IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 09 Issue 09, September 2022
ISSN (Online) 2348 – 7968 | Impact Factor – 6.72
www.ijiset.com

Vulnerability Interrelationship Inspire Bio-Cybersecurity

Seyedali Pourmoafi[1], Stilianos Vidalis[2]

[1] Department of Physics Engineering and Computer Sciences, University of Hertfordshire
Hatfield, Hertfordshire, United Kingdom

[2] Department of Physics Engineering and Computer Sciences, University of Hertfordshire
Hatfield, Hertfordshire, United

[1]s.pourmoafi@herts.ac.uk, [2] s.vidalis@herts.ac.uk

Abstract

With increasing interest in modern technologies, cyber operation infrastructures can be targets for data leakages. Every day, tens of thousands of analysts work in the security operations center to monitor the systems and different devices. They must decide, in seconds, which of the cybersecurity alerts are false alarms, and which can be the next target hack. To fight these types of threats, we need to have good knowledge about different classes of cyber-attacks along with their properties. In this paper, we present a novel scheme based on vulnerability interrelationship and bio-cybersecurity which help to wipe more than one attack at the same time.

Keywords: *Bio-Cybersecurity, immune system, NLP, vulnerability interrelationship, vulnerability tree.*

1. Introduction

Most cybersecurity tools have been notoriously poor at separating the noise from the signal. It is no surprise, since the different methods used by hackers are constantly evolving and mutating along with technology. The static signatures that cybersecurity tools use to detect them are outdated almost as soon as they are released. The main concern is that this knowledge can cause risk and numbness, and make the users or technical teams slow to act when cybersecurity tools detect a threat. However, modern technology has taken on a new dimension that starts with taking the "living" nature of attacks a little more significantly. The big and serious issue with threat detection is that even tiny mutations in cyber-attacks can fool it. Hackers can repackage the same code with only a few minor changes to change its signature. This process can even be automated. This makes hacking computers much cheaper, faster, and easier than defending them [19]. There are different strategies have proposed to address these issues. One of the recent studies takes advantage of bio-cybersecurity or cybersecurity inspires the human immune system.

Bio-inspired computing is a field of study in computer science that aims to create systems that are inspired by biological phenomena [1]. Bio-inspired computing makes use of computers to model nature while also studying nature to improve computer usage. Bio-inspired computing encompasses evolutionary-based genetic algorithms, Artificial Intelligence (AI) and Artificial Neural Networks (ANN), sensor networks (sensory organs), and artificial immune systems. Cyber immunity, which is based on the human adaptive immune system, is a recent area of study [5]. Machine Learning (ML) methods, a subset of artificial intelligence (AI), are frequently used in cyber immune systems. Because it emulates human learning abilities on computers, ML is bio-inspired [13].

1.1 Human immune system

The immune system (IS) of the human body is a remarkably effective defence mechanism that detects a wide range of harmful agents known as pathogens, such as viruses, parasites, and microbes. The immune system is capable of distinguishing pathogens from healthy tissue. The skin, like a firewall, protects our bodies from external threats. It is constantly being renewed and adapted. Our bodies function as police states, with the IS constantly monitoring the internal environment. Even minor infections can take hold and prove fatal in the absence of a functioning IS [2].
The IS consists of an innate immune system and a much younger adaptive immune system (AIS). Innate immunity is present in both, vertebrates and invertebrates, whereas the adaptive immune system is found only in invertebrates [2]. If a pathogen breaches the physical barriers of the body, the innate immune system provides an immediate, but non-specific response. It is not capable of conferring long-lasting immunity. The AIS is activated when a pathogen evades the innate immune system.

The AIS is capable of producing a pathogen-specific, tailored response. It is antigen-specific, and the response is remembered in the event that the same pathogen enters the body again. It can then respond quickly and specifically to antigens. The immune system has the ability to learn, remember, and recognise patterns [3]. Likewise, the AIS serves as the immune system's memory.

