# Better IOT Security

Hello readers,

IOT security is really network security 101. When embedded software devices touch networks that suffer vulnerabilities due to  weaknesses in the firmware, there are often layers of unmanaged or unmanageable  infrastructure within the network's topography, that can create serious complications for an administrator.

POCs include ATM's with vulnerabilities, XP system networks, and IOT devices that have have found their way into networks without any obvious firmware solutions to prevent the spreading of infection. Many companies are unaware of the situation and the ones that are aware are often met with blank stares when they ask about solutions.

## Solutions

Any embedded firmware devices should be updated whenever an available patch is present, but that doesn't make it safe. Use layered routing and common sense to keep IOT devices off of the ordinary internal network, and use Linux on/for the router if possible.

If your networked system is monitoring packets, and you read errors on any machine on the network, check every recent update, and packet capture log. If you see a high volume of unusual traffic going to an embedded system, investigate the cause. If you see an unusual level of data being sent from an embedded system, investigate the cause. If it's sending traffic all over the network, turn it off before investigating the cause.

Precautionary network security software isn't a solution, it's a tool that requires a user and even if it sends real time alerts can go wrong when left unattended due to specific exploits targeting such systems as part of an attack.

Courtesy of Gamer Forever

While the video isn't exactly the best use case for the scenario, the methodology is similar. RTOS type systems and other embedded systems make use of firmware updates but many allow those updates to be delivered without administration. This means that even a false firmware update type of attack may make some embedded systems vulnerable to foreign packet uploads through various means.

## Protecting SSH servers

CentOS has a document on a procedure that can help secure the SSH servers on your network, it's one of the more common methods. Likewise if you are using GitHub you can use scripts provided to limit ssh access.

As for PLCs and other networked hardware, you'll want to search case by case using the name

of the device and ultimately determine how you want to network it into the topography.

Home networks are just as likely to be affected between baby monitors and similar devices touching other networked devices directly via router, or indirectly through third party apps that allow a mobile device to interact with the home network through the device and the router by proxy.

Segregation of network layers is probably enough if your router isn't the weakest point of entry for now but be warned, countless routers are actually part of known botnets due to bad firmware. The same may be true for small businesses, and as such you should really look at securing your whole network from the standpoint of the attacker. While most homes don't need end to end encryption on their network, it becomes a real privacy issue to not at least secure your router.