MARCH 2017

# Protection of Home Networks

A SUGGESTED APPROACH

IAN LOE

# Table of Content

Introduction ..... 2
Background ..... 2
Problem Statement ..... 3
Recommendations ..... 4
  Network ..... 4
    Unified Threat Management ..... 4
    Use of Static IP ..... 5
    Use wired connections ..... 5
  Device Configurations ..... 6
    Change default settings ..... 6
    Disable WPS ..... 6
    Use WPA2-Enterprise for Wifi connection ..... 7
  Best practices for a secure environment ..... 7
    Use outgoing traffic monitors on your computers ..... 7
    Use 2FA for all online services ..... 8
    Browser in a container ..... 8
  Further enhancements to security ..... 8
Conclusion ..... 8

Ian Loe

DN: email=ian@ianloe.net
Date: 2017.03.04 14:59:40 +08'00'

## Introduction

With an increase in the number of Internet of Things (IoT) devices that most consumers have in their homes, together with the rise of cybersecurity threats, there is a need to further strengthen the defense of the home network.

In this paper, I will offer a practical approach to improving the security posture of the home network – both in terms of network deployment architecture and also good practices in the use of network connected devices.

I would be using fibre broadband in my examples but it would be no different for subscribers on ADSL or cable networks.

*This paper is written in the context of the typical Singapore home but can be adapted to fit any broadband connected home.*

## Background

Most homes in Singapore would have been wired for fibre broadband, with the residential wired broadband household penetration rate exceeding 100% as of June 2016 [1]. Many subscribers would have deployed their broadband equipment as installed by the service provider as shown in the example from SingTel below:

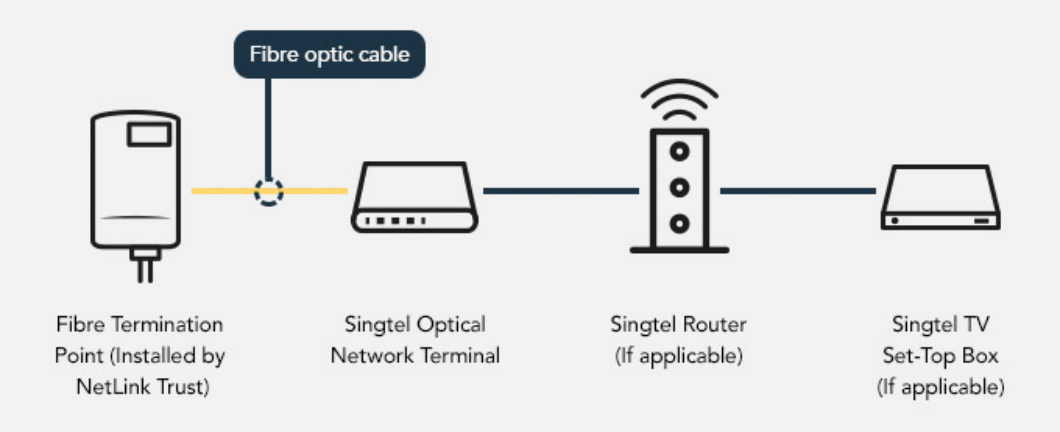


*Figure 1: Singtel fibre installation example*

[1] "Residential Wired Broadband Household Penetration Rate" measures the total number of residential wired broadband subscriptions as a percentage of the total number of households in Singapore, and excludes all wireless access plans (provided via 3G, 3.5G/HSDPA, 4G/LTE, WiMAX or its equivalent and Wi-Fi hotspots). Please note that this does not necessarily reflect the proportion of households with broadband in Singapore as some households subscribe to more than one broadband connection. For a more accurate figure, please refer to IDA's Household Survey findings.

There is a simple connection from the fibre termination point to the optical network terminal and to the router. From this point, almost everything is connected to the single router as can be seen in the Singtel Mio (ADSL) manual below:

