Curriculum vitae

INFORMAZIONI PERSONALI

Marta Catillo

martacatillo@gmail.com - marta.catillo@unisannio.it

ISTRUZIONE E FORMAZIONE

Novembre 2023 — Dottorato di Ricerca in Tecnologie dell'Informazione per l'Ingegneria (XXXV ciclo)

Università degli Studi del Sannio

Tesi: "On the use of machine learning for intrusion detection: public datasets, challenges and solutions"

Luglio 2019 — Laurea Magistrale 110/110 *cum laude* in Ingegneria Informatica *(classe delle lauree magistrali in Ingegneria Informatica LM-32)*

Università degli Studi del Sannio

Tesi: "Rilevazione di attacchi di rete mediante l'anomaly detector ZED-IDS"

Dicembre 2015 — Laurea triennale in Ingegneria Informatica

Università degli Studi del Sannio

Tesi: "Installazione e configurazione di OpenStack su un sistema cluster ad alte prestazioni"

ESPERIENZA PROFESSIONALE

Gennaio 2023 - ad oggi — Assegnista di ricerca presso il DING

Dipartimento di Ingegneria
Università degli Studi del Sannio

Progetto EMELIOT - Engineered MachinE Learning-intensive IoT system
Supporto alla definizione automatica e quality assurance di machine learning pipelines.

Dicembre 2019 - Novembre 2023 — Dottoranda in TECNOLOGIE DELL'INFORMAZIONE PER L'INGEGNERIA presso il DING

Dipartimento di Ingegneria
Università degli Studi del Sannio

Attività di interesse:

- Sicurezza e resilienza degli information system.
- Applicazione delle tecniche di machine learning in ambito computer security.
- Analisi dei dati di rete.
- Architetture parallele.

Settembre 2019 - Dicembre 2019

Borsista di ricerca presso il DING

Dipartimento di Ingegneria
Università degli Studi del Sannio

Vincitrice di una borsa di studio per lo svolgimento di attività di ricerca presso il Dipartimento di Ingegneria dell'Università degli Studi del Sannio.

Attività svolte:

- Valutazione degli overhead connessi all'impiego di politiche di sicurezza avanzate.
- Benchmarking di server e applicazioni web in configurazione "standard" e in configurazioni "sicure".

Luglio 2018 - Luglio 2019

Borsista GARR

Consorzio GARR
Via dei Tizii, 6, 00185 Roma

Vincitrice di una borsa di studio GARR "Orio Carlini" per lo svolgimento di attività di ricerca presso il Dipartimento di Ingegneria dell'Università degli Studi del Sannio.

Attività svolte:

- Sperimentazione di tecniche di machine learning su network data.
- Sviluppo di un sistema di rilevamento delle intrusioni (IDS) mediante tecniche di machine learning per la detection di attacchi di rete noti e non noti *(0-day)*.

ATTIVITÀ DI SUPPORTO ALLA DIDATTICA A LIVELLO UNIVERSITARIO

2020 - ad oggi

Cultore della materia per l'insegnamento Architettura dei Calcolatori

Membro di commissioni d'esame in qualità di cultore della materia per l'insegnamento Architettura dei Calcolatori (9 CFU - corso di laurea triennale in Ingegneria Informatica. Università degli Studi del Sannio).

2020 - ad oggi

Cultore della materia per l'insegnamento Calcolo Parallelo ed ad Alte Prestazioni

Membro di commissioni d'esame in qualità di cultore della materia per l'insegnamento Calcolo Parallelo ed ad Alte Prestazioni (9 CFU - corso di laurea magistrale in Ingegneria Informatica. Università degli Studi del Sannio).

2020 - ad oggi

Cultore della materia per l'insegnamento Data Science

Membro di commissioni d'esame in qualità di cultore della materia per l'insegnamento Data Science (9 CFU - corso di laurea magistrale in Ingegneria Informatica. Università degli Studi del Sannio).

2023 - ad oggi

Cultore della materia per l'insegnamento Sistemi Operativi

Membro di commissioni d'esame in qualità di cultore della materia per l'insegnamento Sistemi Operativi (9 CFU - corso di laurea triennale in Ingegneria Informatica. Università degli Studi del Sannio).

2019 - ad oggi

Supporto alla didattica

Esercitazioni di MPI per il corso di Calcolo Parallelo ed ad Alte Prestazioni (9 CFU - corso di laurea magistrale in Ingegneria Informatica. Università degli Studi del Sannio).

Esercitazioni su deep learning per il rilevamento di anomalie per il corso di Data Science (9 CFU - corso di laurea magistrale in Ingegneria Informatica. Università degli Studi del Sannio).

2020 - ad oggi

Tesi di laurea e tutorato studenti

Svolgimento di attività di tutorato a studenti e correlatore di tesi (supervisione di 3 studenti) presso il Dipartimento di Ingegneria dell'Università degli Studi del Sannio.

