I am putting a Raspberry Pi device on MITnet. What do I need to do to secure it?

Q: I am putting a Raspberry Pi device on MITnet. What do I need to do to secure it?

Answer

The Raspberry Pi device is, despite its size and form factor, a fully functioning computer. While it is easy to deploy an operating system onto an RPi and get started with all sorts of cool projects, the default settings for these operating systems can also be terribly insecure. If you are planning on putting an RPi on MITnet, please note the suggestions on this page and do as many as you can to ensure hackers don't take control of your RPi and use it for nefarious purposes.

These are just preliminary steps. There are further steps one can take to more thoroughly ensure the safety and security of your RPi. For further information, consider looking at: http://www.debian.org/doc/manuals/securing-debian-howto/

> If you only do one thing to secure your RPi, changing the default password will be the most effective in preventing an intrusion into your device.

Ways to Make Your Raspberry Pi More Secure:

Change the Default Username and Password

The password that comes with the default install of Raspbian is publicly available to anyone on the Internet. The default password is likely to be an attacker's first try on any attempt to hack your RPi.

Disable unused services (ftp, www, mysql, etc.)

From both a security and performance perspective, you want as little software running as possible, especially servers listening on open ports. Unless you have a specific need to do so, don't run servers like apache, samba, nfs, or mysql.

log login attempts, especially failed ones

If for some reason your device is compromised, logs may help ascertain how the intruder gained access and the extent of the damage.

Firewall/IPS software, e.g. iptables and fail2ban.

A properly configured firewall will prevent services which need to run from being exploited by outside attackers. For example, a device being used as part of a robotics project on campus may not want or need SSH connections being initiated from outside of MITnet. IPTables can be configured to block connections from sources you aren't expecting them to come from.
Fail2ban is a program that monitors attempts to log into a device and, after a set number of failed attempts, instructs IPTables to block the source of the brute force login attempts. It is a valuable tool to prevent a persistent, targeted, brute force attack against your RPi from succeeding.

update the OS regularly

The operating system itself may be the source of security vulnerabilities being used by hackers to compromise your device. Ensuring you are up to date with the latest version of the OS is the best way to avoid this problem. Raspbian can be configured to run updates automatically using the **cron** and **cron-apt** tools.