Luca **Petrillo**

Esperienze Pregresse

Attualmente sono PhD Stundent in Cybersecurity presso la scuola IMT Alti Studi di Lucca e associato all'IIT-CNR di Pisa. Nel 2023 ho ho conseguito la Laurea Magistrale in Sicurezza dei Sistemi Software presso L'Università degli Studi del Molise difendendo la tesi intitolata "Cybersecurity-related Tweet Classification by Explainable Deep Learning". Nel 2021 ho conseguito la Laurea Triennale in Informatica. Durante questo percorso di studi ho svolto progetti che mi hanno permesso di. A Giugno 2022 ho ottenuto un contratto di collaborazione con il CNR (Istituto di Informatica e Telematica). Durante questo periodo ho lavorato sul progetto di ricerca europeo MEDINA, che ha il compito di contribuire alla politica europea di certificazione della sicurezza del cloud. In questa fase mi sono occupato dello sviluppo del NL2CNL Translator che è un componente del framework MEDINA che esegue task di NLP (Natual Language Processsing) e ha due scopi principali. Il primo obiettivo è quello di selezionare un insieme di metriche che possano essere utili per valutare un determinato requisito di sicurezza, chiamato anche TOM (Technical and Organizational Measure). Dopo aver associato un insieme di metriche a un requisito, il secondo obiettivo è quello di tradurre tali metriche in politiche. In particolare, le metriche sono espresse in NL (Natual Language), mentre le politiche tradotte sono espresse in CNL (Controlled Natural Language). Inoltre mi sono occupato dello sviluppo del DSL Mapper che è un altro componente del framework MEDINA che ha lo scopo di mappare gli obblighi espressi in CNL in politiche eseguibili espresse in DSL. L'output generato da questo componente è in formato Rego (un linguaggio di policy). Questa esperienza mi ha permesso di accrescere le mie competenze e conoscenze nello sviluppo di software di sicurezza, dei linguaggi per politihe di sicurezza e dei progetti di ricerca europei. A Giugno del 2023 ho preso parte al progetto Security Home Gateway 4.0 (SHG), sempre in collaborazione con il CNR, che è un'ecosistema di protezione per i dispositivi IoT e in generale per gli elementi costitutivi di una rete consumer con un dispositivo efficiente e pronto a respingere ogni possibile attacco. Nello specifico mi sono occupato di creare un'interfaccia per Suricata, un sistema di rilevamento delle intrusioni (IDS) di nuova generazione, per permettere la comunicazione tramite API REST. Ad Agosto del 2023 è iniziata la mia collaborazione con il progetto europeo DUCA (Data Usage Control for empowering digital sovereignty for All citizens), dove mi sto occupando di studiare e sviluppare metodologie per la traduzione automatica delle politiche di sicurezza specificate in linguaggio naturale in un linguaggio comprensibile e attuabile in maniera automatizzata. Nello stesso periodo sono stato coinvolto nell'ambito del partenariato esteso "SEcurity and RIghts in the CyberSpace (SERICS)" nel progetto DISE, "Digital soveregnty" per studiare e sviluppare metodologie a supporto della sovranità digitale, in particolare per la definizione e la comprensione semi-automatica delle norme.

Istruzione e Formazione

Dottorato Nazionale in Cybersecurity — *Lucca (LU) - Pisa (PI), Italia*

Scuola IMT Alti Studi Lucca, IIT-CNR — *2023 - in corso*

Vincitore della Borsa di dottorato XXXVIII ciclo - Cybersicurezza, Progetto: "Security policy management for digital sovereignty"

Laurea Magistrale in Sicurezza dei Sistemi Software — *Pesche (IS), Italia*

Università degli Studi del Molise - Dipartimento di Bioscienze e Territorio — *2021 - 2023*

Laurea Triennale in Informatica — *Pesche (IS), Italia*

Università degli Studi del Molise - Dipartimento di Bioscienze e Territorio — *2018 - 2021*

Diploma di Maturità — *Campobasso, Italia*

Istituto Tecnico Industriale "G.Marconi" — *2013 - 2018*

Lingue

LINGUA MADRE: Italiano

ALTRE LINGUE: Inglese

- Ascolto: B1
- Lettura: B1
- Scrittura: B1
- Interazione orale: B1
- Produzione orale: B1

