جامعة الأمير سطام بن عبدالعزيز

كلية هندسة وعلوم الحاسب

قسم هندسة الحاسب

Master of Engineering in Cybersecurity

Faculty Member Guide

2022

1- مقدمة

1- Introduction

نرحب بكم، أعضاء وعضوات هيئة التدريس، ونقدم لكم تعريفاً موجزاً في هذا الدليل عن برنامج ماجستير الهندسة في الأمن السيبراني. تم اعداد هذا البرنامج بكلية هندسة وعلوم الحاسب كأحد برامج الدراسات العليا المميزة في جامعة الأمير سطام بن عبدالعزيز، حيث بدأ قبول الطلاب والطالبات به في العام الدراسي 1440-1441هـ (2019-2020). النقاط التالية تلخص أهمية البرنامج وحاجة المجتمع إليه وأهدافه العامة.

We welcome you, faculty members, and give you a brief introduction in this guide to the Master of Engineering in Cybersecurity program. This program was prepared in the College of Computer Engineering and Sciences as one of the distinguished postgraduate programs at Prince Sattam bin Abdulaziz University, as the admission of male and female students began in the academic year 1440-1441 H (2019-2020). The following points summarize the importance of the program, the community's need for it, and its general objectives.

أهمية البرنامج

- حماية عملية نقل البيانات والمعلومات خلال شبكات الحاسب.
- تأمين البيانات والمعلومات والأنظمة والأجهزة الموزعة في مواقع مختلفة من الهجمات.
- اكتشاف الهجمات والاختراقات التي قد تتعرض لها الأجهزة.
- استرجاع البيانات وإعادة تأهيل الأجهزة المتضررة من الهجمات الأمنية.
- المساهمة في تعزيز الأمن القومي للمملكة المرتبط بالأمن السيبراني من خلال استخدام التقنيات بعد تطويرها ومن خلال المختصين المهرة في المجال والمدربين التدريب الجيد على أعلى المستويات.
- نقل مفهوم تكنولوجيا الأمن السيبراني للطلبة والباحثين وكذلك نقلها للمجتمع

حاجة المجتمع للبرنامج

- هناك حاجة ماسة لخبراء مدربين تدريبا عاليا يمكنهم من القيام بمهمة ضمان سلامة وأمن المعلومات في مختلف مؤسسات المملكة سواء كانت حكومية أو خاصة.
- هناك حاجة ماسة لتثقيف أفراد المجتمع بأهمية وكيفية تأمين البيانات والمعلومات والأجهزة.

2- رسالة وأهداف البرنامج
2-Program Mission and Goals

Program Mission

To provide a suitable environment for producing highly qualified Cybersecurity engineers, capable of solving security issues and assuming leadership to make significant contribution in knowledge society.

أهداف البرنامج

- تزويد الطالب بمعرفة متخصصة ومتعمقة في مجال الأمن السيبراني من بين مجالات فرعية مثل أمن الأجهزة وأمن الشبكات وأمن الأنظمة.
- تعزيز قدرة الخريجين على النجاح في التعامل مع أحدث التطورات في المجال، وصياغة الحلول للتصدي للهجمات، والتخطيط لعالم آمن من خلال الأمن السيبراني.
- تزويد الطلبة بالمهارات الضرورية في مجال الأمن السيبراني للمساهمة في تعزيز الأمن القومي للمملكة المرتبط بالأمن السيبراني من خلال استخدام التقنيات بعد تطويرها.
- تأهيل الطالب لمواصلة الدراسات العليا والبحث العلمي في مجال الأمن السبراني.

Program Goals

PG1: Provide graduates with an in-depth specialization knowledge in cybersecurity, selected from areas such as hardware security, network security and systems security.

PG2: Enhance the ability of graduates to succeed in dealing with the latest developments in the field, formulate solutions to address attacks, and plan for a secure world through cybersecurity.

PG3: Provide graduates with the necessary skills in Cybersecurity to contribute to enhancing the national security of the Kingdom of Saudi Arabia associated with cybersecurity through the adaptation of developed technologies.

PG4: Qualify graduates to pursue more postgraduate studies and scientific research in the field of cybersecurity.

3- مخرجات تعلم البرنامج وسمات الخريجين

3-Program Learning Outcomes and Graduate Attributes

Program Learning Outcomes (PLOs)

The PLOs are classified to three categories: Knowledge (K1, K2), Skills (S1, S2) and Values attributes (V1, V2, V3). These PLOs are as follows:

K1: Describe complex computing problems related to cybersecurity.

K2: Recognize the principles of computing applications and optimum security solutions.

S1: Implement and evaluate a computing-based solution to meet a given set of computing requirements in the context of cybersecurity.

S2: Apply security principles and practices to maintain operations in the presence of risks and threats.

V1: Communicate effectively in a variety of professional contexts.

V2: Respect professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.

