Introduction

We at Team PINC, with a combined 35 years in Silicon Valley devops and security software engineering, are very concerned about IoT security in the home. But not just because of today's devices--we worry as much (or more!) about what happens when devices are in use well beyond their vendor-defined "service life." While making sure that devices are kept up-to-date is a laudable goal, what happens when "up-to-date" is a codebase that hasn't changed in 5 years? 10? 20? A typical home user might get a PC or cell phone every 2-3 years, but they don't expect to replace their sprinkler controller nearly that often. Or their doorbell. Or their thermostat. Devices that are poorly-supported by their manufacturer (or fall out of service life) are *the* longterm threat--look no further than the recent WannaCry malware, which largely affected the no-longer-supported Windows 7, for proof of that!

For these out-of-service-life or poorly-supported devices, there is only one practical option: Containment.

The PINC Approach

PINC stands for **Persistent Internal Network Containment**. Unlike conventional home routers that protect the *inside* from the *outside*, PINC's goal is to sandbox *all devices inside* the home network so that they are protected from each other. As a result, they have as little exposure to malware vectors as possible, and their ability to do damage is contained should they fall victim to compromise. :

1. **Layer 2 Containment**. With PINC, every device is on its own little virtual network with limited access to the other devices in your home. Unlike conventional firewalls that act at higher layers, however, our Layer 2 firewalling technology means that devices needing low-level network access can still get it when appropriate--this is security without losing functionality!

2. **Per-Device Configuration, Baselining, and Reporting**. As a device joins the network, it is scanned against an open database of known devices. Network access is automatically configured according to known baseline behaviors, and an app running on your phone or tablet gets regular reports of out-of-date code, abnormal behavior, and other alerts.

3. **Being a Good Neighbor**. PINC includes a "Good Neighbor" protocol that negotiates with remote websites to shape its outgoing connection behavior. By being a Good Neighbor, you help keep your favorite websites from being attacked by the bad guys, and can help prevent outages as attacks happen.

Combining layer 2 containment with a user-friendly configuration and reporting system and the Good Neighbor Protocol, PINC not only meets the requirements of the IoT Home Inspector Challenge, but can future-proof your home against problems that don't exist yet!