Lecture #1: Course Intro

UCalgary ENSF619

Elements of Software Security

Instructor: Lorenzo De Carli (lorenzo.decarli@ucalgary.ca)

First, the basic details

- Class meets Mon/Wed/Fri between 11AM and 11:50AM in Science A 124 (note, class will not meet every Wednesday!)
- **Instructor:** Lorenzo De Carli (lorenzo.decarli@ucalgary.ca; ICT 240)
- **Office hours:** contact instructor to make an appointment
- **Course web page** (for general info, syllabus and schedule): https://ldklab.github.io/assets/classes/ENSF619/
- **Course Canvas page** (for assignments and grades): https://d2l.ucalgary.ca/d2l/home/648686

What is this class about?

- A review of **applied concepts in software security**
- **Broad structure:**
  - Basic security concepts
  - Software exploits
  - Malware detection
  - Adversarial attacks
  - IoT/CPS security
  - SW supply chain security
  - Web security
  - User issues in security

What is this class **not** about?

- This class is not vocational cybersecurity training - instead, we are going to review **concepts on which the field is built, and novel ideas**
- The class still has a strong applied flavor – i.e., we won’t cover cryptography or formal methods (although those fields are important within security!)

What are the goals of this class?

1. Ensure students understand what are the principles behind modern software security: **why are things the way they are?**
2. Teach students to **think critically** about building secure software and protecting it
3. Prepare students to become **productive researchers** (aka “people who solve problems yet unsolved”) in the field of security

How is this class organized?

- This course is set up as a **research-focused class**.
- **No textbook**
- The bulk of the class will consist in **reading scientific papers, reviewing and discussing them critically**
- Each student will be expected to lead two in-class discussions
- The class will include **two midterms** which will evaluate the students' knowledge and understanding of the reading material (papers)
- Student will also be expected to complete a **research-oriented class project** (more on this later)

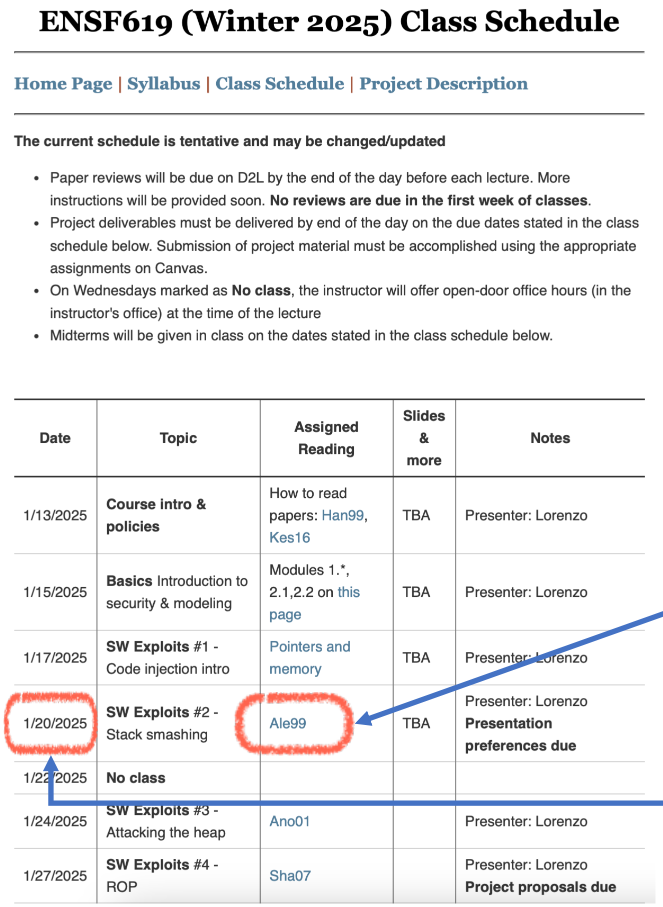
Participation

- Attendance is **required**
- It is acceptable to miss **up to 2 classes**
- **Bottom line:** if you are at risk of missing more than 2 classes, contact me as soon as possible!

