Trustiness Certification of Information Technology Equipment

Manuel Pedro Coelho[†] and Rui Miguel Silva[††],

Lab UbiNET – Computer Science Security and Cybercrime
Polytechnic Institute of Beja, 7800-295 Beja, Portugal

Summary
This paper proposes a system, which assigns trustiness certification to information technology equipment through a series of tests and evaluations. This system is based in a methodology that should be applied in a laboratory, which issues a technical report containing the results of all the methodology steps, including the results of the testing and evaluation, any detected occurrences and the obtained assurance level of trustiness. Both the laboratory and the technical report should be accredited by the respective national competent bodies. This system allows the certification of information technology equipment and in this paper we exemplify with the certification of a desktop computer.

Key words:
Trustiness, Certification, Intrusion detection system, Network Security, Cyber security, Cybercrime

1. Introduction

From the moment the Internet connects all places worldwide, the risks and threats to Information security were enhanced. Cybercrime grows in parallel with the evolution of applications and services that operate in Cyberspace, and takes advantage of the fact that in most cases there are always vulnerabilities that can be exploited. This new wave of crime is reflected in a growing number of Cyber attacks on various organizations and institutions with the purpose to obtain, modify or destroy Information. Also Cyber-espionage between states stems from the increasing use and dependence on Information Technologies (IT) in all sectors of modern societies. Obtaining sensitive Information of a nation can be crucial at a time of tension allowing Cyber attacks to compromise their technological structures. Cyberspace is likely to be appointed as the 5th Field of War, relegating to the background the traditional armed attacks. IT Equipment favor a whole new volume of criminal possibilities, which tend to be more serious when they involve structures like government, military, financial, or other organizations that somehow involve the sovereignty of a country. It is common that purchased IT equipment by organizations, be not subject of a behavioral validation, testing or a trustiness certification, and simply inserted into the organization's network installed only with traditional security applications such as antivirus and firewall. Without trustiness certification of new IT equipment we cannot be sure at the outset that they were not compromised with some sort of malware at some point of their life cycle, thus facilitating access from outside as soon as they are integrated into a computer network. This paper aims to contribute to the process of ensuring safety, through the specification of a system to assess the trustiness of IT equipment integrated into computer networks.

1.1 Cyberspace Events and Compromised Equipment

In recent years there have been some events in Cyberspace related to Cybercrime, Cyber espionage or Cyber warfare and several studies, news papers, and detected cases of new IT equipment such as routers, switches, computers, somehow compromised with some kinds of malware.
Events like the Russia-Georgia crisis back in 2008, where a large scale of attacks against computer networks, websites and state services on the Cyberspace, took place at the same time the land attacks were carry out [1].
Another important event was the Stuxnet malware discovered in 2010. It was designed to attack specific industrial control systems and ensure their control, namely, the operating system SCADA developed by Siemens. The final target was to control Iranian centrifuges for uranium enrichment [2].
The Operation b70 carried out by Microsoft in 2011, conducted an investigation in order to analyze some new computers purchased in different Chinese cities. As result, the malware Nitol was discovered in some analyzed computers [3].
In 2012, two researchers from the Computer Laboratory of the University of Cambridge, Sergei Skorobogatov and Christopher Woods , published a paper called "Breakthrough silicon scanning discovers backdoor in military chip", with the summary of their investigation into the discovery of a backdoor in a chip used in military weapons and equipment [4].
These are only some examples that justify the need of a system like the one proposed in this paper, which can certify trustiness in IT equipment.

2. Background Situation

The interest on IT equipment security is not such a recent concern as it might look like. The United States of America (USA) Government created the Trusted Computer System

Manuscript received December 5, 2013
Manuscript revised December 20, 2013

Evaluation Criteria (TCSEC), also called Orange Book, back in 1985. The criteria defined in this manual classified the automatic processing information systems in hierarchical divisions of safety and security and also provided a basis for evaluating the security effectiveness of controls embedded in those systems [5].
In Europe, back in 1991, after France, Germany, Netherlands and the United Kingdom, based on their own work in this area and with the scope to create a composition and recognition of security standards at an European scale, published the Information Technology Security Evaluation Criteria (ITSEC) as an evaluation standard for structured security systems [6].
These standards experienced some modifications, and other approaches such as the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) also played a role in these matters. Nowadays they tend to fall into disuse and their evolution points to a greater flexibility in specifying the targets of evaluation and an increasing number of products for a wider range of assessment targets, covering different goals and different areas of society.
Although these standards provided directives for security evaluation of IT equipment, there were no trustiness certification of these equipment based in particular tests and evaluations that can assure they were not compromised.