1.2 Cyber Immune System

Cyber immune systems detect attacks based on anomalies detected in normal network traffic rather than their signature. They have learning and memory abilities that allow them to detect and remember previously unknown attacks. They are members of the cybersecurity system family [11]. Cybersecurity refers to the set of technologies and processes that are designed to protect computers, networks, programs, and data from attack, unauthorized access, change, or destruction. ML techniques are commonly used in cyber immune systems [14].
However, in previous or existing works, the researchers have tried to focus on inspiring the human immune system for cybersecurity. Most researchers proposed different approaches to the learning and memory capabilities of cybersecurity, based on the human body [1][13][14][15].
In this study, we have considered both, the vulnerabilities interrelationship and bio-cybersecurity which can cover a group of attacks to improve the security of the systems. To implement this approach, Natural Language Processing (NLP) technique has been used. NLP has the advantage of not requiring rules to be programmed or hardcoded by the programmer but instead learning the rules themselves. They can also learn new rules while running if new, previously unknown anomalies occur.

2. Related Works

We will explain related work from two different points of view, which are keys to our work. The information of Cybersecurity Vulnerabilities source and classification of Vulnerabilities with NLP.

2.1 The Information of Cybersecurity Vulnerabilities Sources:

The cybersecurity domain is not new. It has relied on multiple sources and concepts when it comes to studying security vulnerabilities. For instance, the National Vulnerability Database (NVD) a U.S. government repository of security vulnerability information (https://nvd.nist.gov/), is one of the most common sources which has been used widely. NVD provides a list of different vulnerabilities from 1988, where each vulnerability is identified by its “Common Vulnerabilities and Exposure” (CVE) ID (Common Vulnerabilities and Exposures). The Zero-Day Initiative or ZDI (https://www.zerodayinitiative.com/) is another example, which permits security researchers to report privately 0-Day vulnerabilities to the affected vendors. ZDI is made public the vulnerabilities, which are collaboratively by the affected vendor through a joint advisory. Other useful sources can be listed:

- CVE ® Program Mission
  https://www.cve.org/
- Mozilla's security advisory https://www.mozilla.org/en-US/security/advisories/
- Redhat's product security center
  https://access.redhat.com/security
- The Apache Security Team https://www.apache.org/security/

2.2 B. Information Classification with NLP Support

The use of NLP for the analysis of vulnerability information sources has been largely enabled thanks to recent research, such as database systems [1] and Semantic Web technologies [7]. Among existing works, that used a combination of the NLP with Semantic Web, Tablan et al. [9] suggested QuestIO, a Natural Language Interface (NLI) that permits analysing structured information in a domain-independent style. Or Lopez et al. [10] introduced the PowerAcqua methodology, which is a system for analysing information that is stored in heterogeneous, semantic resources.
However, despite all benefits existing works may have, in our proposed work, we have tried to focus on vulnerability interrelationship by inspiring the human body which is not considered in previous or existing works. In this paper, by finding the relationship between different vulnerabilities, the users are able to address a wide range of risks or vulnerabilities which are related to each other, at the same time. In another word, users can create an environment, where sensitive information or data cannot leak easily, by threat actors.

The rest of the paper is organized as follows. Section 3 provides a system model, evaluation, and vulnerability tree model. The final section (Section 4) concludes this paper.

3. System and Threat Model

Humans or any other living creatures have evolved to develop different natural forms to assist them in avoiding and eliminating danger and adapting to their surroundings in order to survive. These biological predispositions and instincts are from internal body systems to physical ones and aim to outrun possible risks and predators [4]. These biological predispositions and instincts are from internal body systems to physical ones and aim to outrun possible risks and predators. This methodology can be synthetically adopted and implemented in cyber defense strategies to improve a system's resilience in the face of probable vulnerabilities or attacks (Fig1.).

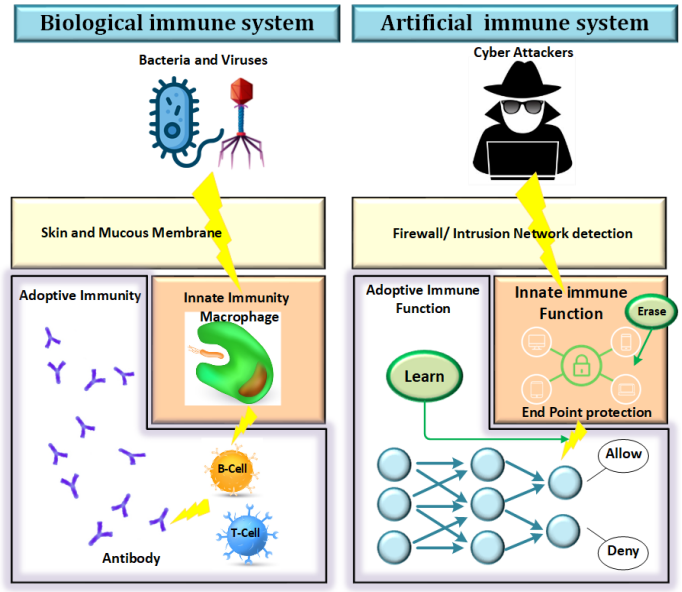

Fig 1. Comparison of biological and artificial immune system.

