INFORMAZIONI PERSONALI

Tommaso Zoppi – ORCID 0000-0001-9820-6047

Via Sernesi 59, 50142 - Firenze, Italy

+39 328 7550629

tommyippoz@gmail.com

Sesso Maschio | Data di Nascita 12/10/1990 (età 32 anni) | Nazionalità Italiana

Data del CV 21/6/2023

Informazioni Generali e Carriera Lavorativa

DETTAGLI CANDIDATURA

Posizione RTD-B INF/01 presso Università degli Studi di Firenze, da decreto rettorale, 30 Maggio 2023, n. 485 (prot. 118406) pubblicato all'Albo Ufficiale (n. 6600) dal 31 maggio al 29 giugno 2023

ESPERIENZA LAVORATIVA

Lug 2019 – OGGI

Ricercatore a Tempo Determinato (Tipologia A, legge 240/10) - INF/01

Dipartimento di Matematica ed Informatica "Ulisse Dini",
Viale Morgagni 65 – 67/A, Firenze (FI), Italia

Attualmente impiegato come RTD-A presso il Dipartimento di Matematica e Informatica "Ulisse Dini" (UNIFI), dove svolge regolarmente attività di didattica, ricerca e collaborazione con aziende. Docente di una media di 6 CFU / anno di corsi erogati alla laurea triennale o magistrale in Informatica SMFN (INF/01) dall'inizio della posizione. Nello stesso periodo, le sue attività di ricerca si sono concentrate su tematiche inerenti la progettazione, implementazione, verifica e validazione di sistemi critici, con particolare riferimento a i) tecniche di rilevazione di anomalie per intrusion o error detection, e ii) architetture di sistema che rispettino specifici requisiti di sicurezza (safety). Durante i suoi anni da RTD-A, è stato co-autore di più di 20 papers ed ha collaborato in diversi progetti di ricerca Europei e Nazionali, ed in particolare ha coordinato le attività tecniche del gruppo di ricerca a cui afferisce per un progetto di ricerca di durata triennale con Rete Ferroviaria Italiana (Convenzione conto Terzi), che finanzia la sua posizione corrente da RTD-A. Tale progetto, conclusosi la scorsa estate, ha portato alla definizione di architetture di sistema di tre diversi sistemi (terra – bordo – manutenzione) che RFI vuole rinnovare ed installare sulla rete ferroviaria, è stato esteso tramite procedura del quinto d'obbligo e rinnovato per altri tre anni (completamento atteso per fine 2024).

Apr 2020 – Dic 2020

Collaborazione. Convenzione CINI – Resiltech – Progetto ProtectID

Resiltech s.r.l, Piazza Nilde Iotti 25, Pontedera (PI), Italia
Partecipazione al progetto ProtectID applicando tecniche note di anomaly detection a supporto di tecniche di autenticazione continua, con un duplice scopo: i) ricavare una proprietà di "spoofing detectability" di diversi tratti biometrici tramite analisi quantitativa di risultati di algoritmi applicati a dataset pubblici, e ii) proponendo un supporto run-time a processi di autenticazione basato sulla rilevazione delle anomalie nei dati rilevati e trasmessi dai sensori biometrici.

Mag 2019 – Dic 2019

Collaborazione. Convenzione CINI – Resiltech – Progetto ProtectID

Resiltech s.r.l, Piazza Nilde Iotti 25, Pontedera (PI), Italia

Partecipazione al progetto ProtectID applicando tecniche note di anomaly detection a supporto di tecniche di autenticazione continua, con un duplice scopo: i) ricavare una proprietà di "spoofing detectability" di diversi tratti biometrici tramite analisi quantitativa di risultati di algoritmi applicati a dataset pubblici, e ii) proponendo un supporto run-time a processi di autenticazione basato sulla rilevazione delle anomalie nei dati rilevati e trasmessi dai sensori biometrici.

Nov 2017 – Giu 2019

Assegnista Post-Doc (INF/01)

Dipartimento di Matematica ed Informatica "Ulisse Dini",

Viale Morgagni 65 – 67/A, Firenze (FI), Italia

Approfondimento di tematiche relative al design, la verifica e la validazione di sistemi critici – in termini di safety ed in termini di security -, con particolare attenzione al rilevamento di errori basato sul concetto di anomalie comportamentali. Ricerca nell'ambito della programmazione in ambiente safety-critical, con riferimento particolare agli standards applicabili per il settore ferroviario, acquisendo conoscenza relativa ai procedimenti da applicare e alle componenti principali coinvolte nel processo di certificazione di software. Durante il periodo di Post-Doc ha completato lo sviluppo di tools per il monitoraggio e l'analisi di dati che erano stati utilizzati per la tesi di dottorato, rendendoli più facilmente fruibili anche da terze parti. Alcuni di

questi tool, ad esempio, sono stati usati come supporto didattico per un corso magistrale LM-18 di cui Zoppi è stato docente a contratto. Ha svolto regolarmente attività per progetti nazionali ed europei ai quali ha partecipato il suo gruppo di ricerca.

Gen 2014 – Mar 2015

Collaboratore CoCoCo per il progetto “Regione Toscana” Secure!

Dipartimento di Matematica ed Informatica “Ulisse Dini”,

Viale Morgagni 65 – 67/A, Firenze (FI), Italia

Collaboratore del gruppo di ricerca RCL nell’ambito del progetto Secure!, bandito dalla “Regione Toscana”. Sviluppo di uno strumento per l’iniezione sistematica di guasti software (software bugs) secondo una nota classificazione di frequenza nota in letteratura come Orthogonal Defect Classification (ODC). Il tool sviluppato consente di modificare un qualunque codice sorgente Java inserendo linee di codice che consentono l’attivazione di tali guasti in base a politiche di attivazione ben definite. Lo strumento è stato inoltre applicato per una campagna di esperimenti su un prototipo del Sistema Secure!, un Crisis Management System strutturato con una architettura orientata ai servizi (SOA). Il sistema è stato instrumentato allo scopo di rilevare dati di performance, che sono stati analizzati poi in termini di anomalie usando un algoritmo disponibile in letteratura.

Giu 2008

Programmatore Junior

Vivido s.r.l, Via Dei Colatori 10, 50019 Sesto Fiorentino (FI), Italia
SQL Stored Procedures, .NET Programming (ASP.NET). Sviluppo di una sezione di un sito web per e-Commerce. Stage estivo di 1 mese.

CONSCENZA DELLE LINGUE

Madrelingua: Italiano

Altre lingue

	COMPRENSIONE		PARLATO		PRODUZIONE SCRITTA
	Ascolto	Lettura	Interazione	Produzione Orale	
Inglese	C1	C1	C1	C1	C1

Certificato B1 fornito da Comitato linguistico di Ateneo (C.L.A.) – Università di Firenze (Italia), 2010
Livello Europeo: B1

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

Esperienze all’Estero

European Union program DEVASSES (Design and Validation of Large Scale Software Systems)
Language: English, Duration of studies in months: 1, Dates Oct-Nov 2016
Foreign country where the academic studies were carried out: Maceiò, Alagoas, Brazil

European Union program DEVASSES (Design and Validation of Large Scale Software Systems)
Language: English, Duration of studies in months: 3 , Dates May-Jul 2015
Foreign country where the academic studies were carried out: Campinas / Maceio, Brazil

Corsi di Lingua Frequentati

B2/C1 'Presentation' English Course erogato da Centro Linguistico di Ateneo (CLA – UNIFI), Apr - Mag 2016

B2.X Praxis English Course erogato da Centro Linguistico di Ateneo (CLA – UNIFI) Feb - Apr 2015

B1.Y Praxis English Course erogato da Centro Linguistico di Ateneo (CLA – UNIFI), Gen - Mar 2015

ALTRE INFORMAZIONI

Competenze Digitali

Competenze informatiche di base: Operating systems (Good), Programming languages (Excellent), Word processing (Fair), Electronic spreadsheet (Good), Data base administrators (Good), Internet skills (Excellent), Data transmission networks (Fair), Web-site creation (Limited), Multimedia (Limited), Programming languages known: (C++, C#, Java, Python, Matlab)

Corso Sicurezza

Completato il corso per la sicurezza: modulo base (Agosto 2021) chiamato “Formazione generale per i lavoratori in materia di sicurezza e salute sul lavoro“ e modulo di approfondimento (Settembre 2021) chiamato “Formazione specifica per lavoratori in materia di salute e sicurezza sui luoghi di lavoro”

Informazioni Personali

Dal 2007 al 2018 ha svolto attività di volontariato presso la parrocchia del proprio quartiere, sia come animatore di gruppi giovanili (età 11-17 anni) sia come aiuto-cuoco per eventi di quartiere. Dotato di automobile propria e di passaporto italiano in corso di validità.

