UNIVERSITÀ DEGLI STUDI DI GENOVA | Dibris

Department of Informatics,
Bioengineering, Robotics,
and Systems Engineering

1st Workshop on Trustworthy Software Ecosystems

March 24, 2021, 09:30-13:15

DIBRIS - University of Genoa

Abstract

Over the years, pervasive computing and communication technologies have fostered new computing paradigms such as the Internet of Things (IoT), Cloud, and Mobile Computing. The ubiquity of these paradigms, their expandability, and their applicability in different problem spaces have made them invaluable in modern computing solutions.

At the same time, however, security becomes a real concern, especially since these systems moved from single, isolated paradigms to complex ecosystems built by the fruitful interactions among several computing paradigms.

The workshop's primary goal is to discuss the many aspects of security and privacy of emerging software ecosystems, with a specific focus on Mobile, IoT, and Cloud computing platforms. The event focuses on these emerging environments by covering the entire ecosystem lifecycle, from the secure design to the notions of security during development (DevSecOps) and operations (VA/PT and risk assessment). The workshop hosts four speakers:

- Eleonora Losiouk, Postdoc at SPRITZ Lab, University of Padova (Italy)
- Henrik Plate, Senior Researcher at SAP (France);
- Andrea Saracino, Researcher at CNR-IIT (Italy)
- Luca Verderame, Postdoc at CSEC Lab, University of Genova (Italy);

Registration & Venue

The workshop will take place online on Google Meet. The event is **completely free** for the participants.

To join the workshop, please register to the Eventbrite event using the link below.

https://www.eventbrite.it/e/biglietti-1st-workshop-on-trustworthy-software-ecosystems-141830977271

At the end of the registration process, each participant will receive the details to join the online event.

Detailed Program

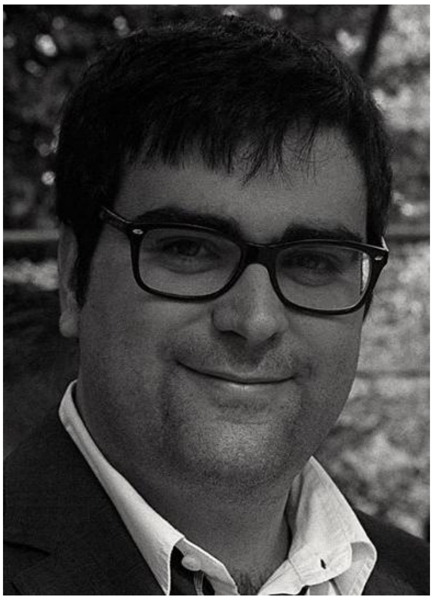
09:30 - 09:45	Registration & Welcome
	SESSION 1 (Moderator: Alessio Merlo)
09:45 - 10:30	**Emerging software ecosystems: a glimpse of challenges and opportunities** Luca Verderame, University of Genoa
10:30 - 11:15	**The Android Virtualization Technique: a Double-Edged Sword for Developing Attacks and Defences** Eleonora Losiouk, University of Padua
11:15 - 11:30	Break
	SESSION 2 (Moderator: Luca Verderame)
11:30 - 12:15	**Threats to the Secure Consumption of Open Source** Henrik Plate, SAP
12:15 - 13:00	**Security and Privacy in Smart Home ecosystems** Andrea Saracino, CNR-IIT of Pisa
13:00 - 13:15	Closing Remarks

Organization & Contacts

Luca Verderame - University of Genoa - luca.verderame@unige.it

Speakers

Luca Verderame



Luca Verderame is a Postdoc research fellow at the Computer Security Laboratory (CSEC Lab) of the University of Genoa (Italy), and the CEO and Co-founder of Talos, a cybersecurity startup and university spin-off.
In 2016 Luca obtained his Ph.D. in Electronic, Information, Robotics and Telecommunication Engineering at the University of Genoa. During his master thesis in 2012, Luca found a severe security vulnerability in the Android operating system and worked with the Android Security Team to develop a patch. His current research interests mainly cover information security applied, in particular, to mobile and IoT environments, as witnessed by his research publications in the field.

Talk Title: “The security tale of emerging software ecosystems: a journey of challenges and opportunities.”

Over the years, pervasive computing and communication technologies have enabled the emergence of new computing paradigms that have gained momentum across a broad spectrum of domains.
In particular, emerging computing paradigms like Mobile, IoT, and Cloud Computing are becoming even more interconnected, thereby moving from single, isolated paradigms to complex ecosystems built by the fruitful interactions among several computing paradigms.
From a security standpoint, this leads to novel and unprecedented attack threats. To deal with such threats, applying state-of-the-art security analysis techniques on single paradigms can be insufficient. Thus, novel analysis methodologies that systematically analyze the entire ecosystem life cycle must be put forward.
This talk will unveil the research challenges and opportunities for the security evaluation of these emerging environments by covering the full ecosystem lifecycle, from the secure design to the notions of security during development (DevSecOps) and operations (VA/PT and risk assessment).

