Response Mechanism for Defending Computer Networks

C. Onwubiko and A.P. Lenaghan

Networking and Communications Research Group
Faculty of Computing, Information Systems and Mathematics
Kingston University, Penrhyn Road, Kingston Upon Thames, KT1 2EE, UK.

Summary:

With the significant reliance of proactive monitoring of computer networks on security information management systems, a requirement is to provide appropriate and comprehensive countermeasures to perceived threats on the entire network. A security response mechanism is proposed that combines both generic and fuzzy response models to provide automated (static and dynamic) security countermeasures, and human assistance to mitigate distributed security threats perceived on a population of the network.

Keywords:

Response mechanism, fuzzy responder, human assistance security threats, computer networks

1 INTRODUCTION

Traditional network security techniques utilise "point type solutions", such as, user authentication, encryption and firewall to protect computer networks as the first line of defence. But it is shown that these techniques are not sufficient in preventing network security attacks [1], in particular, emerging threats that are distributed in nature, and often coordinated (see figure 1). As a result, recent security efforts are shifting their focus from "point type" countermeasures to mechanisms that adopt a more distributed perspective. Point solutions such as firewalls at the LAN/WAN boarder or virus checkers on end users machine are stand-alone systems that operate in isolation and at specific points in the network. There are no centralised analyses to coordinate inputs from these systems, as a result, the countermeasures provided by these types of security initiatives are not adequate in mitigating or addressing the security needs of emerging threats, such depicted in figure 1.

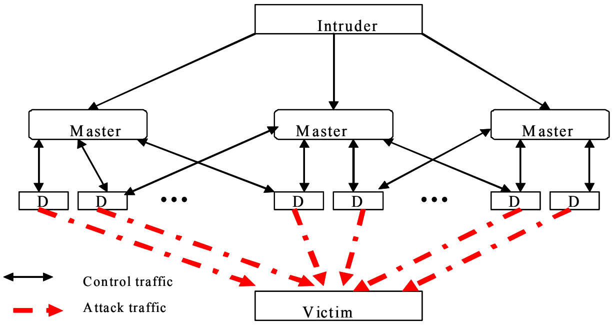

Figure 1: An Instance of a Distributed Attack

Figure 1 is an example of a typical distributed attack system [2]. The "*intruder*" controls a small number of *"masters"*, which in turn control a large number of *"daemons"*. These *daemons* (*denoted with a 'D'*) can be used to lunch packet flooding or other attack types against *"victim*" (a target system by the intruder). *Daemons* are software agents installed on most sites, typically through the exploitation of well-known vulnerabilities that lead to root privilege on the compromised system; in fact, some of the daemon programs do not require root privilege to lunch an attack. One significant characteristic of such attacks is that they are distributed and therefore emanate from different egress points (*the daemons*), although controlled from a single source (*the intruder*).

Point security solutions detect, record, and may take action to mitigate threats. In contrast a distributed security infrastructure operates across a population of the network (entire network). And distributed solutions offer three significant advantages over point solutions, namely their abilities to:

i) Collate information about attacks across a population of hosts rather than an individual host
ii) Analyse information about attacks across a population of hosts rather than an individual host
iii) Coordinate the deployment or reconfiguration of multiple countermeasures across a network.

In these respects they have the potential to identify emerging threats earlier and respond more effectively than point security solutions.

In this paper, we argue for a response mechanism that provides capabilities to coordinate the deployment or reconfiguration of multiple countermeasures across the whole network. Countermeasures provided are automated and human assisted. This richer model (response mechanism) offers capabilities that provide appropriate and extensive security countermeasures to mitigate a wide variety of threats.

A defence system that provides capabilities for automated countermeasures and also cooperates human expertise in providing countermeasures pertinently and significantly offers extensive and appropriate response mechanisms than models that provide only a subset of countermeasures. Our contributions in this paper are:

1. To propose a security response mechanism that offers capabilities for automated and human assisted countermeasures by coordinating generic and fuzzy related responses. Which in turn assists in providing comprehensive and appropriate countermeasures to emerging security threats, and
2. To discuss an approach in realising the proposed response mechanism.

