# Using Case-Based Reasoning for Cyber Attacker Profiling

Stelios Kapetanakis[1], Avgoustinos Filippoupolitis[2], George Loukas[2], Tariq Saad Al Murayziq[1]

[1]School of Computing, Engineering and Mathematics, University of Brighton, Moulsecoomb Campus, Lewes road, Brighton BN2 4GJ, UK
email: {s.kapetanakis, tsa10}@brighton.ac.uk
[2]School of Computing and Mathematical Sciences, University of Greenwich, Maritime Greenwich Campus, Old Royal Naval College, Park Row, Greenwich, London SE10 9LS, UK
{fa52, g.loukas}@gre.ac.uk

**Abstract.** Computer security would arguably benefit from more information on the characteristics of the particular human attacker behind a security incident. Nevertheless, technical security mechanisms have always focused on the attack's characteristics rather than the attacker's. The latter is a challenging problem, as relevant data cannot easily be found. We argue that the cyber traces left by a human attacker during an intrusion attempt can help towards building a profile of the particular person. To illustrate this concept, we have developed an approach using case-based reasoning that indirectly measures an attacker's characteristics for given attack scenarios. Our results reveal that case-based reasoning has the potential of being used to assist security and forensic investigators in profiling human attackers.

**Keywords:** Case-based reasoning, Cyber Security, Intrusion Detection, Artificial Intelligence.

## 1 Introduction

A typical cyber-attack involves a substantial number of steps, each one often being a cyber-attack by itself, such as reconnaissance, social engineering, remote installation of rootkits, recruitment of bots and propagation of malware before attempting to hack into a target system. At each step, the attacker leaves cyber traces, which can potentially lead to profiling and ultimately identifying the person before the next step of an attack, or forensically, after it finishes. While enormous attention has been traditionally placed on the profiling of criminals in physical attacks and identification of intention in the context of physical surveillance, the equivalent in the context of cyber security has remained unexplored. This is considered a major challenge. Henson et al. [1] have argued that cyber criminals' behaviour is different from that of normal criminals and depending on their skills, experience, knowledge, techniques, educational

background, mode of operation and target, their profiles could vary immensely [2]. In terms of technical means too, they are likely to adapt and devise new mechanisms continuously [12, 3].

Here, we examine whether a Case-based Reasoning (CBR) approach can help security and forensic investigators to profile human attackers with regards to their behavioural (e.g. how risk averse they are), demographic (e.g. gender) and technical characteristics (e.g. speed).

The structure of the paper is as follows: Section 2 will give an overview of the literature, Section 3 will explain the methodology followed throughout this research and Section 4 will present the research hypotheses and the relevant results. Finally, Section 5 will conclude this search by summarising the outcomes and indicating the paths for future work.

## 2 Related work

Cyber-attacks have become one of the most serious types of crimes, as the damage they inflict on the victim organisations can be severe. This section aims to investigate work related to cyber profiling and identification of cyber attackers. Our focus is on the human attacker responsible for the cyber-attack.

Cyber-attacks have become one of the most serious types of crimes, as the damage they inflict on the victim organisations can be severe. Work in the early 1990's by Landreth [21] has attempted to classify hackers as in "novices, students, tourists, crashers and thieves" in an effort to reveal their motivation and individual characteristics. The Hacker Profiling Project [22] has equivalently attempted to codify the behavior / background of hackers with the use of questionnaires in a mission to reveal useful characteristics such as age, demographics, personal attributes, etc. Kjaerland's [25] analysis of reported incidents to CERT/CC to classify attacker operation related incidents. In an attempt to expand the classification window Kjaerland has presented the factors that were most likely to happen together. Work on attackers behavior has also been conducted from a psychological point of view. Shaw et al. [26] has presented that elements of malicious cyber activity may be related with history of negative social and personal experiences, lack of social skills, sense of entitlement and ethical flexibility. Watters et al. [27] working from a similar perspective has attempted to apply a qualitative identification of cyber intruder profiles by conducting an ethnographic study of cyber- attacks.

