Experimental Platform for Systems-Security Codesign

TRUST Project

Matt Eby, Janos Mathe, Jan Werner, Chip Clifton

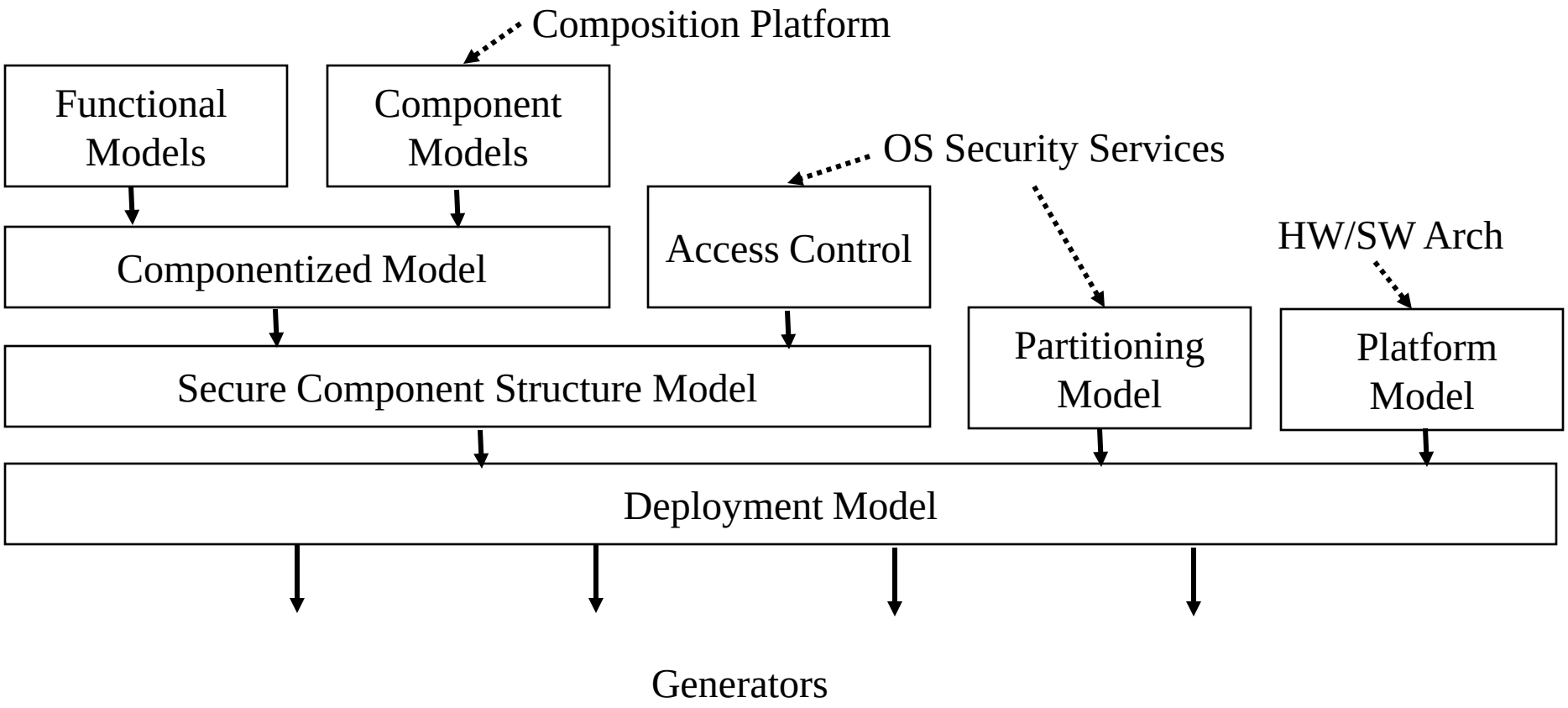
Outline

- Background and Motivation
- Description of Security Testbed
- Current Status of AADL in GME
- Demo

