# COMP 5500 A/CSI 5352 (Fall 2026): Internet Measurements and Security [T, S]

## General Course Information

- **Course Registration Number (CRN):** 31182 (https://central.carleton.ca/prod/bwysched.p_display_course?wsea_code=EXT&term_code=202630&disp=26223346&crn=31182)
- **Classes run:** Sep 09, 2026 to Dec 11, 2026
- **Weekly Schedule:** Monday 11:35am to 2:25pm
- **Room:** Check on Carleton Central
- **Instructor:** Dr. AbdelRahman Abdou (abdou at scs.carleton.ca)
- **Office hours:** By appointment.
- **Office:** HP5130
- **Course prerequisites:** Computer Networking. Computer Security and Cryptography are strongly recommended, but not required.
- **Brightspace access for University of Ottawa Students:** here (https://gradstudents.carleton.ca/faculty-of-graduate-and-postdoctoral-affairs-access-to-brightspace/). University of Ottawa Students who need access to SCS IT resources such, as OpenStack and Nextcloud, must submit a request to SCS Tech Support SCS.Tech.Support@cunet.carleton.ca. The request must be sent from their @cmail.carleton.ca email address, and the email should say which resource is required and for which course (including section).
- **Carleton's Academic Calendar:** here (https://calendar.carleton.ca/academicyear/). Important dates and deadlines can be found here: Dates, Deadlines, and Regulations--Registrar's Office (https://carleton.ca/registrar/regulations/), including class suspension for Fall, Winter breaks, and statutory holidays.
- **Material and Resources:** Research papers. You will need to access them from the digital library of the copyright owners (e.g., IEEE or ACM). For that, you will need to go through the university library online access. In any case, let me know if you have difficulty accessing any of these papers.
    - Additional resources that may be useful:
        - Internet Measurement: Infrastructure, Traffic and Applications (https://www.wiley.com/en-us/Internet+Measurement%3A+Infrastructure%2C+Traffic+and+Applications-p-9780470014615)
        - Why measure the Internet (https://www.internetsociety.org/blog/2020/12/why-were-helping-to-measure-the-internet/)
        - An Overview of Internet Measurements: Fundamentals, Techniques, and Trends (https://epress.lib.uts.edu.au/journals/index.php/ajict/article/view/E1I2122006013)
    - Useful papers on research artifacts:
        - A Survey on Artifacts from CoNEXT, ICN, IMC, and SIGCOMM Conferences in 2017 (https://dl.acm.org/doi/10.1145/3211852.3211864)
        - Open collaborative hyperpapers: a call to action (https://dl.acm.org/doi/10.1145/3314212.3314218)
        - Evaluating the artifacts of SIGCOMM papers (https://dl.acm.org/doi/10.1145/3336937.3336944)
        - The Dagstuhl beginners guide to reproducibility for experimental networking research (https://dl.acm.org/doi/10.1145/3314212.3314217)
        - Learning Networking by Reproducing Research Results (https://dl.acm.org/doi/10.1145/3089262.3089266)
    - Ethics in Internet Measurements:
        - Ethical Considerations in Network Measurement Papers (https://dl-acm-org.proxy.library.carleton.ca/doi/pdf/10.1145/2896816)
    - Useful papers for grad school:
        - How to read a paper (https://web.stanford.edu/class/ee384m/Handouts/HowtoReadPaper.pdf)

  Students are not required to purchase textbooks or other learning materials for this course.

## Course Calendar Description

The course covers measurement methodologies for understanding complex Internet phenomena and behaviors including the spread of vulnerabilities, remote network topologies, attack patterns, content popularity, Internet censorship, service quality, adoption of security

systems, tools for efficient measurements, large-scale data analysis, stats, reproducibility of results, and ethical considerations.

## Grading Scheme

The course has the following grading scheme:

- **20%** reading responses.
- **15%** in-class participation.
- **25%** paper discussion lead.
- **40%** term project.

**Reading Responses.** The 20% on reading responses will be distributed across all the papers we discuss in class. The reading response is *not* a summary of the paper, rather a critical review. This review includes the paper's strengths and weaknesses, as well as the student's own opinion about the paper's motivation, methodology, evaluation, and findings. The **deadline** for emailing the reading response is five minutes before the beginning of each class (i.e., Monday at 11:30am), for all eight student-led classes (i.e., Weeks 3, 4, 6, 8, 9, 10, 11, and 12; see outline below).

