Matteo Rizzi

matteo@rizzi.xyz
@matteounitn:matrix.org
orcid: 0000-0002-5288-3031

Bachelor in Computer Science, Security Administrator and Research Scientist

Born in 1998, 30 September, I hold the positions of Security Administrator at Fondazione Bruno Kessler and Research Scientist in the organization's Security and Trust unit. I joined the S&T unit to explore and improve TLS analysis and delve into identity management. While safeguarding Fondazione Bruno Kessler from cyber threats, I am looking into new opportunities and technologies and working with Istituto Poligrafico e Zecca dello Stato.

Experiences

Fondazione Bruno Kessler (Trento, Italy)

Security Administrator ● Sep, 2022 - Present

Studying the state of the art and applying my expertise of risk analysis, red teaming, blue teaming, OSINT, and offensive technologies; conducting continuous pentests on the infrastructure and introducing new defenses to safeguard and protect Fondazione Bruno Kessler from cybercriminals.

Junior Research Scientist ● Feb, 2021 - Present

Security analysis of the TLS deployments of IPZS projects, TLS Analysis in Android Apps and TLS tool enhancement within the Security & Trust research unit.

Internship ● Feb, 2020 - May, 2020

Study and improvement of TLS analysis tools within the Security & Trust research unit.

Futuro & Conoscenza S.r.l. (Trento & Rome, Italy)

Junior Research Scientist ● Jul, 2021 - Present

Collaboration between Fondazione Bruno Kessler and IPZS to promote the exchange of know-how and competences in the field of security technologies (material and digital) such as identification and and anti-counterfeiting, as well as the creation of a center for the coordination and exploitation of research.

Papers

Demo: TLSAssistant v2

in ACM Symposium on Access Control Models and Technologies, SACMAT ● Jun, 2022

Matteo Rizzi, Salvatore Manfredi, Giada Sciarretta, Silvio Ranise.

A Modular and Extensible Framework for Securing TLS

in 12th ACM Conference on Data and Application Security and Privacy, CODASPY ● Apr, 2022

Matteo Rizzi, Salvatore Manfredi, Giada Sciarretta, Silvio Ranise.

Awards

Premio Tesi - Clusit (Milan, Italy)

Placed 3rd, Associazione Italiana per la Sicurezza Informatica 17th Edition ● Sep, 2022

The "Innovare la sicurezza delle Informazioni" award is given to the most innovative university theses in information security to foster cooperation between companies, institutions, and students in Italy. A point of interchange between the productive and scientific worlds, students and the working world, motivated by participants' demands and experiences.

Teaching and Tutoring

CyberSecurity [at] Buonarroti

Istituto Tecnico Tecnologico Buonarroti, Trento ● May, 2023 - Jun, 2023

Conducted two out of four sessions involving penetration testing of the sensors at Buonarroti High School, with the objective of invalidating data and highlighting the significance of cybersecurity within the industry. The lesson involved the explanation of various techniques employed in cyber attacks, specifically focusing on the Advanced Persistent Threat (APT) and its current methodologies. Real-life examples were provided to illustrate the concepts, such as the Rogue Access Point (Wireless), Man-in-the-Middle (MiTM) attacks, and Web Vulnerability Assessment, all within the context of the school website.

PhD Course Digital Identity 2023

Fondazione Bruno Kessler, Security And Trust Unit ● Apr, 2023

I successfully delivered a lecture on the diverse attacks applicable to TLS in a PhD course, under the guidance of Salvatore Manfredi and Giada Sciarretta. During the lecture, I provided a comprehensive explanation of Oracle Attacks in a cryptographic context, and additionally presented a Proof of Concept showcasing the HeartBleed Vulnerability.

Thesis Supervisor

Riccardo G. in FBK, Security and Trust Unit ● Apr, 2023 - Aug, 2023

Riccardo G., an outstanding student, has successfully developed a groundbreaking module designed to assess the security standards of TLS implementations. He has enhanced the functionality of TLSAssistant, an advanced tool designed to optimize the configuration of TLS protocols for both web servers and Android applications. Riccardo excels in automating user configuration verification, meticulously adhering to guidelines set forth by esteemed organizations such as NIST, BSI, ANSSI, AgID, and Mozilla. Riccardo successfully resolved the PSA-DSS issue for testssl.sh, thereby capturing the attention of NIST.

