Based on the security case pattern provided, here is how the security case for Instant Messaging (IM) software can be presented using a hierarchical tree format:

```

G1: IM software is acceptably secure in its operational environment

- C1: IM software includes features such as message exchange, file transfer, and user authentication

- C2: Operational environment includes user devices, network connections, and server infrastructure

- C3: Acceptably secure means adequate protection against unauthorized access, data leaks, and other security threats

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

--- J1: Protection of IM software assets ensures the software is secure according to defined security standards

---- G2: All identified IM software critical assets are protected

----- C4: Critical assets include Registration information, Registration process, User account information, Authentication information, Login process, and Chat logs

----- J2: Each critical asset can be distinctly protected and verified

------ S2: Respective arguments of IM software critical assets

------- SupportedBy (S2 to G3)

-------- G3: Registration information is protected

---------- S3: Argument based on the data type which the software critical asset belongs to

----------- J3: Types of software assets categorized under PEDD are Process, Environment Entity, Data Exchange, and Data Storage

------------ C5: List of software critical asset types include process-related assets (e.g., Registration process, Login process) and data-related assets (e.g., User account information, Chat logs)

------------- G4: Registration process which belongs to the type 'Process' is protected

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

-------------- G4: Login process which belongs to the type 'Process' is protected

-------------- G4: Chat logs which belong to the type 'Data Exchange' are protected

```

### Explanation:

- The tree starts with Goal 1 (G1) which is about the overall security claim that "IM software is acceptably secure in its operational environment". This is supported by Contexts 1, 2, and 3 (C1, C2, C3) which define the software, the environment it operates in, and what 'acceptably secure' means.

- Strategy 1 (S1) argues that all software assets are under proper protection.

- This is justified by Justification 1 (J1) – stating that protecting these assets supports the overall security of the software.

- Goal 2 (G2) asserts that all identified critical assets are protected, supported by Context 4 (C4) and Justification 2 (J2) – noting that these assets include various components such as registration information and processes, and the protection of each can be distinctly verified.

- Strategy 2 (S2) is about arguing the protection measures for each critical asset of the software.

- Goal 3 (G3) to Goal 4 sub-goals (G4x4 due to multiplicity) detail the protection of individual assets and their respective types, defined and supported by Context 5 (C5) and Justification 3 (J3) – categorized under the PEDD types.

This structure allows the assurance case to unfold from general security claims to specific security measures on critical assets, ensuring comprehensiveness and clarity in presenting the argument for the security of IM software.