However, these and similar pieces of work do not provide technical mechanisms that can make use of a hacker's characteristics in practice and possibly in real-time. So, traditional technical security measures have always revolved around the characteristics of the attack rather than the attacker. Take, for instance, botnet attacks. Defense usually concentrates on an extended number of distributed nodes in an effort to identify common patterns from inbound traffic, looking perhaps for similarities in terms of network characteristics [10, 11, and 12], data mining for identification of concurrent synchronization relationships for bots [13], passively analysing DNS-based black-hole list lookup traffic [14]. In [4], Filippoupolitis et al. showed that an approach that would monitor and take into account the characteristics of the attacker as observed from the side of the victim computer can potentially help build a profile of the attacker and tell whether it is a human or a bot, using a decision tree-based approach.

This work will attempt to identify further whether human attacker identification is possible by applying Case-based reasoning in a similar context. Case-based reasoning has as its foundation logic that "similar problems have similar solutions". As a result its Retrieve, Reuse, Revise, Retain process cycle [15] aims to identify similarity among cases "close" to each other and by matching the closest aims to retrieve past knowledge, adapt it and apply it to any investigated case in an attempt to provide a solution.

Case-Based Reasoning could help in decision support and provide reasoning in cases were uncertainty and fuzziness is present since reasoning is provided based on past evidence and not any proprietary rule system. A lot of work on reasoning upon event cases refers to the workflow analogy where work has been done by Minor et al. [16] on workflow adaptation, Kyong Joo Oh and Tae Yoon Kim [17] on financial traces monitoring and identification of daily condition indicators and Kapetanakis et al. [8, 18, 19, 20] whose work has been mainly focused on business process monitoring and detection of anomalous behaviour on changing business processes.

In particular to Case-based reasoning and intrusion detection, CBR has been applied by Schwartz et al. [23] for the snort intrusion detection system and Micarelli and Sansonetti [24] in anomaly intrusion detection. The latter work has focused on rational architecture and representation of potential anomalous behaviour using CBR.

## 3 Methodology

This section will describe the methodology we adopted for this study in terms of the sample features, the attacker characteristics and their classification based on the details of the experimental data collection.

The main aim of this study is to be able to identify an attacker's profile based on observable characteristics collected from real systems that are susceptible to intrusion attempts. In order to achieve this target a number of features which are tightly related to potential cyber intruders will be evaluated, such as their skill level, risk aversion, education level, gender, predefined goal, speed, mistakes, anti-forensic actions and success [4]. In order to carry out the study, 87 individuals were requested to attack a specified system that had a number of services running (e.g. ftp server, web server, e-mail server, etc.). Each of the participants received (knew) the IP address of the target system and was prompted to attack it by using whatever means necessary to disable, control, or stop the services. Once the attacker was successful in penetrating the system, a cyber-intruder profiling tool was able to detect this event and start recording changes in the values of the system's observable features. While doing this, data were collected, coded, and stored for future use [4].

In the research process, successful attacks were listed, but altogether, each piece of information from the attacks would be used in the detection system. All the actions were closely monitored such as any attempts to alter or delete log files after carrying out their attack. Several factors were taken into consideration while defining each attack, for example the way in which the attackers had or were attempting to have access specific folders. The participants were finally asked to fill in a questionnaire that would detail the values of non-observable features [4].

A Case-Based Reasoning technique was selected based on the nature of the research problem in order to investigate whether successful classification can be made on intrusion attempts. More specifically, our system operated by identifying characteristics of attackers while they were in progress. Any intrusion attempt was been identified by relating it and comparing to data from previous cases. For the needs of this work each attack was regarded as an individual case for the CBR system. All cases were subject to analysis by forensic experts and have been classified based on their attack outcomes. These outcomes were used as evidence for the solution part of the cases.

The ability of Case-based reasoning to express and reason upon specialised knowledge, was one of the main reasons it was chosen for this study. In addition, it uses simple knowledge

that has been well defined in the configuration stage and the information can be understood by the user versus for example rule-based systems [5].

Case-based reasoning was used as a complementary reasoning technique to the Machine Learning one as indicated by Filippoupolitis et al. 2014 [4], based on the assumption that human intrusion to cyber systems is characterised by predominantly fuzziness and uncertainty as this has been identified in related research [6, 7]. Monitoring systems that deal with uncertainty have been shown effective provided a number of decisive measures (e.g. suitable temporal event representation, transformation to graph reasoning, pattern matching, etc.)

