To instantiate the security case pattern for Instant Messaging (IM) software, placeholders `{}` should be replaced with specific details regarding the IM software, and ensure that all elements are considered at an appropriate level of detail. Below is the instantiation as a hierarchical tree structure using G1, G2, and so forth to denote goals, S1, S2 for strategies, C1 through C5 for contexts, J1 through J3 for justifications, and depth levels denoted with dashes ("-"):

```

G1: IM software is acceptably secure in communication systems

- C1: IM software enables secure text, voice, and video communications

- C2: Communication systems including private and business networks

- C3: Acceptably secure means meeting all industry-standard encryption and privacy protocols

- S1: Argument that IM software assets are under protection

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

- G2: All identified IM software critical assets are protected

- C4: List of IM software critical assets (e.g., message stores, user data, transfer protocols)

- S2: Respective arguments for IM software critical assets

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

- G3: Specific IM software critical asset is protected

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

- C5: List of IM software asset types (e.g., stored data, in-transit data)

- J3: Types of IM software assets are according to Protection of Electronic Data Directive (PEDD)

- G4: Type A (e.g., in-transit data) IM software critical asset is protected

- G4: Type B (e.g., stored data on servers) IM software critical asset is protected

- G4: Type C (e.g., user credentials) IM software critical asset is protected

- G4: Type D (e.g., configuration data) IM software critical asset is protected

```

Each instance of `G4` corresponds to a different type as specified, each of which has been articulated to align with the placeholder's specific use cases and security concerns found within Instant Messaging software systems. This hierarchical structure helps form a detailed, clear argument about various security aspects of IM software in communication systems, emphasizing context, strategies, and evidence at each level.

By substituting specific information into the placeholders and delineating the logical connections and support between the elements, we have encapsulated a comprehensive security case argument for the IM software. This illustrates how the original assurance case pattern has been adapted to fit real-world application scenarios.