Home

DDoS

A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a [denial of service](https://searchsecurity.techtarget.com/definition/denial-of-service) for users of the targeted resource. The flood of incoming messages, [connection](https://searchnetworking.techtarget.com/definition/connection) requests or malformed [packets](https://searchnetworking.techtarget.com/definition/packet) to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack

Why this is concerning?

This is concerning because it means the attacker has access to the devices that are infected and the hacker could try to gain access to your network that way. For the most part DDoS infected devices will not change the activity they are meant to do. The device might be slightly slower but for the most part it is an undetectable difference. It is possible to the access to the network through one infected device

<https://internetofbusiness.com/ddos-attacks-double-iot-target-corero/>

How to prevent this

The best way to prevent is to

* Reboot your device regularly some malware will be uninstalled in the reboots.
* Make sure all factory passwords have been reset, to something that is secure.
* Change the password regularly

Cons

The cons are that if each device had its own unique password depending on the number in the home it would be hard to keep track of them. Not all devices have the capabilities to have the password reset. Also it is easy to forget to reboot or not know how frequently to do it, also it might not get rid of every virus. It is hard to keep track of multiple passwords then when you have to change them it can get very difficult to remember. The cost for these solutions is medium because the you the homeowner has to remember to reboot the IoT devices. You would also have to keep track of all passwords for the devices and not make them obvious which can be difficult.

Ransomware

Ransomware is a type of [malware](https://techterms.com/definition/malware) that prevents you from using your computer or accessing certain [files](https://techterms.com/definition/file) unless you pay a ransom. It often [encrypts](https://techterms.com/definition/encryption) files so that they cannot be opened.

<https://techterms.com/definition/ransomware>

Why is this concerning

House hold are targeted because it is likely that homeowners will pay because devices are expensive. The hackers are likely to sure make the ransom money is reasonable for the device that it makes more sense to pay than buy a new one. If that ransom is not payed all of the data will be deleted from the devices or the hackers could change all of the settings of the device.

<https://www.acronis.com/en-us/blog/posts/ransomware-forecast-2018-expect-cars-homes-medical-equipment-and-wearables-be-targeted>

How to prevent this

The best way to prevent this is to make sure that it is as hard as possible to access your devices.

* The passwords are strong and unique for each specific device.
* Make sure it is not possible for devices to download off of the internet and that it will only send and receive data to trusted devices.

Cons

Ransomware is a tricky attack because once it gets in your device will be encrypted and there is nothing you can do but pay or get new devices. All defenses are about keeping out the virus because if it gets in then it is too late. The cons to these approaches are that if each password is strong and unique then all of the making sure all the people in the household know the correct password to each device can be complicated. Also if the device cannot download anything then it might not be able to download updates if they come out. The cost these approaches is low because it is not hard to have secure passwords. It is an inconvenience to not have the newest update but it is safe over all.

Man-in-the-middle

In cryptography and computer security, a man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. https://en.wikipedia.org/wiki/Man-in-the-middle\_attack

Why this is concerning

Man-in-the-Middle is dangerous because if the data is not encrypted on the IoT device before it is sent elsewhere then the hacker could read all the data being sent. Devices can give away information that by itself doesn’t seem to important but there are sophisticated algorithms that can draw very accurate conclusions from the data that would not be expected. It is also concerning because once the hacker has access to the network they can cause other problems as well.

https://www.scmagazineuk.com/billions-bluetooth-devices-vulnerable-mitm-attacks-no-user-action/article/1474116

How to prevent this

Best way to prevent man-in-the-Middle is to make sure that the network that device is communicating over is secure.

* Make sure the network is encrypted and that all devices have encryption running on them. If the data is encrypted it would protect against what the hacker can see.
* Run scans of your network to be sure that only authorized devices are accessing it.

Cons

The cons with that is that if your devices do not come with encryption then you cannot add it onto them. It is also hard to detect if there is someone monitoring the communications between devices. If you are going to scan your network you have to be sure that you know the devices that are supposed to be on the network. It is important to keep track of old devices that are connected also. The cost of this could be high if you don’t already have a way to scan you network for vulnerabilities. It is important to be sure that your network is secure and there is no virus or person on it that shouldn’t be.

Spoofing

Spoofing refers tricking or deceiving computer systems or other computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet.

