Based on the security case pattern provided, here is the instantiation of the security case for Instant Messaging (IM) software using the domain information given. The placeholders are substituted with IM-specific details, and the hierarchical tree format is organized according to the predicates provided.

\*\*Instant Messaging (IM) Software Security Case Tree:\*\*

- G1: Instant Messaging software is acceptably secure in online communication systems

\* C1: Definition and description of Instant Messaging software

\* C2: Definition and description of online communication systems

\* C3: Definition of what it means to be "acceptably secure" in the context of Instant Messaging

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

\* - S1: Argument that IM software assets are under protection

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

\* C4: List of Instant Messaging software critical assets

\* - Registration information

\* - Registration process

\* - User account information

\* - Authentication information

\* - Login process

\* - Chat logs

\* J2: The relationship between IM software assets is clear and can be argued separately

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

\* - G3: Instant Messaging software critical asset is protected

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

\* C5: List of IM software critical asset types according to PEDD classification

\* J3: Types of IM software assets are classified according to PEDD

\* - G4: Instant Messaging software critical asset which belongs to Process is protected

\* - G4: Instant Messaging software critical asset which belongs to Environment Entity is protected

\* - G4: Instant Messaging software critical asset which belongs to Data Exchange is protected

\* - G4: Instant Messaging software critical asset which belongs to Data Storage is protected

This tree reflects how the assurance argument is built up from general to specific, starting with the overall security of the software and narrowing down to specific types of assets and their protection strategies according to the predefined classification. Each connection between the nodes shows the supporting strategy or justification, providing a structured rationale for the security assurance of IM software. This structured layout explicitly showcases how each asset and asset type’s security contributions form a comprehensive security case.