Form: **Course Syllabus**	**Form Number**	
	Issue Number and Date	2/3/24/2022/2963 5/12/2022
	Number and Date of Revision or Modification	
	Deans Council Approval Decision Number	
	The Date of the Deans Council Approval Decision	
	Number of Pages	8

1.	**Course title**	Authentication and Security Models	
2.	**Course number**	1911461	
3.	**Credit hours**	3	
	Contact hours (theory, practical)	3 (theory)	
4.	**Prerequisites/corequisites**	Computer Networks (1901363)+ Cryptography (1911241)	
5.	**Program title**	Cybersecurity Program	
6.	**Program code**	11	
7.	**Awarding institution**	The University of Jordan	
8.	**School**	King Abdullah II School of Information Technology	
9.	**Department**	Computer Science	
10.	**Course level**	4	
11.	**Year of study and semester (s)**	Fourth year, Spring 2024-2025	
12.	**Other department (s) involved in teaching the course**	-	
13.	**Main teaching language**	English	
14.	**Delivery method**	☒Face to face learning ☐Blended ☐Fully online	
15.	**Online platforms(s)**	☒Moodle ☒Microsoft Teams ☐Skype ☐Zoom ☐Others…………	
16.	**Issuing/Revision Date**	October, 2023	

17. Course Coordinator:

Name: Dr. Oraib AbuAlganam	Contact hours: Sun,Tu-10:30-11:30 Mon 10:30-11:30
Office number: 124	Phone number: +9625355000 Extension :22592
Email: O.AbuAlganam@ju.edu.jo	

18. Other instructors:

Name: None

Office number:

Phone number:

Email:

Contact hours:

19. Course Description:

This course introduces students to the growing impact of attackers on identification and authentication systems and additional strain put on the ability to ensure that only authorized users obtain access to controlled or critical resources. Topics covered: **basic cryptology techniques** and their application to contemporary authentication methods, **introduction for Authentication**, **Crypto Hash Functions for Authentication, Message Authentication Codes**, **Digital Signature**, **Trust Models. Key management and distribution, User Authentication**, **Access Control, Wireless Authentication, cloud and IoT authentication**.

20. Course aims and outcomes:

A- Aims:

Goal: Provide the students with a solid foundation in Authentication concepts and practices, preparing them for careers in cybersecurity, network administration, and related fields.

Objectives:

- Understand fundamental of Authentication models.
- Understand fundamental of Active Directory.
- Recognize different Authentication security protocols and their properties.
- Provide hands-on experience with tools and techniques for Authentication Models.
- Understand fundamental of modern Authentication techniques

B- Students Learning Outcomes (SOs):

- Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions. (ABET SO 1)
- Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline. (ABET SO 2)
- Recognize professional responsibilities and make informed and equitable judgments in computing practice based on legal and ethical principles (ABET SO 4)
- Apply security principles and practices to maintain operations in the presence of risks and threats (ABET SO 6)

C- Intended Learning Outcomes (ILOs):

Successful completion of this module should lead to the following learning outcomes:

[Level Descriptor: Knowledge]

A. Knowledge and Understanding (students should)

A1) Gain an understanding of the fundamental concepts and Authentication.
A2) Identifying the cryptography techniques that are related to authentication.
A3) Identify trust relationships involved in access control and authentication systems.
A4) Gain an understanding of the limitations of wireless networks and IoT.

[Level Descriptor: Skills]

B. Intellectual skills: with the ability to

B1) Evaluate different authentication and security models
B2) Analyze and identify different modern authentication models.

[Level Descriptor: Skills]

C. Subject specific skills – with ability to use

C1) Engage practical skills by delving into widely used authentication protocols such as Kerberos and LDAP.

C2) Engage practical knowledge and skills relevant to securing network infrastructure and managing user identities in enterprise environments.