3.1 System models

In this section, we present the vulnerability analysis and explain the the interrelationship between them
Then we show our threat model considered for bio-cybersecurity. Finally, we describe the methodology to draw a vulnerability tree.

3.2 Security Vulnerability Analysis with NLP

NLP-based ontologies can support automation and the integration of vulnerabilities, cyber resiliency, and IT risk management. Based on that vulnerabilities analysis, vulnerabilities assessment involves also textual information, and vulnerabilities management products using NLP can correlate the requirements of various frameworks and methodologies against aggregated data from a cyber environment [6].
In recent years, Cyber-attacks have become one of the world's foremost safety and economic threats. Cybersecurity engineers use CVE, which are industry-standard records, to analyze and address known threats [8].
In this work, we tried to analysis CVE by using NLP and find the vulnerability interrelationship. Our proposed work includes different steps to analysis data and finds interrelationships between different vulnerabilities.

3.2.1 Cybersecurity Data Analysis:

In the proposed method, CVE records have been downloaded directly from CVE ® Program Mission. The dataset, which is the primary state of this study, has been tested and developed in the list of CVEs regarding the Linux kernel.

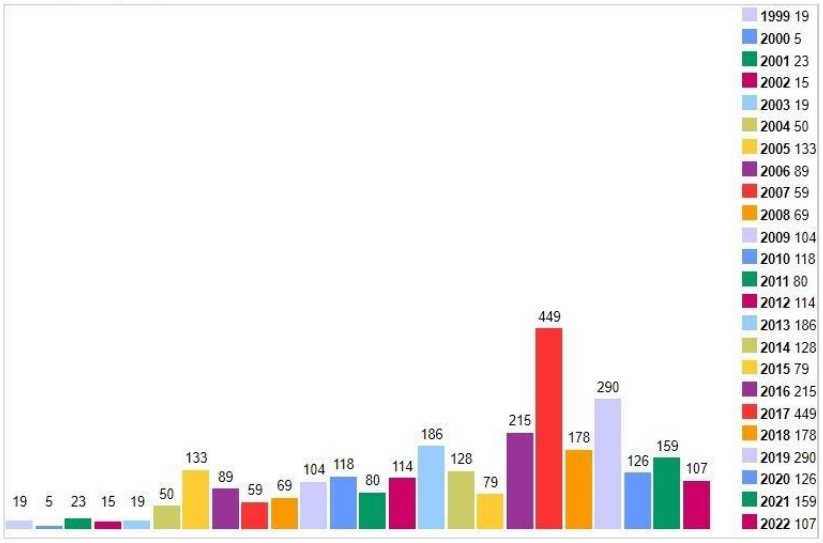

Fig 2. Analyse vulnerabilities by year

Figure 2 shows, the number of vulnerabilities in different years. After categorizing system vulnerabilities based on the year, we classified the vulnerabilities by type to check their interrelationship of them (Fig. 3).