Paper reviews

- Before each class, students must **read the assigned paper** (see https://ldklab.github.io/assets/classes/ENSF619/schedule.html) and **post a review** on the class D2L discussion board (https://d2l.ucalgary.ca/d2l/le/648686/discussions/List)
- During each class, the paper will be presented in details and students will be encouraged to **engage in critical discussion**

Paper reviews - II



ENSF619 (Winter 2025) Class Schedule

Home Page | Syllabus | Class Schedule | Project Description

The current schedule is tentative and may be changed/updated

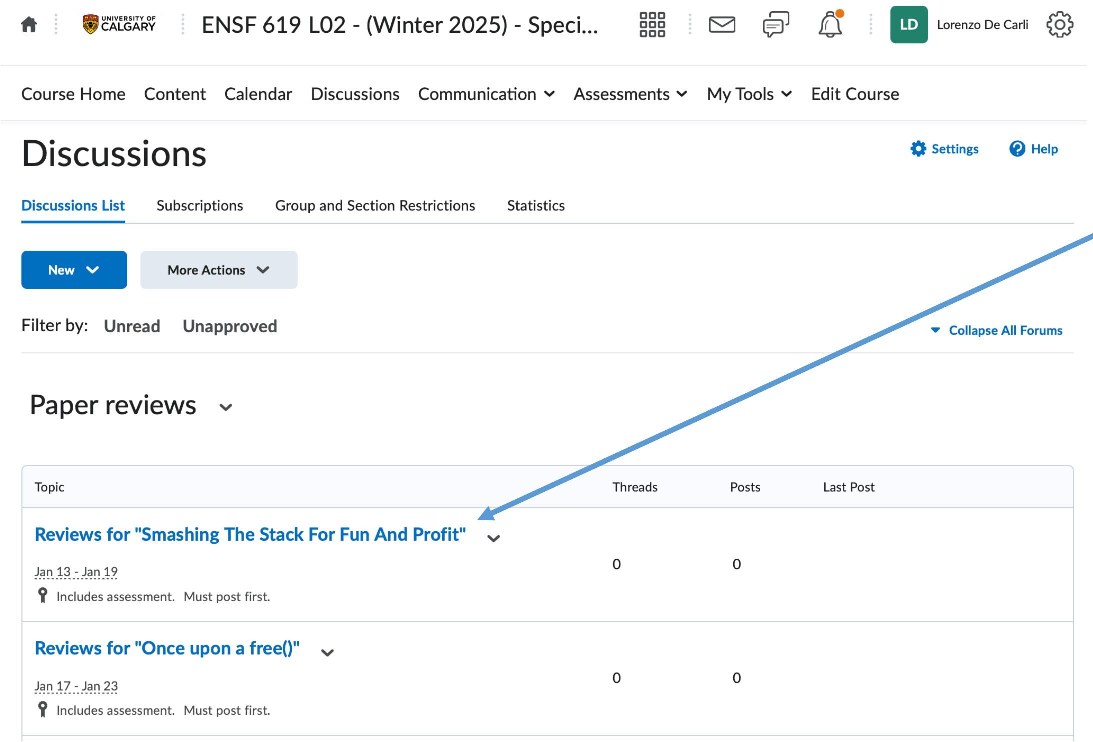
- Paper reviews will be due on D2L by the end of the day before each lecture. More instructions will be provided soon. **No reviews are due in the first week of classes**.
- Project deliverables must be delivered by end of the day on the due dates stated in the class schedule below. Submission of project material must be accomplished using the appropriate assignments on Canvas.
- On Wednesdays marked as **No class**, the instructor will offer open-door office hours (in the instructor's office) at the time of the lecture
- Midterms will be given in class on the dates stated in the class schedule below.

