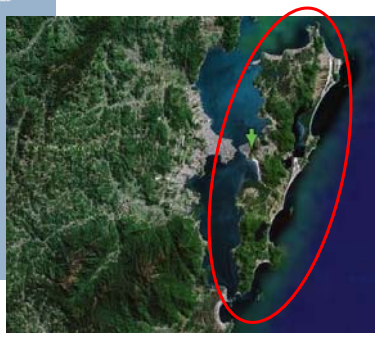
4th Workshop on Middleware for Grid Computing
Melbourne, Australia – November 2006

Composition of a DIDS by Integrating Heterogeneous IDSs on Grids

Paulo F. Silva, Carlos B. Westphall and Carla M. Westphall
Network and Management Laboratory
Department of Informatics and Statistics
Federal University of Santa Catarina, Florianópolis, Brazil

Marcos D. Assunção
University of Melbourne, Australia

Florianópolis, Santa Catarina, Brazil



Ack: Google Maps

Florianópolis, Santa Catarina, Brazil

Outline

- Introduction
  - Integration of Intrusion Detection Systems
  - Distributed Intrusion Detection Systems
- The proposed model
- Implementation
- Experiments
- Conclusions and future work

Intrusion Detection Systems

- Intrusion Detection Systems (IDSs) aim at identifying misuse or anomalous behavior of computer systems
  - Network IDS
  - Protocol-based IDS
  - Application Protocol-based IDS
  - Host-based IDS

Integration of IDSs

- Several IDSs are available in the market
  - Each system has advantages and weaknesses
- Distributed intrusions and attacks
  - Coordinated distributed attacks
  - Information from multiple networks is needed to detect these types of attacks
- The interoperability/integration of different IDS components would improve the time to market of IDSs

Distributed Intrusion Detection Systems (DIDS)

- Allow the correlation of intrusion information from multiple hosts, networks and/or administrative domains
- Help in identifying coordinated attacks
- Can enable a detailed examination of how these attacks progress
- Require a high degree of coordination

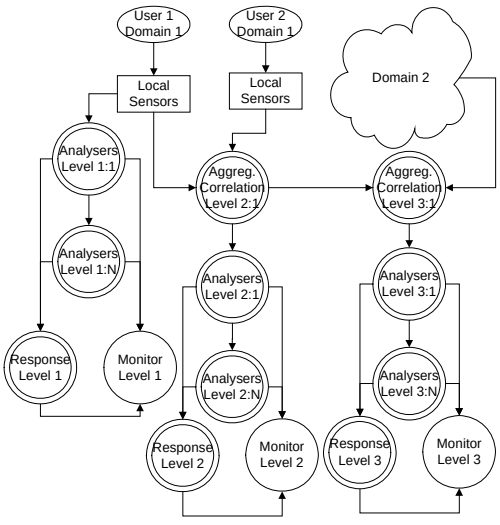
Grid Computing

- Allows the aggregation and sharing of resources spanning multiple administrative domains
- Supports the development of distributed applications and coordination in distributed environments
- Enables the encapsulation of existing IDSs as resources to compose an DIDS

Proposed Model: DIDSoG

- Distributed Intrusion Detection System on Grid
  - A model for integrating heterogeneous IDSs
  - Use of Grid computing for such an integration

DIDSoG: Architecture



- DIDSoG presents a hierarchy of intrusion detection services
- It is organized in several levels of "Scope:Complexity"

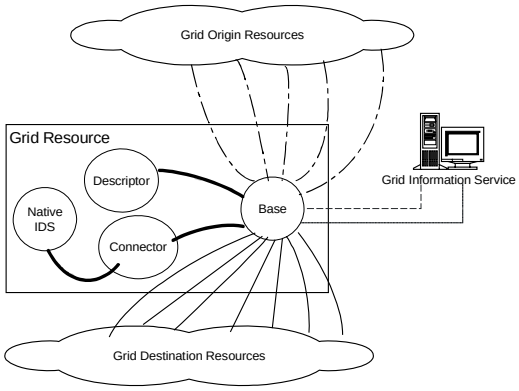
DIDSoG: Architectural Goals

- Resources can act on data from multiple sources (scopes)
- Distribution of the processing activities among several resources (complexity)
- Hierarchical organization:
  - Processing and analysis is performed in phases
  - No resource has full knowledge of the system
  - Existing IDSs can be integrated to DIDSoG
  - Different levels can be managed by different entities

