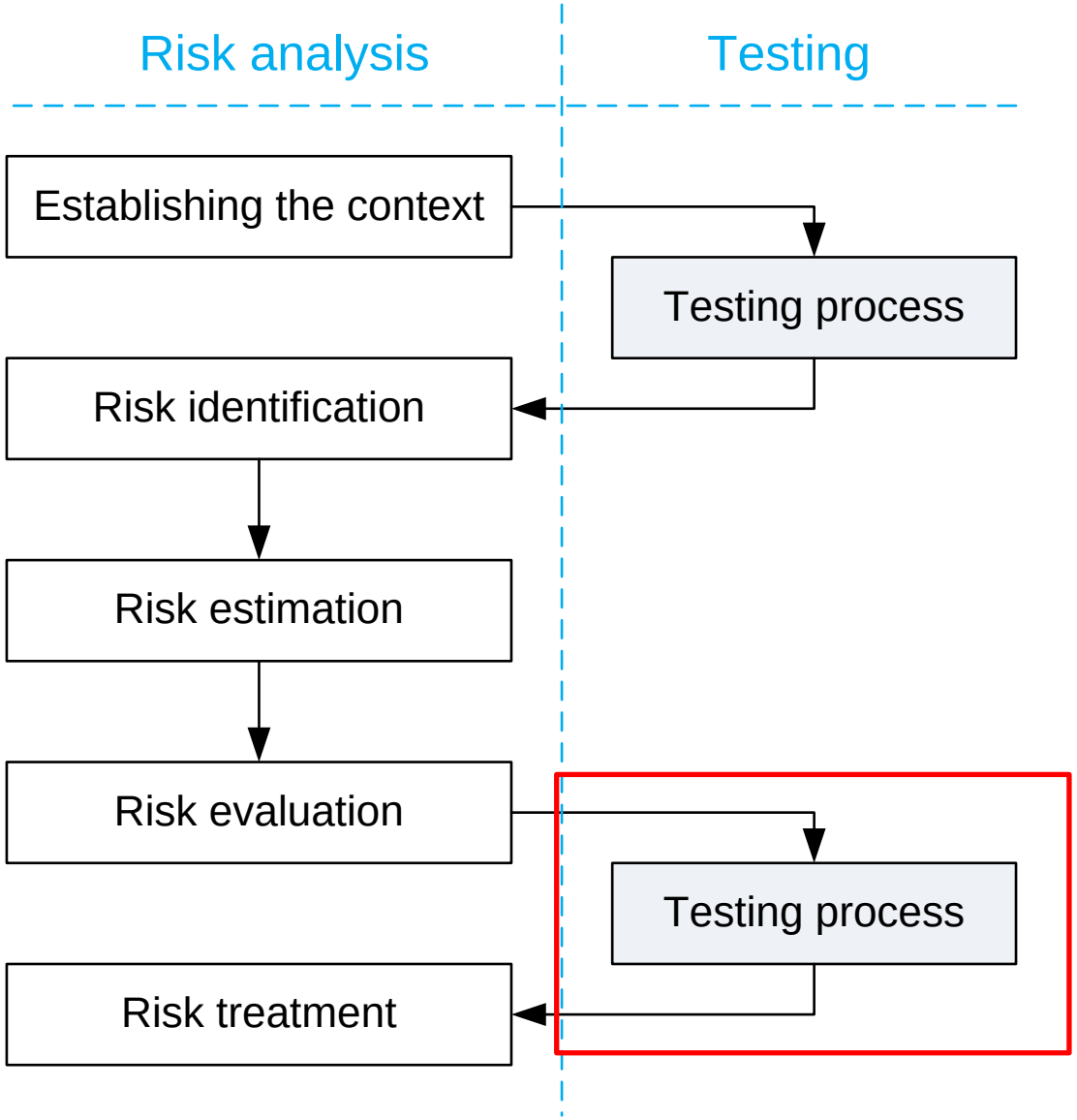
Hvordan teste en risikomodell

Fredrik Seehusen

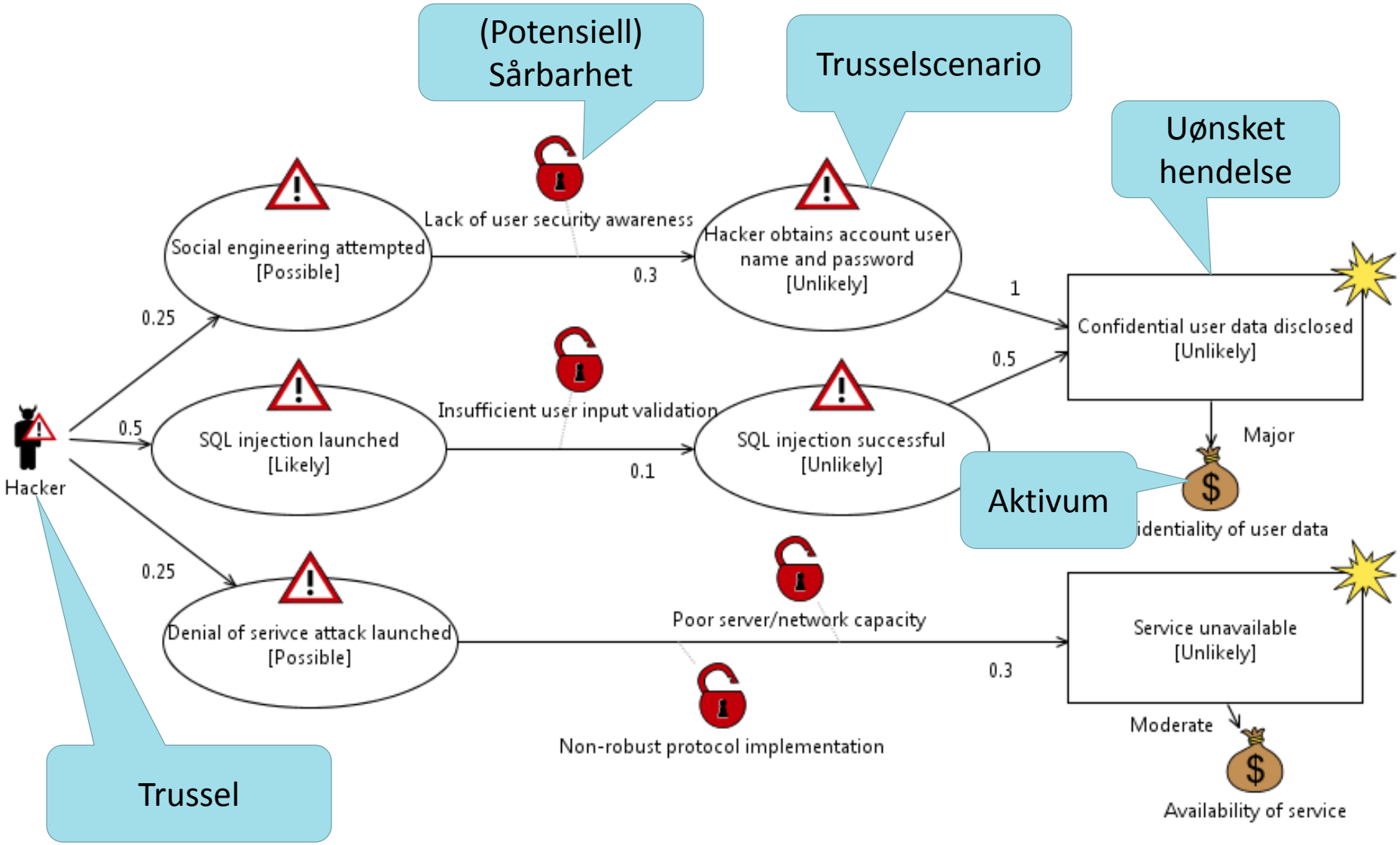
Oversikt

- Når teste en risikomodell?
- Hvorfor teste en risikomodell?
- Hvordan teste en risikomodell ?
  - Hva kan testes i en risikomodell?
  - Hvordan velge det som skal testes?
  - Hvordan påvirkes risikomodellen av testresultatene?
- Erfaringer så langt

