Based on the security case pattern provided and the domain information for Instant Messaging (IM) software, the security case for IM software can be instantiated and displayed in the hierarchical tree format as follows:

```

G1: IM software is acceptably secure in the IM system

- C1: Definition and description of IM software

- C2: Definition and description of IM system

- C3: Definition of acceptably secure

- S1: Argument that IM software assets are under protection

-- J1: Protection of IM software assets supports that IM software is acceptably secure

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

--- C4: List of IM software critical assets

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

---- J2: Relationship between assets is clear and can be argued separately

---- G3.1: Registration information is protected

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

------ C5: List of software critical asset types in PEDD

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

------ G4.1: Registration information which belongs to Data Exchange is protected

---- G3.2: Registration process is protected

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

------ C5: List of software critical asset types in PEDD

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

------ G4.2: Registration process which belongs to Process is protected

---- G3.3: User account information is protected

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

------ C5: List of software critical asset types in PEDD

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

------ G4.3: User account information which belongs to Data Exchange is protected

---- G3.4: Authentication information is protected

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

------ C5: List of software critical asset types in PEDD

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

------ G4.4: Authentication information which belongs to Data Exchange is protected

---- G3.5: Login process is protected

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

------ C5: List of software critical asset types in PEDD

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

------ G4.5: Login process which belongs to Process is protected

---- G3.6: Chat logs are protected

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

------ C5: List of software critical asset types in PEDD

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

------ G4.6: Chat logs which belong to Data Storage are protected

```

In this instantiated security case for IM software:

- The hierarchical structure leverages the GSN elements (Goals, Strategies, Contexts, Justifications) defined in the pattern.

- Each placeholder `{}` has been replaced by specific information relevant to the IM software.

- The GSN structure is followed, with `SupportedBy` and `IncontextOf` relationships creating a clear tree structure.

The steps taken include:

1. Instantiation of each placeholder with specific details relevant to the IM software.

2. Maintenance of the hierarchical and relational structure of an assurance case.

3. Removal of decorators like `Uninstantiated`, `Placeholders`, etc., to create a final security case.