2828 – ANONIMATO Y PRIVACIDAD

UASLP
Universidad Autónoma de San Luis Potosí

FACULTAD DE INGENIERÍA
Área de Ciencias de la Computación

Clave de la materia: 2828
Clave Facultad: 2828
Clave U.A.S.L.P.: ---- **Clave CACEI:** IA
Nivel del Plan de Estudios: I.S.I.: 8 **No. de créditos:** 8
Horas/Clase/Semana: 4 **Horas totales/Semestre:** 64
Horas/Práctica (y/o Laboratorio): 0
Prácticas complementarias: 0
Trabajo extra-clase Horas/Semana: 4
Carrera/Tipo de materia: I.S.I./Electiva de Área de Énfasis
No. de créditos aprobados: ---
Fecha última de Revisión Curricular: 28-abril-2022
Materia y clave de la materia requisito: 2825 – Principios de Seguridad Informática

OBJETIVO DEL CURSO

Analizar y aplicar los conceptos fundamentales y técnicas de anonimato, las aplicaciones que protegen la privacidad y los algoritmos utilizados; a través de la configuración de las redes y sistemas operativos para acceder a los servicios de la red oscura de forma segura.

CONTENIDO TEMÁTICO

1. ANONIMATO

Tiempo Estimado: 16 hrs.

Objetivo: Conocer y analizar los conceptos fundamentales y técnicas básicas de anonimato, así como su aplicación con el mundo actual y los aspectos de seguridad en el Big Data.

1.1. Principios de seguridad informática
1.2. Conceptos
1.3. Relación con el Big Data
1.4. Anonimato y pseudoanonimato de datos
1.5. Métodos de privacidad diferencial

2. PRIVACIDAD

Tiempo Estimado: 16 hrs.

Objetivo: Identificar y analizar la importancia de las aplicaciones que protegen la privacidad y qué algoritmos utilizan.

2.1. Historia y evolución
2.2. Privacidad de datos y ética en la información
2.3. Personalización, algoritmos y aprendizaje automático

3. CRIPTOMONEDAS Y BLOCKCHAIN

Tiempo estimado: 16 hrs.

Objetivo: Conocer y analizar la evolución de las criptomonedas, los mecanismos utilizados en blockchain y cómo se vislumbran estos activos en nuestra sociedad.

3.1. Las criptomonedas
3.2. Blockchain
3.3. Privacy preserving computing

4. DARK NET

Tiempo estimado: 18 hrs.

Objetivo: Analizar y configurar las redes y sistemas operativos para acceder a los servicios de la red oscura de forma segura.

4.1. Uso de sistemas operativos especiales
4.2. Aplicaciones y motores de búsqueda
4.3. Servicios (Onion services)

METODOLOGÍA

Desarrollo del tema por parte del profesor siguiendo el método de aprendizaje basado en problemas. Se espera que el alumno investigue ciertos temas, siguiendo el método de aula invertida. Implementar estrategias de trabajo en equipo cuando sea conveniente (aprendizaje colaborativo). El alumno deberá realizar trabajos prácticos de cada uno de los temas.

EVALUACIÓN

Se realizarán cuatro exámenes parciales de forma colegiada en las fechas establecidas por la Facultad, de acuerdo con el Reglamento de Exámenes. La calificación de los exámenes parciales estará compuesta por la evaluación del examen parcial y por otras actividades, como: tareas, investigaciones, resolución de problemas, ejercicios, etc. La calificación del examen ordinario es el promedio de los cuatro parciales.

BIBLIOGRAFÍA

Bibliografía Básica

Fui, H., *Security and Privacy in Internet of Things: Models, Algorithms, and Implementations*. 1ª Ed., CRC Press, 2016

Ozkaya, E. *Learn Social Engineering: Learn the Art of Human Hacking with an Internationally Renowned Expert*. Packt Publishing, 2018.

McClure, S., Scambray, J., Kurtz, G. *Hacking Exposed 7: Network Security Secrets & Solutions*. Mc Graw Hill, 2012.

Mollin, Richard A. *An introduction to Cryptography*. 2nd ed. Chapman, 2007.

Bibliografía Complementaria

Grime, R. *Hacking the Hacker: Learn From the Experts Who Take Down Hackers*. Wiley, 2017.

Bass, L., Clements, P., Kazman, R. *Software Architecture in Practice*. 2nd Edition, Addison-Wesley, 2003.

Ocariz, Emiliano B. *Blockchain y Smart Contracts: La Revolución de la Confianza*. Alfaomega, 2019.

Privacy friendly alternatives to Google don't track you: *https://nomoregoogle.com/*

Privacy, Blockchain and Onion Routing: *https://medium.com/unitychain/privacy-blockchain-and-onion-routing-d5609c611841*

Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms: *https://www.chaum.com/publications/chaum-mix.pdf*

Cryptography: *https://ieeexplore.ieee.org/document/913211*