Michele Guerra

[redacted]

PRESENTAZIONE

Nato il [redacted]a), il mio percorso accademico ha iniziato a prendere forma all'Università degli Studi del Molise, dove ho conseguito la laurea triennale in Informatica. Qui, sotto la preziosa guida del Prof. Rocco Oliveto e con la collaborazione del Prof. Simone Scalabrino, ho sviluppato e difeso con successo la mia tesi "OCELOT: generazione automatica di casi di test in CLion", un primo passo significativo nel mio viaggio accademico. Proseguendo con determinazione, ho ottenuto la laurea magistrale in Sicurezza dei Sistemi Software, ancora presso l'Università del Molise. Durante questo capitolo della mia formazione, ho presentato "TensorBot: un assistente conversazionale basato su AI per la libreria Tensorflow a supporto dello sviluppatore", un progetto guidato dal Prof. Oliveto, con la co-supervisione del Prof. Gabriele Bavota dall'Università della Svizzera Italiana, dove ho trascorso un periodo di studio, e del Prof. Scalabrino. Questo periodo è stato arricchito anche da una collaborazione con la CCIAA, grazie a una borsa di studio che mi ha permesso di approfondire ulteriormente le mie ricerche. Nel 2021, il mio impegno e la mia passione per la ricerca mi hanno portato ad intraprendere il dottorato di ricerca presso l'UNIMOL, nei laboratori Mosaic e StakeLab, dove ho avuto l'onore di essere guidato da un team di esperti: il Prof. Fausto Fasano ed il Prof. Rocco Oliveto, con la preziosa collaborazione del Prof. Simone Scalabrino. Oggi mi appresto a coronare questo percorso con la difesa della mia tesi di dottorato intitolata "Enhancing Mobile User Privacy through a Context Aware Permission Model", un contributo significativo al campo della privacy degli utenti Android, che riflette il mio impegno verso la ricerca e l'innovazione.

ESPERIENZA LAVORATIVA

2021 – ATTUALE University of Molise, Italia

ESPERIENZE D'INSEGNAMENTO

- Istruttore di laboratorio/Assistente didattico per il corso di laurea triennale in **Programmazione Mobile** tenuto da Fausto Fasano.
- Istruttore di laboratorio/Assistente didattico per il corso di laurea triennale in **Ingegneria del Software** tenuto da Fausto Fasano.
- Istruttore di laboratorio/Assistente didattico per il corso di laurea magistrale in **Software Project Management** tenuto da Fausto Fasano

09/2023 – 01/2024 Abu Dhabi, Emirati arabi uniti

DOTTORANDO IN VISITA PRESSO LA NYU ABU DHABI NEW YORK UNIVERSITY

Durante il mio soggiorno di ricerca all'estero di tre mesi per il dottorato, ho avuto l'opportunità di contribuire a un progetto di ricerca presso il Center fo Cyber Security presso la New York University di Abu Dhabi. Sotto la guida esperta della Professoressa Christina Pöpper, mi sono dedicato allo sviluppo di un framework di sicurezza per l'User Equipment (UE) Android nel contesto delle reti 5G Standalone (SA), creando essenzialmente un Framework di Test di Sicurezza Lato Utente per il 5G Standalone. Il mio contributo principale al progetto è stato lo sviluppo di un sistema automatizzato per la generazione di casi di test, focalizzandomi sulle comunicazioni in uplink e downlink nelle reti 5G SA, con un'attenzione particolare ai messaggi NAS (Non Access Stratum) e RRC (Radio Resource Control). In parallelo, ho esplorato l'applicazione di Large Language Models (LLM) come ChatGPT e Llama2 per la valutazione e la validazione automatica dei risultati dei casi di test (file pcap).

29/02/2020 – 04/04/2020 Lugano, Svizzera

STUDENTE DI MASTER IN VISITA ALL'UNIVERSITÀ DELLA SVIZZERA ITALIANA A LUGANO UNIVERSITÀ DELLA SVIZZERA ITALIANA

Durante questo periodo, sono stato ospite dell'Università della Svizzera Italiana a Lugano, dove ho sviluppato la mia tesi di laurea magistrale con il Prof. Gabriele Bavota e il Prof. Rocco Oliveto nel campo del supporto agli sviluppatori da parte di assistenti virtuali basati su modelli di Machine Learning.

