Jay Chow

Bio-inspired firewalls based on cellular mechanisms

Capstone Research Project Notes

Johns Hopkins University Information Security Institute

Background:

* Security in the internet is highly important today as cyberattacks are gaining complexity
* Security protocols are growing in numbers
* As such, algorithms need to evolve to cope with the need for better security and the growth of security protocols

|  |  |
| --- | --- |
| Cell Membrane | Packet Filter Firewall |
| Phospholipid Bilayer | Firewall |
| Carrier Protein | Security access strategy |
| Glycoprotein | Security access strategy |
| Nutrient | Packet |
| Fluidity |  |
| Perm-selectivity | Filter Protocols |
| Closure property | Filter Protocols |
| Asymmetry |  |

A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on pre-determined security rules. In a cell membrane, there is a permeability barrier that separates the cytoplasm from the exterior environment.

There are 3 characteristics of cell membranes that could be applied to bio-inspired firewalls

1. Fluidity
2. Asymmetry
3. Permselectivity : the preferential permeation of certain ionic species through ion-exchange membranes

In terms of permselectivity, cell membranes use carrier proteins to transport water-soluble molecules from the outside of the cell to the inside of the cell. Cell membranes also use glycoprotein to receive chemical signals. Firewalls use security access strategies to filter packets. In this aspect, there is a similarity.

I propose an improved version of a packet filtered firewall by improving on the packet matching algorithm by using an effective classification algorithm instead of traditional matching algorithms which are linear in run time. Under cellular mechanisms, the cell uses passive transport and endocytosis to deal with the interchange of materials in large, which is efficient. As such, we can relate this efficiency by improving on the security access strategy. Note that there are protein foldings on the walls of cell membranes to only allow certain substances to enter in. This can be related to ingress filtering.

Flaws of a packet-filtered firewall:

1. Susceptible to IP spoofing
2. Implicit
3. No state inspection
4. Speed of filtering
5. Filter protocol can be complex and difficult to design

Proposed bio-inspired solution:

1. Improved packet matching algorithm
2. Add stateful and application filtering BASED solely on cell mechanisms

Relevant background from other papers:

1. Tri-modularization of firewall policies

Firewall policies are notorious misconfiguration errors which could lead to a failure of protecting hosts in the network from malicious users. Firewall policies are monolithic. Inspired by modular programming and code refactoring, the paper introduces 3 kinds of modules: primary, auxiliary and template, which help in the refactoring of a firewall policy into smaller, reusable, comprehensible and more manageable components. The paper discusses algorithms for generating each of the 3 modules for a given legacy firewall policy

A firewall 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, decides whether to allow, reject or deny certain packets to pass through it. As firewalls are developed by different vendors such as Cisco and Checkpoint, the syntaxes and semantics of firewall policy languages vary.

But at the core, most packet filtering rules are expressive in languages that can be translated into an ACL. An ACL firewall policy is an ordered list of rules; each rule has “target 🡪 action”, in which target specifies a set of packets to which this rule is applicable, and action states what should be done with the packet. In an ACL, multiple rules can be applicable to a single packet and the decision of the first rule is applicable to the packet, is imposed on the packet.