Based on your request, here is how the security case for Instant Messaging (IM) software would be structured using the provided pattern:

```

@Assurance\_case

- G1: IM software is acceptably secure in the system

- C1: Description of IM software - A software platform used for direct text, voice, and video communications between users.

- C2: Definition of the system - The entire digital architecture and networks where IM software operates including servers, user devices, and internet connectivity.

- C3: Definition of acceptably secure - Meeting all operational security standards, ensuring data confidentiality, integrity, and availability.

- S1: Argument that IM software assets are under protection

- J1: Protection of 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 – Registration information, Registration process, User account information, Authentication information, Login process, Chat logs.

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

- S2: Respective arguments for IM software critical assets

- G3: Registration information is protected

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

- C5: List of software critical asset types in PEDD - Process, Environment Entity, Data Exchange, Data Storage.

- J3: Types of software assets are according to PEDD

- G4: Registration information which belongs to Data Storage is protected

- G3: Registration process is protected

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

- G4: Registration process which belongs to Process is protected

- G3: User account information is protected

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

- G4: User account information which belongs to Data Storage is protected

- G3: Authentication information is protected

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

- G4: Authentication information which belongs to Data Exchange is protected

- G3: Login process is protected

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

- G4: Login process which belongs to Process is protected

- G3: Chat logs are protected

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

- G4: Chat logs which belong to Data Storage is protected

@End\_Assurance\_case

```

This hierarchical representation directly utilizes the predicates and structure from your security case pattern, applying the specific information relevant to IM software. Each goal (G1 to G4) and strategy (S1 to S3) is nested appropriately to reflect the hierarchy and nature of the argument to be supported. Context (C1 to C5) provides detailed information about each layer, while justifications (J1 to J3) serve as rationale checks ensuring coherence in the security argumentation structure.