**In-class Participation.** The 15% of in-class participation will likewise be distributed across the entire course, 1.88% each class for all eight student-lead classes. You need to be actively involved in the discussions, e.g., asking questions, and commenting on the explanations made by the discussion leader. All students are required to read and understand the papers being discussed in class, as illustrated by the above requirement of reading responses.

**Paper Discussion Lead.** The 25% paper discussion lead is merited based on the students' qualities of presenting papers. Your presentation needs to be as detailed as possible. The presenter/leader must understand the paper quite well, and prepare a slide deck to present a 30-45 minutes presentation explaining the paper. Make sure to cover clearly the paper's objectives, the aspects it is trying to measure, the evaluations used (if any), precautions the authors have taken to (1) ensure the reproducibility of their findings and/or (2) address ethical considerations. Review this guide to a good presentation (https://www.inf.ethz.ch/personal/markusp/teaching/guides/guide-presentations.pdf) (by Professor Püschel, ETH Zürich). Each student is required to sign-up for two papers to present throughout the term. Each presentation is worth 12.5%, which will be commensurate with: the depth of your technical understanding (6%), the quality and professionalism of the presentation (4%), and question handling (2.5%). Selected papers do not have to be on the same day; they could be, but it might be a lot of work for a student to present two papers on one day. The **deadline** for signing-up to leading two paper discussions is Monday, September 21. Papers (in the outline below) under *"Additional Readings"* are optional, but if you like to choose any of these to discuss as a mainstream paper of a class, let me know.

**Term Project.** Finally, the 40% of the project is distributed as follows: 6% planning (including in-class pitch and project proposal), 5% presentation, and 29% on the final report. Every student is required to think about project ideas and discuss them with me. Upon receiving a verbal agreement, students will be required to submit a written 1-page project proposal detailing the project objectives, methodology, and citing relevant literature. The **deadline** for establishing your project idea, and emailing me the written project proposal is October 12. Note that in order to meet this deadline, students will be required to discuss ideas with me early on before they write a proposal. Start thinking about projects early in the course. Don't leave it to the last minute. To decide on a project topic, you may build-upon security research published in previous IMC venues: 2026 (https://conferences.sigcomm.org/imc/2026/accepted-papers/), 2025 (https://conferences.sigcomm.org/imc/2025/accepted-papers/), 2024 (https://conferences.sigcomm.org/imc/2024/accepted-papers/), 2023 (https://conferences.sigcomm.org/imc/2023/program/), 2022 (https://conferences.sigcomm.org/imc/2022/accepted/). You can also lookup papers in the last 2-3 years from IEEE S&P (2026 (https://www.ieee-security.org/TC/SP2026/accepted-papers.html), 2025 (https://www.ieee-security.org/TC/SP2025/accepted-papers.html), 2024 (https://www.ieee-security.org/TC/SP2024/accepted-papers.html)), USENIX Security Symposium (2026 (https://www.usenix.org/conference/usenixsecurity26/technical-sessions), 2025 (https://www.usenix.org/conference/usenixsecurity25/technical-sessions), 2024 (https://www.usenix.org/conference/usenixsecurity24/technical-sessions)), NDSS (2026 (https://www.ndss-symposium.org/ndss2026/accepted-papers/), 2025 (https://www.ndss-symposium.org/ndss2025/accepted-papers/), 2024 (https://www.ndss-symposium.org/ndss2024/accepted-papers/)), and ACM CCS (2026 (https://www.sigsac.org/ccs/CCS2026/program/accepted-papers.html), 2025 (https://sigsac.org/ccs/CCS2025/accepted-papers/), 2024 (https://www.sigsac.org/ccs/CCS2024/program/accepted-papers.html)). Other venues including: Springer Passive and Active Measurements (PAM), Network Traffic Measurement and Analysis (TMA), and ACM Conference on emerging Networking EXperiments and Technologies (CoNext). There are also several occasional measurements workshops like NDSS MADWeb, FOCI, WPEZ. Everyone must then present an 8-minute project pitch in class, ideally using a single slide, on October 19. Finally, the **deadline** to email the final project report is December 23, at 11:59pm EST (Ottawa time). You are highly encouraged to use LaTeX (https://www.latex-project.org/) to prepare your final report. However, feel free to use any document-generation tool, so long as you email me a PDF of your report. The report should not exceed 15 pages in the standard IEEE double-column conference format (https://www.ieee.org/conferences/publishing/templates.html).