The rest of the paper is organised as follows: Section 2 deals with distributed defence infrastructure. Section 3 explains the proposed response mechanism in a distributed defence framework; and in section 4, security response mechanisms and related work are examined; and finally in section 5, we conclude with a discussion.

2 DISTRIBUTED SECURITY INFRASTRUCTURE

A distributed security infrastructure divides the task of securing a network into separate functions for sensing, analysing and responding to threats [3]. The task of securing a network implies:

i) Sensing (detecting) threats: Sensors are distributed across the network to gather and communicate threat evidences perceived.
ii) Analysing (synthesizing) threats evidences: Efficient techniques are utilised to analyse, synthesise and evaluate threat evidences communicated by the sensors.
iii) Responding (mitigating) threats: Adequate countermeasures are deployed in mitigating perceived threats based on collective human and intelligent decision from the analysis.
iv) Coordinating these security inputs is a signalling mechanism (security space) that enables sensors, analysers and responders to connect, contribute and communicate security related information, (see figure 2)

However, the task of responding to threats is further divided into separate functions as we focus on discussing response mechanisms in a distributed defence framework. Subtasks are as follows:

a) Automated Countermeasures: countermeasures automatically deployed by the responders to mitigate perceived threats on a population of the network.
b) Manual Countermeasures: security related information are communicated through alert and alarms messages to security administrators who then apply adequate countermeasures to perceived threats.

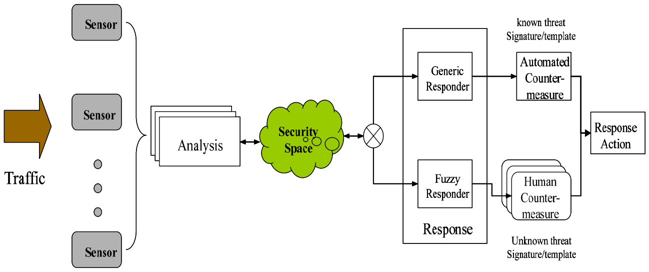

Figure 2: Distributed Defence Framework

Figure 2 is a distributed defence framework underpinned on *sensor, analysis and response* paradigm, discussed in [4, 5, 6]. It is a logical distributed defence framework that defines 4 types of component; *sensor components* that contribute evidence about security related events, *analysis components* that implement autonomous software agents capable of analysing evidence, an abstract *"security space"* through which sensor and analysis components communicate, and finally *response components* implement countermeasures and can be configured to protect networks. The logical components of the framework are realised on physical network nodes. A physical network node may realise one or more logical components and may interact with one or more security spaces. The framework is proposed for detecting distributed threats, however, in this paper we focus on response mechanisms of the framework in mitigating security threats. The underlying concept in this framework is the capability for sensors to connect, contribute and communicate security information to the analysers (analysis module); where threat evidences are fused, synthesized and analysed. At the analysis module appropriate countermeasures are recommended, while at the response component, recommended countermeasures are executed. Responses made could be the reconfiguration of security policies to mitigate the perceived threats, or a combination of sequences of countermeasure actions.

2.1 Definitions

Sensors are security mechanisms that sense, gather and communicate security related information and threat evidences to the analysis components (analysers).

Analysers process sensor data (for example, security evidences gathered by the sensors) to deduce the risk level or potential damage the threat presents to the network, and therefore, inform resultant countermeasures required for the perceived threat agent.

Responders implement recommended countermeasures, for instance, coordinating of some countermeasures or re-configuring security components to nullify perceived threats. It is pertinent to note that the responders are not unintelligent elements that just execute countermeasure action; but also possess the potential to interact, deduce, change or respond differently from pre-assigned response action by the analyser.

A security space is an abstract space (middleware) through which security components (*sensors, analysers* and *responders*) connect, contribute and communicate security related information.

