Secure Software Engineering Lab

Lab 3: Security Risk Assessment

Institute of Software Security (E-22)

1. Objectives

Apply the knowledge acquired in the lectures on the following areas of software security:

- Application of the STRIDE methodology.
- Explore mitigation actions and security control.
- Navigate and leverage the Mitre ATT&CK Catalog.

2. Tasks

1. **Create a Data Flow Diagram (DFD) of the Metaverse**.
   - Use the case study description as a starting point plus the supplementary material.
   - Focus on (i) login, (ii) registration, and (ii) befriending processes.
2. **Identify security threats**.
   - Conduct an iteration of the STRIDE methodology (manually).
   - Copy your DFD into the OWASP Threat Dragon Tool.
   - Conduct STRIDE using the OWASP Tool.
   - Compare the outcome of your manual inspection against the ones from the tool.
3. **Prioritize and mitigate threats**.
   - Estimate and prioritize security risks using heat maps (a.k.a. risk assessment matrix).
   - Select mitigation actions and countermeasures for the identified security threats.
4. **Browse the Mitre ATT&CK Catalog.**
   - Find 5 potential attack procedures applicable to the system under analysis.
   - Hint: `https://attack.mitre.org/techniques/T1585/001/`

3. Materials

Case study, lecture slides, lab slides, supplementary material (social network documentation).

Summer Semester 2022