INNERVENT, INC.

Bakshi

Router
Configuration
Wizard

Mike Perez

COME AND MAKE IT

San Antonio Hackerspace

Bakshi

Router
Configuration
Wizard

Agenda

- Vulnerable Home Routers
- Internet Freedom and OpenWRT
- The Knowledge Gap

- Demo

- Expert Systems and Knowledge bases
- Knowledge from the community

Vulnerable Home Routers

- An example
- 2009
- Time Warner SMC8014 router
- ~65,000 at risk users (wired.com)

vulnerability found by David Chen

Vulnerable Home Routers

- administrative functions and tools
  - hidden by client-side javascript
  - let us repeat: **client-side**

- "hack": disable JS in your browser

- find admin tool to dump config file
  - username/password in **clear-text**

Vulnerable Home Routers

- was there a quick fix?
- was it available for peer-review?
- Public Relations to the rescue!

- New firmware was to be released

Vulnerable Home Routers

"Change the default password? How do you do that? I'll just forget it."

- Immediate gratification
- Good enough
- Too hard, little reward

- Big reward if using Tomato, dd-wrt, etc

Internet Freedom and OpenWRT

"... enables you to use stateful packet inspection, intrusion detection, and any number of other things that normally require several thousand dollars worth of hardware to do effectively."

- Blessing and Curse
  - free and open features
  - ...that nobody knows how to use

The Knowledge Gap

The Knowledge Gap

AmazingJellybean.com

The Amazing Jellybean is a smart ***power switch*** that reboots your devices in the correct order to solve connection problems.

Big caveat before we continue

- OpenWRT already installed
  - programmatic solution for 30-30-30 reboot ?

Demo

views.py
models.py

- PyCLIPS a library wrapper of CLIPS
  - env.RegisterPythonFunction(module_func)

class method signature
  "func(klass, arg1)"
  we do not want to keep track of "klass"

Demo -- CLIPS

developed by NASA in late 80s / early 90s

now an open-source project

Learned once a time in an AI college course

- basketball coach

LISP-like

C-Language Integrated Production System

Demo -- Integrate with Django

proof of concept in CLIPS shell

replace call to
    deffunction setprompt (in decision-nodes.clp)
with our own python equivalent
    setprompt (in views.py)

CLIPS runs in own process; blocking
clips.run(1) to run until one(1) rule is activated
    then check for messages/UCI commands

