For undergraduate students this course is offered as 332:492 Independent research (index 00736 since we have exhausted all available Special Topics course numbers. To register, contact Dr. Sannuti at sannuti@ece.rutgers.edu for a Special Permission number.

Malware Analysis and Reverse Engineering

Time schedule Wed 5PM to 8PM (periods 6,7) in room CoRE 538

Malicious software (malware) plays a part in most computer intrusions and security incidents. Malware analysis and reverse engineering is the art of dissecting malware to understand how it works, how it can be identified, defected or eliminated once it infects a computer. With millions of malicious programs in the wild, and more encountered everyday such as Stuxnet worm, SSL Heartbleed exploits, Apple Shellshock vulnerability, and others that attacked TARGET and Home Depot retailers, malware analysis is critical to respond to prolific cyber security incidents in a timely manner.

This course will introduce students to various categories of existing malicious software that causes harm to a user and computer, including viruses, Trojan horses, worms, rootkits, scareware, and spyware. The course will start with fundamentals of reverse engineering, and proceeds with covering advanced attacking strategies used by the existing malware, and discusses potential countermeasures in real-world production systems. The course will provide an excellent knowledge foundation and hands-on experience with real malware samples for students who seek interests in academia/research as well as industry.

In particular, the course will cover:

- ***Principles and Fundamental Concepts***
  - Assembly languages and program compilation
  - Binary code and ELF/PE data representations
  - Static binary analysis and disassembly
  - Dynamic execution analysis
- ***Attacks and Existing Malware***
  - Malware behavior (e.g., control flow hijacking)
  - Anti-reverse engineering and obfuscation
  - Return-oriented programming
  - Web-based malware and social engineering
- ***Analyses and Security Defenses***
  - Symbolic execution and taint tracking
  - Runtime memory forensics
  - Behavioral detection signatures
  - Security hardening (ASLR, DEP, and CFI)

Instructor: Saman Zonouz saman.zonouz@rutgers.edu