# Course Introduction

## and some motivation

Mainack Mondal

CS 60081
Autumn 2020

# Today's class

- Course logistics
- The story of usability
- The case of contact tracing in brief

# Instructors

- **Mainack Mondal:** usable security and privacy, system security and privacy, operationalizing privacy theories
  - Office: CSE 316
  - Also teaching Cryptography and Network Security

# Two TAs


Avirup Mukherjee

avimukh.250696@iitkgp.ac.in

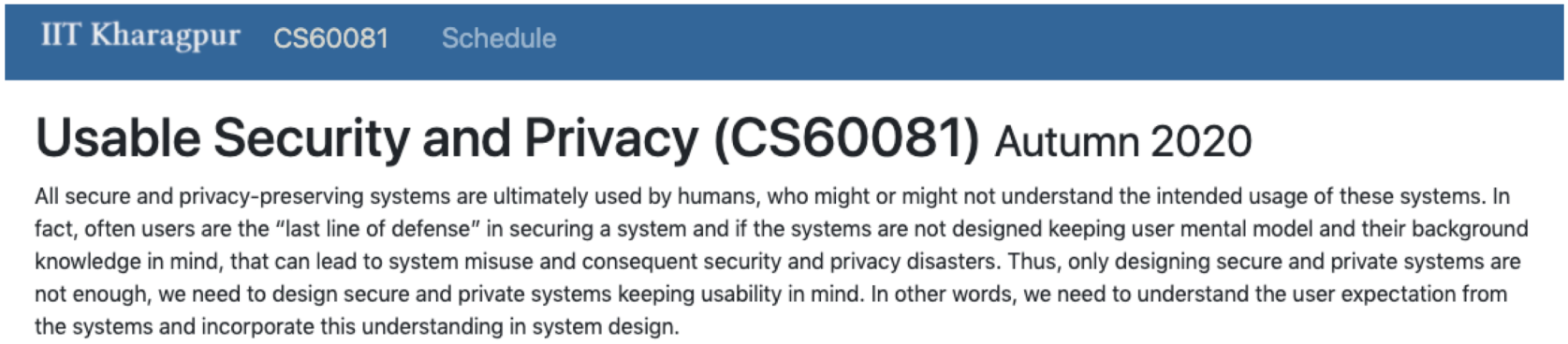


Anju Punuru

anju.punuru@iitkgp.ac.in

# Website

- https://cse.iitkgp.ac.in/~mainack/courses/2020-autumn/usesec/index.html




- Previously co-taught with Dr. Blase Ur, UChicago

# Course timings

- Credit : 3 – 0 – 0

- Monday 3:00 pm - 4:55 pm
- Tuesday 3:00 pm - 3:55 pm
- Wednesday 8:00 pm - 9:30 pm (extra slot, will be used sometimes)

# Mode of teaching

- Live lectures via zoom
  - Zoom link will be announced in MS classroom
- Pre-recoded lectures
  - We will upload the recorded lectures via MS teams
- No Mid/End semesters – continuous evaluation
  - Quiz/viva/term project

# Day-wise breakup

- Monday: Doubt clearing session on last week's pre-recorded lectures
- Tuesdays: time bound quiz from 3:15 pm on CSE Moodle
- Wednesdays late evening: Will often use it as buffer, specifically for project related discussions/activities
- Will upload any change of schedule on MS teams calendar.

# Course evaluation: Quiz

- Weekly quiz (40%)
  - Tuesdays from 3:15 pm
  - 10– 20 minute (will be mentioned) online quiz based on last week's lectures
  - Starting from 15/09/2020
  - On CSE Moodle
    - https://moodlecse.iitkgp.ac.in/moodle/login/index.php
    - Enrollment key: STD31

# Course evaluation: Viva

- Viva (20%)
  - Syllabus : Everything untill that point
  - 1/2  depending on the progress of the course
  - Dates will be announced later and added to the classroom calendar

# Course evaluation: Term project

- 40% of the evaluation
  - Expected: You can apply the knowledge gained from this class on some novel problems
  - Write a small research paper based on it
  - If interesting enough (and you wish) you can work after the course to make it a research paper submission

# Course evaluation: Term project

- Requirements:
  - Submit periodic reports (via Moodle)
  - Give periodic presentations
  - Set time with the instructors to have feedback (“Within that week”)

  Let’s check:

  https://cse.iitkgp.ac.in/~mainack/courses/2020-autumn/usesec/index.html

# Term project: reports

- Write in LaTex with ACM two column format
- Suggested: use overleaf for collaboration

# Term project: exceptions

- Have an idea on usable security/privacy you think you should work on?
- Already have group members?
- Talk to us ASAP (drop a private chat/email)

# Course logistics

- Questions?

