CT437
COMPUTER SECURITY AND FORENSIC COMPUTING

Dr. Michael Schukat

Ollscoil na Gaillimhe
University of Galway

About me

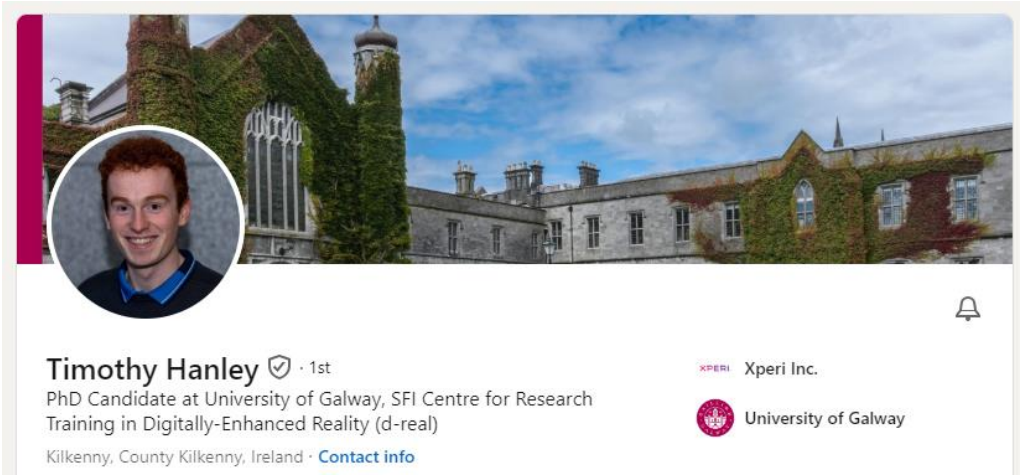
- Professional Background:
  - M.Sc. Computer Science
  - Dr. rer. nat. (Computer Science)
  - (Senior) Lecturer in the School of Computer Science at NUI Galway
  - Senior Embedded Systems Design Engineer (Ireland)
  - Embedded Systems Design Engineer (Germany)
  - Junior Lecturer and Researcher (Germany)
- Research Interests:
  - Many, including cybersecurity
- Contact:
  - michael.schukat@universityofgalway.ie
  - Office CSB3002

My recent Publications in (AI-supported) Cybersecurity

- Detecting Ransomware Encryption with File Signatures and Machine Learning Models (2023)
- A Security Enhancement of the Precision Time Protocol Using a Trusted Supervisor Node (2022)
- The Application of Reinforcement Learning to the FlipIt Security Game (2022)
- Precision Time Protocol Attack Strategies and their Resistance to existing Security Extensions (2022)
- New Framework for adaptive and agile Honeypots (2020)

Your Lab Tutor

- Timothy Hanley: 2nd year PhD student



Cybersecurity versus Computer Security

- **Cybersecurity** is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes
  Source: Cisco
- **Computer Security** is the historically older term coined at a time when the focus was on individual stand-alone computers rather than entire systems

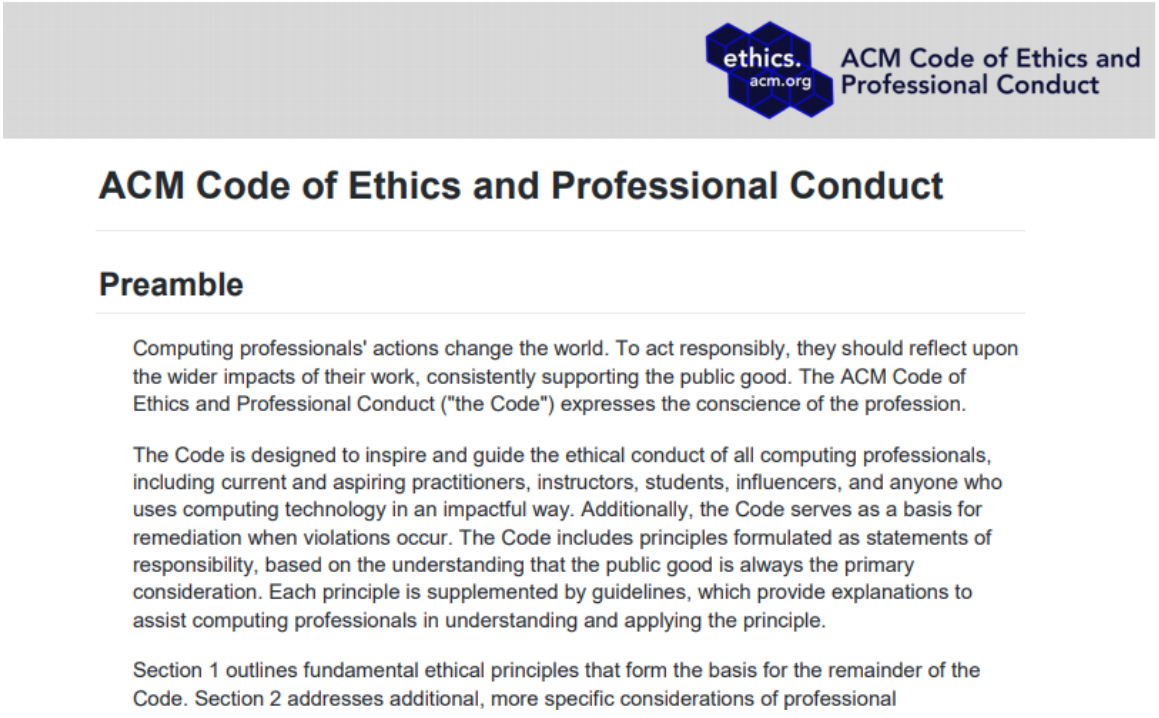
What is Computer Forensics?

