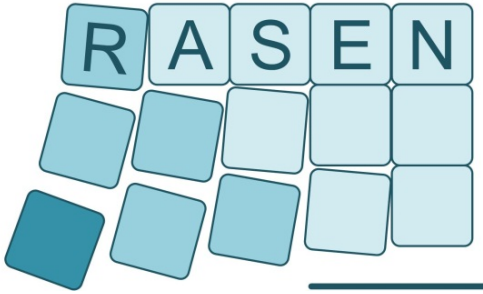


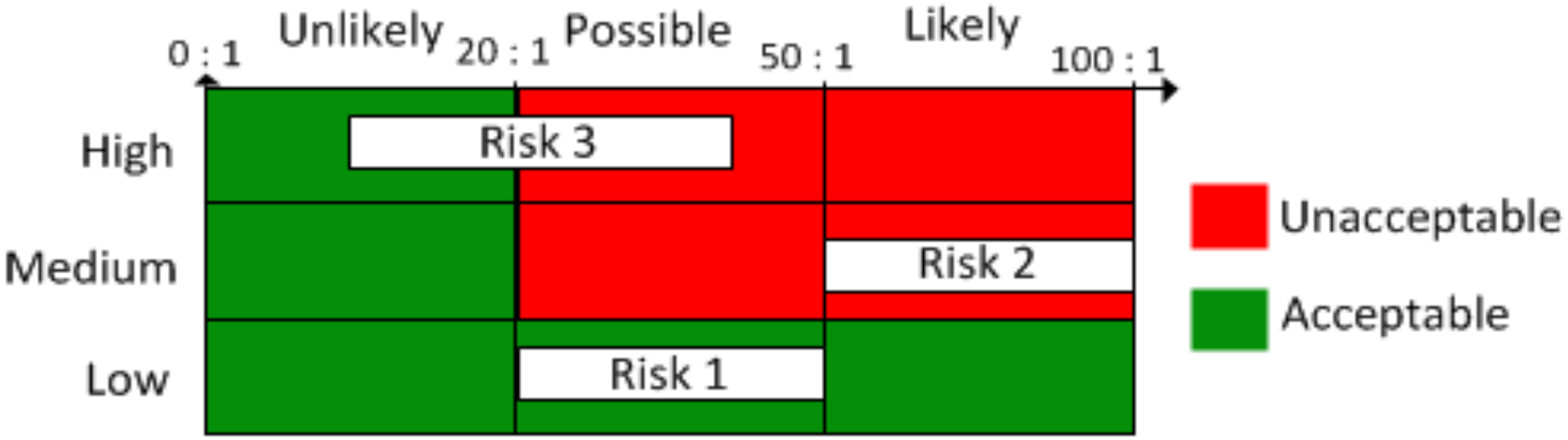
Compositional Risk Assessment and Security Testing of Networked Systems

