Course Introduction

and some motivation

Mainack Mondal

CS 60081
Autumn 2022

Today's class

- Course logistics
- The story of usability
- Some case studies: *why* of usability in security / privacy

Instructors

- **Mainack Mondal:** usable security and privacy, system security and privacy, operationalizing privacy theories
  - Office: CSE 316

Two TAs

Rishabh Maurya

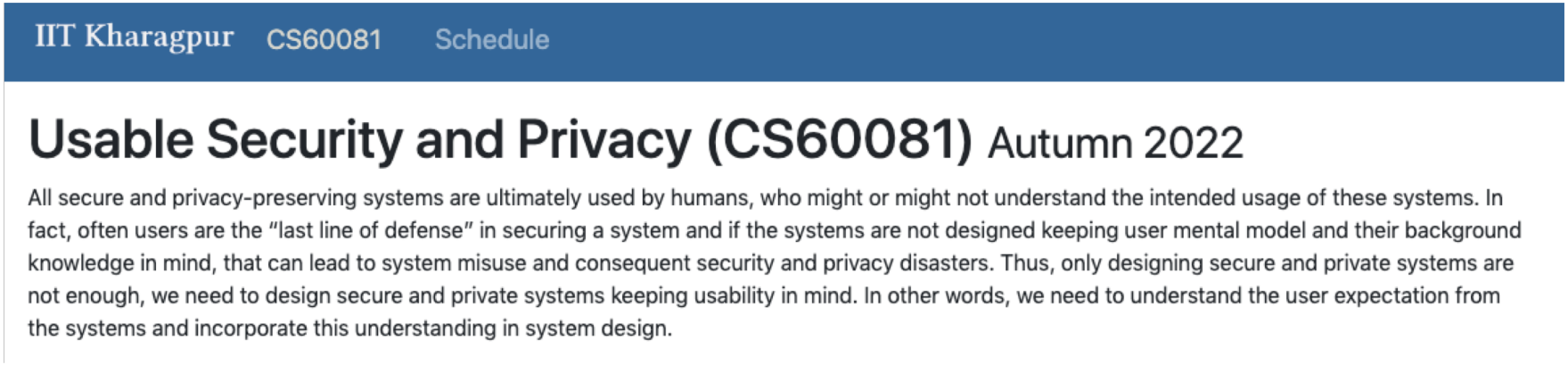
imrishabhm@gmail.com

Debranjan Pal

debranjan.crl@gmail.com

Website

- https://cse.iitkgp.ac.in/~mainack/courses/2022-autumn/usesec/



Course timings

- Credit : 3 – 0 – 0

- Monday 3:00 pm - 4:55 pm
- Tuesday 3:00 pm - 3:55 pm

Mode of teaching

- Offline lectures
  - Please come to the class (no recordings)
- (occasional) Pre-recoded lectures for special topics
  - We will upload the recorded lectures via MS teams
- Two exams + term project + 1 assignment
  - Quiz/viva/term project

Day-wise breakup

- Monday: If needed doubt clearing session on last week's lectures + lecture
- Tuesdays: Regular lecture
- Will upload any change of schedule on webpage and announce on MS teams.

CSE Moodle

- All submissions will be via CSE moodle unless otherwise stated
  - CSE Moodle
    - https://moodlecse.iitkgp.ac.in/moodle/login/index.php
    - Course name: Usable Security and Privacy course (CS60081)
    - Link: https://moodlecse.iitkgp.ac.in/moodle/course/view.php?id=492
    - Enrollment key: USPSTUA22

Course evaluation: Exam

- Two Exams (60%)
  - Syllabus : Everything until that point
  - Dates will be in the webpage and announced in academic calendar

Course evaluation: Term project + Assignment

- 40% of the evaluation
  - Expected: You apply the knowledge gained from this class on a hands on practical problem
  - Write two reports/one presentation based on it
  - If interesting enough (and you wish) you can work after the course to make it a research paper submission
  - Talk to me
  - One assignment to practice knowledge of things you cannot do in term project – e.g., statistics

Course evaluation: Term project

- Requirements:
  - Submit periodic reports (via Moodle)
  - Give periodic presentations

