To create a hierarchical tree format security case for Instant Messaging (IM) software, multiple goals need to be constructed based on the provided pattern and the domain information. Here's the hierarchical structure:

```

Goal (G1, The Instant Messaging (IM) software is acceptably secure in the system.)

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

- Context (C2, Definition and description of system)

- Context (C3, Definition of acceptably secure)

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

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

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

- Strategy (S2, Respective arguments for 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 the software critical asset belongs to)

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

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

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

- Goal (G3, Registration process is protected)

- Strategy (S3, Argument of the type which the software critical asset belongs to)

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

- Justification (J3, Types of 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 the software critical asset belongs to)

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

- Justification (J3, Types of 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 the software critical asset belongs to)

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

- Justification (J3, Types of 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 the software critical asset belongs to)

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

- Justification (J3, Types of 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 the software critical asset belongs to)

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

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

- Goal (G4, Chat logs which belong to Data Storage are protected)

```

In this hierarchical tree, the critical assets of the IM software are:

- Registration information (Data Storage)

- Registration process (Process)

- User account information (Data Storage)

- Authentication information (Data Exchange)

- Login process (Process)

- Chat logs (Data Storage)

Each critical asset is addressed by a Goal (G3) asserting its protection, with associated Strategies (S3) arguing based on the type of the asset, as per the PEDD classification.

This completes a security case ensuring that all core assets of the IM software are accounted for and protected.