CS7NS5, CSU44032
Security & Privacy

Stephen Farrell
stephen.farrell@cs.tcd.ie
Room: spare bedroom:-(

Course Materials:
https://down.dsg.cs.tcd.ie/cs7053
https://github.com/sftcd/cs7053

Recording

- Reminder to self: hit the “record” button
- Lectures will be recorded, recordings available via Blackboard
- If you object to recording, then fire ahead...

Administrivia

- Lectures will be via the modestly named “blackboard collaborate ultra”
  - Monday 1600-1750
  - Wednesday 1700-1750
- Dates (don’t be surprised if I get this wrong;-)
  - Today → April 21st
  - Reading week: March 15th → 19th

“mic line” etiquette

- I get very bored just talking to a screen, so welcome questions/comments any time
- At conferences people line up at the microphone to ask questions - pretending we’re doing that works ok if we have a queue of people with questions
- If I’m rabbiting on (aka “speaking”:-) and you want to comment or ask a question, then just type that in the blackboard chat
- If you want to send audio as well (e.g. if question isn’t yet well-formed) then prepend “+q” to your typed comment, e.g. “+q to ask if that attack happened often”
- I’ll cycle through the people who typed “+q” to get all the questions
- If your question gets answered before you get to the top of the queue, then it’s ok to take yourself out of the queue by typing “-q”
- I really do welcome people sending audio and/or video so don’t be shy!

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;-)
- Default slot: Tuesday 1400 but as that might not suit everyone, please fill in your available slots at the poll:
  - https://dudle.inf.tu-dresden.de/pickanofficehour/
  - If some other slot is way better than Tuesday 1400 we can swap
  - If nothing at all is good we live with that but can swap after reading week

Assessment

- No sit-down exams this year (I guess something has to be good:-)
- 20% for 2 in-term assignments
  - Deadline: end of term
- 80% for exam replacement assignments
  - Do 3 from 5 assignments over 1 or 2 weeks during exam period whenever that turns out to be
  - Structure and content is modelled on old exams so you can benefit from looking at those: 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; use in dissertation/FYP
  - Discuss the security & privacy issues of your dissertation/FYP topic
  - 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

Course Outline

- Background and Introductory concepts
- Cryptography
  - So you can understand how that's used in…
- Core security and privacy protocols (esp TLS)
- Other stuff that's interesting as time permits

Questions?