TECHNOLOGY FOR SECURITY

1.1. Identification

University:	Alma Mater Studiorum – Università di Bologna																	
School:	School of Engineering																	
Course:	Technology for Security																	
ECTS:	6																	
Semester:	*Winter*						X	*Summer*										
Category	*Fundamental course*							*Specialisation course*										X
Module	*MFI*		*MFII*		*MFIII*			*MSI*		*MSII*		*MSIII*		X				
Teachers:	Rebecca Montanari																	
Language:	*English*	X	*Italian*	X	*Swedish*		*Spanish*											

1.2. Learning-outcomes

- knowledge about the fundamentals of information system security and technologies
- understand how to design, use and manage mechanisms and services for addressing intentional attacks to data integrity, confidentiality and availability

1.3. Competencies

- **General**
  - To have critical understanding of security threats and appropriate countermeasures
  - Communication skills
  - To be able to work in an international context

- **Specific**
  - To understand the methods for investigating security in sensor systems
  - To learn the theoretical concepts on which security algorithms and protocols are based
  - To develop security measures tailored to the specific characteristics of sensor systems

1.4. Contents

1. Introduction to security threats and requirements for sensor systems

2. Theory of symmetric ciphers and mechanisms for identification, data confidentiality and authentication. Case studies: RC4, DES, AES, Key distribution center
3. Theory of asymmetric ciphers and mechanisms for identification, data confidentiality and authentication. Case studies: RSA, DSA, PKI.
4. Cryptographic key distribution and trust bootstrapping
5. Code safety, including sandboxing, software fault isolation, and proof-carrying code
6. Network security mechanisms and protocols. Case studies: TLS, IPSec
7. Access control models and mechanisms over how data can be accessed and used
8. Privacy issues and protection mechanisms

1.5. Teaching Methodology

- Lecture sessions.
- Laboratory sessions.

1.6. Evaluation

- Oral exams, including discussion of the laboratory work.

1.7. Bibliography

C Pfleeger & S Pfleeger, *Security in Computing*. Prentice Hall, 2002.
A J Menezes, P C van Oorschot & S A Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996
William Stallings, *Cryptography and Network Security, Principles and Practice,* Prentice Hall, 2003.