and systems of systems. The research shall investigate qualitative and/or quantitative methods for the identification, analysis, classification, and mitigation of threats and hazards, for example aiming to analyze and rank the most probable attack paths, identify the most critical components to be protected, or compare different architectural solutions with different defensive mechanisms.

34. Cybersecurity of Complex Systems

Curriculum: Software, System, and Infrastructure Security

University: University of Genova

Funds: Serics - D.D. n. 341 del 15 marzo 2022

Additional benefits: -

Website: https://www.csec.it/

Contact person: Alessandro Armando, Luca Verderame

Description

This research project focuses on the study of automated or semi-automated methodologies to assess the cyber risk exposure of complex application ecosystems. The candidate will explore emerging scenarios such as Mobile, Cloud, Fog, IoT (Internet of Things), and combinations thereof. Furthermore, all the solutions developed in the project will be evaluated in real-world industrial scenarios.

In detail, the project will be included in one of the following lines of research:

- the design of effective methods for analyzing and quantifying potential cyber risks exposure of complex application environments and the associated supply chain, with specific attention to CI/CD scenarios and the DevSecOps paradigms;

- the identification of proper digital twin technologies to create multi-domain scenarios for testing cyber risk resilience, identifying vulnerabilities, evaluating countermeasures against potential cyber-attacks, and assessing the effectiveness of existing procedures.

35. Towards a Regulatory Sandbox on Cybersecurity

Curriculum: Human, Economic, and Legal Aspects in Cybersecurity

University: University of Florence

Funds: DM 118/2023

Additional benefits: -

Website: -

Contact person: Andrea Simoncini

Description

The project aims to develop a new 'regulatory sandbox' for cybersecurity using a forward-looking approach to regulation, allowing minimal barriers by creating a controlled regulatory testing environment. The 'regulatory sandbox' is a way to connect innovators and regulators, providing a controlled environment for them to cooperate. It facilitates the development, testing and validation of innovative digital tools to ensure compliance with the requirements of existing regulations. The PhD candidate will focus her/his project on studying regulatory sandboxes as a way to co-regulate technological tools and participate in implementing a real regulatory sandbox on cybersecurity in Italy. For these purposes, the candidate will be asked to develop strong state of the art on regulatory sandboxes in Europe and be able to analyse and study relevant European use cases that serve as best practices in operational terms. Activities should also include analysis of legal issues, regulatory compliance and rules on technology. The research activities will be conducted within the Department of Legal Studies of the University of Florence.

36. New generation malware detection through artificial intelligence

Curriculum: Software, System, and Infrastructure Security

University: University of Sannio

Funds: DM 118/2023

Additional benefits: -

Website: -

Contact person: Aaron Visaggio

Description

The research aims to develop novel techniques for the detection of new-generation malware that leverage artificial intelligence techniques.

37. Securing digital identities, authentication and communication in a distributed context

University: Università degli Studi Mediterranea di Reggio Calabria

Funds: DM MUR 118/2023

Website: https://www.diies.unirc.it/scheda_persona.php?id=576

Contact persons: Francesco Buccafurri

Description:

The project focuses on the context of cybersecurity and aims to secure services provided to citizens and organizations. In this scenario, securing communication and protecting digital identity deserve in-depth study. This requires (1) designing distributed solutions not to rely on trusted third parties, (2) guaranteeing that the service applicant is really who claims to be, (3) allowing an entity to communicate anonymously when admitted, (4) allowing disclosing the minimum personal data when required, and (5) providing accountability even if a service is accessed anonymously. The first requirement implicates the adoption of Distributed Ledger Technologies, requirements 2 and 3 involve network security, whereas the last two aspects address the data protection requirements imposed by the GDPR. The student will develop knowledge and skills useful for a wide range of professional possibilities. Furthermore, the student will acquire professionals with solid scientific, methodological, and technological skills in cybersecurity.