Finanziato dall'Unione europea NextGenerationEU

IMT SCUOLA ALTI STUDI LUCCA

MUR

NATIONAL PHD PROGRAM IN IN "CYBERSECURITY" - RESEARCH PROJECTS

Index

1. Cybersecurity at the Factory Plant

Curriculum: Software, System, and Infrastructure Security

University: Università degli Studi di Udine

Funds: DM 352-PNRR: Cleverynext s.r.l.

Additional benefits:

Website:

Contact person: Marino Miculan

Description

The objective of this Ph.D. project is to study and develop advanced techniques for protecting network-connected machines in an industrial plant from cyberattacks. The area is Operational Technology (OT), encompassing both SCADA, DCS, and PLC systems. The problem of identifying and locating cyber vulnerabilities and recognizing anomalies is critical in the operational environment of industrial plants, especially when processes are critical to physical, environmental, and economic security. For this reason, any improvement to the accuracy and precision of the models and algorithms for this purpose represents a step toward full or partial automation of several processes of high economic and social interest.

The Ph.D. candidate will develop specific knowledge of the various methods of analysis and modeling of problems related to cybersecurity of computer networks in industrial plants. The Ph.D. student will be able to design, develop, and test compliance assessment and penetration testing systems for OT networks, adapting them to certain real-world contexts in industrial settings and specific operational requirements. A prototype of a security device equipped with an anomaly detection algorithm for monitoring and protection devices connected to the industrial plant network will be developed.

2. CyberSEAS (Cyber Securing Energy dAta Services)

Curriculum: Software, System, and Infrastructure Security

University: Università degli Studi di Napoli "Parthenope"

Funds: DM-351-PNRR: Ateneo

Additional benefits: Possibility to supplement the scholarship with a research contract

Website:

Contact person: Luigi Romano

Description

CyberSEAS ambition is to improve the resilience of energy supply chains, protecting them from disruptions that exploit the enhanced interactions and extended involvement models of stakeholders and consumers in complex attack scenarios characterized by the presence of legacy systems and the increasing connectivity of data feeds. It has three strategic objectives: 1) countering the cyber risks related to highest impact attacks against electric power and energy systems (EPES); 2) protecting consumers against personal data breaches and attacks; and 3) increasing the security of the Energy Common Data Space. All three objectives are equally important since cyber-criminals are shifting tactics to favor multi-stage attacks for which stealing sensitive data is a precondition for the real attack and enables them to maximize damage and profits (while traditionally, infrastructure cyber-attacks used to be direct attacks on the machinery and typically targeted control systems, not data). To achieve these objectives, CyberSEAS will deliver an open and extendable ecosystem of customizable security solutions providing effective support for key activities, in particular: risk assessment; interaction with end devices; secure development and deployment; real-time security monitoring; skills improvement and awareness; certification, governance, and cooperation. CyberSEAS solutions will be validated through experimental campaigns consisting in the context of realistic use cases.

3. Study and development of algorithms and advanced identification and authentication techniques based on biometric procedures

Curriculum: Software, System, and Infrastructure Security

University: Università di Udine

Funds: DM 352-PNRR: ACRM NET

Additional benefits:

Website:

Contact person: Gian Luca Foresti

Description

During the first year, the doctoral student will delve into the state of the art in computer system security, focusing on identification and authentication techniques based on biometric procedures. He/she will acquire specific databases for training and testing the systems developed during the doctoral activities. During the second year, he/she will classify weaknesses in authentication systems concerning the techniques he/she intends to develop. Different methods of user identification and authentication through insecure communication channels will be designed and implemented, some evaluation tests will be carried out (also choosing an appropriate calculation and ranking method) to select the best methods according to different application contexts. During the third year, based on the obtained results, the student will refine the alignment functions while identifying evolution criteria useful for adapting the proposed technique. The most promising algorithms in different application contexts will be improved, and final evaluation tests will be conducted. The Ph.D. student will prepare several scientific papers for submission to national and international scientific conferences and international scientific journals.

4. Methodologies and techniques for analysis, design, monitoring, and prevention of security and safety of critical rail infrastructure

Curriculum: Software, System, and Infrastructure Security

University: Università degli studi di Napoli Federico II

Funds: Hitachi Rail

Additional benefits: Possibility of supplementing the scholarship with company funds

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

Contact person: Nicola Mazzocca

Description

Critical infrastructures, particularly transportation and mobility infrastructures, are strategic assets that fall within the national security perimeter and provide primary services for citizens and the industrial system. Their security is required to ensure an adequate level of services to citizens. Their security is also to protect them from possible catastrophic damage, such as earthquakes, landslides, and floods, therefore, addressing both "physical" integrity caused by natural events and "cyber" integrity caused by cyber attacks. The objective of the Ph.D. fellowship is to study and research innovative theoretical and practical methodologies to analyze the threats of increasingly connected critical infrastructures and the associated risks to mitigate them with specific mechanisms and policies. Specifically, the study activities will include specific threat analysis, threat analysis, and threat intelligence systems, security and reliability frameworks for selecting and configuring security controls, security assessment and static and dynamic security testing of security properties of systems, as well as proactive protection mechanisms to increase resilience and respond to novel attacks.

5. Methodologies and techniques for preventing, detecting, and mitigating cyberattacks with privacy-preserving tools from eXplainable Artificial Intelligence

Curriculum: Software, System, and Infrastructure Security

University: Università degli Studi di Napoli Federico II

Funds: DM-351-PNRR: Ateneo

Additional benefits: Possibility of supplementing the scholarship with project funds

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

Contact person: Antonio Pescapé

Description

Distributed digital systems, of which the Internet is both an emblematic example and the main communication infrastructure, have become increasingly important for economic and social development on a global scale. With these technologies, however, the range of vulnerabilities and the number and heterogeneity of systems and critical infrastructures subject to attacks have significantly expanded. The objective of the fellowship is foundational and applied research on tools and techniques for prevention, detection and mitigation of cyber attacks with a focus on trustworthiness and privacy. Topics will include methodologies and techniques for Intrusion Prevention/Detection System (IPS/IDS), Anomaly Detection System (ADS), Censorship Detection, Censorship Circumvention, Privacy-preserving Network Monitoring, Surveillance.

