From Software Security Assessment to Security Benchmark

Nuno Antunes, ***University of Coimbra, Portugal,***
nmsa@dei.uc.pt
Address: Departamento de Engenharia Informática
Polo II - Pinhal de Marrocos
3030-290 Coimbra
Portugal
Phone no: +351 916657134

Marco Vieira, ***University of Coimbra, Portugal***
mvieira@dei.uc.pt

Objective, abstract, and duration of the tutorial

Measuring security and comparing systems according to their security is that illusory possibility that every system administrator or architect would like to have. Benchmarking is a "solved" problem in many domains, with performance benchmarks being widely adopted by industry and research, and even dependability benchmarks having already a well-established set of approaches in terms of the research community. The same is not true for security benchmarking.

On the other hand, there is a wide body of techniques and tools that allow for the assessment of system security, including modeling, analysis and testing techniques, each of them applicable in their specific domain, and with specific advantages or disadvantages that makes them more or less fit to the multiple scenarios. However, comparing systems based on the output of these techniques is not so useful, as they are prepared to find problems, which are to be corrected. *After these problems are corrected, what is left to us to compare?*

In this tutorial we will discuss the problematic of security benchmarking from both theoretical and practical perspectives and understand why it is so much difficult to benchmark security than other quality attributes of the system. We will see new approaches that can provide information to help selecting the best alternatives in terms of security. We will also see that there are many interesting open research challenges to be tackled to achieve security benchmarks.

The tutorial will address both current research topics and engineering practice. Case studies will be presented, and future research opportunities will be identified and discussed.

Duration: this tutorial will use half-day.

Outline with approximate timings

1) Introduction

Estimated duration: 20 minutes

This part will *introduce the speakers* and review the necessary background to better understand the material to be presented afterwards. To this end, we will introduce the most important concepts on *software security* including the most relevant security threats. We will also discuss the importance of assessment the security of different systems.

Finally, we will overview the *structure of the tutorial*, to provide the audience with a better insight on the contents to be presented and on the goals to be achieved.

2) Benchmarking Concepts and Dependability Benchmarking

Estimated duration: 45 minutes

This part will cover the notions of benchmarking in general as well as discuss the key concepts behind dependability benchmarking.

We will start from the key concepts of benchmarking, illustrated with the main strategies adopted for the well-known and established performance benchmarking. We will present the typical components of a benchmark, and the properties that it must respect. We will then present strategies for dependability benchmarking, which are well known in the research community although still less adopted in industry practices.

Finally, we will approach resilience benchmarking concepts, as the natural evolution of dependability benchmarking.

3) Security Assessments Techniques and Tools

Estimated duration: 50 minutes

This part will cover the main techniques and tools used for security assessment of different types of systems. We will consider techniques that must be applied manually, but also the ones that can be performed using automated tools, we will delve into the details of their application in practice in real systems and scenarios. We will analyze the merits and limitations of each strategy and discuss when each is the most adequate one. The techniques and tools that we are going to discuss include both research and industry products.

It concludes discussing why all of these activities are not security benchmarking and how far we are from benchmarking when considering security assessment activities.

4) Security Benchmarking: Challenges and Solutions

Estimated duration: 50 minutes

This part will discuss in detail what is different in security that makes it such a difficult property to be benchmarked. Starting from several literature attempts at proposing security

benchmarks, we will discuss the key points in which each one of them took us closer to the goal, and why each one of them did not succeed.

After this, we will present solutions and different techniques that can help solve different parts of the problem. In particular, we will discuss trustworthiness assessment techniques, which more recently are gaining space as an alternative to provide ways to compare systems according to different properties, including security. From this particular perspective, we will discuss what is done and what still the main open research challenges.

5) Closing remarks

Estimated duration: 15 minutes

Based on the conclusions of the previous part, here we will wrap up the tutorial with the discussion of the future potential research directions.

Target audience

The intended audience of this tutorial is researchers and practitioners interested in learning the state-of-the-art on techniques and tools to mitigate the impact of software vulnerabilities. Although we will cover some of the tools used in industry practices nowadays, the attendees do not need previous experience with them, as we will present and discuss how they work. Nevertheless, in the beginning of the tutorial we will set the ground by briefly presenting key background concepts. This way, the only prerequisites necessary is to understand the basic concepts on computer systems dependability and security.

Takeaways:

It is important to emphasize that this is a topic of utmost importance for researchers and practitioners working on computer systems.

In fact, the ascendance of networked information in our economy and daily lives, and the increasing dependence on software applications in general, shows the importance of understanding the best techniques to evaluate and compare different solutions in terms of security. During the tutorial participants will understand the key concepts behind benchmarking, security assessment and learn different approaches to tackle the difficult problem of comparing different systems according to security.

The tutorial will follow a discussion-based approach (including a brainstorming activity close to the end of the tutorial). Attendees will be asked to comment on several aspects related to the topic in general and to the presented case studies in particular. With this we intend to improve discussion dynamics and make participants to share their experience and their understanding regarding this topic.

Proposers Track Record

Nuno Antunes <nmsa@dei.uc.pt> – University of Coimbra, Portugal
https://eden.dei.uc.pt/~nmsa/ Phone: +351 916657134

Nuno Antunes is an assistant professor at the University of Coimbra, where he received his PhD in Information Science and Technology in 2014. Since 2008 he has been researching topics related with detection of software vulnerabilities and assessment of security and dependability in software systems. His work with benchmarking includes techniques for evaluating and comparing techniques and tools to support the assessment of software security. He has participated in many research projects, both at the national and European level.

Marco Vieira <mvieira@dei.uc.pt> – University of Coimbra, Portugal
https://eden.dei.uc.pt/~mvieira/

Marco Vieira is a Full professor at the University of Coimbra, Portugal. He is an expert on security assessment and benchmarking, dependability benchmarking, experimental dependability evaluation, fault injection, and software quality assurance, subjects in which he has authored or coauthored more than 170 papers in refereed conferences and journals. His work on benchmarking has started in 2000 and is widely referenced in the literature. He has participated in more than 20 research projects, both at the national and European level. Marco Vieira has served as PC-chair of ISSRE 2015, EDCC 2018, LADC 2016, DSN 2018, among others.

History of the tutorial

This will be the first presentation of the tutorial.

Supporting materials

This tutorial we be mostly based on brand new material, including a set of slides and a compendium of literature for the attendees' future reference.

The proposers of this tutorial have a large experience on teaching and research in dependability and security topics, including security testing, vulnerability detection and benchmarking. In particular, some of the topic discussed in the tutorial are discussed in the classes of the new University of Coimbra's Master in Security of Informatics.

Although we propose to develop new materials for the tutorial, these will be obviously based on the high quality works available in the literature, which are very well known by the tutorial presenters.