Network Profiling: Content Analysis of Users Behavior in Digital Communication Channel

Clara Colombini, Antonio Colella, Marco Mattiucci, Aniello Castiglione

Network Profiling: Content Analysis of Users Behavior in Digital Communication Channel

Clara Maria Colombini[1], Antonio Colella*[2], Marco Mattiucci[3], and Aniello Castiglione[4]

[1] External researcher at University of Milan, University of Milan, I-20100 Italy.
cmcolombini@email.it
[2] Italian Army, Italian Army General Staff
Via XX Settembre, 123
I-00187 Rome, Italy
antonio.colella@esercito.difesa.it
[3] Raggruppamento Carabinieri Investigazioni Scientifiche (RaCIS)
Caserma "Palidoro". Viale di Tor di Quinto, 119 I-00191 Rome, Italy
marco.mattiucci@carabinieri.it
[4] Dipartimento di Informatica "R.M. Capocelli" - University of Salerno
Via Ponte Don Melillo I-84084 Fisciano (SA), Italy
castiglione@ieee.org

Abstract. In this paper, we focus on a method of analysis of data in a digital communication channel, using the Digital Profiling technique. We believe, in fact, that the massive use of cloud computing and pervasive technology compels us to improve the results of investigative analysis, in case of cyber-crime, reducing the times of job and maximizing the outcome. The method suggested highlights relationships between flowing data in a digital communication channel and the behavioral models of a possible intruder that threaten that communication. We have chosen to use the two typical approaches adopted in literature: the *Top-down* to confirm the facts and the *Bottom-up* to to construct the hypotheses.

Keywords: Digital Profiling; Channel Profiling; Intrusion Protection System; User Behavior; Network Profiling

1 Introduction

It is now known that technology development is pushing the communication means towards prompted use of the network. This causes, in the event of an investigation, that Digital Forensics experts are forced to manage enormous masses of data that flow in the channel, in a very short time. Moreover, the growing

* Corresponding Author. Antonio Colella, Italian Army, Italian Army General Staff, Via XX Settembre,123 - I-00187 Rome, Italy - E-Mail: antonio.colella@esercito.difesa.it, phone number +39 06 4735111.

trend of pervasive computing technology increases the need to tightly control the networks that provide access to servers, storage and databases. An important mean for monitoring the networks is the control of network performance and, in particular, the profiling of the network itself, in order to collect and analyze information of flowing traffic that are generated by routers, firewalls and all other network equipment. In this scenario, we believe that additional method of analysis of the data stream is necessary and that this new method should be able to improve the results of investigation, reducing the times at the same time. What we propose here is to apply the technique of analysis of digital profiling [1] to a communication channel in order to extrapolate the patterns useful to find the profiling of user's digital behavior. From these patterns we can obtain a raw "sample profile" that can be used for the automatic comparison during the monitoring operations of the channel. This approach allows to obtain the immediate detection of any "abnormal behavior" that might reveal the implementation of illegal operations. To better present our research we chose to make a brief overview on profiling of cyber-criminals, Network Security and Intrusion Detection System in order to describe the scenario wherein our model has been applied.

2 Cyber-Crime and Profiling

The application of Digital Profiling (DP) technique in the cyberspace is not easy, especially in terms of appropriate investigation method [2]. The main causes can be summarized as follows:

- inappropriate and incomplete documentation on this subject;
- difficulties to combine the human nature with Computer Science paradigms;
- manifested distrust towards traditional criminal profiling and in general psychological investigations.

Behavior of offender can be the same every attack, but it can also be unique to the individual under analysis, and may occur only sporadically. From the offender's point of view, most of what they do when they are committing a crime is acting normally, for them. From another point of view, they are acting out on needs and patterns developed over the life course, some of which may be abnormal needs and patterns. If there are repeated crime scenes (as with a serial or repeat offender), it is much more likely, with proper examination, that any unique behavior, need, and pattern will be uncovered.

Three elements link crimes in a series:

- method of operation (*modus operandi*);
- ritual (signs of fantasy or psychological need);
- signature (unique combinations of behaviors).

