To create a security case for ACAS Xu based on the provided security case pattern and the domain information, instantiate the placeholders, develop undeveloped components, and remove uninstantiated decorators while integrating details specific to ACAS Xu. Here’s how these elements can be organized in a hierarchical tree format:

```

Goal (G0, "ACAS Xu satisfies security requirements")

Strategy (S0, "Argue through asset protection and secure development requirements")

Goal (G1, "ACAS Xu satisfies the asset protection requirements")

Strategy (S1, "Argue through the different stages of the system development life cycle")

Goal (G3, "Asset protection requirements are met during the architecture design phase")

Strategy (S2, "Argue through deriving security threats from security requirements")

Goal (G5, "ACAS Xu architecture is protected against identified security threats")

Strategy (S3, "Argue over each security threat")

Goal (G0.1, "ACAS Xu architecture is protected against tampering (ST1)")

Goal (G0.2, "ACAS Xu architecture is protected against spoofing (ST2)")

Goal (G0.3, "ACAS Xu architecture is protected against elevation of privileges (ST3)")

Goal (G6, "ACAS Xu architecture is validated")

Goal (G4, "Asset protection requirements are met during other phases") (undeveloped)

Goal (G2, "ACAS Xu satisfies secure development requirements") (uninstantiated and undeveloped)

Context (C0, "Description of ACAS Xu")

Context (C1, "Security requirements are about protecting the system from malicious entities")

Context (C2, "Description of the ACAS Xu architecture")

Justification (J0, "The argumentation is based on satisfaction of security requirements")

Justification (J1, "Detection and mitigation of threats fulfill security requirements")

Assumption (A0, "System security requirements specifications are complete, adequate, and consistent")

Assumption (A1, "Asset inventory is established")

Assumption (A2, "All relevant threats have been identified")

Assumption (A3, "ACAS Xu architecture model is well defined") (uninstantiated)

```

Explanation of the instantiated security case structure:

- \*\*G0\*\* describes the high-level goal, focusing on fulfilling ACAS Xu security requirements.

- \*\*S0\*\* provides a broad strategy by dividing the argument into asset protection and secure development.

- \*\*G1 and G2\*\* reflect sub-goals focused separately on asset protection and secure development.

- \*\*S1\*\* interprets the lifecycle stages for asset protection; \*\*G3 and G4\*\* specify these aimed at design and other phases.

- \*\*S2 and S3\*\* dive deeper into arguments based on specific security threats from which strategies are developed for individual threats (e.g., tampering, spoofing, and privilege escalation).

- Various context, justification, and assumption elements provide necessary definitions and rationalizations behind the structure and strategies used.

This assurance case will further expand as detailed information becomes available for each component and the interactions are appropriately reasoned about and evidenced.