Based on the given security case pattern and the specific details about Instant Messaging (IM) software from the domain information, we will instantiate the placeholders with the detailed information relevant to the IM software. Below is the derived security case in a hierarchical tree format:

```

- G1: IM Software is acceptably secure in the user interaction system

- C1: IM Software includes features such as message transmission, media sharing, and user presence information.

- C2: User interaction system includes all networks, devices, and users interacting via the IM software.

- C3: Acceptably secure means that all critical assets are protected against unauthorized access and data breaches.

- S1: Argument that IM software assets are under protection

- J1: Protection of IM software assets ensures that the software can be considered secure under typical operational conditions.

- G2: All identified IM software critical assets are protected

- C4: Critical Assets include registration information, user account details, authentication processes, chat logs, and login processes.

- S2: Respective arguments of IM software critical assets

- J2: Each critical asset has distinct security measures, easily separable for individual argumentation.

- G3: User account information is protected

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

- C5: Types of software critical assets following PEDD: Process, Environment Entity, Data Exchange, Data Storage

- J3: User account information falls under Data Storage and Environment Entity, needing specific security measures like encryption and secure environment handling.

- G4: User account information, which belongs to Data Storage and Environment Entity, is protected

---- (additional G4s for other critical assets like registration information, authentication information, etc.)

```

In the hierarchical structure displayed above:

- Each "Goal (G#)" describes a security claim that we aim to substantiate through deeper strategies and supporting goals.

- "Strategy (S#)" elements refine the argument, linking overarching goals with more specific sub-goals.

- "Context (C#)" provides background knowledge relevant to the arguments.

- "Justification (J#)" underlines the rationale for why certain strategies or associations are valid and necessary as they relate to the overall security case.

- "Multiplicity" is used here to represent the number of "G4" goals generated based on the different asset types identified in the IM software, each of which gets a similar level of detail argument in "S3".

This structured approach ensures that the security argumentation is comprehensive, addressing different components and aspects of the IM software systematically.