Network traffic collection in the MOC

1. Vision and Goals Of The Project:

Network usage trends come and go, it’s hard to predict the traffic patterns ahead. From network administrator’s perspective, security is the most important fact. Detection of network attacks is based on “acquired knowledge” either the well-known attacks which they are programmed to alert on, or those anomalous actions that deviate from a known regular-operation profile.

Making a tool that can monitor network traffic is not the goal of this project. We have a vision that building a research platform which can be integrated to existing cloud environments is more important(But we will start from basic steps).

High-level goals of our MOC-SECURITY project includes:

a. Providing a way to monitor HTTP traffic that pass through the proxy server, recording all HTTP requests to a time-series database.
b. Detecting potential attack behaviors by analysing data from database.

Users/Personas Of The Project

MOC-SECURITY will be used by the end-users of MOC including researchers from BU, NU, MIT, HU and UMass, Cloud administrators, MGHPCC contributing companies, Commonwealth companies and government institutions, paying users.

It targets only expert users.

2. Scope and Features Of The Project:

This project can be used as a research platform for areas like data mining and network security. For example, data scientists are able to form their own security checking model and apply their models to our platform(for now, we only examine HTTP headers since we will only apply attack detection model that based on HTTP logs) and test their correctness.

a. Collect HTTP requests from all incoming/outgoing packets at proxy server.
    - If possible, we should provide generic interface for capturing all well known requests(not only HTTP), since new behavior models may be introduced later for detecting new kind of attacks that require to analyze non-HTTP requests.
    - Enable support for monitoring selected VM in the cloud.

b. Parse HTTP headers and store them into time-series database.

c. Apply attack detection behavior model(for detecting DOS attack) to the data that is store in the database.

d. Generate alerts if attacks detected and informs admin that proxy server will drop all packets coming from this source address.

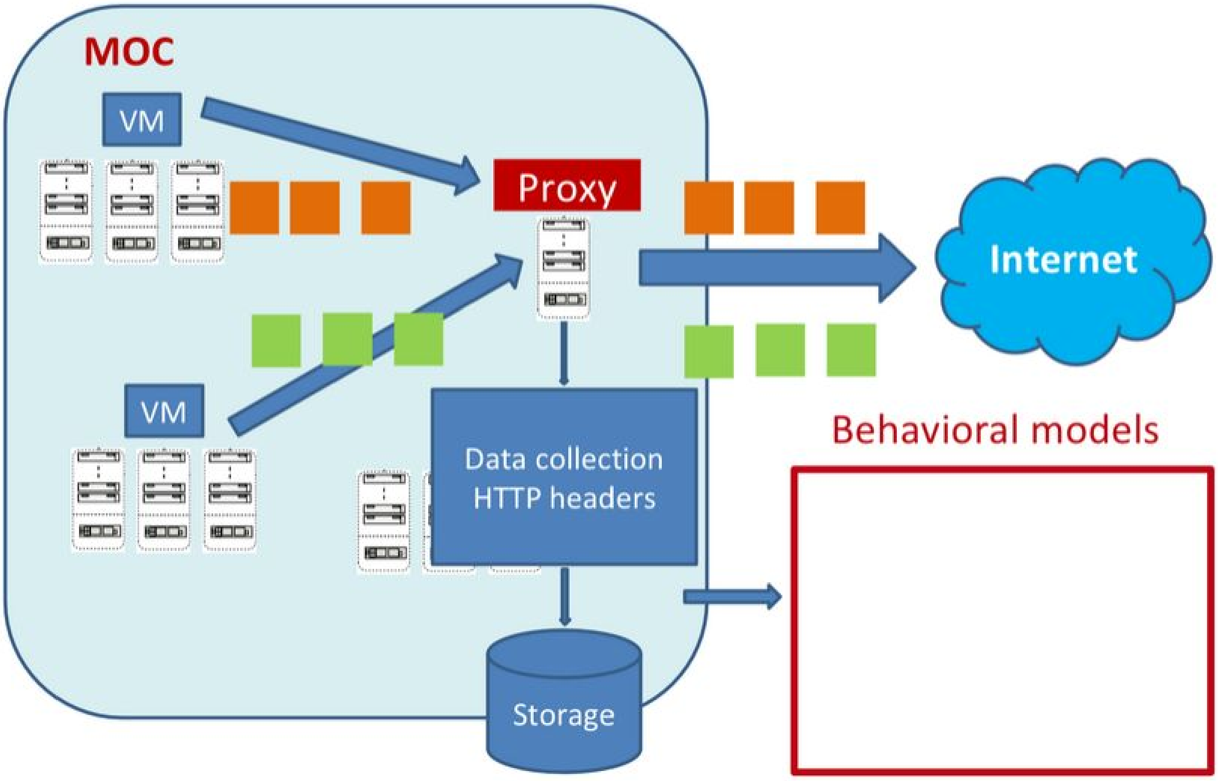

Fig 1 (Project overview)

3. Solution Concept

a. Write a demon that running at proxy server in order to capture all incoming/outgoing packets(HTTPs for now)

b. Extract all fields of HTTP headers and parse them onto a time-serial database
c. Simulate Denial of Service attack behavior from VMs in the cloud and check if the security checking model we have can detect this attack.

4. Acceptance criteria

Minimum acceptance criteria: all HTTP packets' info that pass the proxy can be stored into time-serial database .

Stretch goals are:

a. Simulate a simple attack(e.g. Denial of Service) and use the data to detect it.
b. Test the expansibility of this platform by applying different behavior models(if there's) with required type of network requests.

5. Release Planning:

Release #1 (due by Week 5):

Get familiar with OpenStack environment and implement demon that running on the proxy for capturing HTTP requests in openstack environment.

Since we just get start, we may not able to finish the entire implementation.

Release #2 (due by Week 7):

Complete the implementation. Enhance this implementation, improve its stability and bugs fix. Provide more document support.

Release #3 (due by Week 9):

Enable supports for monitoring selected VM in the cloud.

Release #4 (due by Week 11):

Improve the previous implementation by adding support to parse HTTP headers info from previous collected HTTP requests and store them into time-serial database.

Release #5 (due by Week 13):

Apply the behavior model to the data and detect attacks