2021 – 2022
COLLABORAZIONE PER ATTIVITÀ DI SUPPORTO NELLA GESTIONE DEL PROGRAMMA DI MASTER MASTER POST-LAUREA IN TECNOLOGIE DELL'INFORMAZIONE PER L'INNOVAZIONE E LA COMPETITIVITÀ.

01/09/2019 – 01/09/2020
BORSA DI STUDIO PER PROGETTO DI RICERCA. UNIVERSITÀ DEGLI STUDI DEL MOLISE

Ho ottenuto una borsa di studio per lavorare su un progetto in collaborazione con l'Università degli Studi del Molise e la CCIAA Molise.

ISTRUZIONE E FORMAZIONE

03/2021 – ATTUALE Pesche (IS), Italia
STUDENTE DI DOTTORATO IN SCIENZE APPLICATE Università degli Studi del Molise

Attualmente sono un dottorando presso l'Università degli Studi del Molise (Italia), sotto la guida del Prof. Fausto Fasano e del Prof. Rocco Oliveto. Lavoro presso il STAKE Lab (Laboratorio di Ingegneria del Software e del Conoscimento) e il Centro di Ricerca MOSAIC, affrontando tematiche legate alla Privacy e Sicurezza degli utenti Android e all'Analisi Dinamica dell'utilizzo dei permessi e delle risorse critiche in Android.

01/10/2018 – 26/10/2020 Pesche(IS), Italia
LAUREA MAGISTRALE IN SICUREZZA DEI SISTEMI SOFTWARE Università degli studi del Molise, Pesche, Molise (IT)

Durante il mio percorso di laurea magistrale, ho avuto l'opportunità di ampliare le mie competenze e arricchire le mie conoscenze partecipando a vari progetti di ricerca che spaziavano dai metodi formali, all'AI. Nel corso dello sviluppo del mio progetto di tesi, ho trascorso un periodo presso l'Università della Svizzera Italiana a Lugano, dove ho collaborato con il Prof. Gabriele Bavota. Ho difeso con successo la mia tesi di laurea magistrale nell'ottobre 2020 con una votazione di 110L.

Voto finale 110 cum laude

10/2015 – 25/10/2018 Pesche(IS), Italia
LAUREA TRIENNALE IN INFORMATICA Università degli studi del Molise, Pesche, Molise (IT)

Durante la mia laurea triennale, ho costruito una solida base in informatica e, nell'ultimo anno, ho avuto l'opportunità di lavorare su un progetto di ricerca riguardante la generazione automatica di casi di test in C. Questo progetto mi ha portato a una tesi sperimentale, sotto la supervisione del Prof. Rocco Oliveto. Mi sono laureato (con lode) nell'ottobre 2018, difendendo con successo la mia tesi.

Voto finale 110 cum laude

COMPETENZE LINGUISTICHE

Lingua madre: **ITALIANO**

Altre lingue:

	COMPRENSIONE		ESPRESSIONE ORALE		SCRITTURA
	Ascolto	Lettura	Produzione orale	Interazione orale	
INGLESE	B2	B2	B2	B2	B2
FRANCESE	A1	A1	A1	A1	A1

Livelli: A1 e A2: Livello elementare B1 e B2: Livello intermedio C1 e C2: Livello avanzato

ULTERIORI INFORMAZIONI

PUBBLICAZIONI

Visual Attention and Privacy Indicators in Android: Insights from Eye Tracking – 2024
Guerra, M.; Milanese, R.; Deodato, M.; Perozzi, V. and Fasano, F.

In today's digital landscape, where privacy preservation is of paramount importance, Android has implemented new features to enhance transparency: the Privacy Indicators (PIs). Our study employs eye-tracking technology to investigate how users perceive and interact with these indicators. As a visual alert system, PIs signal when sensitive resources, like camera or microphone, are in use. However, the structure of Android's permission model, susceptible to exploitation by malevolent or commercial apps, places an excessive responsibility on PIs. They act as the final alert for users against the misuse of permissions in unexpected contexts. We conducted a controlled experiment with 29 participants who were exposed to various privacy scenarios while their eye movements were tracked and recorded. Our findings reveal a significant gap in PIs effectiveness, particularly in high-engagement tasks, indicating a need for more eye-catching privacy notifications. These findings suggest the need for redesigning some privacy interfaces to make them more effective. The study's insights contribute to the broader discussion on balancing functionality with user privacy and the methodology of utilizing eye tracking in user experience research.

