Creating an assurance case for instant messaging (IM) software involves identifying the main goal, establishing strategies to achieve that goal, supporting sub-goals, and providing evidence for claims made. Below is a simplified hierarchical tree format for this security case using GSN:

\*\*1. Top Goal\*\*

- \*\*G1: IM software is secure for use.\*\*

\*\*2. Strategies to achieve the top goal\*\*

- \*\*S1: Identify and mitigate security threats.\*\*

- \*\*G2: Threats to data confidentiality are mitigated.\*\*

- \*\*G3: Threats to data integrity are mitigated.\*\*

- \*\*G4: Threats to data availability are mitigated.\*\*

- \*\*S2: Ensure secure user authentication and access control.\*\*

- \*\*G5: User authentication is secure.\*\*

- \*\*G6: Access control mechanisms are robust.\*\*

- \*\*S3: Implement monitoring and response procedures.\*\*

- \*\*G7: Monitoring for security breaches is in place.\*\*

- \*\*G8: Incident response plans are established.\*\*

\*\*3. Sub-goals and evidence for each strategy\*\*

- \*\*G2: Threats to data confidentiality are mitigated.\*\*

- \*\*S2.1: Use encryption for data at rest and in transit.\*\*

- \*\*G2.1: Data at rest is encrypted.\*\*

- \*\*E2.1: Evidence of using AES-256 encryption for stored data.\*\*

- \*\*G2.2: Data in transit is encrypted.\*\*

- \*\*E2.2: Evidence of using TLS for transmitting data.\*\*

- \*\*G3: Threats to data integrity are mitigated.\*\*

- \*\*S3.1: Implement checksums and hashes.\*\*

- \*\*G3.1: Integrity of messages is verified.\*\*

- \*\*E3.1: Proof of SHA-256 hash implementation on messages.\*\*

- \*\*G4: Threats to data availability are mitigated.\*\*

- \*\*S4.1: Ensure redundancy and reliable hosting.\*\*

- \*\*G4.1: IM service is hosted on highly available infrastructure.\*\*

- \*\*E4.1: Details of using cloud services with 99.9% uptime SLA.\*\*

- \*\*G5: User authentication is secure.\*\*

- \*\*S5.1: Implement multi-factor authentication (MFA).\*\*

- \*\*G5.1: Users are authenticated using MFA.\*\*

- \*\*E5.1: Documentation of MFA workflows and implementation.\*\*

- \*\*G6: Access control mechanisms are robust.\*\*

- \*\*S6.1: Role-based access control (RBAC) is in place.\*\*

- \*\*G6.1: Access permissions are managed based on user roles.\*\*

- \*\*E6.1: Role definitions and access rights documentation.\*\*

- \*\*G7: Monitoring for security breaches is in place.\*\*

- \*\*S7.1: Use real-time monitoring tools.\*\*

- \*\*G7.1: Real-time monitoring tools are deployed.\*\*

- \*\*E7.1: Logs and reports from monitoring tools demonstrating their activity.\*\*

- \*\*G8: Incident response plans are established.\*\*

- \*\*S8.1: Develop and test response plans.\*\*

- \*\*G8.1: Incident response plans are documented and regularly tested.\*\*

- \*\*E8.1: Test results and documentation of incident response drills.\*\*

This hierarchical tree outlines the main goals for ensuring the security of IM software and breaks down the strategies and sub-goals, along with the required evidence for each step.