Problem: Cybersecurity of cyber physical systems & internet of things is vital. Security is a continuous process that runs throughout and at times even beyond the life-cycle of a system. Traditional methods of security modeling miss this life-cycle-based dynamicity.

Contribution: We propose an open-source framework based on Pimca, a domain specific systems modeling language highlighting the attack surface[1] during cyber threat analysis[2].

Requirements

- Systems modeling with the intent of highlighting the attack surface
- Security concerns modeling using a graphical language, geared towards automation
- Analysis-agnostic attack surface modeling

Water pump

Pimca language

- Expressive relations modeling complex interactions between components enable deeper security analysis and attack surface reasoning. Well-defined components also expose particular interactions and weaknesses in the attack surface.
- Coarse-grain security-focused systems modeling abstracts away internal architectural details and handles heterogeneous systems with ease.

Attack surface inference

1. How to reach the target?
   Target: Water tank
   Deducing sub-objectives using relations
   - We can infer intermediary targets: Inflow valve, manual valve, pump

2. What are the targets available?
   Capabilities: Social engineering, network access
   Deducing reach based on attacker capabilities
   - The attack surface extends to: Command (through network), manual operator (through social engineering)

Conclusion: Our framework satisfies the intention of highlighting the attack surfaces in a system model. Preliminary validation is done on use cases, which emphasized the system modeling along with the attack surface deduction and refinement enabled by our framework.

Future Works: We intend to model the systems dynamic behavior using a component-by-component basis. We also plan to model an executable attacker so that we can simulate the system-under-attack behavior.