

CS7NS5, CSU44032

Security & Privacy

Stephen Farrell

stephen.farrell@cs.tcd.ie

Course Materials:

<https://down.dsg.cs.tcd.ie/cs7053>

<https://github.com/sftcd/cs7053>

Administrivia (1)

- Lectures are (mostly) **face-to-face**:
 - Monday 1600-1750, LB01
 - Wednesday 1700-1750, LB04
- If you're forced to miss a lecture for good reason, mail me and I'll make a (typically, bad;-) recording available
 - If that happens too many times, I'll reconsider - IOW watching a recording is the exception not the common case
 - Reason: "hybrid" lectures resulted in low attendance ("I'll watch that later") which was highly correlated with worse results

Administrivia (2)

- Dates (don't be surprised if I get this wrong;-)
 - Lectures from Today → April 9th
 - Reading week: March 3th
- I may have some travel during term (week of March 17th) so will record a lecture for March 19th (if travelling)
- We have a couple of holiday Monday's (Feb 3rd, March 17th)
- Pronouns: he/him for me
 - If I get yours wrong, apologies and do let me know

Office Hours

- I'll be hanging out in the “office hours” room on BB collab for about half an hour each week (can be more time if needed)
- Feel free to jump in and ask questions/chat about anything related to the module
 - Yeah, it'll be mostly about assignments;-)
- Initial slot: Wednesday 1430
 - If that slot is terrible I can setup a poll for another, do I need to do that?
 - If no slot is much good we live with that and swap after reading week
- You can *always* send me email: stephen.farrell@cs.tcd.ie

Assessment

- 20% for 2 in-term assignments
 - Deadline is end of term: April 11th 2023
- 80% for sit-down, in-person, exam
 - 2 hours, do 3 of 4 questions
- Old exams at:
 - <https://down.dsg.cs.tcd.ie/old-exams/>

In-term Assignments

- Assignment#1, 15%: Security & Privacy Considerations for your FYP/Dissertation
 - 3-4 pages usually; text should be usable in your dissertation/FYP
 - Discuss the security & privacy issues of your dissertation/FYP topic
 - No FYP or dissertation? (e.g. visiting) then talk to me...
 - See RFCs 3552, 6973 and W3C tech report on sec/privacy considerations
<https://tools.ietf.org/html/rfc3552>
<https://tools.ietf.org/html/rfc6973>
<https://www.w3.org/TR/security-privacy-questionnaire/>
- Assignment#2, 5%: Security Incident:
 - 1 page describing a significant incident that happens **during the course** saying why its significant
 - Or, a github PR for the course materials that I accept
- If you make use of LLM tooling, then you **MUST** declare that (details when assignment set in BB)

Blackboard Stuff

- CSU44032 should be a “child module” of CS7NS5
- You’ll submit assignment files via blackboard
- I’ll set those up in the next short while

Course Outline

- Background and introductory concepts in security and privacy
- (Enough) cryptography so you can understand how that's used in...
- Core Internet security and privacy protocols (esp TLS)
- Other stuff that's interesting as time permits

Questions?

I like questions and comments!

Just interrupt however works
when you have a question or
comment.

The more questions you ask, the less material I cover, and the less revision for your exam.

Puzzle

If you know the answer, please stay quiet!

How might you send a physical secret (written on paper)
to someone far away?