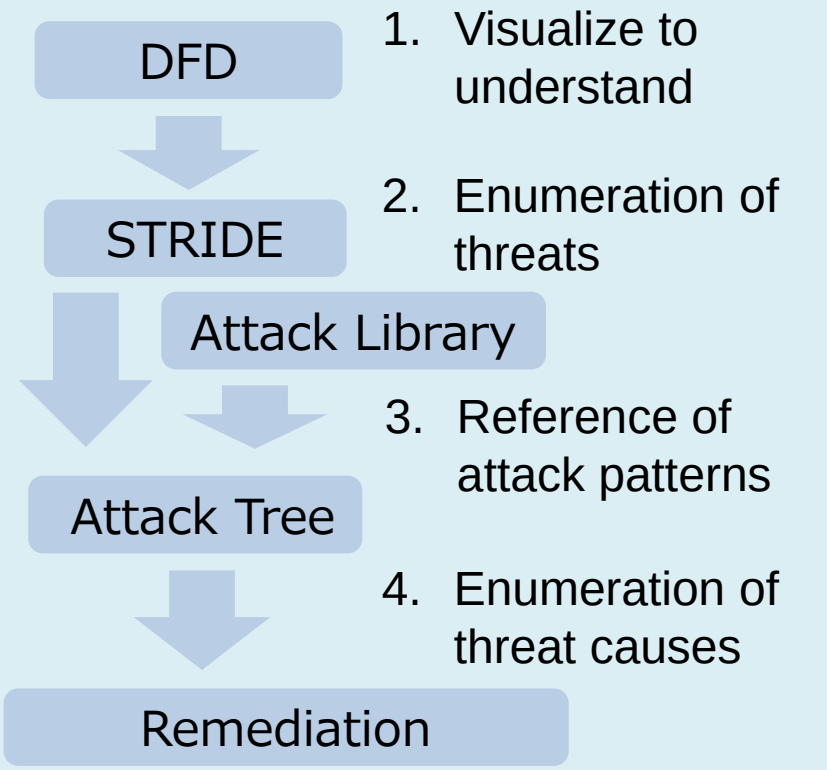
Monthly Research 2016.10
STRIDE Variants and Security Requirements-based Threat Analysis

FFRI, Inc.
http://www.ffri.jp/en/

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

Table of Contents

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

	S	T	R	I	D	E
External Entity	✓		✓			
Process	✓	✓	✓	✓	✓	✓
Data Flow		✓		✓	✓	
Data Store		✓	?	✓	✓	

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

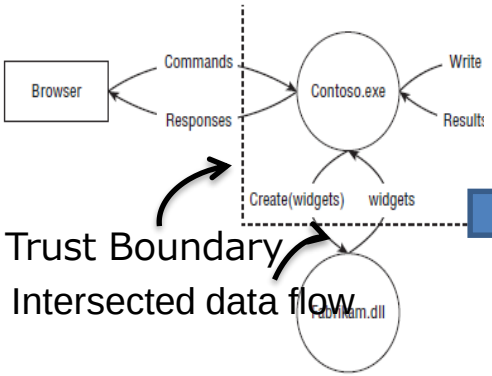


Figure 3-1: The system referenced in Table 3-10

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

#	ELEMENT	INTERACTION	S	T	R
1	Process (Contoso)	Process has outbound data flow to data store.	x		
2		Process sends output to another process.	x		x
3		Process sends output to external interactor (code).	x		x
4		Process sends output to external interactor (human).			x

Table 3-11: STRIDE-per-Interaction (Example)