Demo

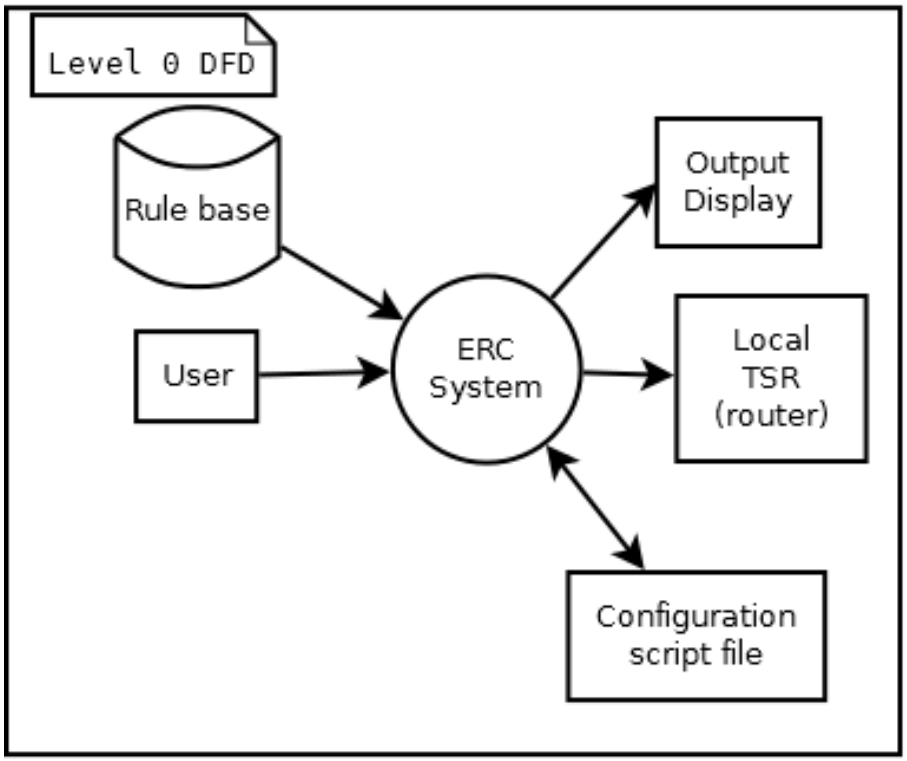
configuration script

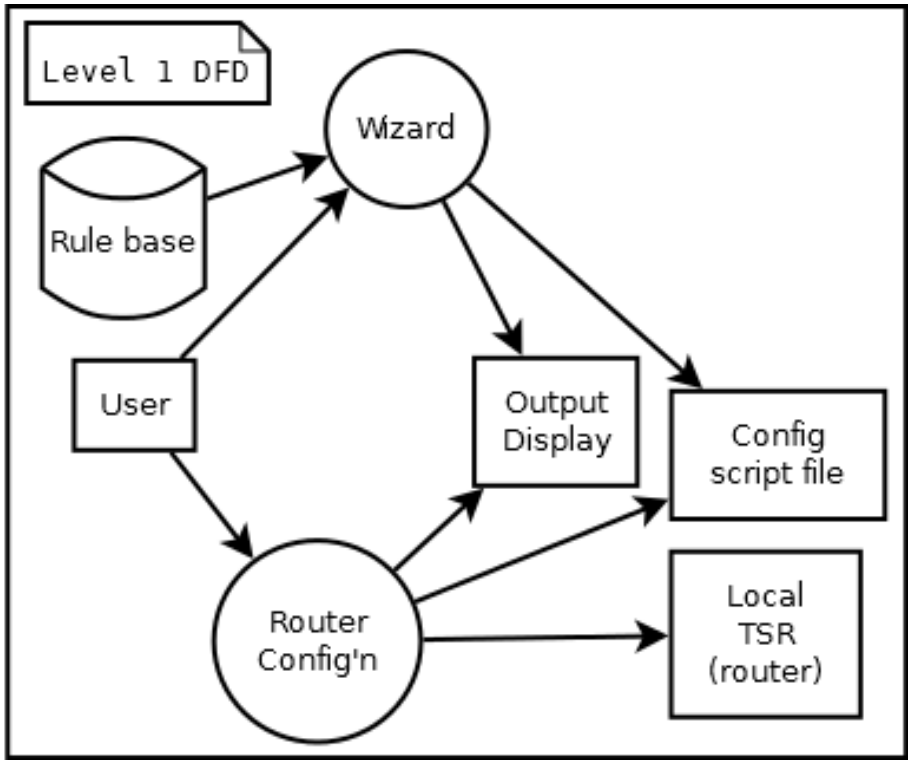
UCI - unified configuration interface

```
root@OpenWrt:~# uci add firewall rule
root@OpenWrt:~# uci set firewall.@rule[-1].src=wan
root@OpenWrt:~# uci set firewall.@rule[-1].target=ACCEPT
root@OpenWrt:~# uci set firewall.@rule[-1].proto=tcp
root@OpenWrt:~# uci set firewall.@rule[-1].dest_port=22
root@OpenWrt:~# uci commit firewall
root@OpenWrt:~# /etc/init.d/firewall restart
```

