

11.1 Assignment Overview Suggested Answers



11.1.1 Class Task Risk Identification – Suggested Answers

- Individually or in small groups:
- Think of as many realistic cyber security threats as possible that your home network might face.
- Explain your answer.
- Present your findings to the group.
- **Time allowed: 15 minutes.**

Threat	Probability	Size	Risk	Justification
Accidentally downloading a virus from the internet				
Failure of any network device (e.g., router, switch or Wireless Access Point)				
Denial of Service Attack Against the Internet Connection				



Denial of Service Attack Against the network				
Man In The Middle Attack				
Infection with a virus from a plugged in USB stick				
Infection with ransomware				
Infection with Malware				
Infection with Spyware				
Failure of the Internet Connection				
Phishing attack				
Connecting an Internet of Things device and not changing the default password				
Having no WPA/ WEP encryption on the Wi-Fi SSID				



Connecting a mobile device (phone or laptop) already infected with a virus				
External network cables being damaged				
House being burgled and devices stolen				
Power failure to house				
Router passwords compromised				
DHCP server failure on the router				
DNS failure				



11.1.2 Class Task Risk Assessment– Suggested Answers

- Individually or in small groups:
- Using all the threats you identified in the previous slide, identify the severity of the threat using the severity matrix.
- Explain your answer.
- Present your findings to the group.
- **Time allowed: 20 minutes.**

Threat	Probability	Size	Risk	Justification
Accidentally downloading a virus from the internet	Very Likely	Major	Extreme	People at home might not be aware of the threats posed from viruses on the internet and access a malicious website and consequently download a virus
Failure of any network device (e.g. router, switch or Wireless Access Point)	Very Likely	Major	Extreme	If a network device fails, then no device (phone, laptop, printer, TV, media streamer) can connect to the network and therefore will be unable to carry out it's function. Streaming TV and music will be unavailable, computers will not get updates or be able to backup data. This would result in a failure of the entire network.
Denial of Service Attack Against the Internet Connection	Unlikely	Moderate	Low	This would mean the home router being flooded with packet requests resulting in any outbound internet connections being queued. This would result in a loss of the internet connection but all devices internal (or local) to the network would still be able to communicate with each other.



Denial of Service Attack Against the network	Unlikely	Major	medium	This would require the attacker to know the SSID and WEP/ WPA-2 password for the Wi-Fi or for the Wi-Fi network to be public, the attacker to be able to join the network and flood the network with packets. This means that genuine traffic between network devices would be slowed dramatically. Any devices using a wired connection would be unaffected, unless the attacker was able to access the router using its public IP and then use NAT to identify the private IP's of the connected devices and ping the router with packets containing these IP addresses.
Man In The Middle Attack	Likely	High	Medium	If an attacker were to access a router in between the home network and a remote device, it would be able to identify any unencrypted traffic between devices. This would only be an issue if any sensitive data (e.g. usernames and passwords) were being transmitted over HTTP, which given the nature of the home users is likely.
Infection with a virus from a plugged in USB stick	Very Likely	Major	Extreme	Home users are still likely to move data from School/ College/ Work to their home network using USB sticks. The chances of one of these picking up a virus from the remote location is very high.
Infection with ransomware	Very Likely	Major	Extreme	Given the nature of the attack, should any device be infected with ransomware, the only way to unencrypt the data would be to pay the ransom. If this is high and payment cannot be made, then all data on the infected network device is lost.
Infection with Malware	Very Likely	Minor	Medium	Given the nature of the attack, should any device be infected with malware, the impact will depend on the nature of the malware, which could vary between irritating popups to the deletion of all network data.
Infection with Spyware	Very Likely	Major	Extreme	Given the nature of the attack, should any device be infected with spyware, and given the general nature of the home users, spyware will be able to identify any usernames, passwords or bank details used for home shopping or banking, as well as login passwords to the network.



