Examples of state definitions

Table of Contents

Examples of state definitions	1
Model, Data and Command	2
Output	2
Output for CONSTANT_STATES_1	2
Output for CONSTANT_STATES_2	3
Output for DEPENDENT_STATES_1	4
Output for DEPENDENT_STATES_2	4
Output for IMPORTING_STATES	5
Output for IMPORTING_BEHAVIORS_AS_STATE	5
Output for IMPORTING_BEHAVIORS_AS_STATE_W_CUSTOMIZATION	5
Output for WILDCARDING	6

Model, Data and Command

Model script
Example data

Command to run

```
./saf.py --db data/db/dnsflows_100rec.sqlite --model tests/bscripts/example_states.b --pretty
```

Model script reproduced:

```
[header]
NAMESPACE = EXAMPLES
NAME = STATES
QUALIFIER = { }[_eventno=1:20]
IMPORT = NET.APP_PROTO.DNSREQRES
[states]
state_A = {sipaddr = '10.1.11.2', dipaddr='10.1.4.2'}
state_B = \{sport > 53\}
state_C = {sipaddr=$state_A.dipaddr}
state_D = {sport=$state_B.sport, dnsqrflag=1}
state_E = DNSREQRES.dns_req()
state F = DNSREQRES.DNS REQ RES()
state_G = DNSREQRES.DNS_REQ_RES(sport > 30000)
state_H = {sipaddr='10.1.*'}
[behavior]
# For now it is important to include the definition of the state on which the
# dependent state is dependent
b1 = (state_A and state_C)
b2 = (state_B and state_D)
[model]
CONSTANT_STATES_1(eventno, eventtype, sipaddr, dipaddr, sport, dport) = (state_A)
CONSTANT_STATES_2(eventno, eventtype, sipaddr, dipaddr, sport, dport) = (state_B)
DEPENDENT_STATES_1(eventno, eventtype, sipaddr, dipaddr, sport, dport) = b1
DEPENDENT_STATES_2(eventno, eventtype, sipaddr, dipaddr, sport, dport) = b2
IMPORTING_STATES(eventno, eventtype, sipaddr, dipaddr, sport, dport) = state_E
IMPORTING_BEHAVIORS_AS_STATE(eventno, eventtype, sipaddr, dipaddr, sport, dport) = state_F
IMPORTING BEHAVIORS AS STATE W CUSTOMIZATION(eventno, eventtype, sipaddr, dipaddr, sport, dport) = sta
WILDCARDING(eventno, eventtype, sipaddr, dipaddr, sport, dport) = state_H
```

Output

Output for CONSTANT_STATES_1

```
Instances satisfying CONSTANT_STATES_1
```

ı							
	Total Matching Ins	stances: 9					
	eventno	 eventtype	sipaddr	dipaddr		sport	d
	1	PACKET_DNS	10.1.11.2	10.1.4.2		10486	
	13	PACKET_DNS	10.1.11.2	10.1.4.2		60435	
	25	PACKET_DNS	10.1.11.2	10.1.4.2		20205	
	37	PACKET_DNS	10.1.11.2	10.1.4.2		47955	
	49	PACKET_DNS	10.1.11.2	10.1.4.2		34950	
	61	PACKET_DNS	10.1.11.2	10.1.4.2		59662	
	73	PACKET_DNS	10.1.11.2	10.1.4.2		62147	
	85	PACKET_DNS	10.1.11.2	10.1.4.2		38762	
	97	PACKET_DNS	10.1.11.2	10.1.4.2		25074	
		· · · · · · · · · · · · · · · · · · ·					

Output for CONSTANT_STATES_2

Instances satisfying CONSTANT_STATES_2												
Total Matching Instances: 9												
eventno	eventtype	sipaddr	dipaddr	sport	d _I							
1	PACKET_DNS	10.1.11.2	10.1.4.2	10486								
13	PACKET_DNS	10.1.11.2	10.1.4.2	60435								
25	PACKET_DNS	10.1.11.2	10.1.4.2	20205								
37	PACKET_DNS	10.1.11.2	10.1.4.2	47955								
49	PACKET_DNS	10.1.11.2	10.1.4.2	34950								
61	PACKET_DNS	10.1.11.2	10.1.4.2	59662								
73	PACKET_DNS	10.1.11.2	10.1.4.2	62147								

85		PACKET_DNS	10.1.11.2	10.1.4.2	38762	I
97		_	10.1.11.2		25074	

Output for DEPENDENT_STATES_1

=======	========	=======	=======
Instances	satisfying	DEPENDENT_	STATES_1
=======	:=======	=======	======

