

COMP 5900 X/CSI 5139IX (Fall 2020): Internet Measurements and Security [T, A, S]

General Course Information

- **Course Registration Number (CRN):** 31179 (https://central.carleton.ca/prod/bwysched.p_display_course?wsea_code=EXT&term_code=202030&disp=12661299&crn=31179) (OCICS (<http://www.ocics.ca/node/5323>))
- **Classes run:** Sep 07, 2020 to Dec 07, 2020
- **Weekly Schedule:** Friday 2:30pm to 5:30pm
- **Room:** Virtual through BigBlueButton on cuLearn
- **Instructor:** Prof. AbdelRahman Abdou (abdou at scs.carleton.ca)
- **Office hours:** Friday, 11am to 12pm (virtual)
- **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.

Course Outline

Week	Date	Topic	Discussion Leader	Material
Week 1	Sep 11	Introduction		<ul style="list-style-type: none"> • Strategies for Sound Internet Measurement (http://www.icir.org/vern/papers/meas-strategies-imc04.pdf) (IMC'04) • SoK: Benchmarking Flaws in Systems Security (http://ssrg.nicta.com/publications/csiro_full_text/vanderKouwe_HABG_19.pdf)
				Case Studies: <ul style="list-style-type: none"> • Affiliate Crookies: Characterizing Affiliate Marketing Abuse (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1.6985.9001.1000.1000.1000) (IMC'15) • What lies beneath? Analyzing automated SSH bruteforce attacks (http://people.scs.carleton.ca/~abdou/passwords_full.pdf)