	ELEMENT	INTERACTION	S	T	R
1	Process (Contoso)	Process has out-bound data flow to data store.	"Database" is spoofed, and Contoso writes to the wrong place.		
		Process sends output to other process.	Fabrikam is spoofed, and Contoso writes to the wrong place.		Fat cla ha cal Co
3		Process sends output to exter-nal interactor	Contoso is confused about the identity of the browser		Bro dis

http://threatmodelingbook.com/index.html

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

	Required Time	Total threats	True positives	Advantages	Disadvantages
STRIDE-per-Element	26.0H	99	54.55%	• Short time • The result is accurate	• Dependent on individual skills • The tool is hard to use
STRIDE-per-Interaction	32.5H	114	26.32%	• Easy to understand the threats • Easy-to-use tool	• require relatively long time • Complexity of applying to large system • many false positive

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

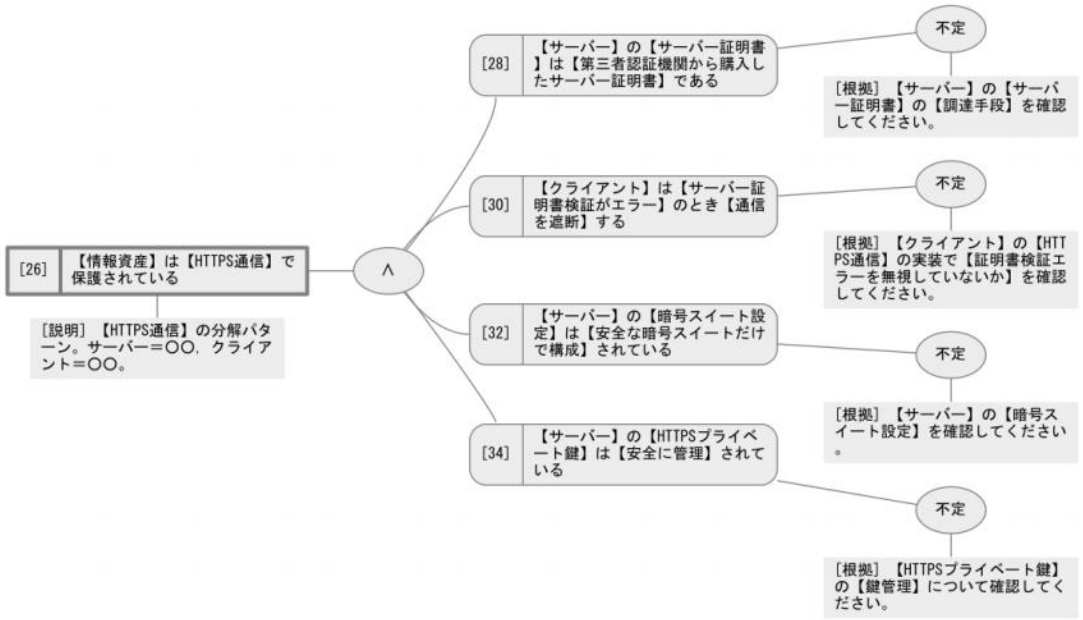


図 15-A-9-15 【HTTPS 通信】分解テンプレート https://www.ipa.go.jp/files/000049366.pdf

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
  - http://threatmodelingbook.com/index.html
- Chapter 6 Privacy Tools
  - https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzaWdzdGF3ZWJ8Z3g6NDRhNmE5N2JhYjQ0ZTkwOA
- Vehicle Control Unit Security using Open Source AUTOSAR
  - http://publications.lib.chalmers.se/records/fulltext/219822/219822.pdf
- Threat Modeling – requirements and design
  - https://www.asteriskresearch.com/wp-content/uploads/2016/01/ThreatModeling_requirements_and_design20160204.pdf
- Chapter 3 STRIDE
  - https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzaWdzdGF3ZWJ8Z3g6MmY4ZTgxNmY5ODFhZWY5MA
- (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
- Threat Analysis Method used for Sony “harmo”
  - https://www.ipa.go.jp/files/000049366.pdf
- FFRI Monthly Research 2016.9
  - http://www.ffri.jp/assets/files/monthly_research/MR201609_Introduction_of_Threat_Analysis_Methods_JPN.pdf