# Ethical considerations

Source: https://myozonelayer.com/2016/11/22/the-4th-monkey-do-no-evil/

# Ethical considerations

- Don’t do evil
- If you feel its wrong, it is wrong
- Cyber offenses are punishable by law
  - The case of Mirai Botnet  -- five years of probation, 2,500 hours of community service, and $127,000 fine.
  - The case of Swatting – people got killed

# Today's class

- Course logistics
- The story of usability
- The case of contact tracing in breif


HERCULES

# Lack of usable security costs billions

- 2019: UK's Information Commissioner's Office (ICO)

"90% of cyber data breaches were caused by user error last year"

# Without usability no effective security

- 2009: Department of Homeland Security (DHS)

  published a list of "hard problems in INFOSEC Research", 11th problem was "Usable security"

  "Security must be usable by persons ranging from nontechnical users to experts and system administrators. Furthermore, systems must be usable while maintaining security. In the absence of usable security, there is ultimately no effective security."

# Understanding how would users behave

- 2008: National Academy of Engineering, US

  Published “Grand Challenges of Engineering”

  ”one of the needs to “secure cyberspace” was to understand how the psychology of computer users can "increase the risk of cybersecurity breaches"

# Humans are important in security

"Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations... But they are sufficiently pervasive that we must design our protocols around their limitations."

-- C. Kaufman, R. Perlman, and M. Speciner Network Security: PRIVATE Communication in a PUBLIC World. 2nd edition. Prentice Hall, page 237, 2002.

# The human threat

- Malicious humans
- Clueless humans
- Unmotivated humans
- Humans constrained by human limitations

# Humans are the weakest link

In practice

"Given a choice between dancing pigs and security, users will pick dancing pigs every time"

-- Edward Felten

# Experiment on the weakest link

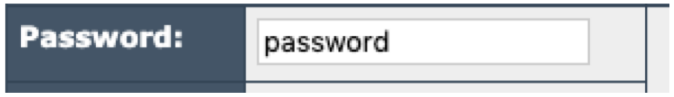
- The U.S. Department of Homeland Security ran a test in 2011 to see how hard it was for hackers to corrupt workers and gain access to computer systems:
- staff secretly dropped computer discs and USB thumb drives in the parking lots of government buildings and private contractors.
- Of those who picked them up: 60 percent plugged the devices into office computers
- If the drive or CD case had an official logo, 90 percent were installed.

# Security and usability

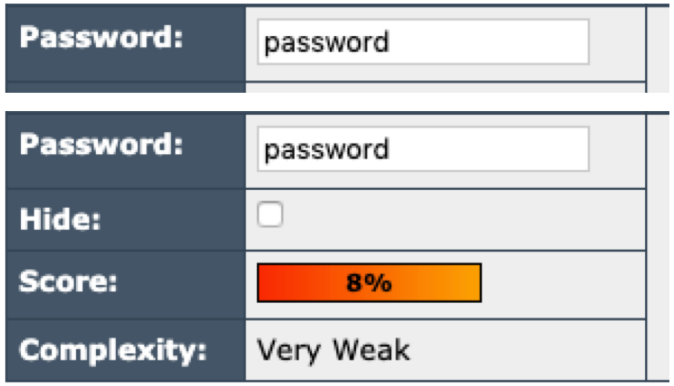
- If a system is secure but not usable
  - User will move to usable (even insecure) systems
- If a system is usable but insecure
  - It will get compromised – can not last long

- When trying to make secure systems usable, we add complexity. Complexity leads to higher chances to doing something wrong, i.e. less secure!