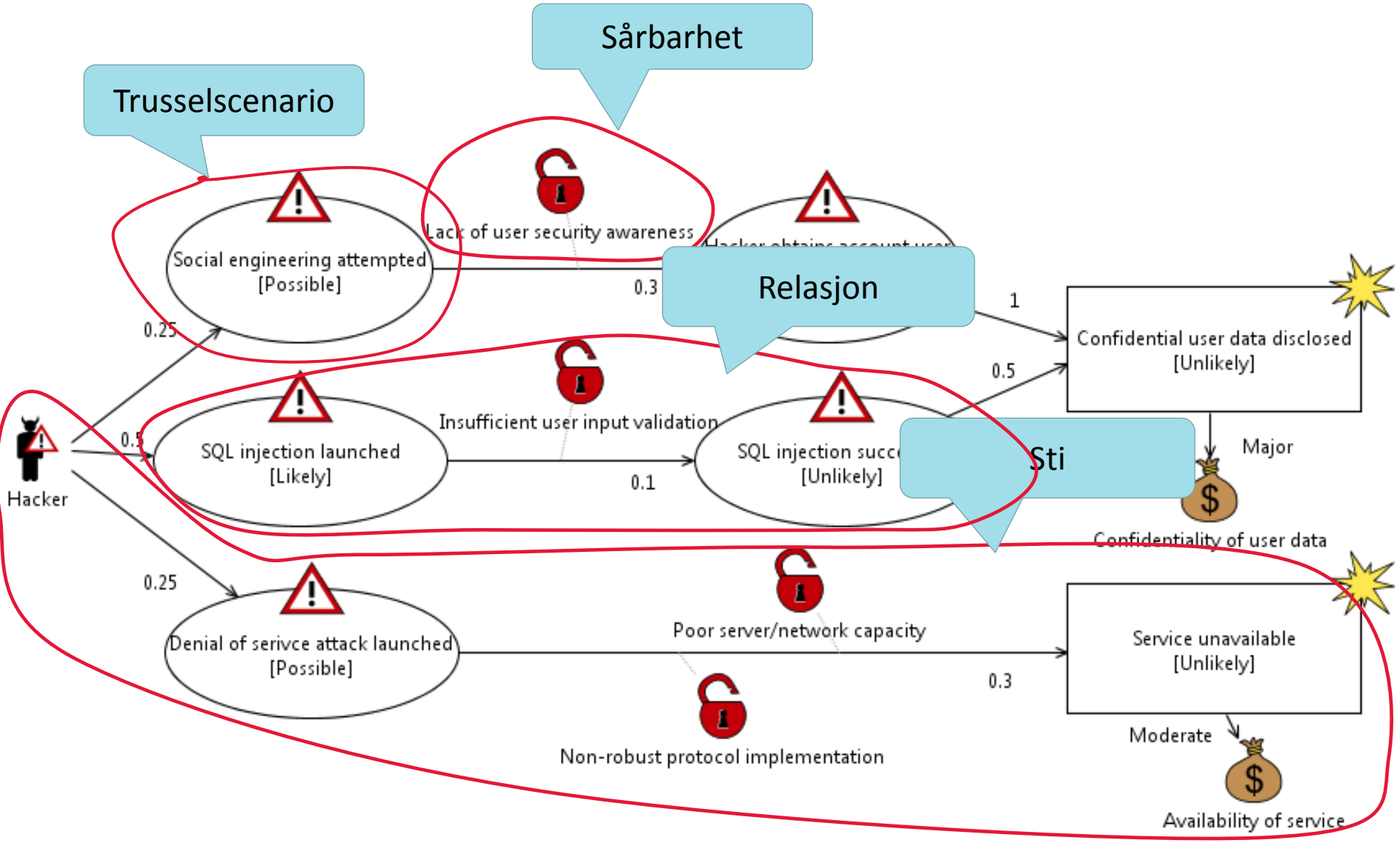
Når teste en risikomodell?