V3: Function effectively as a member or leader of a team engaged in activities appropriate to cybersecurity.

Graduate Attributes

Graduates who successfully completed the program are expected to have the following attributes:

CSE1-Have in-depth knowledge, understanding and skills associated with Cybersecurity.

CSE2-Have the ability for lifelong personal development and learning to be successful in society.

CSE3-Have the ability to evaluate and draw conclusions from information, to find sustainable solutions to complex security problems and make decisions.

CSE4-Have the ability to lead and support others by inspiring them with a clear vision and motivating them to achieve security goals.

CSE5-Have the ability to work under pressure, where the organization's security can be at stake if they do not work carefully and thoroughly.

4- شروط القبول للبرنامج

4- Program admission requirements

فرص القبول بالبرنامج متاحة للطلاب والطالبات مرة في العام الدراسي وفقاً لاستيفاء الشروط العامة والخاصة أدناه:

شروط اللائحة الموحدة للدراسات العليا

- أن يكون المتقدم سعودياً، أو على منحة رسمية للدراسات العليا إذا كان من غير السعوديين.
- أن يكون المتقدم حاصلًا على الشهادة الجامعية من جامعة سعودية أو من جامعة أخرى معترف بها.
- أن يكون حسن السيرة والسلوك ولائقا طبياً.
- أن يقدم تزكيتين علميتين من أساتذة سبق لهم تدريسه.
- موافقة مرجعه على الدراسة إذا كان موظفاً.
- يجوز للقسم المختص أن يشترط لقبول الطالب في مرحلتي الماجستير أو الدكتوراه، اجتياز عدد من المقررات التكميلية من مرحلة سابقة.
- لا يجوز للطالب أن يلتحق ببرنامجين للدراسات العليا في وقت واحد.

شروط الجامعة العامة

- ألا تقل درجة اختبار القدرات العامة للجامعيين عن 60.
- يقبل المبتعثون من موظفي الجامعة أو الجهات الحكومية وفق شروط ومعايير القبول.
- عدد سنوات مرحلة البكالوريوس للمتقدم لا تقل عن أربع سنوات.
- أن يكون الطالب قد حصل على الشهادة الجامعية الأولى عن طريق الدراسة بالانتظام.
- المعدل يكون وفق شروط القبول باللائحة الموحدة للدراسات العليا بالجامعات السعودية وقواعدها التنفيذية بجامعة الأمير سطام بن عبد العزيز.
- معادلة الشهادة الصادرة من خارج المملكة العربية السعودية.
- من يتم ترشيحه للقبول لا يحق له تأجيل قبوله.

الشروط الخاصة بالبرنامج

- أن يكون المتقدم حاصلاً على درجة البكالوريوس من جامعة معترف بها، في تخصص هندسة الحاسب أو التخصصات ذات الصلة مثل :الهندسة الكهربائية، علوم الحاسب، نظم المعلومات، هندسة البرمجيات، وتقنية المعلومات.
- حصول المتقدم على درجة (5) في اختبار IELTS أو ما يعادله.
- اجتياز الاختبار التحريري الذي يعده القسم.
- اجتياز المقابلة الشخصية التي يعقدها القسم.

5- نظام الدراسة للبرنامج

5- Study system for the program

- تسير الدراسة في البرنامج على نظام المستويات (الفصول)، ويتم جدولة المحاضرات حضورياً خلال الفترات المسائية (3-10م) من أيام الأسبوع الرسمية وذلك وفقاً للتقويم الموحد للجامعة.
- تنقسم السنة الدراسية إلى فصلين رئيسين لا تقل مدة كل منهما عن خمسة عشر أسبوعاً ولا تدخل ضمنهما فترتا التسجيل والاختبارات، وفصل دراسي صيفي لا تقل مدته عن ثمانية أسابيع تضاعف خلالها المدة المخصصة لكل مقرر (المادة الخامسة والثلاثون من لائحة الدراسات العليا).
- يقوم القسم بإسناد تدريس مقررات البرنامج إلى أعضاء وعضوات هيئة التدريس من جميع أقسام الكلية وذلك وفقاً للتخصص الدقيق والخبرة في المجال (المادة السابعة من لائحة الدراسات العليا).
- المدة المقررة للحصول على درجة الماجستير لا تقل عن أربعة فصول دراسية ولا تزيد عن ثمانية فصول دراسية، ولا تحسب الفصول الصيفية ضمن هذه المدة (المادة السادسة والثلاثون من لائحة الدراسات العليا).
- لا يتخرج الطالب إلا بعد إنهاء متطلبات الدرجة العلمية، وبمعدل تراكمي لا يقل عن "جيد جداً" (المادة التاسعة والثلاثون من لائحة الدراسات العليا).
- يحسب التقديرات التقدير العام عند تخرج الطالب، بناءً على معدله التراكمي في المقررات الدراسية فقط (القواعد التنفيذية للمادة التاسعة والثلاثون من لائحة الدراسات العليا).