## 4 Profile Detection

For this work a number of experiments were designed and applied in an attempt to evaluate and classify cyber profile behaviours. For this research a pool of 87 real attack patterns were used as both qualitative and quantitative evidence to formulate the case base. The investigated data comprised information regarding the nature of the attack, trace evidence taken from the attack environment and expert ranking of what was the outcome of the attack (a team of human experts have identified all attacks in terms of success or failure). Following the above, each case contained profile information for the attacker in terms of background education, forensics knowledge, networking expertise, etc. Each case was fully anonymised before adding it to the case base as well as cleaned and cleansed for any redundant semantics (noise) information.

For this work two main stages of experiments were conducted to incrementally build upon reasoning and investigate the optimum evidence for argumentation while classifying potential cyber-attacks. The two questions that were attempted to address were:

(a) Which are the characteristics of a successful attack
(b) Can we classify an attack based on its individual attribute characteristics

For the needs of the experiments MyCBR [9] was used (Fig. 1)

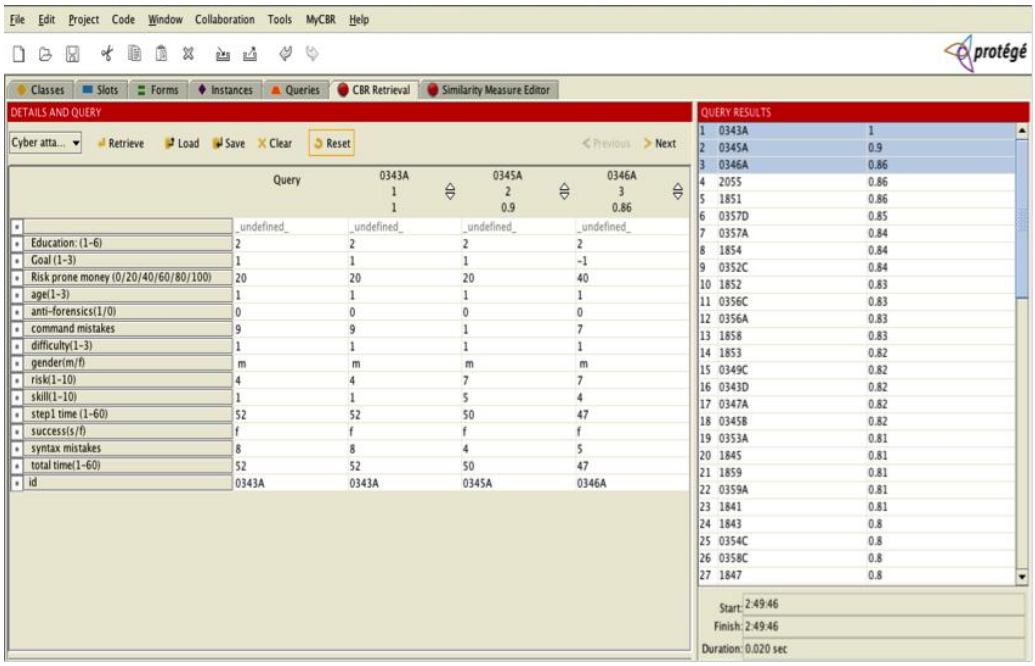


**Fig. 1.** MyCBR [9] used for the calculation of similarities among cases

as the main case-based reasoning framework to accommodate the majority of them using predominantly normalised Euclidean distance to calculate similarity among attributes (equation 1).

$$d(\vec{x},\vec{y}) \sqrt{\sum_{i=0}^{N} \frac{(x_i - y_i)^2}{s_i^2}} \qquad (1)$$

where $s_i$ is the standard deviation of $x_i$, $y_i$ over the sample set of attributes.

For the similarity calculation among evidence traces a simple count of similar type events (Components) algorithm (equation 2) [8] was used since it provides the necessary degree of granularity among traces and has been proven effective [8] in the identification of quantitative event patterns among trace data.

$$\sigma(C, C') = \sum_{i=1}^{no\ of\ event\ types} \frac{N_i^2}{N_{total} \times N'_{total}} \qquad (2)$$

where Ni is the number of events of type i common to both event traces and Ntotal and N'total are the total expected number of events in traces C or C'

For the needs of the initial experiments Euclidean distance similarities were applied with the application of empirical weights based primarily on the attributes and experience ranking from domain experts. As initial result from the similarity measures an attribute matrix was created indicating two clusters of successful and unsuccessful attacks within the pool of the case –base. The rate of the attributes can be seen in Fig 2 below:

