

Enhancing Graph-based Automated DoS Attack Response

– Extended Abstract –

Gabriel Klein, Marko Jahnke

Research Institute for Communication, Information
Processing, and Ergonomics (FGAN-FKIE)

{g.klein, jahnke}@fgan.de

24th March 2009

1 Introduction

‘GrADAR’ is an intuitive approach to create and maintain a model of a computer network and of the availability of its resources from the observations of deployed monitoring systems [JTM07, JTM08]. The graph-based model is able to express both the effects of DoS attacks and characterise the result of available response measures prior to their application in the real-world network. Thus, the approach provides a methodology for automatically selecting response measures to detected attacks. The most appropriate response is chosen based on metrics which are well-known from the pragmatic view of network security officers.

This contribution proposes an extension to our previous GrADAR approach that seeks to incorporate the effects of network and resource workload into the availability estimation. This should permit a more detailed modelling of the current network state and the effects of applied countermeasures to detected DoS attacks.

2 GrADAR Overview

The existing network is modelled as a directed graph, in which the vertices represent network resources, e.g. hardware components, software services, and even users. The edges between the resources represent availability dependency relations between the resources that are determined beforehand either analytically or experimentally. They are labelled with a weighting function that specifies the degree to which a resource is dependent on the other. This graph is called the *dependency graph* and effectively shows the ideal state of the network.

A DoS attack typically affects the availability of resources and there is also the possibility that some resources might no longer be accessible to others. Thus, in a second graph (the so-called *accessibility graph*), availability values are entered for those resources for which such values could be observed. For resources, for which availability cannot be observed, a value is estimated based on the availability of the resources it depends on and the corresponding weighting functions. This is done by propagation in the reverse direction of the resource dependency relation. As opposed to the dependency graph, the accessibility graph shows the actual current state of the network.

Once an attack has been detected, a countermeasure should be selected automatically. Each of the available response measures is applied to a separate incarnation of the accessibility graph. Such an application consists of changing availability values of vertices and/or adding/deleting edges and/or vertices. The resulting graph is known as a *response graph*.

The response graphs are then compared according to adequate metrics (e.g. expected success, application costs) and the countermeasure promising the best overall result is then applied to the actual network. This process is shown schematically in figure 1.

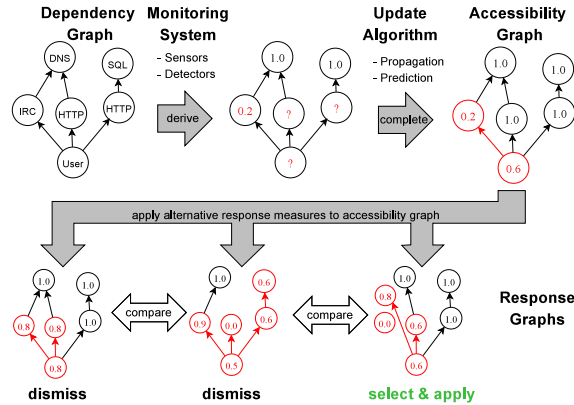


Figure 1: GrADAR — Schematic overview.

3 Proposed Extensions

During the validation of the GrADAR approach it became apparent that correctness and robustness could only be achieved if the precise effects of real-world countermeasures in the graph space could be accurately predicted. In the case of closing a firewall port or establishing a new server, it is relatively easy to specify these effects in terms of changed availability or changing edges in the graph. However, more complex interactions of resources such as putting workload on a resource or limiting access on the basis of stochastic processes (e. g. dropping IP packets in a randomised fashion) are not expressible trivially.

We propose to extend the GrADAR model with additional parameters for the workload of resources. Similar to the characterisation of a resource’s availability as the normalised duration of a transaction which is typical for the resource (see e. g. [M⁺06]), the definition of workload depends heavily on the use cases for the respective resource. It needs to be investigated whether the workload values of the resources depend on others, comparable to the availability dependencies mentioned above. This could allow the propagation of values for predicting the effects of responses in order to determine the most appropriate alternative. Additionally, it is assumed that there are certain relationships between the availability and the workload values.

As a collaborative effort with the Cooperative Cyber Defence Centre of Excellence (CCD-CoE) in Tallinn, Estonia, we plan to investigate the nature of workload effects that could be used for enhancing the prediction of availability values to make the suggested automated response selection process more accurate. The applicability of the enhanced approach needs to be experimentally verified. This should be achieved by comparing predicted workload and availability values with the ones observed by the network monitoring system.

References

[JTM07] M. Jahnke, C. Thul, and P. Martini. Graph based Metrics for Intrusion Response Measures in Computer Networks. In *Proc. of the 3rd LCN Workshop on Network Security. Held in conjunction with the 32nd IEEE Conference on Local Computer Networks*, Dublin, Ireland, Oct 2007.

[JTM08] M. Jahnke, C. Thul, and P. Martini. Comparison and Improvement of Metrics for Selecting Intrusion Response Measures against DoS Attacks. In A. Alkassar, editor, *Proc. of the Sicherheit2008 Conference*, Saarbrücken, Germany, Apr 2008.

[M⁺06] Mirkovich et al. Measuring Denial Of Service. In *QoP’06: Proceedings of the 2nd ACM Workshop on Quality of Protection*, New York, NY, USA, 2006.