To create a security case for Instant Messaging (IM) software, we need to instantiate the given security case pattern by replacing placeholders with concrete or system-specific information. After instantiation, we will remove the pattern decorators.

Let's assume the list of software critical assets for the IM software includes:

1. User Data Protection

2. Message Encryption

3. Contact List Privacy

4. Backend Server Security

Here's the instantiated security case:

### Instantiated Security Case for Instant Messaging (IM) Software

```

G1: Instant Messaging (IM) software is acceptably secure in the communication system

- C1: Definition and description of Instant Messaging (IM) software

- C2: Definition and description of the communication system

- C3: Definition of acceptably secure

- 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

- S2: Respective arguments of IM software critical assets

- C4: List of IM software critical assets

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

- G3: User Data Protection is protected

- S3: Argument of the type which User Data Protection belongs to

- C5: List of IM software critical asset types in PEDD

- J3: Types of IM software assets are according to PEDD

- G4: User Data Protection which belongs to User Information type is protected

- G3: Message Encryption is protected

- S3: Argument of the type which Message Encryption belongs to

- C5: List of IM software critical asset types in PEDD

- J3: Types of IM software assets are according to PEDD

- G4: Message Encryption which belongs to Communication type is protected

- G3: Contact List Privacy is protected

- S3: Argument of the type which Contact List Privacy belongs to

- C5: List of IM software critical asset types in PEDD

- J3: Types of IM software assets are according to PEDD

- G4: Contact List Privacy which belongs to User Information type is protected

- G3: Backend Server Security is protected

- S3: Argument of the type which Backend Server Security belongs to

- C5: List of IM software critical asset types in PEDD

- J3: Types of IM software assets are according to PEDD

- G4: Backend Server Security which belongs to Server type is protected

```

In this hierarchical format, we can see the security case for the Instant Messaging software, with instantiations replacing the placeholders and corresponding relations clearly articulated.