2.2 Security Information Management Systems

Security information management systems (SIMS) are use for proactive monitoring of computer networks for enterprises. SIM solutions encompass security mechanisms distributed across the entire network, such as firewall systems, intrusion detection systems, vulnerability scanner systems and intelligent analysers integrated to provide a unified defence model. They can therefore be used to correlate, normalise and analyse security events from varying network security sensors/sources to provide a unified actionable logic for protecting an enterprise network. *Correlation* is a technique applied to show the relationship of security events coming from different sources in the entire network. This enables the system compare and analyse sequences of security events, thereby allowing for improved detection capabilities. *Normalisation* is a technique applied to format the correlated security events in a particular pattern, which helps in prioritising events in a given context.

The relevance of SIM solutions are seen in areas such as: (a) Enterprise Network Monitoring, (b) Alert Correlation Coordination, (c) Threat Identification and Tracking, and (d) Vulnerability Assessment.

Security information management systems now utilised as complementary defence mechanisms to stand-alone point security solutions in proactive monitoring of computer networks. Proprietary [7, 8] and open source [9] security information management systems are rapidly being deployed.

It is overwhelming to monitor and manage enterprise computer networks for organisations without efficient security information management systems in place; however, the astuteness in SIM solutions are provided by the analysis of security event logs and audit trails coming from numerous security sources (intrusion detection systems, firewalls, security sensors, secure routers, antiviral systems and proxy gateways) that output security logs in different formats.

Event logs or audit trails provide only symptomatic evidence, such as, (high CPU utilisation history, access-list violations, and failed resource) and therefore require detailed examination and analysis to combine these evidences to conclude on the specific threats to computer and network resources.

It is pertinent to note that current security information management implementations are only utilise for detecting security threats; none provides response mechanism capabilities.

2.3 Limitations in existing Response Mechanisms

Response mechanisms to computer networks exist, but they are implemented in a point solution perspective. For example, use of firewalls to drop, reset and log malicious sessions; or the use of intrusion detection systems to execute a filter to detect vulnerability exploit. However, these mechanisms are not implemented in distributed defence perspective, and therefore, are inadequate in mitigating distributed threats seen on the entire network.

Existing response mechanisms, such as, response offered by remediation services, patching and security prevention systems, lack the capability to implement comprehensive countermeasures, such as, adjusting preventive security mechanisms dynamically, self reconfiguration of detection systems, adjusting detector settings, adjusting internal system parameters, or providing a combination of different countermeasures actions [10].

Automated countermeasures applied by existing response mechanisms, such as, drop, reset or log a session are significantly inadequate to appropriately address emerging security threats and often lag behind threats to mission critical information systems [11].

Similarly, there is a concern that monotonic response action, such as use of firewall to drop a session, or use of IDS to alert of a security breach, provided by existing response mechanisms are insufficient to mitigate emerging threats that exploits multiple chains of vulnerabilities in succession in systems [12,13].

Security information management systems now utilised as complementary defence mechanisms to stand-alone point security solutions in proactive monitoring of computer networks in detecting security threats. However, a concern already expressed is if security information management systems can live up to their promise [14].

3 RESPONSE MECHANISM

The proposed response mechanism comprises of five components (see figure 3) namely:

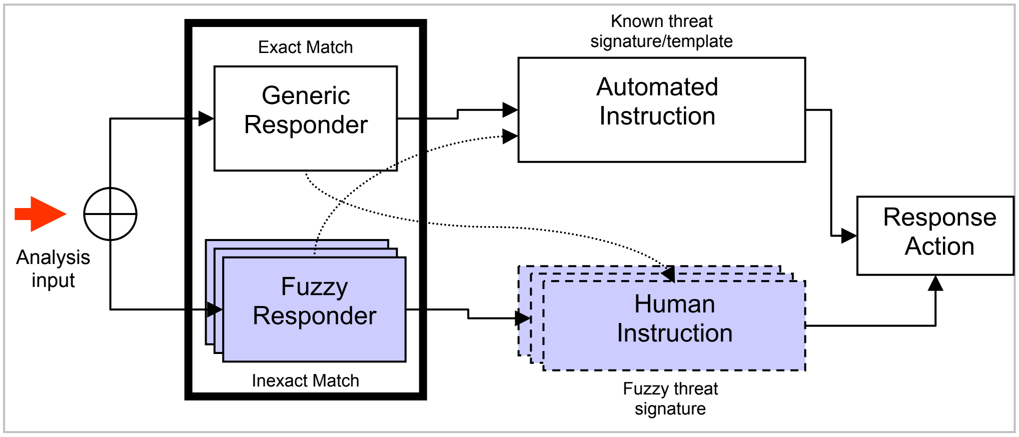

Figure 3: Components of the Response Mechanism

Generic responders apply '*hard*' response to threats. A hard response is a security response applied to a threat with exact or known signature (*threat template*), and therefore stipulates a given set of countermeasures.

Fuzzy responders apply a combination of countermeasures or invoke other security components (for example, detectors) to '*soft*' response. A *soft* response is a security response applied to threats with unknown threat attributes or for freshly identified threats that have no existing countermeasures in place at the given time. ***Automated instructions*** are instructions recommended by generic responders, while ***human instructions*** are instructions recommended by fuzzy responders applied to '*fuzzy-type'* threats by security administrators. ***Response action*** is the resultant countermeasure instruction that must be executed to mitigate a prevailing or perceived threat (see figure 3).

"*Soft*" response to a security threat is employed when the analysis evidence is not so concrete or "crisp", rather suggestive. A "*Hard*" response is implemented when the analysis suggests known security threats that match existing "*threat template or profile*". A Threat template is a template of known security vulnerability definition (*threat signature*); while a *threat profile* is a baseline profile of known security breaches.

The response component executes countermeasure recommendations from the analysis component. And responses to threats can be precise (for known threat signatures), for example, using filters to stop a specific security threat. This implies rule based filters applied to misuse type of intrusive threats, for example, ***if*** *port=80* ***and*** *type=HTTP,* ***and*** *priority=high*, ***and*** *reliability=high*, ***then*** *log*. While some responses can be very fuzzy, in which case, a single countermeasure may not be adequate, and therefore, complex countermeasures are required either as a combination of actions or the reconfiguration of some preventive security mechanisms. Anomaly intrusive activities that use indicators to depict level of threat or threat patterns may be vague and suggestive. For example**,** ***if*** daily utilisation exceeds a certain threshold, and ***if*** packet per second (pps) is higher than baseline threshold (pre-set threshold), ***then*** traffic behaviour suggests some intrusive activities are ongoing. This is not exactly correct, because traffic patterns are seen to change even with normal behavioural utilisation, and may not suggest real attack [15]. Such fuzzy-type threat behaviour requires fuzzy-type countermeasures as discussed in section 3.1.

3.1 Components of the response Mechanisms

Generic Responders: are rule-based responders that apply to threats with known threat attributes (*threat signature*). For example, if the analyser outputs a threat as a *UDP-type worm exploit* using UDP port 3304, it also commits a belief (like a probability) to ascertain its support on the perceived threat. This security evidence is sent to the *generic responder* that then executes a filter to drop, deny and log UDP port 3304 as countermeasures to the perceived threat. When a threat is seen on multiple hosts in the same subnet, the resultant countermeasure is executed on the gateway device that is closest to the infected systems. For instance, when a worm is sensed on a subnet infecting computer networks, the countermeasure applied is on the gateway router or switch, particularly, on the interface carrying traffic to those infected systems. This way, the effectiveness of the applied countermeasures in mitigating the threat is realised. Similarly, when threats seen on an entire network is not localised to a single subnet but rather on different subnets; in which case isolating a specific subnet to apply the resultant countermeasure is difficult since it is perceived on many different subnets. And, applying countermeasures to every subnet may lead to denial of service to a population of the network; the *generic responder* alerts security administrators for human decision-making and countermeasures. This design construct is a significant proposition in this model as we aim to develop an *assistance system* rather than automating all the functions of the system, which could significantly complicate their behaviour.