Signature, in a hacker behavior for instance, is a sort of "trademark" and reflects a compulsion on the part of criminals to go beyond just committing the

crime to "express themselves", reflecting in some way their personality. In a defacing attack, for instance, this aspect is more evident than in others because the acting of hack is visible to everyone. Anyway, the motivations, actions, and modus operandi of traditional crimes respect to cyber-crimes are different. For example, it appears that as of 2009, we have entered a new era where organized cyber-criminals can operate identity theft and resale operations, as well as, engaged in cyber-war. The approach to hacking as multi-stage process leads to individuate three main stages, that are: casing, scanning, and enumeration. For example, the time of action can change from 48/72 hours of constantly working during a network intrusion, to a longer period such as the operations performed by pedophiles. However, hackers have found ways to streamline the efficiency of the classic methodology. In particular, the most recent development has been the use of viruses and trojans as part of the modus operandi. The difference with the past is that the "new" method uses a virus or trojan that is either custom made or standard and has the same effect as one had been hacked into the target system to install a keylogger. Clearly, the new method is considered easier than the old one.

3 Network Security

Before focusing the new approach to DP we should recall some notions of Network Security to better cover the topics useful to face cyber-criminal challenges. Security of a complex system is an active process that have at least four steps. The process can be considered as a circular structure. These steps are generically as follows [3].

- *Estimation of possibilities*: that is concerning the evaluation of policies, procedures, laws, internal regulations, financial availability, technical skills, etc.. All these possibilities are important to determine if the system is able to defend itself.
- *Implementation of protective barriers*: the barriers to intruders, for instance, are implemented by hardware, software, human factor and security policies. They are built in order to carry out a form of prevention from possible damage and, at same time, to increase the perception of the security degree.
- *Intrusion detection system*: that implies identification of violations of security policies and management system.
- *System Response*: that is the step in which is possible to remedy the problem by classifying the solutions and by finding available means in order to not allow that these problems happen in the future.

Thus, the purpose of the cycled structure is to minimize the risk of loss of resources arising from complexity of system. This risk depends mainly on three factors: the possible threats, the potential vulnerabilities as well as the intrinsic value of the resource.

3.1 Network Intrusion

"A wise man always walks with his head down, humble as the dust - it does not matter how smart you are, how many years you studied, how many accomplishments you have already had, one day you will challenge someone with more knowledge than you, with more cunning, with more skills ... " [4].

An intrusion is a violation of security policies and/or of a secure system management. An intruder in a computer system is primarily a curious person [5]. Just such attitude, in fact, guides the early stages of the intrusion even from a technical standpoint. He seeks to identify, by means just apparently with little risky, system vulnerabilities and other data, such as connections, active services, applications, accessible, available ports, the type of operating system, etc.. After this activity, having had determined the vulnerabilities, the attacker can initiate its action of intrusion revealing his true nature through one of the following activities:

- use of a service available to enter the system apparently;
- use of a service, within the limits of its abilities, making him perform functions not budgeted;
- use of a service in order to determine the fall and to eventually assume the privileges at the wake.

At this point the intrusion can actually be accomplished in several ways:

- Copy, alteration and/or removal of data (files, logs, databases, etc..);
- appropriation of other services;
- ownership of privileges and password(s);
- alteration of the software and creation of backdoors;
- creation of a tunnel to the system being attacked and/or to other systems;
- installation of bots/worms for remote communications or surveys.

All this may continue for some time, at least until the intruder or his tracks are not detected or the intruder itself loses interest and ceases to employ resources or damages the system permanently.

4 Intrusion Detection System - IDS

In order to better introduce the authors claims, it is important to recall what is written in the field of network analysis and in particular on the Intrusion Detection System (IDS). These are, in fact, main tools for carrying out an inquiry either for incident response or digital network investigation. The examination of how IDS works and is classified. In fact, allow us to present a new approach based on behavioral profiling of users linked with the device traces left (e.g., a common PC) in a digital communication channel. Obviously, our goal is very difficult to achieve and can not find conclusion in this paper, but further studies needs to be conducted in the near future. Saying that, now we can move to IDS examination.