Hvorfor teste en risikomodell?



Hva kan testes i en risikomodell?



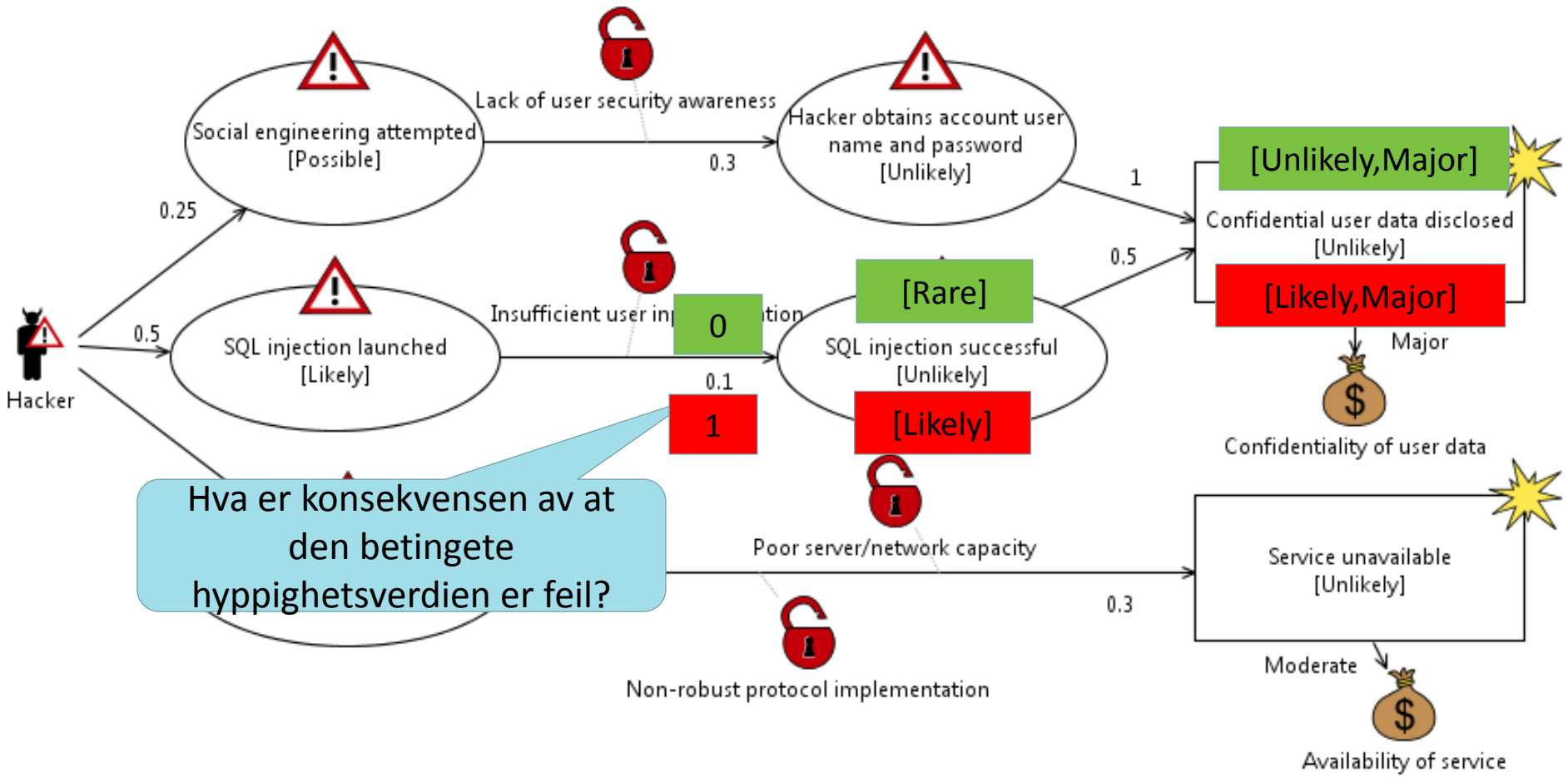
Hva kan testes i en risikomodell?