Fuzzy Responders: are implemented using Dempster-Shafer combined rule as an inference mechanism for countermeasure recommendations to threats. Dempster-Shafer theory of evidence [16] is mathematical theory of evidence based on *belief.* The underlying principle behind D-S theory of evidence is the concept of *belief function* as an adequate representation of one's degrees of belief in an evidence; the notion of *doubt* and *plausibility* used to reason and compute inconsistency in evidence and support belief in the quality of evidence provided respectively; plus the ability to combine a diverse variety of evidence through its *rule of combination. Rule of* combination is use to aggregate multiple sources of evidence to obtain a higher level of abstraction that is better and more meaningful. There are numerous publications in the literature for Dempster-Shafer, see [17, 18].

Inferences obtained using D-S theory of evidence recommend countermeasures, which are implemented either through automated instructions or human assistance approaches. Countermeasures implementation using fuzzy responders include:

i) Adjust preventive security mechanisms, such as, updating anti-virus checkers, executing authentication proxies, or lowering security guards
ii) Redirecting traffic to remediation service for latest patch updates
iii) Adjusting detector setting, for example, using firewall to drop, reset of log a specific session, or using IDS to mitigate perceived sessions
iv) Traffic re-route, similar to traffic redirection,
v) Applying a combination of countermeasures, for example, log a specific session and redirect for remediation.

Automated Instructions: encompass static and dynamic countermeasure instructions applied to threats *with known threat attributes (profile).* Automated response mechanisms provide automated countermeasures to security threats. These include self-reconfiguration of some security measures, such as detectors or analysers; execution of a single or a combination of countermeasures. For example, sending signals to the firewall to block a certain traffic or use of intrusion detection systems to prevent a specific vulnerability incident. These instructions are automated because the perceived threat has a known signature (for *misuse-type*) or a predefined threat profile (for *anomaly-based*). Static automated instructions are *hard responses* such as:

i) Drop a traffic to certain port because of perceived vulnerability
ii) Re-direct traffic to remediation services
iii) Alert and log certain activity due to perceived threat activity
iv) Reset and deny a service if the service/traffic is seen to be illegitimate or of malicious intent.

Human Instructions: are applied when threat analysis suggests very complex threat attributes that either require multiple countermeasure instructions at different network segments, or without known threat templates. These sorts of countermeasures are deployed for freshly identified threats whose signatures are unknown, and appropriate countermeasures not fully developed. However, if the recommended action is one with known template/profile an automated response is applied; otherwise, a fuzzy response is applied, which include both automated and human assistance. Human instructions are administered through the security administrators who evaluate the analysis output over the intended countermeasure and its consequences therein.

The overall response mechanism is designed as an *assistance response system*, where responses are partly automated and partly human assisted. We do not recommend fully automating the system, which may significantly complicate their responses and behaviour.

4 SECURITY RESPONSE INFRASTRUCTURE

The role of responders in a distributed security infrastructure is to execute recommended countermeasures from the analysis component, where security threats are analysed. The premise for cooperating response mechanisms is three fold; firstly the analysis of information from the whole network is more pertinent than any individual countermeasures perspective. Secondly, a response that coordinates multiple countermeasures is potentially more effective than that which can be achieved by the sum of the responses of a set of point countermeasures. Thirdly, a response mechanism that combines both automated and human countermeasures provides extensive and appropriate mitigation to threats than that which can achieve only a subset of all possible countermeasures.

In discussing the needs of a security response infrastructure a separation is made between general design principles and more concrete requirements.