- Computer forensics is a branch of digital forensic science pertaining to evidence found in computers and digital storage media
  The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analysing and presenting facts and opinions about the digital information
  Source: Wikipedia

Some Housekeeping …

Disclaimer

- Please adhere to the **ACM Code of Ethics and Professional Conduct!**
- See Canvas



Use of Canvas

- Announcements
  - **Main communication mechanism, urgent messages may be circulated by email**
- Syllabus
  - Contains module outline, breakdown of marks, etc.
- Modules
  - Compulsory and optional reading materials
- Assessment
- Quizzes
  - In-class quizzes
  - End-of term student feedback questionnaire
- Discussion Forum
  - Mainly used for assignment-related questions
- Quickly attendance (used later for every lecture)
- Virtual Classroom
  - Possibly used for virtual labs

Lecture Organisation / Breakdown of Marks

- 2 hours of lectures per week
  - Wednesday 10:00 – 11:00 in Tyndall Theatre
  - Wednesday 13:00 – 14:00 in ENG-2002
- 2 hours of labs per week (from week 3, tbc)
- There will be a continuous assessment (CA) component worth 30% consisting of
  - 2 assignments
  - in-class quizzes
  - lab worksheets
- The exact CA structure will be shared with you in coming days
- The summer exam has a weight of 70%
  - See Canvas for 2022/23 summer exam
- I'll be also using **Mentimeter** or Vevox for in-class feedback

In-Class Quizzes

- Canvas MCQs, during the lectures
- Open book, addressing content covered during the current or previous week
  - I will provide you with details beforehand
- Typically, 5 randomised questions out of a pool of 20+ questions
- One question is presented at a time, there is no backtracking allowed
- 5 minutes duration

Flipped Learning

- In some lectures we'll apply the concept of **flipped learning:**
  - You'll be notified via Canvas and study the learning materials prior to the weekly lectures
  - If you have specific questions about content, please let me know in good time, so that I can incorporate them into my lecture slots that week

Assignment Content Overview

- The assignments will require you to do the following:
  1. Software development / benchmarking in C using the OpenSSL library
  2. Installation and demonstration of ethical hacking tool (i.e., Metasploit)
     - Extensive use of VM or container
- **Because of various campus restrictions you need to use your own computer / laptop for the assignments**

Some important Ethical Hacking / Penetration Testing Tools

- Kali Linux
  An Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments
- Metasploit
  A software platform for developing, testing, and executing exploits
- Shodan
  Shodan is a search engine for Internet-connected devices
  https://www.youtube.com/watch?v=Db5TPYTgy9c

Learning Materials and Textbooks

- Weekly presentations
- There's no single primary textbook, but William Stalling's
  - Cryptography and Network Security
  - Data & Computer Communications

  provide a good overview
- I'll provide you with links to additional sources, e.g.
  - articles
  - eBooks
  - source code

  as we go along

Main Learning Outcomes

On successful completion of this module you will:

1. Have a knowledge of fundamental cybersecurity principles, including confidentiality, integrity, and availability (CIA triad), as well as an understanding of threats and attack techniques by threat actors
2. Have a solid understanding of modern cryptographic algorithms, modern cryptographic network protocols, and their applications
3. Synthesize cryptographic concepts into algorithms / frameworks to address a given cybersecurity problem
4. Be able to conduct simple information / computer system security assessments using ethical hacking / pen-testing strategies and tools
5. Proficient in the use of cryptographic libraries (i.e., OpenSSL)