ATTIVITÀ EDITORIALE PER RIVISTE SCIENTIFICHE

Editor-in-Chief

Editor-in-Chief della rivista scientifica International Journal of Open Source Software and Processes (IJOSSP).

Reviewer

Peer reviewer per la riviste scientifiche IEEE Access, Software Quality Journal, Journal of Network and Computer Applications, International Journal of Information Security e Transactions on Information Forensics & Security.

PARTECIPAZIONE A COMITATI SCIENTIFICI

Technical Program Committee Member

Componente del comitato scientifico della International Conference on Availability, Reliability and Security (ARES).

Componente del comitato scientifico della International Conference on Cloud Computing Technology and Science (CLOUDCOM).

Componente del comitato scientifico della Safe, Secure and Robust AI Track (S2RAI).

Componente del comitato scientifico dell' International DSN Workshop on Data-Centric Dependability and Security (DCDS).

External reviewer

External reviewer per l'International Symposium on the Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)

Co-chair

Organizzatore e chair di 3 edizioni dell'International ISSRE Workshop on Resiliency, Security, Defenses and Attacks (RSDA).

Local chair

Local chair dell'International Conference on Availability, Reliability and Security (ARES 2023).

PARTECIPAZIONE A PROGETTI DI RICERCA

2022

Titolarità di un incarico di ricerca

Prestazione occasionale per la sperimentazione di sistemi di rilevamento delle intrusioni informatiche. L'incarico di collaborazione è stato conferito da Consorzio Interuniversitario Nazionale per l'Informatica nell'ambito del progetto BOTITS (Boosting OT and IT Security) finanziato da Silicon Valley Community Foundation.

PREMI E RICONOSCIMENTI

Best Paper Award

Best Paper Award alla 14th International Conference on the Quality of Information and Communications Technology (QUATIC 2021) per il lavoro: "A Critique on the Use of Machine Learning on Public Datasets for Intrusion Detection". Catillo, M., Del Vecchio, A., Pecchia, A., Villano, U. (2021). In: Paiva, A.C.R., Cavalli, A.R., Ventura Martins, P., Pérez-Castillo, R. (eds) Quality of Information and Communications Technology. QUATIC 2021. Communications in Computer and Information Science, vol 1439. Springer, Cham. https://doi.org/10.1007/978-3-030-85347-1_19

Travel grant

Vincitrice di un travel grant per l'International Conference on Dependable Systems and Networks (DSN-2023).

Trasferimento tecnologico: premio pari opportunità Start Cup Campania 2022

Premio speciale per la migliore idea d'impresa che promuova il principio delle pari opportunità e l'imprenditorialità femminile.

ALTRI TITOLI DI STUDIO E PROFESSIONALI

2021 **Abilitazione all'esercizio della professione di Ingegnere, Sezione A - Settore Informazione**

Università degli Studi del Sannio

COMPETENZE PERSONALI

Lingua madre: Italiano

Altre lingue

	COMPRENSIONE		PARLATO		SCRITTO
	Ascolto	Lettura	Interazione	Produzione orale	
Inglese	B2 Livello intermedio	B2 Livello intermedio	B2 Livello intermedio	B2 Livello intermedio	B2 Livello intermedio

Livelli: A1/A2: Livello base - B1/B2: Livello intermedio - C1/C2: Livello avanzato
Quadro Comune Europeo di Riferimento delle Lingue

Altre lingue

	COMPRENSIONE		PARLATO		SCRITTO
	Ascolto	Lettura	Interazione	Produzione orale	
Francese	B2 Livello intermedio	B2 Livello intermedio	B2 Livello intermedio	B2 Livello intermedio	B2 Livello intermedio

Livelli: A1/A2: Livello base - B1/B2: Livello intermedio - C1/C2: Livello avanzato
Quadro Comune Europeo di Riferimento delle Lingue

Competenze comunicative

Problem solving, capacità di prendere decisioni.

Atteggiamento costruttivo, ottimo senso di adattamento e flessibilità nella gestione dei compiti grazie alla frequentazione di contesti diversi.

Competenze organizzative e gestionali

Attitudine nella pianificazione, nel perseguimento di obiettivi nel rispetto delle scadenze previste.

Capacità di lavorare in autonomia.

Buone capacità di ascolto e precisione nel conseguire gli obiettivi prefissati.

Capacità di gestione dei progetti.

Predisposizione all'inserimento in contesti multiculturali per lavori di team-working.

