CS 6332 - Systems Security and Malicious Code Analysis

CS 6332 Systems Security and Malicious Code Analysis (3 semester credit hours) Concepts, techniques, and tools to capture the structure, format, and representation of binary code, and transform them for higher level analysis. Use of static analysis including data-flow analysis, point-to analysis, and shape analysis to reason about the abstractions inside binary code. Use of dynamic binary instrumentation to trace the instruction level behavior of both benign and malicious programs. Use of virtual machines to observe the whole system level behavior including OS kernels. Prerequisites: CS 5343 and CS 5348 and knowledge of Assembly Code. (3-0) Y (2016-02-06 00:01:31)