# COMP 5900 E/CSI 5139 IF00 (Fall 2021): Internet Measurements and Security [T, S]

## General Course Information

- **Course Registration Number (CRN):** 31289 (https://central.carleton.ca/prod/bwysched.p_display_course?wsea_code=EXT&term_code=202130&disp=14533511&crn=31289) (OCICS (http://www.ocics.ca/node/5933))
- **Classes run:** Sep 07, 2021 to Dec 10, 2021
- **Weekly Schedule:** Wednesday 2:35pm to 5:25pm
- **Room:** (Zoom link (https://carleton-ca.zoom.us/j/94525151568); passcode available through Brightspace).
- **Instructor:** Dr. AbdelRahman Abdou (abdou at scs.carleton.ca)
- **Office hours:** virtual (Zoom link (https://carleton-ca.zoom.us/j/92032256691); passcode available through Brightspace). Tuesdays and Thursdays, 10:00am to 11:00am.
- **Material and Resources:** Internet Measurement: Infrastructure, Traffic and Applications, 2006 (Textbook by Mark Crovella and Balachander Krishnamurthy), guide to a good presentation (https://www.inf.ethz.ch/personal/markusp/teaching/guides/guide-presentations.pdf) (by Professor Püschel, ETH Zürich), and how to read a paper (http://blizzard.cs.uwaterloo.ca/keshav/home/Papers/data/07/paper-reading.pdf). In addition to the previous helpful resources, the primary materials we will be using throughout the term are the papers in the outline below. I used landing links to the papers as much as I was able to find (e.g., author's copies or technical report versions). For a few papers, however, 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.
- **CULearn for Ottawa U students:** for access, fill out this form (https://gradstudents.carleton.ca/wp-content/uploads/Access-to-CULearn.pdf) and email it to Grad Studies.
- **Course prerequisites:** Computer Networking. Computer Security and Cryptography are strongly recommended, but not required. Otherwise, instructor permission is required.

## Course Summary

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 involvement.
- **25%** paper discussion lead.
- **40%** term project.

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., Wednesday at 2:30pm), for all nine student-lead classes (i.e., Weeks 3 — 7 and 9 — 12; see outline below).

The 15% of in-class involvement will likewise be distributed across the entire course, 1.67% each class for all nine 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 or project presenter. All students are required to read and understand the papers being discussed in class, as illustrated by the above requirement of reading responses.

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. **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 **Wednesday, September 15**. 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.

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 6**. 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: 2020 (https://conferences.sigcomm.org/imc/2020/accepted/), 2019 (http://conferences2.sigcomm.org/imc/2019/program), 2018 (https://conferences2.sigcomm.org/imc/2018/program/), 2017 (https://conferences2.sigcomm.org/imc/2017/program/), 2016 (http://conferences2.sigcomm.org/imc/2016/program.html). You can also lookup papers in the last 2-3 years from IEEE S&P (2021 (https://www.ieee-security.org/TC/SP2021/program-papers.html), 2020 (https://www.ieee-security.org/TC/SP2020/program-papers.html), 2019 (https://www.ieee-security.org/TC/SP2019/program-papers.html)), USENIX Security Symposium (2021 (https://www.usenix.org/conference/usenixsecurity21/technical-sessions), 2020 (https://www.usenix.org/conference/usenixsecurity20/technical-sessions), 2019 (https://www.usenix.org/conference/usenixsecurity19/technical-sessions)), NDSS (2021 (https://www.ndss-symposium.org/ndss2021/accepted-papers/), 2020 (https://www.ndss-symposium.org/ndss-program/2020-program/), 2019 (https://www.ndss-symposium.org/ndss-program/ndss-symposium-2019-program/)), and ACM CCS (2020 (https://sigsac.org/ccs/CCS2020/accepted-papers.html), 2019 (https://sigsac.org/ccs/CCS2019/index.php/program/accepted-papers/) and 2018 (https://www.sigsac.org/ccs/CCS2018/accepted/papers/)). Everyone must then present an 8-minute project pitch in class, ideally using a single slide, on **October 13**. Finally, the **deadline** to email the final project report is **December 17, 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 (30-45 minutes each, plus questions/comments from the audience).
    - 1 for project pitch on October 13 (8 minutes, including questions/comments from the audience).
    - 1 final project presentation on December 1 or December 8 (about 20 minutes, including questions/comments from the audience).
- 10 written paper responses, 1 page each, which includes a review for 2 papers.
- A one page written project proposal on October 6.
- A project final report on December 17.