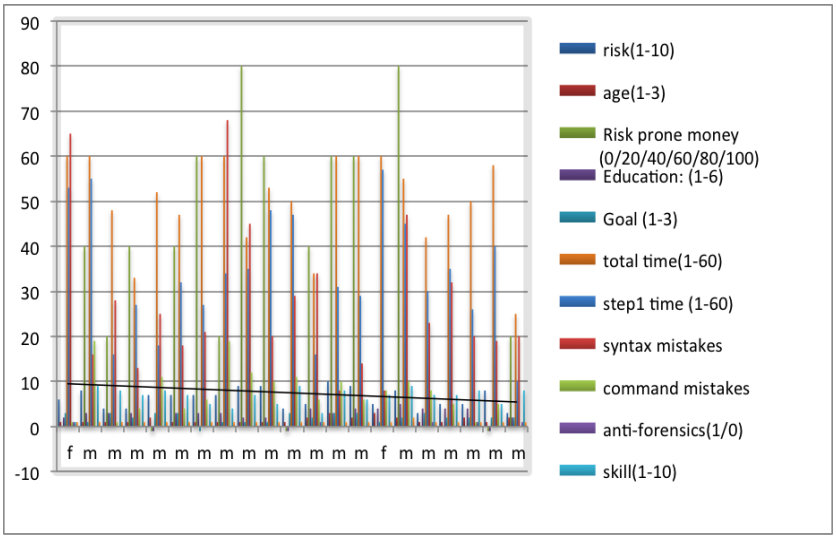


**Fig. 2.** Sample of the successful attacks cluster showing the frequency rates of attributes

As it can be seen from Fig. 2, while addressing the first research question it has been identified that successful attackers were in majority male users (33 successful attacks versus 5 female), were mainly in a high educational profile, were between 25-35 years old and had a lower frequency of syntax and command mistakes coinciding in result to the findings of Filippoupolitis et al. (2014) [4]. The second main cluster with the majority of unsuccessful attacks could also be qualified with specific relevance to gender, education, risk and skill attributes, indicating potentially a pattern for future identification (Fig. 3).

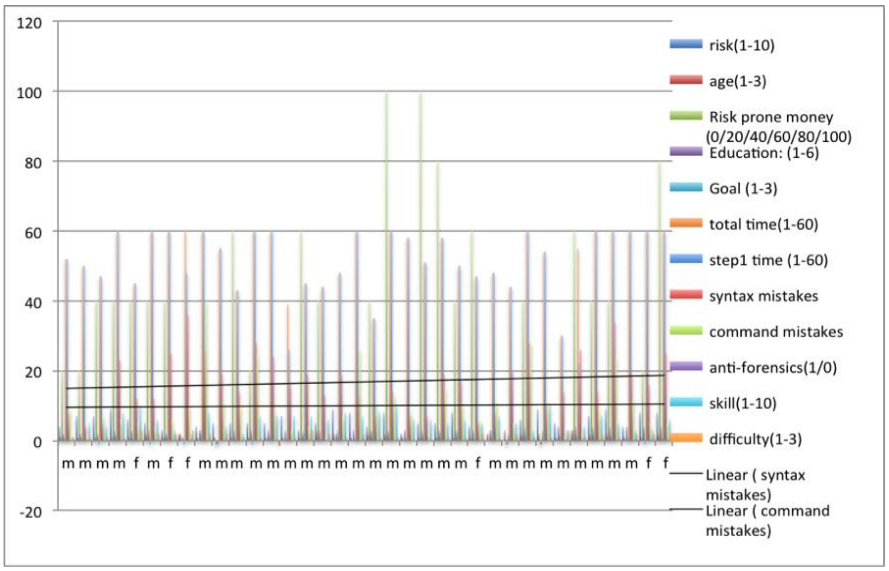


**Fig. 3.** Sample of unsuccessful attacks cluster indicating the attribute frequency rates

Finally, in order to answer the second research question CBR was applied to classify a random selected sample from the case base. For the needs of this stage random samples of 10% - 12% of the case base were selected and their classification information was hidden. CBR was called to classify them using similarity measures and 3NN classification. The experiments were conducted 10 times for each case and the results were averaged. With the selected case-base, CBR has shown variable accuracy between 60 and 80% with an average classification rate of 69% over 6 different samples and approximately 10x 6 x 9 or 10 = 540 to 600 iterations. All the indicated samples contained a random selection of human attacks upon which CBR was called to reason against. CBR has shown similar efficiency in the classification of both intruders and not with precision of 67% and 72% respectively. This efficiency in accuracy can be regarded as positive and was regarded as promising since both of the stated questions have been satisfied from the findings.