Id	Test scenario
TS1	Hacker initiates Social engineering attempted with likelihood 0.25.
TS2	Hacker initiates SQL injection launched with likelihood 0.5.
TS3	Hacker initiates Denial of service attack launched with likelihood 0.25.
TS4	Social engineering attempted leads to Hacker obtains account user name and password with conditional likelihood 0.3, due to Lack of user security awareness.
TS5	SQL injection launched leads to SQL injection successful with conditional likelihood 0.1, due to Insufficient user input validation.
TS6	Denial of service attack launched leads Service unavailable with conditional likelihood 0.3, due to Poor server/network capacity and Non-robust protocol implementation.
TS7	Hacker obtains account user name and password leads to Confidential user data disclosed with conditional likelihood 1.
TS8	SQL injection successful leads to Confidential user data disclosed with conditional likelihood 0.5.

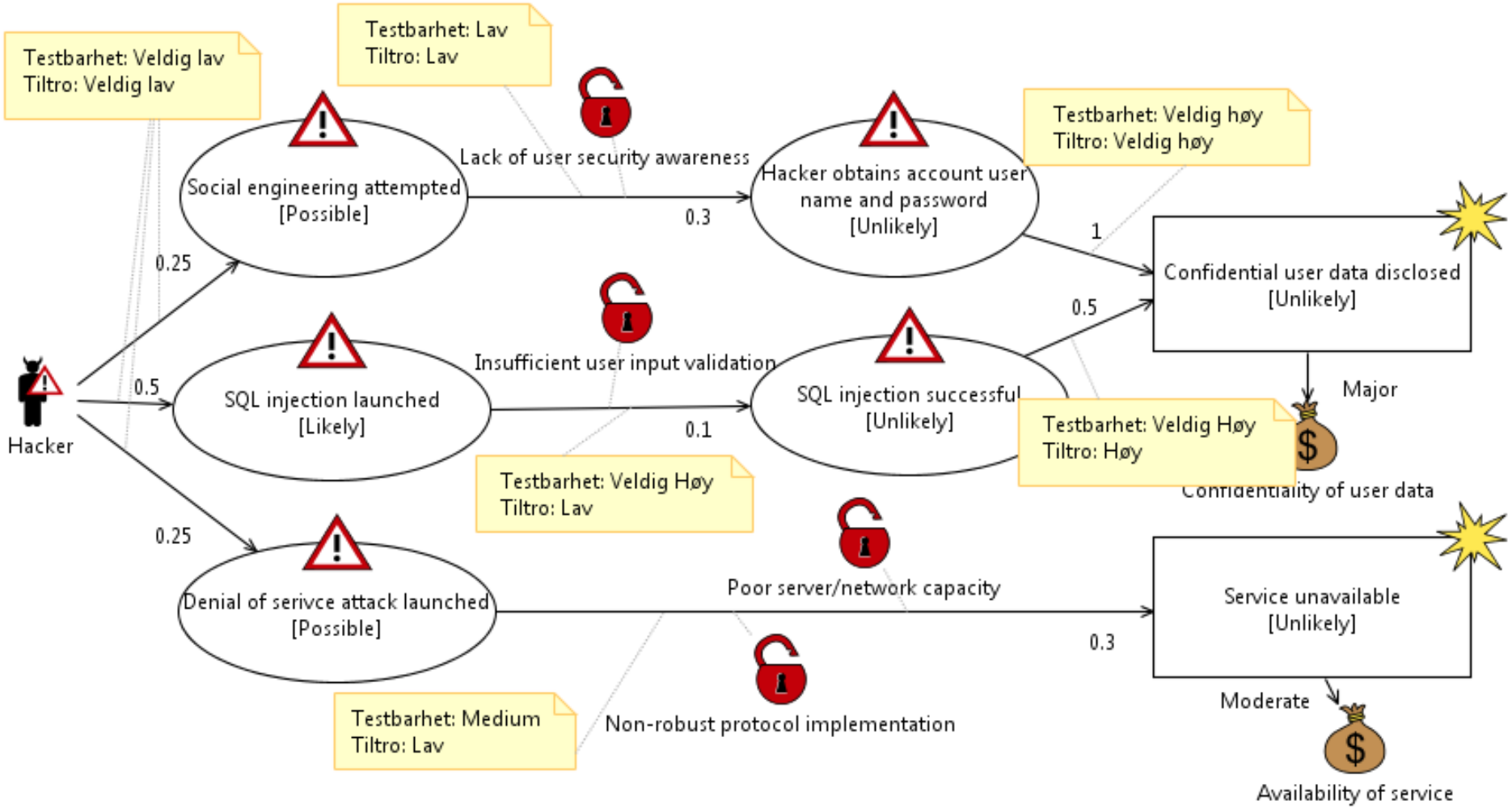
Hvordan velge det som skal testes?