Date	Topic	Assigned Reading	Slides & more	Notes
1/13/2025	**Course intro & policies**	How to read papers: Han99, Kes16	TBA	Presenter: Lorenzo
1/15/2025	**Basics** Introduction to security & modeling	Modules 1.*, 2.1,2.2 on this page	TBA	Presenter: Lorenzo
1/17/2025	**SW Exploits** #1 - Code injection intro	Pointers and memory	TBA	Presenter: Lorenzo
1/20/2025	**SW Exploits** #2 - Stack smashing	Ale99	TBA	Presenter: Lorenzo **Presentation preferences due**
1/22/2025	**No class**			
1/24/2025	**SW Exploits** #3 - Attacking the heap	Ano01		Presenter: Lorenzo
1/27/2025	**SW Exploits** #4 - ROP	Sha07		Presenter: Lorenzo **Project proposals due**

Find paper PDF by following this link

Review due by 1/19 end of the day

Paper reviews - III



Discussions

Paper reviews

Topic	Threads	Posts	Last Post
Reviews for "Smashing The Stack For Fun And Profit" Jan 13 - Jan 19 Includes assessment. Must post first.	0	0	
Reviews for "Once upon a free()" Jan 17 - Jan 23 Includes assessment. Must post first.	0	0	

Click on the discussion topic referring to the paper you just read; submit your review

- Discussions will be due at the end of the day before the lecture in which each paper will be discussed
- **Make sure you are posting your review under the correct discussion topic!**

Paper reviews - IV

- Each review will receive a score between 0 and 10. The review grade for the class will consist of the average of these five review grades
- **Reviews are required** – students are allowed to miss up to two reviews, but no more

Paper reviews - V

- Not everyone is born knowing how to review papers
    - **Can you believe it?**
- For this reason, during the second week reviews will be **graded but not scored**
- At the end of the first week (tentatively) I will send **feedback** to each one of you on how to improve your paper-reviewing skills
- Starting from the third week, **reviews will be graded**

How to read papers

- In order to successfully understand and review scientific papers, it is important to learn **how** to read them
- **Common mistake:** read a paper sequentially the way you would read a book, dedicating equal attention to all parts
    - **It almost never works** - you will drown in the details, miss the big picture, and get very frustrated
    - Instead, try reading a paper selectively, **focusing on the most important parts first**

How to read papers - II

- The trick is to read a paper **multiple times**:
  - **First step:** read abstract, intro and conclusion; skim the beginning of every section in between. **Goal:** understand which problem the paper aims to solve, and get a very basic understanding of how it gets solved
  - **Second step:** read the paper end-to-end, trying to understand the technical details of how problems are solved.
  - For particularly complex papers, **you may need to repeat the second step multiple times**, every time delving deeper into the technical details
- **Additional readings** (linked on the course web page):
  - M. Hanson, “Efficient Reading of Papers in Science and Technology”
  - S. Keshav, “How to Read a Paper”

How to read papers - III

- **Summarizing:** skim the paper first to understand what is the problem being solved, and then try to refine your understanding with further readings

- What happens if you follow this method:

  - **Pass 1:** *this paper proposes some hardware which can execute different networking algorithms*

  - **Pass 2:** *this paper propose a dataflow-based processor which can efficiently run multiple forwarding and classification algorithms, overcoming the limitations of traditional network ASICs*

How to read papers - IV

- What happens if you don’t follow this method and try to understand everything at once:
  - Pass 1: this paper solves a problem in networking
  - Pass 2: this paper solves a problem in networking
  - Pass 3: this paper solves a problem in networking
  - Pass 4: this paper solves a problem
  - Pass 5: this paper
  - Pass 6: ZZzzzzz…

How to read papers - V

- Other tips:
    - **Take notes**
    - Form informal **reading groups** with your classmates so you can read and discuss the paper together
        - **Reviews must still be individual!**
    - **Come to the lecture prepared for discussion** (especially if there are aspects of a paper which you did not understand)