6- نظام الاختبارات للبرنامج

6- Exam system for the program

- يتم اعداد مسودة الاختبار النهائي للمقرر بالتنسيق بين الأساتذة المشاركين في تدريس المقرر.
- تتم مراجعة مسودة الاختبار النهائي للمقرر بواسطة أحد الزملاء من غير المشاركين في تدريس المقرر (Exam Evaluation Report).
- يتم عرض جميع الاختبارات النهائية للمقررات وفقاً لجدول يضعه منسق البرنامج بموافقة القسم.
- بعد رصد الدرجات النهائية للمقرر تتم مناقشة النتيجة واعتمادها بواسطة القسم والكلية (استمارة مناقشة نتائج مقرر Course Results Discussion Form).
- بعد اعتماد النتيجة النهائية يشرع أستاذ المقرر في اعداد ملف المقرر والذي يتضمن توصيف المقرر (المعد مسبقاً عند بداية الفصل)، وتقرير المقرر ومرفقاته من الاستبيانات وأدوات التحليل (نماذج التطوير والجودة للمقرر).
- يتم إجراء الاختبارات في مقررات الدراسات العليا لنيل درجة الماجستير ورصد التقديرات، وفقاً للائحة الدراسة والاختبارات للمرحلة الجامعية الصادرة من مجلس التعليم العالي في جلسته الثانية المعقودة بتاريخ **1416/6/11** هـ. فيما عدا ما يأتي:

- لا يعتبر الطالب ناجحاً في المقرر إلا إذا حصل فيه على تقدير "جيد" على الأقل (المادة الأربعين من لائحة الدراسات العليا).
- يحدد مجلس القسم درجة الأعمال الفصلية لطلاب الدراسات العليا، بما لا يقل عن **30%** ولا يزيد على **60%** من الدرجة النهائية للمقرر، مع مراعاة ما ورد في المادة "**26**" من لائحة الدراسة والاختبارات للمرحلة الجامعية (القواعد التنفيذية للمادة الأربعين من لائحة الدراسات العليا).
- يجوز للطالب إعادة دراسة أي مقرر رسب فيه مرة واحدة فقط وتدخل النتيجتان في المعدل التراكمي (القواعد التنفيذية للمادة الأربعين من لائحة الدراسات العليا).

7- الخطة الدراسية للبرنامج
7- Study plan of the program

المستوى الأول–First Level

الرمز/الرقم	Code/No	اسم المقرر	Course Name	المتطلب السابق	الوحدات الدراسية (Credits)		
					نظري (The)	عملي (Lab)	معتمدة (CH)
هال 600	CE600	الأمن السيبراني المتقدم	Advanced Cyber Security		3	0	3
عال 651	CS651	أمن نظم التشغيل	Operating Systems Security		3	0	3
هال 603	CE603	أمن الحواسب والشبكات المتقدم	Advanced Computer and Networks Security		3	0	3
المجموع					9	0	9

المستوى الثاني–Second Level

الرمز/الرقم	Code/No	اسم المقرر	Course Name	المتطلب السابق	الوحدات الدراسية (Credits)		
					نظري (The)	عملي (Lab)	معتمدة (CH)
هال 602	CE602	أمن الأنظمة اللاسلكية والجوالة	Wireless and Mobile Security		3	0	3
		اختياري 1	Elective 1				3
		اختياري 2	Elective 2				3
المجموع							9

المستوى الثالث–Third Level

الرمز/الرقم	Code/No	اسم المقرر	Course Name	المتطلب السابق	الوحدات الدراسية (Credits)		
					نظري (The)	عملي (Lab)	معتمدة (CH)
		اختياري 3	Elective 3				3
		اختياري 4	Elective 4				3
عال 617	CS617	مناهج وأخلاقيات البحث العلمي	Research Ethics and Methods		3	0	3
المجموع							9

Forth Level–المستوى الرابع						
الرمز/الرقم	Code/No	اسم المقرر	Course Name	المتطلب السابق	الوحدات الدراسية (Credits)	
					نظري (The)	عملي (Lab)	معتمدة (CH)
		اختياري 5	Elective 5				3
عال 616	CS616	مشروع بحثي	Research Project	عال 617			4
المجموع							7