DIDSoG: Resources

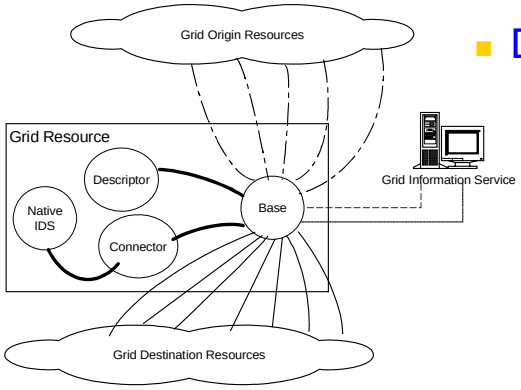
- A DIDSoG Resource:
  - Encapsulates an existing IDS
  - Receives data from other DIDSoG Resources
  - Process the received data using the encapsulated IDS
  - Generates and sends output data to a destination DIDSoG Resource

DIDSoG Resource: Main Components



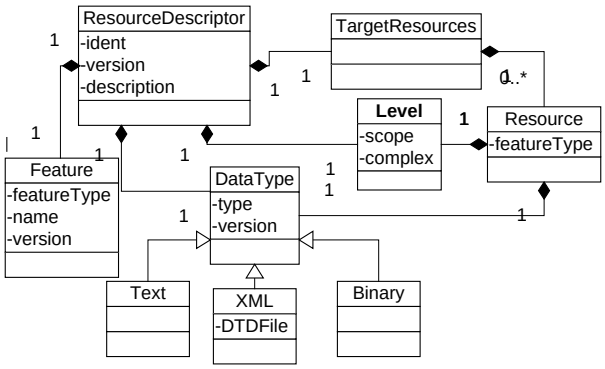
- Base
  - Communication with other resources and with the GIS
- Native IDS
  - The encapsulated IDS
- Connector
  - Information translation

DIDSoG Resource: Main Components



- Descriptor
  - Contains the information that identifies the resource and the destination resource

Descriptor: Resource Information

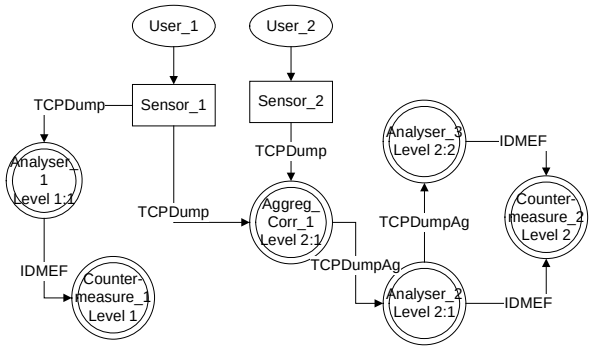


- Features
- Level
- DataType
- Target Resources

Implementation: Description

- GridSim Toolkit 3.3
- Architecture components:
  - Base: DIDSoG_BaseResource
  - Descriptor: DIDSoG_Descriptor
  - Connector: from DIDSoG_BaseResource
  - Native IDS: implemented by IDS
- Simulation of the processing activities of a Native IDS

Experiments: Simulated Environment



- Sensors 1 and 2 generate TCPdump like data
- Analyser_1 generates alerts at attempts to connect to port 23
- Aggreg_Corr_1 aggregates data from sensors 1 and 2
- Aggreg_Corr_1 passes the information to Analyser_2, which verifies if a host is trying to connect to the same port number in multiple hosts

Experiments: Observations

- Heterogeneous IDSs are integrated in a hierarchical way
- Difficult to evaluate the proposed architecture by simulation
  - Simulated IDSs
  - Integration of existing IDSs
  - Use of network traces
- Test and evaluation of DIDSoG
  - Emulation of a Grid environment
  - Test of the DIDS on a Grid test bed

Conclusions

- An architecture for integrating heterogeneous IDSs to compose a DIDS has been proposed
- Components have been modelled using GridSim
- Resources act in a collaborative way, forming an Intrusion Detection Grid
- Resources providing different intrusion detection services were integrated
  - Analysis, correlation, aggregation and alert

Future Work

- Deployment of the model
  - Use of a emulated Grid or a Grid test bed
  - Traces of network events
- Parallel analysis of data
  - Evaluate the performance of the model
- Economic aspects
  - Incentives for IDSs from multiple organizations to cooperate with one another in a Intrusion Detection Grid

Questions

Thank you!

Contact:

Paulo Fernando da Silva
paulo@lrg.ufsc.br

4th Workshop on Middleware for Grid Computing
Melbourne, Australia – November 2006

Composition of a DIDS by Integrating Heterogeneous IDSs on Grids

Paulo F. Silva, Carlos B. Westphall
and Carla M. Westphall
Network and Management Laboratory
Department of Informatics and Statistics
Federal University of Santa Catarina, Florianópolis, Brazil

Marcos D. Assunção
Grid Computing and Distributed Systems Laboratory
University of Melbourne, Australia