Johns Hopkins University Information Security Institute

MSSI Capstone Project Proposal

# Bio-inspired, host-based firewalls based on cellular mechanisms

Team: Jay Chow, Kevin Hamilton, James Ballard

Consultant: Kevin Klous

Advisor: Dr. Lanier A.Watkins(JHUAPL)

## Introduction:

A firewall is an important security technology that is widely deployed in networks, restricting network traffic from one side of the network to the other side. A firewall is part of a computer system or network that is designed to stop unauthorized traffic from flowing from one network to another. Firewalls can be deployed anywhere, and are most commonly seen separating trusted and untrusted components of a network. Firewalls are also useful in differentiating networks within a trusted network. It can create a clear distinction between various divisions in an organization. The main functionalities include filtering data, redirecting traffic, protecting against network attacks.

In the cell membrane, there is a permeability barrier that separates the cytoplasm from the exterior environment. Permselectivity is the preferential permeation of certain ionic species through ion-exchange membranes. Endocytosis is a cellular process in which substances are brought into the cell when the material to be internalized is surrounded by an area of plasma membrane, which forms a vesicle inside the cell to contain the ingested material. Passive transport in the movement of ions and molecular substances across cell membranes without the need of energy while active transport is the movement of molecules from a region of lower concentration to a region of higher concentration with the need of energy. We will look at new natural defensive mechanisms to enable open-source firewalls to be more superior in terms of cyber defense.

## Problem:

Security protocols are growing and cyberattacks are gaining complexity today. As such, algorithms in firewalls need to evolve for better security. A firewall acts as a barrier between a trusted network and an untrusted network, controlling both incoming and outgoing network traffic based on rules and traffic content. It is among the first lines of defenses for protecting a network or a host from malicious users. A firewall intercepts network packets and based on a specific firewall policy, which consists of predetermined rules, decides whether to allow, reject or deny certain packets to pass through it. Current firewalls that too many rules which make them complex to manage. Another problem is that current packet-matching algorithm is slow and inefficient. We see a natural mapping between firewalls and cell membranes in terms of both allowing and blocking network packets and molecules respectively. We will focus on host-based, endpoint firewalls in a distributed setting. This better mimics an organisms that are made up of many cells.

## Objective:

There are 3 main types of firewalls. First, a packet filter or stateless firewall that makes decisions based on each individual packet by examining the headers without the payload. Second, a stateful firewall that makes decisions based on state information formed by multiple packets that are related, tracking the state of traffic by monitoring all connection interactions until it is closed. Lastly, an application firewall controls inputs, outputs and access from/to an application or service. This inspects network traffic up to the application layer. A typical implementation of application firewall is a proxy, acting as an intermediary.

When cells face an invading virus, bacteria, they protect themselves by inserting the wrong amino acid into new proteins to defend themselves against damage. These regulated errors is a novel non-genetic mechanism by which cells could make proteins more resistant to attack when stressed. After modifying source code from an open-source, host-based firewall, we will represent this natural mechanism with a host-based firewall technology in a distributed computing environment by conducting experiments and recording relevant and interesting results.

Milestones:

| Description of Task | Tentative date of completion |
|---|---|
| Rigorous literature review of latest core firewall technology (open source, Cisco and Palto Alto), packet matching algorithm, endocytosis, permselectivity, passive transport and active transport, stress effects on cell membranes | To be conducted over the summer, to be completed by early September 2019 |
| Come out with a performance test or benchmark for existing open-source firewalls | Early October 2019 |
| Write and modify code to add cellular mechanisms and behavior to open-source firewall software by designing and implementing host-based algorithms in a distributed setting. | Mid October 2019 |
| Conduct experiments to measure and evaluate performance before and after the application of cellular mechanisms | End October 2019 |
| Analyze the results and draw conclusions | Mid to End November 2019 |

| | |
|---|---|
| Write a technical report of our findings and publish academic paper with Dr Watkins | Early to Mid December 2019 |

Note: Starting last semester, we have scheduled follow-up meetings with Dr. Watkins on a regular basis. This semester, we have weekly meetings with Dr. Watkins on Thursdays from 10.30am to 11.30am. We will schedule more meetings if needed.

References:

https://ieeexplore.ieee.org

https://dl.acm.org/

https://geekflare.com/best-open-source-firewall'/

https://www.ipfire.org/features

https://opnsense.org

http://www.smoothwall.org

https://www.sciencedaily.com/releases/2009/11/091125134701.htm