For these purposes, artificial intelligence (AI) has proven to be an indispensable tool to capitalize on data collected from the Internet, local area networks, data centers, and applications. However, the adoption of advanced Deep Learning-based solutions is hindered by their inherent black-box nature, which is a limitation to their improvement and an ethical and legal barrier to real-world applications. Therefore, the search for explainable AI techniques (eXplainable AI) will be a necessary tool to make AI models (and the systems that use them) interpretable, manageable, and reliable (trustworthy).

6. Conspiracy Theories on Social Media

Curriculum: Human, Economic, and Legal Aspects in Cybersecurity

University: Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy

Funds: Istituto di Informatica e Telematica

Additional benefits:

Website:

Contact person: Maurizio Tesconi

Description

Conspiracy theories are often denoted as beliefs in the existence of a network of powerful people with malevolent intents who control complex socio-political events, especially when they lack a clear explanation by the authorities or by the scientific community. It is a global phenomenon affecting almost every field of human activity. The conspiracy mindset has notoriously led to episodes of prejudice, witch hunts, obstacles to public health improvements, discrediting science, negative economic impacts, strengthening of radicalized and extremist groups, not to mention wars and genocides. A new generation of radicalization processes seems to take place on social media, where conspiracy theories are shared through many communities that reinforce confirmation bias, segregation, and polarisation. This project proposes a research action on conspiracy spreaders both within and across social media, which will lead to analyzing the conspiracy phenomenon by exploiting a synergy of multidisciplinary expertise in the area of data science and social science. The main objectives will be to define the phenomenon contours identifying the number and typology of the conspiracy theories taking place at a certain time, and to characterize both the users that act as spreaders and those who fall for a conspiracy theory reinforcing its dissemination. This characterization will be carried out through socio-demographic profiling, analysis of social media activity, writing style, psycho-linguistic traits, political orientation, and so on.

7. Automatic software vulnerability detection

Curriculum: Software, System, and Infrastructure Security

University: IMT School for Advanced Studies Lucca

Funds: DM 351-PNRR: Pubblica Amministrazione

Additional benefits: Full board accommodation

Website: https://sysma.imtlucca.it

Contact person: Gabriele Costa

Description

Formal modeling and verification techniques have the potential to provide the strongest security guarantees and to support full automation. However, implementing effective vulnerability detection tools based on these techniques is still an open issue. The main reasons are the poor scalability and the lack of formal semantics of real programming languages. The goal of this project is to investigate novel methodologies that (i) provide formal security guarantees and (ii) can be applied to real world software and services. Many types of analysis may be considered. Among them are, for instance, symbolic exploration, model checking and security testing. Application domains of interest include (but are not limited to) software behavioral anaysis, malware detection and classification, binary and web applications vulnerability disclosure, security assessment of smart contracts.

8. Machine learning for network security and malware detection

Curriculum: Software, System, and Infrastructure Security

University: Università Politecnica delle Marche

Funds: DM 351-PNRR: Pubblica Amministrazione

Additional benefits:

Website: https://www.univpm.it

Contact person: Luca Spalazzi

Description

The research project will aim at developing, testing and validating machine learning techniques for network security, with focus on detection of network traffic generated by malicious entities. This will leverage previous research activities of the proposing research unit concerning the use of machine learning and natural language processing techniques for physical layer authentication over wireless networks and identification of algorithmically generated domain names within DNS queries and responses. Based on such a background, the candidate will address new scenarios possibly involving further types of data (e.g., audit records coming from security information and event management systems - SIEMs) and the identification of more complex threats. The use of collected and extracted information will also be addressed by the candidate, possibly involving its application to a regional Computer Security Incident Response Team (CSIRT). For these purposes, the candidate will be asked to develop and use state-of-the-art software tools for machine learning and cybersecurity, to be applied to the aforementioned contexts.

9. Security mechanisms at system level

Curriculum: Software, System, and Infrastructure Security

University: Scuola Superiore Sant'Anna

Funds: DM-351-PNRR: Ateneo; Co-financed by the ReTiS Laboratory

Additional benefits: Board; Possibility of supplementing the scholarship with project funds; canteen (lunch)

Website:

Contact person: Alessandro Biondi

Description

Research activities will aim to study techniques for detecting cyber attacks and designing defense mechanisms at the system level (e.g., at the operating system level, hypervisor, or in the context of tools such as compilers or neural inference engines). The mechanisms to be designed will be geared toward embedded systems and, therefore, should be resource-efficient and predictable in terms of execution time.

The research activities will be carried out within the ReTiS laboratory (https://retis.santannapisa.it/) of the Scuola Superiore Sant'Anna, where it will be possible to develop prototypes of the designed mechanisms and test them on state-of-the-art embedded platforms, including in the context of applications such as the control of self-driving vehicles.

10. Integrated self-defense of interconnected systems

Curriculum: Software, System, and Infrastructure Security

University: Alma Mater Studiorum - Università di Bologna

Funds: Research funds

Additional benefits:

Website:

Contact person: Franco Callegati

Description

The research project focuses on a near future scenario where IT and OT systems in industrial plants and supply chains will be more integrated. The objective of the research is to propose new methodologies and tools for the assessment of cybersecurity and cyber resilience, and to define the necessary technological and governance measures to be integrated for the continuous improvement of the cyber posture. The research wants to propose innovative methodologies and solutions of general validity in terms of mapping architectures and processes in order to detect vulnerabilities, single points of failure, bottlenecks and other issues that could be addressed through integrated self-defensive components possibly based on AI/ML. To this end, new approaches will be analyzed and evaluated, also based on simulation models of systems, possibly integrated by digital twins, as well as machine/deep learning approaches for the analysis, evaluation, and semi-autonomous treatment of risks. The research will mainly focus on application scenarios such as manufacturing industries, critical infrastructure and smart cities and will consider the main driver technologies, including cloud and edge architectures, 5G and software-defined network infrastructures, taking into account that security, resilience and safety must also be guaranteed for the IoT elements that represent the current frontiers of production, from the so-called digital factory to the servitization of plants and products.

11. Discovery of False Information on digital communication channels

Curriculum: Software, System, and Infrastructure Security

University: Università di Palermo

Funds: DM 351-PNRR: Pubblica Amministrazione

Additional benefits:

Website:

Contact person: Giuseppe Lo Re

Description

The patterns of dissemination of false or partially true information can vary significantly depending on several characterizing factors, including the environment chosen to convey the attack (social networks, websites, messaging systems, etc.), the content transmission mode, and the identity of the source, whether human or artificial.

