

ECE 7420: Computer Security

Instructor	Jonathan Anderson jonathan.anderson@mun.ca CSF-4123	TA(s)	TBA
Office Hours	Mondays 16:00–17:00		
Website	https://introsec.ca		
Communication	In-person or e-mail communications are preferred. Brightspace (https://online.mun.ca/d21/home/478849) will only be used to record grades.		
Calendar entry	Computer Security introduces students to key computer security concepts for applications, hosts, networks and the Web. Students will learn to employ the primitives provided by programming languages, cryptography, operating systems and network protocols for protecting engineered systems and their users.		
Prerequisite(s)	ECE 6500: Computer Architecture, ECE 6610: Communications Networks		
Co-Requisites	ECE 7400: Concurrent Programming		
Schedule	Lecture	MTR 13:00–13:50	EN1000
	Lab	Thu 14:00–17:00	CSF 2112
Credit value	3 credit-hours	Lab hours	Eight 3-hour sessions per semester
Accreditation units	3h/week contact hours	Content categories	100% Engineering Science
Textbook	Van Oorschot, Paul. <i>Computer Security and the Internet: Tools and Jewels</i> , Second Edition. Springer. 2021.		
References	Anderson, R.J. <i>Security Engineering: A Guide to Building Dependable Distributed Systems</i> , 2nd Ed. Wiley. 2008.		

Graduate Attribute Focus: KB (*A knowledge base for Engineering*), PA (*problem analysis*) and Imp (*the impacts of engineering*).

Upon successful completion of ECE 7420, students should be able to:

Learning outcome	Attr–Prof	Assessment
explain how cryptography helps protect engineered systems,	KB–D, Imp–D	case study, exams
explain mitigation techniques such as W^X and ASLR,	KB–A, PA–A	exams
design sandboxable software using language and OS primitives,	PA–A, D–A	assignments, exams
evaluate potential authentication approaches for specified systems,	KB–A, Imp–D	case study, exams
formulate appropriate threat models for engineered systems,	PA–A, Imp–D	case study, exams
specify security policies using both local and network primitives,	PA–A, D–D	assignments, exams
explain how protocols are used to overcome trust limitations,	PA–A, Imp–D	case study, exams
demonstrate practical attacks against processes, hosts, networks, Web applications and their users.	Inv–D, T–D	assignments

1 Assessment

Assignments (5)	10%	Independent exploration of security topics
Labs (6–8)	16%	Guided exploration of security tools
Case study	10%	Independent research into a system, attack or defensive technique
Midterm test	24%	June 22nd
Final exam	40%	

To pass ECE 7420, **you must pass the exam portion of the course**. Exams will be closed-book: students may not bring written materials or electronic devices (including calculators or phones) to their seats.

2 Major Topics

ECE 7420 is structured in four modules. Each module builds on concepts from the previous module but takes a wider perspective, from a single program to a single host to networks to Web applications on the global Internet. You may need to **go back and refresh your memory** on prerequisite material.

This course will focus on computer security, but will necessarily include some discussion of cryptographic primitives. We will take a black-box approach to cryptography, exploring how a consumer of cryptographic primitives would see them within concerning ourselves about their implementation details. This level of detail is **insufficient for the safe use of cryptography**: we will chat more about why this is the case during the course.

2.1 Software security

The first module of the course will focus on security within a single virtual address space (*process*). There will be a focus on the memory safety of programming languages, what it buys you and what it does not.

- review: virtual memory
- review: abstract flat-memory model of computation
- memory safety: program layout, memory safety violations, language-based security
- mitigation technologies: W/X, ASLR, ROP, CFI, fuzzing, RNGs...
- languages and type safety: bytecode-interpreted vs compiled languages and their security models

2.2 System security

The second module will consider *host security*: how operating systems provide protection for users and enforcement of systemic policies on individual computers.

- users, processes and authorization
- leaky abstractions
- authentication and other applications of cryptographic hash functions
- disk encryption: symmetric-key cryptography, disk encryption, cryptographic filesystems...
- compartmentalization: capabilities, system calls, app platforms...
- trusted execution: digital signatures, trusted boot...

2.3 Network security

The third module will explore security primitives, attacks and security-sensitive systems in networks of hosts.

- review: IP, UDP, TCP, ports and services
- attacks: DNS, service vulnerabilities, DDoS...
- services: Kerberos, firewalls, IDS, PKI, packet capture...
- protocols: end-to-end design, SSH, TLS, WPA, OTR...

2.4 Web security

The final module will consider pervasive problems in Web security and — to come full circle — how language and framework design can mitigate or protect against them.

- Authentication: passwords, certificates, OAuth and cookies
- Attacks against websites: SQL injection, CSRF, XSS
- Attacks against users: phishing, tracking...
- Censorship resistance

3 Academic Integrity

Students are reminded of the Memorial University of Newfoundland Code, which states:

All members of the Memorial University of Newfoundland Community, which includes students, faculty, and staff, shall treat others with respect and fairness, be responsible and honest, and uphold the highest standards of academic integrity.

Academic misconduct is governed by section 6.11 of the University Calendar, which begins:

Within the University community there is a collective responsibility to maintain a high level of scholarly integrity. A student is expected to adhere to those principles which constitute proper academic conduct. Academic misconduct cannot be condoned or even appear to be condoned. A student has the responsibility to know which actions, as described under Academic Offences, could be construed as dishonest or improper. A student is reminded that for further guidance on proper scholarly behaviour he/she should seek advice from his/her instructors and faculty advisors.

4 Inclusion and Equity

Students who require accommodations are encouraged to contact the Glenn Roy Blundon Centre, <http://www.mun.ca/blundon/about/index.php>. The mission of the Blundon Centre is to provide and co-ordinate programs and services that enable students with disabilities to maximize their educational potential and to increase awareness of inclusive values among all members of the university community.

The university experience is enriched by the diversity of viewpoints, values, and backgrounds that each class participant possesses. In order for this course to encourage as much insightful and comprehensive discussion among class participants as possible, there is an expectation that dialogue will be collegial and respectful across disciplinary, cultural, and personal boundaries.

5 Student Assistance

Student Affairs and Services offers help and support in a variety of areas, both academic and personal. More information can be found at <http://www.mun.ca/student>.