Competenze Professionali

Software Applicativi	WordPress (*Intermedio*)
Linguaggi di Programmazione	C (*Intermedio*) | Java (*Intermedio*) | Python (*Intermedio*) | Ruby (*Base*)
Ambienti di sviluppo integrato (IDE)	Android Studio (*Intermedio*) | CLion (*Intermedio*) | IntelliJ IDEA (*Intermedio*) RubyMine (*Intermedio*) | PyCharm (*Intermedio*) | Visual Studio Code (*Intermedio*)
Sistemi Operativi	Android (*Intermedio*) | Linux (*Intermedio*) | Microsoft Windows *Intermedio*)
Sistemi di gestione di database	MySQL (*Base*) | SQLite (*Base*) | MongoDB (*Base*)
Sistemi di orchestrazione di container	Docker (*Intermedio*) | Kubernetes (*Intermedio*)

Esperienze lavorative

CNR (Istituto di Informatica e Telematica) *Pisa, Italia*

RICERCATORE ASSOCIATO *Feb 2024 - Dic 2024*

DUCA (Data Usage Control for empowering digital sovereignty for All citizens)

- Ricerca e sviluppo di modelli AI per la traduzione automatizzata di politiche di sicurezza.

DiSE (Digital soveregnty)

- Ricerca e sviluppo di modelli AI per la definizione e la comprensione semi-automatica delle norme e politiche di sicurezza.

EMERALD

- Ricerca e sviluppo di soluzioni per automatizzare il processo di certificazione dei cloud service provider tramite la specifica di requisiti in linguaggio naturale.

CNR (Istituto di Informatica e Telematica) *Pisa, Italia*

COLLABORATORE *Giu 2022 - Apr 2023 / Ott 2023 - Feb 2024*

NL2CNL Translator

- Svilupppo di API REST utilizzando FastAPI, un framework in Python.
- Implementazione di un'interfacia API con gli altri componenti di MEDINA e coordinato tutte le operazioni e i collegamenti con gli altri sottocomponenti interni.
- Sviluppo di un endpoint che dato un requisito, effettua l'associazione tra il requisito e le relative metriche.
- Sviluppo di un endpoint che presi un requisito e una lista di metriche ad esso associate le traduce in un REO (Requirements&Obligations) object.
- Gestione della pipeline CI/CD dei componenti con Docker e Kubernetes.

DSL Mapper

- Svilupppo di API REST utilizzando FastAPI, un framework in Python
- Implementazione di un'interfacia API con gli altri componenti di MEDINA e coordinato tutte le operazioni e i collegamenti con gli altri sottocomponenti interni.
- Sviluppo di un endpoint che genera regole Rego per gli obblighi associati a un determinato requisito.
- Gestione della pipeline CI/CD dei componenti con Docker e Kubernetes.

Security Home Gateway 4.0 (SHG)

- Svilupppo di API REST utilizzando Flask, un framework in Python.
- Creazione di un'interfaccia che, tramite API, consenta la comunicazione con Suricata.

Progetti

Turbaned (Tweet clUsteRization BAsed oN cvE Description) (Software di sicurezza)
https://github.com/lucapetrillo99/turbaned

Tool innovativo che permette di rilevare la presenza di Cve o una loro descrizione all'interno di una raccolta di Tweet

Python Docker

Ulti mateManga (Applicazione Android)

Applicazione Android che permette di consultare, recensire ed avere news su una grande raccolta di manga

Java | Ruby | MongoDB

Yabm (Yet Antoher Bookmark Manager) (Applicazione Android)
https://github.com/lucapetrillo99/yabm

Applicazione Android con un design moderno per la raccolta e la gestione dei segnalibri

Java | SQLite

NL2CNL Translator (Software di sicurezza)
https://git.code.tecnalia.com/medina/public/nl2cnl-translator

Tool per la rapprentazione di requisiti di sicurezza da linguaggio natuale in linguaggio controllato (CNL)

Python | Docker | Kubernetes

DSL Mapper (Software di sicurezza)
https://git.code.tecnalia.com/medina/public/dsl-mapper

Tool utilizzato per la traduzione di requisiti di sicurezza da linguaggio controllato (CNL) in Rego policy

Python | Docker | Kubernetes

SHG (Security Home Gateway 4.0) (Software di sicurezza)
Un ecosistema di protezione per i dispositivi IoT e in generale per gli elementi costitutivi di una rete consumer con un dispositivo efficiente pronto a respingere ogni possibile attacco.