  Let's check:

  https://cse.iitkgp.ac.in/~mainack/courses/2021-autumn/usesec/index.html

Term project: reports

- Write in LaTex/Word with ACM two column format
- Suggested: use overleaf/ Share point 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

- Some case studies: *why* of usability in security / privacy


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

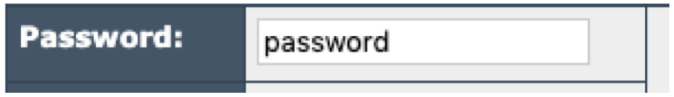
- The U.S. Department of Homeland Security ran a test in 2011 to see how hard it was for hackers to corrupt workers and gain access to computer systems:
- staff secretly dropped computer discs and USB thumb drives in the parking lots of government buildings and private contractors.
- Of those who picked 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

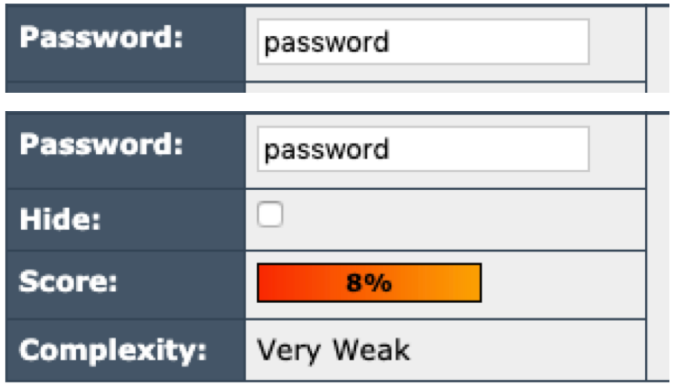
- If a system is secure but not usable
  - User will move to usable (even insecure) systems
- If a system is usable but insecure
  - It will get compromised – can not last long

