Cyber Snapshot

Exploring and Assessing Current Topics

MICHIGAN CYBER COMMAND CENTER (MC3)

September 30, 2019
CS-06-2019

HOME NETWORK SECURITY & IOT DEVICES

OVERVIEW

The Internet of Things (IoT) refers to the billions of smart devices around the world which are connected to the Internet. Many of these devices consist of everyday electronic devices found in our homes and connected to a home network. These smart devices could include security cameras, doorbells, thermostats, appliances, lights, wearables, digital personal assistants (Alexa, Siri, Google), and many more. Due to the widespread adoption of IoT devices, our home networks and IoT devices connected to these networks have become prime targets for malicious actors. The MC3 is aware of numerous vulnerabilities related to these devices that can be exploited to compromise a system. Therefore, the MC3 recommends various home network security best practices to help mitigate the risk of falling victim to these attacks.

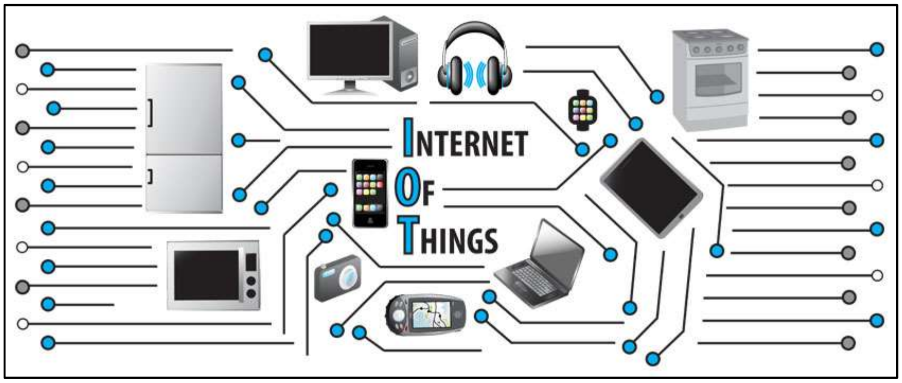


Image Source: NSA.gov

ENABLE WPA2-PERSONAL

Most of our homes' IoT devices are connected to the Internet wirelessly via a router. When setting up a wireless home network, it is important to enable some basic configurations and security features. For example, one of the best ways to secure a home network is by enabling the Wi-Fi Protected Access 2 Personal (WPA2-Personal) protocol. WPA2-Personal is a security method utilizing a password and provides strong data protection and network access control. It provides Wi-Fi users with a high level of assurance only authorized users can access their wireless networks. The older Wired Equivalent Privacy (WEP) protocol is not secure and should not be used.

ESTABLISH A BASELINE

Homeowners should become familiar with which devices are supposed to be connected to their network. Users can identify which devices are connected to their network by either checking their router's connected devices or utilizing a free tool or mobile application to scan their network for connected devices. Once these devices are identified, they can be used as a baseline to identify any new devices connecting to the network which do not belong. Whitelisting is an additional security feature which can be implemented. Whitelisting identifies allowed Media Access Control (MAC) addresses to help prevent any unauthorized devices from gaining network access.

SEGMENTATION

After completing a baseline of which devices should be connected to the home network, homeowners can take precautionary measures with IoT to mitigate security and privacy risks. One good way is by connecting IoT devices to a guest network. Most routers today can enable a guest network. Segmenting the home network with a guest network will allow personal devices to operate on one network and IoT on another. For instance, the kitchen appliances do not need to be connected to the same network as a home computer containing personally identifiable information. This will ensure personal data is segregated from IoT. If configuring a guest network isn't possible, setting up a second router specifically for IoT devices is recommended. Visitors who need access to your home Internet should only be given the guest network password.

UPDATE FIRMWARE

All IoT devices contain firmware. Firmware is the software that controls how a device behaves and is intended to operate. A common attack vector for malicious actors is to exploit outdated firmware on devices. Software developers are constantly writing updates and patches for vulnerabilities detected in the devices their company manufactures. Although these updates are made available to the users, many users neglect installing these updates. Neglecting to install updates leaves their devices vulnerable to an attack by a malicious actor taking advantage of a known exploit. Therefore, it is important to regularly check for updates on IoT devices and ensure these updates are completed.

CHANGE DEFAULT USERNAMES AND PASSWORDS

When a new device is connected to a home network, the device is often preprogrammed with a default username and password. Instead of changing these default usernames and passwords, many users opt for convenience and continue using the same credentials. At the same time, these generic usernames and passwords are easily accessible for anybody to find online and therefore give malicious actors easy access to those devices. It's highly recommended users change these default credentials.

COMMON USERNAMES

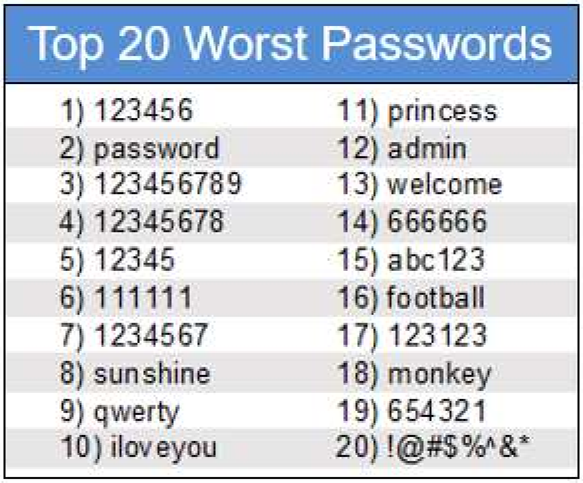
Admin
Administrator
Root
Test
Guest
Info
User

NETWORK DISCOVERABILITY

Homeowners should ensure their IoT devices aren't publicly accessible. Searches using Shodan and Censys may reveal the presence of exploitable devices on your network. Shodan and Censys are public search engines used for research of devices and networks publicly visible on the Internet.

USE STRONG PASSWORDS/PASSPHRASES

Generally, people use passwords containing a simple word or combination of letters, numbers, and characters that is easy to remember. Unfortunately, malicious actors have databases containing millions of these commonly recurring passwords. They can use these passwords to execute a brute force attack, which is an attempt to crack a password by using a trial-and-error approach, trying multiple passwords until the correct password is guessed. To reduce the possibility of a password being guessed, there are several best practices a user can follow. For example, a password should be at least 15 characters in length and should be a mixture of upper and lower-case letters, numbers, and special characters. Additionally, users may consider using a passphrase, which is a sequence of unique words combined. Passphrases are generally longer than passwords while at the same time being easier to remember. As a reminder, the same password should not be used for more than one account. A password manager can be utilized to help create and store complex passwords for individual accounts.



Top 20 Worst Passwords

1) 123456	11) princess
2) password	12) admin
3) 123456789	13) welcome
4) 12345678	14) 666666
5) 12345	15) abc123
6) 111111	16) football
7) 1234567	17) 123123
8) sunshine	18) monkey
9) qwerty	19) 654321
10) iloveyou	20) !@#$%^&*

Data Source: 2018 SplashData Report

RELATED INFORMATION

CS-03-19 - Password Security

Password Security 2019.pdf