However, greater variation in terms of a different data sample could affect the CBR output since the current case base contained attack snapshots in controlled environments. Table 1 below shows a snapshot of the executed experiments. A brief explanation regarding the presented columns/rows: Column *Case id* refers to the anonymised cases. *Actual Ranking* refers to whether the investigated case was an attack or not, Columns *Ranking* refer to the k nearest neighbours of each investigated case, *Averaged* refers to the final decision for the case based on its neighbours classifaction. Finally, F refers to any unsuccessful attack whereas S refers to successful ones.

| Case id | Actual Ranking | Ranking 1st 3NN | Ranking 2nd 3NN | Ranking 3rd 3NN | Ranking 4th 3NN | Ranking 5th 3NN | Ranking 6th 3NN | Ranking 7th 3NN | Ranking 8th 3NN | Ranking 9th 3NN | Averaged 3NN vote |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0346A | F | S | S | S | F | F | S | S | F | F | False Positive |
| 0353A | F | F | F | F | F | S | S | F | F | F | F |
| 0343C | S | S | S | F | F | S | S | S | S | F | S |
| 0348C | S | S | S | S | S | S | S | S | S | S | S |
| 0357D | S | S | S | F | F | F | F | F | S | S | Missed Negative |
| 0360A | S | S | S | S | S | S | F | S | F | F | S |
| 2054 | F | F | F | F | F | F | F | F | F | F | F |

**Table 1.** Snapshot of 3NN classifications for attack traces.

## 5 Conclusions and Future Work

In this paper we presented a Case-based Reasoning approach towards the identification of human attacker cyber profiles during while attempting cyber-attack activities. Attacker characteristics have been identified and classified in an attempt to recognise, isolate and trace a "known" profile from a pool of combinations of real attack data and human intrusion patterns. Case-based reasoning was used to predict and classify the background of an intruder in a number of random generated and averaged samples. CBR in the conducted experiments has been proven successful in revealing and identifying human profiles behind an intrusion attempt as well the prompt patterns in a successful and an unsuccessful attack respectively. Further to the above CBR has seemed to build confidence to the user (investigator) of the system in regards to the followed pattern behind an attack.

As presented in this work the initial results are encouraging, however, a number of additional factors will be investigated in future work in regards to broader reasoning, investigation and acquisition of larger data samples. In parallel the usage of CBR results to real time investigations will be pursued while a system is in service and potentially subject to attack from random individuals. Its incorporation with a cyber-profiling tool will also be investigated.