For this reason, automated verification systems cannot currently provide certain results and can at most provide a probabilistic indication after a verification process (fact-checking) carried out by human operators. Such strategies have multiple limitations, the most obvious is certainly non-timeliness. To fill this gap, the proposed research activity is aimed at the study and definition of new solutions that exploit artificial intelligence methods to support: the detection of polarizing topics on which an attacker could engage a fake news dissemination mechanism; the study of anomalous content dissemination dynamics; the real-time recognition of fake news by jointly analyzing heterogeneous information flows, coming from sources characterized by different levels of reliability; and the realization of secure systems, even from "adversary" attacks. Activities should also include analysis of legal aspects and safeguarding user privacy.

12. Formal methods for system security

Curriculum: Foundational Aspects in Cybersecurity

University: Università degli Studi di Firenze

Funds: DM 351-PNRR: Pubblica Amministrazione

Additional benefits:

Website:

Contact person: Rosario Pugliese

Description

This research activity will address the foundations of computer systems, software, or hardware to devise formal languages and methods for rigorously specifying and reasoning about the security properties of such systems, in addition to their functional correctness. The application of formal methods to security has emerged over recent decades as a well-established research area, and many related tools are applied in practice with increasing success to improve the security of real-world systems. This research activity embraces various possible topics and can be customized based on the candidate's preferences. Relevant to this activity are different kinds of security properties (e.g. authentication, confidentiality, and integrity), approaches (e.g. access control and information flow control), and system abstraction levels (e.g. design, configuration and implementation). One possible aim is to develop formal languages and methods for the specification and management of authorisation policies configured to enforce access control. A few challenges are: proving policies' correctness wrt high-level properties; defining correct-by-construction techniques to synthesise policies from high-level properties; developing formal analysis techniques to estimate the effects of the run-time interference between policy evaluation and system components' behaviour; determining the impact of policy changes, due to their maintenance and evolution over time, on systems components' behaviours.

13. Security of 5G infrastructure and its evolution to 6G

Curriculum: Foundational Aspects in Cybersecurity

University: Università degli Studi di Roma "Tor Vergata"

Funds: DM-351-PNRR: Ateneo

Additional benefits:

Website: http://dottorati.uniroma2.it

Contact person: Giuseppe Bianchi

Description

The emerging network infrastructures for cellular systems referred to as 5G and its evolution 6G are characterized by very high complexity and extreme diversification both in terms of network technologies (different radio accesses, including non-natively cellular accesses such as WiFi and Bluetooth, different infrastructure and transport technologies) and in terms of supporting computing systems (multi-access edge cloud, core cloud, continuum cloud). Such heterogeneity emerges in terms of multiple stakeholders and verticalization of services through so-called network slicing capabilities and has led to an impressive increase in the attack surface. The proposed project aims to address the security, privacy, and availability challenges emerging in the various functional and technological domains of the 5G architecture (radio interface, Multi-access Edge Computing, transport infrastructure, virtualized core network functions, management, and orchestration), covering, in particular, the aspects of continuous security verification and control (e.g., DevSecOps) through all the different phases of the 5G+ technology lifecycle (think, build, test, run&update). Special attention will be paid to the security aspects of 5G location systems and the protection of interfaces between network functions and the development of tools for assessing vulnerabilities at the protocol level.

14. Well-founded cybersecurity techniques

Curriculum: Foundational Aspects in Cybersecurity

University: Università Ca' Foscari, Venezia

Funds: DM-351-PNRR: Ateneo

Additional benefits:

Website:

Contact person: Riccardo Focardi

Description

This project is part of the "Foundational Aspects in Cybersecurity" curriculum and concerns the use of formal methods applied to cybersecurity in order to improve the state of the art of system and network security. In particular, the PhD student will use formal verification techniques and tools in various application areas that the research group in Cybersecurity of Ca 'Foscari actively deals with such as, for example: correctness of programs, secure compilation, security of Web and networks, security of embedded systems. The research aims to find new attacks and propose innovative solutions based on solid foundations and formal proofs of correctness, and will possibly be carried out in collaboration with the University spin-offs.

15. Innovative and practical cybersecurity solutions for systems and infrastructures

Curriculum: Software, System, and Infrastructure Security

University: Università Ca' Foscari, Venezia

Funds: DM 351-PNRR: Pubblica Amministrazione

Additional benefits:

Website:

Contact person: Flaminia Luccio

Description

This project is part of the "Software, System, and Infrastructure Security" curriculum and concerns the study of innovative techniques for the security of software, hardware and communication systems. In particular, the PhD student will develop cybersecurity techniques and tools in various application areas which the research group in Cybersecurity of Ca 'Foscari actively deals with, such as, for example: the correctness and protection of software, identification, Web and network security, embedded systems security, usable security. The research aims to find new attacks and propose innovative solutions with a practical impact, and will possibly be carried out in collaboration with the University spin-offs.

16. Software security: analysis and verification of properties

Curriculum: Software, System, and Infrastructure Security

University: Università di Pisa

Funds: DM-351-PNRR: Ateneo

Additional benefits:

Website:

Contact person: Cinzia Bernardeschi and Gian Luigi Ferrari

Description

The overall topic for the phd project concerns the definition and development of techniques for the analysis and verification of software security. Techniques for ensuring that software is free of bugs and security vulnerabilities, included the disclosure of sensitive data, are of utmost importance, since software vulnerabilities can often be exploited to cause huge damage. Techniques in the scope of the phd project include program analysis based on static analysis (e.g., control flow analysis, taint analysis), abstract interpretation and symbolic execution, supported by constraint solving and SMT. The goals include to significantly extend the power and scalability of currently available techniques to make them applicable to real-world code bases, including concurrent and embedded software, as well as software for IoT systems.

17. Data protection and privacy in innovative application scenarios

Curriculum: Data Governance and Protection

University: Università degli Studi dell'Insubria (Varese)

Funds: DM-351-PNRR: Ateneo

Additional benefits:

Website: http://dawsec.dicom.uninsubria.it/elena.ferrari/

Contact person: Elena Ferrari

Description

The project aims to develop new solutions to support data providers to use and share end-users data by respecting users' privacy. The designed strategies will have to consider, on one side, the protection requirements of end-users and, on the other side, the data provider's economic assets (e.g., data utility, costs). This trade-off requires investigating the best-suited data protection policies and related technologies to enforce user requirements. For this purpose, it is expected to use different techniques, varying from AI to support user's requirements specification to anonymization algorithms. The project will target decentralized scenarios to go beyond traditional centralized architectures and application domains characterized by a massive amount of sensitive data (such as IoT). The Ph.D. student will investigate efficient techniques to support the necessary computation and will analyze the security and privacy properties of the developed methods under different attack scenarios.