Sara S. in FBK, Security and Trust Unit ● Apr, 2023 - Aug, 2023

Sara S. is a brilliant student at the valued Department of Information Engineering and Computer Science, specializing in the ever-changing fields of Computer, Communication, and Electronic Engineering. In her innovative thesis, she delves into the realm of gamification as a powerful tool to elevate cybersecurity awareness programs. Her research revolves around the ingenious concept of presenting cybersecurity content in a manner that is both engaging and impactful. By emphasizing the cultivation of good cyber habits and promoting responsible online conduct, she aims to revolutionize the way we approach cybersecurity education. The candidate conducts in-depth analysis of the theoretical underpinnings and elements of gamification, culminating in the development of a groundbreaking and versatile framework specifically designed for the implementation of cybersecurity awareness initiatives. She has made an important breakthrough in the field of learning enhancement by developing a comprehensive framework that seamlessly integrates approximately fifty papers into a singular, powerful solution.

Internship Tutor

Riccardo G. in FBK, Security and Trust Unit ● Feb, 2023 - Apr, 2023

Riccardo G., an outstanding student, has successfully developed a groundbreaking module designed to assess the security standards of TLS implementations. He has enhanced the functionality of TLSAssistant, an advanced tool designed to optimize the configuration of TLS protocols for both web servers and Android applications. Riccardo excels in automating user configuration verification, meticulously adhering to guidelines set forth by esteemed organizations such as NIST, BSI, ANSSI, AgID, and Mozilla. Riccardo successfully developed a highly efficient database system for the purpose of storing and managing researchers' datasets. The dataset encompassed a diverse range of guideline requirements. Furthermore, the individual adeptly employed testssl.sh, a cutting-edge tool within the TLSAssistant suite, to successfully extract valuable user data. Implemented and integrated the cutting-edge methodology into TLSAssistant as a seamlessly functioning module. Riccardo has successfully developed cutting-edge algorithms that excel in validating user input and parsing complex conditions.Riccardo successfully resolved the PSA-DSS issue for testssl.sh, thereby capturing the attention of NIST.

Andrea B. and Mattia A. in FBK, Security and Trust Unit ● *Jun, 2022 - Jul, 2022 ~ Aug, 2023 - Sep, 2023*

Andrea B. and Mattia A. are two outstanding students from Istituto Tecnico Tecnologico Buonarroti (Trento, Italy). They readily comprehended complicated topics like as databases and overflow threats despite just being in their third year. They are working with me and my colleague Salvatore Manfredi on a project that will raise awareness about security postures (e.g. password management, phishing awareness and more).

Federica M. and Davide M. in FBK, Security and Trust Unit ● *Jul, 2023*

Federica M. and Davide M., two talented pupils from Istituto Tecnico Tecnologico Buonarroti Trento, have successfully developed engaging and interactive videos that effectively explain cognitive biases in cybersecurity. Their videos are designed to be easily comprehensible by all viewers, making the complex subject accessible to a wide audience. They were given guidance on the necessary measures they can take to perform and safeguard themselves against threats so that they can better understand these hazards.

Matilde S. and Mattia C. in FBK, Security and Trust Unit ● *Jun, 2023 - Jul, 2023*

Matilde S. and Mattia C. are two brilliant students hailing from Liceo Steam Rovereto and Istituto Tecnico Tecnologico Buonarroti Trento, respectively, in Italy. They have successfully acquired knowledge in Open Source Intelligence (OSINT) and social media risk assessment. The students successfully acquired the skills necessary to conduct a digital investigation, including the collection of data from online sources. They showed proficiency in analyzing multiple social media platforms and evaluating an individual's "digital footprint" based on the information available.

Federico C. in FBK, Security and Trust Unit ● *Feb, 2022 - Apr, 2022*

I had the opportunity to oversee Federico C., an undergraduate student at University of Trento, thanks to my colleague Salvatore Manfredi. Federico did an excellent job by collecting information on overall webserver use and, more specifically, Public Administration in Italy. Upon learning that NGINX was competing with APACHE, he included several mitigations into NGINX and developed a parser for TLSAssistant.

The parser can quickly scan an NGINX configuration and automatically repair any TLS vulnerabilities discovered. Federico was finally able to analyze the TLS environment in deep and correct additional flaws he discovered in the tool.