Elective Courses – المقررات الاختيارية							
الرمز/الرقم	Code/ No	اسم المقرر	Course Name	المتطلب السابق	الوحدات الدراسية (Credits)		
					نظري (The)	عملي (Lab)	معتمدة (CH)
عال 655	CS655	التحليل الجنائي الحاسوبي	Computer Forensics	هال 600	3	0	3
هال 606	CE606	أمن الحوسبة السحابية	Cloud Computing Security	هال 603	3	0	3
هال 607	CE607	أمن إنترنت الأشياء	IoT Security	هال 603	3	0	3
هال 608	CE608	أمن الأجهزة	Hardware Security	هال 600	3	0	3
هال 609	CE609	موضوعات مختارة في الأمن السيبراني 1	Selected Topics in Cyber Security 1	موافقة المنسق	3	0	3
هال 610	CE610	موضوعات مختارة في الأمن السيبراني 2	Selected Topics in Cyber Security 2	موافقة المنسق	3	0	3
هال 611	CE611	أمن الشبكات وحماية المحيط	Network Security and Perimeter Protection	هال 603	3	0	3
هال 612	CE612	الهندسة العكسية للبرمجيات الخبيثة المتقدم	Advanced Malware Reverse Engineering	هال 600	3	0	3
هال 613	CE613	معالجات التشفير	Cryptographic Processors	هال 600	3	0	3
عال 656	CS656	القرصنة الأخلاقية المتقدمة والتدابير المضادة	Advanced Ethical Hacking and Countermeasures	هال 600	3	0	3
هال 615	CE615	الأمن السيبراني بكتلة البيانات المتسلسلة	Cybersecurity with Blockchains	هال 600	3	0	3

8– توصيف مقررات البرنامج
8– Program course descriptions

Course Code	Course Title	Credits	Prerequisite
CE600	Advanced Cyber Security	3	

Course Description

- **Objectives**:

Upon completion of the course, a student will be able to:

1. Evaluate and assess cyber security needs of an organization.
2. Measure the performance of security systems.
3. Formulate, update and communicate cyber security strategies and policies.

- **Content**:

This course reviews the comprehensive coverage of various aspects of cyber security concepts, Introduction to Information Systems, Information Security, Application Security, Security Threats, Development of secure Information System, Security Issues In Hardware, Security Policies, and Information Security Standards.

- **Assessment Methods**

1. Assignments, Reviews of Research Papers, Reports, …
2. Midterm Exam
3. Final Exam.

Course Code	Course Title	Credits	Prerequisite
CS651	Operating Systems Security	3	

Course Description

- **Objectives**:

Upon completion of the course, a student will be able to:

1. Demonstrate understanding of mechanisms and policies in investigating and defending against operating system attacks.
2. Implement basic operating system security techniques.
3. Evaluate tools and technologies for use in protecting the operating systems.

- **Content**:

This course covers both fundamentals and advanced topics in operating system (OS) security. It includes OS level mechanisms and policies in investigating and defending against real-world attacks on computer systems, such as self-propagating worms, stealthy rootkits and large-scale botnets. It discusses basic OS security techniques such as authentication, system call monitoring, and memory protection. It introduces recent advanced techniques such as system-level randomization, hardware/software virtualization, and other hardware features.

- **Assessment Methods**

1. Quizzes.
2. Homeworks.
3. Midterm and Final Exams.

Course Code	Course Title	Credits	Prerequisite
CE602	Wireless and Mobile Security	3	

Course Description

- **Objectives**:

Upon completion of the course, a student will be able to:

1. Acquire solid knowledge on security principles incorporated in the design of mobile network generations.
2. Explain security models for various mobile device platforms.
3. Illustrate security standards for mobile services and wireless systems.

- **Content**:

This course provides a conceptual overview of the security principles incorporated in the design of several generations of mobile networks, from 2G to 5G. It explores platform security models of the popular mobile device platforms such as iphone operating system (IOS), Android and the Windows Phone. It covers the security of mobile services, such as voice over IP (VoIP), text messaging, Wireless Application Protocol (WAP) and mobile Hyper Text Markup Language (HTML). It also introduces security standards in current wireless systems: WiFi security (Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA-Enterprise).

- **Assessment Methods**

1. Quizzes.
2. Homeworks.
3. Midterm and Final Exams.

Course Code	Course Title	Credits	Prerequisite
CE603	Advanced Computer and Networks Security	3	

Course Description

- **Objectives**:

Upon completion of the course, a student will be able to:

1. Recognize number theory, steganography, symmetric and asymmetric encryption algorithms.
2. Apply hash functions, message authentication codes, digital signatures, key management and user authentication.
3. Appraise techniques and algorithms for Internetworking security.

- **Content**:

In this course, students are introduced to the network security requirements, number theory, steganography, encryption design principles and algorithms, message authentication and digital signature principles and designs, and network system security design.

- **Assessment Methods**

1. Quizzes.
2. Homeworks.
3. Midterm and Final Exams.

Course Code	Course Title	Credits	Prerequisite
CS617	Research Ethics and Methods	3	

Course Description

- **Objectives**:

Upon completion of the course, a student will be able to:

1. Analyze and critically evaluate published articles relevant to their research work.
2. Demonstrate the ability to choose methods appropriate to research aims and objectives.
3. Critique quantitative and/or qualitative research methodologies relevant to their research work.
4. Recognize and identify the ethical principles of research work.