The intrusion detection can be considered as the "*problem of identifying those users or malware and bots that are using (or attempting to use) the resources of a computer system without having the required privileges.*" [6]. In the process IDS the symptoms highlighted by the system or data in digital communications are used to realize that the intrusion has occurred or is occurring. The purpose of the ID is to identify evidence of cyber-attack in order to ensure effective protection of the system. IDS systems can be classified according to the following functional attributes [7] [8]. However, current intrusion detection systems are able to recognize and generate alarms in presence of already known menaces or phenomena, characterized by a specific protocol or communication patterns whose templates should be preconfigured in the IDS attacks knowledge base. This can severely limit their effectiveness in presence of completely new (and unknown) menaces, the so called 0-day attacks. To cope with this problem new ID systems are emerging, based on the concept of anomaly detection, and based on the on-line examination of several linear or nonlinear statistic properties of the ongoing traffic, aiming at inferring the occurrence of anomalous phenomena characterized by some deviance from the "normal" (or baseline network traffic behavior [10].

4.1 Classification According to the Source of Data

a Network based IDSs (NIDSs) [9]: intercept and analyze packets that travel over the network using a "stealth" network card, active real-time and whose use is restricted to the administrator of the network.
b Host based IDSs (HIDSs) [11]: monitor and analyze predetermined log file and in particular the operating system audit log. Operate in either real time or periodically.
c Application-based IDSs (AIDSs): Special HIDS that focus on particular audit log of specific applications.
d Stack-based IDSs (SIDSs) [8] operate directly on the TCP/IP stack by monitoring the passage of packets through the layers of network protocol.

4.2 Classification According to the Method of Analysis

a Fingerprint based IDSs are based on a database of classes of attacks. When a match between an event and a recently recorded class of features is found (or at least match only in part) there is an high probability that the IDS has detected an intrusion in progress.
b Historical profile based IDSs: IDSs commercial and experimental attempt to determine an average profile over the period of use of the controlled system. If the IDS detects an abrupt change in this profile then a possible intrusion or at least an irregular operation is going to occur [12].

4.3 Classification According to the Type of Reaction

a Active IDSs react to the abnormal situation of specific applications running under administrative privileges, changing the system environment (for exam-

ple, isolating resources) and sometimes, if unable to identify the intrusion, even acting directly responsible for the attack on isolating and recording accurately subsequent actions and communications.

b Passive IDSs: report alarms to the system administrator who is responsible for deciding what action to take.

At last, IDSs, while providing an important input to prevent, block and contrast attacks against Digital Forensics analysis, unfortunately, are still very "rigid" in their activities referring to precise patterns and pre-packaged, and also show a marked sensitivity to parameter settings. This means that the implementation of an IDS with a firewall to anticipate barriers in a network system is absolutely valid, but what if it does not follow a long period of evaluation, observation and analysis of statistics on the data provided, the cost of employing be too high compared to the benefits. Without fear of contradiction, an IDS must be chosen with different intervention policies at home and various parameters that can be selected and reviewed at least every 6 months based on precise analytical observations of the behavior of the network system.

In any case, the last goal of modern IDS systems is the timely generation of sufficiently accurate alerts that can be used to trigger automatic protection countermeasures such as the determination and distribution of the proper filtering rules [13] to defeat the detected attacks. In the near future, these mechanism will be properly orchestrated to cooperate in a structured organization working as self-learning distributed security solution [14] or operating like a kind of network immune systems [15] where firewalls and detectors play the roles of network antibodies.

5 Network Profiling of Digital Communication Channel

In order to test the application of the method of behavioral analysis offered by the Digital Profiling of a digital communication channel, and to extrapolate the patterns of behavior, you chose to take a sample analysis of log files for access to a corporate web server on which they are resident, on the web portal and the Intranet.