- **Alvorlighetsgrad:** Et estimat på hvor mye et testscenario påvirker risikoene i risikomodellen.
- **Tiltro**: Et estimat på hvor usikker man er på korrektheten av et testscenario.
- **Testbarhet**: Et estimat på hvor testbart et testscenario er, som oftest ålt i tiden det vil ta å implementere og eksekvere testscenarioet.

Hvordan beregne alvorlighetsgrad?



Hvordan estimere testbarhet og tiltro?



Hva kan testes i en risikomodell?

Id	Test scenario	A	Te	Ti	Priority
TS5	*SQL injection launched leads to SQL injection successful with conditional likelihood 0.1, due to Insufficient user input validation.*	*3*	*4*	*3*	*36*
TS6	*Denial of service attack launched leads Service unavailable with conditional likelihood 0.3, due to Poor server/network capacity and Non-robust protocol implementation.*	*3.2*	*2*	*3*	*19.2*
TS4	Social engineering attempted leads to Hacker obtains account user name and password with conditional likelihood 0.3, due to Lack of user security awareness.	1.5	1	3	4.5
TS1	Hacker initiates Social engineering attempted with likelihood 0.25.	2.5	0	4	0
TS2	Hacker initiates SQL injection launched with likelihood 0.5.	2.5	0	4	0
TS3	Hacker initiates Denial of service attack launched with likelihood 0.25.	2.5	0	4	0
TS7	Hacker obtains account user name and password leads to Confidential user data disclosed with conditional likelihood 1.	1	4	0	0
TS8	SQL injection successful leads to Confidential user data disclosed with conditional likelihood 0.5.	2	4	0	0

Hvordan påvirkes risikomodellen av testresultatene?

