WATERLOO | CHERITON SCHOOL OF COMPUTER SCIENCE

CS634
Security and Privacy in Health Systems

COURSE OUTLINE

Spring 2022

Teaching Team

Dr Ian McKillop, Associate Professor
Cryptography, Security & Privacy Group (CrySP)
David R Cheriton School of Computer Science
and
Co-Director, Professional Practice Centre in Health Systems
School of Public Health Sciences

office: TJB2268 / DC3530[1]
email: ian@uwaterloo.ca (see note on email)
voice: 519 888-4567 ext 37127
web: cs.uwaterloo.ca/~ian

Teaching Assistant

Setareh Ghorshi
ssghorshi@uwaterloo.ca

Pre-requisites

Prereq: MHI, MHE or MPH program enrolment.

Course Overview

This course is for students in the Master of Health Informatics program. The course is patterned after CS458/658, which is offered to students enrolled in Computer Science degree programs.

We will explore the same issues covered in CS458/658, but with a specific focus on the health sector, and with modified expectations regarding computer programming fluency.

The course provides an introduction to security and privacy issues in various aspects of computing, including programs, operating systems, networks, databases, and Internet applications. We will examine the causes of security and privacy breaches, and explore methods to help prevent breaches from occurring.

I hope you enjoy the course.

Table of Contents

A Message from the Professor

This is a long document, but it is an important document to read thoroughly. The structure and delivery approach used for this course may be different from other courses you have taken.

Do not allow yourself to be caught off-guard by not knowing a policy that applies for this course, or for assuming that because something happened one way in another course that this course is structured similarly.

For example, this course does not make use of the CALENDAR feature in LEARN. *You need to track*

[1] At the time of writing this outline, the University is planning for oncampus delivery of most courses, however courses such as this that are a part of a distance delivered program will of course remain online. If you are on-campus and wish to meet with me, drop me a note ahead of time so that I can update you on where I am located.

and record due dates yourself using a process of your choosing.

The GRADES feature in LEARN is also not used in this course. Instead you will find grades and feedback left in your dropbox.

Course Objectives

After completing this course, you will:

1. understand risks and threats to computerized information systems;
2. be able to contribute to the design of secure systems;
3. be familiar with processes to assess the security of information systems and the privacy of information; and
4. be able to play a role in the management of systems that require a high level of security and privacy, such as those used to support the delivery of health services.

Textbook

Charles P. Pfleeger and Shari Lawrence Pfleeger, **Security in Computing**, 5th edition, Prentice-Hall, 2015, ISBN-10: 0-13-408504-3
http://www.informit.com/store/security-in-computing-9780134085043

You don't need to own a copy of the text unless you wish to purchase one. The course textbook is available in an online edition through the library.

There are many excellent books on computer security. That's the good news. The bad news is that references addressing specific threats or remedies can go out of date quite quickly. I know. I have some awesome titles on my shelf for designing security into Windows NT. Pretty valuable books at one point in my career. Nothing but paperweights now.

Having said this, there are good books out there. I'd like us all to be on the lookout this term for crackerjack security and privacy titles that have a health systems focus. It would be even more exciting if you found texts in this field with a public health focus. If you find something interesting, please share it with all of us in the online Virtual Coffeeshop.

Other Useful Resources

Other resources that you might find interesting to follow:

Schneier on Security
https://www.schneier.com/blog
A blog covering current computer security and privacy issues. Bruce Schneier's blog is quite interesting to follow. He's also the fellow who correctly pointed out that many users will do anything to see a dancing pig. (Smile when you see this come up in class.)

The RISKS Digest
https://catless.ncl.ac.uk/Risks. A forum on risks to the public in computers and related systems.

Freedom To Tinker
https://www.freedom-to-tinker.com
A blog which often discusses security and privacy issues, frequently related to copyright and to electronic voting.

Threat Level
https://www.wired.com/threatlevel
A forum dedicated to privacy, crime and security online.

Contacting the Instructor

You should feel free to contact me at any time. My availability is limited only by my meetings schedule.