## References


1. Henson, B., Reyns, B., Fisher, B.: Internet Crime. In W. Chambliss (Ed.), Key issues in Crime and Punishment: Crime and criminal behavior, 155-168 (2011)
2. Krasser, S., Conti, G., Grizzard, J., Gribschaw, J., and Owen, H.: Real-time and forensic network data analysis using animated and coordinated visualization. In: Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC, pp. 42-49. IEEE, June (2005)
3. Pal, P.P., Webber, F., Schantz, R.E., Loyall. J.P.: Intrusion tolerant systems. Proceedings of the IEEE Information Survivability Workshop (ISW-2000) (2000)
4. Filippoupolitis, A., Loukas, G., Kapetanakis, S.: Towards real-time profiling of human attackers and bot detection. In Proceedings of CFET 2014: Cybercrime Forensics Education & Training, Canterbury, UK (2014).
5. Prentzas, J., Hatzilygeroudis, I.: Categorizing Approaches combining rule-based and Case-based reasoning. Expert Systems 24(2), 97-122 (2007).
6. Patcha, A., Park, J. M.: An overview of anomaly detection techniques: Existing solutions and latest technological trends. Journal Computer Networks: The International Journal of Computer and Telecommunications Networking. Volume 51 (12),pp. 3448-3470 (2007)
7. Olusola, A. A., Oladele, A. S., Abosede, D. O.: Analysis of KDD '99 Intrusion Detection Dataset for Selection of a Relevance Features, Proceedings of the World Congress on Engineering and Computer Science 2010, Vol I, IEEE (2010).
8. Kapetanakis, S., Petridis, M., Ma, J., Knight, B., Bacon, L.: Enhancing Similarity Measures and Context Provision for the Intelligent Monitoring of Business Processes in CBR-WIMS, In: Process-oriented Case-Based Reasoning workshop (PO-CBR), ICCBR2011 (2011)
9. Stahl, A., Roth-Berghofer, T.: Rapid prototyping of CBR Applications with the Open Source Tool myCBR. Künstliche Intelligenz, 23(1):34–37, March 2009 (2009).
10. Loukas, G., Oke, G.: Protection against denial of service attacks: a survey. The Computer Journal, 53(7), pp. 1020- 1037, (2010)
11. Oke, G., Loukas, G.: A denial of service detector based on maximum likelihood detection and the random neural network. The Computer Journal 50, no. 6, pp. 717-727, (2007)
12. Loukas, G., Oke, G.: Likelihood ratios and recurrent random neural networks in detection of denial of service attacks. In Proceedings of International Symposium of Computer and Telecommunication Systems, SPECTS (Vol. 7), (2007)
13. Gu, G., Zhang, J., Lee. W.: Botsniffer: Detecting botnet command and control channels in network traffic, in Proceedinds of the 15th Annual Network and distributed System Security Symposium, (2008)
14. Ramachandran, N. F. A., Dagon, D.: Revealing botnet membership using DNSBL counter-intelligence, in Proceedings of 2nd Workshop on Steps to Reducing Unwanted Traffic on the Internet, (2006).
15. Aamodt, A., Plaza, E.: Case-based reasoning; Foundational issues, methodological variations, and system approaches. AI Communications, vol. 7, no. 1, pp. 39-59, (1994)
16. Minor, M., Tartakovski, A. and Bergmann, R.: Representation and Structure-Based Similarity Assessment for Agile Workflows, in Weber, R., O. and Richter, M., M.(Eds) CBR Research and Development, Proceedings of the 7th international conference on Case-Based Reasoning, ICCBR 2007, Belfast, NI, UK, August 2007, LNAI 4626, pp 224-238, Springer-Verlag, (2007)
17. Kyong Joo Oh, Tae Yoon Kim: Financial market monitoring by case-based reasoning, Expert Systems with Applications, Volume 32, Issue 3, Pages 789-800, (2007)

18. Kapetanakis, S., Petridis, M.: Evaluating a Case-Based Reasoning Architecture for the Intelligent Monitoring of Business Workflows. Successful Case-based Reasoning Applications-2. Springer Berlin Heidelberg, pp. 43-54 (2014)
19. Kapetanakis, S., Petridis, M., Knight, B., Ma, J.,Bacon, L. (2010). A Case Based Reasoning Approach for the Monitoring of Business Workflows, Proceedings of the 18th International Conference on Case-Based Reasoning, ICCBR 2010, Alessandria, Italy, Lecture Notes in Artificial Intelligence LNAI 6176 (2010)
20. Kapetanakis, S., Petridis, M. (2012). Enhancing the explanation capabilities of the CBR-WIMS framework for the intelligent monitoring of Business workflows. In: Explanation-aware Computing ExaCt 2012, ECAI 2012.
21. Landreth. B: Out of the Inner Circle: A Hacker's Guide to Computer Security, Microsoft Press, 1985.
22. Chiesa, R., Ducci, S., Ciappi, S.: Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking. CRC Press, 2008.
23. Schwartz, D.G., Stoecklin, S., Yilmaz, E.: A case-based approach to network intrusion detection. Information Fusion, 2002. Proceedings of the Fifth International Conference on (Volume:2 ), pp. 1084 – 1089 (2002)
24. Micarelli, A., Sansonetti, G.: A Case-Based Approach to Anomaly Intrusion Detection. Machine Learning and Data Mining in Pattern Recognition, Lecture Notes in Computer Science Volume 4571, pp. 434-448 (2007).
25. Kjaerland, M.: A taxonomy and comparison of computer security incidents from the commercial and government sectors. Computers and Security, 25:522-538 (2006)
26. Shaw, E.D., Post J., Ruby, K.: Inside the mind of the insider. Security Management, pp. 34-44, (1999)
27. Watters, P. A., McCrombie, S., Layton, R., Pieprzyk, J.: Characterising and predicting cyber attacks using the Cyber Attacker Model Profile (CAMP), Journal of Money Laundering Control, Vol. 15 (4): 430-441, Emerald Group Publishing ( 2012)