The potential topics include (and are not limited to): DLT (Distributed Ledger Technology, e.g., blockchain) based services on the support of decentralized data sharing and auditing, risk assessment and data sharing in zero-trust architectures, data protection under normal and emergency situations, privacy preferences and data protection policies' specification and analysis.

18. Certification Languages for Compliance and Security of Cloud Services

Curriculum: Human, Economic, and Legal Aspects in Cybersecurity

University: Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy

Funds: Progetto Europeo H2020 MEDINA (grant nr. 952633) and Istituto di Informatica e Telematica

Additional benefits: Possibility of supplementing the scholarship with project funds

Website: https://www.iit.cnr.it/en/marinella.petrocchi/ ; https://www.iit.cnr.it/en/fabio.martinelli/

Contact person: Marinella Petrocchi and Fabio Martinelli

Description

The adoption of Cloud Computing in the EU is still limited. One reason for this is lack of security and transparency that customers perceive in this technology. Cloud Service Providers often rely on security certifications and compliance to regulations to improve this transparency. In this context, the EU Cybersecurity Act proposes improving customer trust in the European ICT market through a set of EU-wide certification schemes, such as the European Cybersecurity Certification Scheme for Cloud Service (EUCS) being developed by the European Union Agency for Cybersecurity (ENISA). Unfortunately, the requirements dictated by the certification schemes -EUCS is not an exception- are defined in natural language. They need to be translated into a machine-readable representation, which facilitates their processing. This project aims to automatically transform the natural-language specification of cloud security certification frameworks, like EUCS, into machine-readable expressions, by leveraging Natural Language Processing techniques. Ultimate goals are: a standardized way to technically approach the requirements of a security certification scheme; a framework and working language to express requirements as automatically actionable controls; the reduction of the operation workload for technical staff related to (cloud) security certification processes; the adaptation of the framework to data usage policies for checking compliance to regulations, as the EU Data Act and similar.

19. Cognitive characterization of fake media and media manipulation

Curriculum: Data Governance and Protection

University: University of Siena

Funds: DM-351-PNRR: Ateneo

Additional benefits:

Website: http://clem.dii.unisi.it/~vipp/index.html

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. Multimedia forensic researchers have developed several tools to distinguish genuine media from fake ones, and to identify various forms of media manipulations. Yet, detecting fake media and media manipulations is not enough to prevent the diffusion of fake news and the use of manipulated media for disinformation campaigns; it is necessary that the malevolent use of the manipulations is also identified. The next challenge in media forensic, then, is to link the detection of asset manipulations to the purpose of the manipulations and the role that the assets and their manipulations have in the context wherein they are used. In the above framework the goal of this project is twofold: i) to build suitable cognitive models to study the affective impact that media manipulations and the use of fake media have on the users; ii) to develop a pool of automatic techniques to link the manipulations of a media asset to the intended meaning of the manipulations. Depending on the background of the PhD candidate, research may focus more on cognitive aspects (qualifying the research for the "Human, economic and legal aspects in cybersecurity" curriculum) or on technological aspects (better suited to the "Data governance and protection" curriculum)

20. Human and socio-legal dimensions for a better-safe Cyberspace

Curriculum: Human, Economic, and Legal Aspects in Cybersecurity

University: Università di Firenze

Funds: DM 351-PNRR: Pubblica Amministrazione

Additional benefits:

Website:

Contact person: Andrea Simoncini

Description

Cybersecurity, meaning the security of cyberspace, is more than a technical problem and doesn't only focus the protection of data and infrastructures from intrusions. It encompasses all the human, socio-legal and economic dimensions related to the development of the digital world in today societies. This new and complex research field includes five main areas of inquiry. 1) Models of regulation and Authority enforcement for a safe Cyberspace. 2) Ethical and legal aspects of Cybersecurity. 3) Cybercrime and CyberDiplomacy 4) Social and economic policies for cybersecurity 5) Data governance, national clouds and digital sovereignty. All the research areas are to be matrixed over some main foundational and methodological pillars: fundamental-rights protection, the evolving-upcoming global regulation (EU vs US vs China), the socio-economic impact of cyber-regulation, human and social effects of cyber-society. Phd candidates can focus their project on either one or more cross-cutting research areas. Research projects have to be preferentially designed according to a holistic, multidisciplinary, problem-solving approach and should involve public and private stakeholders, implementing innovative technological, legal, ethical and organizational solutions, such as strengthening key competencies, transfer of technologies and knowledge, and the ability to integrate technologies in systems and services.

21. Methods and tools for the security assessment of critical information infrastructures

Curriculum: Foundational Aspects in Cybersecurity

University: IMT School for Advanced Studies Lucca

Funds: DM 351-PNRR: Pubblica Amministrazione

Additional benefits: Full board accommodation

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

Contact person: Letterio Galletta

Description

Information and communications technologies (ICTs) are increasingly common in our daily activities. Some of the ICT systems, services, networks, and infrastructures form a vital part of our society, providing essential goods and services or constituting the underpinning platform of other critical infrastructures. They are typically regarded as Critical information infrastructures (CIIs) as their disruption would seriously impact vital societal functions. Since cyber threats to CIIs could potentially affect the safety of citizens, many of these systems require a high level of security.

Security engineering for CIIs is a multidisciplinary field involving various topics ranging from secure software development and cryptography to embedded systems design and network security. Formal modeling and verification techniques have the potential to provide strong security guarantees and support vulnerability detection tools. However, developing effective formal methods-based tools for CIIs is still open.

This project aims to study new methodologies and tools based on formal methods for the security assessment of CIIs that could support Macro-regional CSIRT in their activities. The research activity could focus on different aspects, such as network security, protocol security, and application security. Also, different verification techniques may be considered, including, for instance, model checking, fuzzing, static analysis, and security testing.