UCAAT 2014

How to derive high level test procedures from a risk model

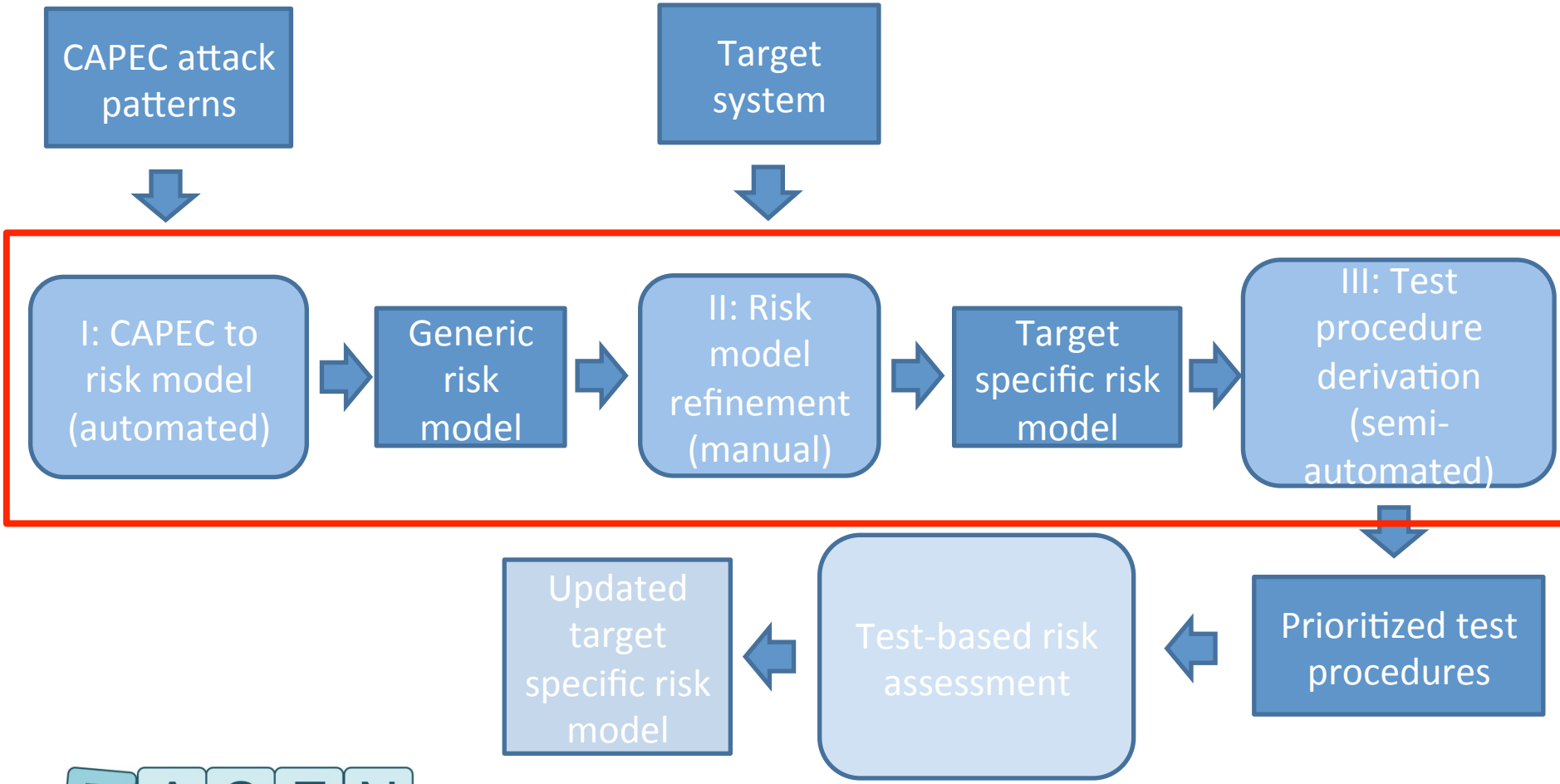
Fredrik Seehusen

Why do test-based risk assessment?



Risk 1: (Possible, Low) = ([20:1, 50:1], Low)
Risk 2: (Likely, Medium) = ([50:1, 100:1, Medium)
Risk 3: ([10:1, 40:1], High)

