To create the security case for Instant Messaging (IM) software based on the provided security case pattern, we will instantiate the generic information into specific details pertaining to the IM software. We will also organize and display it in a hierarchical tree format using dashes to denote different levels.

Here is the instantiated assurance case for the IM software:

```

- Goal (G1, IM software is acceptably secure in the system)

- Context (C1, Definition and description of IM software)

- Context (C2, Definition and description of the system)

- Context (C3, Definition of acceptably secure)

- Strategy (S1, Argument that IM software assets are under protection)

- Justification (J1, Protection of IM software assets supports that IM software is acceptably secure)

- Goal (G2, All identified IM software critical assets are protected)

- Strategy (S2, Respective arguments of IM software critical assets)

- Context (C4, List of IM software critical assets)

- Justification (J2, Relationship between assets is clear and can be argued separately)

- Goal (G3, Registration information is protected)

- Strategy (S3, Argument of the type which Registration information belongs to)

- Context (C5, List of IM software critical asset types in PEDD)

- Justification (J3, Types of IM software assets are according to PEDD)

- Goal (G4, Registration information which belongs to Data Exchange is protected)

- Goal (G3, Registration process is protected)

- Strategy (S3, Argument of the type which Registration process belongs to)

- Context (C5, List of IM software critical asset types in PEDD)

- Justification (J3, Types of IM software assets are according to PEDD)

- Goal (G4, Registration process which belongs to Process is protected)

- Goal (G3, User account information is protected)

- Strategy (S3, Argument of the type which User account information belongs to)

- Context (C5, List of IM software critical asset types in PEDD)

- Justification (J3, Types of IM software assets are according to PEDD)

- Goal (G4, User account information which belongs to Data Storage is protected)

- Goal (G3, Authentication information is protected)

- Strategy (S3, Argument of the type which Authentication information belongs to)

- Context (C5, List of IM software critical asset types in PEDD)

- Justification (J3, Types of IM software assets are according to PEDD)

- Goal (G4, Authentication information which belongs to Data Exchange is protected)

- Goal (G3, Login process is protected)

- Strategy (S3, Argument of the type which Login process belongs to)

- Context (C5, List of IM software critical asset types in PEDD)

- Justification (J3, Types of IM software assets are according to PEDD)

- Goal (G4, Login process which belongs to Process is protected)

- Goal (G3, Chat logs are protected)

- Strategy (S3, Argument of the type which Chat logs belongs to)

- Context (C5, List of IM software critical asset types in PEDD)

- Justification (J3, Types of IM software assets are according to PEDD)

- Goal (G4, Chat logs which belongs to Data Storage is protected)

```

Each level of the tree helps ensure that all critical assets of the IM software are protected according to PEDD classification, thus making the software acceptably secure. This tree structure visualizes the assurance case for the IM software using the instantiated pattern.