Applications and Issues of Distributed Intrusion Detection

Gregor Schaffrath
Communication Systems Group
University of Zürich

5. Juni 2007
Introduction

Overview

- Summary Sonthofen talk
- Applications and Issues
- Approaches
- Discussion
Basic problem

Basic Problem

A -- B -- C
Summary Sonthofen

Research topic split

- Low level communication frameworks
- Detection concepts
- Attack description languages
Summary Sonthofen

Research topic split

- Low level communication frameworks
- Detection concepts
- Attack description languages

Questions

- Structured Mapping?
- One Framework for all possible?
Summary Sonthofen

Research topic split

- Low level communication frameworks
- Detection concepts
- Attack description languages

Conclusions

- No Framework ideally suited for all scenarios
- Structured Evaluation & Research desirable
- Neither Structure, nor Evaluation methodology clear
- Conceptual consolidation scalability unsure
Where’s the gain in distribution?

Scalability

Robustness

Access to Information
Where’s the gain in distribution?

Scalability
- ’Full’ information ’locally’ available
- Issue: processing load
- Goal: load balancing

Robustness

Access to Information
Where’s the gain in distribution?

**Scalability**
- Goal: load balancing

**Robustness**
- ’Full’ information ’locally’ available
- Issue: Information/Analysis quality uncertain
- Goal: redundancy + counter checks/voting

**Access to Information**
Where’s the gain in distribution?

**Scalability**
- Goal: load balancing

**Robustness**
- Goal: redundancy + counter checks/voting

**Access to Information**
- Only partial information ‘locally’ available
- Issue: Central analysis impossible
  - Network resource constraints
  - Policy/Privacy reasons
- Goal: Analysis migration to information source
Can we draw **probabilistic conclusions thereof w.r.t. scenarios?**

**Scalability**

**Robustness**

**Access to Information**
Can we draw **probabilistic** conclusions thereof w.r.t. scenarios?

**Scalability**
- Only split of 1 node

**Robustness**

**Access to Information**
Can we draw **probabilistic conclusions thereof w.r.t. scenarios?**

### Scalability
- Only split of 1 node
- High network resources
- No privacy issues
- High trust
- Arbitrary concepts possibly scalable

### Robustness

### Access to Information
Can we draw **probabilistic** conclusions thereof w.r.t. scenarios?

### Scalability
- Only split of 1 node

### Robustness
- Mirror of 1 node

### Access to Information
Can we draw **probabilistic** conclusions thereof w.r.t. scenarios?

<table>
<thead>
<tr>
<th>Scalability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only split of 1 node</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Robustness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirror of 1 node</td>
</tr>
<tr>
<td>High abstraction communication</td>
</tr>
<tr>
<td>Few privacy issues</td>
</tr>
<tr>
<td>Few network constraints</td>
</tr>
<tr>
<td>Syncronization of concepts needed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access to Information</th>
</tr>
</thead>
</table>

Gregor Schaffrath
Communication Systems Group
University of Zürich

Applications and Issues of Distributed Intrusion Detection
Can we draw probabilistic conclusions thereof w.r.t. scenarios?

**Scalability**
- Only split of 1 node

**Robustness**
- Mirror of 1 node

**Access to Information**
- Cooperation, possibly spanning Administrative Zones
Can we draw *probabilistic* conclusions thereof w.r.t. scenarios?

<table>
<thead>
<tr>
<th>Scalability</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Only split of 1 node</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Robustness</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirror of 1 node</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access to Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cooperation, possibly spanning Administrative Zones</td>
<td></td>
</tr>
<tr>
<td>Bandwidth and Delay Concerns</td>
<td></td>
</tr>
<tr>
<td>Scalability for synchronization of concepts</td>
<td></td>
</tr>
<tr>
<td>Trust issues</td>
<td></td>
</tr>
</tbody>
</table>
Can we draw **probabilistic** conclusions thereof w.r.t. scenarios?

### Issues

1. **Information requirements vs. Information availability**
   - Network constraints
   - High communication efficiency required
   - Requirement on cooperation decisions
   - Requirement on detail knowledge
   - Policy constraints
Can we draw probabilistic conclusions thereof w.r.t. scenarios?

Issues

1. Information requirements vs. Information availability
   - Network constraints
   - High communication efficiency required
   - Requirement on cooperation decisions
   - Requirement on detail knowledge
   - Policy constraints

2. Scalability of unification of concepts
   - Communication: de facto 'Events', 'Alerts'
   - Only syntactical representative
   - Concept consolidation needed
Approaches

Information requirements vs. Information availability

- Reduction of local informational requirements
  1. Reduction of cooperation focus
  2. Expressive communication

- Increase of information availability
  1. Pseudonymization
  2. Increase of Trust
Approaches

Information requirements vs. Information availability

- Reduction of local informational requirements
  1. Reduction of cooperation focus
  2. Expressive communication

- Increase of information availability
  1. Pseudonymization
  2. A posteriori: Legal contracts
  3. A priori: Reduction of misuse potential
Possible next steps

- Investigations into inter-domain scenarios
- Investigations into incentive models
- Investigations into cooperation privacy issues
Discussion

Feasable? Leading astray? Assumptions realistic? ...