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

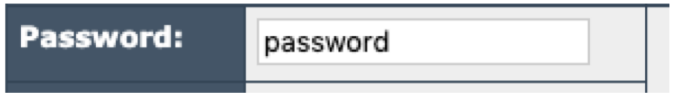
Systems are not good enough

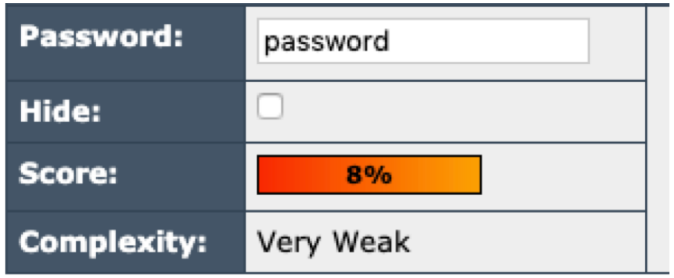


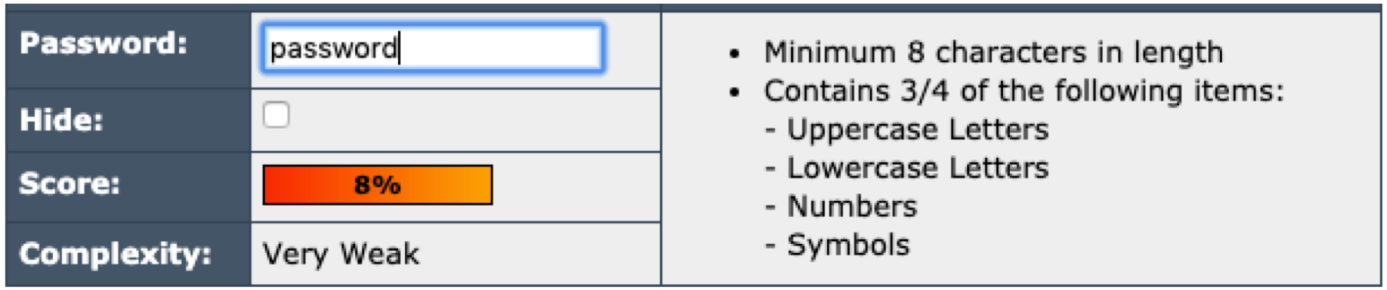
Systems are not good enough



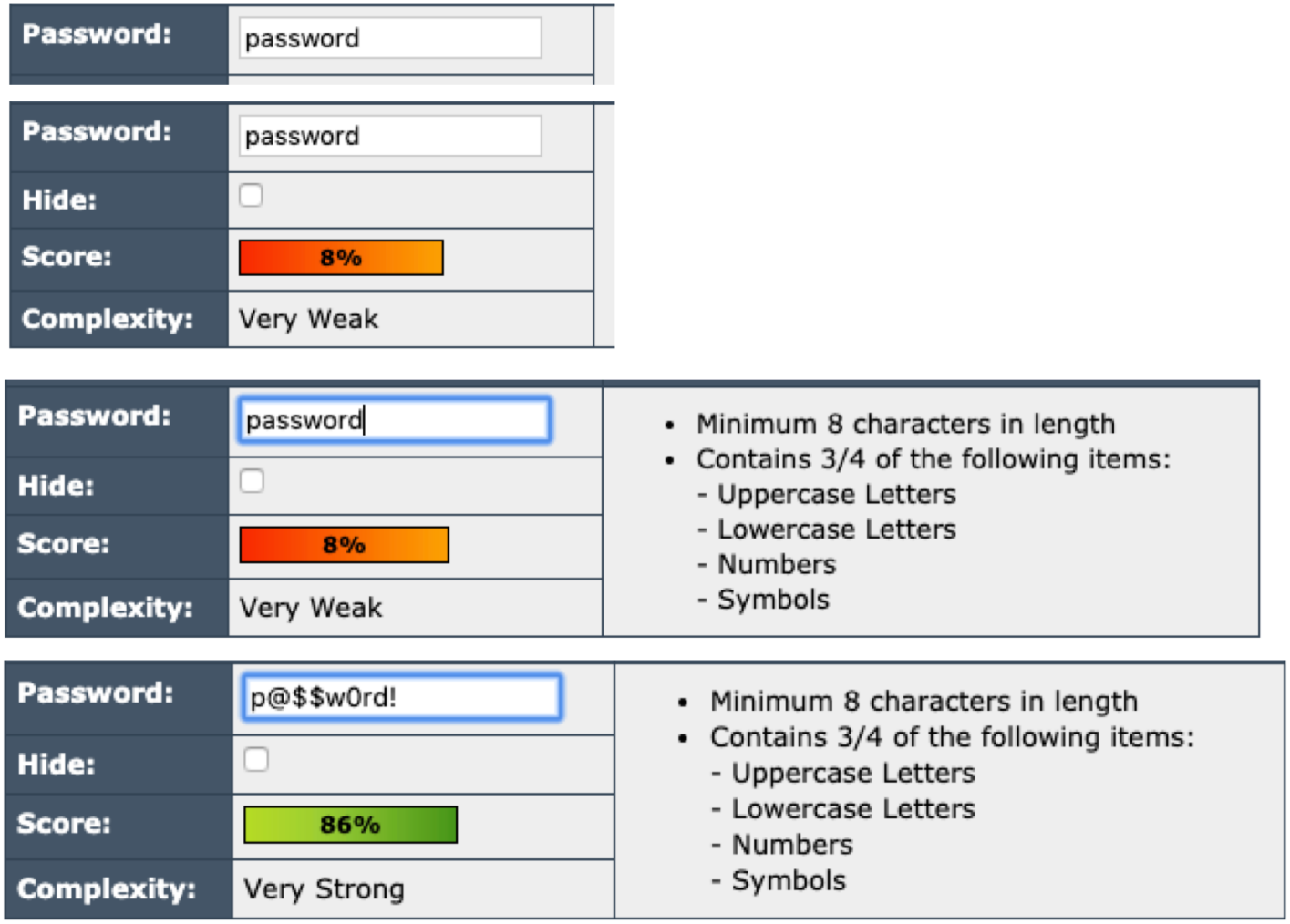
Systems are not good enough



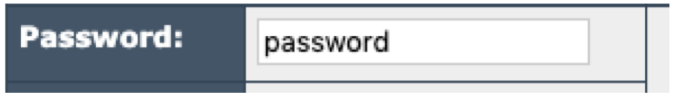


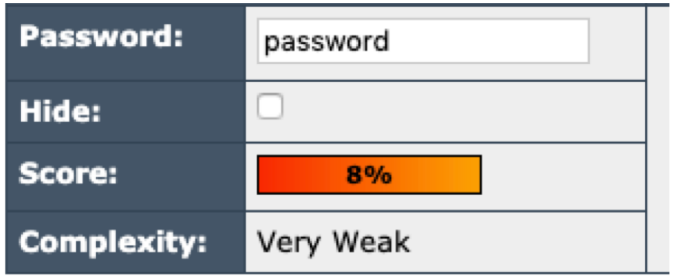


Systems are not good enough

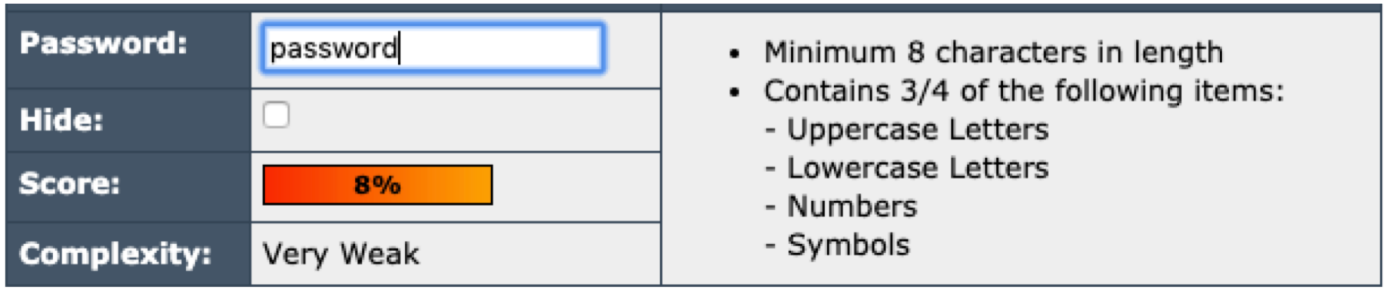


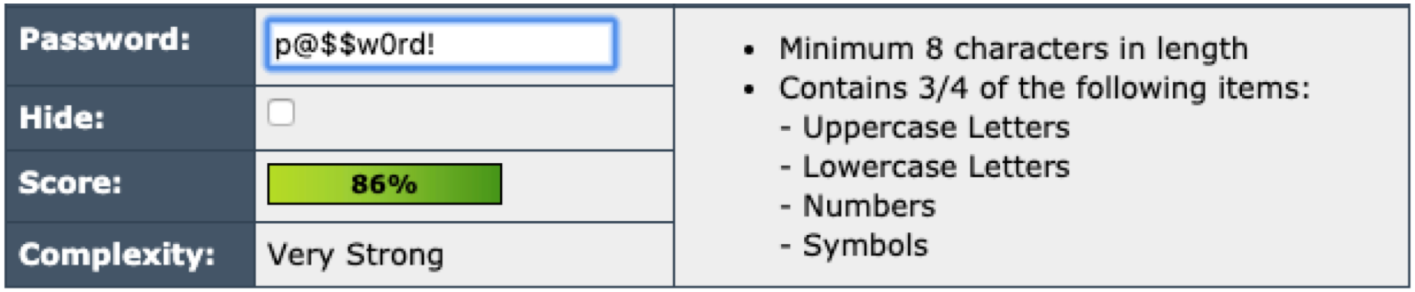
Systems are not good enough





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)

Today's class

- Course logistics
- The story of usability
- Some case studies: *why* of usability in security / privacy

Case study 1: Two-factor authentication

- What is 2-factor authentication?

Case study 1: Two-factor authentication

- What is 2-factor authentication?
  - Factor 1: What you know (e.g., your password)
  - Factor 2: What you have (e.g., OTP on your phone)

Case study 1: Two-factor authentication

- What is 2-factor authentication?
  - Factor 1: What you know (e.g., your password)
  - Factor 2: What you have (e.g., OTP on your phone)