How to review papers

- A paper review is a **discussion of the paper topics, merits, and issues**
- Reviews are fundamental for science - they allow the scientific community to determine the correctness and relevance of scientific work
- For the purpose of this course, writing reviews will force you to **truly reason about each paper, and ensure that you understood the core ideas**

How to review papers - II

- A review of a paper is **not** an unsupported subjective judgement in the style of Youtube comments (“This paper is great”, “This work sucks”, etc.)
- A review of a paper is **not** a summary, however long - it must contain your original assessment of the paper merits and issues

How to review papers - III

- **In order to assess the technical merits of a paper, you must ask yourself questions such as:**
  - Is the problem solved by the paper relevant? What is the impact of the work presented here?
  - Do the experiments satisfyingly back up the paper’s claims?
  - Are the experiments sound?
  - Is the paper theoretically sound?

How to review papers - IV

- **How can I judge if a paper is well-written and clearly presented?**
  - Does the paper clearly state the reasoning and insight behind the solution, and the lessons learned?
  - Does the paper put the results in context (i.e. does it provide background and motivation)?
  - Is the paper written in a clear and concise manner?

How to review papers - V

- For the purpose of this class, **reviews must include**:
  - A **summary** of the contents of the paper, which must include an outline of the core challenges and how they are solved
  - A **discussion of the positives**, if any
  - A **discussion of the negatives**, if any
  - A **conclusion** summarizing your thoughts on the paper
- Each section must consist of a short paragraph; overall length of each review should be approximately between 300 and 500 words

Review grading

- Each review will receive a score between 0 and 10
- Aspects I will evaluate:
  - **Length:** is the review too short or too long ("too long" means that you could have expressed the same concepts in a much smaller number of words) [0-2pts]
  - **Structure:** does the review well-structured as summary of paper/discussion of positives and negatives/conclusion?[0-4pts]
  - **Insight:** does the review formulates an **original**, **insightful** assessment of the paper, or is it just a summarizing and/or repeating what stated in the paper? [0-4pts]
  - **Plagiarism:** Is the review copied and pasted from the results of a Google search?

Bad review examples

- “This paper was great"
- “This paper was great, it showed how TCP congestion issues can be alleviated by incorporating slow start and congestion avoidance”
- “This paper was great, it showed how TCP congestion issues can be alleviated by incorporating slow start and congestion avoidance, but it also had some issue for example some points were not clearly explained. Overall, still pretty cool!”
- “This paper presents” <elaborate summary of the paper w/o any critical consideration>

Good review example

This article describes the slow start and congestion avoidance algorithms, through which TCP is able to tune the rate at which data are sent on the network. The aim of the authors was to create a protocol that (i) could make the best use of the available bandwidth and (ii) could quickly respond to network congestion by reducing the sending rate.

One of the most interesting aspects of the proposed approach is that it is designed for a completely uncooperative network. TCP works without explicit knowledge of the link it is using - it gathers the information it needs while the connection is running. Moreover, congestions are detected without the need of explicit congestion notifications from the gateways. This radical application of the end-to-end principle makes TCP somewhat limited in its features but also very flexible - it does not need any "help" from the underlying levels, so it works almost everywhere. Also, despite its complexity, the TCP state machine requires limited processing power. Therefore, it can be implemented on low-end machines such as embedded devices.

The main problem of Van Jacobson’s approach is that packet losses are always interpreted as a signal of congestion. While this is reasonable - as the author say, this kind of "signal" is always delivered by any type of network - it can cause unnecessary slowdowns in modern WiFi networks. In fact, such radio links are prone to packet losses that are unrelated to congestion and should not trigger congestion avoidance. The consequence is that, on lossy wireless link, often TCP is not able to exploit all the available bandwidth. However, this limitations should be seen in historical perspective: when TCP was designed, the main cause of packet loss was congestion, so the decision makes sense.