We are very fortunate to have a TA helping with the course this term. Our TA (Setareh) and I are online regularly and are easy to contact to meet using TEAMS or other video conferencing platforms.

Like many of us, I receive a large volume of email. While all messages are important, when I'm teaching, the most important messages are those that come from my students. Thus you will always get as prompt a response as I can manage. If you want your messages to automatically rise to the top of my inbox, preface the subject line with CS634.

If you haven't heard from me within 48 hours, something is wrong. I'm either stuck in an airport (probably unlikely this term!), or I became overwhelmed by all the other messages that came that day. Please send again. I won't take offense, and won't consider you to be pestering.

To help reduce email traffic, I've set up an "Ask the Instructor" discussion forum in LEARN which is the right place to ask questions that may be of interest to others in the class.

I'll post answers to that same forum, thus reducing the amount of mail that we all receive. That forum is a great place to post questions where everyone in the class is going to need to know the answer. I will sometimes post and answer questions to the forum myself when I discover something that would benefit from clarification. Be sure to stay abreast of information that gets posted to the Ask the Instructor forum.

You'll also see I've created an "Ask a Colleague" discussion forum that you can use to pose questions that others in the class may be able to answer.

The spam filters in my university email account will reject mail that appears to be spam. Because of this, it is best to send messages to me from your @uwaterloo address.

Read the handout under Background Materials about the email practices we are required to follow if you aren't using a @uwaterloo email account to write to Setareh or me.

Monitor your @uwaterloo account. If we write to you at this address, the university considers that you have received the message.

Delivery Modality

Like all MHI, MHE and MPH courses, this course is delivered online.

Each module includes a series of lectures that you can watch at a time of your own choosing. Each module ALSO has a live class that is "required but optional to attend."

What do I mean by that? I mean that I will join you each module for a live overview of key topics. If you can join in person, that's great. If you are unable to join in person, please view the recording at a time convenient to you during the week.

The **live class happens on the last Thursday of each module** beginning May 5/22. (Typically we use only 30-45 minutes of the timeslot you will see is reserved in LEARN under WebEx.)

At the time of writing I've scheduled live classes for 13h00 in the afternoon. That's when we will hold our first live class on May 5/22. After meeting the class we can decide if a better time is 20h00 on Thursdays. (This is what I tried in the Winter term and it seemed to work well.)

We use WebEx for live classes because WebEx is integrated into the LEARN platform. You will find a link to WebEx meetings just above the Announcements panel on our course home page. There is a tab for scheduled upcoming meetings and a separate tab that gets you access to recorded past classes.

By attending in person, you can ask questions, seek further clarification, and benefit from all the features of a traditional in-class lecture.

As a course on privacy and security, there are some legitimate privacy issues that arise when I record live class discussions. I will discuss these issues, and offer ideas for how these issues can be addressed at our first class.

I appreciate and fully understand that work and other commitments will prevent some of you from being able to join us in person. I do expect, however, that if you have been unable to join us in person that you will watch the "live" class at a convenient time.

Workload

This is a graduate course. The fact that the course is delivered in an online format does not change the workload expectations. If anything, I suspect the logistics of needing to coordinate one's activities around the milestones may actually increase the amount of time that must be committed to the course over that which would be required in a classroom setting. And of course this term we are still wrestling with the impact of COVID-19.

My experience is if you budget 10 hours per week for a grad course, you will have MORE than enough time to watch the module videos and complete assigned tasks. (Assume that a full course load of 3 graduate courses is equivalent to a full time job of 35 hrs/week.)

I understand that there are many other demands on your time. However, these other demands cannot be used as a reason to reduce your commitment to any university education.

Thematic Topics

The course is delivered as a series of seven modules.

