A Guide of ForenGuard Demo

1. This VM image (username & pwd: floodlight) contains the following things:
   a. Mininet + OpenVSwitch
   b. Community Version MongoDB
   c. Instrumented Floodlight Controller
   d. ForenGuard

2. This VM image can help demo the running case in our paper:

3. Steps of demo:
   a. Start mongodb
      mongod --dbpath data/db/ --smallfiles
   b. Create the topology using Mininet
      For example: create a three-switch topology, each switch connects to a host
      mn --controller=remote, port=6653 --topo linear,3
   c. Start our instrumented Floodlight Controller
      java -jar floodlight.jar
   d. Prepare for the MAC spoofing attack
      Check all three hosts’ network configuration
   e. Use h2 to spoof h3’s MAC address
f. Launch the spoofing attack. Use h2 to send network packets to h1. Also at the same time, try to use h3 to make connection with h1 as well.

g. Observation: when h2 is connecting with h1, h3 cannot make the connection with h1 any more. Attack succeeds!

h. Suppose you are the owner of h3. Let’s use ForenGuard to diagnose why you lose network connection with h1.

i. We can use the following command to query for the control plane execution traces of how they forward the traffic from h3 to h1:

   ```
   ```

j. Then we can check the diagnosis results:

k. We can observe that there are four events that are the root causes. When you further check these four events, they are triggered by h2’s spoofing.

l. Don’t forget to clean up MongoDB after the use

   (mongodb shell) > db.dropDatabase()