Parser (Software di sicurezza)
https://github.com/lucapetrillo99/parser

Parser che traduce i programmi C che manipolano l'heap, in istruzioni compatibili con Z3.

Python

TALLM (Text Analysis using Large Language Model (Software di sicurezza)
Strumento che integra diversi Large Language Models per eseguire analisi avanzate su dataset testuali, consentendo attività come la classificazione del testo, la classificazione di token e task di tipo sequence-to-sequence.

Python | Docker

Pubblicazioni

L. Petrillo, F. Martinelli, A. Santone and Francesco Mercaldo. Explainable Security Requirements Classification Through Transformer Models

SPECIAL ISSUE GENERATIVE ARTIFICIAL INTELLIGENCE IN SMART SOCIETIES — *Future Internet 2025, 17(1), 15*

DOI: https://doi.org/10.3390/fi17010015

J. Bianchi, S. Dong, L. Petrillo and Marinella Petrocchi. Automatic Association of Quality Requirements and Quantifiable Metrics for Cloud Security Certification — *Bolzano (Italia)*

4TH ITALIAN WORKSHOP ON ARTIFICIAL INTELLIGENCE AND APPLICATIONS FOR BUSINESS AND INDUSTRIES - AIABI | CO-LOCATED WITH AI*IA 2024 — *25 - 28 Novembre, 2024*

https://arxiv.org/pdf/2503.09460

L. Petrillo, F. Martinelli, A. Santone and Francesco Mercaldo. Toward the Adoption of Explainable Pre-Trained Large Language Models for Classifying Human-Written and AI-Generated Sentences

SPECIAL ISSUE ADVANCES IN LARGE LANGUAGE MODEL EMPOWERED MACHINE LEARNING: DESIGN AND APPLICATION — *Electronics 2024, 13(20), 4057*

DOI: https://doi.org/10.3390/electronics13204057

F. Martinelli, F. Mercaldo, L. Petrillo and Antonella Santone. A Method for AI-generated sentence detection through Large Language Models — *Siviglia (Spagna)*

PROCEDIA COMPUTER SCIENCE VOLUME 246, 2024, PAGES 4853-4862) — *2024 Elsevier*

DOI: https://doi.org/10.1016/j.procs.2024.09.351

F. Martinelli, F. Mercaldo, L. Petrillo and Antonella Santone. Security Policy Generation and Verification through Large Language Models: A proposal *Porto (Portogallo)*

THE 14TH ACM CONFERENCE ON DATA AND APPLICATION SECURITY AND PRIVACY *19 - 21 Giugno, 2024*

DOI: https://doi.org/10.1145/3626232.3658635

G. Iadarola, F. Martinelli, F. Mercaldo, L. Petrillo and Antonella Santone. Cybersecurity-related Tweet Classification by Explainable Deep Learning *Roma (Italia)*

10TH INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS SECURITY AND PRIVACY *26 - 28 Febbraio, 2024*

DOI: https://doi.org/10.5220/0012411100003648

Servizio

PROGRAM COMMITEE

2024 The 2nd International Workshop on Explainable Artificial Intelligence in Bioengineering (EAIB) *Dubrovnik, Croazia*

REVIEWER

2025 International Joint Conference on Neural Networks

2024 International Journal of Computer Virology and Hacking Techniques

2024 28th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems

Curriculum reso sotto forma di dichiarazione sostitutiva di atto di notorietà, ai sensi degli artt. 46 e 47 del D.P.R. 445/2000). Consapevole, secondo quanto prescritto dall'art. 76 del D.P.R. 445/2000, della responsabilità penale cui può andare incontro in caso di dichiarazione mendace, falsità negli atti ed uso di atti falsi, il sottoscritto dichiara che quanto esplicitato nel proprio curriculum vitae et studiorum corrisponde a verità.