The modules for this term are:

Module 1 - *Computer Security and Privacy*
The meaning of computer security; comparing security with privacy; types of threats and attacks; methods of defense

Module 2 - *Program Security*
Secure programs; non-malicious program errors; malicious code; controls against program threats

Module 3 - *Operating System Security*
Methods of protection; access control; user authentication

Module 4 - *Network Security*
Network threats; firewalls, intrusion detection systems

Module 5 - *Internet Application Security and Privacy*
Basics of cryptography; security and privacy for Internet applications (email, instant messaging, web browsing); privacy-enhancing technologies

Module 6 - *Database Security and Privacy*
Security and privacy requirements; reliability, integrity, and privacy; inference; data mining; k-anonymity

Module 7 - *Non-technical Aspects*
Administration of security systems; policies; physical security; economics of security; legal and ethical issues

Module content is delivered using a collection of video lectures with a set of accompanying printable slides. Both can be found in LEARN organised by module.

Please listen to the video recording for Module 1 Part 1 to learn more about using the printed slide deck.

Evaluation

Portfolio (Individual)	80%
Self-test Quizzes (3) (Individual)	20%
Effort Adjustment Factor	0.92 – 1.08

Your final grade is determined using the break-down above but can be affected (upwards or downwards) by the Effort Adjustment Factor. The Effort Adjustment Factor is used in lieu of having a participation grade.

WATCH the video on how the Effort Adjustment Factor works. The video can be found in the IMPORTANT COURSE INFORMATION folder in LEARN.

I find it helpful to remind everyone that online learning does not mean independent study. This is not a course where you can decide what to do, how much to do, and when to do it. Everyone in the class, including me, is counting on your involvement.

Imagine this course to be exactly like a course delivered on campus, It just happens that we are all sitting in front of our computer monitors instead of sitting together in a classroom.

If you have questions about my expectations, be sure to ask.

Details on the deliverables that contribute to your evaluation are described in the sections that follow.

Deliverables

Portfolio Submissions

(Individual activity – do x of y opportunities – see explanation)

Portfolio Items Due: Most portfolio items are due by the end of the module during which the portfolio item(s) were assigned. Dates are published under CONTENT > PORTFOLIO ITEMS.

In every module I will ask you to find nuggets of information about (hopefully!) interesting questions. I'll be honest. Often neither Setareh nor I know the answer to the questions we've posed, and that's what makes the questions fun for everyone. You learn something, and we do as well.

At other times I'll ask you to do a short amount of research on a topic, again, usually involving finding and commenting on something – be it a journal article or something about computer security and privacy.

Minor portfolio tasks are NOT intended to be time intensive. You can often complete a minor portfolio task in under 30 minutes, and in a few paragraphs – certainly in under a page. If you are asked to "find" something, you can submit the URL or the actual e-item along with a short description. There are usually two or three opportunities to complete a minor portfolio task in each module.

In addition to the opportunities in each module to complete some minor portfolio tasks there are three opportunities during the term to complete a "major" portfolio task.

All of this is described in detail on the page *Portfolio Items - Summary of Topics and Due Dates* found in the Portfolio Tasks folder in LEARN. On that page I also provide some ideas on strategizing. Be sure to read that content.

Keep in mind that you must complete minor portfolio tasks during the related module and submit by the due date. You can't go back later in the course and add items to your portfolio for which the due date has already passed.

There might be some minor portfolio tasks for which there is no answer. In this case you can submit a detailed explanation of the approach you used to try to find the answer for credit. You would still earn points.

I will craft one of the major portfolio tasks in the form of a "test" for those who know they excel at "tests." (Yes. There are students who excel at this form of assessment. You will have spotted there is no midterm or final this term, so by having one major portfolio submission with a test-type format these students can tackle a type of deliverable at which they excel.)

Submitting Portfolio Items

When submitting an item to your portfolio dropbox, please title the submission using this naming convention:

Portfolio x – "Topic"

where "Topic" is replaced with whatever word/phrase I have asked you to use in the task description and 'x' is the Portfolio submission number I've assigned. This will ensure you receive credit for your portfolio submission.

To keep us all organised I try to maintain a summary list of the portfolio task numbers and names in the PORTFOLO TASKS folder.