4.1 Design Principles

Three principles guide the proposed approach:

a) The approach should be simple, scaleable, responsive, extensible, flexible, robust and future proof.
b) The goal is to *assist* network security experts in their decisions while still providing lightweight automated response to known threat signatures.
c) The impact of the mechanism on existing network services or infrastructure should be minimized

4.2 Response Infrastructure Requirements

The requirements for a response mechanism to implement a distributed security infrastructure are that, it:

1. Supports both automated and human countermeasures to be implemented that allows the

model to mitigate perceived threats on a population of the network

2. Allows a combination of countermeasures (reconfiguration, remediation, and deployment)
3. Be flexible and sufficiently open ended to accommodate a wide range of countermeasures.

4.3 Related Work

The work presented in this paper is a continued effort to investigate distributed defence security mechanisms to emerging security threats. Current contributions in this area include our security spaces [4], integrated security framework [5], security monitoring analysis mechanisms [6], which discuss and demonstrate signalling requirements, defence paradigm and threat detection for distributed computer networks respectively. DARWINS' project (Detection, Analysis and Response, using a Web-based Infrastructure for Network Security) [19] a medium through which this research work is investigated. And the workshop on logical foundations [7] that outlined the decidability and complexity issues with distributed adaptive defence models.

5 DISCUSSION

In this paper we present a security response mechanism that cooperates with security experts (human security administrators) to provide adequate and efficient countermeasures to distributed security threats perceived on a population of the network. The response mechanisms are encapsulated in a distributed defence framework, underpinned on *sensor, analysis and response* defence paradigm, which has been utilised in security monitoring environments for detection and mitigation of security threats [15]. This work is still ongoing, although, the focus of this paper is regards response mechanisms, but the collective effort is pioneered towards developing a framework that assists security analysts detect and mitigate emerging computer network threats that appear to be distributed and often coordinated; variants of such threats as shown in figure 1.

It is imperative to mention that this work is not aimed at developing another type of IDS (intrusion detection system), but towards a data fusion of sensor evidences (IDS, firewall, scanner and anti-virus evidences) combined to detect threats on federated or distributed LANs. Therefore, this work is viewed to complement IDS, or distributed IDS initiatives, since without these toolkits our work will greatly suffer.

In the future, we plan to investigate how well these mechanisms can be implemented to detect, analyse and mitigate security threats in a testbed environment, where real Internet traffic can be monitored.

Cyril Onwubiko received a B.Sc. degree (1st class honours) in Computer Science and Mathematics from Federal University of Technology, Owerri in 1996 and M.Sc. in Internet Engineering from University of East London in 2002. Currently, he is a PhD research candidate with the Networking and Communications Group, Faculty of Computing, Information Systems and Mathematics at Kingston University. He works as a Security Analyst at COLT Telecom. Group, London, UK and a Security Consultant with the Gerson Lehrman Group, NY, USA. His research interests are in the areas of Computer Network Defence, Network Security, Threat Detection and Cryptanalysis.

Dr. Andrew Lenaghan is a Principal Lecturer in Data Communications, and Field Leader for undergraduate students in Computer Science and Software Engineering; also a member of the Networking and Communications Group, Faculty of Computing, Information Systems and Mathematics at Kingston University.

His research interests are in the areas of Online Handwriting Recognition, Computer Vision, Fuzzy Logic, Graph Theory, Global Positioning, Wireless Networking and Network Security.

REFERENCES

[1] Yang D., Hu C., and Chen Y. (2004) 'A framework of Cooperating Intrusion Detection based on Clustering Analysis and Expert System', *Proceeding of the InfoSecu04, Nov. 14-16, 2004, pg. 150-154, Pudong, China; ACM ISBN: 1-58113-955-1*

[2] CERT (1999); "Result of the Distributed-Systems Intruder tools Workshop", *CERT ® Coordination Center, Software Engineering Institute, Pittsburgh, Pennsylvania USA, November 2-4, 1999.*

[3] Marcus L. (2004), 'Introduction to Logical Foundations of an Adaptive Security Infrastructure', *Proceeding of Foundations of Computer Security (FCS'04) workshop on Logical Foundations of an Adaptive Security Infrastructure (WOLFASI), Turku, Finland 2004, pp.251-266*

