
NSL Presentation 2.20.03

Michael E. Locasto
<locasto@cs.columbia.edu>
Overview

- Our goal lies at the intersection of 3 areas of CS:
  - process migration as a vehicle for
  - survivability of
  - embedded systems

- Solution: postulate AC+common VM+policy
The Problem: Survivability & Fault Tolerance

- The wrinkle: embedded systems & survivable networks of them
  - What are SESs?
  - Why are we talking about them?
  - Is it practical?
  - How do we manage policy?
Functional Survivability in a Network

- Fault tolerance through:
  - replication & redundancy (old approach)
  - heterogeneity (embedded systems have plenty of this)
  - remote execution (no go {RMI,CORBA})
- “essential computation”
- bmwfilms.com
Heterogeneity: Friend & Foe

- More robust, but more diverse
  - problems with state (see later)
- Deploy a Common VM
  - does the VM become a SPF? (Zhang, et al)
- Java ({j/k}vm) vs Linux
The Protocol

- Boss scenario (AC)
- straightforward checkpoint & restart
- (re)registration
- protocol phases & messages
Protocol Sketch

PCXSES Protocol Steps and Phases

Client Device

----- GOOD MORNING {mode} ------>>
<<<< GOOD MORNING {params} ------

----- HELLO | STATE ------>>

<<<< MORPH {^,#b/obj,#obj} ------
<<<< obj def #1 ------
<<<< obj def #2 ------
... 
<<<< obj def #n ------

----- MORPH {ack} ------>>

-------- GOODBYE  --------
<<<<------- GOODBYE -------

Area Controller
Dealing with State

- target may not understand state
- essential state may be hidden by the OS
- key observation: informal “update API”
  - SUI agent:
  - STUDML: state transfer and update meta-language
Dealing with Policy

- describe a language with a machine
- principals, groups, objects, actions, commands, rules
- SQL-like, wrapped in a Java blanket
- syntax examples later
- http://w.c.c.e/~locasto/projects/spcl/docs
- can replace old e.c. with completely different code
Results

- PACMAN (demo)
- protocol, client library, ac

Interesting Questions
  - transparency
  - failure chaining
  - proving failure detection
  - specialization to hardware target (no VM)
Discussion & Questions

- Can we utilize ZAP?
- How can we standardize on a generic policy language?
- How can we make PCXSES transparent?