Here's how the assurance case for an Instant Messaging (IM) software can be instantiated from the given security case pattern. The placeholders are filled based on the specific context of the IM software:

@Assurance\_case

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

- \*\*C1: Instant Messaging software enables real-time text transmission over the Internet\*\*

- \*\*C2: Online communication systems refer to platforms that allow instant voice, video, and text communication\*\*

- \*\*C3: Acceptably secure implies protection against common cybersecurity threats such as data breaches, unauthorized access, and denial of service attacks\*\*

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

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

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

- \*\*S2: Respective arguments of each IM software critical asset\*\*

- \*\*C4: List of IM software critical assets includes user data, communication encryption, and server infrastructure\*\*

- \*\*J2: The relationship between assets is clear and each can be argued separately based on their impact and protection mechanisms\*\*

- \*\*G3: IM software critical asset is protected\*\*

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

- \*\*C5: List of types of IM software critical assets in Protection, Detection, and Deterrence (PEDD)\*\*

- \*\*J3: Types of software assets adhere to industry standards in PEDD, ensuring comprehensive cybersecurity measures\*\*

- - \*\*G4: User data, a software critical asset which belongs to data type, is protected\*\*

- - \*\*G4: Communication encryption, a software critical asset which belongs to network type, is protected\*\*

- - \*\*G4: Server infrastructure, a software critical asset which belongs to hardware type, is protected\*\*

- - \*\*G4: Application codebase, a software critical asset which belongs to software type, is protected\*\*

@End\_Assurance\_case

This assurance case is structured hierarchically, starting with a general security claim for the IM software (G1), followed by strategies and goals that progressively focus on specific aspects of asset protection. Each critical asset type has its own goal (G4) under the respective strategies, justifying how each asset type contributes to the overall security of the IM system. Each context and justification further supports the claim logically, ensuring clarity and completeness in addressing the security needs of Instant Messaging software.