The web server log files record the values for each request received from the server itself. The data are collected in text: when a user accesses a web page, the browser makes a request to the server resources, the system of allocation and management of the web site from which the page is called. The resources required may consist of web files (HTML, PHP,. ASP, etc..), image files or graphics, sound files, video files, and special applications. The web server accesses resources and sends them to your browser, so you can view them. This exchange activities between browser and web server is recorded in the log file, and creates a log of requests to a server by browsers of the users and the resulting responses [16]. The information contained in log files are normally stored in the format known as the *Common Log File Format*, a text file in which each request from browser

to web server corresponds to a string. The log file records only the web pages needed and the resources associated with them as audio files, graphics files, etc.. Each server response - indicating success, error, timeout (i.e. no response) - is recorded by the server log file. Table 1 is a typical line of a log file in the Common Log File Format:

82.68.58.90 - user [01/Feb/1998:10:10:00 +0100] "GET /ind.htm HTTP/1.0" 200 4839

Where each field expresses a particular value.

Field	Definition	Description
82.68.58.90	REMOTEHOST	Fully qualified domain name or IP address of the applicant.
-	RFC931	Server authentication.
User	Auth user	Username with which the user is authenticated.
01/Feb/1998:10:10:00 +0100	DATA	Date and time zone for the request.
GET /ind.htm HTTP/1.0	REQUEST	Type of request.
200	Status	Classification code of the result, identified by the HTTP server sends in response to the client. Indicates whether the file has been traced.
4839	Byte	Number of bytes of the response..

Table 1. Log file in the Common Log File Format

The specific type chosen for the log file was created by experimentation in order to maintain control of accesses to the public for statistical purposes(number of users in different periods of the year, attendance at different hours of the day, pages most viewed, etc...). It also records the accesses to the Intranet, reserved for employees through authentication, where a number of users employees own the publishing rights in areas dedicated to each business structure that provides its own documentation. In particular, the control has been implemented following the discovery of a leak of confidential information, in the published literature within the Intranet. This site discusses and summarizes the application of the method of Digital Profiling used to out line the behavior of digital users in order to detect any misconduct.

5.1 The Method of Analysis

In the analysis of log files, depending on the purpose it is intended, are used to highlight relationships between data and build a result of behavioral models that describe two types of approach:

- Top down: search for confirmation of facts already known or assumed (eg, an action resulting from an intrusion has already occurred)
- bottom-up: to find information useful to construct hypotheses (e.g., the most likely causes that produce a particular result).

This research proposes to apply the method of Digital Profiling [1] with both bottom-up and top-down approach. The cycle of analysis takes place in 6 phases.

Step 1 - Identification of the target.
Step 2 - Collection of data log files.
Step 3 - Identification of characteristic properties (features) from the mass of data collected from log files and collect this information (indicators) contained the features detected.
Step 4 - Detection of possible subjects to which it is possible to attribute behavior Digital.
Step 5 - Analysis of information and construction of the behavior of digital accesses.
Step 6 - Construction of the user profile and usage of digital information obtained, depending on the objective.

5.2 Application of Method: a Case Study

Phase 1 - Objective In the case study,the goal is extrapolation of the profile of users accessing the portal/intranet via the digital reconstruction of the behavior of the various requests that come to the web server. The collection of log files has been confined here in a span of 90 days, identified as the period in which the intrusion occurred.

Phase 2 - Data collection Log files are chosen as standard for access to the IP address of a web portal resident on the web server with one part open to the public and a private Intranet to employees, consisting of an enterprise document repository with access through authentication(username+ password unique to each individual user). These special log files are specifically configured by the company to perform statistics on areas of greatest influx both by external users to the portal by employees in the documentary Intranet, in order to improve the efficiency of the service offered in terms of both external and internal communications. They were chosen for this analysis because of their relative simplicity makes it an ideal sample for a more agile and easy illustration of the application being tested. Log files are structured in records consisting of 8 fields, according Table 2.

