CSExyz: Network Anonymity and Privacy

Credits: 4

Desirable Pre-requisites: Computer Networks, Introductory Course in Systems and Network Security (e.g. Foundations of Computer Security) or any equivalent course. This is a semi-seminar format course aimed towards Ph.D. and M.Tech students. Interested B.Tech students could also audit the class.

Overview of topics to be covered: Historical network anonymity and privacy protocols – MIXes and MIXnets, various theoretical and practical attack strategies against high and low-latency anonymity networks, practical traffic analysis against modern anonymity systems like Tor, Freenet, GNUnet, JAP, defenses against traffic analysis attacks, performance vs anonymity trade-offs, side-channel attacks, covert channel communications, pseudonymity and privacy, Anonymous P2P communication systems (e.g. Oneswarm), traffic analysis against anonymous VoIP communications, Internet censorship and censorship resistance tools and strategies, large-scale Internet surveillance and anti-surveillance, decoy routing.

Post conditions (on students capability after successfully completing the course):

- An appreciation of various research challenges in the area of Network Anonymity and Privacy (e.g. systems, capabilities, vulnerabilities, use cases etc.)
- Ability to undertake research efforts in Network Anonymity and Privacy and allied areas such as network surveillance, censorship and resistance.

Expected number of students: Less than 30.

Course structure:

Good part of the first half of the class (about 5 weeks) would involve the instructor giving lectures to students in topics pertinent to the research areas. The remainder of the classes would involve the students presenting relevant papers (of their choice) to everyone in the class. Students (other than the presenter) would be expected to participate in productive discussion about to various challenges of the research topic being discussed. Moreover every week, each student would be expected to submit a weekly write-up which would mostly be either a review or critique of a paper, or some design questions, relevant to the topics covered in the class (e.g. what do you think could be vulnerabilities in the XYZ system that the authors didn't mention upfront in the paper and could you suggest ways to defend the system against those vulnerabilities). There would be a mid-term where the students would be tested on topics covered during the lectures. For finals, the students would be expected to write a survey paper, reviewing several papers on a chosen topic.

Tentative per-week plan:

Week	Topics to be covered	Nature of assignments
1	- Overview of Anonymous Communication Systems. - Early efforts in anonymous communication systems – Onion Routing, Mixminion, Freenet, Crowds.	Weekly write-up (review, critique, design issues etc.)
2	- Metrics of anonymity – various definitions of anonymity (e.g. k-anonymity, l-diversity), early efforts to quantify anonymity. - Modern Anonymity Networks – Tor.	Weekly write-up (review, critique, design issues etc.)
3	- Modern Anonymity Networks – Gnunet, I2P, JAP, etc. - Practical traffic analysis against Tor – Some important attacks.	Weekly write-up (review, critique, design issues etc.)
4	- Network censorship and anti-censorship.	Weekly write-up (review, critique, design issues etc.)
5	- Scope for future research.	Weekly write-up (review, critique, design issues etc.)
6	- System design paradigms – Onion routing based designs vs probabilistic based routing (e.g. Crowds). - Delay-latency anonymity networks – MIXnets based systems.	Weekly write-up (review, critique, design issues etc.)
7	- Traffic analysis attacks I: theory, implementations, threat, efficacy, defenses.	Weekly write-up (review, critique, design issues etc.)
8	- Traffic analysis attacks II: Large scale adversaries, Sybil based attacks.	Weekly write-up (review, critique, design issues etc.)
9	- Anonymity and performance	Weekly write-up (review, critique, design issues etc.)
10	- Real time anonymous communication.	Weekly write-up (review, critique, design issues etc.)
11	- Network surveillance and censorship, network neutrality	Weekly write-up (review, critique, design issues etc.)
12	- Practical censorship resistance using Tor.	Weekly write-up (review, critique, design issues etc.)
13	- Decoy routing systems	Weekly write-up (review, critique, design issues etc.)

Lectures

Class Presentations

Grading:

25% presentations.

10% class participation

5% attendance

10% mid-term exam

20% Weekly reviews

30% final-term survey paper

List of papers:

TBA

General references:

http://freehaven.net/anonbib/

http://www.cs.yale.edu/homes/jf/Privacy-Pubs.html

http://www.cs.ucsb.edu/~ravenben/classes/595n-s07/papers.html

https://www1.cs.columbia.edu/~smb/classes/s05/ (several papers on anon. communication systems)