Composing models to build higher-level models

The ability to build higher-level models by composing existing models is a key feature of the semantic analysis framework. A user can import existing models from the knowledge base and relate them using the language operators to create models that capture higher-level meaning.

As an example, consider the following diagram shows the chain of simple models being composed to form the model of a network worm. The direction of arrows

Building a model for TCP Flow

As a practical example, consider the simple analysis example where we used the TCP connection setup and TCP connection teardown models from the knowledge base. Individually, each model captures the possible behaviors of TCP during connection start and termination. A new model for TCP flow - capturing a complete TCP Flow - can now be created by simply composing the above two models.

The relevant lines of the TCP flow model are simply the following:

```
 IMPORT = NET.BASE_PROTO.TCPCONNSETUP, NET.BASE_PROTO.TCPCONNTDOWN
tcp_3way_handshake =  TCPCONNSETUP.TCP_CONNSETUP()
tcp_conn_tdown     =  TCPCONNTDOWN.TCP_CONNTDOWN($tcp_3way_handshake)
tcpflow = (tcp_3way_handshake ~> tcp_conn_tdown)
```

We can test this model by applying it over the same sample packet capture. The following output shows that the framework indeed reports 5 complete TCP flows matching the outputs from both the models.

```
###############################################
#    Semantic Analysis Framework - v0.1a    #
###############################################

Reading input event database 'data/sample.sqlite' ..
Found 1105 events in database
       PACKET_TCP - 1105 events [ Fri Feb 26 13:58:06 2010 (1267192686) to Fri Feb 26 13:59:02 2010 (1
Creating temporary directory for storing state /tmp/temp
Initializing global symbol table..
Reading and initializing from the knowledge base 'knowbase'..
Parsing specified model : 'knowbase/net/base_proto/tcpflow.b'..
Processing model TCPFLOW
   QUALIFIER matched 1105 instances
   QUALIFIER matched 1105 instances
   State tcp_pkt_syn .. found 5 instances
   State tcp_pkt_synack .. found 5 instances
   State tcp_pkt_ack .. found 5 instances
 Behavior 3way_handshake .. found 5 instances
 Behavior TCP_CONNSETUP .. found 5 instances
   QUALIFIER matched 1105 instances
   State tcp_pkt_fin .. found 0 instances
 Behavior full_teardown .. found 0 instances
```

```
   QUALIFIER matched 1105 instances
   State tcp_pkt_piggyfin .. found 5 instances
   State tcp_pkt_finack_from_d .. found 0 instances
   State tcp_pkt_ack_from_s .. found 0 instances
 Behavior full_teardown_piggyfin .. found 0 instances
   QUALIFIER matched 1105 instances
   State tcp_pkt_piggyfin .. found 5 instances
   State tcp_pkt_ack_from_d .. found 5 instances
 Behavior half_close .. found 5 instances
   QUALIFIER matched 1105 instances
   State tcp_pkt_syn .. found 5 instances
   State tcp_pkt_rst_sd .. found 0 instances
 Behavior close_by_rst .. found 0 instances
 Behavior TCP_CONNTDOWN .. found 5 instances
 Behavior tcpflow .. found 5 instances
Model TCPFLOW satisfied by 5 instances

============================
Instances satisfying TCPFLOW
============================

Total Matching Instances: 5

-------------------------------------------------------------------------------------------------------
    eventno      |    timestamp     |  timestampusec   |     sipaddr      |     dipaddr      |      sp
-------------------------------------------------------------------------------------------------------
                                                        Behavior: TCP_CONNSETUP.3way_handshake
       1         |    1267192686    |      584044      |   192.168.3.65   |  188.72.243.72   |       1
       2         |    1267192686    |      693493      |  188.72.243.72   |   192.168.3.65   |
       3         |    1267192686    |      694094      |   192.168.3.65   |  188.72.243.72   |       1
                                                          Behavior: TCP_CONNTDOWN.half_close
     231         |    1267192697    |      45567       |   192.168.3.65   |  188.72.243.72   |       1
     232         |    1267192697    |      155003      |  188.72.243.72   |   192.168.3.65   |
-------------------------------------------------------------------------------------------------------
                                                        Behavior: TCP_CONNSETUP.3way_handshake
     233         |    1267192716    |      734749      |   192.168.3.65   |  188.72.243.72   |       1
     235         |    1267192716    |      839227      |  188.72.243.72   |   192.168.3.65   |
     237         |    1267192716    |      839479      |   192.168.3.65   |  188.72.243.72   |       1
                                                          Behavior: TCP_CONNTDOWN.half_close
     384         |    1267192720    |      189433      |   192.168.3.65   |  188.72.243.72   |       1
     385         |    1267192720    |      293200      |  188.72.243.72   |   192.168.3.65   |
-------------------------------------------------------------------------------------------------------
                                                        Behavior: TCP_CONNSETUP.3way_handshake
     234         |    1267192716    |      735142      |   192.168.3.65   |  188.72.243.72   |       1
     236         |    1267192716    |      839360      |  188.72.243.72   |   192.168.3.65   |
     238         |    1267192716    |      839561      |   192.168.3.65   |  188.72.243.72   |       1
                                                          Behavior: TCP_CONNTDOWN.half_close
     508         |    1267192725    |      818246      |  188.72.243.72   |   192.168.3.65   |
     509         |    1267192725    |      818412      |   192.168.3.65   |  188.72.243.72   |       1
-------------------------------------------------------------------------------------------------------
                                                        Behavior: TCP_CONNSETUP.3way_handshake
```

```
      391        |    1267192721    |      488644      |   192.168.3.65   |  188.72.243.72   |       1
      392        |    1267192721    |      662229      |  188.72.243.72   |   192.168.3.65   |
      393        |    1267192721    |      662356      |   192.168.3.65   |  188.72.243.72   |       1
                                                          Behavior: TCP_CONNTDOWN.half_close
      1093       |    1267192737    |      44557       |   192.168.3.65   |  188.72.243.72   |       1
      1094       |    1267192737    |      145090      |  188.72.243.72   |   192.168.3.65   |
-------------------------------------------------------------------------------------------------------
                                                        Behavior: TCP_CONNSETUP.3way_handshake
      1096       |    1267192737    |      520050      |   192.168.3.65   |  188.72.243.72   |       1
      1097       |    1267192737    |      800484      |  188.72.243.72   |   192.168.3.65   |
      1098       |    1267192737    |      800710      |   192.168.3.65   |  188.72.243.72   |       1
                                                          Behavior: TCP_CONNTDOWN.half_close
      1104       |    1267192742    |      960450      |  188.72.243.72   |   192.168.3.65   |
      1105       |    1267192742    |      960702      |   192.168.3.65   |  188.72.243.72   |       1
-------------------------------------------------------------------------------------------------------
```