3. Present Situation

There are some recent documentation and initiatives, related to IT security and Information security. This section gives a global overview on this subject.
In terms of equipment certifications the USA have the CSA international organization that performs testing and certification of products according to certain national and international standards and mark them with that indication. The main goal is to facilitate trade of products through a brand that is recognized by both manufacturers and consumers [7].
In Europe there is as indication of conformity which is CE marking that symbolizes conformity to all the obligations of manufacturers concerning to their products due to certain community policies. The CE Marking is one form of harmonization and unification of procedures, standards and legislation with the purpose of achieving a "single European market" promoting harmonious economic and social development among the various member states [8].
There are also some institutes and laboratories such as the USA National Institute of Standards and Technology (NIST) whose mission is to promote innovation and industrial competitiveness through mechanisms of scientific measurement and quantification of standards and technology to enhance and improve the security, and thus the economy and quality of life [9].
In Europe there is the European Telecommunications Standards Institute (ETSI) whose mission is to produce and coordinate the maintenance of accepted and used standards by its members in the area of Information Technologies and Communication. In these organizations, like in many other standardization organizations, much of its work is carried out by committees and working groups, which are composed by experts and specialists in specific areas. ETSI produces European Standards, Technical Specifications, Technical Reports and Guides with rules, guidelines, advice and recommendations for standardization at European level [10].
Other well-known organization who produces standards in this area is the International Organization for Standardization (ISO). ISO is a network composed by 164 countries and 3335 technical bodies, responsible for the development of standards. ISO standards can bring to organizations, technological, economic and social benefits by helping to harmonize technical specifications of products and services, thus making the industry more efficient and breaking down barriers to international trade benefits. There are some standards related to IT security such as “ISO/IEC 15408-1:2009 - Information technology - Security techniques - Evaluation criteria for IT security”, “ISO/IEC TR 15443-1:2005 - Information technology - Security techniques - A framework for IT security assurance”, “ISO/IEC 27001:2005 – Information technology - Security techniques - Information security management systems”, “ISO/IEC 27003:2010 - Information technology - Security techniques - Information security management system implementation guidance”, among others [11].
The Common Criteria for Information Technology Security Evaluation (CC) is an international standard produced in order to unify all the others related with IT Equipment security, like TCSEC, ITSEC or CTCPEC. CC is the driving force for the widest available mutual recognition of secure IT products. The CC and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that products can be evaluated by competent and independent licensed Laboratories so as to determine the fulfilment of particular security properties, to a certain extent or assurance [12]. The CC tend to be a reference security evaluation standard, enhanced with its acceptance by the ISO.
Although these examples of documentation, organizations and initiatives provide guidelines for implementation of security measures in some IT equipment and systems, specific assurance requisites such as behavioral validation, communications analysis, hardware inside testing, and other tests that can grant and certify new equipment isn’t compromised, aren’t proposed and performed by most organizations. The next sections propose a System which includes a Laboratory, an Ontology and a Methodology in order to certify the trustiness of IT equipment.

4. Laboratory Proposal

In order to certify an IT equipment, it must be first tested and evaluated in a controlled environment, that is, a

Certification Laboratory. This environment must combine safety with expertise in this area and must meet certain requirements.

The ISO "17025 - General requirements for the competence of testing and calibration laboratories", is applied to many laboratories that require specific safety and technical requirements such as forensic, and testing and calibration of sensitive instruments laboratories. This International Standard specifies the general requirements for the competence to carry out tests using standard methods, non-standard methods, and Laboratory-developed methods [13].

