Title of the course: Usable Security and Privacy

1. Credit requirement: (L-T-P: 3-0-0, Credit: 3)
2. Please select the committee for Approval: PGPEC
3. Name of the Dept: CSE
4. Please Specify the Level of the Subject: PG level
5. Whether the subject will be offered as compulsory or elective: Elective

   Prerequisite(s) for the subject, if any (Please give the subject numbers and names): **N/A**

6. **Course Objective**

   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 developing secure primitives are not enough, we need to build 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.

   This course will focus on how to design for security and privacy in systems using a user-centric view by combining concepts from computer systems, human computer interaction (HCI) and secure/private system design. We will introduce core security and privacy technologies, as well as HCI techniques for conducting robust user studies. The course will cover topics like privacy definitions, usable encryption, authentication, retrospective privacy, usability of crypto libraries, web security, anonymity and privacy notice.

7. **Study Materials**

   In this course, we shall use textbooks for building up the fundamental concepts. However, majority of the topics will be covered through lectures on important concepts available in the recently published articles, and presentation of the related papers.

   Books:
   1. Research Methods in Human-Computer Interaction, 2nd edition. (https://www.elsevier.com/books/research-methods-in-human-computer-interaction/lazar/978-0-12-805390-4) Jonathan Lazar, Jinjuan Heidi Feng, Harry Hochheiser, 2017.

8. Syllabus:
(with Lecture wise break-ups)

- Theory **[37L]**
  - Introduction to Security **[2L]**
    - Security definitions and primitives
    - Modelling attackers
    - Modelling systems
    - Different domains of security research
  - Introduction to Privacy **[2L]**
    - privacy definitions
    - contextual integrity
    - challenges in operationalizing privacy
    - k-anonymity, differential privacy
  - Introduction to Usability **[2L]**
    - Reasoning about the Human in the Loop
    - Attacks on the human-in-the-loop systems
  - Usable Encryption **[1L]**
  - Techniques to measure usability of secure/private systems [**2L]**
    - Surveys, interviews, focus Groups, and diary Studies; mental models; user education;
    - Case study: Preserving privacy on Social Media from other users
  - Designing robust and ethical experiments **[2L]**
    - Field studies
    - Case study: Protecting against social Engineering and Phishing attacks
  - Analyzing Qualitative Data **[2L]**
    - Coding techniques; intercoder reliability
  - Analyzing Quantitative Data with Statistics **[2L]**
    - Hypothesis testing and regression
  - Usability using large-scale internet measurement **[2L]**
    - Designing online data-driven measurement studies
    - Case study: Usability of Social Access Control Lists
  - Authentication **[2L]**
    - Passwords: Password crackers and password managers
    - Beyond passwords: Biometric
  - Ensuring Security and Privacy of Smartphone Data **[2L]**
  - Ensuring Retrospective and Longitudinal Privacy of Digital Archives **[2L]**
  - Usability for Developers: Crypto Libraries and Certificates **[2L]**
  - Web Security and Privacy: SSL/TLS/PKI **[3L]**
    - XSS attacks, SQL injection
    - Online Tracking
    - Data Breach
  - Security Warnings **[2L]**
    - Privacy Notice and Choice
  - Privacy and Anonymity Tools **[2L]**
    - Large scale internet surveillance
    - Protecting user privacy and anonymity: Tor, OpenVpn, SoftEther

- Privacy in The Internet of Things **[2L]**
  - bystander privacy; privacy in public places
- Attacks on deep learning systems to compromise security and privacy **[2L]**
- Inclusive Security and Privacy **[1L]**

9. Names of the faculty members of the Department/Centers/School who have the necessary expertise and will be the willing to teach the subject (Minimum two faculty members should be willing to teach the subject)

   Mainack Mondal, Bivas Mitra, Sandip Chakraborty, Niloy Ganguly

10. Do the contents of the subject have an overlap with any other subject offered in the Institute?

    CS60065: Cryptography and Network Security
    MA60031: Cryptography and Security Issues

    a) Approximate percentage of overlap:
       a. CS60065: There is 5% overlap with the proposed course.
       b. MA60031: There is 5% overlap with the proposed course.

