<table>
<thead>
<tr>
<th>1. REPORT TITLE</th>
<th></th>
<th>2. REPORT TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Engineering Risk Analysis (SERA)</td>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. TITLE AND SUBTITLE</th>
<th></th>
<th>5. DATES COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Engineering Risk Analysis (SERA)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. AUTHOR(S)</th>
<th></th>
<th>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Woody /Carol</td>
<td></td>
<td>Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8. PERFORMING ORGANIZATION REPORT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>13. SUPPLEMENTARY NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>The original document contains color images.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>14. ABSTRACT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>15. SUBJECT TERMS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>16. SECURITY CLASSIFICATION OF:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. REPORT unclassified</td>
</tr>
<tr>
<td>b. ABSTRACT unclassified</td>
</tr>
<tr>
<td>c. THIS PAGE unclassified</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>17. LIMITATION OF ABSTRACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAR</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>18. NUMBER OF PAGES</th>
<th>1</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>19a. NAME OF RESPONSIBLE PERSON</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

Form Approved
OMB No. 0704-0188

Approved for public release, distribution unlimited.
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

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)

Applying SERA during requirements specification
- Provides early detection of design weaknesses for remediation
- Reduces residual security risk during operations

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

Certification and Accreditation (C&A) Authorization to Operate

Software Engineering Risk Analysis (SERA)

Importance of Good Design
940 Total CWEs *  
Top 25 CWEs (Most Dangerous)

90% Design Weakness
24% Other Weakness
60% Other Weakness
40% Design Weakness

*MITRE’s Common Weakness Enumeration (CWE)

Source: http://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%).

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

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


Security Engineering Risk Analysis

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

Importance of Good Design

940 Total CWEs *  
Top 25 CWEs (Most Dangerous)

90% Design Weakness
24% Other Weakness
60% Other Weakness
40% Design Weakness

*MITRE’s Common Weakness Enumeration (CWE)

Source: http://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%).

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


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

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)

Applying SERA during requirements specification
- Provides early detection of design weaknesses for remediation
- Reduces residual security risk during operations

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

Software Engineering Risk Analysis

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

Importance of Good Design

940 Total CWEs *  
Top 25 CWEs (Most Dangerous)

90% Design Weakness
24% Other Weakness
60% Other Weakness
40% Design Weakness

*MITRE’s Common Weakness Enumeration (CWE)

Source: http://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%).

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


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