22. Enhanced soft computing techniques for fake news detection

Curriculum: Human, Economic, and Legal Aspects in Cybersecurity

University: Università degli Studi di Salerno

Funds: DM-351-PNRR: Ateneo

Additional benefits:

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

Contact person: Vincenzo Loia

Description

The spread of fake news through the social media is a relatively new problem. Its importance is witnessed by the attention paid by social network platforms such as Facebook, Whatsapp. Fake news can take several different forms in the social media environment, making even more difficult to efficiently detect and contrast them. An example is offered by clickbait headlines, inducing users to open possibly biased articles to gain money from views. The literature trend in this field is about supervised classification approaches. The interest in deep learning (DL) techniques, such as Recurrent Neural Networks and Convolutional Neural Networks, seems to be dominant. Such DL techniques represent the state of the art. Anyhow, there are still some concerns and open issues. First, fake news still has to be fully understood from a linguistic perspective. In this regard, the fuzzy logic (FL) formalism may help. The contributions to the field using FL are still scarce and not offering a formal response to address the open issues. Secondly, both content- and context-aware techniques should be implemented. Finally, it is worth mentioning the lack of widely accepted benchmark datasets. The currently available resources may not be sufficient to check the effectiveness of new models in a real-world scenario. This research project aims to address the main open issues above, prioritizing the FL formalism to obtain more effective DL variants.

23. Cyber Security and Cyber Intelligence measures for Monitoring, Preventing, and Mitigating Radicalisation Pathways

Curriculum: Human, Economic, and Legal Aspects in Cybersecurity

University: Università degli Studi di Salerno

Funds: DM-351-PNRR: Ateneo

Additional benefits:

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

Contact person: Giuseppe Fenza

Description

The role of the Internet in radicalization has been widely discussed since 1990s. Radicalization is the process of pushing an individual towards more extremist views. Online communities play a central role in spreading radicalization since users may disseminate their radical ideologies, gain support and provide instruction in terrorist activity. Additionally, the homophily property underlying recommendation systems traps the users in radicalization pathways, shifting their opinions along the time from moderate to extreme. An effect of this can be echo chambers, where particular opinions can easily start to be re-shared and reinforced, which could have the gradual effect of causing someone to experience a change in mindset. Therefore, tools for user monitoring are required, such as filter bubbles to track information about users' activities combined with AI techniques that can help discover polarized social groups.

The goal of this research project is aimed at finding cybersecurity solutions to contain the radicalization phenomenon. The main topics to investigate to achieve the prefixed goal are listed as follows:

- Community detection and network monitoring
- Echo chamber and group polarization detection
- User interaction analysis by fusing network topology with semantic information
- Influential node identification for inter-community polarization analysis
- Dynamic network graph time-evolution analysis.
- Prediction of group polarization evolution.

24. Cryptographic protocols for the cyberspace

Curriculum: Foundational Aspects in Cybersecurity

University: Università degli Studi di Salerno

Funds: DM 351-PNRR: Pubblica Amministrazione

Additional benefits:

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

Contact person: Alfredo De Santis

Description

The project focuses on the design and the analysis of new cryptographic primitives and protocols, suitable for strengthening communication systems and distributed systems, and tailored for the realization of secure, private, and resilient digital infrastructures. The main cryptographic area on which the efforts will be concentrated is secure computation. The research targets are scalable, efficient, and flexible multiparty solutions, secure against powerful adversarial strategies, privacy preserving, and adaptable to a variety of applicative settings. In particular, the project will be developed along two research lines: - two-party and multi-party computation general protocols will be optimized and properly customized to solve specific issues in traditional computational settings, wired and wireless, and in the newest lightweight infrastructures, quickly evolving during the last years - two-party and multi-party ad-hoc protocols will be designed and analyzed, to solve in a more efficient way, compared to the general solutions, basic problems, of interest by themselves and as intermediate steps in complex problems. Regarding the second research line, among the others, attention will be focused on secret sharing schemes, on protocols for secure set operations, and on encryption/authentication primitives, useful for secure computation, especially in lightweight settings. As well as, on applications of machine learning techniques, both as a constructive tool for protocol design, and as a destructive tool for protocol analysis

25. Keeping systems, data, and your identity secure

Curriculum: Software, System, and Infrastructure Security

University: Università della Calabria

Funds: DM 351-PNRR: Pubblica Amministrazione

Additional benefits:

Website: https://people.dimes.unical.it/andreapugliese

Contact person: Andrea Pugliese

Description

The project plans to study problems related to different aspects of cybersecurity, with the aim of identifying methodological and technological approaches and solutions to the issues that currently present the greatest interest and criticality (including by studying real case studies proposed by public and private actors and stakeholders) aiming at the definition and development of more secure and reliable processes and infrastructures.

The main topics of the project include:

- methods, techniques and tools for the protection of systems, infrastructure and data;
- 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 or her a wide range of professional possibilities, in the public sector (including the National Cybersecurity Agency), in 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 realities that require professionals with solid scientific, methodological, and technological skills in cybersecurity.

26. Advanced usage control approaches for data protection

Curriculum: Data Governance and Protection

University: IIT-CNR

Funds: Progetto Europeo E-CORRIDOR e IIT

Additional benefits: Possibility of supplementing the scholarship with project funds

Website: https://www.iit.cnr.it/en/fabio.martinelli/

Contact person: Fabio Martinelli

Description

The focus of the PhD work is about the study of models and architectures for advanced data usage control approaches for protecting data privacy while ensuring a controlled data sharing, as well as achieving digital sovereignty. The PhD work will include the design of a general architecture of a usage control framework able to enforce policies on data and services offering flexing enforcement and obligation management opportunities. The main feature of such a framework will be the capability to promptly react to changes in the access control context while accesses are in progress, according to what specified in the policy itself. Such architecture will be very modular and flexible in order to be easily configurable to be adapted and customized for a number of relevant use cases that will be identified as part of the PhD work. The PhD work will also include the study of the integration of the usage control framework with novel techniques for preserving the privacy of the framework users.

27. Use of Artificial Intelligence for the protection of Critical Infrastructure

Curriculum: Software, System, and Infrastructure Security

University: Politecnico di Bari

Funds: DM-351-PNRR: Ateneo

Additional benefits:

Website: https://www.poliba.it

Contact person: Eugenio Di Sciascio

Description

Critical Infrastructures represent a set of technological assets that produce vital activities and services for the country by dispatching Primary Services that, when integrated with each other, enable the interoperability of other services (logistics, health, financial). It becomes critical to secure people from any cyber attack. Using AI techniques, this research proposal aims to investigate and implement new capabilities for the management, detection, and response of attacks that can be handled by such infrastructures. Through the adoption of AI techniques and algorithms, new capabilities for monitoring information flows between the entities involved will have to be developed. To achieve the stated objectives, this proposal uses AI approaches to investigate:

- GEOINT: Geospatial information collected from satellite photographs and areas or from map and terrain data.
- MASINT: Measurement and signature information collected from a range of signatures of fixed or dynamic target sources. (Masints are divided into:electro-optics, nuclear, radar, geophysics, materials, and radio frequency).
- OSINT: Information gathering from open sources. Through the development and adoption of threat intelligence techniques based on AI algorithms, it will be possible to improve cyber vulnerability analysis of critical infrastructure, implementation of attack/defense models, and practices to harmonize emergency response.