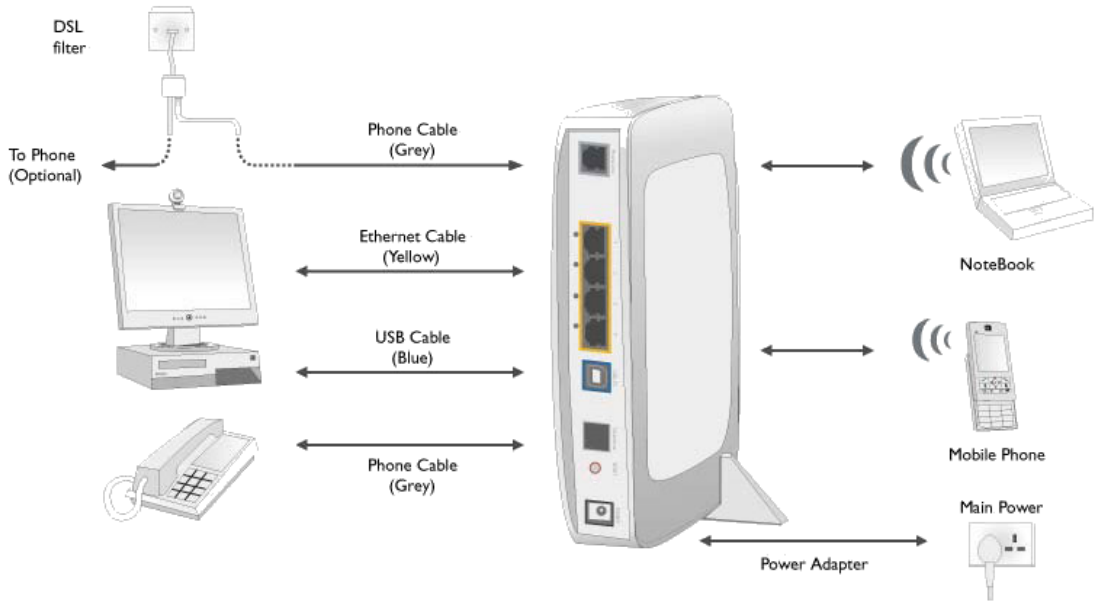


*Figure 2: Singtel Mio connections (from Manual)*

## Problem Statement

With a single network in the home, you are exposing your critical data (e.g. work, personal data, etc.) on your computers to other network connected devices in your home (e.g. TVs, media players, audio equipment, camera, etc.). These IoT devices typically have weaker security posture than your PC or tablets. The move towards building "Smart Homes" have added to this problem with many players rushing out devices with more emphasis on convenience over security. Big name vendors like Samsung are no exception, where a recent research has found that their "SmartApp" can be over-privileged. [2]

There is now a need to segregate your devices to minimise the security risk of the connected home. Beyond the network architecture, there are also configuration best practices that can help further improve the security posture of your home network.

Although many people think there might be nothing of value to protect in their network, your devices at home could still be hijack to be part of a bot army used in a DDoS attack as seen in the Mirai botnet incident.

[2] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. Security Analysis of Emerging Smart Home Applications In Proceedings of 37th IEEE Symposium on Security and Privacy, May 2016

## Recommendations

I would break the recommendations in 3 parts: network, device configurations and good practices to follow.

### Network

One of the first things to realise is that the home network is increasingly becoming more like a business network. Many people would do some work from home and have sensitive personal information stored on their local computers. We all know that most businesses have security appliances like firewalls and intrusion detection/prevention to secure their network, but few follow the same practices at home. Most people would cite the cost or complexity of implementation as a reason for not doing so.

Today, most consumers would spend hundreds of dollars on a high-end router to get maximum speed; the cost of these routers are not far from an entry level security appliance.

### Unified Threat Management

The Unified Threat Management (UTM)[3] device has been around for more than 10 years and is now a commodity item that is affordable to many. Using a UTM device can help restrict cyber-attacks with firewall settings, intrusion detection/prevention (especially over your wireless network) and also segregation of network in various zones.

A recommended approach would be to use the UTM device as the gateway to the internet and set up multiple zones within your environment as shown in figure 3.