2012-04-16 02:35:34 document document.pdf visualization john.smith 10.6.301.0 yes /intranet/office01/data/

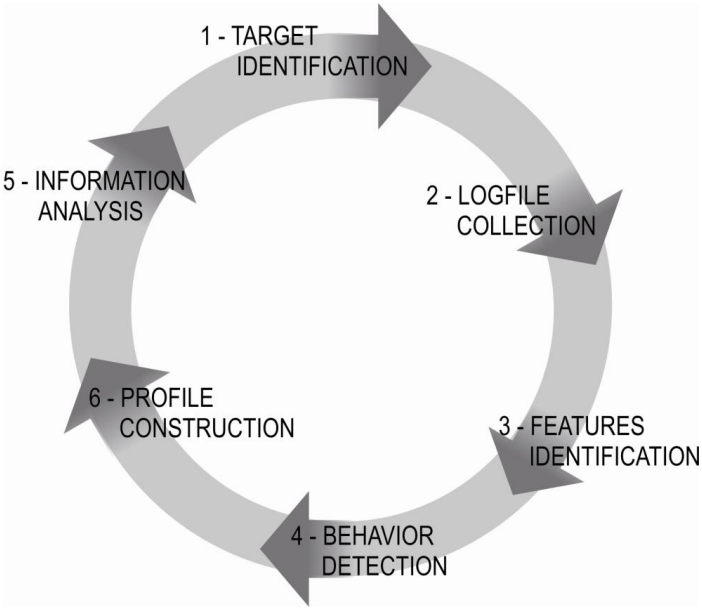

Fig. 1. Network profiling cycle of analysis

Phase 3 - Identification of properties characteristic, features, and relative values, indicators Each field is an ENTITY that has one or more characteristic properties(FEATURES), each of which contains a set of possible values, which are characteristic or factual information(INDICATORS), which will build the behavioral model of each entity.

1. DATE: gives information on the distribution of accesses in the days of the week: year-month-day (in yyy.mm.dd).
2. TIME: provides information on the distribution of accesses in the daytime: hour.minutes.seconds (in hh.mm.ss).
3. USERNAME: contains information on the identity of the user-employee or as an alternative means to access the portal from an external user.
   - firstname.lastname (employee - internal access).
   - anonymous (external access).
4. IP: provides the identification number of the machine from which the user/ employee has logged on, where indicator is IP number.
5. OBJECT TYPE: provides the type of file being accessed:
   - Document: means access to a file;
   - folder: indicates access to a folder or area.
6. OBJECT NAME: contains the name the extension of the file or folder name to which you have access: Name.extension-full name of the file.
7. OBJECT PATH: provides the entire path to the object sought within the web site or Intranet.

Field	Definition	Description
01/Feb/1998:10:10:00 +0100	Data Time	Date and time for the request.
Document	Object Time	Type of object searched by the user, consisting of a document (text / spreadsheet / image, etc..), from an area of the site or the Intranet..
Document.pdf	Object Name	Name of the file object of the request.
Visualization	ACTION	Type of action taken by the user on the file or folder / area sought..
John.smith	USERNAME	Contains the user name, consisting of firstname.lastname and kept in the Active Directory enterprise, with which the user-employee makes the request for access to the portal, which allows him access to the Intranet. In the case of access by a user not recognized by the system, the field describes it as anonymous, with the right of access only to the public.
10.6.301.0	IP	identifies the IP address of the machine, inside the company domain, from which the user has logged-dependent. When accessing from outside the corporate domain, the field identifies it as N.D.
IS	INTRANET	Access to employees or less restricted area by the user.
/intranet/uffice01/data/	OBJECT PATH	Location of the file / folder that the user has accessed.

Table 2. Log files are structured in records consisting of 8 fields

8. ACTION: shows actions performed by the user:
   - Display: visualizes the document in read/download, allowed to all users;
   - creation: allows the publication of a new document or folder (action reserved for users with permission to publish);
   - edit: edits a new document or folder (action reserved for users with permission to publish);
   - delete: allows deletion of a new document or folder (action reserved for users with permission to publish).

