Monthly Research 2016.9

Introduction of Threat Analysis Methods

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

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

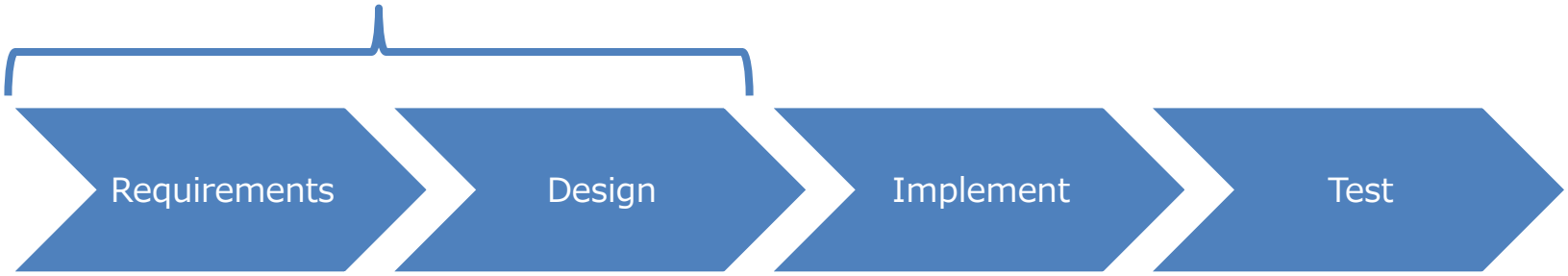
Agenda

- Definition of threat analysis
- Threat analysis process
- Analysis methods
  - DFD(Data Flow Diagram)
  - STRIDE
  - Attack Library
  - Attack Tree
- Conclusions
- References

