Modelo para Integração de Sistemas de Detecção de Intrusão através de *Grids* Computacionais

Paulo Fernando da Silva
Carlos Becker Westphall
Carla Merkle Westphall
UFSC – PPGCC – LRG

Sumário

- Introdução
- Modelo Proposto
- Desenvolvimento
- Testes
- Resultados
- Conclusão

Introdução – Integração

- Diversidade de IDSs:
  - Técnicas e alvos diferentes;
  - Pontos fortes e fracos diferentes;
- Justificativas para Integração:
  - Ambientes heterogêneos com vários IDSs;
  - Ataques envolvem várias redes;
  - Facilidade na migração de pesquisas para produtos;

Introdução – DIDSs x Grids

- DIDSs:
  - Relacionam informações de diferentes origens;
  - Ataques envolvendo várias redes\hosts;
  - Necessitam de um alto grau de coordenação;
- Grids:
  - permitem o compartilhamento coordenado de recursos sobre diferentes redes\hosts;

Introdução – Proposta

- Um modelo para integração de IDSs:
  - Cooperação entre IDSs heterogêneos;
  - IDSs integrados formam um DIDS;
  - Integração através de Grids;
  - IDSs integrados são visto como recursos;
- Modelo Proposto:
  - DIDSoG: Sistema de Detecção de Intrusão Distribuído sobre Grids;

Introdução - Justificativa sobre Grids

- Características de Serviços sobre Grids:
  - Gerência de dados distribuídos;
  - Execução coordenada de múltiplas aplicações;
  - Serviços de auditoria (fraudes e intrusões);
  - Serviços de monitoramento (sensores e alertas);

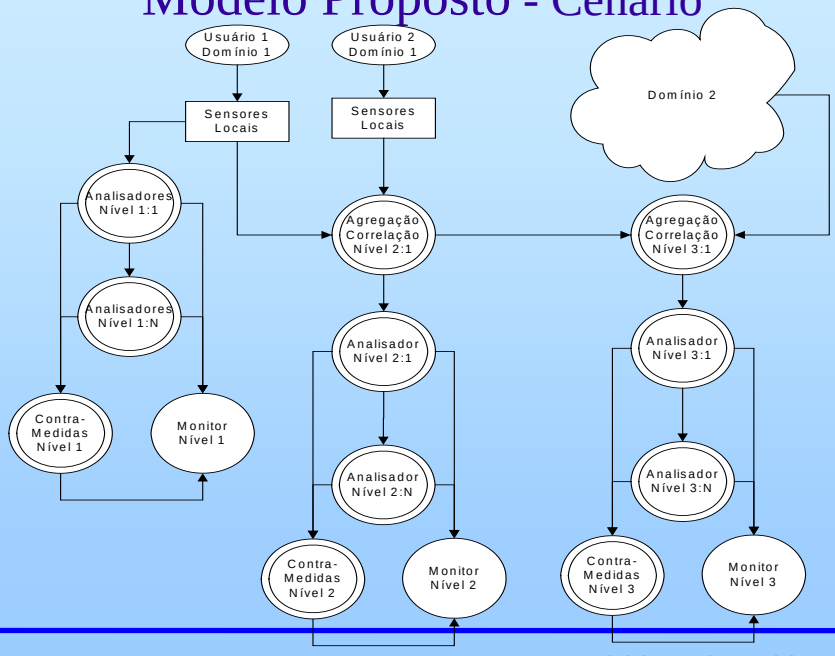
[Foster 2002]

- Os DIDSs possuem características próprias de serviços sobre Grids;
- Grids poderiam prover serviços de suporte aos DIDSs;

Modelo Proposto

- DIDSoG forma uma hierarquia de serviços de detecção de intrusão;
- Funcionalidades dos IDSs participantes são alocadas em algum nível da hierarquia;
- Organizada sob *"Escopo:Complexidade"*:
  - Ex.: Nível 1:1 (Escopo local e complexidade baixa);

