To create a security case for Instant Messaging (IM) software based on the provided security case pattern, we will first remove all pattern-specific decorators and mulitplicities, and then replace placeholders with concrete information related to IM software. Below is the hierarchical tree format using dashes to denote different levels:

1. \*Goal (G1, IM software is acceptably secure in the operational environment)\*

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

- Context (C2, Definition and description of operational environment)

- Context (C3, Definition of acceptably secure)

- Strategy (S1, Argument that IM 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 IM software critical asset 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 type is protected)

- Goal (G3, Registration process is protected)

- Strategy (S3, Argument of the type which the IM software critical asset 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 type is protected)

- Goal (G3, User account information is protected)

- Strategy (S3, Argument of the type which the IM software critical asset 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 type is protected)

- Goal (G3, Authentication information is protected)

- Strategy (S3, Argument of the type which the IM software critical asset 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 type is protected)

- Goal (G3, Login process is protected)

- Strategy (S3, Argument of the type which the IM software critical asset 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 type is protected)

- Goal (G3, Chat logs are protected)

- Strategy (S3, Argument of the type which the IM software critical asset belongs 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 belongs to Data Storage type is protected)

This hierarchical structure represents a complete and instantiated security assurance case for the IM software based on the given predicate rules and domain-specific information.