Phase 4 - Conduct of digital extrapolation Depending on the original purpose, each ENTITY detected can be considered the main actor in which to disclose the information (indicators) derived from the Feature of the other elements of the log file, for the delineation of their digital behavior.

It then considers the set log file L, which belong to the entity E:

$L = E_1 \cdots E_n$

Each entity E is formed in turn by one or more Features f, properties that characterize it: $E = f_1 \cdots f_n$

Each Feature f contains a value that represents the indicator i, i.e., characterizing the information. The goal of the set of indicators is to form the behavior of each Entity. $E = i_1 \cdots i_n$

We discuss here briefly the extrapolation of the behavior pattern of entities subject to company analysis after successful intrusion. Within the log file of the case to identified ENTITIES interest, each of which has its own digital personal behavior. The application of the method can be implemented with two different approaches of cited. In this case we assume knowledge of an intrusion already occurred, and we use a top-down approach, identifying the ENTITIES primary object of the intrusion, i.e. the file containing the stolen information, indicated by the field OBJECT NAME.
Entity OBJECT - Digital model of behavior: the Feature which characterize its behavior contain digital indicators with which it is possible to build the model behavior of the follow Entities.

- OBJECT NAME: indicates not only the file on which the action was done, but how many times it has been accomplished in the time interval considered.
- PATH: identifies the area where the object is contained (in this case within the Intranet with the subfolders), the indicators that they extract provides guidance on:
  - Vulnerabilities in the implementation of security measures for the affected area;
  - presence of other types of confidential documents also present in the object of intrusion.
- ACTION: the type of action that was performed on the object-target:
  - Display (ie the download file);
  - create (upload a file or creating a folder);
  - edit (edit the file as its replacement, moving, renaming the file);
  - delete (delete a file or a folder of files).
- DATE and TIME: the date and time when the operation was performed on the object. Indicators are also obtained from extracts statistical information on the days and hours of the day when the shares were the most frequently performed.
- IP: The IP address of the machine you are logged on (whether fixed or Domain) or IP address of the source provider (if dynamic). It also indicates how many times the same IP has made other actions.

Similarly, but with a bottom-up approach, we can apply the same method of profiling the log file from the user anonymous, useful if you want a model to study the behavior of users who access the web server from outside domain, in order to implement security measures with the aim of preventing any abnormal behavior. In this way we can create a primary entity (USERANONYMOUS), using the primary USER ENTITY, filtered with Feature “Anonymous” from the USERNAME field. The Feature which characterize its behavior contain digital

indicators with which it built its digital model of behavior: ACTION, OBJECT NAME, DATE and TIME, IP.

Phase 5 - Analysis of information and construction of the behavior profile of digital accesses The information derived from the measured indicators are the behavioral profile of the subject being treated as the main entity. In the case of the Entity OBJECT, that is, the file object intrusion, with reference to the time period examined (90 days), the indicators have revealed that it has been shown, by an anonymous user, with an IP not identified, for 5 times in one month:

- 3, Saturday morning, at 10:12 am;
- 4, Sunday morning, at 11:05 am;
- 10, Saturday morning, at 9:55 am;
- 11, Sunday morning, at 10:00 am;
- 17, Saturday morning, at 10:47am.

Similarly,the behavioral profile was obtained USERANONYMOUS, which connects mainly in the evening after 18, Saturday and Sunday morning browsing documents information on services and products offered by the company.

Phase 6 - Comparisons of the obtained profiles and usage of given digital information, depending on the objective Last operation is the comparison between the obtained profiles in order to reveal affinity in the digital behavior. Using connection dates as a filter, we selected users access to anonymous on Saturday and Sunday morning, in the 3 month period. The comparison with the dates reserved for the display of files allowed to isolate two anonymous users online on the dates and times in which the confidential file with the same IP address was downloaded.