Modelo Proposto - Cenário

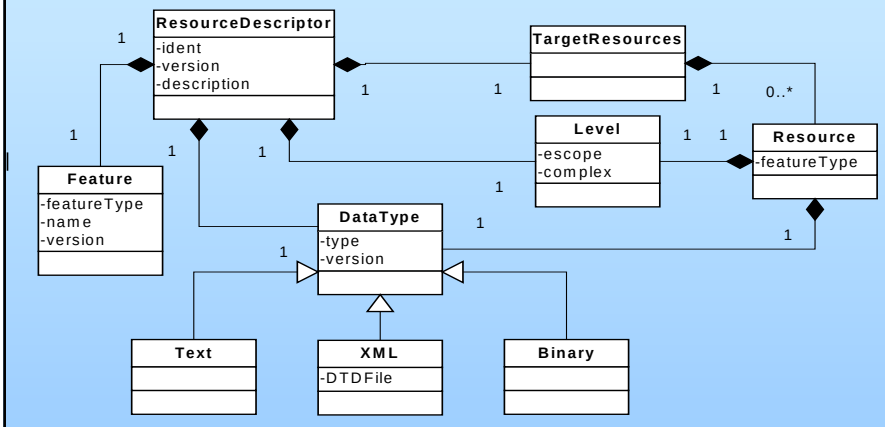


Modelo Proposto - Arquitetura

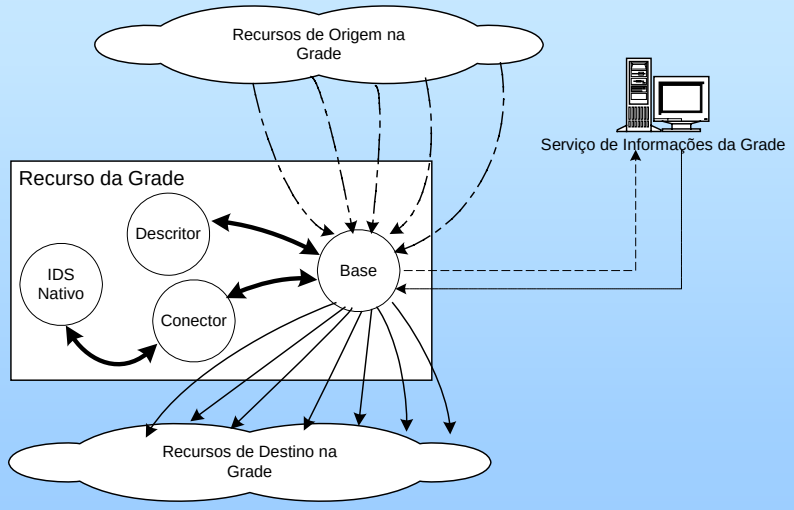
- Determinado recurso do DIDSoG:
  - Recebe dados de outros recursos;
  - Realiza seu processamento;
  - Encaminha dados a outros recursos;

- Descritor define:
  - As características de um recurso no Grid;
  - Os recursos de destino de um determinado recurso;

Modelo Proposto - Descritor



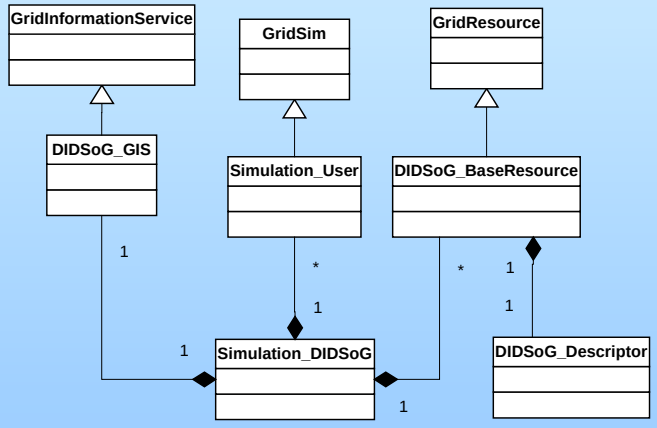
Modelo Proposto - Arquitetura



Desenvolvimento

- Simulador GridSim Toolkit 3.3;
- Componentes da Arquitetura:
  - Base: DIDSoG_BaseResource;
  - Descritor: DIDSoG_Descriptor;
  - Conector: derivar de DIDSoG_BaseResource;
  - IDS Nativo: implementado pelo IDS;

