***SECENTIS 2016*** winter school provides a good overview about current status of IT system security from different perspectives. Some lectures focused on software security enhancement by performing a comprehensive static analysis for the code. Other lectures gives an overview about current level of security attacks and recommended defensive techs, against these attacks. The conference provides also a good overview about data privacy and recommended countermeasures against the violation of data privacy. The discussed topics within the conference are listed below, with brief description about discussed ideas, within each topic.

Static analysis:

Main goal of static analysis process performed on a given program is to clean program code. Cleaning the code could be performed by different activities, such as, the identification of code pieces, which causes presences of vulnerabilities and fix it. Another example of cleaning activities is the identification of unused code and eliminated, thus, program code becomes more readable and reliable.

In this lecture, constraints-based approach for code analysis were elaborated. In addition, some constraints-based languages and tools, were presented. Where, the main focus was on TIP language, for which, a set of sample code for constraints rules was explained. By conclusion, the lecture showed the necessity of using code analysis languages and tools for the enhancement of program security level.

(Static analysis) security testing strategy:

Lecture gives an overview about static analysis methods and tools applied by big vendors like SAP. It went through a set of recommended static analysis tools and methods. It explained these methods and tools challenges and its solutions. By conclusion, it was recommended the usage of tools in complementary way in order to gain better code analysis results. It was stated also, that, static analysis still under development, and the solutions for its challenges need more improvement (e.g. false positive challenge).

End to end secure development in practice:

Lecture explained recommended Secure Software Development Life-Cycle (S2DLC). It described also, possible challenges, which usually face different stakeholders within different phases within the life-Cycle. These phases are listed below, with brief description about performed activities during each phase:-

* ***Security Training***: in this phase, different stakeholders included in system development will be teach about security.
* ***Risk Assessment*** *(threat modelling)*: in this phase software design security will be checked, where, costly design flaws should be catch.
* ***Secure Development & Testing***: in this phase the code will be checked to find and fix the security bugs.
* ***Security Validation***: in this phase, penetration test will be performed on the system to find system vulnerabilities.
* ***Security Response***: in this phase, system owner will react and adapt system based on discovered problem.

Cyber-attacks and defence:   
  
This topic was elaborated in 2 lectures, the first lecture, went through latest kinds of attacks, which targeted Internet of Things systems. Described attacks were classified based on targeted system type, into three classes, being industrial control attacks, corporate systems attacks and home systems attacks. The explanation of these attacks, were enhanced with brief description about attacks malicious activities and examples for exploited system.

Second lecture concentrated on intrusion detection, since, it is considered as first step to defence against cyber-attacks. Where, different approaches for intrusion detection were explained, begin:-

* Rejection based approach: based on attack behaviour recognizing.
* Acceptance based approach: based on usual behaviour recognizing.

The advantages and disadvantages of these approaches were explained in comparable way. By the end, combined approach were presented and recommended for malicious activities detection.

Directions of IT system security:

This lecture gives an overview about different parties in security industry, such as, anti-malware enterprises. It also went through some of presenter experiences in IT security field. Where, some of faced problems and performed solutions were explained.

WEB APPLICATION SECURITY:

This lecture discusses the security of web application, where it analyses steps or phases followed by attackers to exploit given web application. It gives also an overview about all areas from which an attack could be performed and recommended defensive techs, which should be applied.

Data privacy:

This topic was discussed in four lectures. Each one of these lectures discussed a particular aspect of data privacy. Below are a brief description about discussed aspects within each lecture.

***First lecture***: - this lecture focuses on privacy concepts, laws and Privacy Enhancement Techs (PET). Thus, below concept and points were elaborated:-

* The kinds of data which considered private.
* The data source for private data (Internet, social media...)
* Different parties, which could benefits from private data.
* Different parties included in data privacy life cycle.

The lecture describes also a set of privacy requirements, such as, privacy auditing, privacy seal and Privacy Impact Assessments (PIA). By the end, some approaches were recommended for privacy enhancements, such as, having privacy officer, who should verify privacy stratification for a given institute.

***Second lecture***: - this lecture concentrated on the challenges of privacy policies, such as: reading cost of privacy statement (e.g. time and effort). It explained also possible solutions for these challenges. For instance, possible solution for reading cost challenge is the usage of framework for auto reading and checking of privacy statement (e.g. P3P). In this kind of framework user could set his privacy preferences, which are checked automatically over given privacy statement. Thus, this framework reduce the cost of reading and help reader to take precise decision.

***Third lecture:*** this lecture discussed misusing possibility of offline data to violate privacy attributes for a given entity, in particular, entity anonymity. Where, it gives examples, reflects the possibility of privacy violating through some techs, such as, data linking and correlation. As countermeasures, some techs were elaborated, which, could be used to increase anonymity of data. By the end, challenges and countermeasures for trajectory and text data anonymization were elaborated.

***Fourth lecture***: this lecture, discussed online tracking and location identification from different perspectives. At the beginning, an overview was given about used techs for online tracking, such as, cookies and java script. Later, different resources for tracking data are explained (e.g. RFID chips). Additionally, an overview was given about different techs, which could be used for location determination (e.g. WLAN and cameras). By the end, some countermeasures for location identification techs was explained.

***Reported by: Seraj Fayyad***