Based on the given predicates for a security case pattern, here is the derived security case for Instant Messaging (IM) software, displayed in a hierarchical tree format using dashes (-) to denote different levels:

```

- G1: Instant Messaging (IM) software is acceptably secure in the messaging system.

- C1: Definition and description of Instant Messaging (IM) software

- C2: Definition and description of the messaging system

- C3: Definition of acceptably secure

- S1: Argument that IM software assets are under protection

- J1: Protection of software assets supports that IM 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: IM software critical asset is protected

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

- C5: List of software critical asset types in PEDD

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

- G4: User data which belongs to private data is protected

- G4: Message history which belongs to private data is protected

- G4: Encryption keys which belong to security data are protected

- G4: Server access which belongs to internal system access is protected

```

### Explanation:

1. \*\*Goal G1\*\* (Instant Messaging (IM) software is acceptably secure in the messaging system) is the top-level goal.

2. \*\*Contexts (C1, C2, C3)\*\* provide a description and definition necessary for understanding the top-level goal.

3. \*\*Strategy S1\*\* supports Goal G1, and \*\*Justification J1\*\* is used in conjunction with this strategy to argue that protecting software assets supports the security claim.

4. \*\*Goal G2\*\* asserts that all identified software critical assets are protected. This is supported by \*\*Strategy S2\*\*.

5. \*\*Contexts (C4)\*\* and \*\*Justification J2\*\* provide additional information used in the argument for Strategy S2.

6. \*\*Goal G3\*\* states that individual software critical assets are protected. This is supported by \*\*Strategy S3\*\*.

7. \*\*Context (C5)\*\* and \*\*Justification J3\*\* explain the types of software critical assets.

8. \*\*Goal G4\*\* instances capture specific critical assets (User data, Message history, Encryption keys, and Server access) and their respective protection needs based on their types (private data, security data, internal system access).

By following the hierarchical structure, you can depict the relationships and context necessary to argue that the IM software is secure.