The requirements split in two categories: (1) Management requirements which cover matters like: Organization, Management system, Document control, Subcontracting of tests and calibrations, Service to the customer, Control of nonconforming testing and/or calibration work, Corrective action, Internal and Additional audits, Preventive action, Technical records, Management reviews, among others. (2) Technical requirements which cover matters like: Personnel, Accommodation and environmental conditions, Test and calibration methods and method validation, Laboratory-developed methods, Non-standard methods, Validation of methods, Estimation of uncertainty of measurement, Control of data, Equipment, Measurement traceability, Reference standards and reference materials, among others [13].

Once the Laboratory is certified by the national competent bodies according to ISO 17025, it would cover all the needed conditions to perform all required procedures on IT equipment. We additionally propose that the Laboratory must fit inside a Faraday Jail to avoid any kind of uncontrolled communications between the equipment and the exterior world.

5. Ontology Proposal

This section proposes the formalization of an "Ontology for IT Equipment" in order to perform a classification of the equipment in IT equipment classes and associate them with behaviors classes in order to verify which equipment can be tested and evaluated and what types of behaviors should be analyzed.

We can define ontology as an explicit specification of a conceptualization. The term is borrowed from philosophy, where ontology is a systematic account of Existence. For knowledge-based systems, what "exists" is exactly that which can be represented. When the knowledge of a domain is represented in a declarative formalism, the set of objects that can be represented is called the universe of discourse. This set of objects, and the describable relationships among them, are

reflected in the representational vocabulary with which a knowledge-based program represents knowledge [14].

An ontology allows formalizing knowledge about a particular area and sharing this between people and systems. In this sense it is also a goal and a feature of ontologies, that they could be modified and improved, so that they can be used in a larger context in order to serve different purposes in their area.

The process of construction and formalization of an ontology should follow a methodology, use a formal language and adequate tools to aid the process. There are several possibilities, some proprietary and some open-source, some more complex and with more specificities than others. We use the Development 101 Methodology, the Ontology Web Language – OWL and the tool Protégé. This combination is all open source, free to use and among the most used ones.

The Development 101 methodology follows seven steps: 1 - Determine the domain and scope of the ontology; 2 - Consider reusing existing ontologies; 3 - Enumerate important terms in the ontology; 4 - Define the classes and the class hierarchy; 5 - Define the properties of classes (slots); 6 - Define the facets of the slots; and 7 - Create instances [18]. This paper does not comprehensively describe each, but present the main issues of the ontology formalization.

OWL ontologies have similar components to Protégé frame based ontologies. However, the terminology used to describe these components is slightly different from that used in Protégé. An OWL ontology consists of Individuals, Properties, and Classes, which roughly correspond to Protégé frames Instances, Slots and Classes. Individuals, represent objects in the domain in which we are interested. Properties are binary relations on individuals, linking two individuals together. Classes are interpreted as sets that contain individuals [19].

In Protégé, some information was added, such as the project name, description, version, date, and then created the Classes. Two main Classes were created "IT Equipment" and "IT Equipment Behavior Analysis". In the first one, two Subclasses were created "A Equipment capable of connecting directly to the network" and "B Equipment incapable of connecting directly to the network" and in the second one other two Subclasses "C Directly related communications behavior analysis" and "C Indirectly related communications behavior analysis". This classification is due to the fact that the IT equipment communications are the way through which the threats are spread. These steps are illustrated in Figure 1.

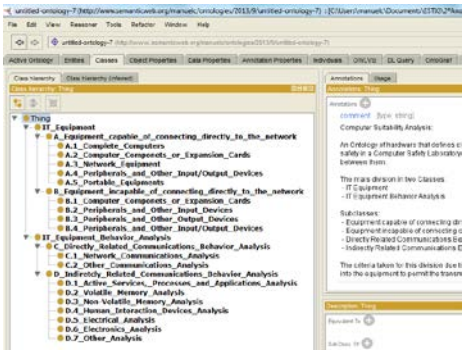

Figure 1 – Ontology Class creation in Protégé

The Individuals, which represent the Class A and B equipment suitable of testing and the Class C and D behaviors to test and evaluate, were created each one assigned to a specific Subclass by the "type" property, as illustrated in Figure 2.