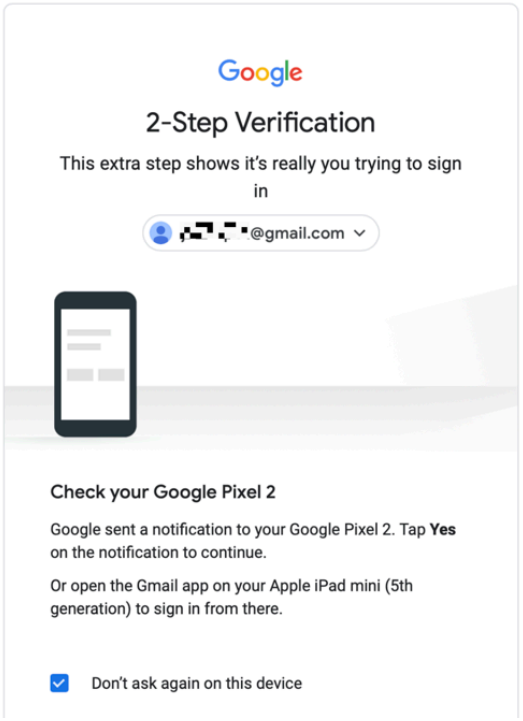


Image: https://zapier.com/blog/google-two-step-verification/

Case study 1: Two-factor authentication

- Problems?
  - User's time it takes increase and attention
  - Losing device – breaking phone

Case study 1: Two-factor authentication

- The story of a Philadelphia librarian
  - Old, often homeless people use public libraries for internet
  - The computers wipe all session information once logged out
  - Every time Gmail ask for two-factor
  - That's good, right? More secure?

Case study 1: Two-factor authentication

- The story of a Philadelphia librarian
  - Old, often homeless people use public libraries for internet
  - The computers wipe all session information once logged out
  - Every time Gmail ask for two-factor
  - That's good, right? More secure?
  - NO

Case study 1: Two-factor authentication

- The story of a Philadelphia librarian

it is very common for poor working-class people to have their cellular service shut-off due to a missed payment on their phone bill. Often, they have had to sell their phone to make rent, or their phone has been stolen or broken and they cannot afford a new one and when they do finally get a new one they are unable to get their old phone number transferred over.

Case study 1: Two-factor authentication

- The story of a Philadelphia librarian

it is very common for poor working-class people to have their cellular service shut-off due to a missed payment on their phone bill. Often, they have had to sell their phone to make rent, or their phone has been stolen or broken and they cannot afford a new one and when they do finally get a new one they are unable to get their old phone number transferred over.

- So?

Case study 1: Two-factor authentication

- The story of a Philadelphia librarian

it is very common for poor working-class people to have their cellular service shut-off due to a missed payment on their phone bill. Often, they have had to sell their phone to make rent, or their phone has been stolen or broken and they cannot afford a new one and when they do finally get a new one they are unable to get their old phone number transferred over.

When this happens, patrons are locked out of their accounts, sometimes permanently, with **no support line to turn to…**an old woman came in to print out paystubs from her email that she needed in order to re-certify her income for her subsidized housing. The certification was due by the end of the day. Because she did not have her old phone and phone number, we were completely unable to get her back into her email.

If she does not recertify her income, she could lose her low-income housing. This elderly woman, looked to be in her 70s, might lose the roof over her head, due to being unable to log into her Google account, because she lost her old phone and with it, her phone number.

Case study 1: Two-factor authentication

- Full story (and her open letter) here: https://docs.google.com/document/d/1f6HPQbUjsIcbjVHkJkAgYmQmBV3PRRHEcx4WL5rxuE8/preview

- Strict two factor is for people who can afford a phone and afford to keep a sustained connection
  - Hurts the poor who perhaps need access most

Case study 2: Encrypting emails

- What is encryption?

Case study 2: Encrypting emails

- What is encryption?
  - The art of hiding information so that only intended recipient can read

