Lars Sorenson
CS 422 – Lab 3 Writeup 4

Packet inspection at the Kernel level would allow for transparent proxying through an application that would inspect the packets, and forward them on without any suspicion of any component in the communication.

If we observe a full TCP/IP Stack, we can identify the opportune moment to inspect the packets.

Application Layer
System Calls
IP Layer
Link Layer
Hardware

Traditionally, a packet to be sent by an application will be passed down to the Sys Calls, then IP, then Link. If we embedded in the Kernel somewhere between System Call and Link Layer, we could inspect any packet that is sent through the operating system without any interaction from the applications attempting to utilize it.

For instance, if we altered the system calls / libraries so that any packet that is send or received from any port or socket is either read through there or redirected through an inspection program, which then loops it back around or forwards it to the proper application.
Another possibility is to intercept any packets that move through the IP layer and do a similar process as before. This would produce similar results as before, and would be further from scrutiny and more transparent.