ICISSP 2024 - 10th International Conference on Information Systems Security and Privacy

An Empirical Study on the Effectiveness of Privacy Indicators – 2023
M. Guerra, S. Scalabrino, F. Fasano and R. Oliveto

The increasing diffusion of mobile devices and their integration with sophisticated hardware and software components has promoted the development of numerous applications in which developers find new ingenious ways to exploit the possibilities offered by the access to resources such as cameras, biometric sensors, and GPS receivers. As a result, we are increasingly used to seeing applications that make extensive use of sensitive resources, potentially dangerous for our privacy. To address this problem, the latest approach to support user awareness in terms of privacy is represented by the Privacy Indicators (PI), a software solution implemented by the operating system to provide a visual stimulus to inform users whenever a dangerous resource is exploited by the app. However, the effectiveness of this approach has not been assessed yet. In this article, we present the result of a study on the effectiveness of using the PI to inform the user every time an app accesses the mobile device camera or microphone. We have chosen these two resources as the PI are currently implemented only for a very limited number of permissions. The controlled experiment involved 122 Android users who were asked to complete a series of tasks on their smartphone through prototypes using the involved resources in an explicit and latent way. Although the PI mechanism is very similar between Android and iOS, we have decided to focus on the former due to its greater diffusion. The results show no significant correlation between the use of PI and the detection of the resource being used by the app, suggesting that the effectiveness of PI in improving sensitive-related resources usage awareness, as currently implemented, is still unsatisfactory. In order to understand if the problem was due to the specific implementation of the PI, we implemented an enhanced version and compared it with the standard one. The results confirmed that an implementation that makes the indicators more visible and that is clearer in highlighting the fact that the app is accessing a resource improves the resources usage awareness.

IEEE Transactions on Software Engineering, vol. 49, no. 10, pp. 4610-4623

A Dynamic Approach to Defuse Logic Bombs in Android Applications – 2023
Fausto Fasano, **Michele Guerra**, Roberto Milanese, and Rocco Oliveto

Logic bombs are a critical security threat in Android applications that can be triggered by specific events or conditions, leading to serious consequences. In this work we focus on apps accessing mobile device resources for sensitive data leakage. Such malicious behaviour can exploit Android permission model by gaining access to sensitive related resources in a legitimate context and later using them in a dangerous one, once the logic bomb is triggered. We propose a dynamic approach by extending RPCDroid, a tool that monitors the behavior of an Android application whenever it accesses specific device resources. To defuse the logic bomb we force an explicit prompt to authorize access requests based on the usage context preventing accesses unbeknownst to the user. We assessed the effectiveness of our proposal using TriggerZoo, a publicly available dataset of apps injected with logic bombs. Our results show that a context aware permission model can effectively prevent uncontrolled access to privacy related data in case a logic bomb is triggered.

DBSec 2023 Data and Applications Security and Privacy XXXVII

RPCDroid: Runtime Identification of Permission Usage Contexts in Android Applications – 2023

Guerra, M.; Milanese, R.; Oliveto, R. and Fasano, F.

Over the years, there has been an explosion in the app market offering users a wide range of functionalities especially since modern devices are equipped with many hardware resources such as cameras, GPS, and so on. Unfortunately, this is sometimes associated to indiscriminate access to sensitive data. This exposes users to security and privacy risks because, although resource usage requires explicit user authorization, once permission is granted, a mobile application is usually free to access the corresponding resource until the permission is expressly revoked or the app is uninstalled. In this work, we introduce RPCDroid, a dynamic analysis tool for run-time tracking of the behavior (UI events and used permissions) of Android mobile applications that use device resources requiring dangerous permissions. We assessed the effectiveness of the tool to identify usage contexts, discriminating between different kinds of access to the same sensitive resource. We executed RPCDroid on a set of popular applications obtaining evidence that, in many cases, mobile applications access to the same resource though different user interactions.

