CPIS-312 Syllabus

Catalog Description

CPIS-312 Information and Computer Security
Credit: 3 (Theory: 3, Lab: 1, Practical: 1)
Prerequisite: CPCS-370
Classification: Department Required

The objective of this course is to equip students with the scientific and mathematical concepts and skills related to information security. Topics include the security of information and software systems, including attacks and data encryption, mathematical foundations, algorithms of cryptography, ways of distributing keys, techniques of data protection over computer networks, and controlling access using passwords.

Class Schedule

Meet 50 minutes 3 times/week or 80 minutes 2 times/week

Lab/Tutorial 90 minutes 1 times/week

Textbook

Steve Suehring, , "Linux Firewalls" 5 edition (2015)

ISBN-13 9780134085043 **ISBN-10** 0134085043

Grade Distribution

Week	Assessment	Grade %
6	Exam 1	15
10	Exam 2	15
12	Group Project	15
14	Lab Exam	20
16	Comprehensive Final Exam	35

Last Articulated

April 12, 2018

Relationship to Student Outcomes

a	b	c	d	e	f	g	h	i	j
x	x	x		x			x	x	

Course Learning Outcomes (CLO)

By completion of the course the students should be able to

1. **Classify the challenges and scope of information security into the basic security reqiurments such as confidentiality, integrity, and availability. (b)**
2. Apply elementary results from Numer Theory and Abstract Algebera in the context of cryptography (a)
3. Explain the importance of cryptographic algorithms used in information security in the context of the overall information technology (IT) industry; (a)
4. Compare between classic and modern ciphers (a)
5. **Analyze the symmetric algorithms for encryption-based security of information (A5/1, DES, 3DES, AES). (a)**
6. **Calculate public-key based asymmetric algorithms for encryption-based security of information (RSA, Diffie-Hellman, PKI). (a)**
7. **Apply the concep of hash functions with applications (MD5, SHA-1, HMAC, Digital Signature) to achive basic goals of Information security. (a)**
8. Explain the use of access control mechanisms used for user authentication and authorization with examples (h)
9. **Differentiate commonly used solutions for security protocols (SSL, IPSec, Kerberos) (i)**
10. Explain the use of such security tools as firewalls and intrusion prevention systems (i)
11. Deploy solutions against common software flaws and malware (i)
12. Explain operating system security functions (i)
13. Explain the importance of physical security and discuss ways to improve physical security of an enterprise (e)
14. Describe the basic process of risk assessment in the context of overall IT security management (h)
15. Test the robustness and vulnerabilities of a system (c)

Coordinator(s)

Prof. Bander Alzahrani, Professor

CPIS-312 Syllabus

Topics Coverage Durations

Topics	Weeks
challenges and scope of information security, basic security concepts such as confidentiality, integrity, and availability.	1
Importance of cryptographic algorithms used in information security in the context of the overall information technology (IT) industry.	1
Comparision of classic and modern ciphers	1
Symmetric algorithms for encryption-based security of information (DES,3DES, AES) and analyze their performance	1
Asymmetric algorithms for encryption-based security of information (RSA, DH, ElGamal) and analyze their performance.	1
Digital Signature & Hash functions	1
Use of access control mechanisms used for user authentication	1
Use of access control mechanisms used for user authorization, use of such security tools as firewalls and intrusion prevention systems	1
Solutions for security protocols (SSL, IPSec, Kerberos)	1
Deployment the solutions against common software flaws and malware	1
Operating Systems and Security	1
Importance of physical security and ways to improve physical security of an enterprise	1
Basic process of risk assessment in the context of overall IT security management	1
Robustness and vulnerabilities of a system	1