Patente di Guida

B

Pubblicazioni scientifiche

PUBBLICAZIONI

Riviste Internazionali

Elsevier COSE [J15] 01/2023: Which Algorithm can Detect Unknown Attacks? Comparison of Supervised, Unsupervised and Meta-Learning Algorithms for Intrusion Detection
Zoppi, T., Ceccarelli, A., Puccetti, T., & Bondavalli, A. (2023). Which Algorithm can Detect Unknown Attacks? Comparison of Supervised, Unsupervised and Meta-Learning Algorithms for Intrusion Detection. Computers & Security, 103107.
DOI: 10.1016/j.cose.2023.103107

IEEE Access [J14] 01/2023: Tolerate Failures of the Visual Camera with Robust Image Classifiers
Atif, M., Ceccarelli, A., Zoppi, T., & Bondavalli, A. (2023). Tolerate Failures of the Visual Camera with Robust Image Classifiers. IEEE Access.
DOI: 10.1109/ACCESS.2023.3237394

IEEE OJITS [J13] 10/2022: Robust Traffic Sign Recognition Against Camera Failures
Atif, M., Ceccarelli, A., Zoppi, T., Gharib, M., & Bondavalli, A. (2022). Robust Traffic Sign Recognition Against Camera Failures. IEEE Open Journal of Intelligent Transportation Systems, 3, 709-722.
DOI: 10.1109/OJITS.2022.3213183

IEEE TETC [J12] 03/2022: On the Properness of Incorporating Binary Classification Machine Learning Algorithms into Safety-Critical Systems
Gharib, M., Zoppi, T., & Bondavalli, A. (2022). On the Properness of Incorporating Binary Classification Machine Learning Algorithms into Safety-Critical Systems. IEEE Transactions on Emerging Topics in Computing.
DOI: 10.1109/TETC.2022.3178631

MDPI Sensors [J11] 03/2022: Towards Enhancing Traffic Sign Recognition through Sliding Windows
Atif, M., Zoppi, T., Gharib, M., & Bondavalli, A. (2022). Towards enhancing traffic sign recognition through sliding windows. Sensors, 22(7), 2683.
DOI: 10.3390/s22072683

IEEE Access [J10] 11/2021: Detect Adversarial Attacks Against Deep Neural Networks With GPU Monitoring
Zoppi, T., & Ceccarelli, A. (2021). Detect Adversarial Attacks Against Deep Neural Networks With GPU Monitoring. IEEE Access, 9, 150579-150591.
DOI: 10.1109/ACCESS.2021.3125920

IEEE Access [J9] 06/2021: Unsupervised algorithms to detect zero-day attacks: Strategy and application
Zoppi, T., Ceccarelli, A., & Bondavalli, A. (2021). Unsupervised algorithms to detect zero-day attacks: Strategy and application. IEEE Access, 9, 90603-90615.
DOI 10.1109/ACCESS.2021.3090957

ACM TCPS [J8] 06/2021 Meta-Learning to Improve Unsupervised Intrusion Detection in Cyber-Physical Systems
Zoppi, T., Gharib, M., Atif, M., & Bondavalli, A. (2021). Meta-Learning to Improve Unsupervised Intrusion Detection in Cyber-Physical Systems. ACM Transactions on Cyber-Physical Systems (TCPS), 5(4), 1-27.
DOI: 10.1145/3467470

Elsevier JNCA [J7] 04/2021: Prepare for trouble and make it double! Supervised–Unsupervised stacking for anomaly-based intrusion detection
Zoppi, T., & Ceccarelli, A. (2021). Prepare for trouble and make it double! Supervised–Unsupervised stacking for anomaly-based intrusion detection. Journal of Network and Computer Applications, 189, 103106.
DOI: 10.1016/j.jnca./2021.103106

IEEE TDSC [J6] 03/2021 MADneSs: a Multi-layer Anomaly Detection Framework for Complex Dynamic Systems.
Zoppi, T., Ceccarelli, A., Bondavalli, A. (2019). MADneSs: a Multi-layer Anomaly Detection Framework for Complex Dynamic Systems. IEEE Transactions on Dependable and Secure Computing 18(2), 796-809.
DOI: 10.1109/TDSC.2019.2908366.

ACM TDS [J5] 03/2021 Unsupervised Anomaly Detectors to Detect Intrusions in the Current Threat Landscape
Zoppi, T., Capecchi, T., & Bondavalli, A. (2020). Unsupervised Anomaly Detectors to Detect Intrusions in the Current Threat Landscape. ACM Transactions on Data Science 2(2), 1-26.
DOI: 10.1145/3441140

Springer JBCS [J4] 01/2021 Development and validation of a safe communication protocol compliant to railway standards
Bertieri, D., Ceccarelli, A., Zoppi, T., Mungiello, I., Barbareschi, M., & Bondavalli, A. (2021). Development and validation of a safe communication protocol compliant to railway standards. Journal of the Brazilian Computer Society, 27(1), 1-26.
DOI: 10.1186/s13173-021-00106-w

Elsevier JISA [J3] 02/2020 On the educated selection of unsupervised algorithms via attacks and anomaly classes
Zoppi, T., Ceccarelli, A., Salani, L., & Bondavalli, A. (2020). On the educated selection of unsupervised algorithms via attacks and anomaly classes. Journal of Information Security and Applications, 52, 102474.
DOI 10.1016/j.jisa.2020.102474

ACM TCPS [J2] 03/2019 Threat Analysis in Systems-of-Systems: An Emergence-Oriented Approach.
Ceccarelli, A., Zoppi, T., Vasenev, A., Mori, M., Ionita, D., Montoya, L., & Bondavalli, A. (2018). Threat analysis in systems-of-systems: an emergence-oriented approach. ACM Transactions on Cyber-Physical Systems, 3(2), 1-24.

DOI: 10.1145/3234513.

Wiley JSEP [J1] 01/2018 Labelling relevant events to support the crisis management operator.
Zoppi, T., Ceccarelli, A., Lo Piccolo, F., Lollini, P., Giunta, G., Morreale, V., & Bondavalli, A. (2018). Labelling relevant events to support the crisis management operator. Journal of Software: Evolution and Process, 30(3), e1874. John Wiley and Sons, Ltd, UK.
DOI:10.1002/smr.1874

Tesi di Dottorato 3/2018 Towards Effective Anomaly Detection in Complex Dynamic Systems.
Tommaso Zoppi, PhD Thesis, Advisors: Andrea Bondavalli, Andrea Ceccarelli.

Conferenze Internazionali

3/2023 SAC [C18] Detection of Adversarial Attacks by Observing Deep Features with Structured Data Algorithms
Puccetti, T., Ceccarelli, A., Zoppi, T., & Bondavalli, A. (2023, March). Detection of Adversarial Attacks by Observing Deep Features with Structured Data Algorithms. In Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing (pp. 125-134).

12/2021 PRDC [C17] Detecting Intrusions by Voting Diverse Machine Learners: Is It Really Worth?
Zoppi, T., Ceccarelli, A., & Bondavalli, A. (2021, December). Detecting Intrusions by Voting Diverse Machine Learners: Is It Really Worth?. In 2021 IEEE 26th Pacific Rim International Symposium on Dependable Computing (PRDC) (pp. 57-66). IEEE.
DOI: 10.1109/PRDC53464.2021.00017

11/2021 LADC [C16] Feature Rankers to Predict Classification Performance of Unsupervised Intrusion Detectors
Zoppi, T., Ceccarelli, A., & Bondavalli, A. (2021, November). Feature Rankers to Predict Classification Performance of Unsupervised Intrusion Detectors. In 2021 10th Latin-American Symposium on Dependable Computing (LADC) (pp. 1-9). IEEE.
DOI: 10.1109/LADC53747.2021.9672586

04/2021 SAC [C15] Understanding the properness of incorporating machine learning algorithms in safety-critical systems
Gharib, M., Zoppi, T., & Bondavalli, A. (2021, March). Understanding the properness of incorporating machine learning algorithms in safety-critical systems. In Proceedings of the 36th Annual ACM Symposium on Applied Computing (pp. 232-234).
DOI: 10.1145/3412841.3442074

04/2021 SAC [C14] Quantitative comparison of supervised algorithms and feature sets for traffic sign recognition
Atif, M., Zoppi, T., Gharib, M., & Bondavalli, A. (2021, March). Quantitative comparison of supervised algorithms and feature sets for traffic sign recognition. In Proceedings of the 36th Annual ACM Symposium on Applied Computing (pp. 174-177).
DOI: 10.1145/3412841.3442072

6/2020 DSN [C13] Into the Unknown: Unsupervised Machine Learning Algorithms for Anomaly-Based Intrusion Detection
Zoppi, T., Ceccarelli, A., & Bondavalli, A. (2020, June). Into the Unknown: Unsupervised Machine Learning Algorithms for Anomaly-Based Intrusion Detection. In 2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S) (pp. 81-81). IEEE. DOI 10.1109/DSN-S50200.2020.00044

11/2019 LADC [C12] Implementation, Verification and Validation of a Safe and Secure Communication Protocol for the Railway Domain (Practical Experience Report)
Bertieri, D., Zoppi, T., Mungiello, I., Ceccarelli, A., Barbareschi, M., & Bondavalli, A. (2019, November). Practical Experience Report: Implementation, Verification and Validation of a Safe and Secure Communication Protocol for the Railway Domain. In 2019 9th Latin-American Symposium on Dependable Computing (LADC) (pp. 1-6). IEEE.
DOI: 10.1109/LADC48089.2019.8995727

10/2019 ISSRE [C11] Evaluation of Anomaly Detection algorithms made easy with RELOAD (Tool Paper)
Zoppi, T., Ceccarelli, A., & Bondavalli, A. (2019, October). Evaluation of Anomaly Detection algorithms made easy with RELOAD. In 2019 IEEE 30th International Symposium on Software Reliability Engineering (ISSRE) (pp. 446-455). IEEE.
DOI: 10.1109/ISSRE.2019.00051

04/2019 SAC [C10] Quantitative Comparison of Unsupervised Anomaly Detection Algorithms for Intrusion Detection
Falcão, F., Zoppi, T., Silva, C. B. V., Santos, A., Fonseca, B., Ceccarelli, A., & Bondavalli, A. (2019, April). Quantitative comparison of unsupervised anomaly detection algorithms for intrusion detection. In Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing (pp. 318-327).
DOI 10.1145/3297280.3297314

12/2018 PRDC [C9] On Algorithms Selection for Unsupervised Anomaly Detection
Tommaso Zoppi, Andrea Ceccarelli, Andrea Bondavalli, In Proceedings of the Pacific Rim Dependable Computing Conference (PRDC 2018, pp. 279-288) Taipei, Taiwan. IEEE Computer Society, USA.
DOI 10.1109/PRDC.2018.00050.