28. Formal Models of Cyber Security

Curriculum: Foundational Aspects in Cybersecurity

University: GSSI

Funds: Decreto MUR n. 351 del 09-04-2022, lett. b. (borse per dottorati di ricerca PNRR)

Additional benefits:

Website: https://cs.gssi.it/emilio.tuosto/

Contact person: Emilio Tuosto

Description

The ambition of this project is to extend the research on security protocols by explicitly accounting for the "human factor". In fact, human behaviour is critical in determining the degree of security of an organisation. Many attacks hinge on people's "misbehaviour". Many factors contribute to "human misbehaviour" that makes critical assets vulnerable. For instance, people may ignore well-specified practices due to negligence, lack of appreciation of the security risks, or misunderstandings (eg, when or how should a rule be applied). Also, protocols and legal requirements may change over time and their compliance may be compromised by miscommunications.

This project will address the following research questions

RQ1: "How human behaviour should be formally specified and taken into account in the analysis of cybersecurity?"

RQ2: "How to support continuous compliance?"

We will develop mechanisms to specify cybersecurity protocols and their usage (aka ceremonies) modelling human behaviour in terms of non-deterministic and probabilistic system. We will study the robustness of cybersecurity protocols in presence of misbehaving roles.

Human behaviour impacts on continuous compliance. Critical applications eg, in the automotive domain, are continuously enhanced through dynamic over-the-air updates. This poses various challenges related to both safety and security and, specifically, there is an increasing demand of continuous compliance with safety and security standards.

29. Cybersecurity of Complex Systems

Curriculum: Software, System, and Infrastructure Security

University: Università degli Studi di Genova

Funds: DM-351-PNRR: Ateneo

Additional benefits:

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

Contact person: Alessandro Armando

Description

The candidate will develop one of the following lines of research:

- Application Cyber Risk Assessment: developing automated or semi-automated procedures for assessing the cyber risk exposure of application ecosystems in emerging scenarios, e.g., Mobile, Cloud, Fog, IoT, and any combination thereof.
- Multi-domain Cyber Range and Cyber Resilience Testing of Physical Cyber Systems: definition of a framework for integration between Cyber Range and digital replicas (Digital Twin) of physical infrastructure (e.g., transportation infrastructure) to create multi-domain scenarios for cyber risk resilience testing activities, procedures, and countermeasures against attacks, evaluation of procedures and training of personnel.

30. Foundations and Methodologies for Secure Programming of CPS

Curriculum: Foundational Aspects in Cybersecurity

University: Università di Camerino

Funds: DM-351-PNRR: Ateneo

Additional benefits:

Website: http://micheleloreti.com

Contact person: Michele Loreti

Description

Modern software architectures, often referred as Cyber-Physical Systems (CPS), are often composed by a large number of entities that interact with each other and with the enclosing environment to reach local and global goals. Formal tools and methodologies are needed to supporting development of secure CPS. In this project we plan to study a framework that, following a "property driven" pattern and integrated in a "secure by design" approach, permits developing secure CPS. The goal of the project is to develop a methodology that, starting from a formal definition of both "functional" and "non-functional" system requirements, permits checking and refining the expected properties along the whole development process. System requirements will be defined at both global and local level. Global properties identify the overall requirements of a system and typically render the expected emerging behaviour. Local properties consider the behaviour of the single components. Tools will be studied to guarantee that the satisfaction of these requirements is preserved at the different stages of development and that lead to the set of formulas that should be satisfied at runtime. These formulas will be also used to instrument runtime monitors. These will guarantee that in the operating environment, which can differ from the one considered at design time, the behaviour emerging from local and global interactions meets with the requirements defined along the development phase.

31. The Anti-Digital Forensics Cyber Kill Chain

Curriculum: Software, System, and Infrastructure Security

University: Università di Catania

Funds: DM-351-PNRR: Ateneo

Additional benefits:

Website:

Contact person: Giampaolo Bella

Description

Criminals hardly ever plead guilty, hence Digital Forensics (DF) comes into play as the lawful discipline to gather and interpret evidence in support of a conviction or of an overturning. Coherently with our computerised times, DF vastly relies on computer support through a number of dedicated techniques and tools.

Yet, following the establishment of DF as a routine practice, criminals have tried out novel heuristics and often adopted or developed a new range of tools to counter and, ultimately, evade that practice. For example, wiping off metadata may dramatically influence a verdict, and full-disk encryption on a storage unit may signify that crucial evidence goes unnoticed. In consequence, Anti-Digital Forensics (ADF) is just peeking out and, due to the basic cybersecurity motto that one needs to play as an attacker to develop the best defence, is worth developing with ethical purposes.

This project aims to: establish ADF as a discipline, elicit its requirements and aims, specify its various sub-application domains and, chiefly, advance an ADF Cyber Kill Chain (CKC) as a field reference. While building the ADF CKC is challenging because it requires a vast skillset covering DF, cybersecurity, data protection and programming, it would largely assist DF experts through the development of counter-evasion strategies.

The ADF CKC will be piloted for the sake of validation over data such as multimedial files and environments such as modern car infotainments.

32. Investigation on GAN- Generated Malware

Curriculum: Software, System, and Infrastructure Security

University: University of Sannio

Funds: DM-351-PNRR: Ateneo

Additional benefits:

Website: https://www.unisannio.it/it/users/visaggio

Contact person: Corrado Aaron Visaggio

Description

The co-evolution of malware and malware detection system is a cycle is becoming faster and faster, and requires the development of effective countermeasures in a similar short time. The increasing adoption of machine learning classifiers for automatically recognizing malicious programs and behaviours related to intrusions, spreading, evasion and survival is exposing protection systems to adversarial attacks. Three approaches are mainly used for producing adversarial examples: gradient-based, optimization-based, and Generative Adversarial Networks(GAN). GAN consists of a iterative competition between two components, the Generator and the Discriminator, where the former produces candidate adversarial examples, while the latter evaluates their effectiveness. The evaluation provided by the Discriminator leads the Generator to modify further the original example. The PhD course will focus on three tasks. As first, the candidate should understand how a GAN can be used to modify existing malware, while preserving behavioural properties of the program, i.e. changes to malware shouldn't affect its correct working. As second task, the candidate should study which kind of methods could be able to detect GAN-generated malware and disarms the harming potential of such a malicious creation. As third task, the candidate should design and execute a comprehensive set of experiments for demonstrating the elaborated theses regarding how to recognize the GAN-generated malware.

