CSE 347/547 | DES 306/525 Usable Security and Privacy
Mid-Sem Exam

Deadline: 2359hrs Sept. 27, 2025 [24hrs]

Instructions:

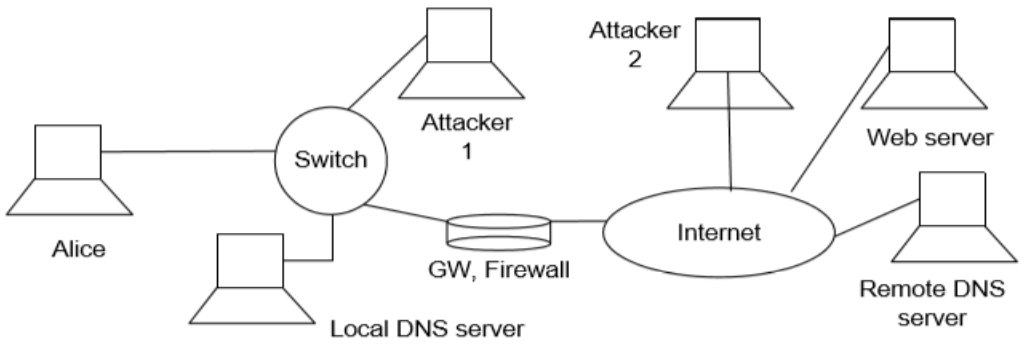
- Open Book. Individual assignment. Group discussions/work strictly prohibited
- Your answers need to be very specific and must include details. More details more points
- Explain with example wherever necessary.
- Include scenarios with assumptions and respective arguments/justifications

Total: 100 +10 points

1. [30 points] A large e-commerce operator (with payment interface) collects customers' data and utilizes third party vendors to perform advanced data analytics for providing value added services to customers.
   (a) [5pts] What are the various threats in data sharing that specifically apply for this e-commerce operator?
   (b) [7pts] e-com operator is only willing to share necessary data. How would you go about enumerating the data fields that you would need to perform user behavior modelling? Do provide the mapping for specific value-added services to user data.
   (c) [10pts] Pick any three value-added service and suggest appropriate user modelling technique. Justify
   (d) [8pts] e-com operator is also interested in advanced payment analytics across platforms. How would you go about integrate that data into your modelling? Elaborate on the complications and your solutions.

   Bonus [10pts]: Provided your model(s) are capable of capturing behavioral characteristics at individual user level, allowing e-com operator to query/suggest for extremely personalized products.

2. [30 points] Cyber Attacks



   a. [9pts] For the above Figure, describe how would you, as a security architect, design and employ usable encryption mechanisms that would prevent MITM based security breaches.
   b. [9pts] For the above usable encryption mechanism, explain the key management protocol in depth. Illustrate few scenarios where your protocol may fail.

c. [12pts] Consider a scenario where attacker 1 and attacker 2 have capability to launch, observe and adapt MITM attacks to inflict maximum damage. How can you provide a more comprehensive solutions for such situations? Justify.

3. [40 points] A university recently upgraded its authentication system for students and staff. To enhance security, they introduced the following changes:
   - All users must log in using multi-factor authentication (MFA), combining passwords with one-time codes sent via SMS.
   - Passwords must be at least 14 characters long, include upper/lowercase, digits, and special symbols, and must be changed every 60 days.
   - Users are automatically logged out after 15 minutes of inactivity and must re-authenticate.
   - The system does not support password managers due to "security concerns."

   As an expert in usable security and authentication, analyze (data based) this situation. In your essay, discuss:

   a. [8pts] How would you go about assessing usability problems caused by the new authentication policies? Elaborate your plan of action with specific illustrations. Include artifacts.
   b. [8pts] Enumerate the security vs. usability trade-offs evident in this deployment. Do elaborate on the process that helped you arrive at the trade-offs.
   c. [6pts] How does user behaviour (e.g., password reuse, insecure workarounds) may undermine the intended security?
   d. [10pts] Suggest design improvements that balance security with usability. The suggestions should include specific implementation (architecture, protocols, techniques, etc) details to given scenario.
   e. [8pts] How could you have prevented or reduced these problems before rollout? Do justify the process. Include artifacts.