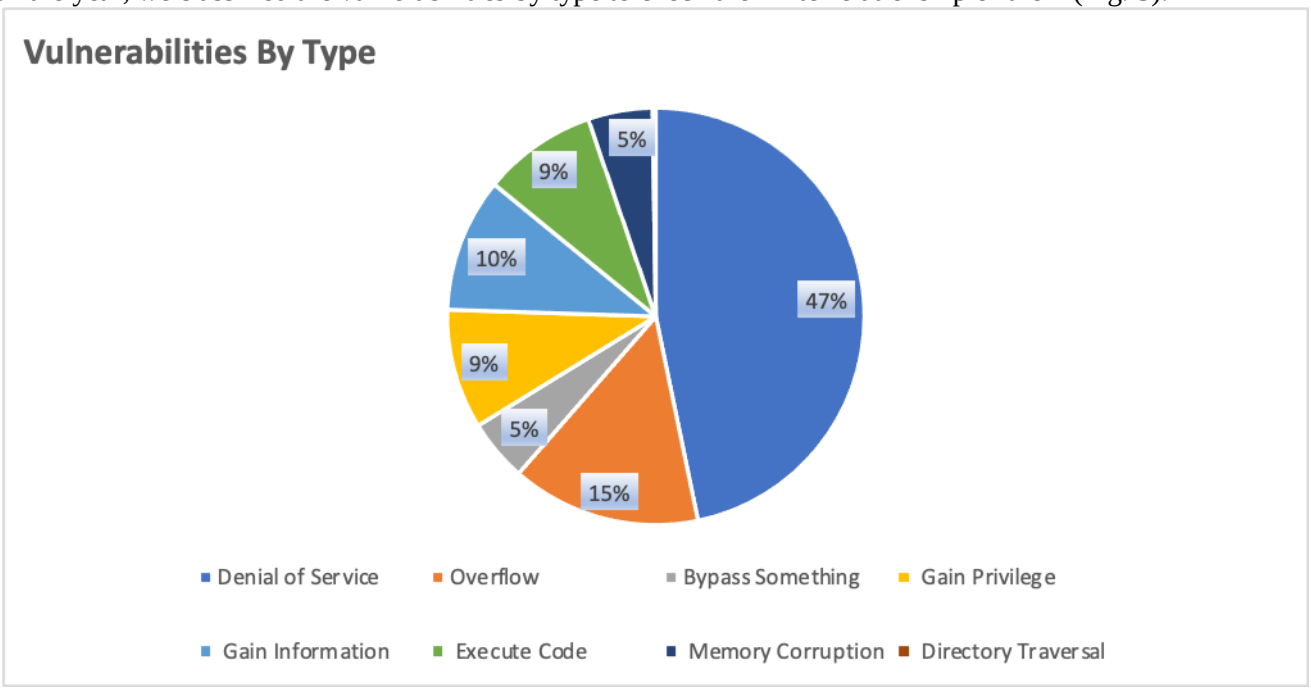

Fig 3. Analyse Vulnerabilities by Type

As Figure 3 illustrates, the most common vulnerabilities which threaten our systems or devices are Denial of Service and Overflow attacks, 47% and 15%, respectively. This is mainly because these kinds of attacks require special programs to run, and threat actors can easily access sensitive information by applying them to a system.
A Denial-of-Service (DoS) attack is defined as an attack that results in the shutdown of a machine or network, making it inaccessible to users. DoS attacks carry out the attacks by flooding the target with high traffic or sending the information or data that triggers a crash. DoS attacks include different types of Pings of Death, SYN Flood, Teardrop, and Buffer Overflow [16].
Buffer Overflow is one of the most comment types of DoS attacks which relies on sending a number of traffic to the network resource that exceeds the default processing capacity of the system [17].

3.3 Evaluation

Table 1. indicates the relation between biology and cybersecurity These similarities have introduced the field of bio-inspired cybersecurity, and it has been recognized by cyber professionals. We also determined that bio-cybersecurity can different vulnerabilities classification.
By this methodology, professional recognition of overlap between biology, cyber operation, and different vulnerabilities has also emerged in the field of cybersecurity, which can identify the blurring of the domain borders between biology and cyber and acknowledges new risks arising from the growingly cyber-physical nature of biotechnology. For example, today, DNA scientists are able to design genetic code that lets hackers inject malware into computer systems or devices. On the other hand, the accessibility of DNA sequences in bioinformatics systems suggests the probability for hackers to change genetic code in a way that converts a benign organism into a harmful pathogen [13].

Table 1. The relationship between Biology and Cybersecurity

Function	**Vulnerability**	**IT Infrastructure Action or Term**	**Cell Biology Action or Term**
Barrier defence	Directory Traversal	Exterior Router Packet Filter/Stateful Inspection Firewalls Intrusion Detection Systems	Plasma Membrane/ Plant cell wall Oligasaccharins “oxidative brust”
Barrier Transmission and Communication	Denial of Service Overflow Execute Code	Tunneling protocols Secure Sockets Layer Virtual Private Networks Advanced Encryption Mechanisms Network Ports	Variety of Member Channels Gap Junctions Facilitated Diffusion and Transporters (i.e., Glucose) Extrasellar matrix signaling
Internal Organization	Bypass Something	Internal Firewalls Network DMZ (Buffer Zones)	Membrane- bound organelles, mitochondria Nuclear pore complex, double membrane envelope
Internal Routing and Sorting	Gain Privilege Gain Information	Email, standard Fax, telephone IPv6 Routers, routing Table	Endocytosis, Exocytosis Golgi Apparatus Cell Nucleus
Virus Defense and Response	Memory Corruption	Infection Carrier System Cleansing (anti-virus s/w) System Isolation System Corruption	Infection Carrier Intracellular digestion, endocytosis Cell Division Cell Death

Now based on our findings we can propose a vulnerability tree for these types of attacks.