Failure of the Internet Connection	Very Likely	Low	Medium	<p>If the internet connection fails, then no device (phone, laptop, printer, TV, media streamer) can connect to the internet and therefore will be unable to carry out its function. Streaming TV and music will be unavailable, computers will not get updates or be able to backup data. The local network would still function as devices would be able to connect to each other.</p>
Phishing attack	Very Likely	Major	Extreme	<p>Given the nature of the attack, should any user receive a sophisticated text or email phishing attack that contains images and text designed to mimic a real email, and given the general nature of the home users, the attack could force users to login to a fake website and so be able to identify any usernames, passwords or bank details used for home shopping or banking, as well as login passwords to the network.</p>
Connecting an Internet of Things device and not changing the default password	Very Likely	Major	Extreme	<p>If an IOT device password has not been changed, it is possible for an attacker to take control of this device and use it against its owner. An IoT device can receive HTTP requests from any device that knows its password, as well as issue HTTP responses.</p> <p>The device can be used to launch a DoS attack to another device by sending HTTP responses to that device, or an attacker can take over the IoT device (e.g. a camera or TV) and use it to spy on (using audio or video) the occupants of the house</p>
Having no WPA/ WEP encryption on the Wifi SSID	Unlikely	Major	Medium	<p>Having no security on the Wi-Fi Network means that the network is visible to the public and anyone can connect to it. This means that an attacker can use the home Wi-Fi to download illegal material to their own device using an IP address given to it by the router, so it looks like the material was downloaded to the network not the attacker. Also, once inside the network an attacker could compromise the network.</p>



Connecting a mobile device (phone or laptop) already infected with a virus	Very Likely	Major	Extreme	Home users are very likely to connect their mobile device to the home network to take advantage of the faster speeds offered by home Wi-Fi rather than using mobile data. The chances of one of these devices picking up a virus from a remote location and infecting the network is very high.
External network cables being damaged	Unlikely	Moderate	Medium	If an attacker were to damage the broadband cables to the house, the internal network would continue to function, but no internet connection would be available. If any security cameras required the internet to notify the homeowner of an intrusion by email or HTTP then although the cameras would still function, they could not notify the occupiers that a burglary was taking place or record the video to the cloud.
House being burgled and devices stolen	Unlikely	Extreme	Medium	Theft of devices results in a total loss of data if there is no cloud-based backup. If there is a local network storage backup, it is hoped that these are not stolen either.
Power failure to house	Unlikely	Extreme	Medium	If there is a power failure, the router will lose power and therefore no device (phone, laptop, printer, TV, media streamer) can connect to the network and therefore will be unable to carry out its function. This would result in a failure of the entire network. In addition, any computers that are on and not running on a battery would lose any unsaved data. Devices running on a battery (laptop, phone) would continue to function while there is power to the device.
Router passwords compromised	Likely	Major	Extreme	If an attacker gains full admin rights to the router, the attacker can implement MAC filtering on the router, only allowing devices with a specific MAC address to connect to the network. This means that all current network devices can be locked out of the network and the attacker now has full control. In addition, the attacker could change the admin password of the router so that nobody can browse to the router and regain control of the router.



DHCP server failure on the router	Likely	Major	Extreme	Failure of the DHCP server means that should any new device within the network restart or reboot, it will be issued with a default IP address that will not match the NETID of the home network, meaning that devices cannot connect to the network or the internet.
DNS failure	Likely	Moderate	High	Failure of the network DNS server means that any HTTP requests to any website will not be resolvable into their IP addresses and so while the home network will continue to function, internet access will be lost, unless websites are accessed via their IP addresses directly.



11.1.3 Class Task Identify the Protection Measure – Suggested Answers

- Individually or in small groups:
- For each of the threats identified in the previous exercise, identify the protection measure you would use
- Explain your answer.
- Present your findings to the group.
- **Time allowed: 20 minutes.**

Threat	Protection Measure
Accidentally downloading a virus from the internet	<ul style="list-style-type: none">• Do not go onto sites know to be compromised• Do not open attachments on emails or texts that look suspicious• Do not open any links in emails that have been moved to your junk or spam folder• Have a legitimate copy of antivirus software installed on your computer• Make sure the antivirus software virus definition database is up to date• Running periodic full scans and regular heuristic scans of your device• Enable web lookaheads and live monitoring of your device by the antivirus software