[Level Descriptor: Competencies]

D. Transferable skills – with ability to

D1) Collaboratively implement an application integrated with a suitable authentication technique as part of a group project

Upon successful completion of this course, students will be able to:

Program SOs ILOs of the course	SO (1)	SO (2)	SO (4)	SO (6)

A1) Gain an understanding of the fundamental concepts and Authentication.	√			
A2) Identifying the cryptography techniques that are related to authentication.	√			
A3) Identify trust relationships involved in access control and authentication systems.		√		
A4) Gain an understanding of the limitations of wireless networks and IoT.	√			
B1) Evaluate different authentication and security models				√
B2) Analyze and identify different modern authentication models.		√		
C1) Engage practical skills by delving into widely used authentication protocols such as Kerberos and LDAP.			√	
C2) Engage practical knowledge and skills relevant to securing network infrastructure and managing user identities in enterprise environments.			√	
D1) Collaboratively implement an application integrated with a suitable authentication technique as part of a group project				√

21. Topic Outline and Schedule:

Week	Lecture	Topic	ILO	Learning Methods (Face to Face/Blended/ Fully Online)	Platform	Synchronous / Asynchronous Lecturing	Evaluation Methods	Resources
1	1.1	Introduction	A1	Face to face lecturing	Moodle	Synchronous		
	1.2	Review of Cryptography	A2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook(s)
	1.3	Project discussion and labs	D1	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
2	2.1	Introduction for Authentication	A1	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook(s)
	2.2	Active Directory	A1, C1, C2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook(s)
	2.3	Lab 1 (operation AAA)	C1, C2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on

3	3.1	Lab2 (Install AD)	C1, C2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
	3.2	Lab3 (Initial setting AD)	C1, C2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
	3.3	Lab4(Clients control)	C1, C2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
4	4.1	Access Control Lab5 (Group polices)	C1, C2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
	4.2	Crypto Hash Functions for Authentication, Message Authentication Codes	A2, A3	Face to face lecturing	Moodle	Synchronous	Midterm, Final, Lab2	Textbook (s)
	4.3	Lab 6 (Crypto Lab seed lab)	C1, C2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
5	5.1	PKI	A2, A3	Face to face lecturing	Moodle	Synchronous	Midterm, Final, Lab3	Textbook(s)
	5.2	key management and distribution	B1, B2	Face to face lecturing	Moodle	Synchronous	Midterm, Final, Lab3	Textbook(s)
	5.3	key management and distribution	B1, B2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
6	6.1	Digital Signature, Trust Models	B1, B2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook(s)
	6.2	Digital Signature, Trust Models	B1, B2	Face to face lecturing	Moodle	Synchronous	Midterm, Final, Lab4	Textbook(s)
	6.3	Lab 7 (PKI Lab)	C1, C2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
7	7.1	Web server (Installation)		Face to face lecturing	Moodle	Synchronous	Midterm, Final, Lab5	Textbook(s)
	7.2	LDAP	C1, C2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook(s)
	7.3	User Authentication , Remote User-Authentication Principles	B1, B2	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Textbook(s)
8	8.1	Remote User-Authentication Principles	B1, B2	Face to face lecturing	Moodle	Synchronous	Midterm, Final, Lab 6	Textbook(s)

	8.2	Lab 8 (Kerberos)	C1, C2	Face to face lecturing	Moodle	Synchronous	Midterm, Final, Lab 6	Textbook(s)
	8.3	Students Project discussion	C1, C2, D1	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
9	9.1	Review		Face to face lecturing	Moodle	Synchronous	Midterm, Lab7, Final	Textbook(s)
	9.2	Midterm		Face to face lecturing	Moodle	Synchronous	Midterm, Lab 7, Final	Textbook(s)
	9.3	Students Project discussion	C1, C2, D1	Face to face lecturing	Moodle	Synchronous	Midterm, Final	Hands-on
10	10.1	**SAML** and **OAuth:**	A3, B1, B2	Face to face lecturing	Moodle	Synchronous	Final	Hands-on
	10.2	**SAML** and **OAuth:**	A3, B1, B2	Face to face lecturing	Moodle	Synchronous	Final	Hands-on
	10.3	Students Project discussion	C1, C2, D1	Face to face lecturing	Moodle	Synchronous	Final	Hands-on
11	11.1	**SAML** and **OAuth:**	A3, B1, B2	Face to face lecturing	Moodle	Synchronous	Final	Hands-on
	11.2	**SAML** and **OAuth:**	A3, B1, B2	Face to face lecturing	Moodle	Synchronous	Final	Hands-on
	11.3	Students Project discussion	C1, C2, D1	Face to face lecturing	Moodle	Synchronous	Final	Hands-on
12	12.1	Wireless Authentication	A4	Face to face lecturing	Moodle	Synchronous	Final	Textbook(s)
	12.2	Wireless Authentication	A4	Face to face lecturing	Moodle	Synchronous	Final	Textbook(s)
	12.3	Students Project discussion	C1, C2, D1	Face to face lecturing	Moodle	Synchronous	Final	Hands-on
13	13.1	cloud and IoT authentication	A4	Face to face lecturing	Moodle	Synchronous	Final	Textbook(s)