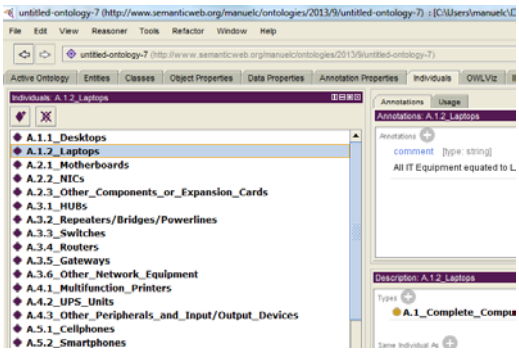

Figure 2 - Ontology Individuals creation in Protégé

After the previous steps, two Properties were created: "doAnalysis" and "doAllAnalysis". The first one relates one Individual from the "IT Equipment" Class with one Individual from "IT Equipment Behavior Analysis" Class, in order to perform only one type of testing from this last Class. When a set of tests are needed, then one Individual must be related to a Class. Once the Classes are hierarchical, this means that all Subclasses and Individuals are related, and all tests should be performed.
Figure 3 illustrates the Property "doAnalysis" for the Class "C.1.1 - Wired Network Communications Analysis" that specifies the tests and analysis that should be performed to the IT equipment.

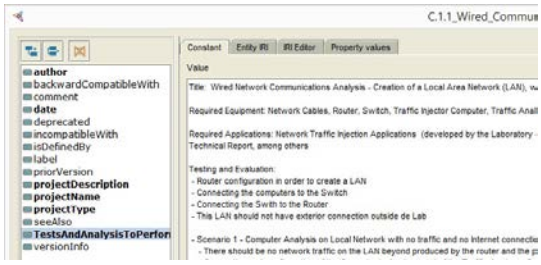

Figure 3 - Property "doAnalysis" for Ontology Class C.1.1

With this ontology is now possible to classify IT equipment into classes and verify what tests and evaluation should be done. An ontology systematization table is proposed in order to resume the ontology, the equipment characteristics and classifications, which tests should be done and other relevant information the Laboratory consider important.

6. Methodology Proposal

This section proposes a methodology for Trustiness Certification of IT Equipment, by the proposed Laboratory using the proposed Ontology.

We present and summary describe the set of steps to be followed by the Laboratory personal that conducts to the certification of the equipment, with a certain level of trustiness. The proposed methodology starts with entrance of the equipment into the Laboratory and ends with the emission of a report for the national competent organizations,.

Figure 4 illustrates the proposed methodology.

