DEVELOPMENT OF A TRANSPARENT NETWORK SECUTRITY DEVICE

A PROJECT REPORT PRESENTED BY

HERATH H.M.S.

to the Board of Study in Statistics and Computer Science of the

POSTGRADUATE INSTITUTE OF SCIENCE

in partial fulfillment of the requirement
for the award of the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

of the

UNIVERSITY OF PERADENIYA

SRI LANKA

2010

DEVELOPMENT OF A TRANSPARENT NETWORK SECUTRITY DEVICE

Herath H.M.S.

Lanka Education & Research Network
20 Ward Place
Colombo 07
Sri Lanka

One weakness in the traditional behavior of a firewall is the fact that it also must route packets after a decision is made, because the device handles packets at the network layer. The device also changes the sender hardware address of the incoming frame when it is sent out through the outgoing interface by replacing it with its own hardware address. Thus it is possible for both inside and outside networks to identify that there exists a device in between.

A transparent device moves packets as they were received by the device without changing the sender hardware address. Such a device can be plugged anywhere in a network - between two routers, or between a router and a switch, or between a switch and a single machine - and be invisible to both devices that it interconnects. This report presents the details of the development of a transparent network security device.

The source code of standard Linux bridge module was modified to act as an efficient two port bridge device, and queue frames directly to the user space using Linux Netlink sockets. The device on which the Linux bridge runs is usually invisible to both the devices that it interconnects. Linux Netlink sockets are used to pass the frames smoothly back and forth between the user space and kernel space. The source code of the well known IDS/IPS Snort was also patched to receive packets from and send back to kernel using the Netlink user space library. The Snort packet decoder and the Snort rule set was used in the usual manner to analyze the frame and to make decisions weather the frame is dropped or passed.

The OpenWrt open source Linux distribution was used to build a small software image of size 4MB which can be used to flash a Sidewinder IXP465 development platform manufactured by ADI Engineering. The effort finally made a portable two port security device (box), small in size to plug anywhere in a network to filter out malicious frames passing through.