Software security patterns and security metrics

Thomas Heyman, Christophe Huygens
DistriNet Research Group
K.U.Leuven
Security patterns

• A pattern
  – a solution to a problem
  – within a specific context
• Example: single access point pattern
• Why security patterns?
  – Capture expert knowledge
  – Domain-independent
  – Reusability!
• Related to our other work
  – Pattern taxonomy
  – Integration of patterns in design process
Associating metrics to patterns

• Patterns: right granularity (?)
• Bringing measuring process closer to application semantics
  – Better integration in development cycle
  – Application state can be monitored more closely
• Core versus ecosystem
  – Some metrics provide feedback on core system security
  – ...others on the hostility of your environment (ecosystem)
• Proactive (state) versus reactive (event) measuring
  – Metrics can be associated to architecture or design as well, similar to code analysis approaches
• Enable aggregation and correlation
  – Combine metrics to form indicators for each objective
  – Flexibility through correlation algorithm (risk posture)
Examples of patterns and metrics

- **Input guard, output guard**
  - #guards vs. #access points for each component
  - #filtering incidents per invocation
  - discrepancies between output guard and input guard results

- **Audit interceptor**
  - #service invocations vs. #audit events

- **Application-level firewall**
  - #firewall invocations vs. #service invocations
  - #denied connections

- **Secure object creator**
  - #illegal access errors (incorrect privilege matching)
### Preliminary results

- Possible to attach at least one metric to each pattern.
- Different types of metrics (see image):
  - depending on the security goal (CIA...)
  - core versus ecosystem
- Valuable contextual info can readily be obtained

<table>
<thead>
<tr>
<th>confidentiality</th>
<th>core</th>
<th>ecosystem</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>firewall/service invoc.</td>
<td>denied fw connections</td>
</tr>
<tr>
<td>i/o-guard discrepancies</td>
<td>o-guard filtering incidents</td>
<td>i-guard filtering incidents</td>
</tr>
<tr>
<td>nb.guards/access points</td>
<td>firewall/service invoc.</td>
<td>denied fw connections</td>
</tr>
<tr>
<td>nb. of audit events/invocation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>integrity</th>
<th>core</th>
<th>ecosystem</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>availability</th>
<th>core</th>
<th>ecosystem</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>anonymity</th>
<th>core</th>
<th>ecosystem</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>accountability</th>
<th>core</th>
<th>ecosystem</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

...
Open issues and questions

- **Next – first validation**
  - Prototype / PoC
  - Need for loss databases, reference tests
- **Does this approach make sense?**
- **Are all applications suited for this approach?**
- **Aggregation/correlation**
  - Possibility to combine metric values into indicators – how?
  - Similarity to IDS problems