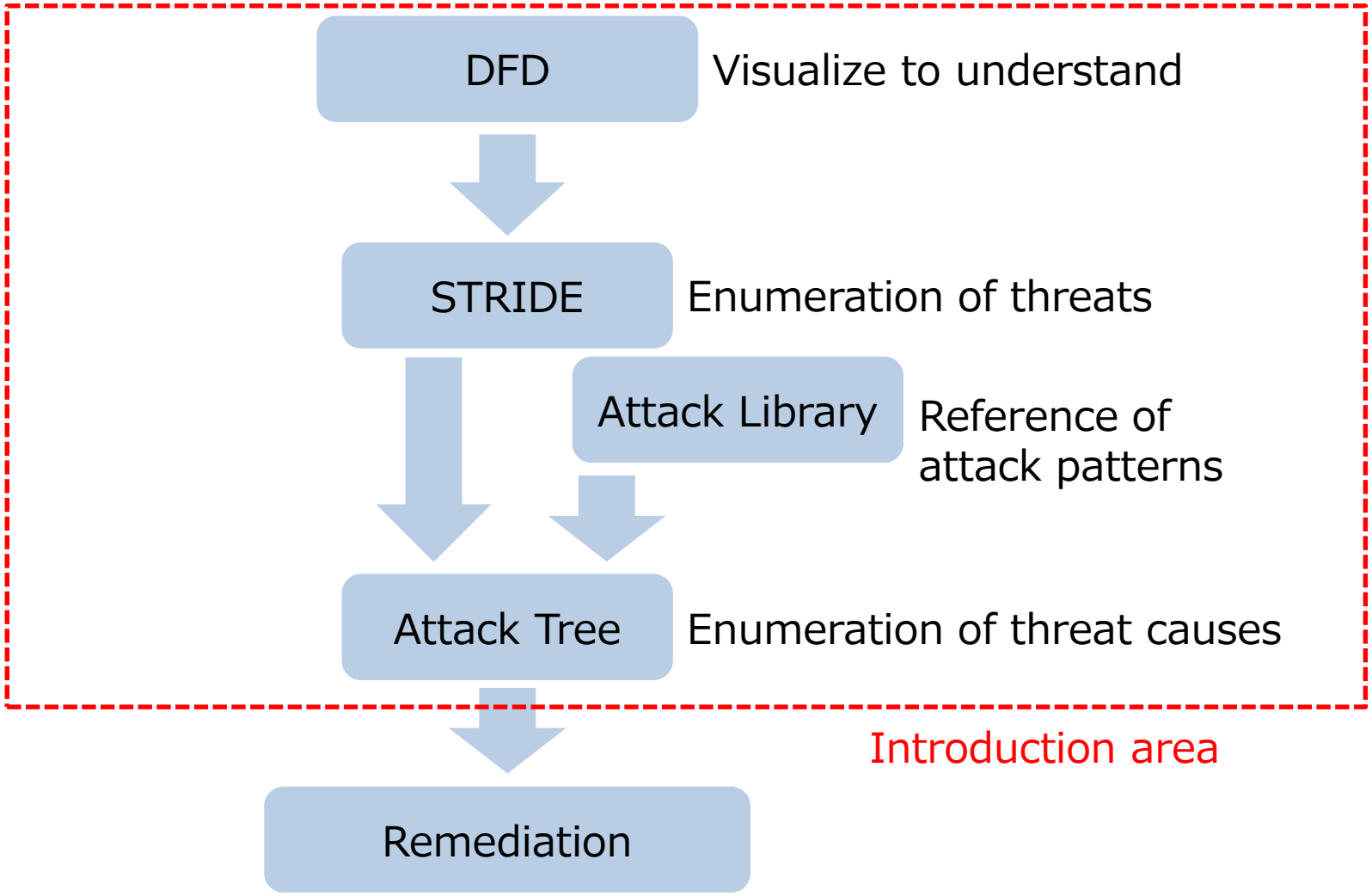
Definition of threat analysis

- Methods to identify threats and evaluate risk
- What is a threat?
  - It is causes of damage to assets.
    - These can be classified by environmental threats and human threats.
- Threat analysis is performed in requirements phase and design phase.
  - If found problems, then fix it

Target of threat analysis

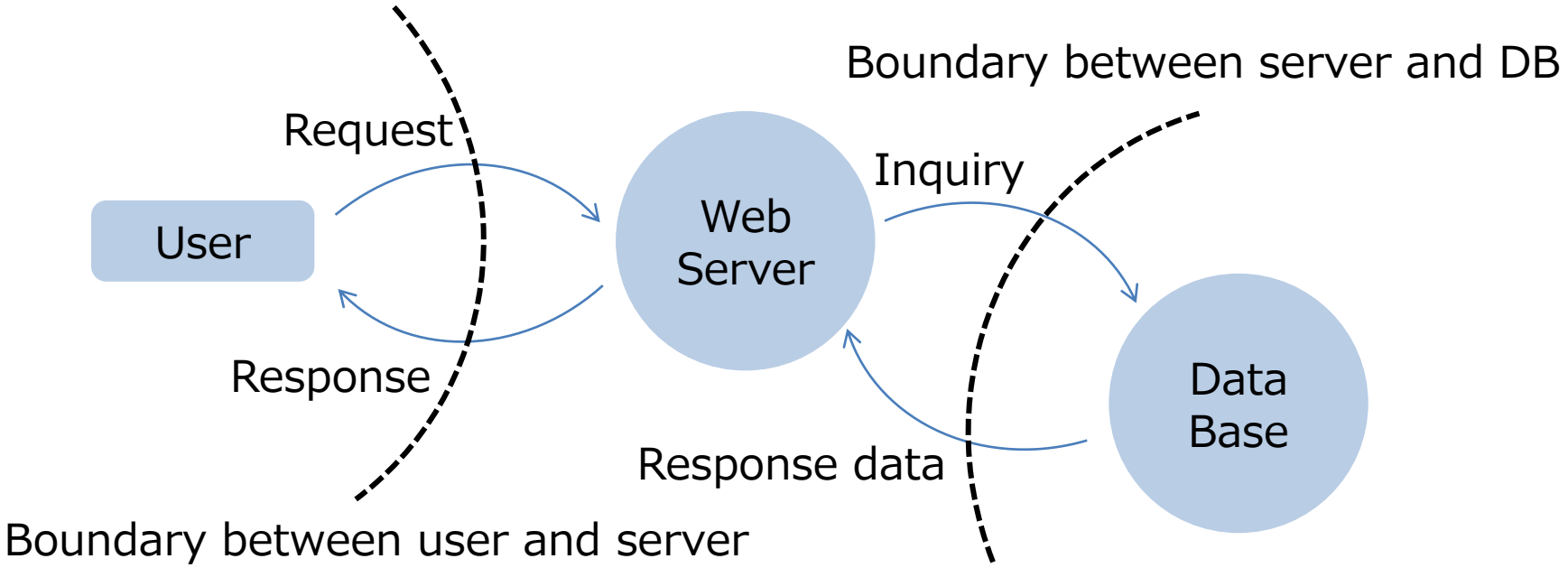


Threat analysis process



DFD(Data Flow Diagram)

- DFD illustrates data flow in a system
  - DFD would help to understand data flow on a system.