<https://techterms.com/definition/spoofing>

Why this is concerning

If there is a clearly open door onto a network such as an insecure IoT device then it is not hard to convincingly masquerade. Therefor it would be a very easy way for an attacker to gather data or send out data without anyone being aware something is wrong with any of the devices.

https://www.iotforall.com/iot-security-concerns-preventing-iot-hacking/

How to prevent this?

The best and most reasonable way is to

* Configure the setting of your router so that it blocks connection requests from outside your network to the IoT device. Make sure that only will connect with request that originate from within your network.
* Make sure the encryption on your router is on so it will encrypt everything and only trusted devices will have a decryption key.

Con

The con with these approaches is that you have to be sure that you know what you are doing. It is possible to change the settings of your router but you have to be sure that you are changing the correct settings. The cost to this is medium because you would have to spend some time researching how to do everything properly so that nothing gets messed up.

Physical Tampering

When a hacker is able to access your device in person and tamper with it, possibly adding malware to it. Once an attacker has physical contact to a device it is very easy for them to download malware on to it. Most devices aren’t equipped to prevent against remote attacks much less physical tampering ones.

Why is this concerning?

Because with these viruses the creator doesn’t have to worry about how to get into the device remotely the entire attack is focused on infecting the device and accomplishing the goal that the creator has in mind. With viruses like that it is easier to make them more malicious because they are custom made to be in your specific environment. This is also concerning because to access most of your IoT devices the attacker is in your home. Once someone gains physical access to your devices it has all kinds of information on you and your activity while home.

<https://danielelizalde.com/iot-security-hacks-worst-case-scenario/>

How to prevent this

To prevent this the easiest way would be

* Physical tampering is easier and harder because you have to physically access the device which can be a lot of work but once the hacker is at the device it is relatively easy to access it.
* Be sure that once the IoT devices are updated and newer models replace the old ones are removed. The older IoT devices that are still connected to the network are weakness.

Cons

If a hacker has risked breaking into your home to access you IoT device it will be very difficult to stop them. If they want to gain information from the devices or downloading malware onto the devices. Most networks have a lot of very weak entry points it is just a matter of finding the correct one. The cost of these solutions is high because it is about being sure that all devices being used are the most secure models which can be more expensive.

Eavesdropping (Remote recording)

Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, videoconference or fax transmission

<https://searchfinancialsecurity.techtarget.com/definition/eavesdropping>

Why is this concerning

This is concerning because through this method of hacking it is possible to gain a wide range of information from the people living in your house. It’s possible to also talk through the device if someone gains access to it. There have been cases where the hacker has talked to a child through baby monitors. It is important to protect devices that have microphones and speakers because of what a hacker could over hear or who they could be talking to.

<https://www.csmonitor.com/Technology/2015/0731/Are-Internet-connected-devices-eavesdropping-on-our-conversations>

How to prevent this

With these types of devices it is very easy to connect to the microphone and speaker

* Make sure that the Bluetooth access to these devices if off or that the settings on it are very restricted.
* Make sure all passwords associated with the device are changed regularly and are secure.

Cons

The cons to this are that you will not be able to use the Bluetooth on the devices which add a level of ease. It will still be possible to gain access to the microphone using other hacking techniques. If the password is changed regularly it is hard to remember and sometimes not secure. The cost of this is low because it is easy to turn off Bluetooth and it is only a slight inconvenience to not have the Bluetooth on constantly.

Trust Between devices on the same network

When a device is automatically connected to others and trusted because it is on the same network. The network assumes the devices that are on it are secure and will allow connections automatically.

Why is this concerning

This is concerning because this is how viruses can spread through a system. It can infect one device and because the IoT devices tend to communicate with each other it spreads. When they connect and send data back and forth if the virus can attach to the data. Or send out a packet with the virus on it. With this method of spreading to devices it is possible to infect all of the devices in the office in a relatively short amount of time. From there it is also possible to spread on to the computers depending on the sophistication of the virus.

How to prevent this

The best way to prevent this,

* Get rid of old IoT devices to stop having obvious entry points to your network.
* Also reboot the devices regularly that way if a virus enters one of your IoT devices the rebooting it could get rid of the malware.

Cons

The cons of this is remembering about all of the old devices you have when you possibly bought the house with them already in it. When there are devices you have forgotten about they are a very easy way to infect one device so getting rid of old devices. Then make sure that all password on devices are secure and unique. The cost of this is low because it is not hard to do either of the suggestions they are simple good solutions.