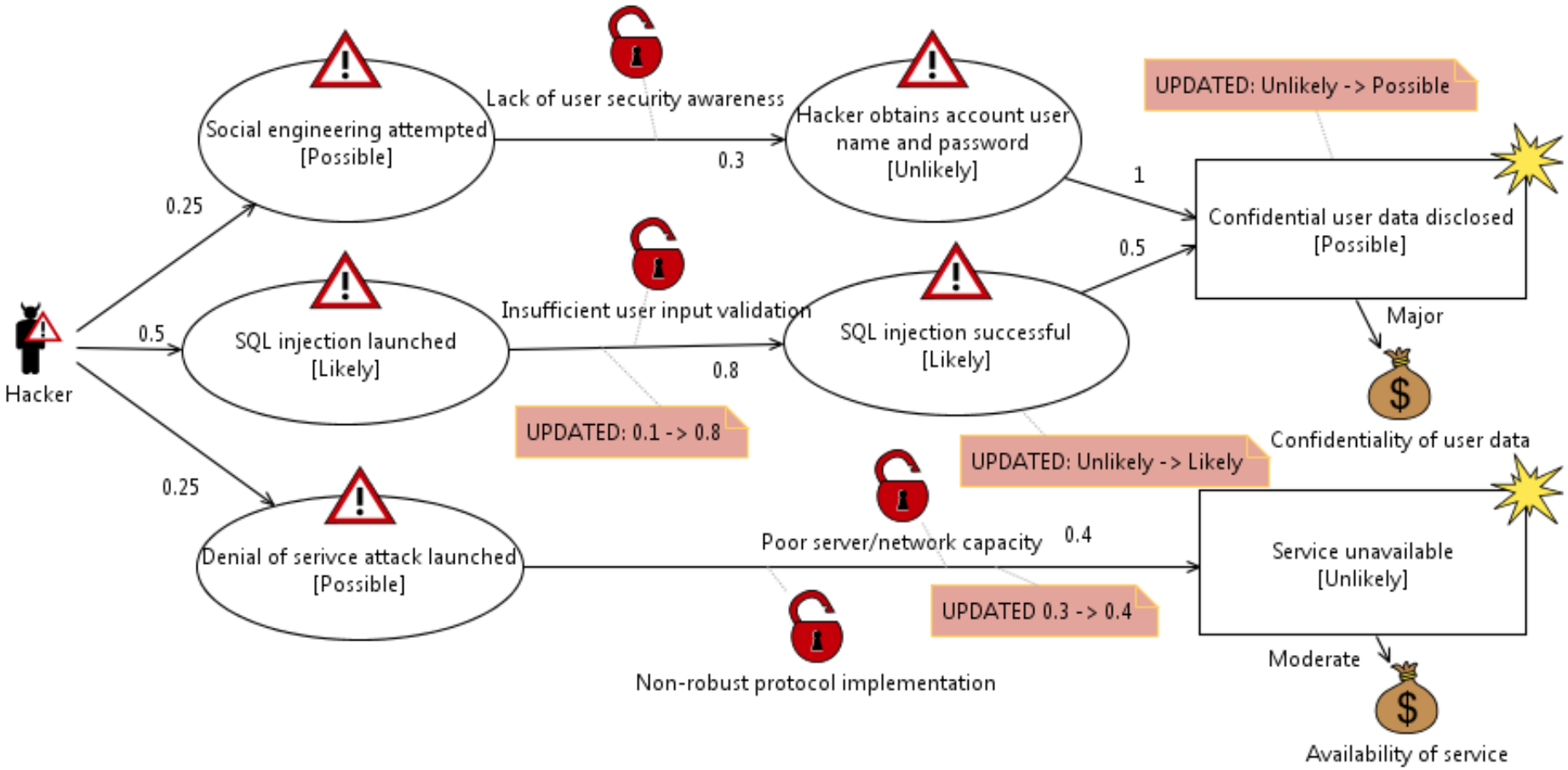
- **Likelihood:** Et estimat på hvor sannsynlig det er at en sårbarhet eksisterer

- **Exploitability:** Et estimat på hvor lett det er å utnytte en sårbarhet gitt at den eksiterer

Hvordan påvirkes risikomodellen av testresultatene?

TID	Vulnerability	Likelihood	Exploitability
TS5	Insufficient user input validation	1	0.8
TS6	Poor server/network capacity	0.4	0.7
TS6	Non-robust protocol implementation	0.2	0.6

Hvordan påvirkes risikomodellen av testresultatene?



Erfaringer så langt

- Testing er nyttig for å verifisere korrektheten av en risikomodell
- Risiko analysen er nyttig for å identifisere relevante tester og for å få en oversikt over sikkerheten til et system
- Testresultatenes påvirkning på risikomodellen har variert i fra case studie til case studie
- Det må jobbes mer med prioriteringen av testscenarier