It is important to follow the naming convention as once your dropbox starts to fill up with portfolio items, it can become difficult for both you and us to track the new versus the old items in your dropbox.

Self-tests (Quizzes)

Individual - do 3 of 3

Quizzes are Due: The self-tests are available for a 7 day window after the end of the modules 2, 4 and 6.

Self-tests help you remain current with the material, and gauge your grasp of what we are discussing on an ongoing basis.

You can attempt each self-test as often as you wish during the 7 days that a self-test is available. Your last grade on each self-test is the only score that counts towards your final mark.

Quiz questions are drawn from a pool of questions for that quiz. This means you will see some random variation in the questions that are presented to you on each subsequent attempt.

Note for students with disabilities

AccessAbility Services collaborates with all academic departments to arrange appropriate accommodations for students with disabilities without compromising the academic integrity of the curriculum. If you require academic accommodations to lessen the impact of your disability, please register with AccessAbility at the beginning of each academic term.

Equity, Diversity and Inclusivity

I welcome and embrace diversity in opinions, backgrounds and beliefs and count on you to do the same.

Demonstrate respect and dignity towards others in the class and in your group settings, as I know you will.

If you have a PGP that you prefer I use, I welcome you sharing if you wish to. My PGP is he/him/his.

For some of us, the name stored in the university's records is sometimes not be the name by which our family and friends know us. Should you have a preferred name, simply let me know. We'll happily update our class list to reflect that choice.

Please also help me correctly pronounce your name should I say it incorrectly. Many of us have names that don't follow English pronunciation patterns. My name is a good example. You would think my name (Ian) is pronounced "eye-an" as the "i" is followed by a vowel, but it is actually pronounced, "eee-an." (You'll make me smile if you call me "eye-an.")

Many of you will have heard my name before and will know how it is pronounced. But unless you can speak Gaelic (I'm from Scotland) I bet nobody in the class can pronounce other names in my family like Eilidh and Oighrig. (Let me know if you can guess! No cheating by checking YouTube.) My family has spent our lives helping teachers learn how to pronounce our names (and spelling our names, letter by letter, when talking to a call centre!), so I will take no offence if you need to help me correctly pronounce your name. In fact, I welcome your help! I love learning new names.

Security Information

In this course, you will be exposed to information about security problems and vulnerabilities with computing systems and networks. You are not to use this or any other similar information to test the security of, break into, compromise, or otherwise attack, any system or network without the express consent of the owner. Depending upon the scenario, attempting any of these actions could be considered not only unethical behavior but also criminal behavior. In particular, you will comply with all applicable laws and UW policies, including, but not limited to, the following:

- UW Policy 33, Ethical Behaviour
- Guidelines on Use of UW Computing and Network Resources
- MFCF Account Usage Policy
- CSCF-Specific Policies

Violations will be treated severely, and with zero tolerance.

The fine print

Sadly, this section of the course outline seems to grow longer by the year as both the University and I seek to ensure that nobody is caught unaware by the University's policies and regulations.

In an effort to ensure no-one finds themselves saying, "I didn't know that," this section summarises information I'm sure won't come as a surprise to experienced grad students:

General University Policies

It is your responsibility to familiarize yourself with University policies regarding academic integrity, accommodations available due to illness, acceptable use of Waterloo's resources, and how to appeal a decision that affects your academic affairs. Those policies form an integral part of this course outline and can be found on the University's website.

Literacy

Written assignments must reflect university level literacy in English.

If English is your second language, consider using grammar and spelling checkers. (This can also be a great idea when English is your first language!)

Late Submissions

Consistent with School policies, late deliverables are marked and then a penalty of 10% for each day late is applied. (Whether 10 minutes late or 24 hours late.) Weekends count as 2 days and a grade of zero is assigned after 5 days. There is normally no exception to this rule without documentation or prior arrangement with the instructor or a TA. University regulations preclude pre-arranged holiday trips, assignments due in other courses, or events like your friend's birthday from being acceptable reasons for a late submission – as legitimate as some of these reasons might seem.

