Security Engineering Risk Analysis (SERA)

“We wouldn’t have to spend so much time, money, and effort on network security if we didn’t have such bad software security.”


**Importance of Good Design**

940 Total CWEs

<table>
<thead>
<tr>
<th>Percentage</th>
<th>CWE Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>40%</td>
<td>Design Weakness</td>
</tr>
<tr>
<td>24%</td>
<td>Other Weakness</td>
</tr>
<tr>
<td>78%</td>
<td>Design Weakness</td>
</tr>
</tbody>
</table>

*MITRE’s Common Weakness Enumeration (CWE)*

Source: http://www.cwe.mitre.org/ as of Feb 9, 2014

**Software Faults: Introduction, Discovery, and Cost**

Faults account for 30–50% percent of total software project costs.

- Most faults are introduced before coding (~70%).
- Most faults are discovered at system integration or later (~80%).

**Goal: Reduce Security Design Risk**

Security design weaknesses

- Are not addressed by security controls or static analysis tools and
- Cannot be easily addressed during operations (e.g., by patching systems)

**Errors during requirements engineering are costly!**

- Defects cost up to 200 times more once fielded than if caught in requirements engineering
- Reworking defects consumes >50% of project effort
- >50% of defects are introduced in requirements engineering

Applying SERA during requirements specification

- Provides early detection of design weaknesses for remediation
- Reduces residual security risk during operations

**Security Engineering Risk Analysis**

1. Establish operational context.
2. Identify risk.
3. Analyze risk.
4. Develop control plan.

**Software Engineering Institute | Carnegie Mellon University.**