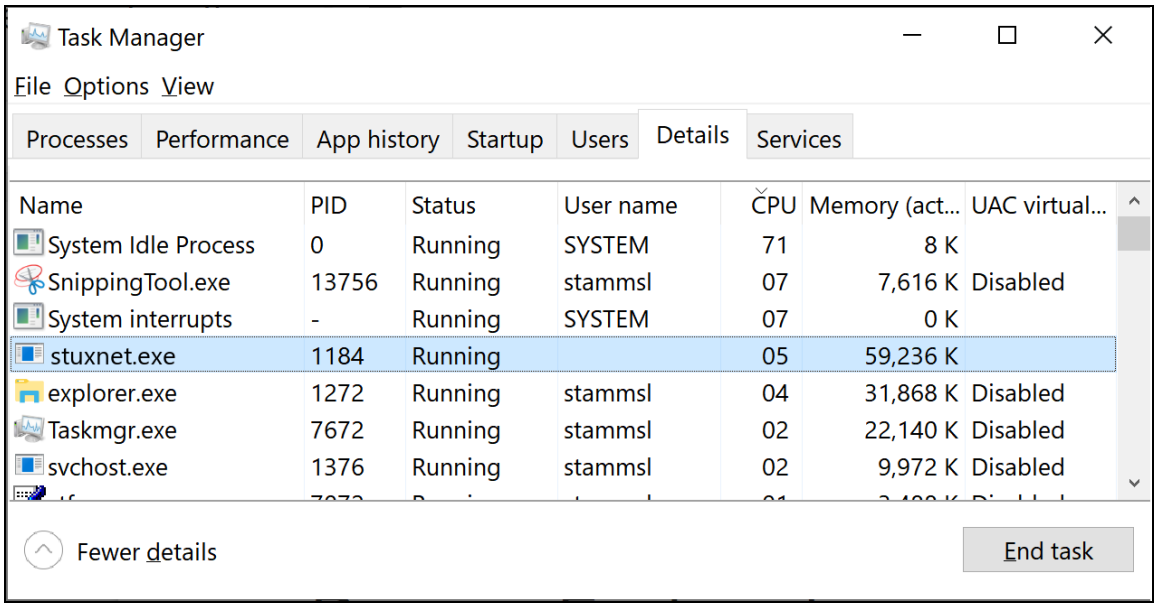
CSSE490/ECE497 (Spring 2018-2019):

Malware Analysis and Reverse Engineering



Oh no.

This program is running on your computer. What is it doing? Is it malicious? In this course, you'll learn how to investigate software to see what it does and how to catch software that is behaving badly. You'll use tools to un-compile code, extract operational semantics, and also attempt to detect programs trying to hide how evil they are.

Instructors: Zak Estrada & Sid Stamm

Prerequisites

ECE 332 with a B or better OR BOTH CSSE 232 and CSSE 332. Proficiency in assembly, OS, debugger, and Compiler Concepts

Course Objectives

Students who successfully complete this course will be able to…

1. Describe a process that would identify the purpose and behavior of a binary executable program.
2. Given a binary executable, analyze and explain its purpose and what it does.
3. Given sample malware, explain changes required to a system to make the malware ineffective.
4. Use modern techniques to create unwanted software (packing, obfuscation, anti-debugging)
5. Use modern techniques to detect and recover from installs of unwanted software (static/dynamic analysis, debugger tracing, manual decompiling)