Having said this, common sense always prevails. If a major ice storm strikes and your home is without electricity for days (is anybody old enough to remember Ottawa in 1998?), I do not want you risking life or limb to find an internet café just so you can submit something on time. Likewise, if you are a healthcare provider who is paged to come in and save someone's life and thus miss the deadline, don't panic. If we have ice storms, tsunamis, or other events truly beyond your control (dare I say, like a pandemic), your TA or I will make alternate arrangements with you. Simply keep us in the loop, as early as possible.

Academic Integrity

I can't encourage you strongly enough to read material the University has prepared for students regarding academic integrity and related university policies. If you have never read these materials, go and READ THEM NOW. All of this information is found on the excellent academic integrity website. https://subjectguides.uwaterloo.ca/gradaiguide.

Claiming you didn't know a policy existed is rarely accepted as an excuse if you find yourself violating a rule – deliberately or accidentally.

In order to maintain a culture of academic integrity, members of the University of Waterloo community are expected to promote honesty, trust, fairness, respect and responsibility. (Check the Office of Academic Integrity for more information.)

It's important that we all recognize that academic misconduct by any individual compromises the educational experience of everyone who is affiliated with Waterloo. You want to be proud of your UW degree, just as I am very proud of my Waterloo degree.

When someone cheats, or takes actions detrimental to the education of others, it diminishes the quality of the degree the rest of us worked so hard to earn. Who wants to have a degree from a University where "the word on the street" is that the degree can be obtained by cheating? None of us!

This is one of the reasons I take academic misconduct so seriously. When someone engages in academic misconduct the real impact is on everyone else who acted honestly and fairly when earning our Waterloo degree. So I encourage you to help me here. If you see cheating, call it out. Let people know this is unacceptable.

By now, all of you should have passed your Academic Integrity milestone.

When completing tasks it is fine to talk to one another, the instructor, or to anyone else but any assistance must be limited to discussion of the problem and sketching general approaches to a solution. You must always create your own solutions, including code and documentation if appropriate.

Basing your solution upon someone else's solution is prohibited, and obviously solutions may not be copied from any source. Nor can you come up with a solution and ask others if they think you have the correct answer. (Be careful here. Students who post their self-created answers to a discussion forum simply to ask if others think they've solved something correctly can be found guilty of academic misconduct if someone takes that solution and submits it as their own.)

To be clear, submitting assignments copied in whole or in part from assignment submissions to a previous offering of this course, or from any offering of any other course, is forbidden, *even if you are resubmitting your own work*. These and any other forms of collaboration on assignments constitute cheating. If you have any questions about whether some activity constitutes cheating, please ask the instructor.

Academic misconduct includes more than plagerism. Academic misconduct also includes cheating, falsification and behaviours that interfere with the rights of other students to pursue their studies. So it's not only about plagiarism, although plagiarism or inappropriate collusion with colleagues seem to be what gets many students into a tough spot.

For sure, penalties vary with the nature of the transgression. But in my many years as a professor, I continue to meet students who think that if they get caught they will simply get zero on their assignment. Instead, I've experienced situations deemed so serious as to see the student being removed completely from their program – their academic careers ended. It happens. Don't let it happen to you.

The University is becoming increasingly vigilant in this area, as it should be. You may have seen on the news that a few years ago a student was charged with a criminal offence for a cheating incident during an exam at Waterloo. That's much more serious than simply failing a course.

Having gone on for a bit about the seriousness with which we approach issues of Academic Misconduct, it is also really important for me to stress that that the University is committed to fairness and equity in our decision-making process. There are avenues open to you should you ever feel a decision I've made, or the University has made, is unreasonable or unfair given the circumstances.

Thanks for reading this section. My hope is we can enjoy a term where the section on Academic Integrity and norms wasn't needed even though the university requires instructors to include this discussion in our outlines.

Grievances

Notwithstanding University of Waterloo policies, a student who believes that a decision affecting some aspect of his/her university life has been unfair or unreasonable may have grounds for initiating a grievance. Read Policy 70, Student Petitions and Grievances, Section 4. When in doubt, please contact the School's lead for graduate advising (Dr Tyas) who will provide further assistance.