Total Matching Instances: 4

eventno	eventtype		sipaddr		dipaddr		sport		dŗ
1	PACKET_DNS		10.1.11.2		10.1.4.2		10486	I	
			Behavior: DE	PENDEN	 T_STATES_1.b1				
8	PACKET_DNS	1	10.1.4.2		10.1.11.2	1	53	1	1(
13	PACKET_DNS	ı	10.1.11.2	l	10.1.4.2	l	60435	I	
			Behavior: DE	PENDEN	T_STATES_1.b1				
20	PACKET_DNS		10.1.4.2		10.1.11.2	I	53		6(

Output for DEPENDENT_STATES_2

=======	========	===========
Instances	satisfying	DEPENDENT_STATES_2
=======	========	

Total Matching Instances: 4

									!
eventno	eventtype	l	sipaddr		dipaddr		sport	I	dı
1	PACKET_DNS	I	10.1.11.2		10.1.4.2		10486	I	
			Behavior: DE	ENDEN'	r_states_2.b2				
2	PACKET_DNS		10.1.6.3		10.1.4.2		53		32
			Behavior: DE	PENDEN'	r_states_2.b2				
3	PACKET_DNS		10.1.6.3		10.1.4.2	1	53	I	32
13	PACKET_DNS		10.1.11.2		10.1.4.2		60435		

Output for IMPORTING_STATES

Total Matching Instances: 2	
eventno eventtype sipaddr dipaddr sport	d _I
1 PACKET_DNS 10.1.11.2 10.1.4.2 10486	
13 PACKET_DNS 10.1.11.2 10.1.4.2 60435	

Output for IMPORTING_BEHAVIORS_AS_STATE

=========	=====	=========	=====	=======						
Instances sati	sfying	J IMPORTING_BEH	AVIOR	S_AS_STATE						
========	=====	=========	====	=======						
Total Matching	Insta	ances: 2								
eventno	 	eventtype	 	sipaddr	 	dipaddr	 	sport		 d <u>r</u>
				Behavior	: DNS_	REQ_RES.b				
1		PACKET_DNS		10.1.11.2		10.1.4.2		10486		
8	I	PACKET_DNS		10.1.4.2	- 1	10.1.11.2		53		1(
				Behavior	: DNS_	REQ_RES.b				
13		PACKET_DNS		10.1.11.2		10.1.4.2		60435		
20		PACKET_DNS		10.1.4.2		10.1.11.2		53		6(

${\bf Output\ for\ IMPORTING_BEHAVIORS_AS_STATE_W_CUSTOMIZATION}$

Instances sati	===== sfying ======	======================================	===== AVIOR: =====	======== S_AS_STATE_W_ ==========	====== CUSTOMI ======	===== ZATION =====		
Total Matching	Insta	nces: 1						
eventno		eventtype		sipaddr		dipaddr	sport	dī
13		PACKET_DNS		Behavior 10.1.11.2	: DNS_R	REQ_RES.b 10.1.4.2	60435	

20	PACKET DNS	10 1 4 2	10.1.11.2	5.3	6(
20	THEREI_DID	10.1.1.2	10.1.11.2	33	

Output for WILDCARDING

					_							
		:==========	========									
Instances satisf	ying WILDCARDING =========											
Instances satisfying WILDCARDING												
Total Matching I	nstances: 20											
10001 11000111119 11												
eventno	eventtype	sipaddr	dipaddr	sport	dr							
1	 PACKET_DNS	10.1.11.2	10.1.4.2	 10486								
	PACKEI_DNS											
2	PACKET_DNS	10.1.6.3	10.1.4.2	53	32							
3	PACKET_DNS	10.1.6.3	10.1.4.2	53	32							
4	 PACKET_DNS	10.1.6.3	10.1.4.2	 53	32							
					32							
5	PACKET_DNS	10.1.6.3	10.1.4.2	53	32							
6	PACKET_DNS	10.1.6.3	10.1.4.2	53	32							
7	 PACKET_DNS	10.1.6.3	10.1.4.2	 53	32							
,												
8	PACKET_DNS	10.1.4.2	10.1.11.2	53	10							
9	PACKET_DNS	10.1.6.3	10.1.4.2	53	32							
10	 PACKET_DNS	10.1.6.3	 10.1.4.2	 53	3.0							
11	PACKET_DNS	10.1.6.3	10.1.4.2	53	32							
12	PACKET_DNS	10.1.6.3	10.1.4.2	53	32							
13	PACKET_DNS	10.1.11.2	10.1.4.2	 60435								
14	PACKET_DNS	10.1.6.3	10.1.4.2	53	32							
15	PACKET_DNS	10.1.6.3	10.1.4.2	53	32							

16		PACKET_DNS		10.1.6.3	l	10.1.4.2		53	l	3:
17		PACKET_DNS		10.1.6.3		10.1.4.2		53	I	3:
18	I	PACKET_DNS	I	10.1.6.3	ı	10.1.4.2	l	53	l	3:
19		PACKET_DNS		10.1.6.3	l	10.1.4.2		53		3:
20		PACKET_DNS		10.1.4.2		10.1.11.2	 	53		6