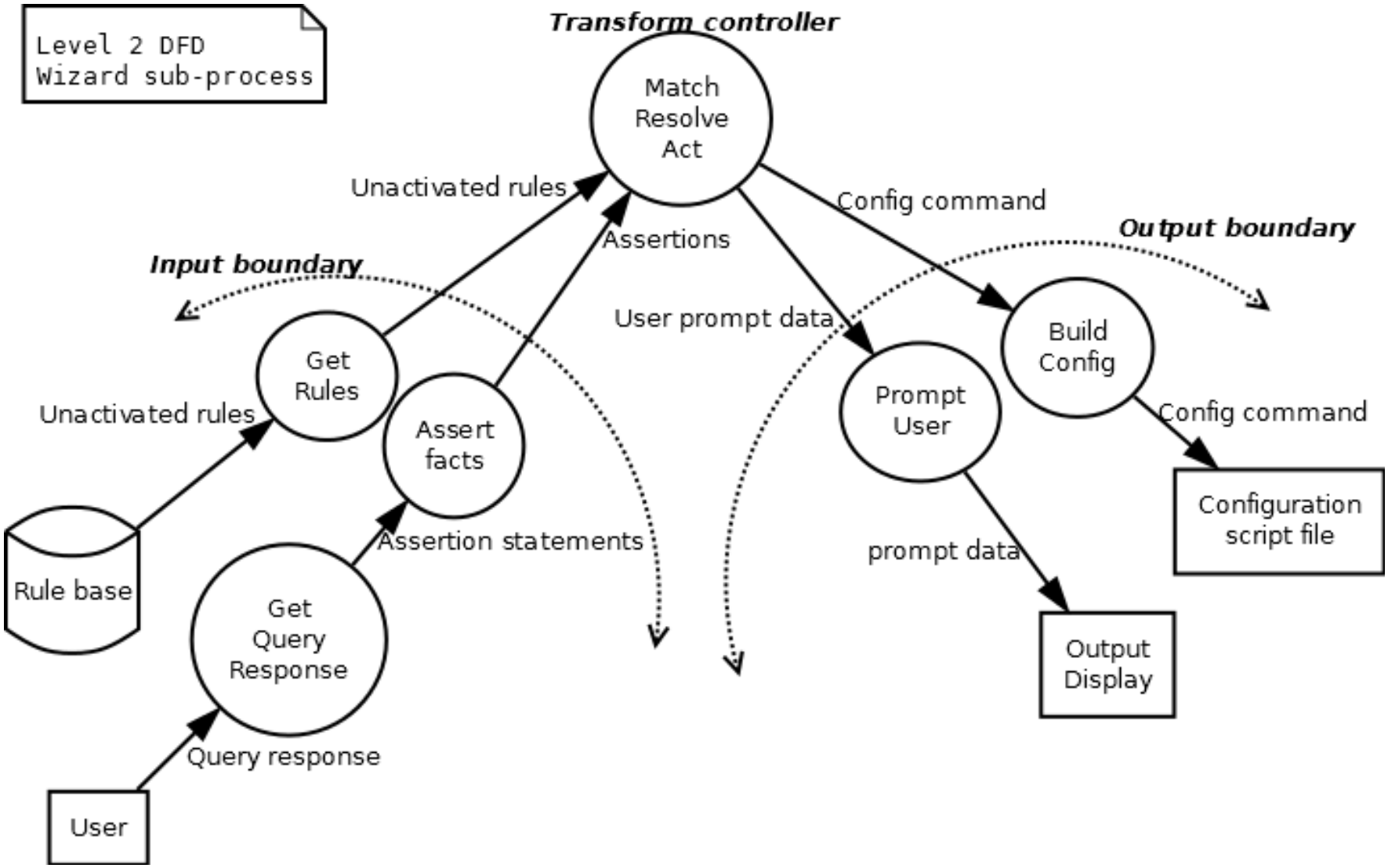
Static Inference Engine
Dynamic Knowledge Base

