Automated Assurance of Security Policy Enforcement

As safety-critical system have become more connected, “closed” system assumptions are no longer valid and security threats affect safe system operation.

Virtual system integration and analysis of embedded software systems has been embraced by the safety-critical system community to address exponential growth in system development cost due to increased interaction complexity and mismatched assumptions in embedded software systems.

In this project, we demonstrate how the virtual system integration approach can be extended to address security concerns at the architectural level to complement code level security analysis.

Our focus is on security policy specification and its enforcement.

We utilize the SAE International Architecture Analysis & Design Language (AADL) industry standard to model and analyze embedded software systems. It includes an annex for fault modeling and analysis.

We analyze security policy specifications for consistency and gaps in flow constraints and isolation requirements.

We analyze the software system architecture for potential enforcement vulnerabilities due to incorrect deployment of security mechanisms.

Security Challenges as Safety-critical Systems Become Connected

Integrated Modular Avionics (ARINC653) Common Networked Processing Platform

Security Attacks on External Channels and System Internal Vulnerabilities

Automated Assurance through Continuous Analysis of Potential Architecture Level Security Policy and Enforcement Vulnerabilities

We leverage the Architecture-Led Incremental System Assurance (ALISA) capability in the Open Source AADL Tool Environment (OSATE).

Executable verification plans identify how potential architecture level security vulnerabilities are addressed through model-based analysis.

Security Challenges as Safety-critical Systems Become Connected

Automated Assurance of Security Policy Enforcement

As safety-critical system have become more connected, “closed” system assumptions are no longer valid and security threats affect safe system operation.

Virtual system integration and analysis of embedded software systems has been embraced by the safety-critical system community to address exponential growth in system development cost due to increased interaction complexity and mismatched assumptions in embedded software systems.

In this project, we demonstrate how the virtual system integration approach can be extended to address security concerns at the architectural level to complement code level security analysis.

Our focus is on security policy specification and its enforcement.

We utilize the SAE International Architecture Analysis & Design Language (AADL) industry standard to model and analyze embedded software systems. It includes an annex for fault modeling and analysis.

We analyze security policy specifications for consistency and gaps in flow constraints and isolation requirements.

We analyze the software system architecture for potential enforcement vulnerabilities due to incorrect deployment of security mechanisms.

Automated Assurance through Continuous Analysis of Potential Architecture Level Security Policy and Enforcement Vulnerabilities

We leverage the Architecture-Led Incremental System Assurance (ALISA) capability in the Open Source AADL Tool Environment (OSATE).

Executable verification plans identify how potential architecture level security vulnerabilities are addressed through model-based analysis.

Carnegie Mellon University Software Engineering Institute

Peter Feiler | phf@sei.cmu.edu