3.4 Vulnerability Tree Model

The vulnerability tree has been modelled as a hierarchy of trees that the top hierarchy considered the main goal of the attacks or parents; it has symbolized with a capital 'V'. There are different ways can be exploited a top vulnerability. Each of these ways has built a branch or leave of the tree. These branches are known as child vulnerabilities and are symbolized with the lower case 'v' (Fig. 4). The vulnerability tree typically depicts the relationship between one vulnerability and other vulnerabilities, as well as the steps that a threat agent should take to reach the top of the tree [18].

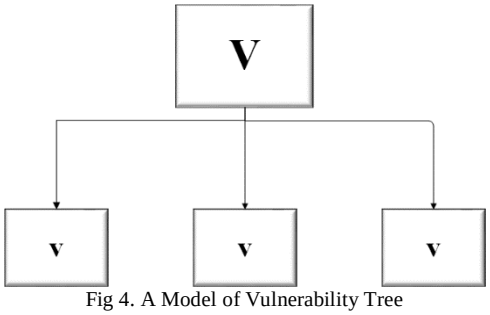

Fig 4. A Model of Vulnerability Tree

As we discussed earlier, DoS and Buffer overflow attacks can threaten systems more than others. They show the same behavior (flooding services or crashing services). Based on table 1 and proposed vulnerability tree, we can conclude that these types of attacks can fall into the barrier transmission and communication function category, in fact, we can classify them in the same category. Therefore, by using the learning and memory capabilities of the bio-cybersecurity to detect and remember so far different attacks as well as the definition of the vulnerability tree, we can propose a model of vulnerability tree (Fig 5).

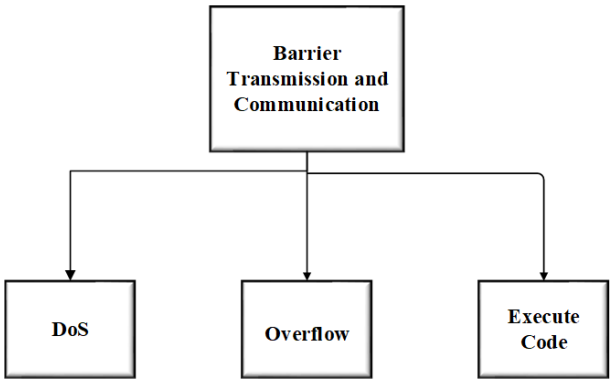

Fig 5. Proposed Vulnerability Tree

Figure 5 illustrates the interrelationship between Barrier Transmission and Communication attacks as parents and other attacks as their children. The interrelationship between these kinds of vulnerabilities can be classified to environment and methodology, which used to get access to their targeted system. By using this model and inspiring the human immune system, we can improve the security of the system.

Cyber immunity is a method that relies on the human immune system that has the ability to learn and identify attacks with unknown signatures. By using vulnerability trees, we can accelerate this process. Since the interrelationship between different vulnerabilities helps us to provide a detection and defense strategy for parents at the top of the tree, which can apply to the children if system faces multi attacks.

4. Conclusion

In this paper biology, cybersecurity and vulnerability interrelationship have been considered jointly, to reduce the risks and dangers, which threaten sensitive data and sensitive information of the systems. In recent years, cyberattacks increase at a significant rate. In this so-called modern world, sensitive information and data can leak easily by attackers. Therefore, detection and defense are the most important parts of any system of security. This methodology is intended to help researchers and system designers gain deep insight into multi attacks and how they are jamming.

References

[1] Guthikonda A, Al-Shaer E, Farooq A, Raja MY. Bio-inspired innovations in cyber security. In2017 14th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT (HONET-ICT) 2017 Oct 9 (pp. 105-109). IEEE.