All above deadlines are firm. Missing deadlines will be subject to point deductions.

## Page Updates and Action Items

- **Sep 8:** **Immediate Action Required:** Sign-up for any two of the papers in the outline below to lead the discussion on these papers. Email me your choices ASAP. It is first-come-first-served.

## Course Outline

| Week | Date | Topic | Material |
|---|---|---|---|
| Week 1 | Sep 8 | Introduction | • Strategies for Sound Internet Measurement (http://www.icir.org/vern/papers/meas-strategies-imc04.pdf) (IMC'04)<br>• SoK: Benchmarking Flaws in Systems Security (http://ssrg.nicta.com/publications/csiro_full_text/vanderKouwe_HABG_19.pdf) (Euro S&P'19)<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) |
| Week 2 | Sep 15 | 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>Additional 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>See also: Twitter's random tweets (https://developer.twitter.com/en/products/tweets/sample.html), Alexa's (https://aws.amazon.com/alexa-top-sites/) top 1M sites (http://s3-us-west-1.amazonaws.com/umbrella-static/index.html) (and relevant snallygaster (https://github.com/hannob/snallygaster/) tool), RIPE Atlas (https://atlas.ripe.net/), Caida Ark (http://www.caida.org/projects/ark/), Shodan (https://www.shodan.io/), Luminati (https://luminati.io/), ProxyRack (https://www.proxyrack.com/), Infatica (https://infatica.io/), Internetwache (https://en.internetwache.org/), Selenium browser (https://www.selenium.dev/), crt.sh (crt.sh), Certs databse (https://www.ccadb.org/cas/intermediates), thingful (thingful.net). |
| Week 3 | Sep 22 | DNS Security | • Roll, Roll, Roll your Root: A Comprehensive Analysis of the First Ever DNSSEC Root KSK Rollover (https://www.isi.edu/~hardaker/papers/2019-10-ksk-roll.pdf) (IMC'19)<br>• An Empirical Study of the Cost of DNS-over-HTTPS (http://www.eecs.qmul.ac.uk/~tysong/files/DoH.pdf) (IMC'19)<br>• An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come? (https://www.liubaojun.org/uploads/1/1/8/3/118316462/imc2019.pdf) (IMC'19)<br>Additional 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) |

| | | | |
|---|---|---|---|
| Week 4 | Sep 29 | 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>Additional 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 6 | Adoption of Internet Security Systems | • Tracing Cross Border Web Tracking (https://conferences.sigcomm.org/imc/2018/papers/imc18-final154.pdf) (IMC'18)<br>• Towards a Rigorous Methodology for Measuring Adoption of RPKI Route Validation and Filtering (https://ccronline.sigcomm.org/wp-content/uploads/2017/09/sigcomm-ccr-paper134.pdf) (ACM CCR'18)<br>• Server-side Adoption of Certificate Transparency (https://www.ida.liu.se/~nikca89/papers/pam18.pdf) (PAM'18)<br>• Coming of Age: A Longitudinal Study of TLS Deployment (https://eprints.networks.imdea.org/1884/1/imc_ssl.pdf) (IMC'18)<br>Additional Readings:<br>• Measuring HTTPS Adoption on the Web (https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-felt.pdf) (USENIX Sec.'17) |
| Week 6 | Oct 13 | Privacy and Tracking (and project pitches) | • Project pitch presentations (8 minutes each).<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)<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) |
| Week 7 | Oct 20 | HTTPS and TLS | • Analysis of the HTTPS Certificate Ecosystem (https://jhalderm.com/pub/papers/https-imc13.pdf) (IMC'13)<br>• 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>• 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>Additional Readings:<br>• CAge: Taming Certificate Authorities by Inferring Restricted Scopes (https://jhalderm.com/pub/papers/cage-fc13.pdf) (FC'13) |
| ~~Week 8~~ | ~~Oct 27~~ | Fall Break. | **(No Classes)** |
| Week 9 | Nov 3 | Internet Measurements for Social, Security, and Economic Analysis | • On the Origins of Memes by Means of Fringe Web Communities (https://arxiv.org/pdf/1805.12512.pdf) (IMC'18)<br>• Follow the Money: Understanding Economics of Online Aggregation and Advertising (https://people.cs.umass.edu/~phillipa/papers/GECK.pdf) (IMC'13) |