    b) Reasons for offering the new subject in spite of the overlap

CS60065 Cryptography and Network Security

Syllabus: Introduction: Basic objectives of cryptography, secret-key and public-key cryptography, one-way and trapdoor one-way functions, cryptanalysis, attack models, classical cryptography. Block ciphers: Modes of operation, DES and its variants, RCS, IDEA, SAFER, FEAL, BlowFish, AES, linear and differential cryptanalysis. Stream ciphers: Stream ciphers based on linear feedback shift registers, SEAL, unconditional security. Message digest: Properties of hash functions, MD2, MD5 and SHA-1, keyed hash functions, attacks on hash functions. Public-key parameters: Modular arithmetic, gcd, primality testing, Chinese remainder theorem, modular square roots, finite fields. Intractable problems: Integer factorization problem, RSA problem, modular square root problem, discrete logarithm problem, Diffie-Hellman problem, known algorithms for solving the intractable problems. Public-key encryption: RSA, Rabin and EIGamal schemes, side channel attacks. Key exchange: Diffie-Hellman and MQV algorithms. Digital signatures: RSA, DAS and NR signature schemes, blind and undeniable signatures. Entity authentication: Passwords, challenge-response algorithms, zero-knowledge protocols. Standards: IEEE, RSA and ISO standards. Network issues: Certification, public-key infrastructure (PKI), secured socket layer (SSL), Kerberos. Advanced topics: Elliptic and hyper-elliptic curve cryptography, number field sieve, lattices and their applications in cryptography, hidden monomial cryptosystems, cryptographically secure random number generators.

MA60031 Cryptography and Security Issues

Syllabus: Prerequisites: Linear algebra, Modern Algebra, Number Theory, Data Structures and Algorithms. Some Topics in Elementary Number Theory: divisibility, Euclidean and other algorithms relevant to cryptography, Algebraic aspects: Finite Fields, Quadratic Residues and reciprocity. Some simple Cryptosystems: Concepts and techniques of cryptography and its applications. Cryptographic primitives, including one-way hash functions, Public Key Cryptography: RSA, attacks on RSA, ElGamal (signature, encryption), DES, SHA. Diffie-Hellman key exchange, Rabin's oblivious transfer, Shamir's 3-pass protocol, Feige-Fiat Shamir identification, Fiat-Shamir signature, Chaum digital signature, Yao's millionaire problem, computing with encrypted data, secret sharing (Shamir, Blakley), Discrete log knapsack: zero-knowledge proof of discrete log, of private RSA key. Tamper proofing audits trails. Watermarking and digital rights. Primality and various methods of Factorization, Authentication, digital signatures, key exchange. Attacks on protocols. Case studies of protocol failures. Dictionary attack, salt, SKEY, SKID. Multiple-key cryptography, secret splitting, time stamping, group signatures, bit commitment, fair coinflipping, mental poker, interactive zero-knowledge proofs and how to make them noninteractive, blind signatures, oblivious transfer, simultaneous contract signing, digital certified mail, simultaneous exchange of secrets, secure electronic voting, secure multiparty computations, anonymous message broadcasting, digital cash. Elliptic Curves and Elliptic Curve Cryptography, Hyper-elliptic Curve Cryptography.

Comments: CS60065 and MA60031 are postgraduate courses primarily focusing on cryptographic and cryptanalytic techniques. The proposed course uses some concepts from CS60065 and MA60031 to cover some of the basic building blocks for designing secure and private systems. However, majority of the syllabus for the proposed course is complementary to these existing cryptography-centric courses since Usable privacy and security specifically start from the secure and private system/protocol implementation and then cover techniques to assess human-in-the-loop design dimensions for these systems.

The proposed course has therefore minimal overlap with CS60065 and MA60031. It will be useful for postgraduate students and research scholars to grasp the advanced topics in-depth, whereas undergraduate students can get the basic essence of current advances in usably secure and private system design.