Chapter 1
A Black-Box Framework for Malicious Traffic Detection in ICT Environments

Carlos Alberto M. S. Teles
Federal Center for Technological Education of Rio de Janeiro (CEFET-RJ), Brazil

Carlos Roberto Gonçalves Viana Filho
Federal Center for Technological Education of Rio de Janeiro (CEFET-RJ), Brazil

Felipe da Rocha Henriques
Federal Center for Technological Education of Rio de Janeiro (CEFET-RJ), Brazil

ABSTRACT

Information security is gradually becoming an area that plays an important role in our daily lives as information and communications technology assets grow with increasingly connected environments. Increasingly we have information from society having their data leaked due to information security flaws in both hardware and software of ICT assets. To identify failures of ICT assets, through the detection of malicious traffic, this chapter proposes a black-box-based framework that aims to detect malicious traffic. The black-box method allows monitor the network without accessing the software or hardware details. In the proposed framework, information security and network resource usage are used together in order to provide a reliable detection of malicious traffic. Firstly, the authors collected network traffic information, generating a dataset from open source networking tools. The proposed detection scheme can identify risks and threats like malware, suspect traffic, and others. The scheme was validated verifying the correlation between network security alerts and network resource usage.

DOI: 10.4018/978-1-7998-5728-0.ch001

INTRODUCTION

The security of today's technological environments is highly dependent on the proper behavior of the various Information and Communications Technology assets that make up them – where ICT assets are used to contemplate all kind of hardware and software capable of performing computational processing and engaged in information technology and communications activities. The term ICT refers to the combination of computer with telecommunications technologies and has in computer networks, and especially on the Internet, its greatest expression (Miranda, 2016). In fact, the inadequate functioning of a simple element of a computer system, whether hardware or software, can compromise the entire security of that system. It is therefore essential to develop mechanisms to ascertain and attest that ICT assets meet desirable security requirements. This objective, however, is a huge challenge, as the ICT assets used in today's computer systems become increasingly complex. ICT assets are at into increasingly critical activities and relevant to the society's well-being.

One approach that has gained increasing strength in the compliance of products, services, processes, systems and people to regulatory requirements is the implementation of Conformity Assessment Programs (CPAs) (Fernandes, 2011). These programs deal systematically, using traditional quality management techniques, such as inspections, tests, sampling and audits, to analyze compliance with pre-established requirements in standards and regulations, for each product, process, service or professional under evaluation. Conformity Assessment programs are already used in various areas to verify compliance with the most diverse types of requirements, including calibration of measurement instruments, energy efficiency, electromagnetic compatibility, radiation detection, thermal insulation, ergonomics and civil construction (Inmetro, 2019).

In the area of ICT asset security, the use of CPAs to verify compliance with cybersecurity requirements has gained a strong impulse in the last decade with the publication of international standards ISO/IEC 15408-1:2009 (Information technology - Evaluation criteria for IT security) and ISO/IEC 19790:2012 (Information technology - Security techniques - Security requirements for cryptographic modules) (Leszczyna, 2018). However, even if the area of information security is moving towards international standardization and the search for systematic testing procedures for conformity assessment, the evaluation of ICT assets includes advanced technical challenges arising from the complexity of the behavior of such assets, which requires research to develop systematic and conclusive tests.

In recent years, there have been cases of compromised ICT assets (Kirtley & Memmel, 2018). Several models of babysitting suffered security incidents, where in some cases there was the sending of scary audios to children, in addition to the theft of access credentials to Apple and Google stores, and the improper obtaining of the authorization of other users to remotely view and control the monitor. According to (Cziesla, Kemper, Muntermann, & Sinanaj, 2015), several companies have had their data breached by the NSA through security breaches in ICT assets. In (Restuccia, D'Oro, & Melodia, 2018), it has been proven that internet-connected cars, through Internet of Things (IoT) devices, can be controlled remotely. More worrying cases, however, involve medical devices and can have fatal consequences in the event of failure (Restuccia, D'Oro, & Melodia, 2018).

Addressing information security issues of ICT assets has become an important issue. Thus, the U.S. Senate recently proposed the 2017 IoT Bipartisan Cybersecurity Improvements Act, which aims to boost Information Security on Internet-connected devices (Restuccia, D'Oro, & Melodia, 2018). According to a study by (Chen, Woo, Brumley, & Egele, 2016), through the extraction and evaluation of vulnerabilities in embedded devices, it was found that the highest incidence of failures is in the network layer. Thus,