An Example of use the Threat Modeling Tool
Agenda

- About threat analysis support tool
- Examples of tools
- Analysis target system
- Analysis result
  - How to read result
  - Overview of threats
- Effective usage
  - About template
  - Additional definition of threat information
- Conclusions
- References
About threat analysis support tool

• There are various analysis support tools.
  – DFD drawing, automated threat identification

  – Benefits of tools
    • Reduce analysis time by automatically identifying threats and generating a report
    • Possibility to discover potential threats you could not find
    • Reducing dependency on individual skills
      – The same analysis result can be obtained for the same input data.
Examples of tools

- Microsoft Threat Modeling Tool
  - DFD creation, tool to derive threats automatically from DFD
- TRIKE
  - DFD creation, drawing tool including security requirements
- SeaMonster
  - Attack tree and misuse case drawing tool
    - A misuse case is an unintended operation.
- SecurITree
  - Attack tree creation tool

- In this report, we explain an example of use the Microsoft Threat Modeling Tool 2016.
Analysis target system

• The target is a general network camera system.
• The figure below is a DFD created using the tool.
  – Add elements and data flow of the system to design view.
Analysis result - How to read result

• The analysis result can be confirmed on the analysis view.
  – A threat list contains properties and outline of threats.
    • It is necessary to check whether the found threats actually.
      – Example: The web server could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
        » The above threat does not exist on a page without input form.
  – It is possible to describe priority and countermeasure for each threat.
    • The priority is setting to 'high' by default, user should change it.
    • It is useful for sharing status with multiple analysts.
Analysis result - Overview of threats

- 47 threats were pointed out in the system.
  - Spoofing 10 cases
  - Tampering 8 cases
  - Repudiation 4 cases
  - Information Disclosure 3 cases
  - Denial of Service 12 cases
  - Elevation of privilege 10 cases

- Many threats are related to web server.
  - Many categories of threats have been found there.

- The descriptions of the threat are general.
  - If a threat information is insufficient, user should add information.
Effective usage - About template

- What you can do by adding templates.
  - You can apply any picture to elements to make nice-looking DFD.
  - You can add threat information defined yourself.
- The following figure shows an entry screen when creating a template.
Effective usage - Additional definition of threat information

- Analysis efficiency will be improved by templates.
  - More extended analysis becomes possible by adding templates of threat information.

- Template example
  - Title: Unauthorized access with default password.
  - Include: target is [Web Service]
  - Description:
    If you do not change the default password, attackers may compromise the system.
Conclusions

• Pros
  – It can be used easily because threats will be listed automatically from a DFD.
  – It helps secure system design.
  – You can share threats information and priority with your team.

• Cons
  – Threats that do not exist may be false detected.
    • You should confirm the feasibility of analyzed threats.
References

- Threat Modeling
- SDL Threat Modeling Tool
- Microsofts New Threat Modeling Tool
  - https://blog.secodis.com/2016/07/06/microsofts-new-threat-modeling-tool/
- TRIKE
  - http://octotrike.org/
- SeaMonster
  - https://sourceforge.net/projects/seamonster/?source=navbar
- SecuriTree
  - http://www.amenaza.com/