NETWORK FIREWALL

PROJECT PROPOSAL

CECS 478 COMPUTER SECURITY

PROFESSOR MEHRDAD ALIASGARI

FALL 2015

Group Name: Access Denied

Bob Wei (ID# 006663564)

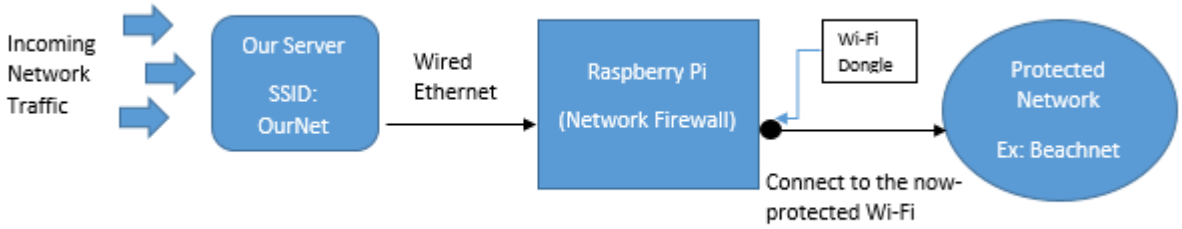
Sarah Shibley (ID# 010959713)

Motivation/Problem Statement

For our computer security project this semester, we would like to build a network firewall that can analyze incoming and outgoing network traffic, block or re-prioritize traffic that could be harmful to the network, and test the traffic that makes it through to ensure we were successful in only allowing the good traffic. By undertaking this project we hope to learn about deep packet inspection, types of network traffic, tools used in network traffic analysis, networking hardware, network traffic filters, gateways, proxies, and many other topics surrounding network security.

Proposed Solution/Approach

We plan to implement our own network traffic firewall to block malicious or unwanted traffic on a given wifi network. To do this, we will use a simple router (that we already have in our possession) that will send traffic that connects to it to a Raspberry Pi, which will act as a gateway and/or a proxy. The Raspberry Pi will then block or limit traffic as we specify it to and will let the rest of the traffic on through to the network through a WiFi dongle. Our network firewall will use tcpdump to analyze incoming traffic packets. Then we will use tools such as Linux Traffic Control to block or limit certain types of traffic that we determine to be harmful to the network. Once we have blocked certain types of traffic, we will use Wireshark to test the traffic that comes through to make sure that all malicious traffic has been blocked. Our Firewall will work with multiple OSI layers by at least acting as a packet filter and circuit-level gateway, and possibly as an application gateway and/or proxy server.



Implementation Details:

Platform:

- Raspberry Pi: will house our network firewall to block malicious network traffic.

Hardware:

- Raspberry Pi
- Wifi Dongle
- Router

Language:

- BASH scripting language

- Any others that our needed for the configuration

Components:

- tcpdump on Raspberry pi: analyze network traffic packets
- Packet Filter on Raspberry pi: block unwanted incoming/outgoing network packets
- Wireshark on our PCs: analyze incoming packets and test the traffic that is being passed through, as well as reading tcpdump files.
- Circuit-level gateway on Raspberry Pi: secures TCP and UDP connections
- Application Gateway on Raspberry Pi (optional): creates an app specific proxy
- Proxy Server on Raspberry Pi? (optional): disguises individual ip addresses on the network

Detailed Timeline (Tentative Schedule):

9/14: Purchase raspberry pi, set up and configure hardware:

  - Sarah: configure router (decide wifi/LAN settings, passwords, ip addressing, etc.)
  - Bob: configure raspberry pi (install OS, size/model SD card, etc.)

9/21: Research different types of network traffic based on testing with Wireshark (Bob and Sarah)

10/5: Implement Packet Filter

  - Bob will focus on: Source IP, time of day, queues
  - Sarah will focus on: Destination IP, protocol, Website

10/19: Create Circuit-level gateway

  - Bob: incoming traffic
  - Sarah: outgoing traffic

11/2: Additional components of the firewall – if too much to do both, both Bob and Sarah will focus on one of them only.

  - Bob: Proxy Server
  - Sarah: Application gateway

11/16: Testing and Troubleshooting

11/23: Finalize Documentation