| | | | |
|---|---|---|---|
| Week 10 | Nov 10 | Internet Censorship | • Global Measurement of DNS Manipulation (https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-pearce.pdf) (USENIX Sec.'17)<br>• Incentivizing Censorship Measurements via Circumvention (https://censorbib.nymity.ch/pdf/Nisar2018a.pdf) (SIGCOMM'18)<br>• Where The Light Gets In: Analyzing Web Censorship Mechanisms in India (https://arxiv.org/pdf/1808.01708.pdf) (IMC'18) |
| Week 11 | Nov 17 | Analyzing Attacks | • Internet Protocol Cameras with No Password Protection: An Empirical Investigation (http://users.eecs.northwestern.edu/~hxb0652/HaitaoXu_files/PAM2018.pdf) (PAM'18)<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)<br>• Who Knocks at the IPv6 Door?: Detecting IPv6 Scanning (https://dl.acm.org/citation.cfm?id=3278553) (IMC'18) |
| Week 12 | Nov 24 | 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://djw.cs.washington.edu/papers/hotnets-reverse-final.pdf) (SIGCOMM'04)<br>• Census and survey of the visible Internet (https://www.isi.edu/~johnh/PAPERS/Heidemann08a.pdf) (IMC'08) |
| Week 13 | Dec 1 | Stats and Final Project Presentations | •<br>•<br>•<br>Additional Readings:<br>• SketchLearn: Relieving User Burdens in Approximate Measurement with Automated Statistical Inference (https://www.cse.cuhk.edu.hk/~pclee/www/pubs/tech_sketchlearn.pdf) (SIGCOMM'18) |
| Week 14 | Dec 8 | Final Project Presentations | Project presentations |

# University Policies

For information about Carleton's academic year, including registration and withdrawal dates, see Carleton' Calendar (https://calendar.carleton.ca/academicyear/).

**Pregnancy Obligation.** Please contact your instructor with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details, visit Equity Services (https://www.carleton.ca/equity/wp-content/uploads/Student-Guide-to-Academic-Accommodation.pdf).

**Religious Obligation.** Please contact your instructor with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details, visit Religious/Spiritual Observances (https://carleton.ca/equity/focus/discrimination-harassment/religious-spiritual-observances/).

**Academic Accommodations for Students with Disabilities.** If you have a documented disability requiring academic accommodations in this course, please contact the Paul Menton Centre for Students with Disabilities (PMC) (https://www.carleton.ca/pmc) at 613-520-6608 or pmc@carleton.ca for a formal evaluation or contact your PMC coordinator to send your instructor your Letter of Accommodation at the beginning of the term. You must also contact the PMC no later than two weeks before the first in-class scheduled test or exam requiring accommodation (if applicable). After requesting accommodation from PMC, meet with your instructor as soon as possible to ensure accommodation arrangements are made.

**Survivors of Sexual Violence.** As a community, Carleton University is committed to maintaining a positive learning, working and living environment where sexual violence will not be tolerated, and survivors are supported through academic accommodations as per Carleton's Sexual Violence Policy. For more information about the services available at the university and to obtain information about sexual violence and/or support, visit Carleton's Sexual Violence support (https://carleton.ca/sexual-violence-support).

**Accommodation for Student Activities.** Carleton University recognizes the substantial benefits, both to the individual student and for the university, that result from a student participating in activities beyond the classroom experience. Reasonable accommodation must be provided to students who compete or perform at the national or international level. Please contact your instructor with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. More information can be found here (https://carleton.ca/senate/wp-content/uploads/Accommodation-for-Student-Activities-1.pdf).

**Medical Certificate.** Please use the official medical certificate form (https://www.carleton.ca/registrar/forms) for the deferral of assignments due to medical reasons.

**Student Academic Integrity Policy.** Every student should be familiar with the Carleton University student academic integrity policy. A student found in violation of academic integrity standards may be awarded penalties which range from a reprimand to receiving a grade of *F* in the course or even being expelled from the program or University. Some examples of offences are: plagiarism and unauthorized co-operation or collaboration. Information on this policy may be found in the Undergraduate Calendar.

**Plagiarism.** As defined by Senate, "plagiarism is presenting, whether intentional or not, the ideas, expression of ideas or work of others as one's own". Such reported offences will be reviewed by the office of the Dean of Science.

**Unauthorized Co-operation or Collaboration.** Senate policy states that "to ensure fairness and equity in assessment of term work, students shall not co-operate or collaborate in the completion of an academic assignment, in whole or in part, when the instructor has indicated that the assignment is to be completed on an individual basis". Please refer to the course outline statement or the instructor concerning this issue.