Competenze tecniche

Conoscenza del linguaggio di programmazione Python, e, in particolare, delle seguenti librerie:

- Pandas, NumPy, SciPy (per calcoli scientifici ed analisi statistiche)
- Matplotlib, Seaborn (visualizzazione dati)
- Tensorflow, Keras (machine learning)

Conoscenza dei principi, delle metodologie e delle tecniche/teorie della cybersecurity e del panorama attuale degli attacchi informatici in diversi ambienti (Desktop/Web/Mobile/IoT).

Conoscenza dei software e delle distribuzioni Linux orientate all'analisi e al test della sicurezza (Kali Linux e suite di software inclusi).

Conoscenza degli scanner Nessus e Metasploit e dei principali strumenti di monitoraggio della comunicazione: Wireshark, tcpdump, Netcat, ecc.

Conoscenza di tecniche di analisi per ambiti di ricerca OSINT.

Conoscenza e capacità di utilizzo di strumenti di analisi e valutazione delle performance di una architettura di calcolo parallelo.

Sviluppo in ambiente parallelo con MPI e OpenMP.

Conoscenza di WSDL, SOAP, XML, JSON, Axis, Axis2 e REST.

Conoscenze di sistemi distribuiti e del middleware Java RMI.

Conoscenza della piattaforma Java Enterprise e di alcuni suoi strumenti per lo sviluppo di middleware di comunicazione (JBoss, JMS, JMX).

Programmazione web statica e dinamica tramite HTML e tecnologie JSP e Servlet, Java Bean, RESTful Web Services.

Competenze di Sistemi Operativi.

Conoscenze sull'architettura dei processori e programmazione *assembly*.

Sviluppo di applicazioni *mobile* per Android.

Conoscenze di UML, architetture software e design pattern.

Capacità di utilizzo e gestione di strumenti di controllo e versioning del codice quali SVN e Git.

Competenze informatiche

Ottima conoscenza dei pacchetti Microsoft Office e OpenOffice.

Linguaggi di programmazione: Java, C, Assembly, Python, Bash/Shell Scripting.

Conoscenza del linguaggio di markup LaTeX.

Patente di guida

B, automunita.

CERTIFICAZIONI

2004

European Computer Driving License (ECDL) - AICA

2018

Fundamentals of Deep Learning for Computer Vision - NVIDIA Deep Learning Institute, Licenza ID 11274c0e27d143c18bbb51325cedecd8

PUBBLICAZIONI SCIENTIFICHE

Articoli su riviste internazionali

M. Catillo, M. Rak, U. Villano, "*Discovery of DoS attacks by the ZED-IDS Anomaly Detector*". Journal of High Speed Networks 25 (4), 349-365 (2019).

M. Catillo, L. Ocone, M. Rak, and U. Villano, "*Black-box Load Testing to Support Auto-scaling Web Applications in the Cloud*". International Journal of Grid and Utility Computing 12 (2), 139-148 (2021).

M. Catillo, A. Pecchia, M. Rak, and U. Villano, "*Demystifying the role of public intrusion datasets: A replication study of DoS network traffic data*". Computers & Security 108, 102341 (2021).

M. Catillo, A. Pecchia, and U. Villano, "*Autolog: Anomaly detection by deep autoencoding of system logs*". Expert Systems with Applications 191, 116263 (2022).

M. Catillo, A. Pecchia, and U. Villano, "*No more DoS? An empirical study on defense techniques for web server Denial of Service mitigation*". Journal of Network and Computer Applications 202, 103363 (2022).

M. Catillo, A. Del Vecchio, A. Pecchia, and U. Villano, "*Transferability of machine learning models learned from public intrusion detection datasets: the CICIDS2017 case study*". Software Quality Journal 30 (4), 955-981 (2022).

M. Catillo, M. Rak, and U. Villano, "*A survey on auto-scaling: how to exploit cloud elasticity*". International Journal of Grid and Utility Computing (IJGUC) 14 (1), 37-50 (2023).

M. Catillo, M. Rak, and U. Villano, "*A Deep Learning Method for Lightweight and Cross-Device IoT Botnet Detection*". Applied Sciences 13 (2) (2023).

M. Catillo, A. Pecchia, and U. Villano, "*CPS-GUARD: Intrusion detection for cyber-physical systems and IoT devices using outlier-aware deep autoencoders*". Computers & Security 129, 103210 (2023).

M. Catillo, A. Pecchia, and U. Villano, "*Successful intrusion detection with a single deep autoencoder: theory and practice.* ". Software Quality Journal 32 (I) , 95-123 (2023).

M. Catillo, A. Pecchia, and U. Villano, "*Exploring the effect of training-time randomness on the performance of deep neural networks for intrusion detection.* ". Soft computing 28 (3), 1957-1969 (2024).

Articoli in atti di conferenze

M. Catillo, M. Rak, and U. Villano, "*Auto-scaling in the Cloud: Current Status and Perspectives*". In Advances on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC). Springer International Publishing, 2019, pp. 616–625.