- **Content**:

This course provides graduate students knowledge and research skills through critical exploration of research language, ethics, and approaches. The course introduces the language of research, ethical principles and challenges, and the elements of the research process. Graduate students will use these theoretical underpinnings to begin to critically review literature relevant to their field or and determine how research findings are useful in forming their understanding of their work. The student must present a seminar in one of the currents researches or projects in the area.

- **Assessment Methods**

1. Assignments, Reviews of Research Papers, Reports, …
2. Midterm Exam. 3. Final Exam.

Course Code	Course Title	Credits	Prerequisite
CS655	Computer Forensics	3	CE600

Course Description

- **Objectives**:

Upon completion of the course, a student will be able to:

1. Create a method for gathering, assessing and applying new and existing legislation and industry trends specific to the practice of digital forensics.
2. Adhere to the ethical standards of the profession and apply those standards to all aspects of the study and practice of digital forensics.
3. Evaluate the effectiveness of available digital forensics tools and use them in a way that optimizes the efficiency and quality of digital forensics investigations.

- **Content**:

Computer forensics is concerned with the post-analysis of computer systems that have already been compromised. Forensic tools and techniques combine information accumulated from various systems to reconstruct the behaviors and actions of cyber criminals. Computer forensics focuses on the reconstruction of events that have led to system corruption, with the goals of recovering critical data, aiding authorities in tracking those who may have caused the security breach, and learning techniques used by hackers to improve the protection of systems and prevent similar breaches in the future.

- **Assessment Methods**

1. Assignments, Reviews of Research Papers, Reports, …
2. Midterm Exam. 3. Final Exam.

Course Code	Course Title	Credits	Prerequisite
CE606	Cloud Computing Security	3	CE603

Course Description

- **Objectives**:

Upon completion of the course, a student will be able to:

1. Recognize the security concepts pertaining to cloud computing.
2. Acquire solid knowledge on the design principles of secure cloud computing.
3. Summarize the privacy aspects that should be considered in the cloud.

- **Content**:

This course reviews the current state of data security and storage in the cloud, including confidentiality, integrity, and availability. The topics should include: the identity and access management (IAM) practice for authentication, authorization, and auditing of the users accessing cloud services; security management frameworks and standards that are relevant to the cloud; privacy aspects that should be considered in the cloud; importance of audit and compliance functions within the cloud.

- **Assessment Methods**

1. Quizzes
2. Assignments
3. Reports
4. Midterm and Final Exam

Course Code	Course Title	Credits	Prerequisite
CE607	IoT security	3	CE603

Course Description

- **Objectives**:

Upon completion of the course, a student will be able to:

1. Recognize the security architecture of IoT and its security countermeasures.
2. Compare between the threats in IoT and traditional ad hoc networks.
3. Illustrate the security challenges and solutions in IoT.

- **Content**:

This course deals with ensuring the safety of devices and networks interconnected under the fabric of the Internet of Things (IoT). It covers device/physical security, network security, data security, operating system security, and server security**.** It introduces recent advanced topics such as IoT authentication, single-server authentication, multi-server authentication schemes, attacks and remedies, and analytical matrices and tools.

- **Assessment Methods**

1. Quizzes
2. Assignments
3. Reports
4. Midterm and Final Exam

Course Code	Course Title	Credits	Prerequisite
CE608	Hardware Security	**3**	**CE600**

Course Description

- **Objectives**:

Upon completion of the course, a student will be able to:

1. Recognize the vulnerabilities in the current digital systems design flow.
2. Differentiate the different types of physical attacks on digital systems.
3. Illustrate the security challenges and solutions in the electronic hardware.

- **Content**:

This course gives students a comprehensive understanding of hardware security starting from fundamentals to practical applications. Students should understand the vulnerabilities in the current digital systems design flow and the physical attacks to these systems. The topics should include: fundamentals of physical attacks, countermeasures against physical attacks, Side channel attacks (cache attacks, power analysis attacks, timing attacks, scan chain attacks) and countermeasures, Hardware Trojan and trusted integrated circuit (IC) design, Trust platform module (TPM), physical unclonable function (PUF).

- **Assessment Methods**

1. Quizzes
2. Assignments
3. Reports
4. Midterm and Final Exam

Course Code	Course Title	Credits	Prerequisite
CE609	Selected Topics in Cyber Security 1	**3**	Coordinator approval

Course Description

- **Objectives**:

Upon completion of the course, a student will be able to:

1. Learn about the state of the art topics that arise in the cyber security field.
2. Classify and describe vulnerabilities and protection mechanisms of popular network protocols, web protocols, software and hardware systems.
3. Analyze / reason about basic protection mechanisms for modern OSs, software and hardware systems.

- **Content**:

In this course, a topic or a set of topics that will be determined and approved by the department to reflect the most recent issues in the field of cyber security that might appear after approval of the study plan.

