Here is the instantiated security case for Instant Messaging (IM) software using the given security case pattern. The hierarchical tree structure is represented using dashes (-) to denote different levels:

```

- Goal (G1, IM software is acceptably secure in the intended deployment system)

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

- Context (C2, Definition and description of intended deployment system)

- Context (C3, Definition of acceptably secure)

- Strategy (S1, Argument of that 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 of 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 Registration information 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 Registration process 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 User account information 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 Authentication information 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 Storage is protected)

- Goal (G3, Login process is protected)

- Strategy (S3, Argument of the type which the Login process 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 Chat logs belong 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 is protected)

```

In this hierarchical structure:

- The top-level goal (G1) states the main objective: that IM software is acceptably secure in its intended deployment system.

- Context elements (C1, C2, C3, C4, C5) provide definitions and descriptions necessary to understand the goals and strategies.

- Justification elements (J1, J2, J3) provide rationale behind the strategies and goals.

- Strategies (S1, S2, S3) describe the approach to providing evidence for each claim.

- Lower level goals (G2, G3, G4) break down the top-level claim into more specific claims about protecting individual critical assets of the IM software.

This structure ensures that all critical assets of the IM software, including registration information, registration process, user account information, authentication information, login process, and chat logs, are adequately protected, contributing to the overall security of the software.