4/2017 SAC [C8] Exploring Anomaly Detection in Systems of Systems
Tommaso Zoppi, Andrea Ceccarelli, Andrea Bondavalli, In Proceedings of the Symposium on Applied Computing (SAC '17), Marrakech, Morocco, 3-7 April 2017, pp. 1139-1146, ACM, New York, NY, USA.

DOI 10.1145/3019612.3019765

3/2017 SmartGIFT [C7] A modeling framework to support resilient evolution planning of smart grids.
Zoppi, T., Bessler, S., Ceccarelli, A., Lambert, E., Lau, E. T., & Vasenev, A. (2017). Smart Grid Inspired Future Technologies (SmartGIFT 2017) Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), vol 203, (pp. 233-242). Springer, Cham (Switzerland).
DOI 10.1007/978-3-319-61813-5_23.

3/2017 SmartGIFT [C6] A tool for evolutionary threat analysis of smart grids.
Zoppi, T., Ceccarelli A., Mori M. (2017). Smart Grid Inspired Future Technologies (SmartGIFT 2017) Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST), vol 203, (pp. 205-211). Springer, Cham (Switzerland)
DOI 10.1007/978-3-319-61813-5_20.

9/2016 SAFECOMP [C5] Context-Awareness to improve Anomaly Detection in Dynamic Service Oriented Architectures Tommaso Zoppi, Andrea Ceccarelli, Andrea Bondavalli, in Proceedings of Computer Safety, Reliability and Security (SAFECOMP 2016, pp. 145-158), Trondheim, Norway. Springer International Publishing, Switzerland.
DOI 10.1007/978-3-319-45477-1_12.

4/2016 EnergyCON [C4] Towards a collaborative framework to improve urban grid resilience.
Jung, O., Bessler, S., Ceccarelli, A., Zoppi, T., Vasenev, A., Montoya, L., … Chappell, K. (2016). In proceedings at the 2016 IEEE International Energy Conference, ENERGYCON 2016 (pp 1-6). IEEE, USA
DOI:10.1109/ENERGYCON.2016.7513887.

6/2016 SOSE [C3] On the impact of emergent properties on SoS security.
Mori, M., Ceccarelli, A., Zoppi, T., & Bondavalli, A. (2016). In proceedings at the 2016 11th Systems of Systems Engineering Conference, SoSE 2016 (pp 1-6),
DOI:10.1109/SYSOSE.2016.7542895

1/2016 HASE [C2] Presenting the proper data to the crisis management operator: A relevance labelling strategy. Zoppi, T., Ceccarelli, A., Lollini, P., Bondavalli, A., Lo Piccolo, F., Giunta, G., & Morreale, V. (2016). In Proceedings at the IEEE International Symposium on High Assurance Systems Engineering, 2016-March (pp 228-235). IEEE Computer Society, USA
DOI:10.1109/HASE.2016.31

9/2015 SAFECOMP [C1] A Multi-Layer Anomaly Detector for Dynamic Service-Based Systems
Andrea Ceccarelli, Tommaso Zoppi, Massimiliano Itria, Andrea Bondavalli, in Proceedings of Computer Safety, Reliability and Security (SAFECOMP 2015, pp. 166-180), Delft, Holland. Springer International Publishing, Switzerland
DOI 10.1007/978-3-319-24255-2_13.

Workshops

09/2022 MLCS [W6] Towards a General Model for Intrusion Detection: An Exploratory Study
Zoppi, T., Ceccarelli, A., & Bondavalli, A. (2023, January). Towards a General Model for Intrusion Detection: An Exploratory Study. In Machine Learning and Principles and Practice of Knowledge Discovery in Databases: International Workshops of ECML PKDD 2022, Grenoble, France, September 19–23, 2022, Proceedings, Part II (pp. 186-201). Cham: Springer Nature Switzerland.

04/2021 ItaSEC [W5] Spoofing detectability as a property of biometric characteristics
Zoppi, T., Schiavone, E., Bicchierai, I., Brancati, F., & Bondavalli, A. (2021). Spoofing detectability as a property of biometric characteristics. CEUR Workshop Proceedings, 2940 92-105.

07/2019 CSR [W4] An Initial Investigation of Sliding Windows for Anomaly-Based Intrusion Detection
Tommaso Zoppi, Andrea Ceccarelli, Andrea Bondavalli,
CSR Workshop of CyberSecurity and Resilience in Internet of Things, IEEE Services, Milan (Italy).
DOI 10.1109/SERVICES.2019.00031.

2/2017 REFSQ [W3] Towards security requirements: Iconicity as a feature of an informal modeling language. Vasenev, A., Ionita, D., Zoppi, T., Ceccarelli, A., & Wieringa, R. (2017). Joint Proceedings of
REFSQ-2017 Workshops, Doctoral Symposium, Research Method Track, and Poster Track;
Essen; Germany; 27 February 2017, CEUR Workshop Proceedings, vol. 1796, 15 pages. CEUR-WS, Aachen.

9/2016 SRDS Student Forum [W2] Challenging Anomaly Detection in Complex Dynamic Systems
Tommaso Zoppi, Andrea Ceccarelli, Andrea Bondavalli, in Proceedings of Symposium on Reliable Distributed Systems (SRDS 2016 - Student Forum Session pp 213-214), Budapest, Hungary. IEEE Computer Society, USA.
DOI 10.1109/SRDS.2016.036

6/2014 SORT [W1] A Testbed for Evaluating Anomaly Detection Monitors Through Fault Injection
A. Ceccarelli, T. Zoppi, A. Bondavalli, F. Duchi and G. Vella, in Proceedings of the 5th IEEE Workshop on self-organizing real-time systems (SORT 2014, pp. 358-365), Reno, Nevada, USA. IEEE Computer Society, USA.
DOI 10.1109/ISORC.2014.31.

Contributi a Conferenze senza Proceedings

On the Efficacy of Metrics to Describe Adversarial Attacks
AAAI Workshop of Artificial Intelligence for Cyber Security (AICS)

2/2023 AICS-AAAI23 Disponibile su arxiv -> Puccetti, T., Zoppi, T., & Ceccarelli, A. (2023). On the Efficacy of Metrics to Describe Adversarial Attacks. arXiv preprint arXiv:2301.13028.

8/2022 ECMP 2022
MACARON: data collection and Machine leArning to improve radiomiCs And support Radiation Oncology
Autori: Tommaso Zoppi, Silvia Calusi, Stefania Pallotta
Lavoro presentato alla DIY-Fair session della conferenza ECMP di fisica medica. E' stato presentato il sistema MACARON in oggetto al progetto omonimo, con presentazione interattiva e panel.

6/2022 WCRR 2022
A SIL4 Interface to Remotely Handle Track Possession
Autori: Alberto Cirillo, Lorenzo Esposito, Innocenzo Mungiello, Sergio Repetto, Andrea Bondavalli, Tommaso Zoppi
Lavoro presentato al World Congress on Railways, la conferenza di punta nel mondo industriale ferroviario, da personale RFI

Capitoli di Libri
10/2017 CECRIS Experience [BC1]
STECA – Security Threats, Effects and Criticality Analysis: Definition and Application to Smart Grids.
Mario Rui Baptista, Nuno Silva, Nicola Nostro, Tommaso Zoppi and Andrea Ceccarelli. In Certifications of Critical Systems - The CECRIS Experience (pp.167-182). River Publishers, Denmark.
DOI:10.13052/rp-9788793519558. - ISBN:9788793519565

Didattica, didattica integrativa e servizio agli studenti

ATTIVITA' DIDATTICA A LIVELLO UNIVERSITARIO

Set 2019 – OGGI

Docente del corso di "Architetture degli Elaboratori". Responsabile di 3 CFU (su un totale di 12 CFU) per il corso al primo anno del CDS in Informatica SMFN, riguardanti: linguaggi di basso livello (assembly), programmazione di basso livello, dettagli dell'assembly RISC-V ed esempi di programmazione con tale linguaggio. AA 19-20, 20-21, 21-22. Nell'AA 22-23 ha un carico di 7/12 CFU (percentuale maggioritaria rispetto alla totalità del corso), responsabile di un programma che include la parte di laboratorio assembly e tutta l'architettura del processore RISCV a ciclo singolo, pipeline e memoria virtuale.

Mag 2022

Corso di Dottorato "Unsupervised Anomaly-Based Intrusion Detection". Responsabile di 9/18 ore (metà corso) che hanno incluso sia argomenti teorici sia la loro applicazione pratica.

