How to derive high level test procedures from a risk model

Fredrik Seehusen
Why do test-based risk assessment?

![Risk Assessment Diagram]

- **Risk 1**: (Possible, Low) = ([20:1, 50:1], Low)
- **Risk 2**: (Likely, Medium) = ([50:1, 100:1], Medium)
- **Risk 3**: (Unlikely, High) = ([10:1, 40:1], High)
Overview of method

I: CAPEC to risk model (automated)
   CAPEC attack patterns
   Generic risk model

II: Risk model refinement (manual)
    Target system
    Target specific risk model

III: Test procedure derivation (semi-automated)

Updated target specific risk model
Test-based risk assessment
Prioritized test procedures
Step I: CAPEC instances to generic risk models

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>(CAPEC-34, HTTP Response Splitting)</td>
</tr>
<tr>
<td>Typical likelihood of exploit</td>
<td>Medium</td>
</tr>
<tr>
<td>Attack motivation-consequences</td>
<td>(Execute unauthorized code or commands, {Confidentiality, Integrity, Availability}), (Gain privileges / assume identify, {Confidentiality})</td>
</tr>
<tr>
<td>CIA impact</td>
<td>(High, High, Low)</td>
</tr>
<tr>
<td>CWE ID (Related weaknesses)</td>
<td>CWE-113 Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting'), CWE-697 Insufficient Comparison, CWE-707 Improper Enforcement of Message or Data Structure, CWE-713 OWASP Top Ten 2007 Category A2 - Injection Flaws</td>
</tr>
</tbody>
</table>
Step I: CAPEC to generic risk model

Typical likelihood of exploit

CIA impact

Name

CWE ID (Related weaknesses)

Attack motivation consequences

RASEN - 316853
Step II: Risk model refinement

CAPEC-34

- CWE-713: OWASP Top Ten 2007 Category A2 - Injection Flaws
- CWE-707: Improper Enforcement of Message or Data Structure
- CWE-697: Insufficient Comparison
- CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')

Dangers:
- Execute unauthorized code or commands due to CAPEC-34 attack
- Gain privileges / assume identity due to CAPEC-34 attack

Conditions:
- Low Availability

CAPEC-62

- CWE-694: Improper Control of a Resource Through Lifetime
- CWE-715: OWASP Top Ten 2007 Category A5 - Cross Site Request Forgery (CSRF)
- CWE-732: Incorrect Permission Assignment for Critical Resources
- CWE-352: Cross-Site Request Forgery (CSRF)

Dangers:
- Modify application data due to CAPEC-62 attack
- Read application data due to CAPEC-62 attack
- Gain privileges / assume identity due to CAPEC-62 attack

Conditions:
- High Confidentiality
- High Integrity
Step II: Risk model refinement
Step II: Risk model refinement

R1: Attacker gains unauthorized access to core database with customer data
R2: Attacker causes service unavailability
R3: Attacker gains unauthorized access to user data
III: Test procedure derivation (semi-automated)
### III: Test procedure derivation (semi-automated)

<table>
<thead>
<tr>
<th>Test procedure</th>
<th>Sensitivity</th>
<th>Effort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check that Cross Site Request Forgery (aka Session Riding) leads to Cross Site Request Forgery (aka Session Riding) successful with conditional likelihood [0.001, 0.1], due to vulnerabilities OWASP Top Ten 2007 Category A5 - Cross Site Request Forgery (CSRF), Incorrect Permission Assignment for Critical Resource, Cross-Site Request Forgery (CSRF) and Improper Control of a Resource Through its Lifetime.</td>
<td>2.138E-4</td>
<td>1 day</td>
</tr>
<tr>
<td>Check that HTTP Response Splitting leads to HTTP Response Splitting successful with conditional likelihood [1.0E-4, 0.001], due to vulnerabilities Insufficient Comparison, Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting'), Improper Enforcement of Message or Data Structure and OWASP Top Ten 2007 Category A2 - Injection Flaws.</td>
<td>3.152E-8</td>
<td>1 day</td>
</tr>
</tbody>
</table>
Conclusion

- We have presented a method for risk-based test procedure derivation
- We believe that the method
  - reduces the effort of making the risk model (since much of the process is automated by transformation from CAPEC)
  - produces a risk model which is suitable for test identification
  - provides a sound basis for test prioritization