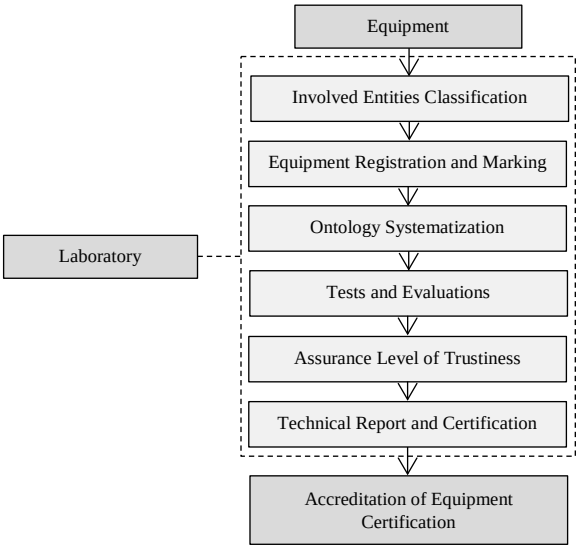

Figure 4 –Methodology for Trustiness Certification of IT Equipment

The "Involved Entities Classification" step specifies all the entities that participate in the whole process (manufacturer, client, Laboratory and the accreditation body details). In the "Equipment Registration and Marking" step all the elements should be marked and registered in a database (equipment, manuals, schemes). The "Ontology Systematization" step should be the result of the equipment classification by the ontology (an IT equipment should be classified in a Class which will be associated to an Individual or a Class of tests to be performed). The "Tests and Evaluations" step will perform the actions described in the previous step (the Laboratory should have access to any test results performed by the manufacturer, perform a network traffic sniffing and analysis in the target organization where the IT equipment will operate, conduct independent functional tests and analysis based on the ontology specifications, perform penetration testing and perform testing with other specific security software). The "Assurance Level of Trustiness" step will assign a grade off assurance, based on any registered events (a 5 scale is proposed depending on the number and type of detected anomalies). The "Technical Report and Certification" should be based on a document template and include all the methodology step results and descriptions (this document will be the result of all the procedures to the IT equipment and should be used as base for the certification.). The "Accreditation of Equipment

Certification" step will be performed by the national competent organizations, by analyzing the Technical Report.

7. Example

This section presents an application example of the Trustiness Certification Methodology of IT Equipment proposed in this paper. We take a common desktop computer as equipment for certification. Due to paper objectives and space constrains, only the most important steps will be presented. Some particular considerations will also be introduced in order to make the example as more reliable as possible.

The selected desktop computer equipment was an ACER Model VERITON X680G with Windows 7 Pro. The Ontology Systematization step resulted in a IT Equipment classification Class "A.1.1 – Desktops" which was associated to the IT Equipment Behavior Analysis Classes "C – Directly Related Communications Behavior Analysis" and "D – Indirectly Related Communications Behavior Analysis".

The "Tests and Evaluations" step will be focused here by specifying de Individual "C.1.1 - Wired Network Communications Analysis". All the other Individuals from Classes C and D are not presented. First, a network traffic packet sniffing on the organization where the IT equipment will work, was performed in several day periods. For this purpose, a tool was developed in order to capture packets and save the results in a "pcap" file format. Although there are several sniffing tools (Kismet, Nmap, Snort, Ntop, TCPdump, or Wireshark), most of them add metadata to "pcap" files, so, the sniffing tool was developed in Python (v.2.7.3) using the capabilities of "scapy", a library that allows a large number of possible operations in the handling of data packets and network operations. Basically the use of "sniff" function [20], can capture a specific number of network packets, as in (1), or perform that capture for a time period, as in (2). The developed tool allows the specification of different time capture intervals (morning.pcap, afternoon.pcap).

packets=sniff(count=int(packet_number)) (1)

packets=sniff(timeout=total_time) (2)

Once the packets are captured, they can be saved into a file using the "wrpcap" function [20], as in (3).

wrpcap("file.pcap", packets) (3)

Figure 5 illustrates the developed sniffing tool.

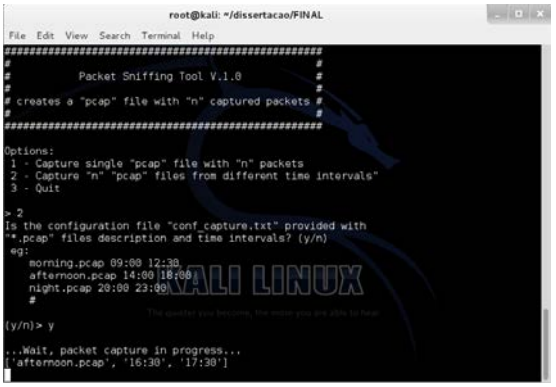

Figure 5 – Configurable sniffing tool

For the C.1.1 Individual, a set of scenarios is proposed, in order to test the desktop. An independent LAN should be configured in the Laboratory, with the purpose of deceive the desktop in test by letting it "think" it is connected to the organizations LAN and "behave" according to that fake scenario. This will be done by injecting the captured network traffic in this controlled LAN environment. An analysis of what the desktop in test send trough it's network card should be performed by a sniffer computer in order to detect behaviors such as sending compromised packets, unknown protocols, big packets, tampered packets, or other strange behaviors that could mean the stealing of Information. Both Packet Injector and Sniffer Computers, run Kali Linux.

Figure 6 illustrates the controlled LAN scenario.