Overall, I really enjoyed this paper. Van Jacobson's algorithm is solidly based on previous work on queuing and network congestion, detailed mathematical analysis and sparkling intuitions. The language is plain and clear, with vivid images and a touch of irony which keeps the attention of the reader. Contributions and ideas from other authors are always clearly recognized.

In-class presentation

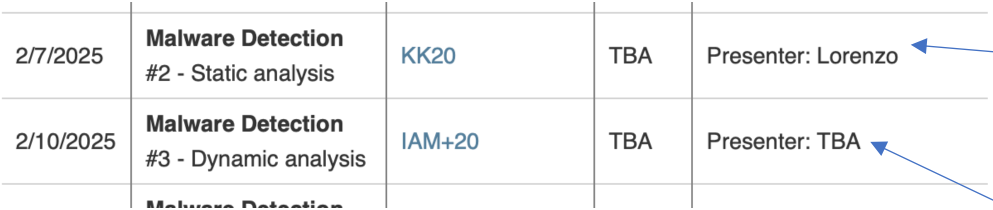
- Each student will need to **present two of the papers on the class schedule**
- Each presentation will be graded 0 to 10
- Overall grade average of the two presentations

In-class presentation - II

- As soon as possible, and **before the ”presentation preference” deadline on the class schedule**, each student must send me:
  - A list of three or more papers that they are willing to present (in order of preference)
  - Whether they wish to present once or twice
- Assignment of students to papers is **first-come first-served** (the sooner you decide, the higher the probability that you will get the paper you prefer)

In-class presentation - III

- Only the class lectures marked as “Presenter: TBA” on the class schedule are **available** for student presentations



2/7/2025	**Malware Detection** #2 - Static analysis	KK20	TBA	Presenter: Lorenzo
2/10/2025	**Malware Detection** #3 - Dynamic analysis	IAM+20	TBA	Presenter: TBA
	Malware Detection			

Not available

Available for student presentations

- I will lead the discussion for roughly the first month of class to give you an idea of what’s expected of you

In-class presentation - grading

- **Many way to succeed, only one way to fail**
- **Failure:** download the slides from the paper’s authors, read them to the class
- **Success:**
    - Provide interesting insights into the paper’s topic
    - Foster a lively discussion among your classmates
    - Perform a live demo to explore some of the points in the paper
    - Review implementation code
    - … the possibilities are endless! **(play to your strengths)**

Presentation - requirements

- You must have enough material to cover a **45-minute slot** (including Q&A)
- Also, you must make an effort to **engage your classmates**: ask questions, solicit opinions!
- You must discuss the assigned paper, but **you are not limited to i**t: you can discuss related topics, or other interesting papers in the same area
- Take it seriously, and **start early** (and, if in doubt, reach out to me)

Midterms

- **2 midterms**, each covering roughly half of the class topics
  - Second midterm may include questions about fundamental concepts **reviewed in the first half of the class**
- **No final exam**
- Refer to **class schedule** for midterm dates

Class project

- For the class project, students will be expected to **complete a guided research project**
- Student should work in teams of two people
- Each team must work on a **different project idea**
- You may either pick one of the project ideas on the class website or come up with **your own project idea**
- You are not limited to the topics discussed in class - **you can make your project about any topic as long as it is related to security!**
- If you are working on security-related research projects with your advisor, you may consider choosing a project **related to your research**

Class project - II

- Completing the project will involve:
  - Coming up with a **project proposal** outlining the problem you want to solve, why it is relevant, and how you are going to solve it
  - Performing any **implementation and evaluation** work the project may require
  - Giving a **project presentation** in front of the class
  - Write a **final project report** detailing the work you did
- **You should start thinking about your project topic and searching for a teammate as soon as possible**
  - Also, look at the **list of project ideas in Canvas**, under the “Files” tab, in the “Project material” folder

Class project - III

- All details on **requirements**, **deliverables** and **grading** are available on the class website at https://ldklab.github.io/assets/classes/ENSF619/project.html
- All **deadlines** can be found on the class schedule at https://ldklab.github.io/assets/classes/ENSF619/schedule.html

