NIRS

Network Intrusion Detection & Active-Response System

EXECUTIVE SUMMARY

MSc DCNDS Group 4
Department of Computer Science, University College London
Gower Street, London

Adedayo Adetoye
Andy Choi
Marina Md. Arshad
Olufemi Soretire

Supervisor: Steve Hailes

September 2003

Executive Summary

Introduction

Security is an important consideration in today's inter-networked global community. Communication networks, while playing an important role in governments, businesses, and organizations have become the target of malicious attacks. A particularly notorious attack is the Denial of Service (DoS) attack on data communication networks, which has the potential of crippling government networks and posing great threats to national safety and security, or business networks causing financial loss and loss of services with the attendant frustration of customers. There has therefore been a lot of effort in the research and business communities to find lasting solutions to this ever-increasing problem of network security. An approach is to create a database of known attacks and their solutions in form of Intrusion Detection Systems (IDS), which look for patterns matching the ones in the pattern repository to detect attacks. While this is a very good approach in detecting known attacks, it suffers in its inability to detect unknown or mutating attacks. The other approach to pattern or signature based detection is based on Anomaly Detection. It defines a profile for the system it is protecting and any deviation from that profile definition is considered an attack.

Intrusion detection is not the whole story, effective response to detected intrusion is equally as important. Many establishments depend on the expertise of their system administrators to interpret IDS logs and apply necessary system policies as a means of curbing further incidence of attacks. Many IDS also come with the option to respond to attacks defined in their repositories. But, since the repositories contain known attacks, the IDS could only respond to those defined attacks. The effectiveness of automatic response when using anomaly-based detection is generally dependent on the quality of the detection system.

Objectives and Scope

This project proposes an active response system to denial of service attacks on data communication networks. Using network traffic profiles, a collaborating community of software agents provide end-to-end security from intrusion detection to active response to DoS attacks. Given the accuracy of anomaly-based approaches, the proposed system will not replace but complement signature-based IDS. The security requirements of the agent system like authentication, or inter-agent communication protocols, and system policy description or specification will not be considered

Methodology

The use of traffic profiles for detecting denial of service attacks on data communication networks was proposed. It is believed that traffic characteristic is a common factor that could be used to identify network DoS attacks. Using a network-profiling agent, a protocol differentiated traffic profile was created during normal network usage. This formed the training set over which intrusion detection was based. In the detection mode, the profile previously generated was used to find anomaly; this was associated with a probability which indicated the level of confidence the detection system had that a sample constituted an intrusion or not. If the level of confidence exceeded a threshold an alert was sent to the response system, based on this a rate-limiting function was applied to the network.

Results

Using the Receiver Operating Characteristic (ROC) curve, a metric commonly used in the IDS measurement Community, the optimum operating point of the detection system was determined and used during active response to an emulated attack. The result of measurement showed that it is possible to detect and respond to DoS attack using network traffic characterisation. This is also a proof of concept for traffic profile-based IDS.

Conclusion

A traffic profile-based approach could be used as a defensive measure against DoS-type network attack. The objective of the project was realised. We concluded that active response using anomaly-based detection is feasible as a mitigation mechanism for such attacks.