To create a security case for Instant Messaging (IM) software using the provided security case pattern, we first replace all placeholders with specific information relevant to the IM software. Below is the instantiated security case represented in a hierarchical tree structure:

```

G1: IM software is acceptably secure in the system

- S1: Argument that IM software assets are under protection

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

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

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

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

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

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

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

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

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

------ G4.1: Registration information, a Data Storage, is protected

------ G4.2: Registration process, a Process, is protected

------ G4.3: User account information, a Data Storage, is protected

------ G4.4: Authentication information, a Data Exchange, is protected

------ G4.5: Login process, a Process, is protected

------ G4.6: Chat logs, a Data Storage, is protected

- C1: Definition and description of IM software

- C2: Definition and description of the system

- C3: Definition of 'acceptably secure'

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

- C4: List of IM software critical assets: Registration information, Registration process, User account information, Authentication information, Login process, Chat logs

- C5: List of IM software critical asset types according to PEDD: Process, Environment Entity, Data Exchange, Data Storage

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

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

```

This structured hierarchy reflects how goals (G), strategies (S), contexts (C), and justifications (J) are interconnected to support the main claim that the IM software is acceptably secure in its operational environment. Each lower-level goal and strategy specifically addresses the protection of critical assets and their types, corresponding to the needs of securing the IM software comprehensively.