- **Assessment Methods**

1. Quizzes
4. Assignments
5. Reports
4. Midterm and Final Exam

Course Code	Course Title	Credits	Prerequisite
CE610	Selected Topics in Cyber Security 2	**3**	Coordinator approval

Course Description

- **Objectives**:

Upon completion of the course, a student will be able to:

1. Learn about the state of the art topics that arise in the cyber security field.
2. Classify and describe vulnerabilities and protection mechanisms of popular network protocols, web protocols, software and hardware systems.
3. Analyze / reason about basic protection mechanisms for modern OSs, software and hardware systems.

- **Content**:

In this course, a topic or a set of topics that will be determined and approved by the department to reflect the most recent issues in the field of cyber security that might appear after approval of the study plan.

- **Assessment Methods**

1. Quizzes
2. Assignments
3. Reports
4. Midterm and Final Exam

Course Code	Course Title	Credits	Prerequisite
CE611	Network Security and Perimeter Protection	**3**	**CE603**

Course Description

- **Objectives**:

Upon completion of the course, a student will be able to:

1. Acquire knowledge about the design of secure networks
2. Acquire knowledge about the different security techniques
3. Critically analyze a network configuration (using tools as appropriate) in order to identify its security issues.
4. Formulate recommendations for stakeholders at various levels within an organization, to harden network infrastructure to achieve a desired security situation.

- **Content**:

In this course, students are introduced to the design of secure computer networks. Exploitation of weaknesses in the design of network infrastructure and security flaws in network protocols are presented and discussed. Network operation systems and network architectures are reviewed, together with the respective security related issues. Issues related to the security of content and applications such as emails, DNS, web servers are also addressed. Security techniques including intrusion detection, forensics, cryptography, authentication and access control are analyzed. Security issues in IPSEC, SSL/ TLS and the SSH protocol are presented.

- **Assessment Methods**

1. Quizzes. 2. Assignments. 3. Reports. 4. Midterm and Final Exams.

Course Code	Course Title	Credits	Prerequisite
CE612	Advanced Malware Reverse Engineering	3	CE600

Course Description

- **Objectives**:

Upon completion of the course, a student will be able to:

1. Applying malware analysis methodology and technology
2. Identify known anti-reverse engineering techniques and some advanced malware functionality.
3. Discuss professional problems, analysis and conclusions in the field of malware analysis, both with professionals and with general audience.

- **Content**:

This course exposes the student to various techniques and procedures employed in the practice of software analysis to detect and remove affected code. The areas explored will consist of trends in malicious code growth, common attack vectors, surface analysis of malware, run-time analysis of malware, system monitoring, debuggers, static reverse engineering of malware, and disassemblers to identify obfuscation techniques and Anti-reversing methods.

- **Assessment Methods**

1. Assignments, Reviews of Research Papers, Reports, …
2. Midterm Exam. 3. Final Exam.

Course Code	Course Title	Credits	Prerequisite
CS656	Advanced Ethical Hacking and Countermeasures	3	CE600

Course Description

- **Objectives**:

Upon completion of the course, a student will be able to:

1. Discuss anatomy of computer attacks and countermeasures to protect valuable data.
2. Explore advanced techniques and attacks to which all modern-day complex applications may be vulnerable.
3. Focus on how to use countermeasures tools and techniques.

- **Content**:

In this course we introduce the students to the latest hacking tools and techniques to understand the anatomy of computer attacks and countermeasures to protect valuable data. Understanding different attack vectors using hand-on techniques and tools that a hacker utilizes to attack computing devices in order to steal valuable and private information.

- **Assessment Methods**

1. Assignments, Reviews of Research Papers, Reports, …
2. Midterm Exam
3. Final Exam.

Course Code	Course Title	Credits	Prerequisite
CE613	Cryptographic Processors	3	CE600

Course Description

- **Objectives**:

Upon completion of the course, a student will be able to:

1. Acquire the necessary skills to implement cryptographic primitives on reconfigurable hardware.
2. Use the proper software tools and hardware kits to develop cryptographic hardware accelerators.
3. Compare between the different implementations of cryptographic primitives using the different design metrics.

- **Content**:

The objective of this course is to build knowledge and skills necessary for efficient implementations of cryptographic primitives on reconfigurable hardware. The implementation platform will be a field programmable gate array (FPGA) containing a general-purpose processor and additional reconfigurable fabric for implementations of custom hardware accelerators. Team projects require design of selected cryptographic primitives followed by comparison and contrast of various implementation alternatives, such as software, custom FPGA hardware, and hybrid hardware-software co-design. Topics may include binary finite field arithmetic, block ciphers, hash functions, counter mode of operation for block ciphers, public key cryptosystems, hardware/software co-design methodologies with FPGAs, software development and profiling, high level synthesis, on- chip buses, hardware/software interfaces, custom hardware accelerators and side channel attacks.

