CS763 Secure Software Development

HW 1: Cyber Attacks and Secure Software Development Process

**Name:**

**Instructions:**

1. Please name your file as CS763\_yourusername\_hw1.
2. All questions must be answered on an INDIVIDUAL basis. If your answer is inspired by the discussion with other students, you need to mention their names in your acknowledgement section.
3. State clearly all your assumptions if anything is ambiguous. Always ask if you have any questions.
4. Please **correctly cite and list any (online) references. Please pay attention to the academic conduct code, particularly the definition of plagiarism**.
5. Please submit your homework through Blackboard on time.
6. Thank You!

**Questions (100%):**

1. Search the Internet for a cyber attack in the last two or three years. Describe the attack in more details (e.g. who, when, what) and also address the following questions: (50%)
   1. Who are attackers and targets? When and How was the attack done? What underlying vulnerabilities were exploited?
   2. How much damage did the attack cause? What are possible mitigations?
2. Compare Seven touchpoints, Microsoft SDL and OWASP SAMM model, describe the similarities and differences in your own words. Which model would you like to adopt if you are in charge of a software development project? States your assumptions (about the project, develop team, organization) and relational. (50%)

## **Feedback:**

1. How long did you take to complete this homework? Is it too hard, too easy or OK?
2. Were lectures clearly present on this topic? Did this homework help you learn this topic? How well do you understand this topic?
3. Do you have any other feedback?