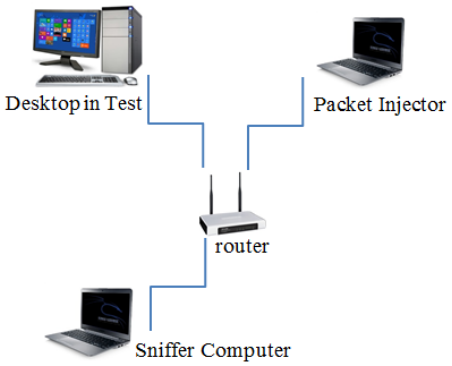

Figure 6 - C.1.1 Individual testing scenario

The injection of the captured network traffic in this controlled LAN environment was made using another developed and configurable tool. This one reads from a file what and how often should the content of "pcap" files be sent to this controlled LAN environment. Like the previous one, this tool was developed in Python and also takes advantage of "scapy" library, by reading the packets from the created files [20], as in (4).

packets=rdpcap("file.pcap") (4)

Once the packets are read, they can be injected using the "sendp" function [20], as in (5).

sendp(packets)
(5)

The sniffing and analysis in this example used Wireshark due to its simplicity, set of options and efficiency. A filter [21] can be created to see only the out coming traffic from the desktop in test, as in (6).

ip.src == 192.168.1.100
(6)

Then some filters [21] can be added in order to scan for suspect behaviors such as in (7) that filters suspect retransmission packets; as in (8) that filters TCP packets with reserved fields different than zero; or as in (9) that filters destination unreachable ICMP packets.

expert.message=="Retransmission (suspected)"
(7)

tcp.flags.res!=0
(8)

icmp.type == 3
(9)

In this example no suspect packets where sniffed so, a Python tool was developed in order to exemplify the detection of abnormal network traffic. This tool can send an ICMP flooding [20], as in (10); TCP packets with reserved fields value different than zero [20] as in (11); or use unknown protocol packets [20], as in (12).

*packet=fragment(IP(dst=IP_dest)/ICMP()/("X"*60000))*
(10)

packet=IP(dst=str(IP_dest))/TCP(reserved=14L, flags="A")

(11)

```
class UnknownP (packet):
(12)
    name="Unknown Protocol"
    fields_desc=[ ShortField("field1",5),
          XByteField("field2",3) ,
          IntEnumField("field3" , 1 ,
          { 1: " field1", 2: " field2" , 3: " field3" } ) ]
```

Figure 7 illustrates the Wireshark detection of a TCP packet with reserved fields value different than zero.

In order to exemplify what a compromised IT equipment can perform without user knowledge, such as collection and transmission of information, two Python tools were developed. These tools take advantage of socket interfaces, by implementing a client/server architecture. The client tool will be executed in the "victim" side (using the Desktop in Test) and the server in the "attacker" side (using the Sniffer Computer). The tools were developed using TCP sockets for Windows systems.

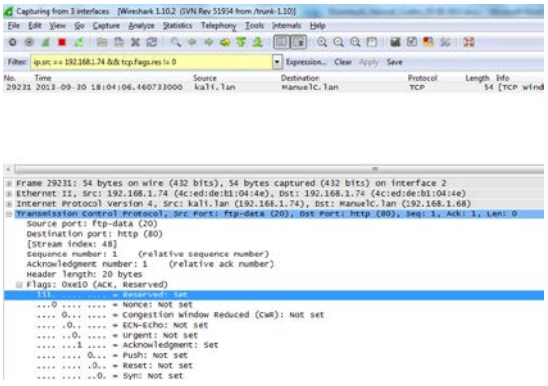

Figure 7 - Wireshark suspect packet detection

The basic operations of the client application are creating the socket [22], as in (13).

