To instantiate the given security case pattern for an Instant Messaging (IM) software and creating a security case, we will replace the placeholders with specific information relevant to the IM software. Below is the instantiation and representation in a hierarchical tree format:

@Assurance\_case

- G1: Instant Messaging (IM) software is acceptably secure in IM system.

- C1: Instant Messaging (IM) software including all its modules and functional interfaces.

- C2: IM system environment including server and client applications.

- C3: 'Acceptably secure' defined as meeting specific security standards (e.g., SSL/TLS for transmission, encrypted storage).

- S1: Argument that IM software assets are under protection.

- J1: Protection of IM software assets supports that IM software is acceptably secure.

- G2: All identified IM software critical assets are protected.

- C4: List of IM software critical assets includes user authentication credentials, message history, user contacts.

- S2: Respective arguments of IM software critical assets.

- J2: Relationship between assets is clear and can be argued separately.

- G3: Each IM software critical asset is protected.

- S3: Argument for each type of asset which the IM software critical asset belongs to.

- C5: Types of IM software assets include user data, configuration settings.

- J3: Types of IM software assets are defined as per Protection, Encryption, Data Integrity, and Denial of Service.

- G4 (x4 instances for each type of asset): Each type of IM software critical asset is protected.

@End\_Assurance\_case

Explanation:

- \*\*G1 - G4\*\*: Represent specific goals about the security assurance of the IM software.

- \*\*S1 - S3\*\*: Are strategies explaining how the goals are supported.

- \*\*C1 - C5\*\*: Contexts provide definitions and lists that provide detailed context relevant to the IM software.

- \*\*J1 - J3\*\*: Justifications support the strategies and ensure that there's reasoning behind the protection measures for the IM software.

- \*\*Multiplicity at S2 - G4\*\*: Indicates that for each type of asset (as identified and justified), there are protection strategies and goals in place.

- \*\*Depth levels\*\*, denoted by dashes, indicate how each element is nested and supported within the assurance case structure. Each lower level supports the level above it.

This security case structure ensures that for each critical asset of the IM software, there is an explicit argument and evidence supporting its security, thereby confirming that the software operates in its intended environment securely.