Summer 2020
CPSC 3220 / ECE3220 Assignment 1

Due date: before midnight on the night of Monday, June 21
Submission: submit a pdf copy of the paper using Canvas
(do not submit a Word document or other format)

Grading: 20% introduction, definitions, and relationships
30% three examples (10% each)
30% CVEdetails, vulnerability types and trends
10% discussion on bugs in operating systems
10% bibliography and style

This is an individual assignment and will be checked by Turnitin.

Write a 3.5-4 page paper on operating system vulnerabilities and bugs.

(1) Provide an introduction and explain the purpose of CVEs. In the introduction, be sure to briefly define CVE, CWE, and CVSS, and explain how they are related.

(2) Discuss CVE 2018-0825 as an example and explain CWE 119.

For more details, see:

C.-C. Craciun, "Getting to the Bottom of CVE-2018-0825 Heap Overflow Buffer," blog, 9 Mar. 2018; https://www.ixiacom.com/company/blog/getting-bottom-cve-2018-0825-heap-overflow-buffer.

C. Kanaracus, "Two Nasty Outlook Bugs Fixed in Microsoft's Feb. Patch Tuesday Update," blog, 13. Feb. 2018; https://threatpost.com/two-nasty-outlook-bugs-fixed-in-microsofts-feb-patch-tuesday-update/129931/

(3) Discuss CVE 2018-4160 as an example and explain CWE 125.

For more details, see:

K. Backhouse, "Negative Integer Overflows in Apple's NFS Diskless Boot (CVE-2018-4136, CVE-2018-4160)," blog, 25 Apr. 2018; https://lgtm.com/blog/apple_xnu_nfs_boot_CVE-2018-4136_CVE-2018-4160

(4) Discuss CVE 2018-5344 as an example and explain CWE 416.

For more details, see:

L. Torvalds, "Loop: Fix Concurrent lo_open/lo_release," 6 Jan. 2018; https://github.com/torvalds/linux/commit/ae6650163c66a7eff1acd6eb8b0f752dcfa8eba5#diff-01765c0f9a2dc5c24c5a424b82b97b62

The code for loop.c is available at https://github.com/torvalds/linux/blob/master/drivers/block/loop.c. (Click on the history tab to see the list of changes.)

(5) Using the sources below, give brief definitions of the following seven vulnerability types used by CVEdetails. Use CVEdetails to identify the distribution of these reported vulnerability types in "Linux Kernel", "Mac Os X", and "Windows 10" so far for 2018.

Denial of service
Code execution
Overflow
Memory corruption
Bypass something
Gain information
Gain privileges

M. Base-Bursey, "Mobile Vulnerabilities: The Culprits Your Business Needs to Know About," blog, 2 Nov. 2017; https://www.wandera.com/blog/mobile-vulnerabilities-ios-android/.

I. Chadwick, "Mobile OS Vulnerabilities: The Lurking Culprits In Your Mobile Fleet," 20 Dec. 2017 (modified 1 Mar. 2018); https://www.mobliciti.com/mobile-os-vulnerabilities-mobile-fleet/.

(Note that there is not a one-to-one mapping between each CVE entry on CVEdetails.com and a vulnerability category.)

(6) Scan the following paper and identify where most bugs are located in an operating system, as well as the average lifetime. Discuss the reasons that the authors offer to explain clustering of bugs in an operating system.

A. Chou, et al., "An Empirical Study of Operating Systems Errors," Proc. 2001 ACM Symp. Operating Systems Principles (SOSP 01), pp. 73-88.

link to article: https://dl.acm.org/citation.cfm?id=502042.

(A 2011 update that studies Linux versions 2.6.0 to 2.6.33 is available at https://dl.acm.org/citation.cfm?id=1950401.)

(7) Include a bibliography formatted according to pp. 32-37 of
https://www.computer.org/cms/Computer.org/Publications/docs/ 2016CSStyleGuide.pdf

Target your paper to an audience of fellow students.

If you use a quote or a close paraphrase from a source document, cite the source either in a footnote or using the number of the corresponding bibliographic entry in a reference section. (The paper must not be constructed as a mere collection of quoted materials. Use your writing skills to construct a readable and useful technical paper.)

If you include a diagram or table taken from another source, cite the source in a caption immediately under the diagram or table.