Computer Security Syllabus

Version: 20201010

Module description

With the increasing value of data stored on computer systems and the prevalence of viruses, malware and hacking, computer security has become a crucial part of the work of computer scientists. With an understanding of the modern security landscape, you will be able to write better, more secure software. The module will prepare you to think about security issues in your further studies and professional work.

This module aims to provide you with an understanding of the need for computer security and the technologies that support it. It has both a theoretical component that will teach you mathematical underpinnings of security systems and a practical element that will help you discover the pitfalls of security design and to comprehend the mathematics underlying the protocols by working on small examples.

The module consists of the following topcis:

1. Introduction to computer security and malware
2. Network security
3. Operating system security
4. Understanding cryptography
5. RSA public-key cryptography
6. Cryptographic protocols and key management
7. Blockchain protocols, part 1
8. Blockchain protocols, part 2
9. Security models
10. Social Issues in Computer Security

Module goals and objectives

The learning objectives for this module are:

1. Understanding the several ways in which computer systems can be attacked and how defences can be implemented
2. Understanding the role that cryptography plays within the broader subject of computer security and how it is used in blockchain technology
3. Understanding how to Implement simple cryptographic algorithms
4. Assessing the security needs given a particular situation
5. Designing and breaking the security systems
6. Analysing case studies and problems for given situations

Textbook and Readings

This module makes use of a wide range of reading material which you will encouter as you work through the course. The material is available via the online library and it includes journal and magazine articles as well as some textbook references. There will also be discussion prompts asking you to do some independent research using online sources.

Module outline

The module consists of 10 topics, each of which spans two weeks.

Topic 1 Introduction to computer security and malware	Week 1 Introduction to computer security and malware Week 2 Malware analysis
Topic 2 Network security	Week 3 Network security - DoS attacks and botnets Week 4 Network security - defence with firewalls and

	intrusion detection systems
Topic 3 Operating system security	Week 5 Operating system security - filesystems and windows Week 6 Operating system security - GNU/Linux, Android and containerisation
Topic 4 Understanding cryptography	Week 7 Understanding Cryptography - history, asymmetric and asymmetric Week 8 Understanding cryptography - transposition and substitution
Topic 5 RSA public-key cryptography	Week 9 RSA public-key cryptography - primes, Phi and security Week 10 RSA public-key cryptography - proof that RSA works
Topic 6 Cryptographic protocols and key management	Week 11 Cryptographic protocols and key management,

	part 1 Week 12 Cryptographic protocols and key management, part 2
Topic 7 Blockchain protocols, part 1	Week 13 Blockchain protocols, part 1 Week 14 Blockchain protocols, part 2
Topic 8 Blockchain protocols, part 2	Week 15 Blockchain protocols, part 3 Week 16 Blockchain protocols, part 4
Topic 9 Security models	Week 17 Security models, part 1 Week 18 Security models, part 2
Topic 10 Social Issues in Computer Security	Week 19 Social Issues in Computer Security, part 1 Week 20

	Social Issues in Computer Security, part 2

Activities of this module

The module is comprised of the following elements:

- Lecture videos. In each topic, you will find a sequence of videos.
- Readings. Each topic may include several suggested readings. These are a core part of your learning, and, together with the videos, will cover all of the concepts you need for this module.
- Practice Quizzes. Each topic will include practice quizzes, intended for you to assess your understanding of the topics. You will be allowed unlimited attempts at each practice quiz. There is no time limit on how long you take to complete each attempt at the quiz. These quizzes do not contribute toward your final score in the class.
- Discussion Prompts. Each topic includes discussion prompts. You will see the discussion prompt alongside other items in the lesson. Each prompt provides a space for you to respond. After responding, you can see and comment on your peers' responses. All prompts and responses are also accessible from the general discussion forum and the module discussion forum.

How to pass this module

The module has two major assessments each worth 50% of your grade:

- Assessed coursework. There is one assessed coursework, in the middle of the module. This involves some written research work and some cryptography work.
- Unseen examination.

Activity	Required?	Deadline	Estimated time	% of final

		week	per course	grade
Midterm coursework	Yes	1-10	25 hours	50%
End of term examination	Yes	22	25 hours	50%