Set 2021 – Feb 2023

Docente del corso di "Data Collection and Machine Learning for Cyber-Physical Systems". Titolare del corso erogato in lingua inglese alla Magistrale in Informatica SMFN, responsabile di 4 CFU (su un totale di 6 CFU), riguardanti: basi di metrologia, monitoraggio di sistemi, fault injection e robustness testing, analisi dati, classificazione basata su intelligenza artificiale (anomaly detection), algoritmi supervisionati, non supervisionati e meta-learning. AA21-22, riattivato per l'AA23-24.

Set 2018 – Feb 2022

Docente del corso di "Quantitative Analysis of Systems". Responsabile di 3 CFU (su un totale di 9 CFU) erogato in lingua inglese alla Magistrale in Informatica SMFN, riguardanti: fondamenti di teoria delle misure, monitoraggio, testing, fault injection, robustness testing, pianificazione di campagne di esperimenti, cenni di analisi di dati, tools di monitoraggio e/o intrusion detection e/o analisi dati, con attenzione particolare al rilevamento di errori. A.A. 18-19, 19-20, 20-21 (corso non attivato per l'AA 21-22)

Nov 2014 – Ago 2019

Supporto didattico nella preparazione di esercizi, organizzazione di esami scritti e per la preparazione / revisione di materiale didattico (es. dispense, slides) per il corso di Architetture degli Elaboratori (I anno della laurea triennale in Informatica L-31, Facoltà di SMFN, Università di Firenze)
AA 14-15, 15-16, 16-17, 17-18 e 18-19.

Gen 2015 – Ott 2017

Tutor per il cdl in Informatica L-31 (Bando di concorso per la formazione di graduatorie relative al reclutamento di tutor per la realizzazione di attivita' di tutorato nei corsi di laurea triennali e nei primi anni dei corsi di laurea magistrali a ciclo unico ai fini della riduzione della dispersione studentesca a.a. 2014/2015 e 2015/2016). In aggiunta al supporto studenti per la revisione di esercizi e/o argomenti di esame, le attività principali svolte nei 30 mesi di tutoraggio si sono articolate in

- Partecipazione ad to Open Days per presentare il corso di informatica a studenti delle scuole superiori (Gennaio 2015-16-17);
- Supporto didattico (laboratorio) per il corso di Basi di Dati (II anno della laurea triennale L-31);
- Supporto didattico (laboratorio) per il corso di Programmazione (I anno della laurea triennale L-31);
- Supporto a professori durante gli esami scritti.

Didattica presso Università Estere Ott 2021 – Dic 2021

Docente del corso " Quantitative and Experimental Analysis of Systems". Docente per un corso di 30 ore erogato in lingua inglese ed in modalità remota presso l'Universidade estadual do Campinas (Campinas – BR) a titolo gratuito. Il corso, orientato a studenti di Maestrado (equivalente della magistrale italiana) ha approfondito tematiche di basi di metrologia, monitoraggio di sistemi, fault injection e robustness testing, analisi dati, classificazione basata su intelligenza artificiale (anomaly detection).

Supporto alle Attività del Corso di Laurea in Informatica Gennaio 2020 – IN CORSO

Organizzazione Calendario appelli del CDL Triennale L-31 e Magistrale LM-18 in Informatica SMFN all'Università di Firenze. Interazione con i docenti, il presidente del corso di laurea ed i rappresentanti degli studenti per l'organizzazione del calendario esami e prove intermedie (ove previste) allo scopo di garantire una distribuzione bilanciata degli esami rispetto agli appelli in calendario. Negli anni 2020 e 2021 l'attività implicava anche l'interazione con la scuola per la prenotazione aule e l'inserimento degli esami nei sistemi informativi; dal 2022 questa attività viene svolta dal docente responsabile di ciascun corso.

Studenti di Dottorato Co-Supervisionati

Tommaso Puccetti (XXXVIII ciclo del dottorato in Informatica, Matematica, Statistica – Curriculum Informatica) per il periodo Nov 2022 – Ott 2025. Co-Supervisore assieme ad Andrea Ceccarelli

Tesi Magistrali Supervisionate

Tommaso Puccetti (4/2021): Sviluppo, Verifica e Validazione di un Protocollo Ferroviario per la Trasmissione Dati in Sicurezza

Tesi Magistrali Co-Supervisionate

Lorenzo Salani (10/2021): Analisi e valutazione di un framework GAN nella generazione di datasets di attacchi
Lorenzo Sarti (10/2021): Sviluppo di software SIL0 per sistemi di manutenzione nel dominio ferroviario
Giulia Dallai (7/2019): Analisi di Azzardi per un Sistema di Interfaccia Mobile Remota per la Manutenzione delle Linee Ferroviarie
Lavinia Masini (4/2019): Analisi quantitativa di architetture safety critical per un sistema di controllo

ferroviario
Duccio Bertieri (10/2018): Sviluppo Di Un Protocollo Di Comunicazione Sicuro In Ambiente Ferroviario

Tesi Triennali Supervisionate

Cosimo Giraldi (07/2023): Benchmark di Librerie XAI per Dati Tabulari
Luigi Cennini (4/2023): Valutazione di un Safety Wrapper per Machine Learners nel contesto della classificazione di immagini
Stefano Gazzini (04/2023): Trasformare dati tabulari in immagini per migliorare la classificazione: DNNs superano i MLs?
Leonardo Baragli (04/2023): Applicazione e valutazione di tecniche di domain adaptation per intrusion detection systems
Matteo Gonfiantini (04/2023): Machine learning per la classificazione di documenti economici
Daniele Bettazzi (12/2022): L'elaborazione del linguaggio naturale applicato alle cartelle cliniche italiane
Leonardo Bargiotti (2/2022): Come Posso Fidarmi Di Un Machine Learner?
Jacopo Vezzosi (12/2021): Analisi preliminare della difficoltà di un problema di classificazione binaria tramite Feature Rankers
Marco Pellegrino (10/2021): Soluzioni basate su Reti Neurali Artificiali per l'analisi di Dati Tabulari
Alessandro Montaghi (6/2020): Meta-Learning per la combinazione di intrusion detectors
Tommaso Capecchi (4/2020):Confronto di Algoritmi Unsupervised per Anomaly-based Intrusion Detection
Antonio Caia (2/2020): Anomaly Detection In Smart Grid: Confronto Di Algoritmi Unsupervised Per L'analisi Dei Consumi
Dario Taddei (2/2020): Anomaly Detection in Sistemi Safety-Critical: Analisi e Discussione dell'Adeguatezza della Matrice di Confusione
Manuel Rettani (12/2019) Anomaly detection per la Rilevazione di Attacchi ai Sensori Biometrici

Tesi Triennali Co-Supervisionate

Mattia d'Autilia (7/2019) Pianificazione Ed Esecuzione di Test Software Unitari Secondo le Normative Ferroviarie
Arturo Bianchi (2/2019): Protocollo Vitale Standard: Descrizione e Sviluppo di un Protocollo di Comunicazione Sicuro in Ambiente Ferroviario.
Andrea Chimenti (2/2019): Studio e Sviluppo di Algorithmi a Finestra Scorrevole per Anomaly Detection
Filippo Faldetta (2/2019): Una Metodologia e la sua Validazione per Rilevare Attacchi tramite Combinazioni di Anomaly Detectors
Lorenzo Salani (2/2019): Collegamento tra Attacchi ed Anomalie: Analisi delle Anomalie Riportate nei Datasets di Intrusion Detection

Titoli

Titolo di dottore di ricerca o equipollenti, ovvero, per i settori interessati, il diploma di specializzazione medica o equivalente, conseguito in Italia o all'Estero

PERCORSO DI STUDI

Nov 2014 – Nov 2017 — **Dottorato in Informatica** (EQF level 8)

Tesi discussa Mar 2018

Ciclo XXX - PhD program in Matematica, Informatica, Statistica (Firenze - Perugia – IndAM)

Curriculum: Informatica (Computer Science)

I principali temi affrontati durante la tesi hanno riguardato la costruzione e la validazione di sistemi critici, in particolare: monitoraggio, fault injection, rilevazione degli errori anomaly-based, risk analyses. Durante i tre anni, ha partecipato a converenze ed eventi internazionali, oltre a lavorare in un gruppo di ricerca attivo anche in termini di progetti nazionali/europei. Questo ha garantito la possibilità di lavorare e di discutere di temi comuni con ricercatori e/o studenti provenienti da università straniere, oltre alla collaborazione con alcune aziende nei progetti sopracitati. Nel contesto di questi progetti, Zoppi è stato visiting PhD student in Brasile per un totale di 4 mesi.

Tesi: Towards Effective Anomaly Detection in Complex Dynamic Systems
(Supervisori: Andrea Bondavalli, Andrea Ceccarelli). Tesi discussa il 5 Marzo 2018.

Ott 2012 – Lug 2014 — **Laurea Magistrale in Informatica** (EQF level 7)

Laurea Magistrale in Informatica, INF/01 Classe LM-18.

- Voto 110 Lode / 110
- Tesi: Metodologia, Ambiente di Test e Analisi Dati per l'Identificazione di Indicatori Middleware e di Sistema finalizzati alla Rilevazione di Anomalie (Supervisore: Andrea Bondavalli).
- Tesi discussa il 14 Luglio 2014.

Ott 2009 – Ott 2012 — **Laurea Triennale in informatica** (EQF level 6)

Laurea Triennale in informatica, INF/01 Classe L-31.

- Voto 110 Lode / 110
- Tesi: Sviluppo di Applicazioni Android orientate all'Adattività (Supervisore: Michele Loreti).
- Tesi discussa il 15 Ottobre 2012.