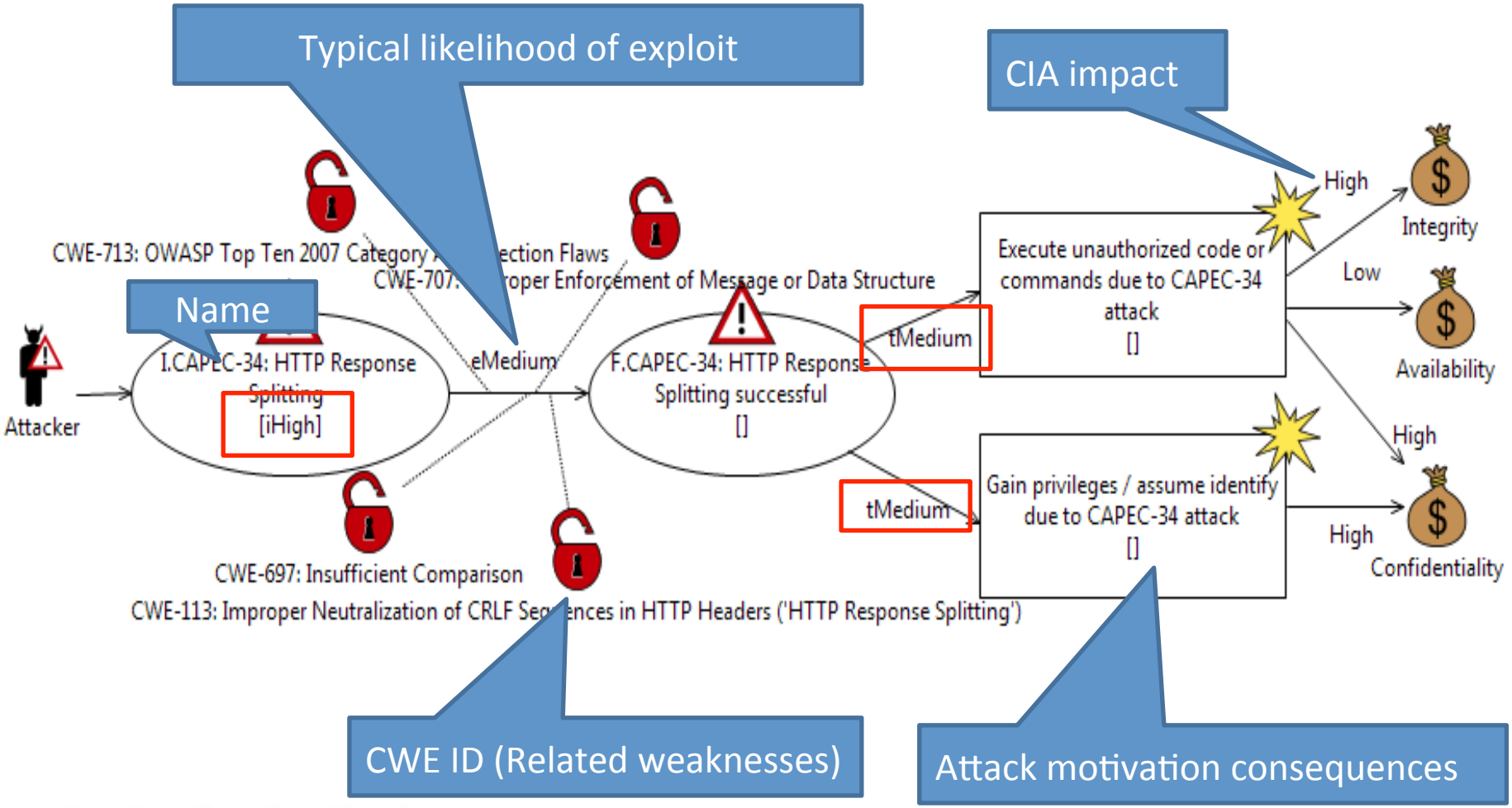
Overview of method



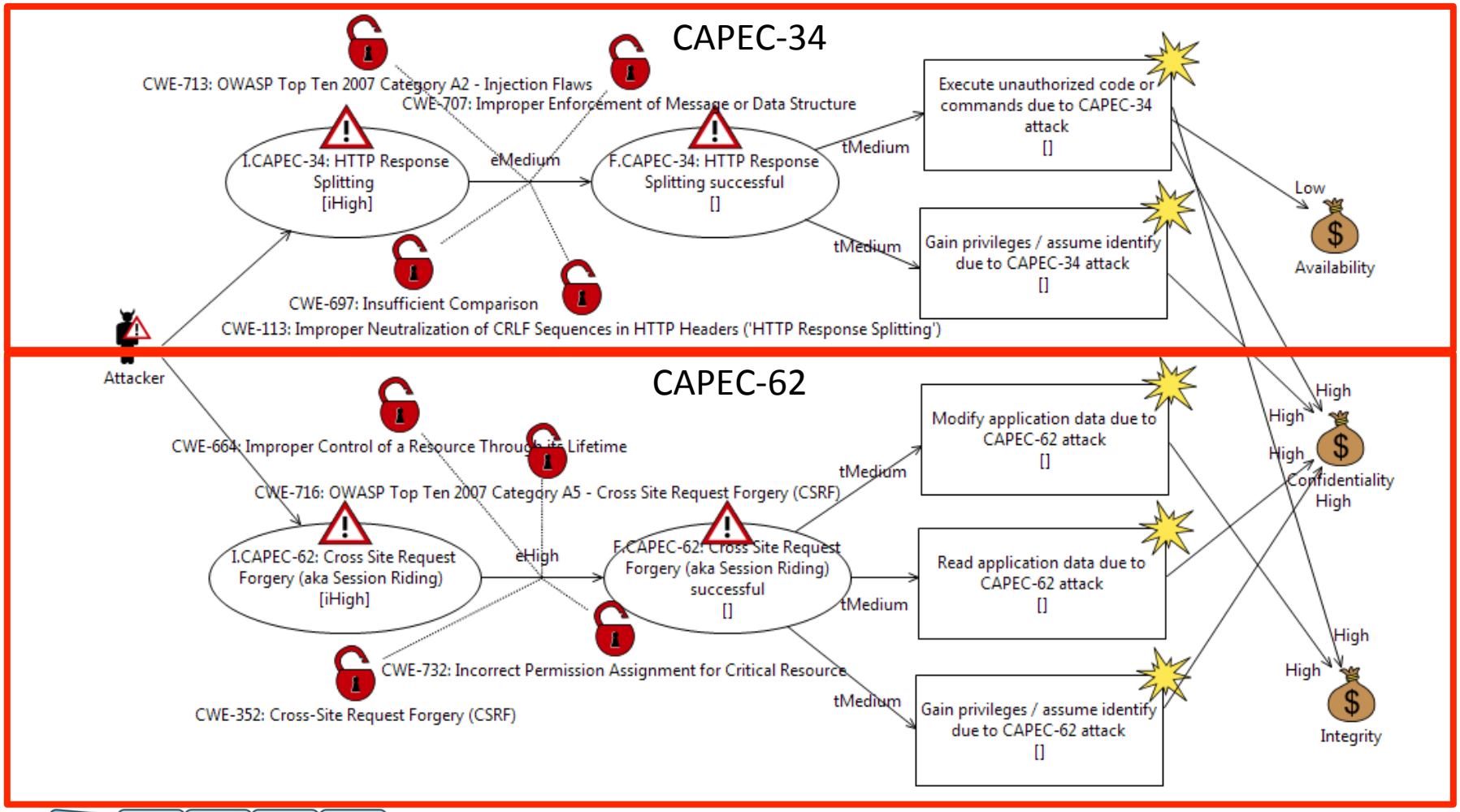
Step I: CAPEC instances to generic risk models

Attribute	Description
Name	(CAPEC-34, HTTP Response Splitting)
Typical likelihood of exploit	Medium
Attack motivation-consequences	(Execute unauthorized code or commands, {Confidentiality, Integrity, Availability}), (Gain privileges / assume identify, {Confidentiality})
CIA impact	(High, High, Low)
CWE ID (Related weaknesses)	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