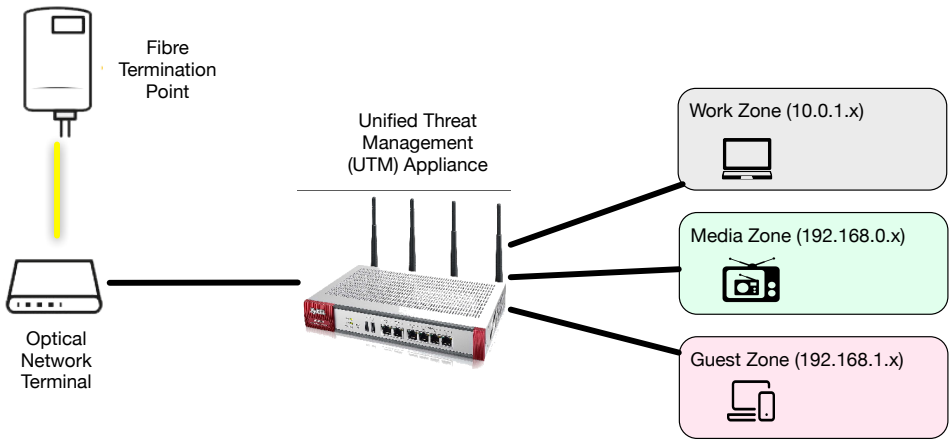


*Figure 3: Recommended network architecture for home*

[3] Unified threat management (UTM) or unified security management (USM), is the evolution of the traditional firewall into an all-inclusive security product able to perform multiple security functions within one single system: network firewalling, network intrusion detection/prevention (IDS/IPS), gateway antivirus (AV), gateway anti-spam, VPN, content filtering, load balancing, data loss prevention, and on-appliance reporting. - IDC. September 2007. Unified Threat Management Appliances and Identity-based Security: The Next Level in Network security. IDC Go-to Market Services.

The UTM device firewall should be set to allow only specific ports and destinations for all known applications. This would involve a bit of planning and understanding of your usage patterns. It is also recommended to create several network subnets to separate the devices based on security risk profiles; for example, a work subnet should be set at the highest security level with network ant-virus, anti-spam and intrusion detection. The trade-off would be the performance impact, but given the nature of the usage, this should not be very obvious to the end user.

With the increase in IP based media streaming (e.g. Netflix, Hulu, IPTV, YouTube, etc.) it is recommended that you use a dedicated media player to stream, rather than exposing your computer to malicious content. These media players can be attached to a media subset that would have lower security risk, thus a lower security settings could be used to allow better network performance. Firewall rules still have to be set to segregate this zone from the other zones.

Another good zone to have is a guest network where the access goes straight to the internet thus bypassing the internal network. This is important as you do not know the security posture of any guest devices (e.g. notebooks, phones, tablets, etc.) that can be a potential carrier for malware.

### Use of Static IP

Another good practice from the network perspective is to limit the use of Dynamic Host Configuration Protocol (DHCP)[4] in your network. Although DCHP is convenient, the devices in your home network is probably not going to change very often. Turning off DHCP and assigning Static IP can help reduce the attack surface and forces you to keep track of all connected devices in your network. One of the biggest problems in securing any network is not knowing what is connected to it, therefore having a clear catalogue of connected devices can help you perform a more effective audit of the network. The exception to this would be the guest network where DHCP should be used.

### Use wired connections

The use of wired connections can minimise the risk of network disruption by rogue application such as wifijammer[5] (https://github.com/DanMcInerney/wifijammer). This is a technique frequently used by attackers to force you off a legitimate access point onto a rogue access point set up by them.

[4] Dynamic Host Configuration Protocol (**DHCP**) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

[5] To "jam" WiFi (or any other form of radio communication), you basically blast out a lot of random noises on the frequencies that particular technology uses.

## Device Configurations

Many networks are breeched because of poor configuration of devices, the most obvious of which is leaving default values for names and passwords.

### Change default settings

By leaving your default device names and passwords, hackers would be able to tell a lot about your network devices. For example, most wireless routers and access points would have the manufacturer's name as part of the default SSID; with this information, hackers can check using the default passwords from the internet and gain access to your device. I would recommend changing the login user from the default "admin" or "administrator" to something unique and hard to guess to add another level of complexity.

Do not just click "Next" during the setup of any of your devices. Make sure you review the default settings carefully before making a selection, and use the security features for your device. If it allows you to set up a passcode lockout ("three strikes and you're out") and enable encryption, you can add another layer of protection to your device.[6]

### Disable WPS

Many modern routers and access points have Wi-Fi Protected Setup (WPS) to help connect devices with a push of a button. There are many problems with WPS which has been captured by Sophos in one of their blogs back in 2015:

> The first problem with WPS turned out to be the cryptographic protocol by which a client and a router convince each other they know the 8-digit PIN.
>
> Firstly, the eighth digit of the PIN is a check digit, computed from the first seven, so the PIN is effectively only seven digits long.
>
> Secondly, you prove you know the PIN in two stages (M4 and M6 above), each of which proves you know half of the PIN.
>
> Thirdly, the protocol terminates immediately if you make a mistake after M4, where you verify the first half of the PIN.
>
> In other words, once you have tried 12340000 and failed, you immediately know that every PIN from 12340000 to 12349999 is incorrect.
>
> You don't need 100,000,000 guesses to try every possible PIN (108, the quantity of different 8-digit numbers).
>
> You need 10,000 guesses (104) to lock in the first four digits of the PIN, plus 1000 guesses (103) to finish the job with the three variable digits in the second half.
>
> That makes a brute force attack just 0.01% as time-consuming as you'd expect, given 8 digits of PIN.