M. Catillo, M. Rak, and U. Villano. "*2L-ZED-IDS: A Two-Level Anomaly Detector for Multiple Attack Classes*". In Web, Artificial Intelligence and Network Applications (WAINA). Springer International Publishing, 2020, pp. 687–696.

M. Catillo, L. Ocone, M. Rak, and U. Villano, "*Auto-scaling Applications in the Cloud by Simple Indexes with Complex Loads*". In *Proc.* 29th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE). IEEE, 2020, pp. 76-81.

M. Catillo, A. Pecchia, and U. Villano, "*Towards a Framework for Improving Experiments on DoS Attacks*". In Quality of Information and Communications Technology (QUATIC). Springer International Publishing, 2020, pp. 303-316.

M. Catillo, A. Pecchia, M. Rak, and U. Villano, "*A case study on the representativeness of public DoS network traffic data for cybersecurity research*". In *Proc.* 15th International Conference on Availability, Reliability and Security (ARES). Association for Computing Machinery (ACM), 2020, pp. 1-10.

M. Catillo, A. Pecchia, and U. Villano, "*Measurement-Based Analysis of a DoS Defense Module for an Open Source Web Server*". In Testing Software and Systems (ICTSS). Springer International Publishing, 2020, pp. 121-134.

R. Della Corte, C. Gutierrez, J. Hong, and M. Catillo, "*Message from the RSDA 2020 Workshop Chairs*". In *Proc.* 31st International Symposium on Software Reliability Engineering Workshops (ISSREW). IEEE, 2020.

M. Catillo, A. Del Vecchio, A. Pecchia, and U. Villano, "*A Critique on the Use of Machine Learning on Public Datasets for Intrusion Detection*". In Quality of Information and Communications Technology (QUATIC). Springer International Publishing, 2021, pp. 121-134.

M. Catillo, A. Del Vecchio, L.Ocone, A. Pecchia, and U. Villano, "*USB-IDS-1: a Public Multilayer Dataset of Labeled Network Flows for IDS Evaluation*". In *Proc.* 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W). IEEE, 2021, pp. 1-6.

R. Della Corte, M. Catillo, J. Ferreira, and G.J. Li, "*Message from the RSDA 2021 Workshop Chairs*". In *Proc.* 32nd International Symposium on Software Reliability Engineering Workshops (ISSREW). IEEE, 2021.

M. Catillo, A. Del Vecchio, A. Pecchia, and U. Villano, "*On the quality of network flow records for IDS evaluation: a collaborative filtering approach*". In Testing Software and Systems (ICTSS). Springer International Publishing, 2021, pp. 196-209.

M. Catillo, A. Pecchia, and U. Villano, "*Botnet Detection in the Internet of Things through All-in-one Deep Autoencoding*". In *Proc.* 17th International Conference on Availability, Reliability and Security (ARES). Association for Computing Machinery (ACM), 2022, pp. 1-7.

M. Catillo, A. Pecchia, and U. Villano, "*Simpler Is Better: On the Use of Autoencoders for Intrusion Detection"*. In Quality of Information and Communications Technology (QUATIC). Springer International Publishing, 2022, pp. 303-316.

R. Della Corte, M. Catillo, J. Ferreira, and G.J. Li, "*Message from the RSDA 2022 Workshop Chairs*". In *Proc.* 33rd International Symposium on Software Reliability Engineering Workshops (ISSREW). IEEE, 2022.

M. Catillo, A. Pecchia, and U. Villano "*Machine Learning on Public Intrusion Datasets: Academic Hype or Concrete Advances in NIDS?*". In *Proc.* 53rd International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S). IEEE, 2023, pp. 132-136.

M. Catillo, A. Del Vecchio, A. Pecchia, and U. Villano "*A Case Study with CICIDS2017 on the Robustness of Machine Learning against Adversarial Attacks in Intrusion Detection*". In *Proc.* 18th International International Conference on Availability, Reliability and Security (ARES). ACM, 2023, pp. 1-8.

Dati personali

Autorizzo il trattamento dei miei dati personali ai sensi del Decreto Legislativo 30 giugno 2003, n.196 "Codice in materia di protezione dei dati personali".

Autocertificazione

La sottoscritta Marta Catillo, consapevole che le dichiarazioni false comportano l'applicazione delle sanzioni penali previste dall'art.76 del D.P.R. 445/2000, dichiara che le informazioni riportate nel seguente curriculum vitae, redatto in formato europeo, corrispondono a verità.
La sottoscritta Marta Catillo dichiara di essere a conoscenza dell'art.75 del D.P.R. 28.12.2000, n.445 relativo alla decadenza dai benefici eventualmente conseguenti al provvedimento emanato qualora l'Amministrazione, a seguito di controllo, riscontri la non veridicità del contenuto della suddetta dichiarazione.