**Information Security**

**Chapter 1: Cybersecurity and the Security Operations Center**

1. **Lab 4 - Understand Vulnerabilities of Wireless and Other Common Technologies**

**Objectives**

Understand vulnerabilities of wireless and other common technologies.

**Background / Scenario**

Nearly every “secure” system that is used today can be vulnerable to some type of cyberattack.

**Required Resources**

PC or mobile device with internet access.

**Instructions**

* + 1. Click on the below links and watch the videos.

[How hacking actually looks like](https://www.youtube.com/watch?v=jTIUgshJjds)

[Pegasus: the spyware technology that threatens democracy](https://www.youtube.com/watch?v=G7H9uo3j5FQ&t=9s)

["I Remove It Before Using The Phone!" Edward Snowden](https://www.youtube.com/watch?v=0dGqR4ue8dg)

[Top hacker shows us how it's done](https://www.youtube.com/watch?v=hqKafI7Amd8&t=777s)

* + 1. Choose one of the hacks discussed in the videos and use your favorite search engine to conduct some additional research on the hack.
    2. For the hack chosen in Step 1b, answer the questions below. Be prepared to share your work in a full class discussion.

## Answer the following questions.

Questions:

* + 1. What is the vulnerability being exploited?

A vulnerability is the weakness that can be exploit by the cyber criminals to gain ones data illegally. Pegasus is a spyware developed by Israeli cyber arms company NSO. When the spyware is inside in your mobile or pc it do anything it wants without even being noticed. It can know what you are typing in your messenger and to whom you are talking to. It can even turn on your microphone or camera. This spyware has been used for targeted surveillance of journalists, human rights activists, and political dissidents.

Pegasus exploits zero-day vulnerabilities, which are security flaws in software that have not yet been discovered or fixed. The spyware is designed to take advantage of these vulnerabilities to gain access to a target's device, bypassing its security features.

* + 1. What information, data, or control can be gained by a hacker exploiting this vulnerability?

By exploiting zero-day vulnerabilities in a target's device, a hacker using Pegasus spyware can gain access to a wide range of sensitive information, data, and control. This can include:

* Personal information such as contacts, emails, text messages, and call logs
* Location data, including GPS coordinates and information about the target's movements
* Audio and video recordings made by the device's microphone and camera
* Passwords and other sensitive information stored on the device
* The ability to install additional malware on the device or remotely control it

In essence, by exploiting zero-day vulnerabilities, a hacker can gain complete access to and control over a target's device, allowing them to gather a wide range of sensitive information and potentially use that information for malicious purposes.

* + 1. How is the hack performed?

# The exact method of how Pegasus is delivered to a target's device can vary, but it typically involves tricking the target into clicking on a malicious link or opening a malicious attachment, which then infects the device with the spyware. The link or attachment may be disguised as a legitimate message or update, making it more likely that the target will click on it.

# Once installed on the target's device, Pegasus takes advantage of zero-day vulnerabilities in the device's operating system and other software to gain access to sensitive information, data, and control. The software can also install additional malware and remotely control the device, allowing the attacker to continue to gather information and control the device even after the initial infection.

# It is important to note that Pegasus is a highly sophisticated piece of spyware that is primarily used by government agencies and other organizations with significant resources. The average individual is unlikely to be targeted by Pegasus, but it is still important to be cautious when opening links and attachments from unknown sources and to keep your devices and software updated to protect against known vulnerabilities.

* + 1. What about this particular hack interested you specifically?

I am really wonder how the spyware exists inside a device without being even noticed. It is really amazing and very risky at the same time. One can do anything using such spywares.

* + 1. How do you think this particular hack could be mitigated?

Mitigating the risk posed by the Pegasus spyware and similar hacks involves taking a multi-layered approach to security. Some of the key steps that can be taken to reduce the risk of being targeted by this type of attack include:

* Keeping software and operating systems up to date: Software vendors often release patches for known vulnerabilities, and updating to the latest version can help protect against exploits that target these flaws.
* Avoiding suspicious links and attachments: Be cautious when opening links and attachments from unknown sources, as these can be used to deliver malware like Pegasus to your device.
* Using anti-malware and antivirus software: Installing and regularly updating anti-malware and antivirus software can help detect and remove malware, including spyware like Pegasus, from your device.
* Practicing good security habits: Simple security habits like using strong passwords, enabling two-factor authentication, and backing up important data can help protect against a wide range of threats, including those posed by spyware like Pegasus.
* Staying informed: Keeping up to date on the latest threats and vulnerabilities can help you better understand the risks and take steps to protect against them.

It's also important to note that while these steps can help reduce the risk of being targeted by Pegasus and similar spyware, there is no guarantee of complete protection. The use of zero-day vulnerabilities and sophisticated tactics make these types of attacks particularly difficult to defend against. However, by taking a multi-layered approach to security and being cautious when using your devices and software, you can significantly reduce your risk of falling victim to these types of attacks.