**Summary of deliverables**: In summary, over the course of the term, each student will deliver:

- 4 presentations:
  - 2 for leading paper discussions **in the students' selected weeks** (30-45 minutes each, plus questions/comments from the

audience).
    - 1 for project pitch **on October 19** (8 minutes, including questions/comments from the audience).
    - 1 final project presentation **on December 7 or December 11** (about 30 minutes, including questions/comments from the audience).
- Written paper responses for **each week** of student-led presentations. Each response is 1 page, which includes a review for the papers that will be discussed class.
- A one page written project proposal **on October 12**.
- A project final report **on December 23**.

All above deadlines are firm. Missing deadlines will be subject to FULL point deductions. Late deliverables are never accepted for any reason. Submissions are done over email, and there is no "grace period" with respect to a deadline.

## Course Outline (selected papers are subject to change)

| Week | Date | Topic | Material |
|---|---|---|---|
| Week 1 | Sep 14 | Introduction | • Strategies for Sound Internet Measurement (http://www.icir.org/vern/papers/meas-strategies-imc04.pdf) (IMC'04)<br><br>Case Studies:<br>• Affiliate Crookies: Characterizing Affiliate Marketing Abuse (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.698.3506&rep=rep1&type=pdf) (IMC'15)<br>• What lies beneath? Analyzing automated SSH bruteforce attacks (http://people.scs.carleton.ca/~abdou/passwords_full.pdf) (Passwords'15)<br><br>Additional (optional) Readings:<br>• SoK: Benchmarking Flaws in Systems Security (https://ieeexplore.ieee.org/abstract/document/8806739) (Euro S&P'19) |
| Week 2 | Sep 21 | Measurement Tools | Tools:<br>• Zmap (https://zmap.io/): ZMap: Fast Internet-wide Scanning and Its Security Applications (https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_durumeric.pdf) (USENIX Sec.'13)<br>• Censys (https://censys.io/): A search engine backed by Internet-wide scanning (https://dl.acm.org/citation.cfm?id=2813703) (CCS'15)<br>• King: estimating latency between arbitrary Internet end hosts (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.408.9208&rep=rep1&type=pdf) (IMC'02)<br><br>Additional (optional) Readings:<br>• Planetlab: an overlay testbed for broad-coverage services (http://an.kaist.ac.kr/courses/2009/cs540/papers/planetlab_CCR.pdf) (ACM CCR'03)<br>• Avoiding traceroute anomalies with Paris traceroute (https://hal.inria.fr/hal-01097553/document) (IMC'06)<br><br>See also: **Datasets and Measurement tools (measurements.html)** |
| Week 3 | Sep 28 | DNS Security | • Home is where the hijacking is: understanding DNS interception by residential routers (https://dl.acm.org/doi/10.1145/3487552.3487817) (IMC'21)<br>• Measuring DNS-over-HTTPS performance around the world (https://dl.acm.org/doi/10.1145/3487552.3487849) (IMC'21)<br>• Cache me Outside: A New Look at DNS Cache Probing (https://link.springer.com/chapter/10.1007/978-3-030-72582-2_25) (PAM'21)<br><br>Additional (optional) Readings:<br>• TraffickStop: Detecting and Measuring Illicit Traffic Monetization Through Large-Scale DNS Analysis (https://www.researchgate.net/profile/Zhou_Li24/publication/332544947_TraffickStop_Detecting_and_Measuring_Illicit_Traffic_Monetization_Through_Large-Scale_DNS_Analysis/links/5cbb9445299bf12097747a16/TraffickStop-Detecting-and-Measuring-Illicit-Traffic-Monetization-Through-Large-Scale-DNS-Analysis.pdf) (Euro S&P'19)<br>• A Longitudinal, End-to-End View of the DNSSEC Ecosystem (https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-chung.pdf) (USENIX Sec.'17)<br>• Comparative Analysis of DoT and HTTPS Certificate Ecosystems (https://www.ndss-symposium.org/wp-content/uploads/madweb2021_23027_paper.pdf) (NDSS MADWeb'21) |