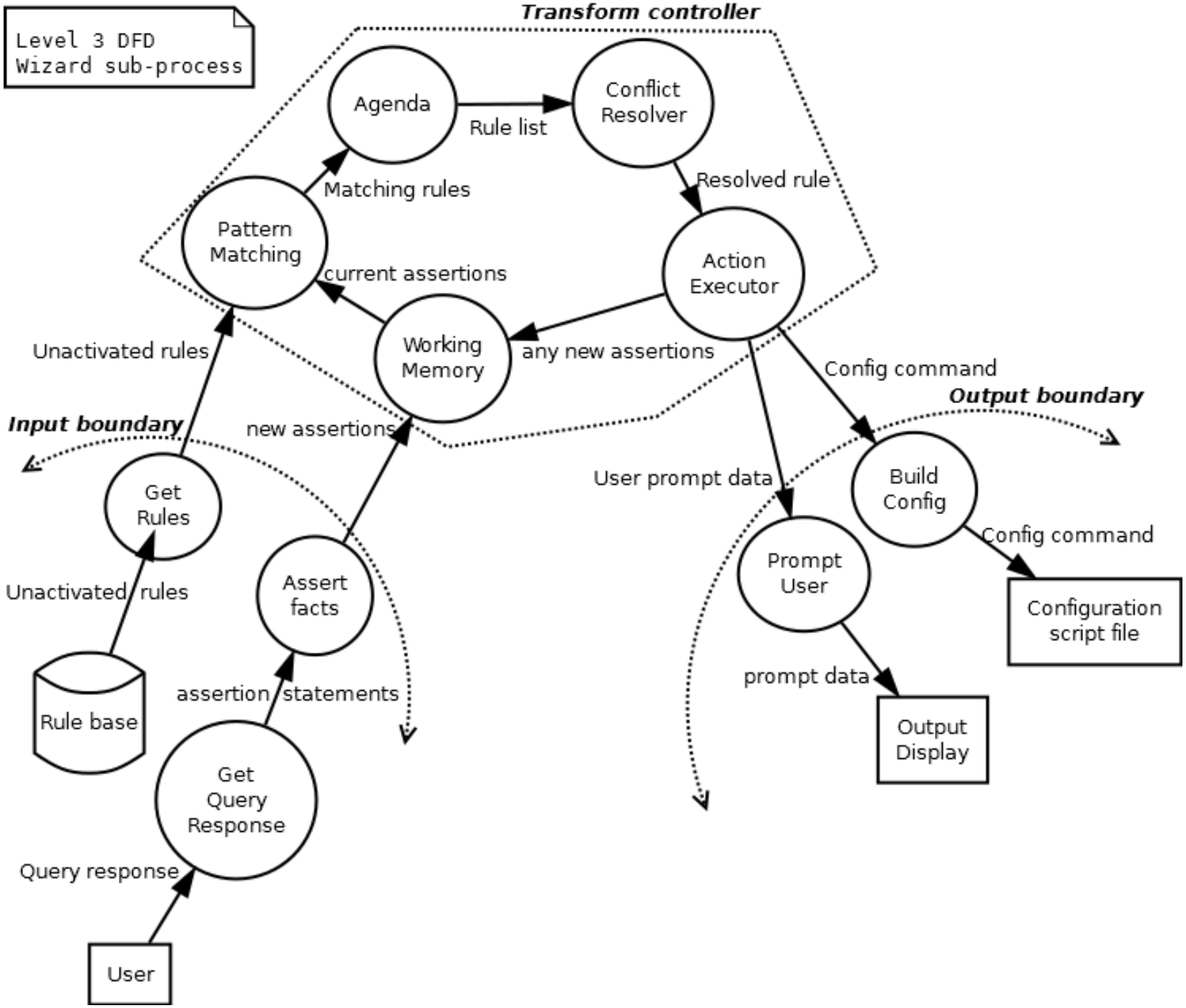
The Bakshi / ERC System



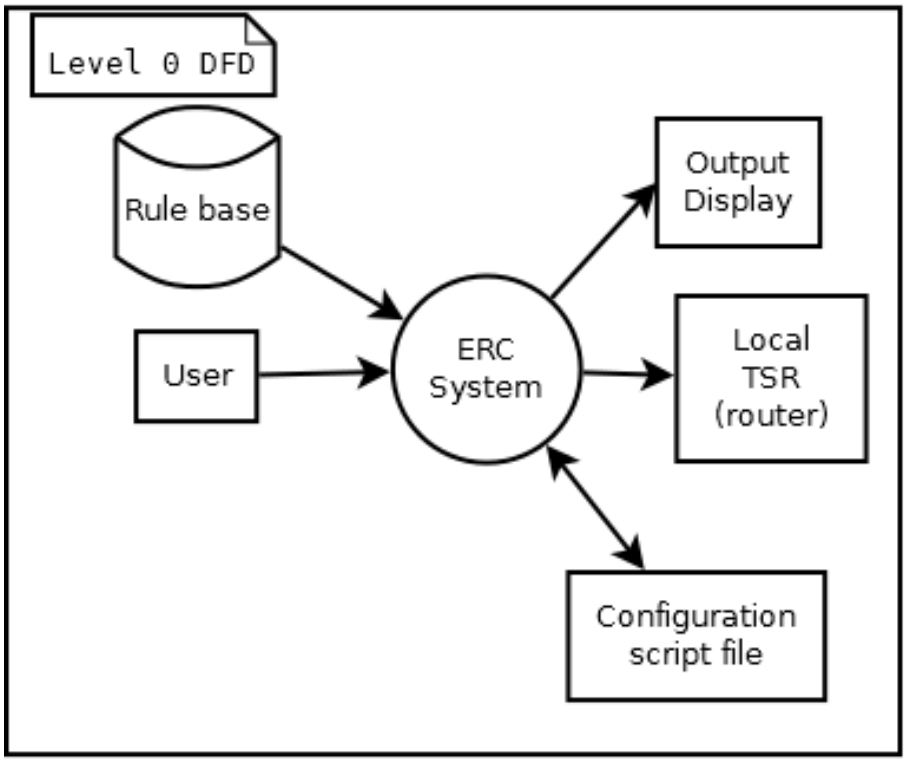


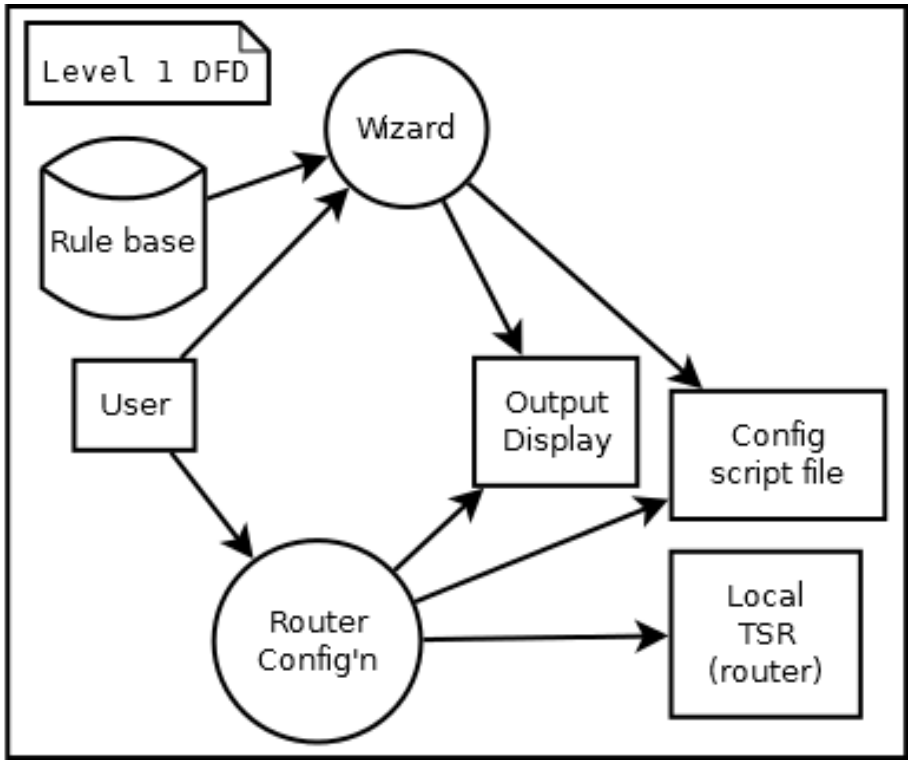
The Bakshi / ERC System



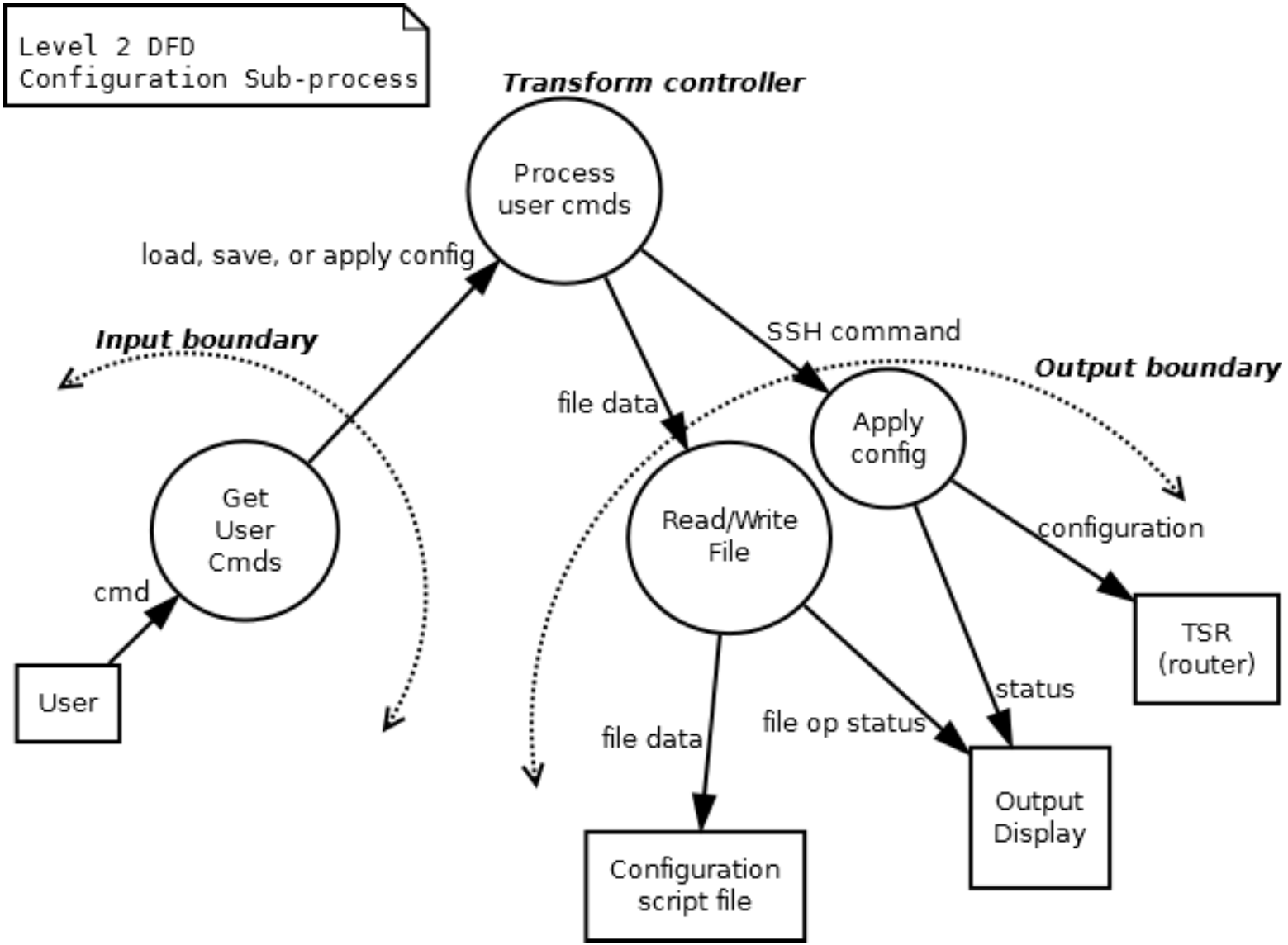

Level 3 DFD
Wizard sub-process
Transform controller
Agenda
Rule list
Conflict Resolver
Resolved rule
Matching rules
Pattern Matching
current assertions
Action Executor
Working Memory
any new assertions
Unactivated rules
Input boundary
new assertions
Config command
Output boundary
Get Rules
User prompt data
Build Config
Config command
Unactivated rules
Assert facts
Prompt User
Configuration script file
prompt data
Rule base
assertion statements
Output Display
Get Query Response
Query response
User

The Bakshi / ERC System





The Bakshi / ERC System



Expert Systems/Knowledge Bases