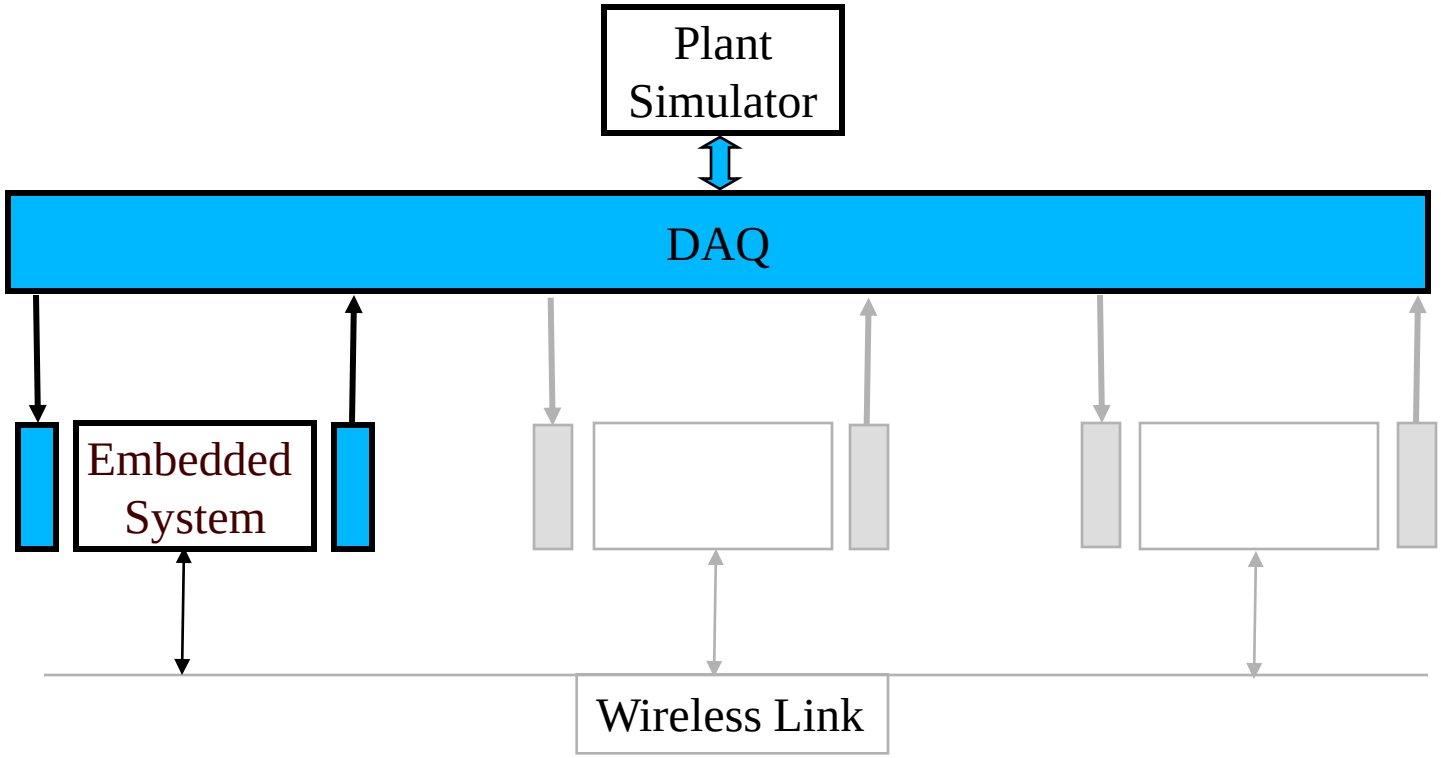
Background and Motivation

- Team for Research in Ubiquitous Secure Technology (TRUST)
  - NSF cybersecurity Science and Technology Center
- What are the semantics of secure systems?
- How are security policies on the model level enforced?

Overview: Codesign Models



Overview: System Architecture



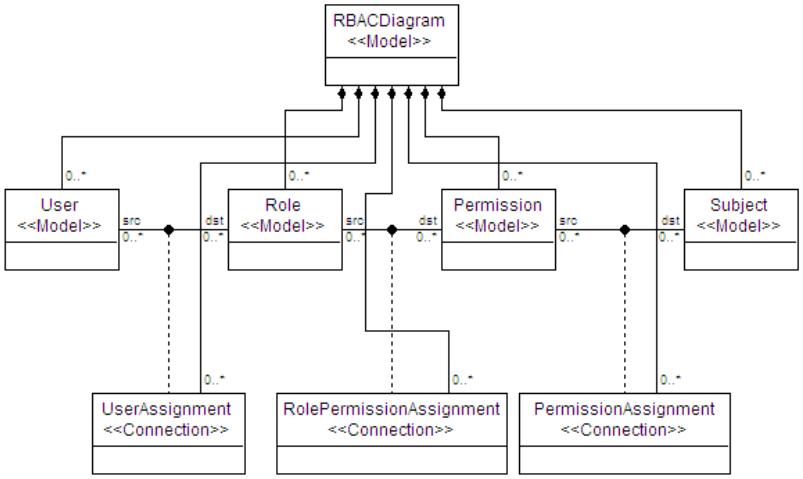
Security Testbed Platform

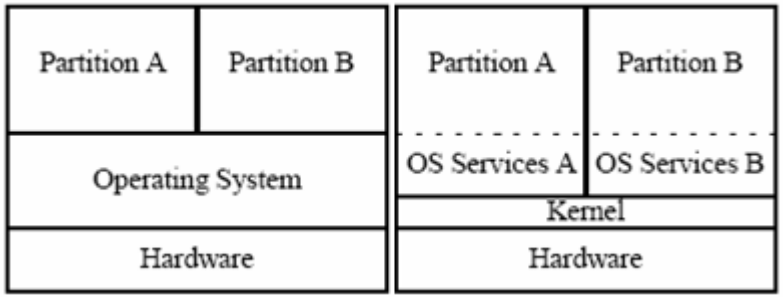
- Single board computer SBC4495 from Micro/Sys
  - Cyrix Intel 486 compatible processor
  - Analog and Digital IO
  - Wired or Wireless Sensor Network

- Linux Security Mechanisms
  - Gentoo 2005.1 with 2.4.32 kernel
  - Grsecurity enhanced kernel
  - Kernel working in privileged mode (ring0)
  - Userspace programs working in unprivileged mode (ring3)
  - User identifiers UID
  - Group identifiers GID
  - chroot()

Security enhancements for AADL

- Component level access control – Role Based Access Control
- Partitioning – embedding components in separate domains





Current Status of AADL MetaModel

- AADL concepts currently in GME
  - Software Components
    - Data, Subprograms, Threads, Thread Groups, Processes
  - Execution Platform Components
    - Processors, Memory, Buses, Devices
- Future Work
  - Modes, Properties, End-To-End Flows, Port Groups

Current Tool Status

- Textual AADL Generator
  - Weather Predictor Example (Pages 58-60 in AADL Standard Document)
- C Code Generator
  - DC Motor Controller
  - Future Work: Quad Rotor UAV Control System

Questions ?

- Security is a growing concern in embedded systems
- Security needs to be provisioned in system design models
- Model-driven approach has potential in addressing security concerns