Discipline

A student is expected to know what constitutes academic integrity to avoid committing an academic offence, and to take responsibility for his/her actions. (Check the Office of Academic Integrity for more information.) A student who is unsure whether an action constitutes an offence, or who needs help in learning how to avoid offences (e.g., plagiarism, cheating) or about "rules" for group work/collaboration should seek guidance from the course instructor, academic advisor, or the undergraduate associate dean. For information on categories of offences and types of penalties, students should refer to Policy 71, Student Discipline. For typical penalties, check Guidelines for the Assessment of Penalties.

Appeals

A decision made or penalty imposed under Policy 70, Student Petitions and Grievances (other than a petition) or Policy 71, Student Discipline may be appealed if there are grounds. A student who believes he/she has a ground for an appeal should refer to Policy 72, Student Appeals.

Writing Style, Page Layout, Submission Length and References

There is no "academic writing" required in this course. (Such as is required for a journal article, essay, or thesis.) Instead, your **written submissions should employ a business writing style.** Grammatically correct point form is fine when appropriate. Short, concise sentences are welcomed.

Submissions must reflect university level literacy in English.

You will note I rarely specify particular fonts or sizes, page margins, line spacing, page layouts, etc. for submissions. I will leave it to you (just as your employer will do) to make decisions regarding how you wish to present your recommendations in a professional manner. **Presentation style is assessed.**

You can use any convention you wish when citing sources. (APA, Chicago, or even something you've created yourself, etc.) Our only criteria is that you provide sufficient information for us to be able to locate a source you are citing should we wish to do so.

Turnitin.com and alternatives

Text matching software (such as Turnitin) may be used to screen assignments. Contact me if you wish to explore an alternate process for screening your submissions.

Publishing Course Content

Sites encouraging students to publish course materials (lectures, slides, solutions, etc.) have sprung up like mushrooms. As a result, the university has asked that we include this statement in our course outlines…

This course contains the intellectual property of your instructor, TAs, and/or the University of Waterloo. Intellectual property includes items such as:

- Lecture content, spoken and written (and any audio/video recording thereof);
- Lecture handouts, presentations, and other materials prepared for the course (e.g., PowerPoint slides);
- Questions or solution sets from various types of assessments (e.g., assignments, quizzes, tests, final exams); and
- Work protected by copyright (e.g., any work authored by the instructor or TAs or used by the instructor or TAs with permission of the copyright owner).

Course materials and the intellectual property contained therein, are used to enhance a student's educational experience. However, ***sharing intellectual property without the intellectual property owner's permission is a violation of intellectual property rights and is illegal.*** For this reason, it is necessary to ask the instructor, TAs and/or the University of Waterloo for permission before uploading and sharing the intellectual property of others online (e.g., to an online repository).

Permission from an instructor, TAs or the University is also necessary before sharing the intellectual property of others from completed courses with students taking the same/similar courses in subsequent terms/years. In many cases, instructors might be happy to allow distribution of certain materials. However, doing so without expressed permission is a violation of intellectual property rights.

Please alert the instructor if you become aware of intellectual property belonging to others (past or present) circulating, either through the student body or online. The intellectual property rights owner deserves to know (and may have already given their consent).

That's it for the fine print.

Enjoy the term. Let me know what's working in the course, and what doesn't work. Let me know topics that you'd like to see us explore. Be engaged. Your grad school experience will be something you remember for your whole life. Make it the best experience you can.

(h) CS634 Outline v1h

Revision History
S14 v1a built from CS458/658 W14
S16 v1a built from CS698 S14
S17 v1a built from CS634 S16
S18 v1a built from CS634 S17 – new deliverables
S18 v1b date clarifications
S19 v1b deliverable clarifications; summary added
S20 v1d portfolio chgd, grading changed, index added
S21 v1g built from S20 v1d
S22 v1h built from S21 major section reorg of v1f