CSC 545 – REVERSE ENGINEERING

CREDIT HOURS: 3
PREREQUISITES: CSC 341; 455 or 447; or Instructor Permission. CSC 562 is recommended
GRADE REMINDER: Must have a grade of C or better in each prerequisite course

CATALOG DESCRIPTION

Coverage of incorporating security technologies and methods into new and existing systems; learning how attackers expose vulnerabilities; analyzing threats; applying methods to prevent and defeat attacks; and understanding the ethical responsibilities and obligations associated with developing, acquiring, and operating software systems.

PURPOSE OF COURSE

Learn and understand the threats to an operating environment through examination of both operating systems and malware. Practice practical reverse engineering on various operating systems (PC, Linux, OSX). Study threats and prevention techniques applied to various OS threats. Examine both application and OS level vulnerabilities, including malware. Examine and learn how to defend against networking attacks.

EDUCATIONAL OBJECTIVES

Upon successful completion of the course, students should be able to:

1. Describe the types of safety and security risks associated with network infrastructures.
2. Deploy appropriate countermeasures, such as layers, access controls, privileges, intrusion detection, encryption, and coding checklists.
3. Explain how adversaries are able to identify vulnerabilities and generate exploits for public and private software systems via operating systems and malware
4. Detect data exfiltration activities and conduct detailed analysis to describe the malignant logic and potential impacts.
5. Explain a variety of methods by which attackers can damage software or data associated with software via weaknesses in the design or coding of the system at the assembly level, or by infiltrating the OS with malware; and demonstrate or explain how to prevent such weaknesses.
6. Analyze threats to software systems and operational environments.
7. Design and plan for effective countermeasures such as access control, authentication, intrusion detection, encryption, and coding checklists.

COURSE CALENDAR

This course meets for a minimum of 37.5 lecture contact hours during the semester, including the final exam. Students have significant assignments based on readings from the primary literature, participate in classroom discussions regarding current research topics, complete periodic homework and laboratory/programming assignments, and periodic exams in addition to the final exam. Students are expected to prepare for any class assignments or quizzes over the material covered in class or in the reading

material. Successful completion of these activities requires at a minimum six additional hours of outside of classroom work each week.

CONTENT **Hours**

Introduction to Reverse Engineering 3
- Overview and course Introduction
- Common tools

Application-level Vulnerabilities.....9
- Stack vulnerabilities
- Heap vulnerabilities

OS-level Vulnerabilities.....9
- DLLs
- DLL injection
- Authentication, Authorization and Credentials

Malware 9
- Malware categories
- Malware and obfuscation
- Coding malware
- Malware forensics

Miscellaneous Threats 9
- Networking attacks
  - Routing
  - Remote exploitation
- Cyber defense

Exams (plus final).....6

TOTAL 45

REFERENCES

Eldad Eilam, Reversing: Secrets of Reverse Engineering, Wiley, 2005

Stuart McClure, Joel Scambray, George Kurtz, Hacking Exposed 7: Network Security Secrets and Solutions, Seventh Edition. McGraw Hill Osborne Media , 2012

Michael Sikorski and Andrew Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press, 2012.

Bruce Dang, Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation, Wiley, 2014