

# Course Introduction

## and some motivation

Mainack Mondal

CS 60081  
Autumn 2021



# Today's class

- Course logistics
- The story of usability
- The case of privacy in India

# Instructors



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

# Two TAs



Shivam Kumar Jha

[code@thealphadollar.me](mailto:code@thealphadollar.me)



Naimesh Pramanik

[naimeshriju111@gmail.com](mailto:naimeshriju111@gmail.com)

# Website

- <https://cse.iitkgp.ac.in/~mainack/courses/2021-autumn/usesec/>

IIT Kharagpur CS60081 Schedule

## Usable Security and Privacy (CS60081) Autumn 2021

All secure and privacy-preserving systems are ultimately used by humans, who might or might not understand the intended usage of these systems. In fact, often users are the “last line of defense” in securing a system and if the systems are not designed keeping user mental model and their background knowledge in mind, that can lead to system misuse and consequent security and privacy disasters. Thus, only designing secure and private systems are not enough, we need to design secure and private systems keeping usability in mind. In other words, we need to understand the user expectation from the systems and incorporate this understanding in system design.

- 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

# Mode of teaching

- Live lectures via zoom
  - Zoom link will be announced in MS classroom
- Pre-recorded lectures
  - We will upload the recorded lectures via MS teams
- Three tests + term project + 1 assignment
  - Quiz/viva/term project

# Day-wise breakup

- **Monday:** Doubt clearing session on last week's pre-recorded 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 (Autumn 2021-22)
    - Link:  
<https://moodlecse.iitkgp.ac.in/moodle/course/view.php?id=418>
    - Enrollment key: STU60081

# Course evaluation: Test / viva

- Three tests / Viva (60%)
  - Syllabus : Everything until that point
  - Dates are in the webpage

# 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/2020-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
- The case of contact tracing in brief



# 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

**Password:**

# Systems are not good enough

<b>Password:</b>	<input type="text" value="password"/>
<b>Password:</b>	<input type="text" value="password"/>
<b>Hide:</b>	<input type="checkbox"/>
<b>Score:</b>	<div style="background-color: #ff4500; color: white; padding: 2px; display: inline-block;">8%</div>
<b>Complexity:</b>	Very Weak

# Systems are not good enough

<b>Password:</b>	<input type="text" value="password"/>
------------------	---------------------------------------

<b>Password:</b>	<input type="text" value="password"/>
<b>Hide:</b>	<input type="checkbox"/>
<b>Score:</b>	<div style="background-color: #ff4500; color: white; padding: 2px; display: inline-block;">8%</div>
<b>Complexity:</b>	Very Weak

<b>Password:</b>	<input type="text" value="password"/>	<ul style="list-style-type: none"><li>• Minimum 8 characters in length</li><li>• Contains 3/4 of the following items:<ul style="list-style-type: none"><li>- Uppercase Letters</li><li>- Lowercase Letters</li><li>- Numbers</li><li>- Symbols</li></ul></li></ul>
<b>Hide:</b>	<input type="checkbox"/>	
<b>Score:</b>	<div style="background-color: #ff4500; color: white; padding: 2px; display: inline-block;">8%</div>	
<b>Complexity:</b>	Very Weak	

# Systems are not good enough

<b>Password:</b>	<input type="text" value="password"/>
------------------	---------------------------------------

<b>Password:</b>	<input type="text" value="password"/>
<b>Hide:</b>	<input type="checkbox"/>
<b>Score:</b>	<div style="width: 8%; background-color: orange; text-align: center;">8%</div>
<b>Complexity:</b>	Very Weak

<b>Password:</b>	<input type="text" value="password"/>	<ul style="list-style-type: none"><li>• Minimum 8 characters in length</li><li>• Contains 3/4 of the following items:<ul style="list-style-type: none"><li>- Uppercase Letters</li><li>- Lowercase Letters</li><li>- Numbers</li><li>- Symbols</li></ul></li></ul>
<b>Hide:</b>	<input type="checkbox"/>	
<b>Score:</b>	<div style="width: 8%; background-color: orange; text-align: center;">8%</div>	
<b>Complexity:</b>	Very Weak	

<b>Password:</b>	<input type="text" value="p@\$w0rd!"/>	<ul style="list-style-type: none"><li>• Minimum 8 characters in length</li><li>• Contains 3/4 of the following items:<ul style="list-style-type: none"><li>- Uppercase Letters</li><li>- Lowercase Letters</li><li>- Numbers</li><li>- Symbols</li></ul></li></ul>
<b>Hide:</b>	<input type="checkbox"/>	
<b>Score:</b>	<div style="width: 86%; background-color: green; text-align: center;">86%</div>	
<b>Complexity:</b>	Very Strong	

# Systems are not good enough

<b>Password:</b>	<input type="text" value="password"/>
------------------	---------------------------------------

<b>Password:</b>	<input type="text" value="password"/>
<b>Hide:</b>	<input type="checkbox"/>
<b>Score:</b>	<div style="width: 8%; background-color: orange; text-align: center;">8%</div>
<b>Complexity:</b>	Very Weak

<http://www.passwordmeter.com/>

<b>Password:</b>	<input type="text" value="password"/>	<ul style="list-style-type: none"><li>• Minimum 8 characters in length</li><li>• Contains 3/4 of the following items:<ul style="list-style-type: none"><li>- Uppercase Letters</li><li>- Lowercase Letters</li><li>- Numbers</li><li>- Symbols</li></ul></li></ul>
<b>Hide:</b>	<input type="checkbox"/>	
<b>Score:</b>	<div style="width: 8%; background-color: orange; text-align: center;">8%</div>	
<b>Complexity:</b>	Very Weak	

<b>Password:</b>	<input type="text" value="p@\$w0rd!"/>	<ul style="list-style-type: none"><li>• Minimum 8 characters in length</li><li>• Contains 3/4 of the following items:<ul style="list-style-type: none"><li>- Uppercase Letters</li><li>- Lowercase Letters</li><li>- Numbers</li><li>- Symbols</li></ul></li></ul>
<b>Hide:</b>	<input type="checkbox"/>	
<b>Score:</b>	<div style="width: 86%; background-color: green; text-align: center;">86%</div>	
<b>Complexity:</b>	Very Strong	



# Security & Privacy

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

+

# Human-Computer Interaction

(CHI, UbiComp, CSCW)

=

# Usable Security and Privacy

(PETS, SOUPS)

# 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: opinion

- Needed to protect from government and companies? 5
- Needed to protect from only companies? 1
- Needed to protect from only government? 0
- Not needed? 0