To create a hierarchical tree for the Instant Messaging (IM) software security case using the provided security case pattern, we can structure it as follows. Each element from the pattern is substituted with relevant information from the domain of IM software.

### Instant Messaging Security Case Hierarchical Tree

- \*\*Goal (G1, "Instant messaging software is acceptably secure in the system")\*\*

- \*\*Context (C1, "Definition and description of instant messaging software.")\*\*

- \*\*Context (C2, "Definition and description of the system.")\*\*

- \*\*Context (C3, "Definition of what is meant by 'acceptably secure'.")\*\*

- \*\*Strategy (S1, "Argument that instant messaging software assets are under protection")\*\*

- \*\*Justification (J1, "Protection of software assets supports that software is acceptably secure")\*\*

- \*\*Goal (G2, "All identified instant messaging software critical assets are protected")\*\*

- \*\*Context (C4, "List of instant messaging software critical assets: registration information, registration process, user account information, authentication information, login process, chat logs.")\*\*

- \*\*Strategy (S2, "Respective arguments for each instant messaging software critical asset")\*\*

- \*\*Justification (J2, "Relationship between assets is clear and can be argued separately")\*\*

- \*\*Goal (G3, "Instant messaging software critical asset is protected")\*\*

- \*\*Strategy (S3, "Argument based on the type to which the software critical asset belongs")\*\*

- \*\*Context (C5, "List of software critical asset types in PEDD: Process, Environment Entity, Data Exchange, Data Storage")\*\*

- \*\*Justification (J3, "Types of software assets are according to PEDD classification")\*\*

- \*\*HasMultiplicity (S2, G4, "Number of software critical asset = 4")\*\*

- \*\*Goal (G4, "Instant messaging software critical asset {specific asset}, which belongs to {specific type}, is protected")\*\*

- \*Potentially this goal is expanded multiple times, one for each critical asset, such as:\*

- \*\*Goal (G4a, "Registration information, which belongs to Data Storage, is protected")\*\*

- \*\*Goal (G4b, "Registration process, which belongs to Process, is protected")\*\*

- \*\*Goal (G4c, "User account information, which belongs to Data Storage, is protected")\*\*

- \*\*Goal (G4d, "Login process, which belongs to Process, is protected")\*\*

- \*\*Goal (G4e, "Chat logs, which belong to Data Exchange, are protected")\*\*

This hierarchy showcases how strategies support the overall goal of making the instant messaging software acceptably secure by specifically securing each critical asset. 구충 with key contexts and justifications provide a rational basis for each element of the strategy. The critical assets and their specific classifications (from PEDD) are directly argued within the respective goals and strategies.