- **Assessment Methods**

1. Quizzes.
2. Assignments.
3. Reports.
4. Midterm and Final Exams.

Course Code	Course Title	Credits	Prerequisite
CE616	Research Project	4	CS617

Course Description

- **Objectives**:

Upon completion of the course, a student will be able to:

1. Demonstrate that has acquired specialization and skills in a particular part of the cyber security field.
2. Formulate a moderate sized problem and select and justify an approach to solve the problem within certain constraints.
3. Be able to watch ethical principles throughout the work.
4. Prepare a written report on the work done
5. Make an oral presentation that should accurately summarize the work done.

- **Content**:

In this course, the student will use the skills and knowledge gained during his studies to demonstrate the ability to design an information security project from the design stage to the implementation and testing stage. This is done under the supervision of a faculty member in the department.

- **Assessment Methods**

1. Project presentation and discussion in front of a committee.
2. Evaluation of the project report.

Course Code	Course Title	Credits	Prerequisite
CE615	Cybersecurity with Blockchains	3	CE600

Course Description

- **Objectives**:

Upon completion of the course, a student will be able to:

1. Describe how blockchains work and the underlying technology of transactions and blocks.
2. Demonstrate the deployment of blockchains in the public domain and how to maintain transparency, privacy and security without any central controlling or trusted agency.
3. Explore platforms to build applications on blockchain technology with challenges and future of cybersecurity.

- **Content**:

In this course, students are introduced to the common cyber threat landscape and common attacks such as malware, phishing, insider threats, and distributed denial-of-service (DDoS). Understand the workings of Blockchain technology, Ethereum and Hyperledger architecture and how they fit into the cybersecurity ecosystem. Write distributed application on Ethereum Blockchain and the Hyperledger Fabric framework. Security triad and its adaptation with Blockchain. Core concepts of cybersecurity, such as DDoS protection, public key infrastructure (PKI)-based identity, two- factor authentication (2FA), and Domain Name System (DNS) security. Role of Blockchain in transforming cybersecurity solutions. Real-world deployment examples of Blockchain in security cases. Short-term challenges and future of cybersecurity with Blockchain.

- **Assessment Methods**

1. Quizzes. 2. Homeworks. 3. Group projects. 4. Midterm and Final Exams.

Kingdom of Saudi Arabia
Ministry of Education
Prince Sattam Bin Abdulaziz University
College of Computer Engineering & Sciences

Exam Evaluation Report

An electronic copy, **Or**, a signed hard copy of this report should be sent to the Course Coordinator to carry out appropriate changes. The Course Coordinator should also keep a copy of this report in the course file

Section A: General Information			
Program Name		***Year/Semester***	
Course Code		***Course Title***	
Exam Date		***Number of Students***	
Course Coordinator		***Instructor Name(s)***	
Reviewer Name			

Section B: Evaluation of Exam

Note that: 4= Excellent*, 3=Good, 2=Needs Improvement, 1= Deficient*

Criteria	Score	Comments
1. The questions are of adequate standard and are designed well to check the course learning outcomes (CLOs) appropriately		
2. There is a diversity in the exam questions (objective - essay)		
3. The Exam evaluates different levels of Lower thinking skills - Memorization, Comprehension and Application skills		
4. The Exam evaluates different levels of Higher thinking skills - Analysis, Synthesis and Evaluation skills		
5. Questions cover most of course topics		
6. Questions are clear and adequate for students level		
7. Questions are free of spelling or grammatical errors		
8. Marks are distributed fairly on questions		
9. Questions are adequate for exam time		
10. Answer of questions are clear and not overlapping with other answers		

Section C: Comments

Any other comments

Please ensure that you sign and date below, if sending a hard copy of this report

Signed		Date	

استمارة مناقشة نتائج مقرر
Course Results Discussion Form

1. Course Information

Course Code-Title	
Semester-Year	
Section Number	
Indicate Other Sections (If any)	
Instructor Name	

2. Result Summary

Status of Students	Number of Students	Status of Students	Number of Students
Enrolled		Examined	
Passed		Failed	
Withdrawal		Deprived	

3. Distribution of Grades

Grade	Passed		A+	A	B+	B	C+	C	D+	D	F
	No	Ratio									
Number											

4. Chart of Grades

5. Records of student results (from e-gate)

6. Committee Comments on the Results

1. ……

2. ……

3. ……

Committee Chairman

Name: ……..……..…… **Signature:** ……..……..…… **Date**: ……..…

7. Instructor Feedback on the Comments

1. ……

2. ……

3. ……

Signature: ……..…..……..**Date**: ……..……

8. Department Council Recommendations

1. ……..

2. ……

3. ……..…

Department Chairman

Name: ……..……..**Signature**: ……..**Date**: …….

9. College Council Approval

College Dean

Name: ……..……..**Signature**: ……..**Date**: …….