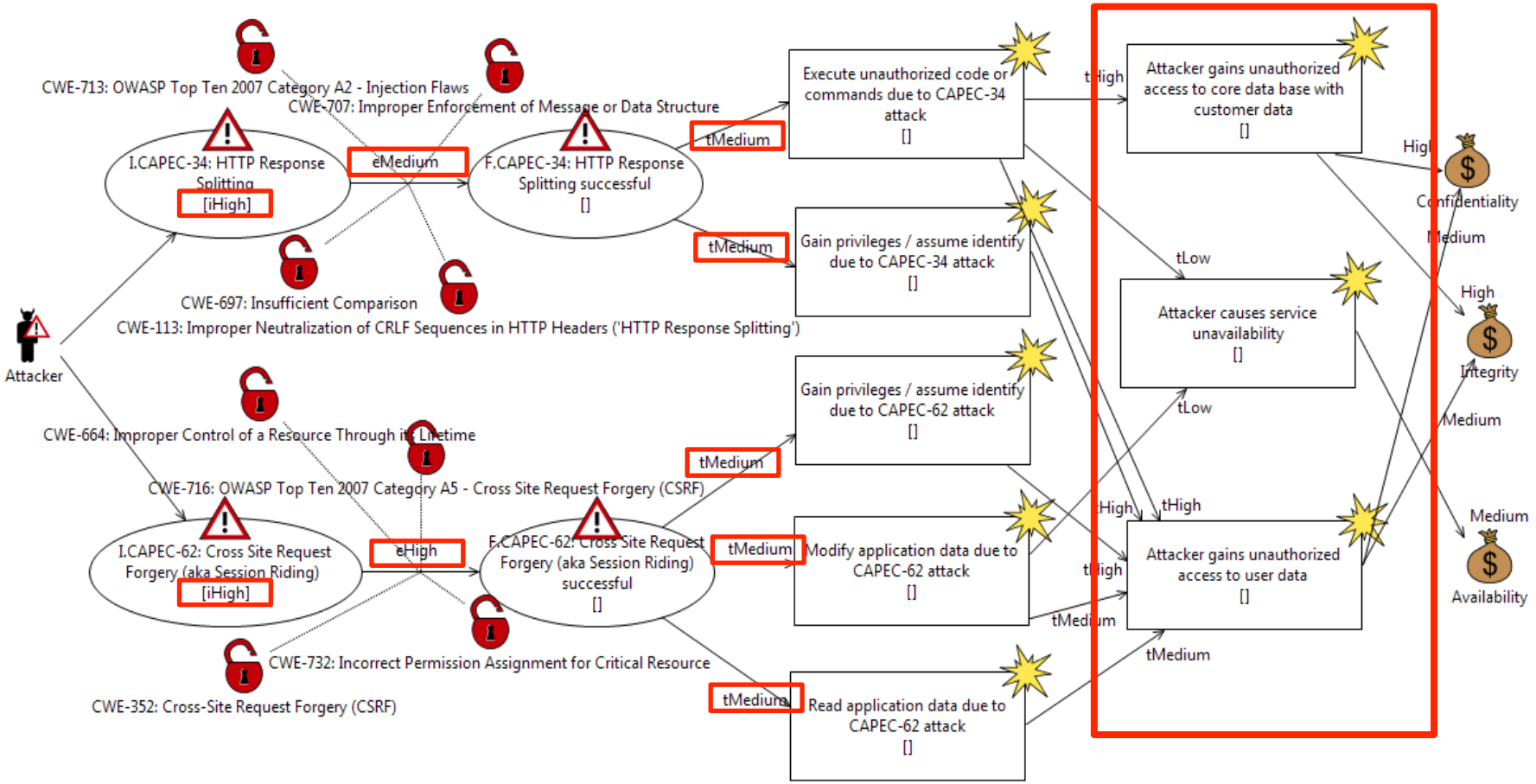
Step I: CAPEC to generic risk model



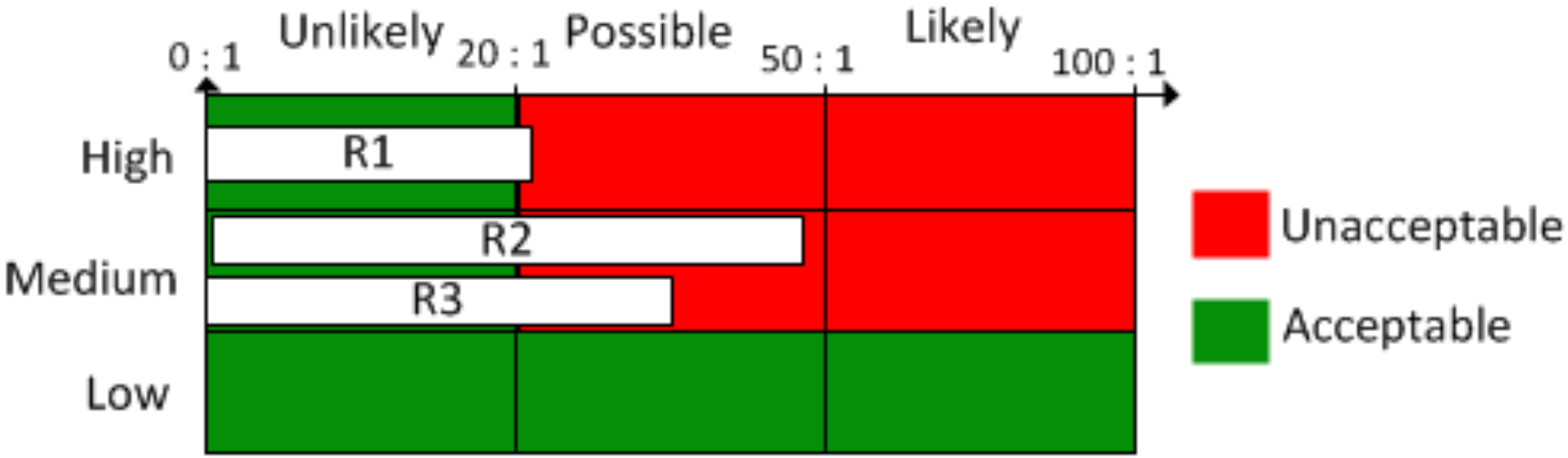
Step II: Risk model refinement



Step II: Risk model refinement



Step II: Risk model refinement

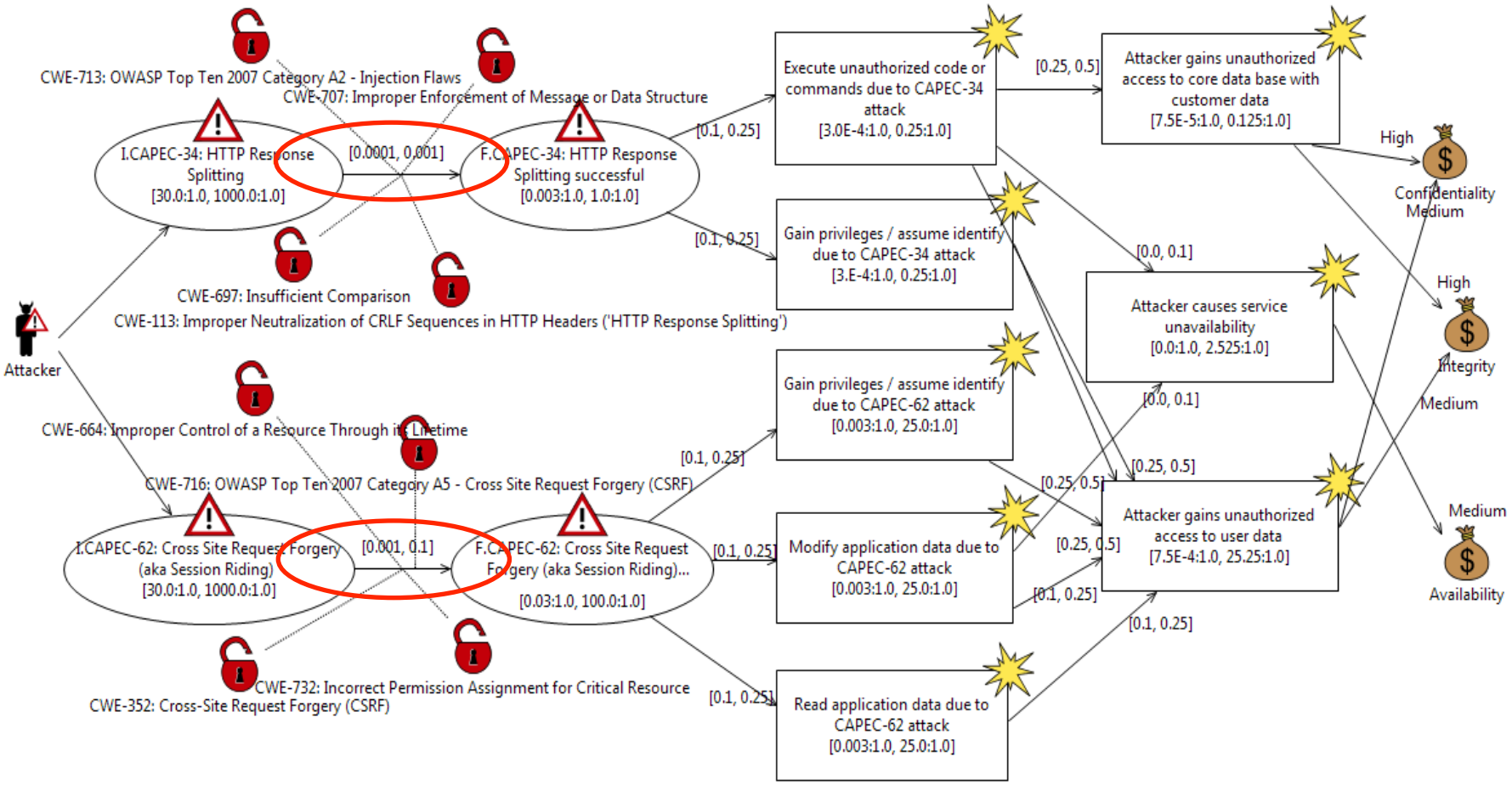


R1: Attacker gains unauthorized access to core data base with customer data

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)

Test procedure	Sensitvity	Effort
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.	2.138E-4	1 day
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.	3.152E-8	1 day

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