Contribution ID: **11** Type: **Oral**

An Active Security Infrastructure for Grids

Monday, 12 April 2010 15:30 (20 minutes)

To date, grid security activities have largely focused on prevention mechanisms, i.e., authorization,authentication, and secure communications. Here we present an Active Security Infrastructure (ASI) for grids, the design of which focuses on the areas of detection (e.g. intrusion detection), and reaction, i.e., taking action to prevent, or to recover from, a security incident. The infrastructure is composed of a distributed monitoring and control layer and an analysis layer. Communication between layers is via a grid information system.

Detailed analysis

Monitoring the current state of security is a vital task for those administering a grid. To secure a grid it is important that security information be available to site administrators in a timely and efficient way. ASI comprises a distributed monitoring and control layer and an analysis layer. The monitoring is performed using standard security monitoring tools (e.g. Snort) that have been enabled to allow any information gathered to be introduced into the grid information system. This information is analysed using an alert correlation approach based on the definition of attack scenarios. These scenarios model attacks as a sequence of steps, where each step takes the system from an initial secure state to a final compromised state. The output of the analysis is a single high priority correlated alert, possibly comprised from several lower priority alerts, and optionally an new grid policy. The grid policies generated by the analysis layer are distributed to the control layer, again through the grid information system, where they are enforced and any actions that should be taken to mitigate a possible security incident are applied.

Conclusions and Future Work

ASI delivers an end-to-end monitoring and control solution. The monitoring component combines standard NIDS and HIDS, and so is able to detect a broad range of intrusion types. It also allows for the dynamic addition of extra tools. The analysis component provides aggregation and and correlation services as well as dynamic grid policy generation. The policies automatically generated by the analysis can be used to provide active control on grid resources. Our experience deploying ASI on the Grid-Ireland infrastructure has shown it to be a useful addition to current grid security.

Impact

Grid-Ireland was established in 1999 to develop and coordinate the provision of a national grid service for the academic research community in Ireland. Grid-Ireland currently has a point-of-presence (Gateway) at 18 institutions. The day-to-day running of the Gateways is centrally managed by the Grid Operations Centre (OpsCentre) based in Trinity College Dublin. As the first stage in the full deployment of ASI on the Grid-Ireland infrastructure the monitoring component has been installed at 10 of the 18 Grid-Ireland sites. The analysis component is hosted at the OpsCentre. ASI has been continuously monitoring the Grid-Ireland infrastructure since June 2008, although several previous prototypes were deployed prior to this. At time of writing some 14 million alerts have been collected from the monitoring component to a security alert repository, the vast bulk of which are from Snort monitoring at the sites. Although the alert repository provides a useful auditing

tool in its own right, clearly it would not be practical for a human operator to detect a potential attack from amongst such a large number of alerts. It is for this reason that the analysis component is required.

Keywords

Grid information system, intrusion detection, IDS, alert correlation

URL for further information

https://www.cs.tcd.ie/Stuart.Kenny/index.php?id=activesecurity

Primary author: Dr KENNY, Stuart (TCD)

Co-author: Dr BRIAN, Coghlan (TCD)

Presenter: Dr KENNY, Stuart (TCD)

Session Classification: Security

Track Classification: Software services exploiting and/or extending grid middleware (gLite, ARC, UNICORE etc)