Based on the provided security case pattern and the domain information about Instant Messaging (IM) software, here is the instantiated security case represented in a hierarchical tree format:

@Assurance\_case

- G1: Instant Messaging software is acceptably secure in the IM system

- C1: Definition and description of Instant Messaging software

- C2: Definition and description of the IM system

- C3: Definition of acceptably secure

- S1: Argument that software assets are under protection

- J1: Protection of software assets supports that software is acceptably secure

- G2: All identified IM software critical assets are protected

- C4: List of Instant Messaging software critical assets

- S2: Respective arguments of IM software critical assets

- J2: Relationship between assets is clear and can be argued separately

- G3: IM software critical asset is protected

- S3: Argument of the type which the IM software critical asset belongs to

- C5: List of IM software critical asset types in PEDD (Process, Environment Entity, Data Exchange, and Data Storage)

- J3: Types of IM software assets are according to PEDD

- G4: Registration information is protected (which belongs to Data Exchange)

- G4: Registration process is protected (which belongs to Process)

- G4: User account information is protected (which belongs to Data Storage)

- G4: Authentication information is protected (which belongs to Data Storage)

- G4: Login process is protected (which belongs to Process)

- G4: Chat logs are protected (which belongs to Data Storage)

@End\_Assurance\_case

This hierarchical tree format represents the assurance case detailing the security of assets within Instant Messaging software according to the specified security goals, strategies, contexts, and justifications. Each goal and strategy is supported by subsequent steps, linked with defined contexts that provide a comprehensive understanding and justification of each assertion.