Studi Pre-Universitari

Diploma di Scuola Superiore: ITIS Meucci (Perito Industriale Capotecnico)
Esame di Maturità tenutosi nell'anno: 2009, Valutazione 100/100

Documentata attività di formazione o di ricerca presso qualificati istituti italiani o stranieri

ATTIVITA' DI FORMAZIONE AGGIUNTIVA

Visiting Researcher

10-11/2016 Universidade Federal do Alagoas, Maceiò, Alagoas – Brazil.
Visiting researcher per il progetto della Comunità Europea DEVASSES (Design and Validation of Large Scale Software Systems). Pianificazione di lavori finalizzati all'anomaly detection con studenti e ricercatori locali. Questo ha permesso di ampliare il lavoro di tesi e di iniziare a scrivere articoli, che sono stati poi accettati qualche anno dopo.

05-07/2015 Universidade Estadual do Campinas (UNICAMP), Campinas, Sao Paulo, Brazil, e Universidade Federal do Alagoas, Maceiò, Alagoas – Brazil.
Visiting researcher per il progetto della Comunità Europea DEVASSES (Design and Validation of Large Scale Software Systems). Prima esperienza come visiting student finalizzata allo scambio di idee e di conoscenze con ricercatori e studenti locali.

Scuole di Dottorato

17-21/01/2016 SecureCI Winter School.
Questa scuola di dottorato si propone l'obiettivo di approfondire tematiche legate alla cyber-sicurezza per quanto riguarda le infrastrutture critiche. Alla scuola hanno partecipato esperti provenienti sia da università italiane che estere.

Corsi Seguiti

03/2016 Aspects of Distributed and Real-Time Computing, prof. Edgar Nett
Temi del corso: What is real-time computing about, presentation of the principal issues, and reflection of its main contributions in the context of embedded systems. Notions and reasoning about temporal specifications, predictability, time and clocks, sketching the main principles and issues of clock synchronization, scheduling policies, scheduling algorithms, and real-time tasks. Discussion of Worst Case Execution Times (WCETs)

Realizzazione di attività progettuale relativamente ai settori concorsuali nei quali è prevista

PARTECIPAZIONE A PROGETTI DI RICERCA

Progetti Nazionali

RFI-URV-SIPAC

(Convenzione conto terzi) Rete Ferroviaria Italiana - Analisi, Valutazione e Supporto alle attività V&V per i sistemi safety-critical URV e SIPAC" nell'ambito di Accordo Quadro "Sistemi Embedded per applicazioni ferroviarie" (Giu 2022 – OGGI).
Finanziamento progetto: circa 550 000 euro
Ruolo del Candidato: partecipazione tecnica, coordinamento attività (gestione scadenze di deliverables, timesheets, interazioni con personale amministrativo)
Il progetto esplora le architetture sicure per i sistemi ferroviari SIL4 e vede una cooperazione tra il gruppo RCL e il dipartimento R&D di RFI - Rete Ferroviaria Italiana allo scopo di ideare architetture e meccanismi per i sistemi SIL4, insieme a prototipi di sottosistemi specifici. Alcuni dei principali obiettivi del progetto sono descritti di seguito.
- Definizione di architetture, hazard analyses, ed implementazione componenti per il sistema di manutenzione SIPAC di RFI.
- Progettazione a norma CENELEC del sistema URV di RFI, ovvero un rotabile teleguidato che mira a scansionare le linee ferroviarie allo scopo di controllarne la perfetta efficienza e stato di salute prima del passaggio di treni.

PNRR

PNRR – CN1 Spoke 6 High Performance Computing (Set 2022- OGGI)
Finanziamento progetto: circa 55 000 euro
Ruolo del Candidato: co-assegnatario dei fondi per borse-assegni da bandire
Responsabilità scientifica nell'ambito dello Spoke 6 del PNRR CN1-HPC Centro Nazionale 1 - High Performance Computing, Big Data e Quantum Computing. Nell'ambito del PNRR CN1, Spoke 6, sono attualmente responsabile assieme ad Andrea Ceccarelli per 2 assegni (da bandire ed eventualmente rimodulare in altre posizioni contrattuali) per un totale di 55 500 Euro.

MACARON

Bandi Competitivi RTD – UNIFI. MACARON: data collection and Machine leArning to improve radiomiCs And support Radiation ONcology (Gen 2022 – OGGI)
Finanziamento progetto: circa 60 000 euro
Ruolo del Candidato: **Coordinatore, assegnatario dei fondi e responsabile di un assegnista di ricerca (da Feb 2023 – Feb 2024) per tale progetto.**
Il progetto biennale punta ad analzzare i dati delle cartelle cliniche e di imaging (TC) che vengono raccolti ai controlli periodici dei pazienti in radioterapia allo scopo di predire l'andamento della malattia e suggerire quindi un percorso di cure più adeguato e personalizzato sulla situazione specifica del paziente. Il progetto vede la collaborazione delle unità operative INF/01 (Informatica) e FIS/07 (Fisica Medica) con intervento occasionale di personale medico di Radioterapia alla AUO Careggi, che beneficieranno direttamente dei risultati di tale progetto.

SPaCe

POR-FESR 14-20 SPaCe - Smart Passenger Center Regione Toscana (Ott 2020 - OGGI).
Finanziamento Progetto (quota UNIFI): 280 000 euro
Ruolo del Candidato: partecipazione tecnica
L'obiettivo del progetto SPaCe è la realizzazione di: un sistema basato sull'intelligenza artificiale (AI) per la valutazione dello stato interno di veicoli su gomma e su rotaia con passeggeri a bordo, un sistema di supervisione e di controllo della flotta veicoli in tempo reale, dedicato all'ottimizzazione del numero medio di passeggeri per veicolo ed un dispositivo di bordo per interconnettere nodi e sensori all'interno della LAN del veicolo (utilizzando infrastrutture cablate e/o wireless) e di offrire servizi di base per il funzionamento della rete stessa. Definizione di meccanismi di rilevazione delle intrusioni a protezione dei canali di trasmissione tra le componenti del sistema SPaCe.

RFI-SuperoQuinto

(Convenzione conto terzi) Rete Ferroviaria Italiana - Architetture Fail-Safe e Fault-Tolerant delle Piattaforme SEC e PMF con Dimostratori della Piattaforma IRM e del Protocollo PVS" nell'ambito di Accordo Quadro "Sistemi Embedded per applicazioni ferroviarie". **Supero del Quinto** (Mar 2021 – Set 2021).
Attivazione della procedura di "Supero del Quinto" con finanziamento di 130 000 euro riguardante il contratto triennale con RFI di cui sotto, per un finanziamento aggiuntivo allo scopo di finalizzare i lavori iniziati nel contratto regolare, quindi sulle stesse tematiche e responsabilità.

RFI-SEC-PMF

(Convenzione conto terzi) Rete Ferroviaria Italiana - Architetture Fail-Safe e Fault-Tolerant delle Piattaforme SEC e PMF con Dimostratori della Piattaforma IRM e del Protocollo PVS" nell'ambito di Accordo Quadro "Sistemi Embedded per applicazioni ferroviarie" (Lug 2018 – Lug 2021).
Finanziamento progetto: circa 650 000 euro
Ruolo del Candidato: partecipazione tecnica, coordinamento attività (gestione scadenze di deliverables, timesheets, interazioni con personale amministrativo)
Il progetto esplora le architetture sicure per i sistemi ferroviari SIL4 e vede una cooperazione tra il gruppo RCL e il dipartimento R&D di RFI - Rete Ferroviaria Italiana allo scopo di ideare architetture e meccanismi per i sistemi SIL4, insieme a prototipi di sottosistemi specifici.
Responsabile tecnico del progetto, coordinando studenti e collaboratori afferenti a tale progetto. Alcuni dei principali obiettivi del progetto sono descritti di seguito.
- Definizione di architetture per sistemi di bordo treno e di stazione.
- Definizione di regole per l'implementazione del software SIL4 nel settore ferroviario, comprese regole di

codifica, stili di codifica e metriche di qualità software.
- Piano di Verifica e Validazione, includendo Hazard Analyses preliminari.
- Visualizzazione sicura di informazioni critiche per la sicurezza sui dispositivi OTS commerciali (ad esempio, tablet) finalizzata all'utilizzo come terminali operatore.
- Implementazione del "Protocollo Vitale Standard" per consentire comunicazioni sicure tra sottosistemi, in conformità agli standard CENELEC appositi.

PROTECT-ID

PON – MISE 2016 PROTECT ID "Processi e tecnologie innovative per la protezione delle identità digitali e delle informazioni personali in rete". Partners: Engineering Ingegneria Informatica, Poste Italiane, ResilTech, ICT-SUD, Alkemy. Coinvolgimento come collaboratore di Resiltech s.r.l. (Mag – Dic 2019)
Finanziamento progetto: non noto, collaboratore esterno
Ruolo del Candidato: partecipazione tecnica come consulente e contributo a due deliverables di progetto
ProtectID ha l'obiettivo di costruire un insieme di servizi e soluzioni innovative (definendo e validando nuovi modelli e componenti software) di sicurezza nel contesto della gestione dell'Identità Digitale, con particolare riferimento alla protezione della privacy e alla condivisione delle informazioni personali in rete.
Anomaly detection come supporto a tecniche di autenticazione biometrica continua, con un duplice scopo: i) analizzare l'impatto dei singoli tratti biometrici misurandone il contenuto informativo tramite tecniche di analisi di dati allo stato dell'arte, e ii) proponendo un approccio al calcolo del trust level necessario a mentenere l'autenticazione basato sulla rilevazione delle anomalie nei dati rilevati e trasmessi dai sensori biometrici.