[2] Spiering MJ. Primer on the immune system. Alcohol research: current reviews. 2015;37(2):171.

[3] Farmer JD, Packard NH, Perelson AS. The immune system, adaptation, and machine learning. Physica D: Nonlinear Phenomena. 1986 Oct 1;22(1-3):187-204.

[4] Hassan M, Mylonas A, Vidalis S. WHEN BIOLOGY MEETS CYBER-SECURITY. Journal of Information System Security. 2016 Jul 1;12(3).

[5] Tarao M, Okamoto T. Toward an artificial immune server against cyber attacks: enhancement of protection against DoS attacks. Procedia Computer Science. 2016 Jan 1;96:1137-46.

[6] Igbe, Obinna. "Artificial immune system based approach to cyber attack detection." PhD diss., The City College of New York, 2019.

[7] Urbanska M, Ray I, Howe AE, Roberts M. Structuring a vulnerability description for comprehensive single system security analysis. Rocky Mountain Celebration of Women in Computing, Fort Collins, CO, USA. 2012 Nov.

[8] Rodriguez C, Zamanirad S, Nouri R, Darabal K, Benatallah B, Al-Banna M. Security vulnerability information service with natural language query support. InInternational Conference on Advanced Information Systems Engineering 2019 Jun 3 (pp. 497-512). Springer, Cham.

[9] Tablan V, Damljanovic D, Bontcheva K. A natural language query interface to structured information. InEuropean Semantic Web Conference 2008 Jun 1 (pp. 361-375). Springer, Berlin, Heidelberg.

[10] Lopez V, Fernández M, Motta E, Stieler N. Poweraqua: Supporting users in querying and exploring the semantic web. Semantic web. 2012 Jan 1;3(3):249-65.

[11] Bitam S, Zeadally S, Mellouk A. Bio-inspired cybersecurity for wireless sensor networks. IEEE Communications Magazine. 2016 Jun 23;54(6):68-74.

[12] Pourmoafi S, Vidalis S. Bio-Cyber Operations Inspired by the Human Immune System. In European Conference on Cyber Warfare and Security 2021 Jun 1 (pp. 534-XIV). Academic Conferences International Limited.

[13] Wlodarczak P. Cyber immunity. InInternational Conference on Bioinformatics and Biomedical Engineering 2017 Apr 26 (pp. 199-208). Springer, Cham.

[14] Mthunzi SN, Benkhelifa E, Bosakowski T, Hariri S. A bio-inspired approach to cyber security. InMachine Learning for Computer and Cyber Security 2019 Feb 5 (pp. 75-104). CRC Press.

[15] Rauf U. A taxonomy of bio-inspired cyber security approaches: existing techniques and future directions. Arabian Journal for Science and Engineering. 2018 Dec;43(12):6693-708.

[16] Mahjabin T, Xiao Y, Sun G, Jiang W. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks. 2017 Dec;13(12):1550147717741463.

[17] Gupta S. Buffer overflow attack. IOSR Journal of Computer Engineering. 2012 May;1(1):10-23.

[18] Vidalis S, Jones A. Using vulnerability trees for decision making in threat assessment. University of Glamorgan, School of Computing, Tech. Rep. CS-03-2. 2003 Jun 30.

[19] Abraham C, Chatterjee D, Sims RR. Muddling through cybersecurity: Insights from the US healthcare industry. Business horizons. 2019 Jul 1;62(4):539-48.

First Author Seyedali Pourmoafi is a lecturer of Computer Science in School of Physics, Engineering and Computer Science (SPECS), University of Hertfordshire. He received BSc and Msc from University of Herefordshire. The main area of his research is cybersecurity and operating system and new working. He received an award as a second paper in In European Conference on Cyber Warfare and Security in Jun of 2021. He is finishing up my Ph.D. study in Cybersecurity. His research interests are in the areas of Information Security, Information Operations, Digital Forensics, Threat Assessment, Profiling and effective computer defense mechanisms

Second Author Dr Stilianos Vidalis is Deputy Head of Department of Computer Science, School of Physics, Engineering and Computer Science (SPECS), University of Hertfordshire. He received his PhD in Threat Assessment under the context of Information Security in July 2004. His research interests are in the areas of Information Security, Information Operations, Digital Forensics, Threat Assessment, Profiling and effective computer defense mechanisms and he has published a number of papers in those fields.