

CCY4502 Usable Security (HCI)**COURSE INFORMATION**

Prerequisites	Academic Year & Level		Teaching Methods			Credit Hrs.
	Year	Semester	Lecture	Tutorial	Laboratory	
CCY2001	4	7/8	2	2	--	3

COURSE AIM

To get the students to:

- Design for security and privacy from a user-centered perspective
- Explore different Human-computer interaction techniques.
- Learn how to design and build secure systems with a human-centric focus.
- Learn about basic principles of human-compute and apply these insights to the design of secure systems

COURSE WEEKLY CONTENTS

- 1 Course Aim and Course outline, Fundamentals of Human-Computer Interaction: users, usability, tasks
- 2 Cognitive models
- 3 Design for usability
- 4 Prototyping, cybersecurity case study
- 5 Usability studies and testing
- 6 Quantitative and qualitative evaluation, cybersecurity case study
- 7 7th week Assessment
- 8 Strategies for Secure Interaction Design
- 9 Authority and guidelines for interface design
- 10 Usable Authentication: authentication mechanisms
- 11 Biometrics, two-factor authentication
- 12 12th week Assessment
- 13 Usable Privacy: privacy settings, and a user-centric privacy space framework
- 14 Personal data sharing
- 15 Data inference

STUDENT GRADING & ASSESSMENT

Weeks	Exams	Assign.	Quizzes	Reports	Present.	Lab.	Total
1 to 7	←		30	MARKS		→	30
8 to 12	←		20	MARKS		→	20
1 to 15	←		10	MARKS		→	10
16 or 17			Final Exam				40

REFERENCES

Textbook	Lorrie Faith Cranor; Simson Garfinkel, Security and Usability: Designing Secure Systems that People can Use, O'reilly Media
	Simson Garfinkel and Heather Richter Lipford. Usable security: History, Themes, and Challenges, Springer