Bachelor projects in IT security

Supervisors: Michael Kirkedal Thomsen, Troels Larsen

(We have room for about 3 of 4 projects more)
(so first come, first serve)

Fuzzing with AFL

- Fuzzing is an automated method for finding vulnerabilities in software
    - Study, describe, compare different fuzzing techniques
    - Validate existing vulnerability findings with AFL

Dynamic domains in malware

- Some malware use domain generation algorithms (DGA) in communications with their command and control servers

  - Survey DGA functions for different malware specimen

  - Describe models for detection of such DGA, in DNS traffic, from the domain name itself

  - Find, generate data sets to test models

Live remote memory forensics

- Remote live interrogation of running machines scales better than traditional full memory acquisition

  - Study techniques for remote live memory analysis
  - Compare with traditional acquisition techniques
  - Evaluate reliability, coverage, scalability
  - Create proof of concept

DKOM and robust signatures in memory forensics

- With Direct Kernel Object Manipulation (DKOM) adversaries alter objects in memory in attempts to evade detection

  - Study, describe memory objects
  - Survey techniques to perform DKOM
  - Test DKOM on a set of objects in a VM setup with Volatility
  - Develop robust signatures for object scanning