Monthly Research 2016.10
STRIDE Variants and
Security Requirements-based Threat Analysis

E-Mail: research-feedback[at]ffri.jp
Twitter: @FFRI_Research
Table of Contents

• About threat analysis
• STRIDE Variants
  – STRIDE-per-Element
  – STRIDE-per-Interaction
  – Comparative the variants STRIDE
• Security Requirements-based Threat Analysis
• Conclusions
• References
About Threat Analysis

- This report illustrates threat analysis continued from previous research
- We explain STRIDE variants for enumeration of threats
- In addition, we introduce security requirements-based threat analysis method as one of the different choices
STRIDE-per-Element

- Apply to STRIDE elements of DFD to find threats
  - The elements are Process, Data Flow, etc.,.
- This method can find threats by the routine
- Process
  1. Retrieve elements from the DFD
  2. Find threats from element-STRIDE table
  3. Check whether the records in the table are appropriate
    - The table is not almighty

<table>
<thead>
<tr>
<th></th>
<th>S</th>
<th>T</th>
<th>R</th>
<th>I</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Entity</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data Flow</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data Store</td>
<td>✓</td>
<td>?</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
STRIDE-per-Interaction

- Find data flow at an intersection of a trust boundary
- Find threats at "origin, destination, interaction" in Dataflow

- About Trust Boundary
  - Borderline of the organization or interface
    - For example, between the Web server and browser

- Microsoft Threat Modeling Tool
  - It has been supported STRIDE-per-Interaction from version 2014
  - It analyzes also non-intersection data flow as an additional feature
STRIDE-per-Interaction

- Process
  1. Create a table of elements, interactions and potential threats
  2. Create a DFD
  3. Extract the data flow at the intersection of trust boundary
  4. Enumerate threats
     - Comparing interactions and origin or destination of data flow
  5. Create a table of the comparison result

Table 3-10: STRIDE-per-Interaction: Threat Applicability

<table>
<thead>
<tr>
<th>#</th>
<th>ELEMENT</th>
<th>INTERACTION</th>
<th>S</th>
<th>T</th>
<th>R</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Process (Contoso)</td>
<td>Process has outbound data flow to data store.</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Process (Contoso)</td>
<td>Process sends output to another process.</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Process (Contoso)</td>
<td>Process sends output to external interactor (code).</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Process (Contoso)</td>
<td>Process sends output to external interactor (human).</td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
Comparison of the STRIDE variants

- Students of the Chalmers University of Technology analyzed the same system using two STRIDE variants
  - Analysis target is a SecOC module of AUTOSAR
    - SecOC provides functions for secure communication between ECUs
  - True positives
    - Comparison of true threat rate
  - They were assessing the Microsoft Threat Modeling Tool which supports each variant

<table>
<thead>
<tr>
<th></th>
<th>Required Time</th>
<th>Total threats</th>
<th>True positives</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>STRIDE-per-Element</td>
<td>26.0H</td>
<td>99</td>
<td>54.55%</td>
<td>• Short time&lt;br&gt;• The result is accurate</td>
<td>• Dependent on individual skills&lt;br&gt;• The tool is hard to use</td>
</tr>
<tr>
<td>STRIDE-per-Interaction</td>
<td>32.5H</td>
<td>114</td>
<td>26.32%</td>
<td>• Easy to understand the threats&lt;br&gt;• Easy-to-use tool</td>
<td>• require relatively long time&lt;br&gt;• Complexity of applying to large system&lt;br&gt;• many false positive</td>
</tr>
</tbody>
</table>
Security Requirements-based Threat Analysis

- This method has been proposed by Masaru Matsunami of Sony DNA
- It extracts security requirements from design and specification
- It was used for threat analysis of "harmo" system by the Sony

Process

- Find "actor" and "assets" from specification documents
- Extract threat event based on template ["actor" "can / can't" "read/write/execute" to "assets"]
  - Threat event: Malicious third party can read personal data
  - If necessary find also "Location"
- Security requirement is found on the basis of threat events
  - Security requirement is found on the basis of threat events
- Draw a security analysis graph on the basis of security requirements
Security Requirements-based Threat Analysis (cont’d.)

- About security analysis graph
  - A security requirement is written on top of a tree
  - The security requirement is a proposition
  - Nodes are written conditions to achieve the proposition
  - You can confirm whether there is a countermeasure at nodes
Security Requirements-based Threat Analysis (cont’d.)

- Advantages
  - Available in an early design phase
    - DFD is not essential
  - It can also be used by a non-expert of threat analysis with knowledge database of a security analysis graph

- Disadvantages
  - Require relatively long time if there is no knowledge database of a security analysis graph
Conclusions

• STRIDE-per-Element
  – Required time is short, but tool is inconvenience
  – Good for the security specialist

• STRIDE-per-Interaction
  – Easier than the other method, but it takes a long time and many false positive
  – It will be good if you have enough resource for threat analysis

• Security Requirements-based Threat Analysis
  – Available in an early design phase

• There are various threat analysis methods
  – You should select suitable methods taking into conditions of threat analysis
    • Available time, accuracy, analyst level, etc.
References

• Threat Modeling
• Chapter 6 Privacy Tools
  – [https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzaWdzdGF3ZWJ8Z3g6NDRhNmE5N2JhYjQ0ZTkwaOA](https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzaWdzdGF3ZWJ8Z3g6NDRhNmE5N2JhYjQ0ZTkwaOA)
• Vehicle Control Unit Security using Open Source AUTOSAR
• Threat Modeling – requirements and design
• Chapter 3 STRIDE
  – [https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzaWdzdGF3ZWJ8Z3g6MmY4ZTgxNmY5ODFhZWRY5MA](https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzaWdzdGF3ZWJ8Z3g6MmY4ZTgxNmY5ODFhZWRY5MA)
• (ISC)² Japan Chapter kickoff event
  – [http://isc2chapter.jp/wp-content/uploads/2014/03/%E4%BB%95%E6%A7%98_%E8%A8%AD%E8%A8%88%E3%81%AE%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E5%88%86%E6%9E%90.pdf](http://isc2chapter.jp/wp-content/uploads/2014/03/%E4%BB%95%E6%A7%98_%E8%A8%AD%E8%A8%88%E3%81%AE%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E5%88%86%E6%9E%90.pdf)
• Threat Analysis Method used for Sony “harmo”
• FFRI Monthly Research 2016.9