*International Journal of Innovative Computing, Information and Control*
Volume **1**, Number **4**, December **2005**

ICIC International ©2005 ISSN 1349-4198
pp. 715–725

# SECURITY IN HETEROGENEOUS LARGE SCALE ENVIRONMENTS USING GRID TECHNOLOGY

Michael Pilgermann, Evangelos Morakis
Stilianos Vidalis and Andrew Blyth
School of Computing
University of Glamorgan
Pontypridd, CF37 1DL, UK
{ mpilgerm, emorakis, svidalis, ajcblyth }@glam.ac.uk

Received September 2004; revised June 2005

Abstract. *The Information Security Team of the University of Glamorgan has started developing a GRID for digital security in heterogeneous large-scale environments. This paper will present an overview of the next generation Intrusion Detection Systems that will unite organisations in forming Virtual Communities for collectively defending their informational infrastructures against cyber-threats. The solution will use Peer-to-Peer distributed data analysis/mining approaches in order to overcome the current architectural and design limitations that are hampering the use and wider development of IDSs.*
**Keywords:** Digital security, GRID, Peer to peer, Data mining, Data unification, IDS, Virtual communities

1. **Problem Statement.** In our modern electronic world, securing a large-scale environment can be seen as a complex problem that requires a lot of resources and intensive computing power. Organisations are forced to allocate considerable resources in protecting their information assets but statistics [9] indicate that there is no stopping to hacking activities. The authors believe that security can only be achieved through effective policing.

One tool for "policing" the cyber-world is the Intrusion Detection Systems (IDS). Over the last decade IDSs have become increasingly important for the protection of computer networks. Apart from other evolutions in the IDS area, such as everlasting new detection mechanisms [10], generalisation [14] and aggregation [18] of alerts, a tendency for implementing Enterprise Intrusion Detection Systems has become conspicuous. What we need is an automated tool that will be able to detect, deter and react to any type of illegal cyber activity. The Information Security Research Team (ISRG) of the University of Glamorgan has chosen the GRID approach for solving the complex problem of ensuring digital security in heterogeneous large-scale environments.

Current technologies do not easily facilitate the flow of information across organisational and political boundaries. Consequently many organisations are forced to face network-based intrusions into their systems with little to no help from other organisations in the same supply chain. There is a need for the defenders of the Computing Information Infrastructures to come together and form a number of communities in order to take actions collectively against the perpetrator of an attack, and promote a culture of security