Here's the instantiated security case for Instant Messaging (IM) software using the given security case pattern, displayed in a hierarchical tree format using dashes (-) to denote different levels:

```

G1: The IM software is acceptably secure in the provided environment.

- C1: Definition and description of IM software

- C2: Definition and description of the provided environment

- C3: Definition of acceptably secure

- S1: Argument that IM 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

- S2: Respective arguments of IM software critical assets

- C4: List of IM software critical assets

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

- G3: Registration information is protected

- S3: Argument of the type which the registration information belongs to

- C5: List of software critical asset types in PEDD

- J3: Types of software assets are according to PEDD

- G4: Registration information which belongs to Data Storage is protected

- G3: Registration process is protected

- S3: Argument of the type which the registration process belongs to

- C5: List of software critical asset types in PEDD

- J3: Types of software assets are according to PEDD

- G4: Registration process which belongs to Process is protected

- G3: User account information is protected

- S3: Argument of the type which the user account information belongs to

- C5: List of software critical asset types in PEDD

- J3: Types of software assets are according to PEDD

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

- G3: Authentication information is protected

- S3: Argument of the type which the authentication information belongs to

- C5: List of software critical asset types in PEDD

- J3: Types of software assets are according to PEDD

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

- G3: Login process is protected

- S3: Argument of the type which the login process belongs to

- C5: List of software critical asset types in PEDD

- J3: Types of software assets are according to PEDD

- G4: Login process which belongs to Process is protected

- G3: Chat logs are protected

- S3: Argument of the type which the chat logs belong to

- C5: List of software critical asset types in PEDD

- J3: Types of software assets are according to PEDD

- G4: Chat logs which belong to Data Storage is protected

```

In this instantiated security case:

- The goal (G1) is to claim that the IM software is acceptably secure in the provided environment.

- The strategy (S1) argues that the protection of IM software assets supports the claim.

- The argument (G2) states that all identified critical assets of IM software are protected.

- The strategy (S2) provides respective arguments for each critical asset.

- The strategy (S3) breaks it down further by the type of critical asset according to PEDD (Process, Environment Entity, Data Exchange, Data Storage).

- Contexts (C1, C2, C3) provide definitions and descriptions relevant to the primary goal.

- Context (C4) lists the critical assets.

- Justifications (J1, J2, J3) support the arguments made at various levels.

- Each goal (G3 and G4) and strategy follow suit to ensure the comprehensive protection of every critical asset like registration information, registration process, user account information, authentication information, login process, and chat logs, with regards to their type and classification.