ICISSP 2023 - 9th International Conference on Information Systems Security and Privacy

Dangerous Permissions in Android: Open Issues and Pitfalls – 2022

The increasing diffusion of mobile devices has promoted the development of numerous applications in which developers find new ways to exploit the possibilities offered by access to resources such as the camera. As a result, we are increasingly used to seeing applications that make extensive use of sensitive-related resources, potentially dangerous for our privacy. To address this problem, the latest approach to support user awareness in terms of privacy is represented by the Privacy Indicators(PI), a solution implemented by Android to provide a visual led to inform users whenever the app exploits a dangerous resource. For these reasons, our goal was to investigate the effectiveness of PI in helping users identify the use of a resource. We also wanted to investigate the behavior of applications in terms of permissions used and possible malicious behavior at runtime. As a final goal, we proposed a software solution that protects users from misused permissions.

Ph.D. Expo UNIMOL

CPMDroid: Analysis of Contextualized Permission Usage for Malicious App Detection in Android – 2022

User Authentication through Keystroke Dynamics by means of Model Checking: A Proposal – 2019

The current authentication systems based on password and pin code are not enough to guarantee attacks from malicious users. For this reason, in the last years, several studies are proposed with the aim to identify the users basing on their typing dynamics. In this paper, we propose the adoption of formal methods to discriminate between different users by exploiting a set of keystroke features. The idea behind the proposed method is to identify the users silently and continuously during their typing on a monitored system. To perform such user identification effectively, we consider a feature vector able to capture the typing style that is specific to each given user. By considering this feature model, in detail we propose to consider model checking with logic temporal properties to discriminate between different users using a set of keystroke features.

2019 IEEE International Conference on Big Data (Big Data)

OCELOT: a search-based test-data generation tool for C – 2018

Automatically generating test cases plays an important role to reduce the time spent by developers during the testing phase. In last years, several approaches have been proposed to tackle such a problem: amongst others, search-based techniques have been shown to be particularly promising. In this paper we describe Ocelot, a search-based tool for the automatic generation of test cases in C. Ocelot allows practitioners to write skeletons of test cases for their programs and researchers to easily implement and experiment new approaches for automatic test-data generation. We show that Ocelot achieves a higher coverage compared to a competitive tool in 81% of the cases. Ocelot is publicly available to support both researchers and practitioners.

ASE 18: Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering

CONFERENZE E SEMINARI

Presentations at conferences

- ICSE 2024 - International Conference on Software Engineering
- ICISSP 2024 -International Conference on Information Systems Security and Privacy
- DBsec 2023 - Conference on Data and Applications Security and Privacy

- ICISSP 2023 - International Conference on Information Systems Security and Privacy
- Applied Sciences Ph.D. Research Track: New Research Frontiers at the University of Molise
- Ph. D. Expo Unimol

Participation in Conferences, Doctoral Schools and Courses

- ACNS 2024 - 22nd International Conference on Applied Cryptography and Network Security | Abu Dhabi, UAE
- SIESTA 2019 - International Summer School on Software Engineering
- BigDat 2020, 6th International Winter School on Big Data, per complessive 41 ore di lezione
- Global Game Jam 2020 presso l'Università degli Studi del Molise
- USI Hackathon 2019 presso l'Università della Svizzara Italiana
- SANER 2017

PROGETTI

2022 – ATTUALE

App Unimol Manutenzione evolutiva e correttiva dell'applicazione mobile dell'Università degli Studi del Molise (realizzata con il framework Ionic), supervisione del progetto e coordinamento del lavoro degli sviluppatori secondo la metodologia Scrum, predisposizione e configurazione dei tool di CI/CD (repository condiviso, issue tracker, pipeline per il controllo della qualità del codice, pipeline per la build automatica, ...), attività di code review, quality assurance e formazione degli sviluppatori.

Link https://play.google.com/store/apps/details?id=it.unimol.app.studenti&hl=it&gl=US

2020 – 2023

Sito web di Ateneo UNIMOL Ideazione, sviluppo e manutenzione del sito web di Ateneo dell'Università degli Studi del Molise (realizzato in Wordpress).

Link https://www2.unimol.it/