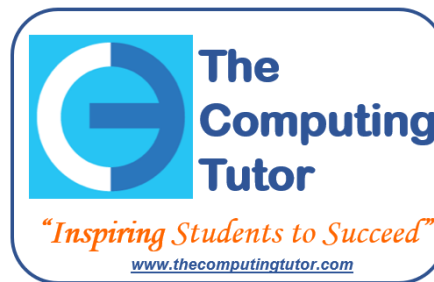
Failure of any network device (e.g. router, switch or Wireless Access Point)	<ul style="list-style-type: none"> • Give the router time to reboot • Connect the router to an Uninterruptible Power Supply in case of power failure • Have a backup router, switch or WAP ready in case of failure
Denial of Service Attack Against the Internet Connection	<ul style="list-style-type: none"> • Disable the internet connection until the attack stops • Notify your ISP immediately
Denial of Service Attack Against the network	<ul style="list-style-type: none"> • Install a firewall and monitor for inbound traffic, block the IP addresses of the attacker • Change the Wi-Fi password to a new, strong password • Change the SSID of the network • Enable MAC address filtering on the router, only allowing devices with a known MAC address to connect to the network • Restart the DHCP server and issue new IP addresses to all connected devices
Man In The Middle Attack	<ul style="list-style-type: none"> • Use a VPN for all external traffic • Ensure that any web communication that involves transmission of sensitive data is encrypted and is using HTTPS
Infection with a virus from a plugged in USB stick	<ul style="list-style-type: none"> • Have a legitimate copy of antivirus software installed on your computer • Make sure the antivirus software virus definition database is up to date • Running periodic full scans and regular heuristic scans of your device • Enable web lookaheads and live monitoring of your device by the antivirus software • Configure the antivirus software to automatically scan any USB device plugged into a computer
Infection with ransomware	<ul style="list-style-type: none"> • Have a legitimate copy of antivirus software installed on your computer • Make sure the antivirus software virus definition database is up to date • Running periodic full scans and regular heuristic scans of your device



Infection with Malware	<ul style="list-style-type: none"> • Have a legitimate copy of antivirus software installed on your computer • Make sure the antivirus software virus definition database is up to date • Running periodic full scans and regular heuristic scans of your device
Infection with Spyware	<ul style="list-style-type: none"> • Have a legitimate copy of antivirus software installed on your computer • Make sure the antivirus software virus definition database is up to date • Running periodic full scans and regular heuristic scans of your device
Failure of the Internet Connection	<ul style="list-style-type: none"> • Reboot the router • Notify your ISP technical support immediately
Phishing attack	<ul style="list-style-type: none"> • Do not open attachments on emails or texts that look suspicious • Do not open any links in emails that have been moved to your junk or spam folder • Educate all technical inexperienced network users on what modern phishing emails look like
Connecting an Internet of Things device and not changing the default password	<ul style="list-style-type: none"> • Do not connect an IoT device • Change the IoT device password to a unique, strong password immediately
Having no WPA/ WEP encryption on the Wifi SSID	<ul style="list-style-type: none"> • Enable WPA2, WEP encryption • Add a new, strong password – ensure all Wi-Fi enabled devices can connect
Connecting a mobile device (phone or laptop) already infected with a virus	<ul style="list-style-type: none"> • Have a legitimate copy of antivirus software installed on your computer • Make sure the antivirus software virus definition database is up to date • Running periodic full scans and regular heuristic scans of your device as well as the infected device
External network cables being damaged	<ul style="list-style-type: none"> • Ensure external cables are shielded in thick cable protection where possible • Make sure external cables are hard to access



House being burgled and devices stolen	<ul style="list-style-type: none"> • Make sure devices are shut down at the end of the day • Make sure each device has a strong password so that if stolen a thief cannot gain access to the data • Try to make sure devices are hidden from view • Ensure all doors and windows are locked when the house is empty
Power failure to house	<ul style="list-style-type: none"> • Ensure all critical devices are connected to a UPS (Uninterruptible Power supply) • Make sure critical data is saved and backed up on a regular basis • Enable cloud-based backups
Router passwords compromised	<ul style="list-style-type: none"> • Ensure router password changed from factory default • Make sure new router password is very strong • Turn off router and all other devices connected to the network • Notify ISP immediately
DHCP server failure on the router	<ul style="list-style-type: none"> • Reboot router • Issue all devices with fixed IP addresses not using DHCP • Have backup router with working DHCP
DNS failure	<ul style="list-style-type: none"> • Use public DNS like Google (8.8.8.8) which is always available



No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the TheComputingTutor

All text copyright © TheComputingTutor 2020. All rights Reserved.

