Based on the provided security case pattern predicates and the domain information about Instant Messaging (IM) software, I will instantiate the pattern to create a security case. Here is the fully instantiated security case represented in a hierarchical tree format:

```

G1: IM software is acceptably secure in the operational environment

- S1: Argument that IM software assets are under protection

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

- G2: All identified IM software critical assets are protected

- S2: Respective arguments of IM software critical assets

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

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

- 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 software critical asset belongs to

- C5: List of software critical asset types in PEDD includes Process, Environment Entity, Data Exchange, Data Storage

- J3: Types of software assets are according to PEDD

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

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

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

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

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

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

- C1: Definition and description of IM software includes features for information exchange, internal structure, and interactions with external components

- C2: Definition and description of the operational environment includes the software's interaction with user devices and internet connectivity

- C3: Definition of acceptably secure includes protecting confidentiality, integrity, and availability of all critical assets

```

This security case instantiation provides a structured argument that all critical assets in the IM software are sufficiently protected, addressing all identified risks and vulnerabilities related to these assets. Each goal and strategy layer maps directly to specific components or types of IM software assets based on their categorization in the PEDD (Process, Environment Entity, Data Exchange, Data Storage), with detailed context and justifications provided for clarity and completeness of the security claims.