33. Application of zero-knowledge techniques to IoT constrained devices

Curriculum: Software, System, and Infrastructure Security

University: Università di Camerino

Funds: DM-351-PNRR: Ateneo

Additional benefits:

Website: http://www.leonardomostarda.net

Contact person: Leonardo Mostarda

Description

Zero-Knowledge proofs (ZK-proofs) have become widely adopted in various contexts such as blockchain, finance, voting, ethical behavior and anonymous authentication. This advanced cryptography is capable of proving the correctness of financial transfers, protocol interactions or more generally state updates without disclosing sensitive information. ZK-proofs not only guarantee privacy but also allow trust of a multi-party computation when the entities involved do not trust each other. The application of ZK-proofs is particularly challenging in IoT systems since IoT constrained devices can have limited memory and computation power. These IoT devices require efficient ZK-proofs in terms of space and computation. Although some ZK-proofs techniques can keep the size of data (e.g., by aggregation with recursive proofs) they have not been tailored in the context of IoT constrained devices. The aim of the project is to advance the state-of-the-art of ZK-proofs in the contest of IoT constrained devices as an efficient solution for IoT systems integrated with blockchain. Such integration can result in a secure and scalable decentralized IoT system that can see applications in various contexts such as the Industry 4.0 and Smart Cities. The proposed solution will be validated in real industrial scenarios.

34. Hardware implementation of Post Quantum Cryptography algorithms

Curriculum: Software, System, and Infrastructure Security

University: Politecnico di Torino

Funds: DM 351-PNRR: Pubblica Amministrazione

Additional benefits:

Website: https://cybersecnatlab.it

Contact person: Paolo Prinetto

Description

Over the coming years, with the growing of Quantum Computing, it is expected that Post Quantum Cryptography (PQC) will replace the current public-key cryptography paradigm. PQC leverage on mathematical elements which are not straightforward to implement on standard processor, as well as require non-negligible computational power and resources to be executed. Therefore, the interest in hardware accelerator for PQC is continously increasing. In 2017 NIST started a standardization process for PQC algorithm. Since then, in the literature, implementation of the different candidate protocols has been proposed, mainly in pure software or through hardware-software co-design methodology. However, very few pure hardware design has been proposed. The PhD work will focus on pure hardware implementation of PQC algorithms, following two main approaches: (i) to build an Application Specific Integrated Circuit (ASIC) to accelerate the requested algorithm. This solution can reach the best perfomance, but it requires a considerable design effort and relative non-recurrent costs. (ii) to integrate PQC algorithm directly in the processor pipeline with smaller hardware accelerator. This in-pipeline acceleration approach can be evaluated on open Instruction Set Architecture (ISA) processors, such as the RISC-V architecture. The hardware design should minimize resource utilization, in terms of area and power, exploiting parallel and pipelined computations.

35. Data protection in emerging scenarios

Curriculum: Data Governance and Protection

University: Università degli Studi di Milano

Funds: DM-351-PNRR: Ateneo

Additional benefits:

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

Contact person: Pierangela Samarati

Description

The availability of highly performing systems and services for gathering, storing, and processing data, and of analysis techniques on large data collections, bring great benefits on a personal, business, economic and social level. The collection, sharing and analysis of data, with contributions from different sources and different actors is in fact a great enabling factor for an increasingly digitally evolved society. On the other hand, a strong obstacle to the true realization of this vision is represented by legitimate considerations on data protection. In fact, the (real or perceived) loss of control over data by those who have the authority over them, and the potential compromise of data confidentiality, represent a strong obstacle on the creation of an open framework for information sharing and analysis. The goal of the project is to contribute to the development of advanced solutions enabling the different actors with control over their data in the various data release, sharing, and analysis scenarios. The research can entail investigation in different areas, including: data governance frameworks to support the protection requirements; policy languages and models to express them and techniques for enforcing them; approaches for effective and efficient access to data, offering computation and management functionality, while ensuring the confidentiality and integrity of data and computations; approaches for selective controlled data sharing and release, for the protection of information and computation models in distributed, pervasive, and intelligent scenarios.

36. Human-centered Framework to integrate trustworthy and cyber intelligence in digital systems

Curriculum: Human, Economic, and Legal Aspects in Cybersecurity

University: Università degli Studi di Bari Aldo Moro

Funds: DM-351-PNRR: Ateneo

Additional benefits:

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

Contact person: Danilo Caivano

Description

The intelligent systems that pervade our society and interact with users daily, without users being aware of it, need to be regulated, monitored, and constantly analyzed to ensure fair and explainable results and the satisfaction of ethical, security, and privacy criteria. Such systems generate an output that can be, from time to time, a content, prediction, recommendation, or decision that influences the users' behaviors and the environment with which they interact. If the decisions made by the systems are not verified, fair, and explainable, there is a reputational and economic risk to organizations that can impact the security of users and the organization itself. It is therefore important not only to constantly monitor the behavior of such systems to avoid unfair or even wrong outcomes but also to establish metrics that measure the risks and countermeasures to be put in place to mitigate risks to users' security. The European Community has issued several guidelines in recent years to ensure that these systems meet a suitable level of accuracy, robustness, and security. It becomes, therefore, essential to establish an assessment framework that provides a gap analysis, risk assessment, and remediation plan to validate these systems and make them compatible with current regulations.

37. Design of novel security firmware for modern microarchitectures

Curriculum: Software, System, and Infrastructure Security

University: Università di Trento

Funds: Research funds

Additional benefits:

Website: http://www.disi.unitn.it/~crispo

Contact person: Bruno Crispo

Description

Modern microarchitectures implement numerous security mechanisms at the hardware level that are not or only partially exploited by existing software. This doctoral scholarship concerns the study, design, implementation, and validation of new software security services that exploit these new hardware mechanisms. These services, typically running within Trusted Execution Environments (TEE), will complement and/or enrich existing ones (e.g., secure boot, integrity attestation, cryptographic functions, etc.) in order to provide a rich set of security services to operating systems. These services will be designed, implemented, and verified using open and public specifications. The Ph.D. also includes the study of existing secure execution environments in order to assess the causes behind the many flaws and vulnerabilities that have emerged in recent years.