Secure!

POR CReO 2007-2013 Regione Toscana Secure! (Mar - Apr 2015) - http://secure.eng.it/.
Finanziamento progetto (quota UNIFI): non noto – collaboratore esterno (CoCoCo)
Ruolo del Candidato: partecipazione tecnica
Il progetto Secure! mira a studiare l'applicabilità e l'efficacia di meccanismi, modelli e tecnologie di crowd-sourcing per la prevenzione e/o la mitigazione di crisi, intese come problemi di ordine pubblico, disastri naturali e terrorismo.
Definizione di uno strumento in grado di analizzare data streams provenienti dai sensori, allo scopo di verificarne la qualità ed intervenire tramite azioni di filtraggio e – laddove necessario – rimozione, considerando anche possibili azioni malevole atte a compromettere tali sensori. Sviluppo di una struttura di monitoraggio ed esecuzione degli esperimenti per rilevare dati comportamentali sul prototipo del sistema Secure!, una struttura orientata ai servizi supportata da middleware Java-based.

Progetti Europei

ADVANCE

H2020 Marie-Curie ADVANCE (Gen 2019 – OGGI, sospensione di quasi due anni causa pandemia) - http://advance-rise.eu/
Finanziamento progetto (totale): circa 650 000 euro
Ruolo del Candidato: partecipazione tecnica, organizzazione workshops
Il progetto "Addressing Verification and Validation Challenges in Future Cyber-Physical Systems" (ADVANCE) è u progetto di Transfer-of-Knowledge e punta allo scambio di conosenze ed anche di docenti, studenti e ricercatori tra le università ed aziende consorziate nel progetto, sia europee (Firenze, Budapest, Coimbra, Resiltech s.r.l) sia sudamericane: Campinas (BR), INPE (BR), Los Andes (COL). Il progetto mira ad individuare le chellenges più importanti per lo sviluppo di sistemi Cyber-fisici (CPS), che oggi costituiscono lo standard si sviluppo di sistemi hardware-software che danno ampia importanza alle interconnessioni con altri sistemi e/o tra componenti diverse
Data la mobilità ridotta causa pandemia, il progetto è stato sospeso per più di un anno. Partecipazione ai ToK meetings (ultimo fisico a Natal, BR, a Novembre 2019) e organizzazione di workshops collegati al progetto.

DEVASSES

DEVASSES FP7-IRSES (Nov 2014 – Dic 2017) - http://devasses.eu/
Finanziamento progetto (totale): circa 350 000 euro
Ruolo del Candidato: partecipazione tecnica, secondments
Il progetto DEVASSES si pone l'obiettivo di studiare lo sviluppo di sistemi critici orientati ai servizi, con l'obiettivo principale di Transfer-of-Knowledge tra i diversi partner.
Visiting student in Brasile per un totale di 4 mesi, 2 mesi ad UNICAMP, Campinas - Sao Paulo, e 2 mesi UFAL, Maceiò – Alagoas. Questo ha consentito di interagire, scambiare opinioni e condividere il lavoro corrente di ricerca tramite seminari con studenti e ricercatori locali, che hanno fornito feedbacks importanti per il completamento e la prosecuzione del lavoro di tesi.

IRENE

IRENE JPI Urban Europe Project (Nov 2014 – Giu 2017) - http://ireneproject.eu/
Finanziamento progetto (quota UNIFI): circa 178 000 euro
Ruolo del Candidato: partecipazione tecnica
Coinvolgimento nel progetto IRENE - Improving the Robustness of Urban Electricity Networks – che mira ad identificare le migliori strategie per mitigare possibili cali di tensione o interruzione di servizio in Smart Grids, identificando possibili vulnerabilità e valutandone i rischi associati.
Realizzazione di una threat analysis di alcuni possibili scenari di smart grid, orientata principalmente all'identificazione ed analisi di cyber-threats.

Organizzazione, direzione e coordinamento di centri o gruppi di ricerca nazionali e internazionali o partecipazione agli stessi e altre attività di ricerca quali la direzione o la partecipazione a comitati editoriali di riviste e collane

GRUPPO DI RICERCA E COLLABORAZIONI

Afferenza a Gruppo di Ricerca

Sono membro del gruppo Resilient Computing Lab (Dipartimento di Matematica e Informatica, Università degli Studi di Firenze, http://rcl.dimai.unifi.it/). Le attività del gruppo si concentrano principalmente sulla ricerca e sperimentazione di sistemi, infrastrutture e sistemi di sistemi affidabili e sicuri, sia per quanto riguarda la progettazione che la verifica e validazione, curando sia aspetti pratici e teorici.
All'interno del gruppo di ricerca, ho curato in particolare gli aspetti di progettazione di sistemi safetycritical, monitoring, e testing, collaborando con altri membri del gruppo, e con gruppi di altre università nazionali ed internazionali.
Nel periodo più recente, mi sono dedicato principalmente sui seguenti temi: i) definizione e applicazione di meccanismi per la rilevazione di anomalie utilizzando strumenti di Machine Learning, ai fini di identificare attacchi e guasti nel sistema, ii) definizione di sistemi sicuri (sia in termini di safety che di security) di supporto ad applicazioni ferroviarie e standards ad essi correlati, e iii) impatto di guasti di sensori e telecamere sul dato da essi generato (es. immagini) con applicazioni al Traffic Sign Recognition.

Ulteriori Affiliazioni

Ulteriori Affiliazioni:

- CINI Consorzio Interuniversitario Nazionale per l'Informatica, con partecipazione ai laboratori Embedded Systems & Smart Manifacturing e Cybersecurity
- Florence Center for Data Science (https://datascience.unifi.it/index.php/members/)

Partecipazione a Progetti di Ricerca (dettagli nel titolo precedente)

La partecipazione al gruppo di ricerca mi ha permesso di prendere parte a:
Progetti di Ricerca Regionali e Nazionali con diversi ruoli

- Partecipazione a Project Meetings: PIN 2010 TENACE
- Partecipazione e Contributo Deliverables: POR CeO 2007-2013 Secure!, POR CReO FESR 2020 SPaCe
- Coordinatore unico: RTD-UNIFI MACARON
- Co-Coordinatore: PNRR CN1-HPC

Progetti Europei con diversi ruoli:

- Task Leader e Contributo Deliverables JPI IRENE
- Secondments e Contributo Deliverables FP7-DEVASSES
- Organizzazione Eventi di progetto MSCA-H2020-ADVANCE

Inoltre il gruppo di ricerca lavora regolarmente con Aziende:

- Rete Ferroviaria Italiana: partecipazione, responsabilità tecnica di attività, e rapporto con uffici su 2 progetti di ricerca su accordi quadro "Sistemi Embedded per applicazioni ferroviarie"
- CINI-Resiltech: Consulenza su 2 diversi progetti di ricerca

In totale, i finanziamenti ottenuti dal gruppo di ricerca dal 2014 (da quando sono membro) eccedono i tre milioni di euro.

Collaborazioni a Livello Internazionale

La partecipazione al gruppo di ricerca, a progetti di ricerca regionali, nazionali, europei e industriali ha portato alle seguenti collaborazioni personali a livello internazionale:

- con l'Università di Twente (UTWENTE), principalmente nelle figure di Alexandr Vasenev e Lorena Montoya, con i quali ho lavorato nel progetto IRENE e con i quali sono co-autore di una pubblicazione a rivista
  (rivista TCPS) Threat analysis in systems-of-systems: an emergence-oriented approach
  e di una pubblicazione con tutt il consorzio del progetto IRENE
  (conferenza EnergyCON) Towards a collaborative framework to improve urban grid resilience
- con l'Universidade estadual do campinas (UNICAMP), principalmente nelle figure di Regina Moraes e Leonardo Montecchi, che ho incontrato nei progetti FP7-DEVASSES e MSCA-H2020-ADVANCE. Assieme alla prof.ssa Moraes sono stato co-chair del workshop WAFERS nel 2019, mentre il prof. Montecchi mi ha personalmente invitato a tenere il corso di 30 ore online "Tópicos Avançados em Engenharia de Software I" ad UNICAMP nel 2021 e poi come membro esterno della commissione di esame per laurea magistrale
- con l'instituto Nacional do Pesquisa Espacial (INPE), nella persona di Fatima Mattiello, che ho incontrato nel contesto del progetto MSCA-H2020-ADVANCE e con la quale sono stato co-chair del workshop WAFERS nel 2019
- con Queen Mary University of London (QMUL), l'Austrian Institute of Technology (AIT) l'azienda Ethos, partners nel progetto IRENE e con i quali sono co-autore di una pubblicazione
  (conferenza EnergyCON) Towards a collaborative framework to improve urban grid resilience
- con l'Universidade Federal do Alagoas (UFAL), nella figura del prof. Baldoino Fonseca, che ho incontrato nel progetto FP7-DEVASSES, mi ha ospitato mentre ero visiting researcher e con il quale ho una pubblicazione in cui siamo co-autori
  (conferenza SAC) Quantitative comparison of unsupervised anomaly detection algorithms for intrusion

detection
- con Critical Software s.p.a., azienda portoghese, nella figure di Mario Rui Baptista e Nuno Silva, che ho incontrato presso la mia universtà nel 2016 e con i quali abbiamo portato avanti un lavoro che ha poi portato alla stesura di un capitolo di libro
(capitolo libro CECRIS) STECA–Security Threats, Effects and Criticality Analysis: Definition and Application to Smart Grids
- con Mohamad Gharib, inzialmente Università di Trento, poi Università di Firenze, ed adesso University of Tartu (Estonia), con il quale ho collaborato per diversi mesi, originando poi una recente pubblicazione a rivista
(rivista TETC) On the properness of incorporating binary classification machine learning algorithms into safety-critical systems

TRASFERIMENTO TECNOLOGICO E DI CONOSCENZA

Mar 2021, Mar 2022, Mar 2023 — Lezione al Cyberchallenge.IT. 2 ore di didattica su Assemby RISC-V. Basi di programmazione assembly e possibili punti di attacco lavorando con linguaggi a basso livello

Feb 2020, Feb 2022 — Lezione alla Scuola Marescialli dei Carabinieri: Tecniche di OSINT. Lezione di 3 ore ripetuta più volte per diverse classi di studenti Marescialli (circa 100-150 studenti per classe) su esempi di indagini utilizzando strumenti di Open Source INTelligence (OSINT). Per l'anno 2022 le lezioni si sono svolte in modalità mista (alcuni studenti in presenza, altri collegati in videoconferenza).