Image: https://www.okta.com/identity-101/password-encryption/

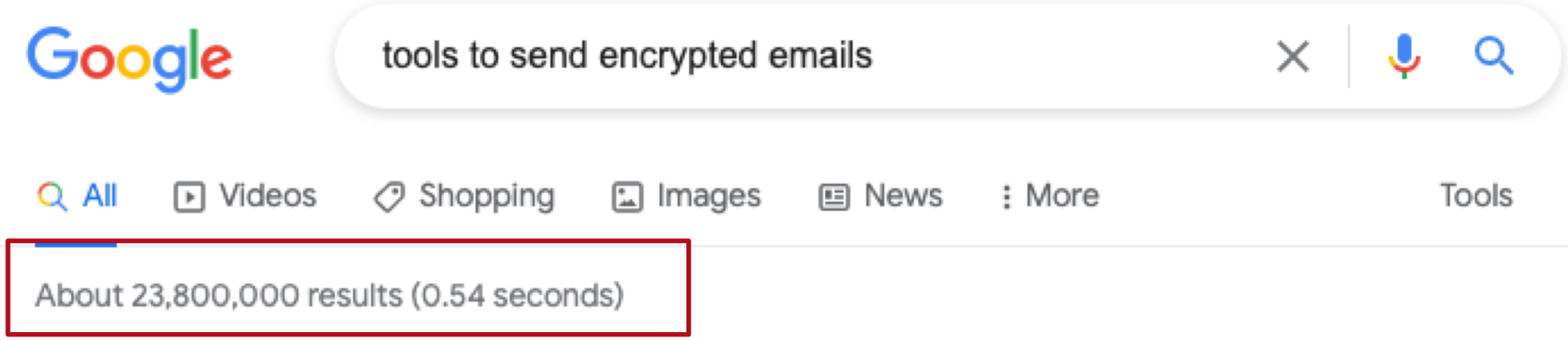
Case study 2: Encrypting emails

- How many of you use it to send emails?

Image: https://www.okta.com/identity-101/password-encryption/

Case study 2: Encrypting emails

- How many of you use it to send emails?



- Why so low?

Image: https://www.okta.com/identity-101/password-encryption/

Case study 2: Encrypting emails

- Current way you use encryption

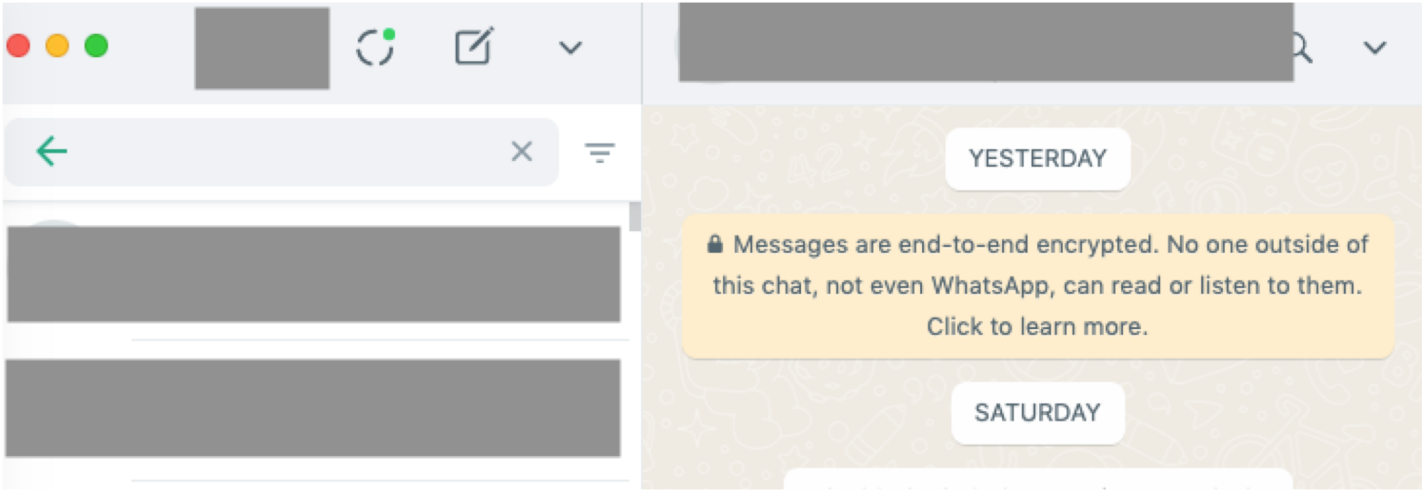


Image: https://www.okta.com/identity-101/password-encryption/

Case study 2: Encrypting emails

- Current way you use encryption

- In this case to ensure usability, the software proactively generate key and encrypt/decrypt