38. Cyber security applied to 4/5G Mission Critical Networks and Applications

Curriculum: Software, System, and Infrastructure Security

University: IMT School for Advanced Studies Lucca

Funds: DM 352-PNRR: Leonardo SpA

Additional benefits: Full board accommodation

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

Contact person: Mirco Tribastone

Description

The Ph.D. student will focus her/his activities on studying new methodologies and tools for security assessment and design of secure telecommunications networks in 4/5G technology for Mission and Business Critical applications. This type of communication infrastructure and its applications are a vital asset for all public and private emergency response organizations that use them for their operations. Their disruption or failure can impact the vital functions of these organizations, cause possible loss of life, and possibly impact the safety of citizens and operators.

Formal modeling and verification techniques have the potential to provide robust security assurances and support vulnerability detection tools. However, developing effective tools based on this methodology is still an open issue. The research activity will focus on several aspects, such as the definition of a formal methodology that enables the secure and resilient cyber design of the network solution (access, transport, core network, and applications) also about cloud deployment models, verification of security at the network, protocol and application levels (with particular focus on Police Force use case applications).

In addition, the research activity will consider as reference the specifications, recommendations, and best practices of the main international bodies in the field of communications security and, in particular:

- The 3GPP security standards (Release 16 and later)
- The NIST ZTA (U.S National Institute of Standards and Technology) guidelines.
- European Commission guidelines (EU toolbox for 5G security, NIS directive, ENISA line guide).

Security of open RAN architectures, as specified by the O-RAN Alliance Security Focus Group, will also be the research subject.

Various verification techniques may be considered, including, e.g., model checking, fuzzing, static analysis, and security testing.

The research product will also involve publications of an applied nature on communication solutions developed by Leonardo S.p.A. for broadband 4/5G telecommunications networks.

39. Evolutionary application of AI techniques in cybersecurity

Curriculum: Software, System, and Infrastructure Security

University: IMT School for Advanced Studies Lucca

Funds: DM 352-PNRR: Thales Group

Additional benefits: Full board accommodation

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

Contact person: Rocco De Nicola, Simone Soderi

Description

The research project will be in the context of heterogeneous application domains such as critical infrastructure, manufacturing, and public administration, and aims to enable the integration of Artificial Intelligence and Machine Learning algorithms on Cyber Security Intelligence, Cyber Monitoring and Cyber Attack Simulation platforms, and to enrich their analysis and detection effectiveness and to achieve the following objectives:

- implementation of automatic mechanisms for learning behaviors on the network and systems in order to develop advanced correlation rules for early detection of possible attacks and anomalies;
- reduction of alerts generated by monitoring platforms to only significant events that need to be investigated, ensuring full support to cyber operators during the incident analysis activity through the possibility of "navigating" the specific correlation and behavioral investigation path;
- build a theoretical/practical framework that enables mechanisms for predictive analysis of possible cyber attacks towards the assets that need to be protected (simulation, predictive alerting), also through the refinement of AI techniques used in cyber defense to avoid the limitations of current applications about the risk of missing so-called "weak signals"

The study will use an existing complex Security Intelligence /CSOC - Cyber Security Operation Center platform to develop the research project and the various AI and Machine Learning algorithms to be implemented, aiming to realize a demonstrable PoC- Proof of Concept.

Added to this is the need to adequately protect Big Data that is created by cyberinfrastructure (logs, events, network flow, data enrichment, metadata, Threat Intelligence, Data lake, Threat Hunting, etc.). Therefore, the research project will include a specific study to identify and implement quantum/post-quantum encryption techniques appropriate for protecting complex, heterogeneous, and distributed databases such as the analyzed Big Data Cyber.

40. **Analysis of a highway operator's automated critical IT and OT infrastructure systems and identification of innovative cybersecurity solutions**

Curriculum: Software, System, and Infrastructure Security

University: IMT School for Advanced Studies Lucca

Funds: DM 352-PNRR: Autostrade per l'Italia, S.P.A.

Additional benefits: Full board accommodation

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

Contact person: Letterio Galletta, Massimiliano Masi

Description

Critical infrastructure is a system whose destruction, disruption or even partial or momentary unavailability significantly weakens a country's efficiency and normal functioning, as well as the security and economic-financial and social system. A particular type of critical infrastructure is air, sea, rail, and road transport. Although ENISA and the EU Commission have produced several publications and guidelines on critical infrastructure protection for the energy, financial, or maritime transport sectors, a specific guideline for the road transport sector is lacking.

The first objective of this research activity is to define a methodology that enables the design of a system that enables road transport, that is secure from its design or in its re-engineering, that goes to avoid data silos, and that facilitates the exchange of knowledge and expertise among international stakeholders, such as road operators, smart cities, and emergency responders.

The second objective of this activity is to design and implement innovative technical solutions in the area of cybersecurity for the road transport sector, particularly highway tunnel automation and smart road systems. The activity will mainly consider IT/OT/IoT systems that realize the critical infrastructure and services delivered by cloud systems. Special attention will be given to the safety and availability aspects of the systems.

41. Development of technologies for automatic recognition of (deep) fake news on OSN

Curriculum: Human, Economic, and Legal Aspects in Cybersecurity

University: Università degli Studi di Catania

Funds: DM 352-PNRR: Ermes Cyber Security S.R.L.

Additional benefits: Possibility of supplementing the scholarship with company funds

Website: https://www.dmi.unict.it/~battiato/

Contact person: Sebastiano Battiato

Description

The generation and spread of fake news is a social problem with major repercussions on security and privacy, as well as a technique often used by attackers to carry out targeted attacks on companies and institutions. Cases have emerged in which fraud and credential theft attacks have been carried out, starting from fake news, with significant economic losses and social damage. Moreover, attackers are increasingly resorting to AI-based techniques such as Deep Fake and Fake Speech. The purpose of the Ph.D. will be to explore the world of online disinformation and to develop methodologies that analyze texts, multimedia content, and interactions on social networks to detect attacks based on AI-generated synthetic content. These technologies will then be applied to collect information and metadata about the players involved in the attacks (the attackers, victims, and any intermediaries) to facilitate correlations and simplify intelligence functions.