11- لوائح وأدلة ذات الصلة بالبرنامج

11- Program related regulations and guides

اللائحة أو الدليل	الرابط
خطة وتوصيف ماجستير الهندسة في الأمن السيبراني	https://dps.psau.edu.sa/sitesuploads/dps/page/2020-12/0_خطة%20وتوصيف%20ماجستير%20الهندسة%20في%20%20الامن%20السيبراني.pdf
دليل برامج الماجستير للعام الجامعي 1442هـ	https://dps.psau.edu.sa/sitesuploads/dps/prints2021-02/دليل%20برامج%20الدراسات%20العليا%20للعام%20الجامعي%201442هـ.pdf
اللائحة الموحدة للدراسات العليا في الجامعات السعودية وقواعدها التنفيذية بجامعة الأمير سطام بن عبد العزيز 1439-1440هـ	https://dps.psau.edu.sa/sitesuploads/dps/prints2021-02/لائحة%20الدراسات%20العليا%20وقواعدها%20بجامعة%20سلمان.pdf
لائحة الدراسة والاختبارات للمرحلة الجامعية والقواعد التنفيذية	https://dar.psau.edu.sa/sitesuploads/dar/node/7164/%2020%20الدراسة.compressed.pdf
دليل كتابة البحث العلمي	https://dps.psau.edu.sa/sitesuploads/dps/prints2021-02/دليل%20كتابة%20البحث%20العلمي.pdf

12– استمارات ونماذج الدراسات العليا

12– Postgraduate forms and applications

الاستمارات والنماذج	الرابط ومحتوياته
التطوير والجودة	https://dps.psau.edu.sa/ar/content/2021-12-08 نموذج NCAAA (وصف مقرر) https://etec.gov.sa/en/productsandservices/NCAAA/AccreditationProgrammatic/Pages/graduateprograms.aspx نموذج NCAAA (تقرير مقرر)
الإجراءات الأكاديمية	https://dps.psau.edu.sa/ar/content/2021-03-04-1 شروط القبول لبرامج الدراسات العليا المتاحة للفصل الثاني من العام الجامعي ١٤٤٢ نموذج طلب تحويل إلى جامعة الامير سطام نموذج تمديد دراسة لطلاب الماجستير نموذج تحويل مسار الدراسة– ماجستير نموذج تعهد لطالب دراسات عليا نموذج طلب منح فرصة إضافية لرفع المعدل التراكمي نموذج طلب منح فرصة إضافية – المعدل مذكرة عرض على العمادة لإعادة قيد طالب نموذج حذف استمارة طلب التحاق بالدراسات العليا (للطالبات) استمارة طلب التحاق بالدراسات العليا (للطلاب) نموذج تأجيل قبول معتمد
مناقشة الرسائل ومنح الدرجة	https://dps.psau.edu.sa/ar/content/2021-03-03-1 نموذج مناقشة مشروع بحث لرسالة ماجستير أو أطروحة دكتوراة نموذج تقرير سنوي عن سير الدراسات العليا نموذج تعيين مشرف لطالب ماجستير أو دكتوراة نموذج السماح بالإشراف للأستاذ المساعد تقرير متابعة تقدم الطالب في رسالته للفصل نموذج اعتماد خطة رسالة جامعية نهائي اجراءات التخرج وتسليم الرسالة لطلاب الدراسات العليا بعد التعديل نموذج مناقشة مشروع بحث لرسالة ماجستير أو أطروحة دكتوراة نموذج تشكيل لجنة مناقشة لطلبة الماجستير نموذج (5) صفحة الغلاف نموذج (4) لصفحة الإجازة نموذج (3) إعلان نتيجة مناقشة رسالة الماجستير نموذج (2) تقرير لجنة مناقشة الرسالة نموذج (1) تحديد موعد مناقشة، – قرار إجراء تعديلات الرسالة

13– دليل الاتصال
13- Contact guide

مكتب عميد الكلية			
الاسم	مسمى الوظيفة	الايميل	التحويلة
د. عادل بن باجد بن بصيّص	عميد الكلية	a.binbusayyis@psau.edu.sa	8310
أ. ذياب بن سعد الغامدي	مدير مكتب العميد	t.alghamdi@psau.edu.sa	8300
أ. بندر بن فرحان العنزي	سكرتير مكتب العميد	b.alenezi@psau.edu.sa	8311

وكالة الكلية للدراسات العليا والبحث العلمي			
الاسم	مسمى الوظيفة	الايميل	التحويلة
د. عبدالله بن قنيفذ القحطاني	وكيل الكلية	aq.alqahtani@psau.edu.sa	8382

قسم هندسة الحاسب			
الاسم	مسمى الوظيفة	الايميل	التحويلة
د. سليمان عبدالله عبدالرحمن النذير	رئيس القسم	s.alnatheer@psau.edu.sa	8390
د. عاطف على إبراهيم محمد	منسق البرنامج	aa.mohamed@psau.edu.sa	8349