			Tools:	<ul style="list-style-type: none"> 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) Censys (https://censys.io/): A search engine backed by Internet-wide scanning (https://dl.acm.org/citation.cfm?id=281370): King: estimating latency between arbitrary Internet end hosts (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1.1) (IMC'02)
Week Sep 2	18	Measurement Tools	Additional Readings:	<ul style="list-style-type: none"> Planetlab: an overlay testbed for broad-coverage services (http://an.kaist.ac.kr/courses/2009/cs540/papers/planetlab_CCI) Avoiding traceroute anomalies with Paris traceroute (https://hal.inria.fr/hal-01097553/document) (IMC'06) <p>See also: Twitter's random tweets (https://developer.twitter.com/en/products/tweets/sample.html), Alexa's (https://aws.amazon.com/s3-us-west-1.amazonaws.com/umbrella-static/index.html) (and relevant snallygaster (https://github.com/hannob/snallygaster), Atlas (https://atlas.ripe.net/), Caida Ark (http://www.caida.org/projects/ark/), Shodan (https://www.shodan.io/), Luminati (https://luminati.com/), Infatica (https://infatica.io/), Internetwache (https://en.internetwache.org/), Selenium browser (ht (crt.sh), Certs databse (https://www.ccadb.org/cas/intermediates), thingful (thingful.net).</p>
				<ul style="list-style-type: none"> Roll, Roll, Roll your Root: A Comprehensive Analysis of the First Ever DNSSEC Root KSK Rollover (https://www.isi.edu/~har) (IMC'19) An Empirical Study of the Cost of DNS-over-HTTPS (http://www.eecs.qmul.ac.uk/~tyson/files/DoH.pdf) (IMC'19) An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come? (https://www.liubaajun.org/uploads/1/1/8/3/118316462/imc2019.pdf) (IMC'19)
Week Sep 3	25	DNS Security	Additional Readings:	<ul style="list-style-type: none"> TrafficStop: Detecting and Measuring Illicit Traffic Monetization Through Large-Scale DNS Analysis (https://www.researchgate.net/profile/Zhou_Li24/publication/332544947_TrafficStop_Detecting_and_Measuring_Illicit_Tr_Scale_DNS_Analysis/links/5cbb9445299bf12097747a16/TrafficStop-Detecting-and-Measuring-Illicit-Traffic-Monetization-1-Analysis.pdf) (Euro S&P'19) A Longitudinal, End-to-End View of the DNSSEC Ecosystem (https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-paper-17.pdf) (USENIX Sec.'17)
				<ul style="list-style-type: none"> Augur: Internet-Wide Detection of Connectivity Disruption (https://www.computer.org/csdl/proceedings/sp/2017/5533/00) Waves of Malice: A Longitudinal Measurement of the Malicious File Delivery Ecosystem on the Web (https://dl.acm.org/do) (AsiaCCS'19) You've Got Vulnerability: Exploring Effective Vulnerability Notifications (https://zakird.com/papers/sec16-vuln-notification)
Week Oct 4	2	Internet Vulnerability Analysis	Additional Readings:	<ul style="list-style-type: none"> Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices (https://www.usenix.org/system/files/corfinal228.pdf) (USENIX Sec.'12)
				<ul style="list-style-type: none"> Towards a Rigorous Methodology for Measuring Adoption of RPKI Route Validation and Filtering (https://ccronline.sigcomm.org/content/uploads/2017/09/sigcomm-ccr-paper134.pdf) (ACM CCR'18) Server-side Adoption of Certificate Transparency (https://www.ida.liu.se/~nikca89/papers/pam18.pdf) (PAM'18) Coming of Age: A Longitudinal Study of TLS Deployment (https://eprints.networks.imdea.org/1884/1/imc_ssl.pdf) (IMC'18)
Week Oct 5	9	Adoption of Internet Security Systems	Additional Readings:	<ul style="list-style-type: none"> Measuring HTTPS Adoption on the Web (https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-felt.pdf)
				<ul style="list-style-type: none"> All students Project pitch presentations (8 minutes each). Tracing Cross Border Web Tracking (https://conferences.sigcomm.org/imc/2018/papers/imc18-final154.pdf) (IMC'18) Third-Party Web Tracking: Policy and Technology (https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6234427) Internet Protocol Cameras with No Password Protection: An Empirical Investigation (http://users.eecs.northwestern.edu/~hxb0652/HaitaoXu_files/PAM2018.pdf) (PAM'18) Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach (http://content/uploads/2019/09/ren-imc19.pdf) (IMC'19)
Week Oct 6	16	Privacy and Tracking (and project pitches)		<ul style="list-style-type: none"> Analysis of the HTTPS Certificate Ecosystem (https://jhalderm.com/pub/papers/https-imc13.pdf) (IMC'13) 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) Does Certificate Transparency Break the Web? Measuring Adoption and Error Rate (https://storage.googleapis.com/pub-tdata/pdf/314fca4308f1dd1faeeb975bf25f6904af0264f9.pdf) (S&P'19)
Week Oct 7	23	HTTPS and TLS	Additional Readings:	<ul style="list-style-type: none"> CAGE: Taming Certificate Authorities by Inferring Restricted Scopes (https://jhalderm.com/pub/papers/cage-fc13.pdf) (FC'13)
Week Oct 8	30	Fall Break.	(No Classes)	
Week Nov 9	6	Internet Measurements for Social, Security, and Economic Analysis		<ul style="list-style-type: none"> On the Origins of Memes by Means of Fringe Web Communities (https://arxiv.org/pdf/1805.12512.pdf) (IMC'18) Short Text, Large Effect: Measuring the Impact of User Reviews on Android App Security & Privacy (https://publications.cis) (S&P'19) Follow the Money: Understanding Economics of Online Aggregation and Advertising (https://people.cs.umass.edu/~phillij)
Week Nov 10	13	Internet Censorship		<ul style="list-style-type: none"> Global Measurement of DNS Manipulation (https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-pear) Incentivizing Censorship Measurements via Circumvention (https://censorbib.nymity.ch/pdf/Nisar2018a.pdf) (SIGCOMM'18) Where The Light Gets In: Analyzing Web Censorship Mechanisms in India (https://arxiv.org/pdf/1808.01708.pdf) (IMC'18)

Week 11	Nov 20	Analyzing Attacks	<ul style="list-style-type: none"> • DROWN: Breaking TLS using SSLv2 (https://drownattack.com/drown-attack-paper.pdf) (USENIX Sec.'16) • An Internet-Wide View of Internet-Wide Scanning (https://jhalderm.com/pub/papers/scanning-sec14.pdf) (USENIX Sec.'14) • Who Knocks at the IPv6 Door?: Detecting IPv6 Scanning (https://dl.acm.org/citation.cfm?id=3278553) (IMC'18)
Week 12	Nov 27	Stats and Final Project Presentations	<ul style="list-style-type: none"> • Material TBD. • Project title: TBD. • Project title: TBD. <p>Additional Readings:</p> <ul style="list-style-type: none"> • SketchLearn: Relieving User Burdens in Approximate Measurement with Automated Statistical Inference (https://www.cse.cuhk.edu.hk/~pcline/www/pubs/tech_sketchlearn.pdf) (SIGCOMM'18)
Week 13	Dec 4	Final Project Presentations	<ul style="list-style-type: none"> • Project title: TBD. • Project title: TBD. • Project title: TBD.

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 Equity Services (<https://www.carleton.ca/equity/wp-content/uploads/Student-Guide-to-Academic-Accommodation.pdf>).

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.