Based on the provided security case pattern and domain information concerning Instant Messaging (IM) software, a detailed security case can be constructed as follows, filling placeholders with IM-specific data:

```

G1: IM software is acceptably secure in the IM system

- S1: Argument that software assets are under protection

- C1: Definition and description of IM software

- C2: Definition and description of the IM system

- C3: Definition of what is "acceptably secure"

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

- G2: All identified software critical assets are protected

- S2: Respective arguments of software critical assets

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

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

- G3: 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: Process, Environment Entity, Data Exchange, Data Storage

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

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

- G3: User account information is protected

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

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

- G3: Authentication information is protected

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

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

- G3: Login process is protected

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

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

- G3: Chat logs are protected

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

- G4: Chat logs, which belong to Data Storage, is protected

```

This security case represents a structured reasoning aligned from the top-level security goals of ensuring that IM software is "acceptably secure" within the IM system, down to the protection of each critical asset categorised according to the PEDD classification. This hierarchical structuring not only shows the relationship between elements but helps in detailed analysis and understanding of how each security aspect is addressed, adhering to the predicates defined in the GSN approach.