Computer Virology

1. **Course number and name**: 020VIRES5 Computer Virology

2. **Credits and contact hours**: 4 ECTS credits, 2x1:15 (course + lab)

3. **Name(s) of instructor(s) or course coordinator(s):** Maroun Chamoun

4. **Instructional materials:** Handouts posted on the Web

5. **Specific course information**
   a. **Catalog description**:
   Introduction: The taxonomy of malware and its capabilities, History of malware - Reverse engineering: tools, obfuscation, packers, anti-debug techniques, x86 and x64 Assembly, Binary Code Analysis – Buffer overflows: Memory Corruption Bugs, Stack Overflow, Format String Attack, Integer Overflow, Fuzzing, Exploitation and Mitigation Techniques, Protection Mechanisms - The theory of malware: Turing Machine, The Halting Problem and Decidability, Adleman's proof of the undecidability of the presence of a virus, Cohen's experiments on detectability and self-obfuscation – Self-reproducing Malware: script and macro-virus, executable file virus, system virus and rootkit, Antivirus: Antivirus techniques, Antivirus Relay, Protection techniques, Antivirus Benchmarking and Testing – SPAM: Common techniques of SPAM and SPAM filtering.

   b. **Prerequisites*:*** None

   c. **Required** for CCE Software Engineering option students; **Selected Elective** for CCE Telecommunication Networks option students.

6. **Educational objectives for the course**
   A critical element of a complete education for the graduating professional computer scientists must include knowledge about viruses, their nature, and their destruction.
   a. **Specific outcomes of instruction:**
      - Prepare the newest computer professionals with the expertise needed to work in a computing environment which includes computer viruses and other forms of malware.
      - Have specific reversing skills in the deconstruction of various x86 assembler obfuscation tricks used by malware in order to be an expert malware reverser.
      - Identify and describe major programming errors and ways to mitigate the impact of discovered vulnerabilities.
      - Identify key characteristics of malware and ways to mitigate the threat of malware.

b. PI addressed by the course:

PI	1.1	1.2	1.3	2.1	2.4	4.1	4.2
Covered	x	x	x	x	x	x	x
Assessed			x				

7. Topics and approximate lecture hours

- Introduction: The taxonomy of malware and its capabilities: viruses, Trojan horses, rootkits, backdoors, worms, targeted malware; History of malware (2 lectures)
- Reverse engineering: Hex Editors, Disassemblers, Debuggers, obfuscation, packers, anti-debug techniques, x86 and x64 Assembly, memory organization, Binary Code Analysis (3 lectures)
- Lab: Reverse engineering tools and cracking software (1:15)
- Homework1: De-obfuscation of an obfuscated perl code (6 hours of mini-project)
- Homework2: Cracking a serial number (8 hours of mini-project)
- Buffer overflows: Memory Corruption Bugs, Stack Overflow, Heap Overflow, Format String Attack, Integer Overflow, Fuzzing, Exploitation and Mitigation Techniques, Protection Mechanisms (3 lectures)
- Lab: Format string attack (2:30)
- Homework3: Fuzzing and exploiting a vulnerable server (10 hours of mini-project)
- The theory of malware: Turing Machine, The Halting Problem and Decidability, Adleman's proof of the undecidability of the presence of a virus, Cohen's experiments on detectability and self-obfuscation (2 lectures)
- Script and macro-virus: VBA and Microsoft office virus, propagate macro-virus by infecting Normaldot template, macro-worms, VBscript and Javascript worms, shell script virus (2 lectures)
- Lab: Shell script virus on Linux (1:15)
- Executable file virus: PE and ELF executable file format, Adding Viral Code: Appenders and Prependers, Code Interlacing Infection, Companion Viruses, Virus algorithm (3 lectures)
- Lab: Writing Linux executable virus using C and Assembly language (3:45)
- System Virus and Rootkit: Computer bootstrapping, File system structure, Boot structure viruses, Windows Kernel architecture, Behavioral Viruses, Anti-Antiviral Techniques, User-mode and Kernel-mode Rootkit (3 lectures)
- Lab: Writing a Linux Kernel-mode Rootkit (1:15)
- Anti-virus: Protecting Against Viral Infections, Antiviral Techniques: Scanning; Spectral analysis; Heuristic analysis; File integrity checking; Behavior Monitoring; Code emulation, Antivirus Relay, Assessing of the Cost of Viral Attacks, Computer "Hygiene Rules", What To Do in Case of a Malware Attack (2 lectures)
- Lab: Implementing an Anti-virus Relay (1:15 hours)
- SPAM: opting -in and –out, Spammers' Strategies: Consolidation; Outsourcing; Affiliation based models, Technical countermeasures: Closing the "open relays"; Blacklists; Whitelists; Filtering systems; Teergrubing; Greylisting; Turing Test (2 lectures)