Enhancing Intrusion Response in Networked Systems

Maria Papadaki , Steven Furnell, Paul Dowland, Benn Lines, Paul Reynolds
Network Research Group, Department of Communication and Electronic Engineering, University of Plymouth, UK

Abstract

Increasing levels of attacks and misuse, as well as continuing organisational dependence upon computing and networked systems, have served to make intrusion detection systems an increasingly important security technology. However, although intrusion detection methods have received extensive research focus, the task of *responding* to attacks has received relatively little attention, particularly in the context of automated and active response systems.

The research relates to the design and practical evaluation of a novel architectural framework for intrusion response strategies, based on the identification of the range of factors influencing the response decision process and the adaptation of decisions according to custom response policies. The research is based on the Intrusion Monitoring System (IMS) architecture, and argues that a more comprehensive and reliable response framework is required in order to facilitate further automation of active responses. The poster presents a categorisation of the factors influencing response decisions, along with an overview of the proposed response architecture. It also presents details of an operational prototype system that is being developed, based upon the response architecture proposed.

Factors Influencing Intrusion Response

In order to address the automated response issue, it is important that further attention is given in the identification and assessment of factors that influence the response decision process.

Figure 1 depicts the main factors, split according to whether they relate to the incident or the IDS. The *incident* is the trigger for the response and still represents the principal influence over what should be done. However, assessment of the other factors enables the responder to establish the context of the incident, and select appropriate responses accordingly.

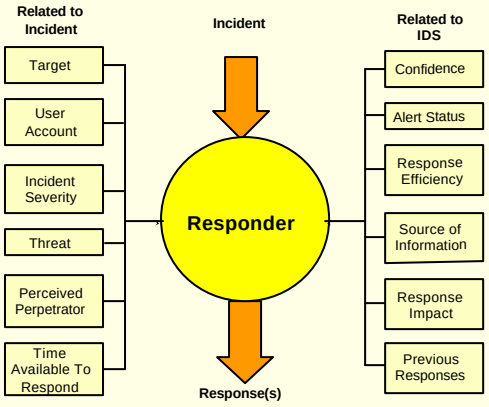

Figure 1: Contextual factors influencing intrusion response

The Intrusion Monitoring System (IMS)

IMS is a conceptual architecture for intrusion monitoring and activity supervision, based around the concept of a centralised host handling the monitoring of a number of networked client systems.

From the perspective of this research project, a significant element of the architecture is the Responder module, which is shown alongside other relevant entities in Figure 2 below.

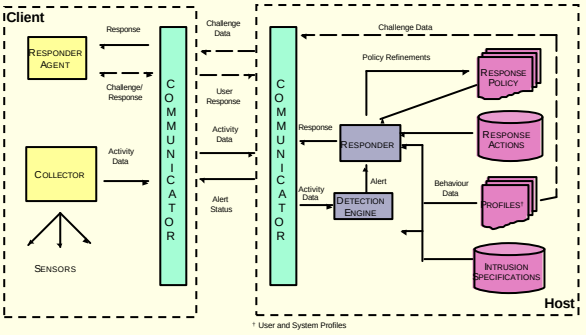

Figure 2: The Intrusion Monitoring System (IMS)

The **Responder** is responsible for monitoring the Alerts sent from the Detection Engine and, after considering them, in conjunction with other contextual factors, taking appropriate actions where necessary (e.g. correcting vulnerabilities, updating software, issuing authentication challenges, limiting access rights and increasing the monitoring level).

If the actions selected by the Responder need to be performed on the client side, a local **Responder Agent** is responsible for initiating and managing the process.

Having gathered all of the available information, the actions that should be initiated in different contexts are then specified in the **Response Policy**.

A Prototype Responder System

A prototype is being implemented to demonstrate the main response features of IMS, including the ability to make decisions based on the information from IDS alerts and other contextual factors. In the absence of a full Detection Engine, a console interface is provided to enable simulated intrusion alerts to be directed towards the Responder (see Figure 3).

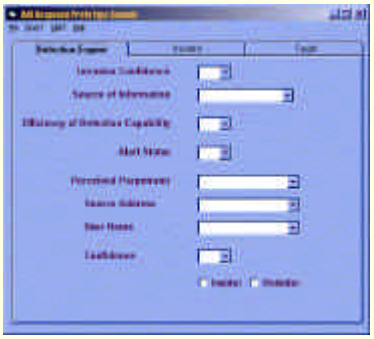

Figure 3 : Prototype Console Interface

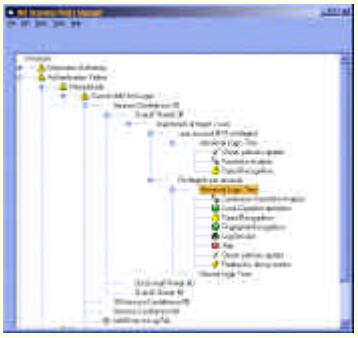

Figure 4 : IMS Response Policy Manager

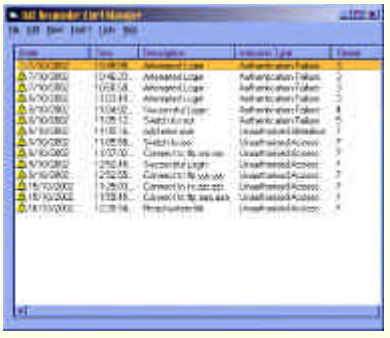

Figure 5 : IMS Responder Alert Manager

The Responder largely bases its decision upon the Response Policy, which can be accessed by selecting the **Response Policy Manager tool**, illustrated in Figure 4.

At the most basic level, there will be a one to one correspondence between a type of incident and an associated type of response. However, a more likely situation is that the desired response(s) to an incident will vary, depending upon other contextual factors.

During normal operation, the Responder logs the details of responses that have been issued so that they can be tracked and reviewed by a system administrator. This is achieved via the Alert Manager interface (see Figure 5), which contains a list of suspected incidents, allowing them to be selected and reveal the response action(s) initiated for them.

Papadaki M, Furnell S.M, Lee S.J, Lines B.M, and Reynolds P.L. 2002. "Enhancing Response in intrusion detection systems", *Journal of Information Warfare*, Volume 2, Issue 1, pp90-102.
Papadaki M, Furnell S.M, Lines B.M, and Reynolds P.L. 2002. "A Response-Oriented Taxonomy of IT System Intrusions", *Proceedings of Euromedia 2002*, M.Roccetti (ed.), Modena, Italy, 15-17 April 2002, pp87-95.
Dowland P.S, Furnell S.M, and Papadaki M. 2002. "Keystroke Analysis as a Method of Advanced User Authentication and Response", *Security in the Information Society: Visions and Perspectives*, M.A.Ghonaimy et al (eds), pp215-226.
Irakleous I, Furnell S.M, Dowland P.S, and Papadaki M. 2002. "An experimental comparison of secret-based user authentication technologies", *Information Management & Computer Security*, vol. 10, no. 3, pp100-108.
Papadaki M, Magklaras G, Furnell S.M, and Alayed A. 2001. "Security Vulnerabilities and System Intrusions – The need for Automatic Response Frameworks", *Proceedings of IFIP 8th Annual Working Conference on Information Security Management & Small Systems Security*, Las Vegas, 27-28 September 2001.
Furnell S.M, Magklaras G.B, Papadaki M, and Dowland P.S. 2001. "A Generic Taxonomy for Intrusion Specification and Response", *Proceedings of Euromedia 2001*, Valencia, Spain, 18-20 April 2001, pp125-131.

www.network-research-group.org