| | | | |
|---|---|---|---|
| Week 4 | Oct 5 | Internet Vulnerability Analysis | • Short Text, Large Effect: Measuring the Impact of User Reviews on Android App Security & Privacy (https://publications.cispa.saarland/2815/1/main_sp.pdf) (S&P'19)<br>• Augur: Internet-Wide Detection of Connectivity Disruption (https://www.computer.org/csdl/proceedings/sp/2017/5533/00/07958591.pdf) (Oakland'17)<br>• Waves of Malice: A Longitudinal Measurement of the Malicious File Delivery Ecosystem on the Web (https://dl.acm.org/doi/pdf/10.1145/3321705.3329807) (AsiaCCS'19)<br>• You've Got Vulnerability: Exploring Effective Vulnerability Notifications (https://zakird.com/papers/sec16-vuln-notifications.pdf) (USENIX Sec.'16)<br><br>Additional (optional) Readings:<br>• Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices (https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final228.pdf) (USENIX Sec.'12) |
| ~~Week 5~~ | ~~Oct 12~~ | Thanksgiving | **(No class)** |
| Week 6 | Oct 19 | Privacy and Tracking (and project pitches) | • Project pitch presentations (8 minutes each).<br>• Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach (https://moniotrlab.ccis.neu.edu/wp-content/uploads/2019/09/ren-imc19.pdf) (IMC'19)<br><br>Additional (optional) Readings:<br>• Third-Party Web Tracking: Policy and Technology (https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6234427) (Oakland'12)<br>• Tracing Cross Border Web Tracking (https://conferences.sigcomm.org/imc/2018/papers/imc18-final154.pdf) (IMC'18) |
| ~~Week 7~~ | ~~Oct 26~~ | Fall Break | **(No class)** |
| Week 8 | Nov 2 | HTTPS and TLS | • In Log We Trust: Revealing Poor Security Practices with Certificate Transparency Logs and Internet Measurements (https://www.net.in.tum.de/fileadmin/bibtex/publications/papers/pam18ctlog.pdf) (PAM'18)<br>• Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks (https://dl.acm.org/doi/10.1145/3372297.3417252) (CCS'20)<br>• Does Certificate Transparency Break the Web? Measuring Adoption and Error Rate (https://storage.googleapis.com/pub-tools-public-publication-data/pdf/314fca4308f1dd1faeeb975bf25f6904af0264f9.pdf) (S&P'19)<br><br>Additional (optional) Readings:<br>• CAge: Taming Certificate Authorities by Inferring Restricted Scopes (https://jhalderm.com/pub/papers/cage-fc13.pdf) (FC'13)<br>• Analysis of the HTTPS Certificate Ecosystem (https://jhalderm.com/pub/papers/https-imc13.pdf) (IMC'13) |
| Week 9 | Nov 9 | Hate, Harassment, and Online Abuse | • TROLLMAGNIFIER: Detecting State-Sponsored Troll Accounts on Reddit? (https://arxiv.org/pdf/2112.00443) (Oakland'22)<br>• On the Origins of Memes by Means of Fringe Web Communities (https://arxiv.org/pdf/1805.12512.pdf) (IMC'18) |
| Week 10 | Nov 16 | Internet Censorship | • How Great is the Great Firewall? Measuring China's DNS Censorship (https://www.usenix.org/system/files/sec21-hoang.pdf) (USENIX Sec.'21)<br>• ICLab: A Global Longitudinal Internet Censorship Measurement Platform (https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9152784) (Oakland'20) |
| Week 11 | Nov 23 | Analyzing Attacks | • Weaponizing Middleboxes for TCP Reflected Amplification (https://www.usenix.org/system/files/sec21-bock.pdf) (USENIX Sec.'21)<br>• Who Knocks at the IPv6 Door?: Detecting IPv6 Scanning (https://dl.acm.org/citation.cfm?id=3278553) (IMC'18)<br><br>Additional (optional) Readings:<br>• DROWN: Breaking TLS using SSLv2 (https://drownattack.com/drown-attack-paper.pdf) (USENIX Sec.'16)<br>• An Internet-Wide View of Internet-Wide Scanning (https://jhalderm.com/pub/papers/scanning-sec14.pdf) (USENIX Sec.'14) |

| | | | |
|---|---|---|---|
| Week 12 | Nov 30 | Internet Core | • BGP Communities: Even more Worms in the Routing Can (https://people.mpi-inf.mpg.de/~fstreibelt/preprint/communities-imc2018.pdf) (IMC'18)<br>• When the Dike Breaks: Dissecting DNS Defenses During DDoS (https://indico.dns-oarc.net/event/29/contributions/647/attachments/624/1005/paper.pdf) (IMC'18)<br>• Neither Snow Nor Rain Nor MITM... An Empirical Analysis of Email Delivery Security (https://jhalderm.com/pub/papers/mail-imc15.pdf) (IMC'15)<br>Additional Readings (non-security):<br>• Reverse Engineering the Internet (https://dl.acm.org/doi/abs/10.1145/972374.972376) (SIGCOMM'04)<br>• Census and survey of the visible Internet (https://www.isi.edu/~johnh/PAPERS/Heidemann08a.pdf) (IMC'08) |
| Week 13 | Dec 7 | Final Project Presentations | |
| | Dec 11 | Final Project Presentations | |
| Week ∞ | Dec 23 | Final project report due | **(No class)** |

