To instantiate an assurance case for Instant Messaging (IM) software based on the security case pattern described, we will provide specific instances and contextual information applicable to IM software. Below, the hierarchy of the instantiated assurance case is presented in a tree structure format:

```

@Assurance\_case

- G1: Instant Messaging (IM) software is acceptably secure in user communication systems.

- C1: IM software includes user-to-user messaging, file transfers, and voice/video communication.

- C2: User communication systems include desktop and mobile platforms across various Operating Systems.

- C3: Acceptably secure means ensuring confidentiality, integrity, and availability of communication.

- J1: Protecting IM software critical assets ensures the security of user communications.

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

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

- C4: IM software critical assets include user data, authentication information, and network configuration.

- J2: Each asset type like authentication information and network configurations has distinct protection mechanisms which are clearly defined, making the execution of the protective measures on these assets justifiable.

- S2: Respective arguments of IM software critical assets

- G3: User data as a critical asset of IM software is protected.

- S3: Argument of the type which the user data belongs to

- C5: List of IM software critical asset types include personal user information, chat logs, media files shared over IM, and cryptographic keys for encryption.

- J3: The types of user data assets are managed and protected according to Personal Data Protection Directives (PEDD).

- G4: User data, which is a type of personal information, is protected.

- (An assumption could be made that there are further sub-types within user data such as personal identification data and conversation history, each treated distinctly in separate claims or goals which are currently undeveloped)

@End\_Assurance\_case

```

This tree represents the hierarchical structure of the assurance case derived for the Instant Messaging software, described at various levels of detail, each supporting the higher level goal or strategy:

1. \*\*Level 1:\*\* Begins with the primary goal (G1) highlighted with its context (C1, C2, C3) and justification (J1) linked.

2. \*\*Level 2:\*\* Outlines the strategy (S1) supporting the main goal.

3. \*\*Level 3:\*\* Discusses the protected status of all critical assets (G2) with its contexts and justifications.

4. \*\*Level 4:\*\* Looks into detailed arguments for separate critical assets grouped under (S2).

5. \*\*Level 5 and 6:\*\* Explores further the protection of specific types of assets like user data and the respective categories or types these assets belong to, supported by detailed context and justification.

This structured approach helps to clearly address, argue, and justify how different elements of the IM software uphold security measures effectively.