Example of a protocol vulnerability: ARP Cache Poisoning and man-in-the-middle attack
Review by Frank Fetters

This paper discusses a well documented class of attacks that is resurfacing due to the new networks which have both wireless and wired components. The paper explains numerous ways to attack these newly formed wire/wireless networks. The common weakness of all these attacks is that all the wireless access points are all connected to a hub or switch which are all susceptible to this class of ARP attacks. The main problem is that because the wireless access points act as hubs and switches, they connect to other hubs and switches and connect the two networks which allow intruders who previously wouldn’t have access to the wired network, access through the wireless network.

The paper then goes on to discuss a few different ways to prevent these attacks. The overall theme of these prevention methods is to separate the wired and wireless networks. This is done with either one large firewall, lots of individual firewalls, or by requiring vpn tunnels to communicate across.

The paper was very informative and clearly demonstrated a whole suite of attacks on the new wire/wireless networks which are becoming more prevalent. (our own university has begun implementing this ).

While the main focus was on the ARP suite of attacks, the main message of the paper was more of a warning for future application and device developers to take the extra time to revisit vulnerabilities that wired networks have had to deal with. It is the age-old advice to “measure twice, and cut once”. By reviewing and taking past vulnerabilities into consideration while designing new products, we can avoid having to go back and fix and patch and possible redesign the new products.