Based on the provided security case pattern and the domain information for the Instant Messaging (IM) software, we can create a security case for the IM software by instantiating the placeholders with the relevant information. The critical assets for IM software include registration information, registration process, user account information, authentication information, login process, and chat logs.

Here's the hierarchical tree format representation of the security case for IM software:

```

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

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

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

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

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

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

- Goal (G3.1, Registration information is protected)

- Strategy (S3.1, Argument of the type which Registration information belongs to)

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

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

- Goal (G4.1, Registration information which belongs to Data Storage is protected)

- Goal (G3.2, Registration process is protected)

- Strategy (S3.2, Argument of the type which Registration process belongs to)

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

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

- Goal (G4.2, Registration process which belongs to Process is protected)

- Goal (G3.3, User account information is protected)

- Strategy (S3.3, Argument of the type which User account information belongs to)

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

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

- Goal (G4.3, User account information which belongs to Data Storage is protected)

- Goal (G3.4, Authentication information is protected)

- Strategy (S3.4, Argument of the type which Authentication information belongs to)

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

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

- Goal (G4.4, Authentication information which belongs to Data Storage is protected)

- Goal (G3.5, Login process is protected)

- Strategy (S3.5, Argument of the type which Login process belongs to)

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

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

- Goal (G4.5, Login process which belongs to Process is protected)

- Goal (G3.6, Chat logs information is protected)

- Strategy (S3.6, Argument of the type which Chat logs information belongs to)

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

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

- Goal (G4.6, Chat logs which belongs to Data Storage is protected)

```

This representation shows the hierarchical relationship of goals, strategies, contexts, and justifications, starting from the top-level goal of achieving acceptable security for the IM software down to specific goals for protecting individual critical assets.