[7]

[6] The US FTC has a list of consumer recommendations for online security here https://www.consumer.ftc.gov/blog/what-you-need-know-secure-your-iot-devices

[7] Info from Sophos : https://nakedsecurity.sophos.com/2015/04/13/we-told-you-not-to-use-wps-on-your-wi-fi-router-we-told-you-not-to-knit-your-own-crypto/

### Use WPA2-Enterprise for Wifi connection

Most users would already know by now that WEP and WPA are not recommended as they can be compromised. Majority of users use WPA2-PSK with a pre-shared key, but this carries the risk of leaking the password from a single weakly protected device. The recommendation here is to use WPA2-Enterprise.

The Personal or Pre-Shared Key (PSK) mode of WPA2 does not provide adequate security. The encryption keys in WPA2-PSK are more vulnerable to cracking and static encryption keys are a problem when devices are lost or stolen.

The Enterprise mode of WPA2 gives you dynamic encryption keys distributed securely after a user logins with their username and password or provides a valid digital certificate. Users never see the actual encryption keys and they are not stored on the device. This protects you against rogue, lost or stolen devices.

There are many more reasons to use WPA2-Enterprise which can be found here: http://www.esecurityplanet.com/views/article.php/3907721/15-Reasons-to-Use-Enterprise-WLAN-Security.htm

One of the main barriers to using WPA2-Enterprise at home is the lack of access to a RADIUS server for the credentials. There are free open sourced solutions you can use to build and host it yourself or you can use a SaaS solution such as Ironwifi (http://ironwifi.com/ ) which provides a free service for 1 access point up to 10 users.

## Best practices for a secure environment

There are many good practices you can follow to further enhance your security posture and I will list a few which are easy to implement.

### Use outgoing traffic monitors on your computers

There are many solutions on the market that can help you monitor and block suspicious outgoing connections from your computer. For example, for the Apple OS X platform, there are "Hands Off!" (https://www.oneperiodic.com/products/handsoff/) and "Little Snitch" (https://www.obdev.at/products/littlesnitch/index.html). These products can alert you to outgoing traffic and you can grant or deny access per application. This would dramatically help in unintentional data leaks of your private information.

### Use 2FA for all online services

Most online services like web mail, file sharing, github, etc. would have the ability to add a 2nd factor authentication. I would recommend you use it. For higher security, you can consider using a FIDO[8] (Fast IDentity Online) U2F (Universal 2 Factor) token. Some of the benefits of using FIDO U2F are:

- Based on public key cryptography
- Keys stay on device
- No server-side shared secrets to steal
- Protects against phishing, man-in-the-middle and replay attacks
- Biometrics, if used, never leave device
- No link-ability between services or accounts
- No 3rd party in the protocol

### Browser in a container

This is a novel idea that can help prevent damage from malicious scripts in rogue or compromised websites, or accidently clicking on malicious links. The idea is to run your browser in a container. There are many online articles and virtual machines you can download to do this. The benefit of doing this is that in the case of a malware infection via the browser, the damage is contained within the container and can be recovered more easily. An example of a site that has instructions on how to do this is http://www.wikihow.com/Browse-Safely-Using-a-Virtual-Machine

### Further enhancements to security

There are many more advanced ways to secure your home network if you have advanced knowledge of other security domains like identity and access management where you can implement access right to various accounts to all your devices and applications. A good place to look is RCDevs (http://www.rcdevs.com/) where you can get the complete solution to either host it at home or on cloud services like Amazon.

## Conclusion

The world is no longer safe and your home network today is more vulnerable than ever. While the recommendations here are valid for today, there is a need to also evolve with the improvement in technologies and also the new threats that are surfacing each day. It pays to be vigilant and always audit your home network to make it is safe.

*Remember: Only the paranoid survive* ☺

[8] FIDO is the World's Largest Ecosystem for Standards-Based, Interoperable Authentication https://fidoalliance.org/about/what-is-fido/