Mag 2019, Mag 2020 — Lezione al Cyberchallenge.IT. 3 ore di didattica su Anomaly-based Intrusion Detection, con esempi e utilizzo di tool per l'elaborazione di dati provenienti da dataset pubblici di intrusioni.

Nov - Dic 2017 — Docente del corso "C and C ++ software for safety-critical systems". 50 ore di didattica divise in 13 lezioni, tenutosi al dipartimento di R&D di Rete Ferroviaria Italiana per dipendenti RFI. Il corso esplora le problematiche principali per la scrittura di codice in ambienti safety-critical, con esempi pratici. Oltre a fornire nozioni di base sulla programmazione orientata agli oggetti ed alla sua applicabilità in ambiente safety-critical, è stato assegnato un progetto agli studenti che ha poi portato alla realizzazione di un semplice controllore dell'accesso dei treni in stazione, in conformità agli standard applicabili (es. regole MISRA C/C++).

ATTIVITA' DI SUPERVISIONE

Supervisione di Assegnisti — Muhammad Atif (Feb 2023 – Feb 2024): Assegnista su progetto MACARON (del quale il candidato è coordinatore) per una borsa dal titolo "Machine Learning to Conduct Analyses in the Medical Physics and ICT Domains"

Studenti di Dottorato Co-Supervisionati — Tommaso Puccetti (XXXVIII ciclo del dottorato in Informatica, Matematica, Statistica – Curriculum Informatica) per il periodo Nov 2022 – Ott 2025. Co-Supervisore assieme ad Andrea Ceccarelli

Tesi Magistrali Supervisionate — Tommaso Puccetti (4/2021): Sviluppo, Verifica e Validazione di un Protocollo Ferroviario per la Trasmissione Dati in Sicurezza

Tesi Magistrali Co-Supervisionate — Lorenzo Salani (10/2021): Analisi e valutazione di un framework GAN nella generazione di datasets di attacchi
Lorenzo Sarti (10/2021): Sviluppo di software SIL0 per sistemi di manutenzione nel dominio ferroviario
Giulia Dallai (7/2019): Analisi di Azzardi per un Sistema di Interfaccia Mobile Remota per la Manutenzione delle Linee Ferroviarie
Lavinia Masini (4/2019): Analisi quantitativa di architetture safety critical per un sistema di controllo ferroviario
Duccio Bertieri (10/2018): Sviluppo Di Un Protocollo Di Comunicazione Sicuro In Ambiente Ferroviario

Tesi Triennali Supervisionate — Cosimo Giraldi (07/2023): Benchmark di Librerie XAI per Dati Tabulari
Luigi Cennini (4/2023): Valutazione di un Safety Wrapper per Machine Learners nel contesto della classificazione di immagini
Stefano Gazzini (04/2023): Trasformare dati tabulari in immagini per migliorare la classificazione: DNNs superano i MLs?
Leonardo Baragli (04/2023): Applicazione e valutazione di tecniche di domain adaptation per intrusion detection systems
Matteo Gonfiantini (04/2023): Machine learning per la classificazione di documenti economici
Daniele Bettazzi (12/2022): L'elaborazione del linguaggio naturale applicato alle cartelle cliniche italiane
Leonardo Bargiotti (2/2022): Come Posso Fidarmi Di Un Machine Learner?
Jacopo Vezzosi (12/2021): Analisi preliminare della difficoltà di un problema di classificazione binaria tramite

Feature Rankers
Marco Pellegrino (10/2021): Soluzioni basate su Reti Neurali Artificiali per l'analisi di Dati Tabulari
Alessandro Montaghi (6/2020): Meta-Learning per la combinazione di intrusion detectors
Tommaso Capecchi (4/2020):Confronto di Algoritmi Unsupervised per Anomaly-based Intrusion Detection
Antonio Caia (2/2020): Anomaly Detection In Smart Grid: Confronto Di Algoritmi Unsupervised Per L'analisi Dei Consumi
Dario Taddei (2/2020): Anomaly Detection in Sistemi Safety-Critical: Analisi e Discussione dell'Adeguatezza della Matrice di Confusione
Manuel Rettani (12/2019) Anomaly detection per la Rilevazione di Attacchi ai Sensori Biometrici

Tesi Triennali Co-Supervisionate

Mattia d'Autilia (7/2019) Pianificazione Ed Esecuzione di Test Software Unitari Secondo le Normative Ferroviarie
Arturo Bianchi (2/2019): Protocollo Vitale Standard: Descrizione e Sviluppo di un Protocollo di Comunicazione Sicuro in Ambiente Ferroviario.
Andrea Chimenti (2/2019): Studio e Sviluppo di Algorithmi a Finestra Scorrevole per Anomaly Detection
Filippo Faldetta (2/2019): Una Metodologia e la sua Validazione per Rilevare Attacchi tramite Combinazioni di Anomaly Detectors
Lorenzo Salani (2/2019): Collegamento tra Attacchi ed Anomalie: Analisi delle Anomalie Riportate nei Datasets di Intrusion Detection

PARTECIPAZIONE A COMITATI EDITORIALI

Guest Editor

Guest Editor per la Special Issue « Machine Learning and Safety: Friends or Foes? « per la rivista MDPI Safety, assieme ad Emanuele Bellini ed Andrea Bondavalli (deadline sottomissioni – Agosto 2023)

Revisore per Riviste Internazionali

2022 Artificial Intelligence Review
2022 MDPI Sensors
2022, 2023 IEEE Internet of Things Journal
2021, 2022 Expert Systems with Applications (ESWA)
2021, 2022 Elsevier Computers & Security (COSE)
2021, 2022 Pattern Recognition (PR)
2021 IEEE Transactions on Sensor Networks (TOSN)
2021 Computer Networks
2021, 2022 Elsevier Information Sciences (INS)
2020 IEEE Transactions on Dependable and Secure Computing (TDSC)
2020 Artificial Intelligence in Medicine
2020 Big Data Research
2020, 2023 Neural Networks (NEUNET)
2020, 2021 Applied Soft Computing (ASOC)
2019 Journal of the Brazilian Computer Society (JBCS)
2019, 2021, 2022 Journal of Systems Architecture (JSA)
2019 Wiley Systems Engineering
2018 International Journal of Critical Computer-Based Systems (IJCCBS) – EDCC Special Issue
2018, 2019 Journal of Network and Computer Applications (JNCA)
2017, 2018, 2021 IEEE Systems Journal

Conseguimento della titolarità di brevetti, nei settori in cui è prevista

Nessun brevetto da riportare

Conseguimento di premi e riconoscimenti nazionali e internazionali per attività di ricerca

PREMI E RICONOSCIMENTI

Best Paper Award

Best Pratical Experience Report per il paper "Implementation, Verification and Validation of a Safe and Secure Communication Protocol for the Railway Domain" presso la conferenza LADC 2019.

Premio di Tesi Magistrale

Premio per la Tesi "Metodologia, Ambiente di test ed analisi dati per lo studio di anomalie relative a indicatori middleware e di sistema" , Dipartimento di Matematica e Informatica "Ulisse Dini", D.D. N. 5923 del 23 ottobre 2015 (Decreto di Vincita DD n. 6775 del 26/11/2015).