	13.2	cloud and IoT authentication	A4	Face to face lecturing	Moodle	Synchronous	Final	Textbook(s)
	13.3	Students Project discussion	C1, C2, D1	Face to face lecturing	Moodle	Synchronous	Final	Hands-on
14	14.1	Students Project discussion	C1, C2, D1	Face to face lecturing	Moodle	Synchronous	Final, Lab6	Textbook(s)
	14.2	Students Project discussion	C1, C2, D1	Face to face lecturing	Moodle	Synchronous	Final	Textbook(s)
15	15	**Final Exam**						

22. Evaluation Methods:

Opportunities to demonstrate achievement of the SLOs are provided through the following assessment methods and requirements:

Evaluation Activity	Mark	Topic(s)	SLOs	Period (Week)	Platform
Midterm Exam	25		1,2,4,6	9	JUExams
Labs	4	Access control		2	Windows server 2019
		Active Directory		3,4	Kali Linux
		Crypto Hash, PKI		4,5	
		Authentication protocols		8,10	Kali Linux
Quiz	6		4,6	10	
Project	15	Selected	1,2,4,6	8-14	auth0.com , LDAP
Final	50	All	1,2,4,6	15	JUExams

23. Course Requirements

(e.g: students should have a computer, internet connection, webcam, account on a specific software/platform…etc):

- Computer + security tools
- Virtual environments

- Internet connection
- Account on Moodle

24. Course Policies:

A- Attendance policies:

Maximum allowable absence 15% of number of lectures per semester.

B- Absences from exams and handing in assignments on time:

Students are expected are expected to completely adhere to the assignments strict deadlines, absolutely no exceptions are given.

It's student's responsibility to inform his instructor about his absence from any exam during period not exceeding 3 days.

If you miss the midterm, then a makeup exam will not be provided unless you submit a valid absence excuse, within three days from the midterm, to your lecturer. This excuse must be signed and stamped from the UJ hospital in order to be valid. If your lecturer accepts the excuse, then you will be able to take the makeup. You need to follow up the departmental announcements regarding the makeup date and time. Please note that the lecturer may either accept or reject your excuse based on UJ regulations.

C- Health and safety procedures:

Full safety of the computer labs.

D- Honesty policy regarding cheating, plagiarism, misbehavior:

Students' cheating, plagiarism and misbehavior will be transformed to special committee.

E- Grading policy + Weighting (i.e. weight assigned to exams as well as other student work)

Intended grading scale

0 – 40	F
41-49	D-
50-53	D
54-57	D+
58-61	C-
62-66	C
67-70	C+
71-75	B-
76-79	B
80-84	B+
85-89	A-
90-100	A

F- Available university services that support achievement in the course:

Equipped Computer labs.

25. References:

Required book (s), assigned reading and audio-visuals:

A- Cryptography and Network Security: Principles and Practice, William Stallings, 8th Edition, 2021

B- Stallings, Network Security Essentials, 4ed, 2011

C- Schneier, Cryptography Engineering, 2010

D- Security protocol repositories

26. Additional information:

ملاحظة1: في حالة التغيب عن امتحان الـ Mid Term لن يكون هناك امتحان تعويضي إلا في حالة وجود عذر وحالة طارئة من المستشفى. على الطالب إبراز العذر لمدرس المادة في فتره لا تتجاوز الثلاثة أيام من تاريخ الامتحان, وللمدرس الحق في قبول أو رفض العذر , وحسب التعليمات.

ملاحظة2: لتفادي المشاكل والأخطاء التي تنتج, لا يجوز إجراء النقل الداخلي بأي حال من الأحوال.

For more details on University regulations please visit http://www.ju.edu.jo/rules/index.htm

Moodle:

http://elearning.ju.edu.jo/

Name of Course Coordinator: Dr. *Oraib AbuAlganam* Signature: -------- Date: February, 2025

Head of Curriculum Committee/Department: -----------------Signature: -------------------

Head of Department: --Signature: -------------------

Head of Curriculum Committee/Faculty: ----------------------Signature: -------------------

Dean: ---Signature: -------------------