CS7NS5/CSU44032

Security & privacy

Stephen Farrell

stephen.farrell@cs.tcd.ie
x2354, Room WR3.4

Course materials:

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

https://github.com/sftcd/cs7053

Slideware + some papers

Administrivia

- Lectures:
  - Mon 1600-1800, LB04
  - Wed 1700-1800, LB04
- Dates:
  - Term: Today -> April 10th
  - Reading week: Mar 2nd – Mar 6th
  - Me away: week of Mar 21st
    - Will let you know what's on closer to time

Examination

- 80%/20% exam/assignments marking split
- Old exam questions/solutions:
  - https://down.dsg.cs.tcd.ie/old-exams
- Assignment 1 (15%)
  - “security & privacy considerations”
- Assignment 2 (5%)
  - “security incident” or PR for course repo
- Due date: any time up to the last day I'm marking exam papers, April 1st if you prefer a specific date
- Submit **PDF** via blackboard
- Email me if any issues

Assignment Tasks

- Security & Privacy Considerations:
  - 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/
- Security Incident:
  - 1 page describing a significant incident that happens **during the course** saying why its significant
  - Or, a github PR that's accepted

Course Outline

- Introduction
- Security and privacy concepts
- (Enough) cryptography (AES, RSA, ...)
- (To grok) core security standards (TLS,...)
- Stuff that's interesting for the last few weeks (liable to change)

Puzzle

(If you know the answer already, please STFU/stay quiet!)

How do you send a secret message via courier (when you don't trust the courier)?