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
(13)

Once the socket is created, a port and an address are assigned to it [22]. The port is a non-privileged arbitrary one and the IP address is the one given by the ISP of a 3G router connected to the "attacker" Computer, as in (14). Client waits until server is executed, then makes the connection.

s.connect((HOST, PORT))
(14)

Next step is listening to the receive data by the socket [22], as in (15).

data = s.recv(1024)
(15)

Once some option is received from server, collected information will be sent back. First the client collects information, save it into a file, sends the file to the server and then deletes the file. Examples of collected information are: system information (computer name, routing table, network interfaces, or active process among others), hardware information (computer type, processor type, SO type, or hardware installed among others), registry information (HKEY CLASSES ROOT, HKEY CURRENT USER, or HKEY LOCAL MACHINE among others), a captured photo from the webcam, or an audio captured file from the microphone. The information can be accessed using system calls by importing "os", "sys" [23] and "platform" [24] libraries, as in (16).

call("ipconfig" + " /all >> sys_info.txt", shell=True)
(16)

The photo can be taken using “cam” function by importing “VideoCapture” [25] library, as in (17) and (18).

```
cam = Device()
```
(17)

```
cam.saveSnapshot('photo.jpg')
```
(18)

The audio can be recorded using “stream” function by importing “pyaudio” [26] library, as in (19), (20) and (21).

```
p = pyaudio.PyAudio()
```
(19)

```
stream = p.open(format = FORMAT,
                channels = CHANNELS,
                rate = RATE,
                input = True,
                frames_per_buffer = chunk)
```
(20)

```
all = [ ]
for i in range(0, RATE / chunk * RECORD_SECONDS):
                data = stream.read(chunk)
                all.append(data)
```
(21)

The client application can be camouflaged in order to go unnoticed to the user. For this purpose PyInstaller was used with the options “onefile” and “noconsole”, as in (22), which permits creating only one executable file that will run in background, without any console window [27].

```
python pyinstaller.py –onefile –noconsole client.py
```
(22)

The basic operations of the server application are creating the socket, binding the socket to the port and address, listen for any client and then accept [22] the connection, as in (23).

```
conn, addr = s.accept()
```
(23)

These tools were tested between computers through the Internet, and the “victims” didn’t know what was happening during the client execution. They aim to demonstrate how information can be leaked from infected computers.

These tests and actions are performed in the previously described controlled LAN scenario of the organization where the Desktop in Test will be used. In case it had been compromised with some kind of malware that could be detected by testing and analyzing its hardware, behaviors and communications. Others tests of Individuals from Classes C and D include actions such as testing all other communications interfaces (HDMI, USB, or Bluetooth among others), analysing active services, processes and applications in the system, testing hardware components (Motherboard, RAM, Processor, or Hard Disk among others) with proper equipment, penetration testing to the equipment, among other tests and analysis performed with specific applications and tools.

8. Conclusions and Future Work

This paper addresses the security and trustiness of IT equipment. In modern societies there are a whole new range of threats possibilities such as Cybercrime, Cyber espionage and Cyber warfare, which are facilitated by the increasing use of technologies, and their interconnection through the Internet.

The world situation points to an increasing number of these threats and the sophistication and variety of methods used to engage them. These methods may include use of malware for various purposes, which can be introduced into IT equipment for its dissemination through the Internet or already by infecting new devices. Most companies just acquire the equipment without any trustiness certification, assuming they are free of any threats since they are new.

In order to give a level of assurance to new IT equipment, this paper proposed a trustiness certification system based on a specific methodology and ontology of IT equipment, to be performed by a certified Laboratory. The result of the tests and evaluations performed are included in a technical report that will be accredited by the competent national bodies. The Assurance Level of Trustiness obtained should assure that de equipment is free of any threats.

As future work we consider to continue the development and specification of tests to be performed as well as the implementation of a real world prototype of the proposed Laboratory.

References

[1] U. C. C. Unit, "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," U.S. Cyber Consequences Unit, 2009.

[2] "Symantec," [Online]. Available: http://www.symantec.com /content/en/us/home_homeoffice/html/cybercrimereport/.

[3] Microsoft, "Operation b70 - Nitol Malware Research and Analysis".

[4] S. S. e. C. Woods, "Breakthrough silicon scanning discovers backdoor in military chip," 2012.

[5] U. S. o A. D. o Defense, Trusted Computer System Evaluation Criteria, United States of America: Department of Defense, 1985.

