Based on the provided security case pattern, we can now create a security case for ACAS Xu by following the steps outlined in the context.

First, we will replace the placeholders with the appropriate information specific to ACAS Xu. Then, we will remove all additional assurance case pattern decorators and ensure we have a hierarchical tree structure.

Below is the hierarchical tree representation for the security case of ACAS Xu:

```

- G0: ACAS Xu satisfies security requirements

- C0: Description of ACAS Xu

- C1: SR are requirements about protecting the system from malicious entities

- J0: The argumentation is based on satisfaction of SRs

- A0: System SRS are complete, adequate, and consistent

- S0: Argue through asset protection and secure development requirements

- G1: ACAS Xu satisfies the asset protection requirements

- A1: Asset inventory is established

- S1: Argue through the different stages of the system development life cycle

- G3: Asset protection requirements are met during the architecture design phase

- C2: Description of the ACAS Xu architecture

- S2: Argue through derivating security threats from SRs

- G5: ACAS Xu architecture is protected against identified security threats (STs)

- A2: All relevant threats have been identified

- S3: Argue over each security threat

- G0.1: ACAS Xu architecture is protected against ST1 (Tampering)

- G0.2: ACAS Xu architecture is protected against ST2 (Spoofing)

- G0.3: ACAS Xu architecture is protected against ST3 (Elevation of Privileges)

- G6: ACAS Xu architecture is validated

- C3: Description of ACAS Xu architecture model

- A3: ACAS Xu architecture model is well defined in {formal method}

- G4: Asset protection requirements are met during other phases (undeveloped)

- G2: ACAS Xu satisfies secure development requirements (undeveloped)

```

In this structure:

- We've instantiated the placeholders with information relevant to ACAS Xu.

- We've removed additional assurance case pattern decorators.

- We've created an instance of the goal for each identified threat (G0.1, G0.2, and G0.3) based on the security threats (ST1, ST2, and ST3).

- Assumptions, contexts, justifications, and strategies are properly positioned to support their respective goals.