5.3 Considerations

In this paper it is shown the possibility to apply the Digital Profiling to a data stream with the aim to extrapolate the profile of the entity of interest by looking at a set of log files resulting as the access log of a web server in a given time interval. The application of the method is also possible on any other entity within a log file, in order to extrapolate the digital behavior of “someone” (or “something”) of interest. A second factor to be considered is that it is also possible to make a comparison between different behaviors in order to build broader profiles, composed of different behaviors of the “actors” who populate the data flow. Indeed, where there is no availability of specific log files, it is possible to reconstruct the profile by comparing different behaviors of the different entities available in a given log file.

6 Conclusions

The Digital Profiling of a set of log file could be very useful for the identification of a perpetrators of a cyber-crime (e.g., phishing, attacks on servers, etc.), where the extrapolation of the digital behavior of selected entities, as subject of a set of log file, can make the reconstruction and subsequent analysis of the modus operandi of the offender (i.e., the intruder in case of a network intrusion). The proposed approach is able to reveal information about:

- Target of the attack (fraud, Denial of Service, political attack, etc.);
- tools and techniques used for intrusion (rootkits, shells, worms, social engineering, etc.);
- technical skills used;
- possible correlation with measures of social engineering;
- time chosen for the attack (day/night, intra/end of week, etc.);
- duration of the attack and possible frequency (single or fragmented in predetermined time intervals, etc.);
- correlation of the moment chosen for the attack with external events;
- choices of victims (national or foreign government institution, bank, commercial organization, etc.);
- typology of (eventual) anti-forensic techniques adopted;
- achievement of goal.

References

1. Clara Colombini, Antonio Colella: Digital Profiling: a Computer Forensics Approach. ARES 2011: 330-34, (2011)
2. Clara Colombini, Antonio Colella: "Digital scene of crime: technique of profiling users" to appear in Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), (2012)
3. Stefano Aterno, Francesco Cajani, Gerardo Costabile, Marco Mattiucci, Giuseppe Mazzaraco, "Computer Forensics e Indagini Digitali", Manuale tecnico-giuridico e casi pratici, Experta srl.(2011)
4. R. Bejtlich: The Tao of network security monitoring. Addison Wesley. (2005)
5. Debra Littlejohn Shinder and Michael Cross: Scene of the Cybercrime (2 ed.). Syngress Publishing.(2008)
6. Biswanath Mukherjee, Todd L. Heberlein and Karl N. Levitt: Network Intrusion Detection. IEEE Network. 8(3): 26-41. (1994)
7. Bace R., Mell P.:Intrusion Detection Systems. National Institute of Standards and Technology Special Publication on IDS.(2001)
8. Laing B.: How to guide: implementing a network based intrusion detection system. (2001)
9. Roesch M.: "Snort - Lightweight Intrusion Detection System for Networks", 13th System Administration Conference - LISA '99, Seattle, WA. (1999)
10. Palmieri Francesco and Fiore Ugo: "Network anomaly detection through nonlinear analysis", Computers & Security, 29 (7): 737-755, Elsevier (2010)
11. Crosbie M. J., Kuperman B.A.: A building block approach to Intrusion Detection. RAID. (2001)

12. Stephenson P.R.: The application of Intrusion Detection Systems in a Forensic Environment. Recent Advances in Intrusion Detection - Raid. Toulose, France. (2001)
13. Palmieri Francesco and Fiore Ugo: "Containing large-scale worm spreading in the Internet by cooperative distribution of traffic filtering policies", Computers & Security, 27 (1-2): 48-62, Elsevier (2008)
14. De Santis Alfredo, Castiglione Aniello, Fiore Ugo and Palmieri Francesco: "An intelligent security architecture for distributed firewalling environments", Journal of Ambient Intelligence and Humanized Computing, 1-12, Springer Berlin / Heidelberg (2011), url = http://dx.doi.org/10.1007/s12652-011-0069-8
15. Palmieri Francesco and Fiore Ugo: "Automated detection and containment of worms and viruses into heterogeneous networks: a simple network immune system"Int. J. Wire. Mob. Compututer, 2 (1):47-58. Inderscience Publishers, Geneva, Switzerland.(2007)
16. T. Farinella: Tecnologia database per l'analisi di log file di Web Server. Universita' degli Studi di Modena e Reggio Emilia.(2005)