Ivan V. in FBK, Security and Trust Unit ● *Feb, 2022 - Apr, 2022*

Thanks to my colleague Salvatore Manfredi, I have overseen the internship of an undergraduate student at University of Trento, Ivan V. . Ivan, a talented student, researched the TLS area to see what new threats had emerged. Ivan encountered ALPACA, Racoon, Zombie POODLE, Golden DOODLE, 0-Length OpenSSL, and Sleeping POODLE after researching the literature. Using POODLE variations as a starting point, Ivan investigated the optimal method for integrating these vulnerability checks into TLSAssistant. Ivan progressively included all prior vulnerability assessments (i.e. ALPACA, POODLE variants and Racoon). Not only did he incorporate them into our tool, but he also corrected and made the external tool TLSScanner more efficient by statistically demonstrating it by scanning the Alexa top 50,000 websites.

Public Events

Notte Della Ricerca 2023: SIAMO AL SICURO? METTIAMOCI ALLA PROVA! (58)

Un viaggio nel mondo della sicurezza informatica - Museo della Scienza MUSE ● Sept 29, 2023

Through games and hands-on demonstrations, various topics related to cybersecurity will be presented. The most dangerous cyber attacks will be explored, as well as the behaviors to be adopted to ensure maximum protection of online data privacy and digital identity.

Wired Next Fest 2023: Cybersecurity non è solo roba da nerd

Ex-Scuole Damiano Chiesa, Rovereto ● May, 2023

Child grooming, posting sensitive information online and/or on social media, ransomware that takes control of your data for ransom. All threats that the latest device and constantly updated antivirus can help protect against, but not enough. Human error often opens the floodgates and destroys the best defenses. Thus, cybersecurity begins with culture. Learn the first and most important defense methods to protect your data and family.

Cybersecurity: the experience of two young professionals

LiceoSteam, Rovereto ● Apr, 2023

Dialogue with Giada Sciarretta and Matteo Rizzi, two experts from the Center for Cyber Security at the Bruno Kessler Foundation who will share their career paths, showing how one can get to play important roles in cybersecurity and digital innovation by following different paths. The discussion was also an opportunity to understand the importance of digital security in public administration and to stimulate students' interest in cybersecurity with real-world examples.

Projects

Security of the Trentino eHealth Infrastructure

APSS - Provincia Autonoma di Trento and Fondazione Bruno Kessler ● Sept, 2023 - Present

In an innovative collaboration between eHealth and FBK, a cutting-edge initiative has been undertaken to enhance the Sanitary system of Trentino. This ambitious project aims to fortify the infrastructure and application with a robust layer of cybersecurity, ensuring the utmost protection of citizens' personal and sensitive information against potential external threats.

European Digital Identity Wallet

Authentication flows, issuing and safe storage of the documents ● 2022 - Present

I am currently engaged in an esteemed partnership between Istituto Poligrafico and Zecca dello Stato, collaborating under the valued banner of FBK. Our focus lies in the realm of cybersecurity, specifically in the development of The European Identity Wallet. This groundbreaking initiative entails the creation of a sophisticated personal digital wallet, empowering individuals to seamlessly authenticate their identities, securely store crucial documents, and efficiently manage their electronic records.

Linux Hardening for Banks

Allitude - Cassa Centrale Banca ● Jul, 2023

Development of comprehensive guidelines for enhancing the security of Linux servers and systems, with a specific focus on fortifying the operating systems and kernels utilized within banking environments.

Multi-CIE System

Ideation of the Multi-CIE function in the CieID App ● Jan, 2022 - March, 2022

The CieID App allows users to verify themselves for public services in Italy by using the CIE Card, commonly known as Carta di Identità Elettronica (eID card). Worked as part of a team to develop the best method for storing multiple eID cards in the APP while keeping the highest level of security and determining the optimum balance of security and usability.

breaking-telegram

PoC script to break Telegram ● 2021

Simple PoC script that allows you to exploit telegram's "send with timer" feature by saving any media received with this functionality, automatically.

TLSAssistant

Starting from Version 1.3 ● 2020 - Present

Fully-featured tool that combines state-of-the-art TLS analyzers with a report system that suggests appropriate mitigations and shows the full set of viable attacks.

iHashDNA

Perceptual hashing library in python ● 2020 - 2022 (Suspended)

Python library to easily check if two images are similar without machine learning by using Perceptual Hashing (phash and whash combined), with ban and unban image system.