- Why not just use if-then-else?

Combinatorial Explosion

- pattern-matching algorithm (e.g. Rete)
- regular expressions

Knowledge Base Design

- Certainty factors
  - probability

- backward-chaining
  - goal-driven approach
  - good for determining if a known solution is optimal

- forward-chaining
  - data-driven approach
  - good for finding ***any*** solution given data or facts

http://www.csie.ntu.edu.tw/~sylee/courses/clips/design.htm

Knowledge from the community

Domain Experts not Programmers

Programming not required*

*However, knowledge representation is hard.
Main disadvantage of Expert Systems is quality

Further Work

- OpenWRT installation
  - can it be done programmatically?
- Help grow the knowledge base!

- CLIPS is not easy for non-programmers
  - strip syntactic sugar; leave knowledge representation
    - plain text
    - YAML
  - abstract UCI/script commands
    - macros?

Business Domain Development (BDD)

Cucumber (Ruby)

Lettuce (Python)

Behave (Python)

Feature: Fight or flight

In order to increase the ninja survival rate,

As a ninja commander

I want my ninjas to decide whether to take on an opponent based on their skill levels

Scenario: Weaker opponent

Given the ninja has a third level black-belt

When attacked by a samurai

Then the ninja should engage the opponent

Scenario: Stronger opponent

Given the ninja has a third level black-belt

When attacked by Chuck Norris

Then the ninja should run for his life

Q & A

Mike Perez

Please add to the KB!

https://github.com/meekprize/bakshi

---> decision-nodes.clp

@10bitworks
meekprize@gmail.com

10bitworks every Saturday 1-6pm
1020 Roosevelt San Antonio TX 78210