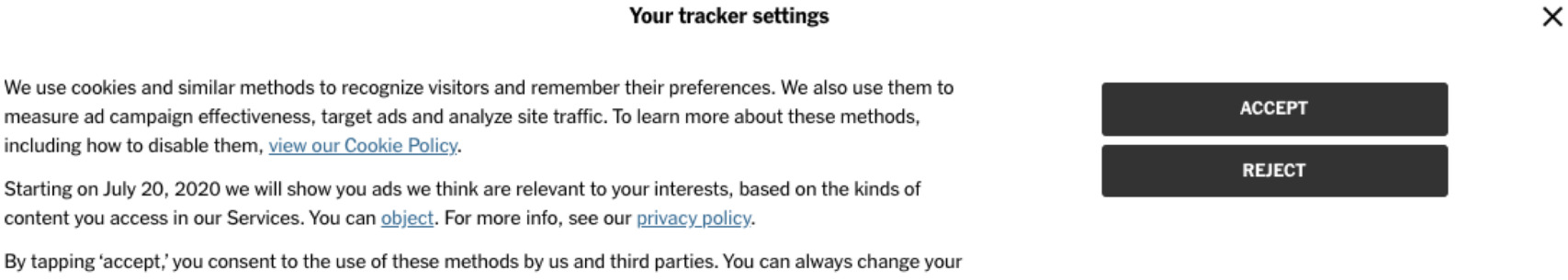
Image: https://www.okta.com/identity-101/password-encryption/

Case study 3: Cookie banners

- What are cookie banners?

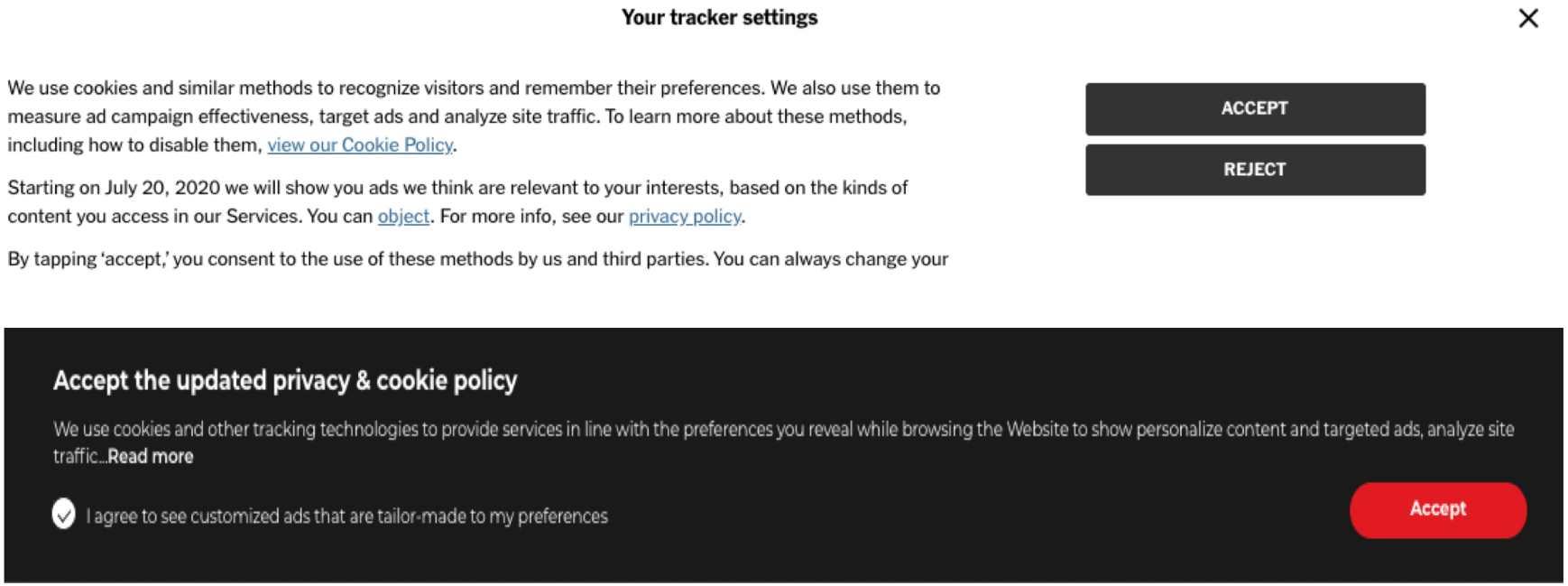
Case study 3: Cookie banners

- What are cookie banners?