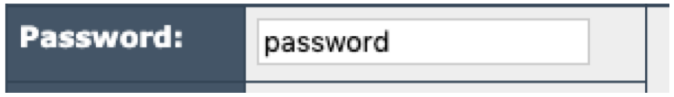
# Systems are not good enough

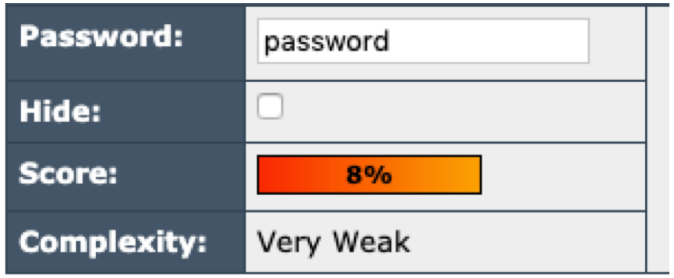


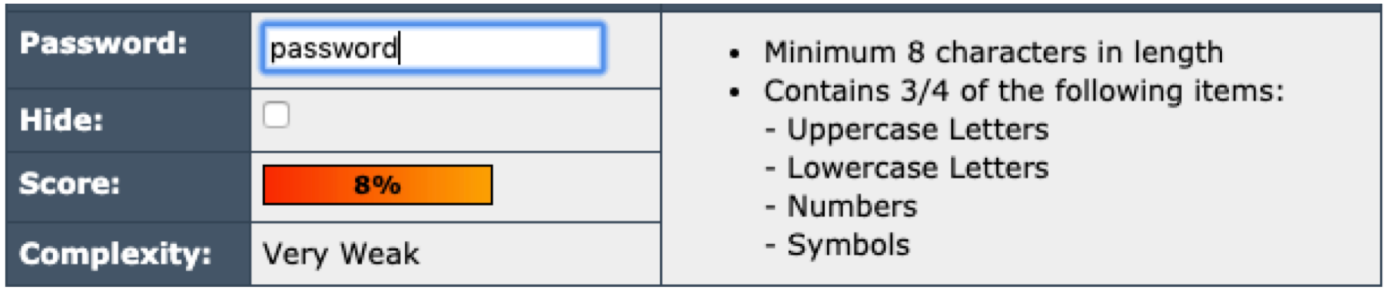
# Systems are not good enough



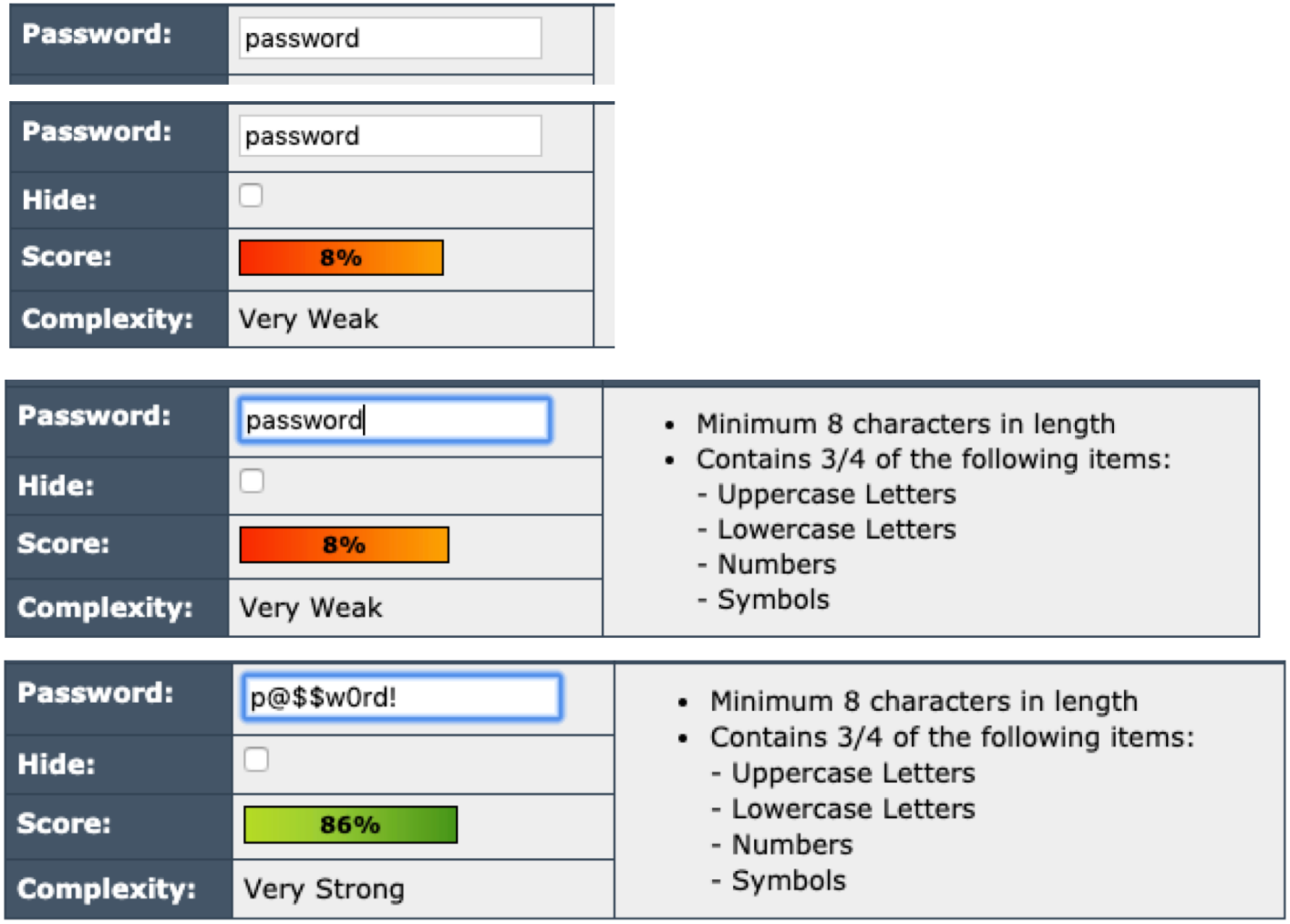
# Systems are not good enough



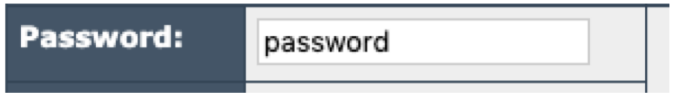



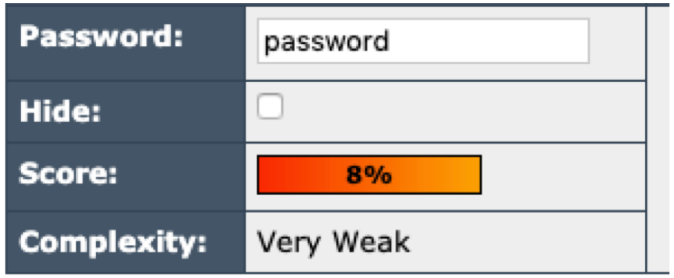



# Systems are not good enough

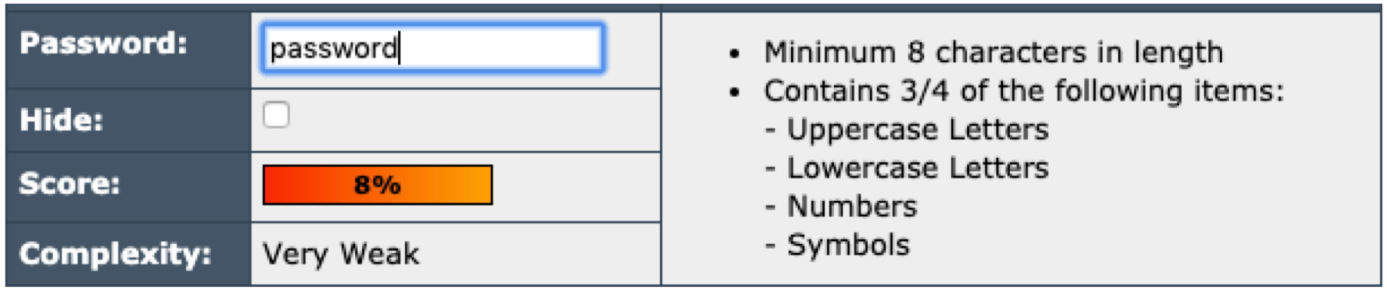


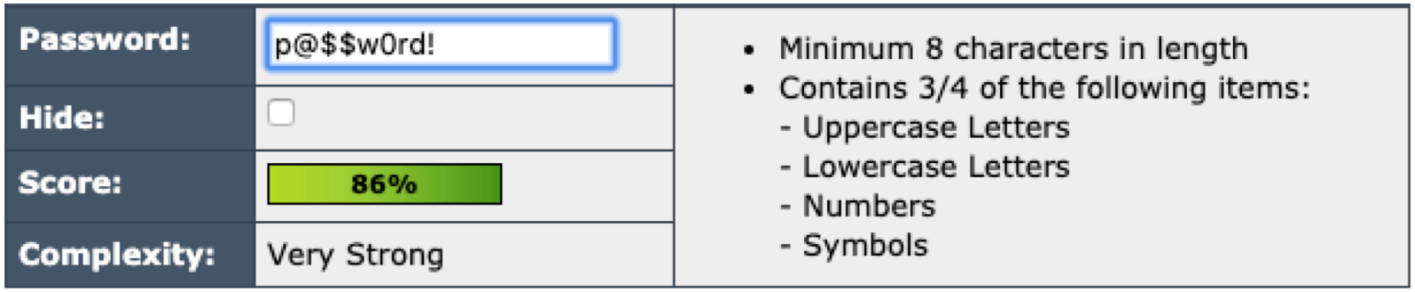
# Systems are not good enough




http://www.passwordmeter.com/



# Security & Privacy

(CCS, Usenix Securiy, IEEE S&P, NDSS)

+

# Human-Computer Interaction

(CHI, UbiComp, CSCW)

=

# Usable Security and Privacy

(PETS, SOUPS)

# Contact tracing

- Contact tracing is the process of identifying, assessing, and managing people who have been exposed to a disease to prevent onward transmission.

- Contact tracing for COVID-19 requires identifying people who may have been exposed to COVID-19 and following them up daily for 14 days from the last point of exposure.

# Contact tracing apps

# Contact tracing : opinion

- Privacy worries? 1
- Necessary? 3
- None? 1
- Both? 9