To create a security case for Instant Messaging (IM) software based on the given security case pattern, we'll instantiate the placeholders with specific context applicable to IM software.

Here’s the instantiated security case in a hierarchical structure (using dashes to denote the structural hierarchy as requested):

@Assurance\_case

- \*\*Goal (G1)\*\*: Instant Messaging software is acceptably secure in the communication system.

- \*\*Context (C1)\*\*: Instant Messaging software allows real-time text transmission over internet.

- \*\*Context (C2)\*\*: A communication system consisting of servers and clients using the Instant Messaging software.

- \*\*Context (C3)\*\*: "Acceptably secure" means meeting all specified privacy, integrity, and availability requirements.

- \*\*Supported by (S1)\*\*: Argument that software assets are under protection.

- \*\*Justification (J1)\*\*: Protection of software assets supports that IM software is acceptably secure.

- \*\*Goal (G2)\*\*: All identified Instant Messaging software critical assets are protected.

- \*\*Context (C4)\*\*: List of IM software critical assets could include user data, chat logs, server database, and authentication mechanisms.

- \*\*Supported by (S2)\*\*: Respective arguments of software critical assets.

- \*\*Justification (J2)\*\*: Clear relationship between assets ensures that they can be argued about separately and effectively.

- \*\*Goal (G3)\*\*: Instant Messaging software critical asset is protected.

- \*\*Supported by (S3)\*\*: Argument of the type which the software critical asset belongs to.

- \*\*Context (C5)\*\*: List of software critical asset types in Practical Encryption and Data Security (PEDD) includes databases, user authentication data, and communication logs.

- \*\*Justification (J3)\*\*: Types of IM software assets conform to categories as per PEDD - ensuring specific protection measures are applicable.

- \*\*Goal (G4)\*\*: Instant Messaging software critical asset, which belongs to a specified type (user authentication data), is protected.

- \*\*Has Multiplicity\*\* (S2 to G4, "1:4"): Each critical asset type must satisfy this goal under S3, assuming 4 types identified.

@End\_Assurance\_case

This hierarchical structure embeds deeper context and reasoning with each level, justifying why certain strategies, contexts, and goals are relevant to ensure the overall security of the Instant Messaging software.