Partecipazioni in qualità di relatore a congressi, convegni e seminari di interesse nazionale e internazionale

PARTECIPAZIONE E ORGANIZZAZIONE CONVEGNI

Comitati di Programma e Organizzazione

2024 Track Leader per la Safe, Secure and Robust AI (S2RAI) track alla conferenza Symposium on Applied Computing (SAC24)
2024 Fast Abstracts Chair per European Dependable Computing Conference (EDCC 2024)
2023 Workshop Co-Chair per WAFERS - Workshop on vAlidation and verification in FuturE cybeR-physical Systems (ISSRE 2023 Workshop)
2023 TPC member for the Symposium on Reliable and Distributed Systems (SRDS)
2023 TPC member for European Conference on Artificial Intelligence (ECAI)
2023 Industrial Relationships Co-Chair per Italian Workshop on Embedded Systems (IWES 2023)
2023 TPC member for Data-Centric Dependability and Security (DCDS 2023 – DSN Workshop)
2023 TPC member per Computer Security and Reliability (CSR 2023)
2022 TPC Member per Workshop on Resiliency, Security, Defenses and Attacks (RSDA 2022 – ISSRE Workshop)
2022 TPC Member per Software Qualty, Reliability, Safety (QRS 2022)
2022 TPC Member per WAFERS - Workshop on vAlidation and verification in FuturE cybeR-physical Systems (LADC 2022 Workshop)
2021 TPC Member for Pacific Rim Dependable Computing – Fast Abstracts (PRDC 2021 – FA)
2020 TPC Member for International Conference on Information Science and Applications (ICISA 2020)
2020, 2023 TPC Member for European Conference on Machine Learning (ECML-PKDD)
2019 Workshop Program Co-Chair per WAFERS - Workshop on vAlidation and verification in FuturE cybeR-physical Systems (LADC 2019 Workshop)
2019 fino a 2023 TPC Member per Machine Learning for CyberSecurity (MLCS – ECML Workshop)
2019 Workshop Co-Chair per ITASEC 2019
2017 fino a 2023 TPC Member per Systems of Systems Engineering Conference (SoSE)

Relatore a Conferenze

Ital-IA (3° Convegno Nazionale CINI Sull'intelligenza Artificiale)

05/2023 **Speaker** al workshop AI for CyberSecurity (Pisa, Italy)
Titolo: Which Algorithm can Detect Unknown Attacks? Comparison of Supervised, Unsupervised and Meta-Learning Algorithms for Intrusion Detection

05/2023 Italian Conference on Cybersecurity (ITASEC23)
Speaker alla Track Anomaly and Intrusion Detection (Bari, Italy)
Titolo1: Which Algorithm can Detect Unknown Attacks? Comparison of Supervised, Unsupervised and Meta-Learning Algorithms for Intrusion Detection
Titolo2: Prepare for Trouble and Make it Double! Supervised – Unsupervised Stacking for Anomaly-Based Intrusion Detection

09/2022 Italian Workshop on Embedded Systems (IWES 2022)
Speaker alla Track Artificial Intelligence On-Device and Simulation (Bari, Italy)
Titolo: On Deploying Machine Learners into Embedded Systems

09/2022 European Conference on Machine Learning (ECML 2022)
Speaker al workshop Machine Learning for CyberSecurity (Grenoble, France)
Titolo: Towards a General Model for Intrusion Detection: An Exploratory Study

06/2022 CINI Workshop on Embedded Systems
Tutorial Speaker (Verona, Italy)
Titolo: Detecting Unknown Attacks through Unsupervised Anomaly-Based Intrusion Detection

10/02/2022 ItalIA (2° Convegno Nazionale CINI Sull'intelligenza Artificiale)
Speaker alla track AI per Cyber-Security (online)
Titolo: Beyond Supervised Learning: Unsupervised Machine Learning to Detect Intrusions

04/01/2022 HICSS (52 Hawaiian International Conference on System Sciences) – online
Tutorial Leader/Speaker:
Titolo: Dealing With Zero-Day Attacks Through Unsupervised Anomaly-Based Intrusion Detection

02/12/2021 Pacific Rim Dependable Computing Conference - PRDC 2021
Speaker alla track Archiecture and System Design (online)
Titolo: Detecting Intrusions by Voting Diverse Machine Learners: Is It Really Worth?

24/11/2021 10th Latin-American Dependable Computing Conference (LADC 2021)
Session Chair per il workshop WAFERS
Speaker alla track Main Track (online)
Titolo: Feature Rankers to Predict Classification Performance of Unsupervised Intrusion Detectors

09/04/2021 Italian Conference on Cybersecurity – ItaSEC
Speaker at the Scientific Track - Anomaly Detection and Covert Channels session (online)
Titolo: Spoofing detectability as a property of biometric characteristics

29/06/2020	Dependable Systems and Networks - DSN 2020 **Tutorial Leader/Speaker** (online) Titolo: Into the Unknown: Unsupervised Machine Learning Algorithms for Anomaly-Based Intrusion Detection
28-31/10/2019	International Symposium on Software Reliability Engineering (ISSRE 2019) **Speaker** at the R11 – Security Session (Berlin, Germany). Titolo: Evaluation of Anomaly Detection algorithms made easy with RELOAD
08-09/07/2019	IEEE Services – CSR Workshop **Speaker** at the Workshop Cyber Security and Resilience in the Internet of Things (Milano, Italia). Titolo: An initial investigation on sliding windows for anomaly-based intrusion detection
08-12/04/2019	Symposium on Applied Computing - SAC 2019 **Speaker** at the Dependable, Adaptive, Distributed Systems Session (Limassol, Cyprus). Titolo: Quantitative comparison of unsupervised anomaly detection algorithms for intrusion detection
04-07/12/2018	Pacific Rim Dependable Computing Conference - PRDC 2018 **Speaker** at the Main Track (Taipei, Taiwan). Titolo: On algorithms selection for unsupervised anomaly detection
04-06/04/2017	Symposium on Applied Computing - SAC 2017 **Speaker** at the Main Track – SATTA Session (Marrakech, Marocco). Titolo: Exploring anomaly detection in systems of systems
27-28/03/2017	SmartGIFT 2017 **Speaker** at the "IRENE" workshop, 2 presentazioni separate (London, UK). Titolo: A tool for evolutionary threat analysis of smart grids Titolo: A modeling framework to support resilient evolution planning of smart grids
29-31/01/2017	PhD Minisymposium **Speaker** at the Student Session (Department of Measurement and Informatics Budapest – Hungary) Titolo: Executing Online Anomaly Detection in Complex Dynamic Systems
26-29/09/2016	Symposium on Reliable Distributed Systems - SRDS 2016 **Speaker** at the Student Forum session (Budapest, Hungary) Titolo: Challenging Anomaly Detection in Complex Dynamic Systems
20-23/09/2016	Computer Safety, Reliability and Security - SAFECOMP 2016 **Speaker** at the Main Track - Anomaly Detection and Resilience session (Trondheim, Norway) Titolo: Context-awareness to improve anomaly detection in dynamic service oriented architectures
18-20/08/2016	CuriousU summer school **Speaker** at the 'Cybersecurity' Session, University of Twente (Enschede - NL)
07-09/01/2016	High Assurance Systems Engineering Symposium - HASE 2016 **Speaker** at the Main Track - Networked Systems session (Orlando, Florida, US) Titolo: Presenting the proper data to the crisis management operator: A relevance labelling strategy
22-25/06/2015	Dependable Systems and Networks - DSN 2015 **Speaker** at the Student Forum Session (Rio de Janeiro, Brasil) Titolo: Multi-layer anomaly detection in complex dynamic critical systems
Relatore Invitato ad Eventi	(Lug 2023) ARTISAN PhD School, Wien, Austria (Future Event) Invited speaker per una lezione alla seconda edizione della scuola di dottorato ARTISAN (role, application and implications of ARTificial Intelligence in Security-related ApplicatioNs), lezione dal titolo " Meta-Learning for Intrusion Detection: Teamwork or Clash?" (Lug 2022) ARTISAN PhD School, Valence, France Invited speaker per una lezione alla scuola di dottorato ARTISAN (role, application and implications of ARTificial Intelligence in Security-related ApplicatioNs), lezione dal titolo " Machine Learning for Intrusion Detection Systems: Design and Evaluation" (Aug 2016) CuriousU Summer School University of Twente (UT), Enschede, The Netherlands. Invited speaker ad una scuola estiva per studenti magistrali e di PhD ad una sessione di cyber-security, presentando il lavoro portato avanti nel contesto del progetto IRENE sulla cyber-security di Smart Grids.
Revisore (non TPC) per Conferenze Internazionali	2019 ACM Symposium on Applied Computing - SAC 2019 (Sub-Reviewer) 2019, 2021 Hawaiian International Conference on System Sciences (HICSS) 2018 ACM International Symposium on Mobility Management and Wireless Access - MobiWac 2018 2018 IEEE International Symposium on Reliable and Distributed Systems – SRDS 2018 (Sub-Reviewer) 2016 - 2023 Dependable Systems and Networks – DSN (Sub-Reviewer)
Partecipazione a Meeting	20-21/1/2022 IFIP WG Winter Meeting Partecipazione al Meeting invernale dell'IFIP WG 10.4 a tema "AI and Dependability: And the twain shall meet"

Diploma di specializzazione europea riconosciuto da Board internazionali, relativamente ai settori concorsuali nei quali è prevista

Non applicabile per il SSD INF/01

AUTORIZZAZIONE AL TRATTAMENTO DI DATI PERSONALI

Autorizzo il trattamento dei miei dati personali presenti nel curriculum vitae ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 e del GDPR (Regolamento UE 2016/679).

DICHIARAZIONE SOSTITUTIVA DI CERTIFICAZIONE (art. 46 e 47 D.P.R. 445/2000)

Il sottoscritto Tommaso Zoppi, ai sensi e per gli effetti degli articoli 46 e 47 e consapevole delle sanzioni penali previste dall'articolo 76 del D.P.R. 28 dicembre 2000, n. 445 nelle ipotesi di falsità in atti e dichiarazioni mendaci, dichiara che le informazioni riportate nel presente curriculum vitae corrispondono a verità.

Luogo e Data **Firma**

Firenze, 21/6/2023