Class project – core steps

- The project consists in **conducting a research effort and writing a scientific paper about it**
- To maximize the probability of success, the process has been broken in several steps:
  - Project proposal
  - Two intermediate project reports
  - Project presentation to the class
  - Final project report (also requires delivering any implementation and dataset generated while performing the project)

Format of deliverables

- All deliverables will need to be uploaded using the **appropriate D2L assignment**
- The project proposal, the intermediate report and final report are in the form of PDF documents
  - All your documents **must follow the IEEE article template available at** https://www.ieee.org/conferences/publishing/templates.html

Format of deliverables - II

- The final project presentation **must** consist of a PowerPoint document in pptx format
- You will need to complete and upload your presentation to D2L **by the end of the day before the presentation**
- Each team will have a 20-minute slot to complete the presentation

Format of deliverables - III

- At the end of the project, each team must deliver a **project packet** consisting of:
  - The **final project report** in PDF format as described previously
  - All **code, implementation, and datasets** generated and/or used as part of the project
  - A document describing the **specific contribution of each person in the project team**

Project proposal

- Due **two weeks from now**
- Refer to the project description on the website for specifics
- You **must** discuss your project idea with me before delivering the proposal
- It is your responsibility to ensure that the proposal document matches all requirements in terms of **content, length and format**

Expectations

- All students are generally expected to **attend all classes and deliver all assignments** in order to successfully complete it
    - Exceptions: each student may miss up to two classes and two paper reviews per semester
    - If you cross or are about to cross this threshold, **contact me immediately!**
- **Late assignments will not be accepted/graded**
- **Not meeting the attendance requirement, and/or failing to deliver all assignments, and/or behaving disrespectfully to the instructor and the classmates will entail failing the class**, regardless of the grades obtained in the other assignments

Grading

- **Graded paper reviews:** 20%
- **In-class paper presentations:** 10%
- **Midterm #1:** 15%
- **Midterm #2:** 15%
- **Final project:** 40%
  - Each of the project proposal, intermediate report #1, intermediate report #2 and project presentation counts for 15% of the project grade
  - The final project packet counts for 40% of the project grade
- The instructor may assign up to **two extra percentage points to the final grade** to students that perform particularly well in the class and/or demonstrate engagement and enthusiasm.

Some considerations

- The more you engage in **questions** and **discussion** during the class, the more you will benefit from the class
  - **Other students will benefit too** since a good discussion always bring up original points of view and interesting remarks
  - You may also **contribute** by **posting your comments and questions on the Canvas discussion** for the paper
- **Tips for discussion:** be prepared to articulate your point of view and to discuss it against objections; be prepared to change your mind; **be respectful of classmates**

Some considerations - II

- This class is going to be **challenging** in some respects, especially if you are new to paper-reading and research
- **… but that's the whole point:** challenge you so you can learn skills you did not possess before
- For this reason, there is a **zero-tolerance policy on plagiarism:** if you present online material as your own, have someone else do the work for you, etc., for even one assignment - **you will be referred to the Engineering office for misconduct**

Class (and instructor) introduction

Who am I?

- **Lorenzo De Carli**
    - **Assistant Professor of Computer Science**
    - Politecnico di Torino (Torino, Italy):
        - B.Sc. (2005), M.Sc. (2007) in Computer Engineering
    - University of Wisconsin-Madison:
        - M.Sc. (2010), Ph.D. (2016) In Computer Science
    - Assistant Professor of CS at Colorado State University from 2017 to 2018
    - Now at WPI ☺
    - Interested in **Networking**, **Programming Languages**, **Security**

Who are you?

- I am going to ask each of you to introduce her/himself:
  - Name
  - Status at UCalgary (degree, department, etc.)
  - Expertise/knowledge in security, if any
  - Why are you taking this class?
  - One or more facts about yourself that everyone should know ☺