ה kurs: ויוו קורס

מותנש: ד"ר דוד מובשבי

 dmovshovitz@idc.ac.il

 dmovshovitz@idc.ac.il

 מספר הקורס: 3168

 שעת קורס: 3

 בחרה: 3

 דרישת הקורס: 

 קוד קבוצה: 222316801

 שפה לימוד: עברית

 מбереж: סופי

 תניי הקורס:

 קוד:

 52 - חשבוני אינפורטס 우리나
 53 - חשבוני אינפורטס 우리나
 54 - עונש וקינויים לא
 55 - עונש וקינויים לא
 56 - מתרגמת בידוד
 57 - מבני תרגום
 69 - מדע ותורת הקבוצת
 417 - מבוא למדעי המחשב
Digital products and services are usually composed from a mobile app, a web server application running on a cloud infrastructure. As a result, these digital systems are facing unique information security threats, at the network layer, at the infrastructure layer, and at the application layer (client-side and server-side). In the course we will discuss these threats and how to secure these systems by implementing security mechanisms and security best practices.

We will learn how to secure the infrastructure used to run the digital products and services, and how to secure the application layer both on the client-side (i.e. the mobile app) and on the server-side (i.e. the API based (web) application) by implementing authentication, session-management, and authorization. In addition, we will discuss application layer vulnerabilities (e.g. insufficient input validation) and related attacks (e.g. injection attacks and XSS), and will learn how to prevent them by implementing secure coding best practices.
In the course we will learn:

- The information security threats to digital products and services
- Authentication & Session Management
  - Mobile and Web application authentication
  - Mobile and Web application session management
    - CSRF attack and mitigations
  - Web Single Sign-On (SSO) and SAML
- Authorization & Access Control
  - Access Control fundamentals
    - The least privileges principle and how it should affect application architecture
    - Distributed access control for service-based architecture
  - Android access control mechanisms
    - Android file system security and vulnerabilities
    - Android System Resources Access Control model
      - Activity Permissions & Activity Hijacking
      - Service exported attribute & Intent spoofing
      - Service permissions & Service Hijacking
      - Content Providers Permissions & Related attacks
- Injection attacks
  - SQL Injection and related evasion techniques,
  - OS/LDAP/XPath and other injection attacks,
Since the course is covering many topics and there is no text book, the presentations are very detailed and cover all the subjects discussed in the course in detail.

A list of recommended books, academic papers and other web resources for extended reading will be published on the course web-site.