[6] CotE Communities, Information Technology Security Evaluation Criteria-ITSEC, Luxembourg,: Luxembourg: Office for Official Publications of the European Communities, 1991.

[7] C. Group, "CSA International," CSA Group, 2013. [Online]. Available: http://www.csa-international.org.

[8] E. Commission, Guide to the implementation of directives

based on the New Approach and the Global Approach, European Commission, 2000.

[9] U. D. o. Commerce, "National Institute os Standards and Technology," U.S. Department of Commerce, 2013. [Online]. Available: http://www.nist.gov/.

[10] ETSI, "European Telecommunications Standards Institute," ETSI, 2013. [Online]. Available: http://www.etsi.org/.

[11] I. O. f. Standardization, "International Organization for Standardization," International Organization for Standardization, 2013. [Online]. Available: http://www.iso.org.

[12] C. Criteria, "Common Criteria," Common Criteria, 2013. [Online]. Available: http://www.commoncriteriaportal.org/.

[13] ISO/IEC 17025 - General requirements for the competence of testing and calibration laboratories, ISO/IEC , 2005.

[14] T. R. Gruber, "A Translation Approach to Portable Ontology Specifications," Knowledge Systems Laboratory, CS Dept., Stanford University, Stanford, California, 1992.

[15] S. JeongAhKim, "Evaluation of Ontology Development Methodology with CMM-i," *Fifth International Conference on Software Engineering Research, Management and Applications*, 2007.

[16] E. ,. K. B. Tim Berners-Lee (MIT, "W3C," W3C, 2012. [Online]. Available: http://www.w3.org.

[17] S. C. f. B. I. Research, "Protégé," Stanford Center for Biomedical Informatics Research, 2013. [Online]. Available: http://protege.stanford.edu/.

[18] S. University, "Abstract: Ontology Development 101: A Guide to Creating Your First Ontology," Stanford University, 2000. [Online]. Available: http://www.ksl.stanford.edu/people/dlm/papers/ontology-tutorial-noy-mcguinness-abstract.html.

[19] M. Horridge, A Practical Guide To Building OWL Ontologies Using Protégé 4 and CO-ODE Tools, The University Of Manchester, 2011.

[20] P. Biondi, "Scapy," 2010. [Online]. Available: http://www.secdev.org/projects/scapy/doc/index.html.

[21] W. Foundation, "Wireshark," Wireshark Foundation , 2013. [Online]. Available: http://www.wireshark.org/.

[22] P. S. Foundation, "Socket Programming HOWTO," Python Software Foundation, 2013. [Online]. Available: http://docs.python.org/2/howto/sockets.html.

[23] P. S. Foundation, "The Python Standard Library," Python Software Foundation, 2013. [Online]. Available: http://docs.python.org/2.7/library/.

[24] P. S. Foundation, "Access to underlying platform's identifying data," Python Software Foundation, 2013. [Online]. Available: http://docs.python.org/2/library/platform.html.

[25] M. Gritsch, "Video Capture," 2012. [Online]. Available: http://videocapture.sourceforge.net/.

[26] H. Pham, "PyAudio 0.2.7," Python Software Foundation, 2013. [Online]. Available: https://pypi.python.org/pypi/PyAudio/.

[27] G. Bajo, M. Zibricky and H. Goebe, "Pyinstaller," 2013. [Online]. Available: http://www.pyinstaller.org/.

Manuel Pedro Coelho received his B.Sc degree, from the Technology and Management School of the Polytechnic Institute of Beja in Portugal in 2007. Now is concluding his M.Sc. at the same institution in Computer Science Security Engineering. His main focus of research is on Network Security and System Security. He has professional experience on management and administration of computer networks.

Rui Miguel Silva received his B.Sc, M.Sc. and PhD (2009) degrees at Technical Superior Institute from the Technical University of Lisbon in Portugal. He is Professor at the Technology and Management School of the Polytechnic Institute of Beja in Portugal since 1997. Its main research activities are centered on Network Security, Offensive Security and Cryptology for Resource Constrained Devices. He has professional experience form cooperation with some national and international governmental organizations in the domains of cybercrime and cyber security.