STRIDE

- What is the STRIDE?
  - This method is possible to identify threat which might occur in a system.
  - It is the acronym of the elements of the information system.

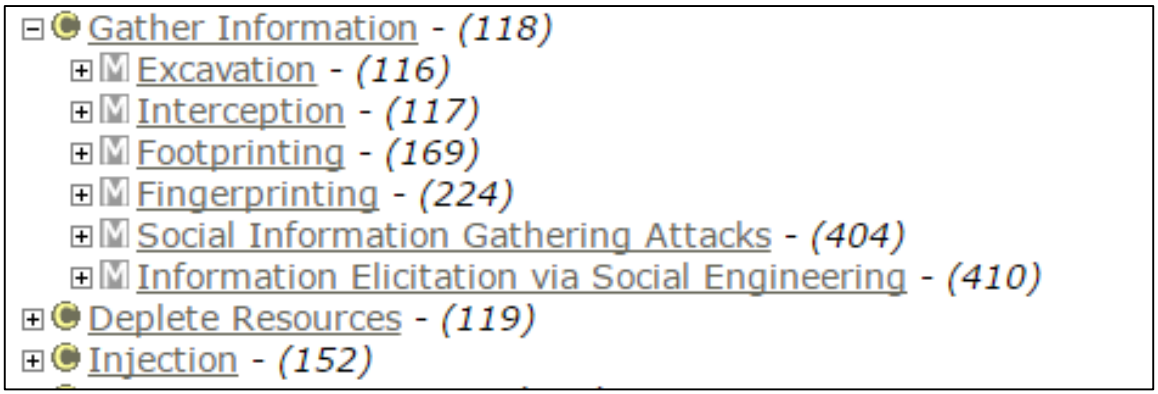
Threat characteristics	Example
Spoofing	Spoofing the owner
Tampering	Forge data
Repudiation	Delete logs
Information Disclosure	Leak of credit card number
Denial of Service	Put a load on the server
Elevation of Privilege	Get of administrative privileges

The STRIDE usage example

- This description is using DFD on page 5 (in this presentation).
- Spoofing
  - The third party gain unauthorized access to the system.
- Tampering
  - Tampering the contents of the database
- Repudiation
  - Delete the access log of the Web server
- Information disclosure
  - Leak of customer information from database
- Denial of Service(DoS)
  - The server is down by sending a large number of requests
- Escalation of privilege
  - Execution of malicious programs in the Web server

Attack Library

- What is the Attack Library?
  - It is list of attack method.
    - The CAPEC is an Attack Library that created by the MITRE.
  - If you use the Attack Library, threat enumeration will be efficient.
  - The collected information can be reused.
  - Attack Library is useful to making Attack Tree.

