Using the provided security case pattern, here is a hierarchical tree representation of the derived security case for 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

- 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 (undeveloped)

- C3: Description of ACAS Xu architecture model

- A3: ACAS Xu architecture model is well defined in formal methods

- J1: Detection and mitigation of threats fulfill SRs

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

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

```

This tree structure utilizes indentations to show the hierarchical relationship between goals (G), strategies (S), contexts (C), justifications (J), and assumptions (A). Each element has been instantiated with specific details relevant to the ACAS Xu system. Elements that are marked as undeveloped (G4, G6, G0.X) or uninstantiated (G2) in the original pattern are noted accordingly.