Eleonora Losiouk

Eleonora Losiouk is a Postdoc Fellow working in the SPRITZ Group of the University of Padova, Italy. In 2018, she obtained her Ph.D. in Bioengineering and Bioinformatics from the University of Pavia, Italy. She has been a Visiting Fellow at EPFL in 2017. Her main research interests regard the security and privacy evaluation of the Android Operating System and the Information-Centric Networking. She has been recently awarded a Fulbright Fellowship for visiting the International Computer Science Institute in Berkeley, USA e received the Seal of Excellence for her Marie Skłodowska-Curie individual project proposal.

Talk Title: The Android Virtualization Technique: a Double-Edged Sword for Developing Attacks and Defences

Android virtualization enables an app to create a virtual environment, in which other apps can run. Originally designed to overcome the limitations of mobile apps dimensions, nowadays this technique is becoming more and more attractive for developing novel Android malwares and defence mechanisms. During this talk, I will illustrate two use cases that refer to a malicious and a legitimate usage of the Android virtualization technique, respectively.

Concerning the malicious usage, I will introduce Mascara, the first repackaging attack that exploits the virtualization technique and bypasses the existing countermeasures. Mascara is executed by a malicious app, that looks like the add-on of a victim app. However, the malicious add-on creates a virtual environment where the victim app is executed together with additional attacker's code and attacked. Mascara leverages on the design features of virtual environment to launch its attack, meanwhile being resilient to any runtime detection mechanism against Android virtualization.

Considering the legitimate usage of the virtualization, I will present a privacy issue that concerns the Android app ecosystem. In particular, an mHealth app installed on a user's phone can reveal sensitive information about the user's health. Due to Android's open design, any app, even without permissions, can easily check for the presence of a specific app or collect the entire list of installed apps on the phone. Many third parties are interested in such information: our survey of 2917 popular apps in the Google Play Store shows that around 57% of these apps explicitly query for the list of installed apps. Therefore, we designed and implemented HideMyApp (HMA), an effective and practical solution that relies on the definition of virtual environment where sensitive apps can run, meanwhile being hidden by the Android

OS and other installed apps. HMA does not require any changes to the Android operating system or to apps yet still supports their key functionalities.

Henrik Plate

Henrik Plate is a senior researcher at SAP Security Research. He received his MSc in Computer Science and Business Administration in 1999 from the University of Mannheim and holds a CISSP certification. His current interest focuses on the security of open source software supply chains, and he is a co-author of Eclipse Steady, which supports the detection, assessment and mitigation of vulnerable code in Java and Python applications. Prior research topics include security policies and configuration validation.

Talk Title: Threats to the Secure Consumption of Open Source

Open source software is omnipresent, all across the technology stack, on every device, both in commercial and non-commercial software. But recent years saw an increase of attacks leveraging the security issues of today's open source supply chains, e.g., the Equifax data breach, which was due to the use of a component with known vulnerabilities, or the supply chain attack on the npm package event-stream, with which malicious code was injected into binaries downloaded millions of times every week. This presentation will provide an overview about the current threat landscape and discuss on-going community efforts aiming to overcome those issues and (re)establish developer trust into open source ecosystems and infrastructures.

Andrea Saracino

Andrea Saracino (Ph.D. 2015, M.Eng. 2011) is a Researcher at Institute of Informatics and Telematics of the National Research Council of Italy. His research is focused on security of mobile and distributed systems, with an emphasis on intrusion and malware detection in Android devices. He is also interested in access and usage control applied to mobile and cloud systems. He is the project coordinator of the H2020 project SIFIS-Home (GA#

952652) and he is (or has been) involved in a number of EU-project such as EU-H2020 Cybersane, EU-H2020 C3ISP, EU-H2020 NeCS, EU-H2020 Cybersure, EIT-Digital Trusted Cloud and IoT.

Talk Title: “Security and Privacy in Smart Home ecosystems”

Smart-home are increasingly raising concerns related to cybersecurity. Threatened by smart device vulnerabilities, increased attention by attackers and with their direct effect on the physical world and their capability to monitor the private life of users, smart homes are a hot topic for security research. In this presentation we are going to survey the main security issues typical of smart home environments and we will analyse approaches for handling security, based on security by design approach, techniques for intrusion detection and enforcement of data privacy with a focus on privacy preserving analysis of multimedia streams.