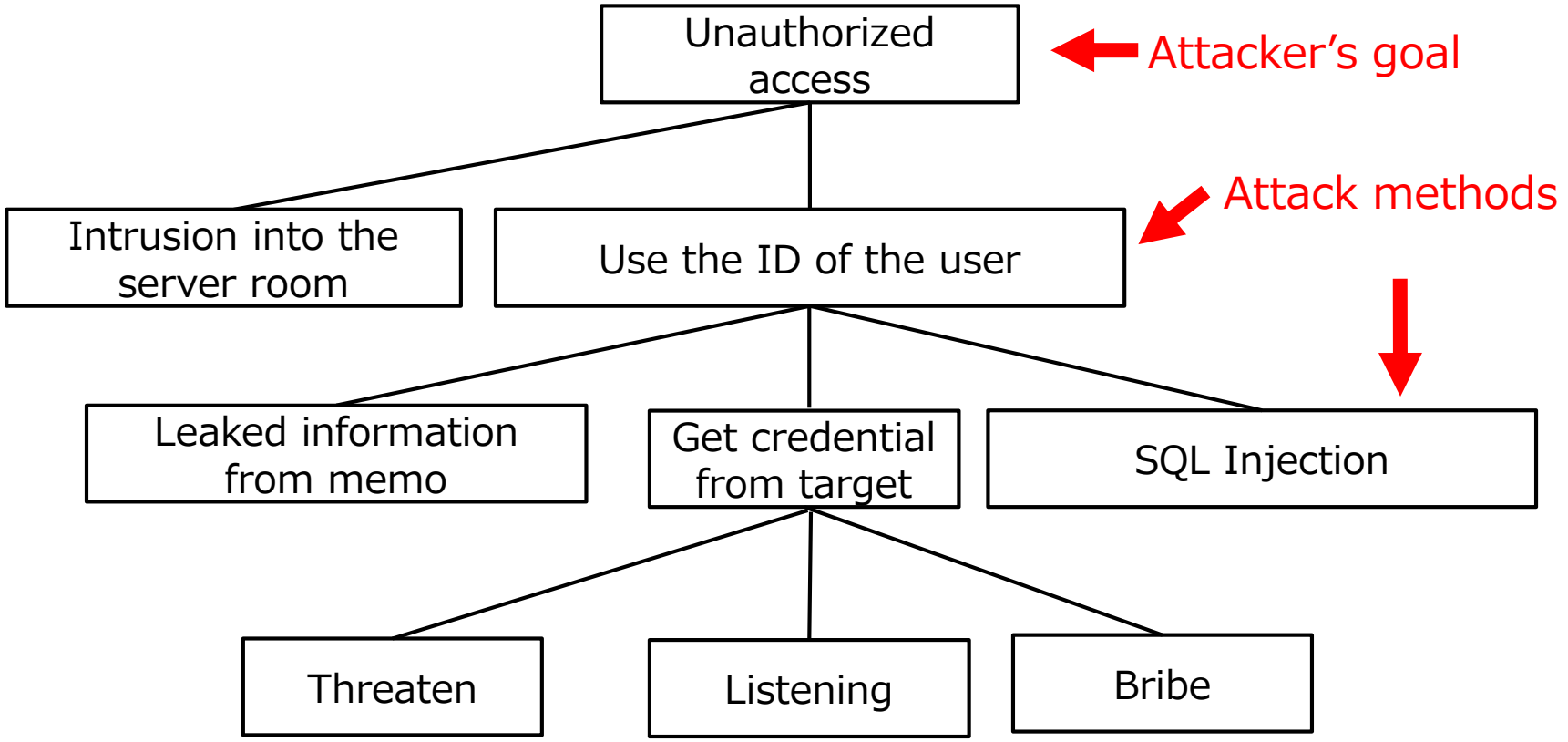


https://capec.mitre.org/

Attack Tree

- What is Attack Tree?
  - It is enumerated causes of threat.
    - Attack Tree is expressed by tree structure.
- Pros
  - Attack tree can visualize the attack methods.
  - It is possible to quickly discover the vulnerability.
- Cons
  - It takes time to create the Attack Tree.
- How to create Attack Tree
  1. Write the attacker's goal to root.
  2. Write attack methods to nodes.

Example of Attack Tree



Conclusions

- Threat analysis begins from DFD.
- STRIDE is easy to use because the threat's property has been patterned.
- Attack library would help to perform a threat analysis more efficiently.
  - The CAPEC will be the reference of Attack Library.
- Attack Tree is useful when considering measures.
- You can obtain various information by performing threat analysis.
  - The information is a weak point to the attack.
  - It will lead to finding latent threats.

References

- Threat Modeling
  - http://as.wiley.com/WileyCDA/WileyTitle/productCd-1118809998.html
- Strategies for Threat Modeling
  - https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzaWdzdGF3ZWJ8Z3g6NmE4NDhjYWNhOGYxMDBlOQ
- STRIDE
  - https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzaWdzdGF3ZWJ8Z3g6MmY4ZTgxNmY5ODFhZWY5MA
- Attack Trees
  - https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzaWdzdGF3ZWJ8Z3g6M2UzZDhjYWE5ZmU2NzJjYQ
- Attack Libraries
  - https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzaWdzdGF3ZWJ8Z3g6YmVkN2EwODFjMDcxMjg3
- CAPEC
  - https://capec.mitre.org/
- Threat Modeling Analysis
  - https://msdn.microsoft.com/ja-jp/library/aa561499.aspx