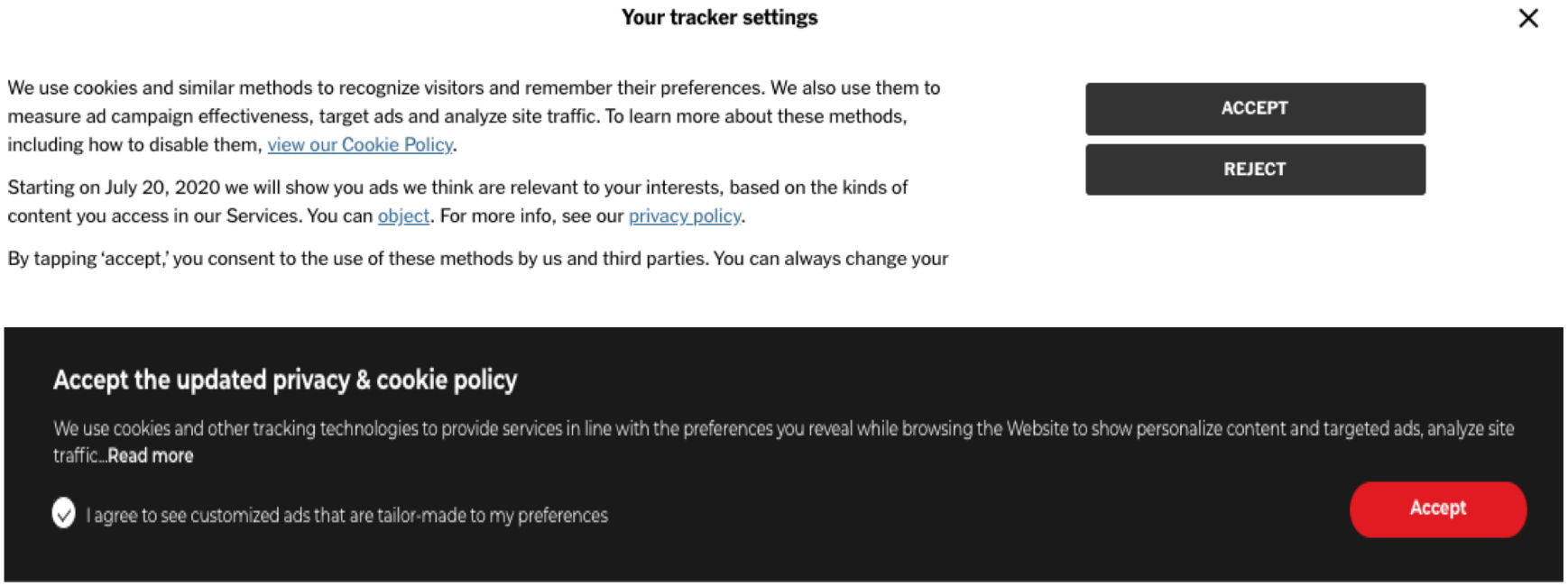
Case study 3: Cookie banners

- What are cookie banners?



Case study 3: Cookie banners

- What are cookie banners?



- Just having a cookie banner is not enough for privacy

Case study 4: Privacy in India

Privacy in India: needed?

- When you hear need for privacy what cases do you think of as someone living in India? Speak up.
  - No important data, no need
  - Even if the data is important, no idea of the attacker
  - Need privacy for facebook / insta/ social media sharing
  - Need privacy for E-commerce activities, payment options
  - Need privacy for Bitcoin wallets
  - Need privacy for Data breach in companies like air india by say phishing

Privacy law in India needed? opinion

- Need
  - Aadhar and sharing data from aadhar
  - UPI information, razorpay
  - Cookies, ad sense
  - Phone number

- Not need
  - Difficult to implement
  - Lot of research before a mandate

Privacy in India: needed?

- It is not clear what is the privacy expectation in India
  - A designer needs to uncover the expectation before they can go ahead with building systems
  - How?

Moving forward

- We will now objectively learn what security, privacy and usability means
- Then we will move on to checking areas where people mixed usability with sec/priv to build systems for users