Project Acronym: MEDIS

Project Title: A Methodology for the Formation of Highly Qualified Engineers at Masters Level in the Design and Development of Advanced Industrial Informatics Systems

Contract Number: 544490-TEMPUS-1-2013-1-ES-TEMPUS-JPCR

Starting date: 01/12/2013 **Ending date:** 30/11/2016

Deliverable Number: 2.3

Title of the Deliverable: AIISM teaching resources - Mobile and Cloud Computing Platforms
Task/WP related to the Deliverable: Development of the AIISM teaching resources - Mobile and Cloud Computing Platforms

Type (Internal or Restricted or Public): Internal

Author(s): Radu Dobrin and Sasikumar Punnekkat

Partner(s) Contributing:

Contractual Date of Delivery to the CEC: 30/09/2014

Actual Date of Delivery to the CEC: 30/09/2014

Project Co-ordinator

Company name :	Universitat Politecnica de Valencia (UPV)
Name of representative :	Houcine Hassan
Address :	Camino de Vera, s/n. 46022-Valencia (Spain)
Phone number :	+34 96 387 7578
Fax number :	+34 963877579
E-mail :	husein@upv.es
Project WEB site address :	https://www.medis-tempus.eu

Context

WP 2	Design of the AIISM-PBL methodology
WPLeader	Universitat Politècnica deValència (UPV)
Task 2.3	Development of the AIISM teaching resources - Mobile and Cloud Computing Platforms
Task Leader	MDU
Dependencies	UPV, MDU, TUSofia, USTUTT, UP

Author(s)	Radu Dobrin and Sasikumar Punnekkat
Contributor(s)	
Reviewers	

History

Version	Date	Author	Comments
0.1	01/03/2014	Radu Dobrin and Sasikumar Punnekkat	Initial draft
1.0	19/09/014		Final version

Table of Contents

1 Executive summary

WP 2.3 details the learning materials of the Advanced Industrial Informatics Specialization Modules (AIISM) related to the Mobile and Cloud Computing Platforms.

The contents of this package follows the guidelines presented in the MDU's documentation of the WP 1 (Mobile and Cloud Computing Platforms)

- The PBL methodology was presented in WP 1.1
- The list of the module's chapters and the temporal scheduling in WP 1.2
- The required human and material resources in WP 1.3
- The evaluation in WP 1.4

The rest of the document is organized as follows: Section 2 introduces the course and the outlines. Section 3 details the lectures, divided in subsections for each chapter. Section 4 describes the labs. There is a special subsection for each chapter. Section 5 gives an overview to the seminars. Each seminar has its own subsection. Finally section 7 lists the bibliography and the references.

2 Introduction

This chapter will cover the security related issues that a system connected to the internet might experience, suggest solutions and discuss the role based access control approach. 2 Lectures will be conducted mainly focusing on security in mobile communication and security and control.

At the end of the lecture, the students will be able to:

- Understand the basics of security related issues
- Start implementing a simple role based access control to their projects

3 Lectures

The lecture 1 in this chapter introduces computer security and the need for it in embedded systems. It outlines the template for a threat model [2][3] after positioning security in the big picture of dependability [1]. Later, some of the most common computer security threats [4] [5] [6] [8] [9] [11] [12] are discussed using the threat model discussed earlier, and a real world example where computer security was compromised that lead to significant losses is discussed. Lecture 1 of this chapter is accessible in file Lecture 9_Security-1.pptx.

Lecture 2 presents some of the ways to secure computer systems that are of interest to this course. Specifically, it discusses cryptography, virtual private networks and role based access controls to secure computer systems. Further, the role based access control mechanism is discussed in detail. Lecture 1 of this chapter is accessible in file Lecture 10_Security-2.pptx.

4 Lab

This chapter consists of two labs aimed at strengthening the fundamentals of students in the area of computer security. In the first lab, students use a famous open source web application called webgoat [13] that is widely used for training security professionals to actually exploit some of the threats discussed in the lectures. This will enable students to understand the intricacies involved in securing embedded systems.

In the second lab, the students will implement role based access control for the mobile app that controls the water tank controller. Specifically, the students will implement two roles:

User- can only get readings and monitor for alarms
Admin- can get readings as well as set the values of temperature, water level etc

5 Seminar

In the seminar corresponding to the first lecture, the students are expected to write a 1-page report that discusses the solutions of the lab. They are also required to discuss the possible strategies that could have been adopted to prevent a STUXNET like incident: The Real Story of Stuxnet, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/

In the seminar corresponding to the second lecture the students are expected to write a 1-page report where they discuss the solutions for the lab, especially answering the following questions:

Is this the best solution?

Can the security be breached, e.g., using any of the techniques that you learned?

How can you further improve security?

What are the challenges involved in securing such systems

6 Miniproject

In the first miniproject, the students will write a 4 page report on how they can apply security concepts for embedded systems

- Merits
- Demerits
- Some recent advances
- Open problems

In the second miniproject, the students will perform a literature survey on encryption techniques, with particular focus on mobile devices and embedded systems:

- State of the art
- Impact on size, weight and power constraints

Emerging challenges
Open problems

7 References

[1] Basic concepts and taxonomy of dependable and secure computing, Avizienis, A. ; Laprie, J.-C. ; Randell, B. ; Landwehr, C., IEEE Transactions on Dependable and Secure Computing, 2004

[2] Threat Modeling: A Process To Ensure ApplicationSecurity, http://www.sans.org/reading-room/whitepapers/securecode/threat-modeling-process-ensure-application-security-1646

[3] Template Sample: Web Application Threat Model, https://msdn.microsoft.com/en-us/library/ff649779.aspx

[4] Understanding Denial-of-Service Attacks (Security Tip (ST04-015)), https://www.us-cert.gov/ncas/tips/ST04-015

[5] Anoymous, http://en.wikipedia.org/wiki/Anonymous_%28group%29

[6] The Real Story of Stuxnet, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/

[7] Building a Cyber Secure Plant, http://www.totallyintegratedautomation.com/2010/09/building-a-cyber-secure-plant/

[8] World's largest Denial of Service attack caused by vulnerability in the infrastructure of the web, http://www.independent.co.uk/life-style/gadgets-and-tech/worlds-largest-denial-of-service-attack-caused-by-vulnerability-in-the-infrastructure-of-the-web-9122200.html

[9] Denial-of-Service Attacks, http://www.cert.org/historical/advisories/ca-1997-28.cfm

[10] The Helminthiasis of the Internet, ftp://ftp.isi.edu/in-notes/rfc1135.txt

[11] SQL Injection, https://technet.microsoft.com/en-us/library/ms161953%28v=SQL.105%29.aspx

[12] Social Engineering: Manipulating the Source, http://www.sans.org/reading-room/whitepapers/engineering/social-engineering-manipulating-the-source-32914

[13] Webgoat https://www.owasp.org/index.php/WebGoat_Installation