

Tutorial Proposal

Dimitrios Serpanos
Computer Technology Institute and Press DIOPHANTUS
University of Patras, Professor
serpanos@cti.gr

1 Title: Malware Analysis and Detection

2. Abstract

Malicious software threatens the security of computer systems from desktops to cloud servers, from mobile devices to industrial systems. Malware is increasingly used by threatening actors to target private corporations, public organizations and critical infrastructures as well as individuals. Recent cases of attacks, such as SolarWinds attack and the ransomware attacks on Advantech, Canon and Cognizan, are only a few publicly known cases, that demonstrate the extent and importance of the problem. Such attacks have significant financial impact, due to damages, and lead to data leakage with unpredictable and long-term consequences. Current estimates are that the yearly cost of malware is above \$ 6 trillion by 2021, while more than 350,000 new malware samples and potentially unwanted applications are detected every day.

Significant effort is spent to design effective and efficient malware analysis and detection systems. These efforts include the use of program sample features derived from static analysis as well as from dynamic analysis. In static analysis, features are extracted from binary files without executing them. As static analysis is limited due to obfuscated malware, dynamic analysis is employed as well, where suspicious programs are executed in virtual environments and measurements are made. Features and measurements from static and dynamic analyses are provided to classifiers, which differentiate malware from benign programs, using classification techniques. Such classifiers typically employ machine learning techniques such as random forests, support vector machines and, increasingly, deep learning neural networks. In the latter case, significant amounts of reliable data are required for effective and efficient training of the classifiers.

In this tutorial, we will present malware analysis and detection techniques and tools. First, we will cover techniques and tools for static analysis and then, we will cover dynamic analysis ones. We will present common and advanced classifiers, addressing also the problem of data availability. Finally, we will present a complete, open software platform that combines static and dynamic analysis as well classifiers for effective malware detection.

3. Objectives:

To present state-of-the-art methods and tools for malware analysis and detection, covering all stages of analysis -static and dynamic- and classification.

4. Topics covered:

The tutorial will cover all aspects of malware analysis and will present tools and examples for popular operating systems (Windows, Linux, Android). The covered topics include:

- Principles of malware analysis and detection
- Static analysis
- Dynamic analysis
- Malware classification

- Open problems and future directions

5. Projected Audience/Background:

Researchers, professionals and graduate students active or interested in malware analysis. The needed background is basic knowledge in computer security, programming, operating systems, and machine learning.

6. Tutorial content:

- Introduction to malware analysis and detection
- Static analysis methods and tools
- Dynamic analysis methods and tools
- Malware classification methods
- Open software malware analysis and detection platform
- Open problems and future directions

7. Physical/Virtual presentation: the tutorial can be delivered either in-person or through teleconference.

8. Presenter Experience:

The presenter has long and strong experience in presentation of research results (more than 100 conference papers) and has given 3 tutorials as follows:

- A. Lalos, C. Koulamas and D. Serpanos, "Secure and Efficient Industrial IoT: Architectures and Technologies." CPS&IoT'2021 Summer School on Cyber-Physical Systems and Internet-of-Things, Budva, Montenegro, June 9, 2021 [1.5 hours].
- A. Kalogeras, C. Koulamas and D. Serpanos, "Industrial Internet-of-Things: Architectures, Designs and Challenges." DATE 2018, Dresden, Germany, March 19, 2018 [4hours].
- S. Mukhopadhyay, D. Serpanos and M. Wolf, "Internet-of-Things: Design Methodologies and Tools for the Internet-of-Things." DATE 2016, Dresden, Germany, March 14, 2016 [3 hours].

9. Presenter Bio

Dimitrios Serpanos is President of the Computer Technology Institute and Press DIOPHANTUS (CTI) and Professor of Electrical and Computer Engineering at the University of Patras, Greece. He holds a PhD and MA in Computer Science from Princeton University (1990 and 1988, respectively) and a Diploma in Computer Engineering and Informatics from the University of Patras (1985). His research interests include cybersecurity, cyber-physical and embedded systems, and computer architecture.

Before joining the University of Patras in 2000, he served as faculty at the Department of Computer Science at the University of Crete (1996-2000) and as Research Staff Member at IBM Research, T.J. Watson Research Center (1990-1996). During 2013-2016, he was Principal Scientist at the Qatar Computing Research Institute (QCRI).

He has served as President of the University of Western Greece (2010-2013) and as Director of the Industrial Systems Institute (ISI)/ATHENA for two terms (2016-2021 and 2008-2013).

Professor Serpanos has received the Golden Core Award from the IEEE Computer Society (2017). He served on the IEEE CS Board of Governors (2017-2020), where he was Secretary (2020) and Treasurer (2019). He is a Senior Member of the IEEE and a member of ACM, NYAS, and AAAS.