

Application Of Ewatch Information Assurance Probes

Stephen C. Fortier & Jeff Rees
AverStar, Inc.
1593 Spring Hill Road, Suite 700
Vienna, Virginia 22182
(703) 827-2606
[sf, jeff.rees]@averstar.com

31 March 2000

Abstract

Purpose

This paper describes of our research in the area of real time distributed on-line intrusion detection. The EWatch technology was originally developed for application performance monitoring. EWatch has a number of capabilities that could be of value in areas other than application performance monitoring, the target of our product development. AverStar is developing information assurance probes, to be applied within the EWatch framework, to identify and alert the presence of malicious code in a distributed, real-time environment.

Methods

AverStar has developed a general-purpose interceptor capability that we have adapted to intercept messages being passed between various different technologies. Currently, these include COM, CORBA (VisiBroker), and ISAPI, and we're working on NSAPI and ODBC. As such, we are able to observe method invocations and parameter values on arbitrary components executing in a distributed system (i.e. we can record all component-level activity on a set of host computers). These include URL GET and POST operations in web servers (IIS and iPlanet, aka Netscape), the origins of user-level.

In addition, we are able to correlate events across distributed systems --- not just on a time basis, but also on a causality basis (i.e., method M on host H calls method N on host I). This is all very useful in application performance monitoring, enabling us, for example, to provide a component/process/host-level breakdown of the time spent processing user transactions --- even across technology and host boundaries.

Results

Currently, EWatch knows very little about what it's monitoring, simply correlating events along transaction paths. This technology has been very successful in monitoring application performance.

New or breakthrough aspect of work

The potential exists, however, to add intelligence to its interceptors, enabling them to detect interesting events when they occur in an individual process, and to add intelligence to its correlation engine, enabling EWatch to detect anomalous behavior relative to some predefined pattern, say, where the pattern might be expressed in terms of events occurring anywhere in a distributed system. As such, EWatch does provide a framework on which a variety of more sophisticated analysis capabilities could be built.

Conclusions

This paper will describe the results of configuring a number of EWatch probes to monitor malicious code or anomalous behavior across a distributed environment. This effort will explore a number of known attacks, as well as explore EWatch's application to denial of service attacks.