[4] Lenaghan A., Onwubiko C., Hebbes L. and Malyan R.R. (2005), 'Security spaces for Protecting Users of Wireless Public Hotspots', *Proceeding of the IEEE -EUROCON 2005, IEEE Region 8, Belgrade, Serbia & Montenegro, Nov. 21-24, 2005*

[5] C. Onwubiko and A.P Lenaghan (2006); "An Evolutionary Approach in Threats Detection for Distributed Security Defence Systems"; *Proceeding of the 4th IEEE Conference on Intelligence and Security Informatics (ISI 2006), San Diego, California, USA, 23-24 May2006; ISBN: 3-540-34478-0, pp. 696 – 698.*

[6] C. Onwubiko, A.P. Lenaghan and L. Hebbes (2006) "An Integrated Security Framework for Assisting in the Defense of Computer Networks "; *Proceeding of the Joint IST Workshop on Sensor Networks & Symposium on Trends in*

Communications, SymptoIC'06, Bratislava, SLOVAKIA, 24 – 27 June 2006.

[7] Arcsight (2005), 'Enterprise Security Management', http://www.arcsight.com/ [29/01/06]

[8] Cisco Systems Inc (2005) 'CiscoWorks Security Information Management Systems (SIMS)', http://www.cisco.com/en/US/products/sw/cscowork/ps5209/ [29/01/06]

[9] OS-SIM (2004), 'Open Source Security Information Management', www.ossim.net/ [29/01/06]

[10] WOLFASI (2004), 'W*orkshop on Logical Foundations of an Adaptive Security Infrastructure (WOLFASI*)', http://www.aero.org/support/wolfasi/ [29/01/06]

[11] Onwubiko C. and Lenaghan A.P. (2005), 'Vulnerability Assessment: Towards and Integrated Security Infrastructure', *Proceeding of the International Conference on Computer Science & Information Systems (ICCSIS 2005), June 2005, Athens, Greece. ISBN: 960-88672-3-1*

[12] S. Kaushik; Efficient Automated Network Vulnerability Assessment: *In Supplementary proceedings of the 13th IEEE International Symposium on Software Reliability Engineering (ISSRE 2002)*, Annapolis, MD, November 2002.

[13] A. Shnitko; Practical and Theoretical Issues on Adaptive Security: Workshop on Logical Foundations of an Adaptive Security Infrastructure (WOLFASI);A sub-workshop of the LICS Foundations of Computer Security (FCS'04) Workshop, LICS '04; July 12-13, 2004,Turku, Finland.

[14] B. Schneier (2004), "Security Information Management Systems: Solution, or Part of the Problem?", *IEEE Security & Privacy , September/October 2004*

[15] Onwubiko C. and Lenaghan A.P. (2006), 'Spatio-Temporal Relationships in the Analysis of Threats for Security Monitoring Systems', *Proceeding of the 2nd International Conference on Computer Science & Information Systems (ICCSIS 2005), June 2006, Athens, Greece.*

[16] D. L. Hall, S. A. H. McMullen (2004) " Mathematical Techniques in Multisensor Data Fusion", ©2004 Artech House, INC., 685 Canton Street, Norwood, MA 02062, ISBN: 1-58052-335-3, 2nd Edition

[17] C. Katar (2006), "Combining Multiple Techniques for intrusion Detection*", IJCSNS International Journal of Computer Science and Network Security, Vol. 6, No. 2B, February 2006*

[18] L. Xu, A. Krzyzak, C. Y. Suen (1992), "Methods of Combining Multiple Classifiers and Their Applications to Handwriting Recognition", *IEEE Transactions on Systems, MAN, and Cybernetics, Vol. 22, No. 3, May/June 1992*

[19] Networking and Communications Research Group (NCG), Kingston University (2005), 'DARWINS - Detection, Analysis and Response, using a Web-based Infrastructure for Network Security' http://ncg.kingston.ac.uk/frames.htm