Motivation

Inherently tied to core characteristics of Grid infrastructures, new problems and challenges arise in comparison to conventional distributed systems, e.g., the support for the heterogeneity of the resource providers and for the highly dynamic virtual organizations (VO). The goal of the GIDS project was, on the one hand, to enhance the identification and detection of potential attacks and threats, and on the other hand to adopt early warning and reporting mechanisms to the Grid. The focus was to develop a concept for GIDS and to deploy a production-ready system for the D-Grid. Until the end of the project in June 2012 these tasks have been accomplished.

The main idea of GIDS is to cooperatively federate and exchange attack data among the participating resource providers in a data privacy compliant and lawful manner, while obeying individual security information policies found at the participating organizations.

Challenges & Highlights

Local IDS' data reporting on attacks on the Grid are collected and processed in the context of GIDS. As a matter of fact, parts of this data may also include personal data or even allow relating the data to a certain single person, which in turn let the project face the applicable German data protection act (BDSG). The BDSG regulates the collection, use, and distribution of personal data. In addition this data may also reveal critical security breaches to which one of the partners may potentially be vulnerable. On the other hand, it is important for the cooperative analysis of the collected data to gather as much unchanged information as possible. Thus, the main challenge was to find a suitable way to deal with the partially contradictory requirements to detect security incidents while ensuring the lawful handling of sensitive data.

For the project's success, it was important to guarantee every participating site its autonomy. In turn, this implied that no orders could be issued about which components have to be used or policies to be enforced. Due to this fact, the choice of the open source solution Prelude as a core component had been made. Since it is natively compatible to a variety of security systems and easily adaptable, Prelude as simple data collecting entity for the resource providers or even delivers local IDS functionality.

Each data has to be manipulated according to the data privacy protection concept as it is shared with other resource providers. This manipulation includes filtering any data in accordance with local information sharing policies. Additionally any personal data is anonymized or pseudonymized to comply with the legal regulations. Afterwards it is published via a bus system that guarantees essential security features, i.e. data integrity, confidentiality, and authenticity. By means of a global correlation engine, global intrusion detection was implemented to improve the preciseness and performance of security alerts, with special reference to distributed attacks.

To support Virtual Organizations (VOs), a user portal has been developed which allows VO managers and Grid users to retrieve information about the current security status of each resource in the Grid.

Potential applications & future issues

All components of the Grid-based intrusion detection system together with the underlying infrastructure were rolled out successfully and are in productive operation now. A variety of sensors are applied at different Grid sites and resource providers. The basic infrastructure to host the bus system as well as the global correlation engine is also in productive operation. A Grid user can access the portal website which is now part of the DFN-CERT infrastructure as an operational service. Due to the focus on scalability and adaptability the system could be used within international infrastructures in the future as well.

Logo:
Project abstract:

The GIDS project connects the local security systems of resource providers in the D-Grid. Several sensors collect potential attack data on each Grid site, which then are distributed throughout the GIDS infrastructure. A central system aggregates and analyzes these data and hereby helps administrators and Grid users to keep track of the Grid-wide security status.

Project duration:
01.07.2009 - 30.06.2012

Bibsonomy show project publications:
0

Bibsonomy use tabs to list publications:
0

Members:
szongott

Project manager:
M.Sc. Christian Szongott

Project research areas:

E-Science
Distributed Services

URL:
http://www.grid-ids.de/

Research Area:
E-Science

Status of the Project: