National University of Engineering (UNI)
School of Cybersecurity
Syllabus 2024-II

1. COURSE

CY231. Component Security (Mandatory)

2. GENERAL INFORMATION

2.1 Course	:	CY231. Component Security
2.2 Semester	:	9^{th} Semester.
2.3 Credits	:	3
2.4 Horas	:	2 HT; 2 HP;
2.5 Duration of the period	:	16 weeks
2.6 Type of course	:	Mandatory
2.7 Learning modality	:	Face to face
2.8 Prerrequisites	:	• CY221. Software Security. (8^{th} Sem) • CY241. Connection Security. (8^{th} Sem)

3. PROFESSORS

Meetings after coordination with the professor

4. INTRODUCTION TO THE COURSE

This course focuses on the security of software and hardware components, addressing their design, procurement, testing, and analysis. Students will learn to identify and mitigate vulnerabilities, strengthen component security, and understand their impact on overall system security.

5. GOALS

- Apply secure design principles for software and hardware components.
- Evaluate and mitigate vulnerabilities in components, including the supply chain.
- Understand the importance of component security testing and its role in developing secure systems.

6. COMPETENCES

2) Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline. (Assessment)

5) Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline. (Usage)

6) Apply security principles and practices to maintain operations in the presence of risks and threats. (Assessment)

7. TOPICS

Unit 1: Diseño de componentes (12 hours)

Competences Expected: 2,6

Topics	Learning Outcomes
• Seguridad del diseño de componentes – Este tema cubre las amenazas a la seguridad de los artefactos de diseño de componentes (por ejemplo, esquemas, listas de red y máscaras), como troyanos de hardware, piratería de propiedad intelectual, ingeniería inversa, manipulación, análisis de canales laterales y falsificación. También introduce técnicas para proteger los componentes del acceso y uso no autorizados. • Principios del diseño de componentes seguros. – Este tema cubre principios tales como establecer una política de seguridad sólida, tratar la seguridad como una parte integral del diseño del sistema, plataformas informáticas confiables, cadena de confianza, reducir el riesgo, seguridad en capas, simplicidad de diseño, minimizar los elementos del sistema en los que se puede confiar y evitar elementos innecesarios. mecanismos de seguridad. • Identificación de componentes – Este tema cubre técnicas como marcas de agua, huellas dactilares, medición, identificaciones cifradas y funciones físicas no clonables para proteger componentes contra el robo de propiedad intelectual y garantizar la autenticidad de los componentes. • Técnicas de ingeniería anti-inversa – Este tema cubre técnicas como la ofuscación y el camuflaje del diseño para dificultar la ingeniería inversa de los diseños e implementaciones de componentes. • Mitigación de ataques de canal lateral – Este tema cubre técnicas para defenderse contra ataques de canal lateral dirigidos principalmente a algoritmos criptográficos. Las técnicas defensivas incluyen reducción de fugas, inyección de ruido, actualizaciones frecuentes de claves, funciones físicas aleatorias y cadenas de escaneo seguras. • Tecnologías antimanipulación – Este tema cubre técnicas para hacer que los componentes sean resistentes a ataques físicos y electrónicos, incluidas técnicas de protección física, sistemas a prueba de manipulaciones y sistemas de respuesta a manipulaciones.	• Explique cómo la seguridad de los componentes de un sistema podría afectar la seguridad del sistema [Usar] • Describir las formas en que la confidencialidad del diseño de un componente puede verse comprometida [Usar] • Describir formas de obtener información sobre la funcionalidad de un componente con información limitada sobre su diseño e implementación [Usar]

Readings : [**Anderson2020**], [**NIST-SP800-160v1**]

Unit 2: Adquisición de componentes (8 hours)	
Competences Expected: 2	
Topics	**Learning Outcomes**
• Riesgos de la cadena de suministro – Amenazas y riesgos de seguridad tanto para el hardware como para el software en la adquisición de componentes. • Seguridad de la cadena de suministro – Describe estrategias como la seguridad física. – fabricación dividida – trazabilidad – inspección y validación de carga – Inspecciones para detectar y prevenir compromisos de seguridad de los componentes durante el proceso de adquisición. • Investigación de proveedores – Este tema incluye estrategias como la acreditación de proveedores para establecer proveedores y transportistas de componentes confiables.	• Enumerar las fases del ciclo de vida de un componente [Usar] • Enumere los artefactos de diseño de componentes que pueden requerir protección [Usar] • Dé ejemplos de varios principios de diseño de componentes seguros y explique cómo cada uno protege la seguridad de los componentes [Usar] • Describir varias técnicas para proteger los elementos de diseño de un circuito integrado [Usar] • Enumere los puntos comunes de vulnerabilidad en la cadena de suministro de un componente [Usar] • Describir los riesgos de seguridad en una cadena de suministro de componentes [Usar] • Describir formas de mitigar los riesgos de la cadena de suministro [Usar]
Readings : [**Knapp2012**]	

Unit 3: Pruebas de componentes (8 hours)	
Competences Expected: 2,6	
Topics	**Learning Outcomes**
• Principios de las pruebas unitarias. – Herramientas y técnicas de prueba a diferencia de las pruebas a nivel de sistema. • Pruebas de seguridad – Herramientas y técnicas como las pruebas fuzz para probar las propiedades de seguridad de un componente más allá de su corrección funcional.	• Enumere los puntos comunes de vulnerabilidad en la cadena de suministro de un componente [Usar] • Describir los riesgos de seguridad en una cadena de suministro de componentes [Usar] • Describir formas de mitigar los riesgos de la cadena de suministro [Usar] • Diferenciar entre pruebas unitarias y de sistemas [Usar] • Enumere varias técnicas para probar las propiedades de seguridad de un componente [Usar]
Readings : [**Dustin2008**]	

Unit 4: Ingeniería inversa de componentes (10 hours)	
Competences Expected: 6	
Topics	**Learning Outcomes**
• Diseño de ingeniería inversa. – Describe herramientas y técnicas para descubrir el diseño de un componente en algún nivel de abstracción. • Ingeniería inversa de hardware – c describe herramientas y técnicas para descubrir la funcionalidad y otras propiedades del hardware de un componente, como las funciones de un circuito integrado. • ingeniería inversa de software – Este tema describe herramientas y técnicas como el análisis estático y dinámico para descubrir la funcionalidad y las propiedades del software de un componente.	• Enumere las razones por las que alguien aplicaría ingeniería inversa a un componente [Usar] • Explicar la diferencia entre análisis estático y dinámico en software de ingeniería inversa [Usar] • Describir una técnica para realizar ingeniería inversa en la funcionalidad de un circuito integrado [Usar]
Readings : [**Dang2014**]	

Unit 5: Diseño de componentes (10 hours)

Competences Expected: 2,6

Topics	Learning Outcomes
• Seguridad del diseño de componentes – Este tema cubre las amenazas a la seguridad de los artefactos de diseño de componentes (por ejemplo, esquemas, listas de red y máscaras), como troyanos de hardware, piratería de propiedad intelectual, ingeniería inversa, manipulación, análisis de canales laterales y falsificación. También introduce técnicas para proteger los componentes del acceso y uso no autorizados. • Principios del diseño de componentes seguros. – Este tema cubre principios tales como establecer una política de seguridad sólida, tratar la seguridad como una parte integral del diseño del sistema, plataformas informáticas confiables, cadena de confianza, reducir el riesgo, seguridad en capas, simplicidad de diseño, minimizar los elementos del sistema en los que se puede confiar y evitar elementos innecesarios. mecanismos de seguridad. • Identificación de componentes – Este tema cubre técnicas como marcas de agua, huellas dactilares, medición, identificaciones cifradas y funciones físicas no clonables para proteger componentes contra el robo de propiedad intelectual y garantizar la autenticidad de los componentes. • Técnicas de ingeniería anti-inversa – Este tema cubre técnicas como la ofuscación y el camuflaje del diseño para dificultar la ingeniería inversa de los diseños e implementaciones de componentes. • Mitigación de ataques de canal lateral – Este tema cubre técnicas para defenderse contra ataques de canal lateral dirigidos principalmente a algoritmos criptográficos. Las técnicas defensivas incluyen reducción de fugas, inyección de ruido, actualizaciones frecuentes de claves, funciones físicas aleatorias y cadenas de escaneo seguras. • Tecnologías antimanipulación – Este tema cubre técnicas para hacer que los componentes sean resistentes a ataques físicos y electrónicos, incluidas técnicas de protección física, sistemas a prueba de manipulaciones y sistemas de respuesta a manipulaciones.	• Explique cómo la seguridad de los componentes de un sistema podría afectar la seguridad del sistema [Usar] • Describir las formas en que la confidencialidad del diseño de un componente puede verse comprometida [Usar] • Describir formas de obtener información sobre la funcionalidad de un componente con información limitada sobre su diseño e implementación [Usar]

Readings : [**Anderson2020**]

8. WORKPLAN

8.1 Methodology

Individual and team participation is encouraged to present their ideas, motivating them with additional points in the different stages of the course evaluation.

8.2 Theory Sessions

The theory sessions are held in master classes with activities including active learning and roleplay to allow students to internalize the concepts.

8.3 Practical Sessions

The practical sessions are held in class where a series of exercises and/or practical concepts are developed through problem solving, problem solving, specific exercises and/or in application contexts.

9. EVALUATION SYSTEM

********* EVALUATION MISSING ********

10. BASIC BIBLIOGRAPHY