Based on the defined predicates and provided elements, the instantiated security case for Instant Messaging (IM) software is depicted below in a hierarchical tree format. For clarity, placeholders are instantiated with appropriate examples and values specific to IM software.

```

- Goal (G1, Instant Messaging (IM) software is acceptably secure in communication systems)

- Context (C1, IM software includes applications capable of instant voice and message exchange)

- Context (C2, Communication systems include network infrastructure and software platforms supporting IM)

- Context (C3, Acceptably secure refers to the protection against unauthorized access and data integrity)

- Strategy (S1, Argument that IM software assets are under protection)

- Justification (J1, Protection of software assets supports that the software is acceptably secure)

- Goal (G2, All identified IM software critical assets are protected)

- Context (C4, List of IM software critical assets includes user data, communication logs, server access protocols)

- Strategy (S2, Respective arguments of IM software critical assets)

- Justification (J2, Relationship between assets is clear and can be argued separately)

- Goal (G3, IM software critical asset is protected)

- Strategy (S3, Argument of the type that the IM software critical asset belongs to)

- Context (C5, List of software critical asset types includes user authentication, encrypted data storage, secure communication channels)

- Justification (J3, Types of software assets are arranged according to PEDD - Privacy, Encryption, Data integrity, Denial of service protection)

- Goal (G4, IM software critical asset which belongs to encryption is protected)

- (Further instances of G4 for other types, such as privacy, data integrity, and denial of service protection, based on HasMultiplicity relation with specification of handling 4 types)

```

This hierarchy details how the protection strategy for critical IM software assets is constructed and supported by multiple levels of goals, strategies, and contexts, addressing each type of software critical asset with respective protections. Each node reflects the applied predicate rules and instantiated placeholders.