## Graduate Academic Advisors

The Graduate Advisors for the School of Computer Science are available in Room 5302 HP; or by email (mailto:grad.scs@carleton.ca). The graduate advisors can assist with understanding your academic audit and the remaining courses required to meet graduation requirements.

## SCS Computer Laboratory

Students taking a COMP course can access the SCS computer labs. The lab schedule and location can be found here (https://carleton.ca/scs/tech-support/computer-laboratories/). All SCS computer lab and technical support information can be found here (https://carleton.ca/scs/tech-support/). Technical support staff may be contacted in-person or virtually, see this (https://carleton.ca/scs/tech-support/contact-it-support/) page for details.

## Mental Health and Wellness

The Carleton Wellness Website (https://wellness.carleton.ca/) is a wonderful resource link to include in the course outline for students

## Academic Accommodations and Regulations

**Academic Accommodations.** Carleton is committed to providing academic accessibility for all individuals. You may need special arrangements to meet your academic obligations during the term. The accommodation request processes are outlined on the Academic Accommodations website (https://students.carleton.ca/course-outline/).

**Chat GPT/Generative AI Usage.** As our understanding of the uses of AI and its relationship to student work and academic Integrity continue to evolve, students are generally required to discuss their use of AI in any circumstance not described here with the course instructor to ensure it supports the learning goals for the course. However, note the following:

- Many of the assessed activities in this course were designed to be completed by an individual working alone. Unless it is explicitly stated otherwise, the use of any AI system will be considered academic misconduct. This includes, but is not limited to, chatbots or code generators (e.g., ChatGPT, Google Gemini, Microsoft Copilot), research assistants (e.g., Elicit), and image generators (e.g., Stable Diffusion, Dall-E), etc.
- An exception to the above rule is made for automated grammar and punctuation checking tools (such as Grammarly).
- References to any material you use but did not originate must use the IEEE/APA/MLA citation style. Failure to reference materials correctly can result in severe penalties, and the use of manufactured (i.e., falsified) or misleading references will be treated as evidence of plagiarism and considered academic misconduct.
- Everything you submit for evaluation (i.e., assignments, quizzes, tutorials, examinations, etc.) must be the result of your own work and only your own work. If you copy more than five consecutive words or any non-trivial snippet of code from a single source without providing a valid reference, then that is considered plagiarism.

**Academic Integrity.** Students are expected to uphold the values of academic Integrity, which include fairness, honesty, trust, and responsibility. Examples of actions that compromise these values include but are not limited to plagiarism, accessing unauthorized sites for assignments or tests, unauthorized collaboration on assignments or exams, and using artificial intelligence tools such as ChatGPT when your assessment instructions say it is not permitted.

Misconduct in scholarly activity will not be tolerated and will result in consequences as outlined in Carleton University's Academic Integrity Policy (https://carleton.ca/secretariat/wp-content/uploads/sites/158/Academic-Integrity-Policy-2021.pdf). A list of standard sanctions in the Faculty of Science can be found here (https://science.carleton.ca/students/academic-integrity/).

Additional details about this process can be found on the Faculty of Science Academic Integrity (https://science.carleton.ca/students/academic-integrity/) website.

Students are expected to familiarize themselves with and abide by Carleton University's Academic Integrity Policy (https://carleton.ca/secretariat/wp-content/uploads/sites/158/Academic-Integrity-Policy-2021.pdf). Claiming ignorance of or confusion about the academic integrity standards as described in the Policy does not excuse a student from responsibility for violations of those standards.

**Student Rights & Responsibilities.** Students are expected to act responsibly and engage respectfully with other students and members of the Carleton and the broader community. See the 7 Rights and Responsibilities Policy (https://carleton.ca/studentaffairs/student-rights-and-responsibilities/#sect1.1) for details regarding the expectations of non-academic behaviour of students. Those who participate with another student in the commission of an infraction of this Policy will also be held liable for their actions.