Architecture-based Self-securing Systems

Prof. David Garlan, Carnegie Mellon University

http://www.cs.cmu.edu/~able/research/sos/

Providing assurable run-time security enforcement and repair.

The objective of this project is to provide the scientific foundations for self-security based on using architecture models to reason about system observations and plan runtime adaptations.

We seek to provide scientific principles analogous with those that exist for physical control systems:

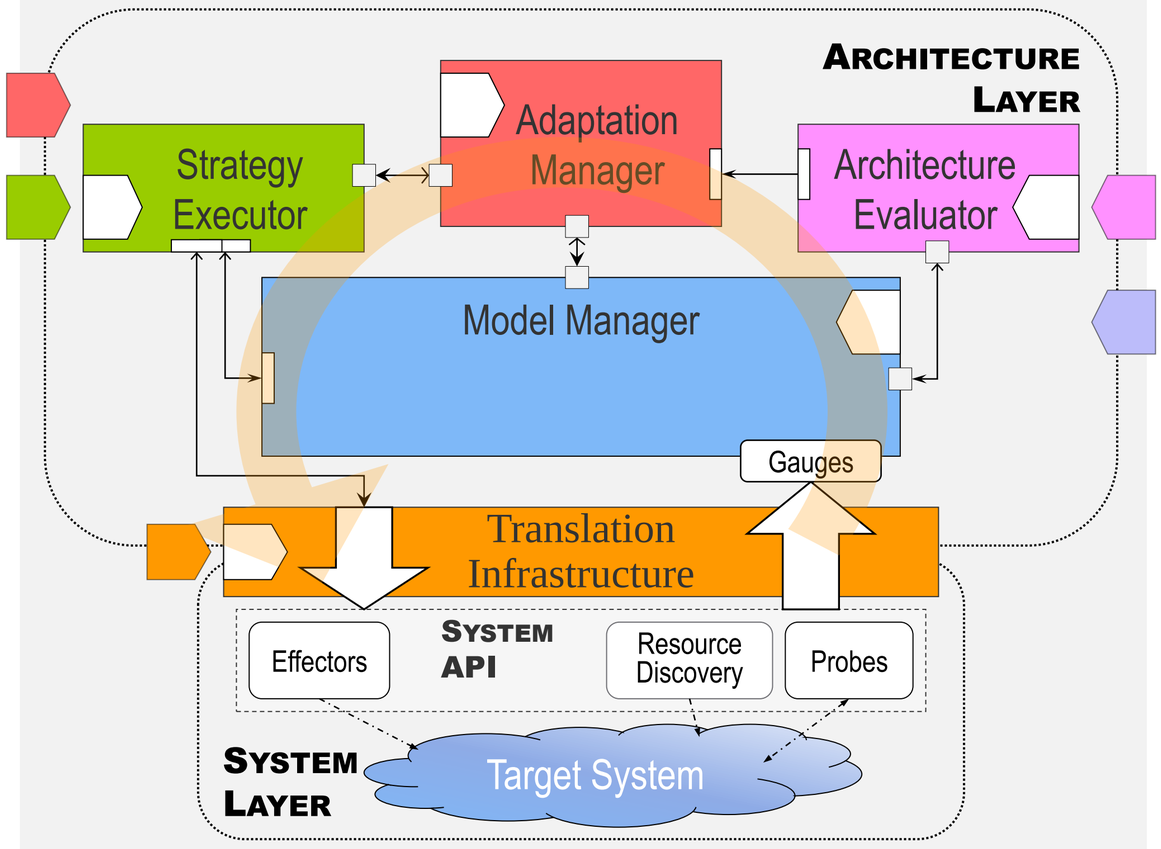
New Theories for rational choice of repair to maximize utility

New Analyses to assure properties of repair strategies

New Principles to reason about observational completeness

New Reasoning about security diagnosis in the presence of security

Rainbow Self-Adaptive Infrastructure



Approach

Use **architecture models** of the system as the basis for reasoning about security properties

- Architecture models are a suitable abstraction to reason about multiple system quality attributes
- Observations of the running system can be analyzed architecturally to decide the appropriate adaptation action in a given context

Security requires new approaches in:

Monitoring: Reasoning about sufficiency, dynamic retargeting and focusing

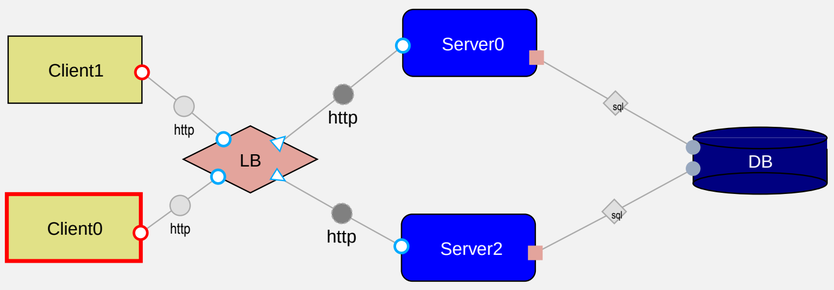
Detection and Localization: Detecting and learning root causes, abstracting observations

Repair Handling: Encoding security repairs so they are analyzable, improve through learning, planning.

Actuation: System hooks for security problems, soundness of actuation

Progress (since project start of 4/2012)

- Rainbow testbed hosted on ProtoGENI EmuLab virtual network platform-as-service
- Proof-of-concept Denial of Service case study



  - Blacklisting malicious clients, issuing challenges, re-authentication

- Initial fault diagnosis and localization for security
  - Spectrum-based techniques applied at run-time to detect attacks and vulnerabilities
- Creating taxonomy of security repair tactics (with Prof. Malek at GMU)
  - Know what to apply when and what the consequences are
- Linking static analysis and dynamic repair (with Prof. Aldrich at CMU)
  - To ensure that properties that cannot be checked statically can be mitigated dynamically

2012 Science of Security Community Meeting
Nov. 29-30, 2012
National Harbor, MD
http://cps-vo.org/group/sosmtg

Vote Here

institute for SOFTWARE RESEARCH
Carnegie Mellon University