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

```

G1: IM software is acceptably secure in the system

- C1: IM as a form of real-time communication software

- C2: Operational environment for IM software

- C3: Acceptably secure means fulfilling specified security requirements

- S1: Argument of that IM software assets are under protection

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

- G2: All identified IM software critical assets are protected

- C4: List of IM software critical assets includes User Accounts, Authentication Information, Chat Logs

- S2: Respective arguments of IM software critical assets

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

- G3: Specific IM software critical asset is protected

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

- C5: List of software critical asset types in PEDD includes Process, Environment Entity, Data Exchange, Data Storage

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

- G4: Specific IM software critical asset which belongs to a type is protected

- G4: User account information, a type of Data Storage, is protected

- G4: Authentication information, a type of Data Exchange, is protected

- G4: Chat logs, a type of Data Storage, is protected

- G4: Registration information, a type of Data Storage, is protected

```

### Explanation:

- \*\*G1\*\* is the top-level goal stating that the IM software is acceptably secure within its operational system. This is contextualized by three contexts detailing what is meant by 'IM software', 'system', and 'acceptably secure'.

- \*\*S1\*\* formulates the overarching strategy claiming protection over software assets.

- \*\*J1\*\* justifies that if software assets are protected, it leads to acceptable security.

- \*\*G2\*\* branches off into identifying and ensuring the protection of all critical assets.

- \*\*S2\*\* supports G2 by arguing for each critical asset's protection. Supported by C4 (listing assets) and J2 (rationalizing the approach).

- \*\*G3-Evaluation\*\* of the protection measures for individual critical assets. Connects to \*\*S3-arguments\*\* based specific asset types and their protection.

- \*\*G4\*\* details specific protections per asset type, aligned with the PEDD classification, further validating the security measures are correct and adequate.