Afeefah Manzoor

Northern Virginia Community College

Babur Kohy

Nick Pesce Presentaion Writeup

On April seventh, Nick Pesce gave a presentation on CWE’s known as Common Weakness Enumeration. Nick Pesce graduated from Philadelphia Community College with an Associates Degree. Mister Pesce worked with the Bell Systems and designed circuits while he went to school at night and received a bachelor’s degree from Spring Garden college in Information Technology, later he received his MBA in finance from Saint Joseph University and a master’s in management of technology from Stevens Institute. After working in telecommunications for twenty-five years and received early retirement. Now, Mister Pesce has been working at Mitre for the past seventeen years.

The presentation Mister Pesce gave covered the Common Weakness Enumeration, or CWE, and other ways companies and developers can try to catch any weaknesses in their applications before they deploy them and into their systems. When industrial applications can be used by over thousands of users, it is important for developers and companies to make sure that they have minimal exploits since attacks are happening all the time, and adversaries will go after everything. Companies want some sort of insurance and currently insurance companies do not offer insurance plans for the cyber world, the only thing security professionals can do is to try to mitigate these attacks.

The recent SolarWinds attack that happened early in 2020 by the adversaries hacking into one of the many servers that deploy patches. The adversaries were able to hack into the system and inject a malicious code in the patch and when the patch was deployed, it in turn infected many large companies such as Zoom and Twitter. A software that could help prevent vulnerable applications and softwares to be prevented from being installed with malicious code in them is FireEye. FireEye takes the application or software, then places into them a container and tries to explode the application. This is done by the FireEye software trying to find any and every possible vulnerability in a secure container, so it does not mess with the already established company cyber ecosystem. Some types of weaknesses that are looked for include backdoors-which are placed by developers and sometimes forgotten to be taken out, Denial of Service attacks- which flood the applications with many applications at the same time to make the system vulnerable, Direct Access Attacks that flood the applications with packets to make the system vulnerable, if there is a possibility to eavesdrop, if privilege escalation is possible, spoofing, or other malwares are hidden in the application or software.

Common Weakness Enumeration(CWE) helps determine if the software is secure since it is a list of common weaknesses that are identified by industry across the world and maintained by Mitre. CWE’s currently have over two hundred common weaknesses that have been discovered and cover both hardware and software. They update the CWE lists whenever industry professionals identify another common weakness. The CWE lists also have documented who submitted and when these new weaknesses are identified and are used during the development phase. If a developer wants to check that their software does not anything from the CWE lists then they can either look manually through the over two hundred long weaknesses list or buy a software to do it for them.

When developing software many developers like to have a backdoor since it is much easier to work with and patch the system, but it can cause many issues, like an adversary gaining access, if it is not removed before the application or software is deployed. With so many different weaknesses there are, it will be a lot easier and more thorough to have a tool to look through the code and see if any of the common weaknesses can be found in it. Currently there are two types of these softwares, one is a static tool which will list potential areas that will need to be checked by the developer, the other one is a dynamic tool that will run the code and looks at every area as well as will try every possible outcome to check if there is proper error detection. The question that I asked Mister Pesce is that when developers use either the static or dynamic tools, are the developers essentially checking that their validation does not have any backdoors? The answer that Mister Pesce gave was that the developers have code in front of them that the software runs through the different code checking tools- either static or dynamic- with three or four different tools. Then when the developers get the results and reviews these results. In some cases, some may not be valid meaning that the software is correct but there is a possibility of an error.

I did not know about Common Weakness Enumeration but knew that something like this process occurs. Mister Pesce went into further detail and cleared up the the miss understanding and clarified how companies and developers look for weaknesses in their applications or softwares and how to mitigate them.

References:

Pesce, N. (2021, April 7). *Common Weakness Enumeration*. Lecture presented at Nick Pesce Presentation in Zoom.