Video Response Scripts

Question 1:

Define confidentiality, integrity, and availability, i.e., the goals of security. Describe an example of attacks that violated each of these properties. In particular, your examples should be from real events (e.g., Stuxnet, Snowden leaks, etc.) and your slides should include links to appropriate sources.

When discussing the goals of computer security, we are addressing three important aspects of any computer-related system: **confidentiality, integrity, and availability.**

**Confidentiality, also referred to as as secrecy or privacy,** ensures that computer-related assets are accessed only by authorized parties. Meaning, only those who should have access to something will get that access.

An example of an attack that violated this principle would be the recent breach of T-Mobiles security, which gave hackers unauthorized access to the records of over 50 million of T-mobiles customers.

https://www.wsj.com/articles/t-mobile-hacker-who-stole-data-on-50-million-customers-their-security-is-awful-11629985105

**Integrity** means that assets can be modified only by authorized parties or only in authorized ways. In this context, modification includes writing, changing, changing status, deleting, and creating.

An example of a data integrity breach would be when the US & Israel used Stuxnet malware to infiltrate an Iranian nuclear refinery. The malware modified programs running the facility and caused a shutdown.

https://spectrum.ieee.org/the-real-story-of-stuxnet

**Availability** means that assets are accessible to authorized parties at appropriate times and those parties should never be prevented from accessing those assets.

An example of an attack on availability would be when “lizard squad” used a DDOS attack on Sony’s playstation newtork in 2014 which left it’s internet service for its gaming consoles down for more than a day.

https://variety.com/2014/digital/news/why-hackers-took-down-sonys-playstation-network-1201289668/

Question 2:

Wu and Lu describe CVE-2019-12819 as an example of a Hypocrite Commit in Section II.C of "On the Feasibility of Stealthily Introducing Vulnerabilities..." However, their description is a bit hard to understand, and I think you can do better. Please define the concept of a Hypocrite Commit and explain why this patch is an example of one.

A hypocrite commit is a patch of code which is less than 30 lines and appears to fix small issues in a given OSS codebase. However, it instead opens the doors of the immature vulnerabilities or absent conditions already found in the greater codebase and creates an actual vulnerability by linking them together.

This stealthy technique can get past the eyeball test of any single validator in the OSS community because the chances are extremely low that one person can have knowledge of all immature vulnerabilities or absent conditions spread throughout the codebase. For this reason, hypocrite commits can be an incredibly effective way to stealthily introduce vulnerabilities to large OSS codebases such as Linux.

The patch introduced by Wu and Lu in their “On the feasibility of stealthily introducing vulnerabilities” research study into Linux is an example of a hypocrite commit. This is the case because it’s less than 30 lines of code, appears to fix a common reference count leak, but creates a new vulnerability by exploiting an immature vulnerably already found in the codebase.

The patch of code does this by using a function called put\_device() to implicitly free memory when the reference count of an object reaches zero. However, with this common error a dedicated system function is called, which then once again frees the same memory, creating what is called a user-after-free vulnerability.