Desenvolvimento - Simulador



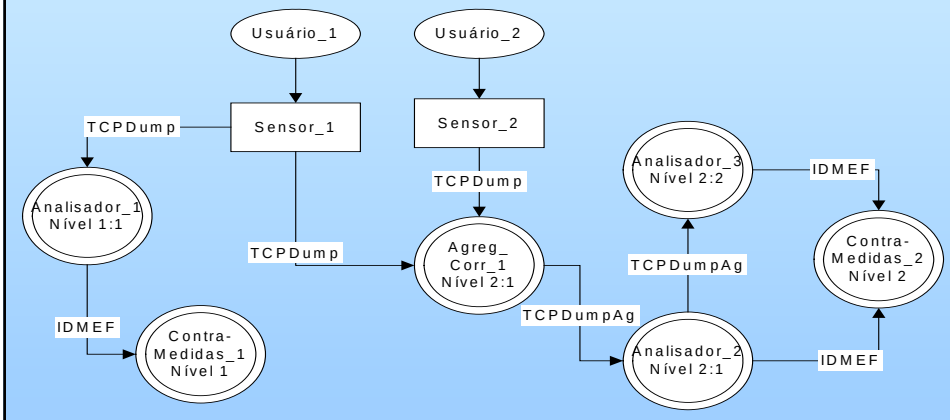
Testes

- Foram desenvolvidos simuladores de IDSs:
  - coleta, análise, correlação e contra-medidas;
- Foram desenvolvidos componentes conectores para cada um dos IDSs;
- Foram especificados Descritores para cada um dos IDSs:
  - através documentos XML;

Testes - Descritor

```
<?xml version="1.0" encoding="UTF-8"?>
<ResourceDescriptor ident="Analisador_2" version="1">
        <description>Descritor para integracao de Analisador simulado</description>
        <Feature>
                <Analyser>
                        <name>IDS Analisador Simulado</name>
                        <version>1.0.0</version>
                </Analyser>
        </Feature>
        <Level escope="2" complex="1"></Level>
        <DataType>
                <Binary>
                        <TCPDumpAg version="3.9.4"></TCPDumpAg>
                </Binary>
        </DataType>
        <TargetResources>
                <Resource>
                        <Feature>
                                <Response></Response>
                        </Feature>
                        <Level escope="2" complex="1"></Level>
                        <DataType>
                                <XML>
                                        <IDMEF version="1.0.0"></IDMEF>
                                        <DTD>./idmef-message.dtd</DTD>
                                </XML>
                        </DataType>
                </Resource>
                <Resource>
                        <Feature>
                                <Analyser></Analyser>
                        </Feature>
                        <Level escope="2" complex="2"></Level>
                        <DataType>
                                <Binary>
                                        <TCPDumpAg version="3.9.4"></TCPDumpAg>
                                </Binary>
                        </DataType>
                </Resource>
        </TargetResources>
</ResourceDescriptor>
```


Testes – Simulação



Resultados e Discussão

- DIDSoG forma uma grade de serviços de detecção de intrusão;
- O modelo apresenta flexibilidade:
  - Escopo, complexidade e descritores;
- Componente Conector:
  - Adaptações e conversões;
  - Filtros e logs;

Resultados e Discussão

- Integração de informações de diferentes origens (escopo);
- Integração de diferentes técnicas de detecção de intrusão (complexidade);
- Organização hierárquica:
  - Processamento em fases;
  - Redução da sobrecarga dos sensores;
  - Facilita a expansão do DIDSoG;
  - Permite a gerência em níveis de escopo;

Conclusão

- GridSim possibilitou a simulação do DIDSoG;
- Foram desenvolvidos os componentes da arquitetura DIDSoG;
- IDSs heterogêneos cooperaram entre si formando um DIDS através de um simulador de Grids;

Conclusão

- DIDSoG demonstrou ser uma solução:
  - para integração de IDSs heterogêneos;
  - para detecção de ataques distribuídos;
- Trabalhos Futuros:
  - desenvolver em uma plataforma de Grid e IDSs reais;
  - incorporar serviços de segurança;
  - permitir análise paralela por um mesmo IDSs Nativo;

Obrigado!
Perguntas?

Contato:
Paulo Fernando da Silva
paulo@lrg.ufsc.br