# Accepted Manuscript

A Cloud-based platform for the emulation of complex cybersecurity scenarios

Angelo Furfaro, Antonio Piccolo, Andrea Parise, Luciano Argento, Domenico Saccà

PII: S0167-739X(16)30704-X
DOI: https://doi.org/10.1016/j.future.2018.07.025
Reference: FUTURE 4343

To appear in: *Future Generation Computer Systems*

Received date : 30 November 2016
Revised date : 4 April 2018
Accepted date : 14 July 2018

Please cite this article as: A. Furfaro, A. Piccolo, A. Parise, L. Argento, D. Saccà, A Cloud-based platform for the emulation of complex cybersecurity scenarios, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.07.025

# A Cloud-based Platform for the Emulation of Complex Cybersecurity Scenarios[☆]

Angelo Furfaro[a,b,*], Antonio Piccolo[a,b], Andrea Parise[b], Luciano Argento[a], Domenico Saccà[a]

[a] *DIMES, University of Calabria – P. Bucci 41C, 87036 – Rende (CS), Italy*
[b] *Open Knowledge Technologies srl – Piazza Vermicelli, 87036 – Rende (CS), Italy*

**Abstract**

In the last few years, cybersecurity has become a hot topic because of the ever-increasing availability of Internet accessible services driven by the diffusion of connected devices. The consequent exposition to cyber threats demands for suitable methodologies, techniques and tools allowing to adequately handle issues arising in such a complex domain. This paper describes the architecture of SmallWorld, a scalable software platform designed to reproduce realistic scenarios achieved by the immersion of real systems into a software defined virtual environment. SmallWorld enables the assessment, teaching and learning of cybersecurity related aspects in different areas and for various purposes. It exploits innovative and state-of-the-art virtualization and simulation techniques for reproducing in a realistic setting a dynamic environment where large distributed computer systems can be deployed and from where they can interact with real life entities. One of the main features of SmallWorld is the support for designing and building complex scenarios which are dynamic and reactive and where a number of autonomous software agents can be deployed. Agents are able to reproduce the behaviors of human users and/or malicious applications into a SmallWorld scenario making it a more realistic testing environment. The practical use of SmallWorld is shown by means of two realistic case studies.

*Keywords:* cybersecurity, virtual environments, cloud-based systems

## 1. Introduction

Cybersecurity issues have an ever increasing social-economical impact both for citizens and enterprises. The success of a single cyber attack can lead to enormous financial losses, theft of intellectual property and loss of customer confidence and trust. It was estimated that cybercrime has a comprehensive monetary impact of billions of dollars per year, on society and government [1]. If we consider that last year saw a total of 304 million cyberattacks samples [2], more than a quarter of all malware samples ever recorded were produced in 2015 (27.63%), with Trojans, PUPs (Potentially Unwanted Programs) and distinct families of Cryptolocker causing considerable damage among larger businesses worldwide, the overall picture is extremely alarming. Therefore the availability of tools allowing to learn how to handle cyber space threats and to assess the effectiveness of prevention and defense solutions, is critical for the safeness of IT services. Traditionally, security assessment and penetration testing activities are performed on real networks while the training of security specialists is made on insulated and static virtualized systems. As stated in [3], the cost of cyber crime can be moderated by deploying enterprise security governance practices. The presence

[☆] A preliminary version of this paper appeared in the Proceedings of the 2nd IEEE International Conference on Cloud Computing Technologies and Applications (CloudTech 2016), Marrakesh, Morocco, 2016.

[*] Corresponding author

*Email addresses:* a.furfaro@dimes.unical.it (Angelo Furfaro), a.piccolo@dimes.unical.it (Antonio Piccolo), andrea.parise@okt-srl.com (Andrea Parise), l.argento@dimes.unical.it (Luciano Argento), sacca@unical.it (Domenico Saccà)