Minor Works

Threat-intelligence-telegram

A bot to quickly get information about an IP using threat intelligence. ● 2023

Mallodroid

Conversion in Python 3 and enhancements ● 2020 - 2021

telegram-deep-fakes-bot

Easy implementation and use of the first order model ● 2020

Rappresentanti Bot

HelpDesk Telegram bot to support DISI Students in University of Trento ● 2019

Education

University of Trento (Trento, Italy)

Bachelor of Computer Science ● Sept, 2017 - Mar, 2021

Thesis in *TLS Analyzers for Android Apps - State-of-the-art Analysis and Integration in TLSAssistant.*

I.I.S. Primo Levi (Badia Polesine, Italy)

High School Diploma ● Sept, 2012 - Sept, 2017

Final elaborate in *psychoanalysis of James Joyce and the artificial intelligences*.

Certifications

CyberWiser - CyberRange And Capacity Building in CyberSecurity

Module	Date	Certificate
P-01-M-01	May 19, 2021	Download
P-01-M-02	May 20, 2021	Download
P-02	May 20, 2021	Download
P-03	May 20, 2021	Download
P-04	May 25, 2021	Download
P-05	June 4, 2021	Download
P-06	June 4, 2021	Download

Microsoft

Module	Date	Certificate
Into the Breach	February 07, 2023	Verify
Microsoft Azure Security Technologies (A)	March 07, 2023	Download

First Certificate

Cambridge Assessment English - B2 ● Apr, 2017

ECDL Base

ECDL / ICDL Certification ● May, 2016

Technical and Programming Skills

I am widely proficient in everything that touches the cybersecurity realm. My areas of expertise include security testing, vulnerability assessment, cyberrisk assessment, network security (e.g. DmZ, firewalls, honeypots), privacy, trust, OSINT, and digital identity. During the Machine Learning course, I worked with advanced deep learning systems (such as a convolutional neural network to identify Covid-19 from radiography, in 2020), achieved the highest gpa in multimedia data security (e.g. invisible and visible watermarking, compression resistant watermarking and classifying differences from video compression applied by Facebook and Youtube). I also earned the highest GPA in the Offensive Technologies course, in which I learned how to perform attack and defense in the cyberspace.

Throughout my career, I have discovered numerous flaws —some of them critical— in the infrastructures used by the Fondazione Bruno Kessler. I was also able to collaborate with the Postal Police while researching new technologies in the field. In addition, I managed to analyze the CIEApp (Carta Identità Elettronica) with the Open Web Application Security Project (OWASP). Threat intelligence is a topic that deeply interests me.

Programming Skills

Language	Knowledge Level
Python, Java, C (and C++), SQL	*Proficient*
Kotlin, PHP	*Intermediate*
RUST	*Basic (willing to improve)*
JS, PolyML, R, ASM	*Basic*

Known Standards

Name	Common Name	Level
ISO 23220	Building blocks for identity management via mobile devices	Proficient
ISO 18013-5	Mobile Driving License	Proficient
ISO 29003	Identity proofing	Proficient
ISO 29115	Entity authentication assurance framework	Proficient
EUDI Wallet Framework	European Digital Identity Architecture and Reference Framework	Proficient
NIST 800-63-3	Digital Identity Guidelines	Intermediate
ISO 27001	Information security management systems, Requirements	Basic
NIST 800-53	Security and Privacy Controls for Information Systems and Organizations	Basic
RFC 3227	Guidelines for Evidence Collection and Archiving	Basic

Interests and Soft Skills

Work Interests

What i really want to do in my future ● 2023

I am passionate about *CyberSecurity, Privacy, Forensics and Digital Identity*, as well as the solutions that embrace these areas, which include (but are *not limited to*) *Security Protocol Analysis, Access Control, Zero-Trust and Zero-Knowledge methods, Malware Analysis and AI-Powered CyberSecurity*. I am particularly intrigued by the idea of developing novel solutions and conducting scientific research in these fields.

University of Trento (Trento, Italy)

Student Representative for DISI ● Nov, 2018 - Nov, 2022

Department Of Information Engineering And Computer Science

Press on the QR to download the PDF