Universidad Autónoma de Baja California
Facultad de Ciencias Químicas e Ingeniería

Plan de Ingeniero en Software y Tecnologías Emergentes

Seguridad del Software(371)
Meta 5.1 Aleatoriedad en Software

Docente:
Carlos Francisco Alvarez Salgado

Actividad:
Ensayo del texto

Participante(es):
Luis Eduardo Galindo Amaya (1274895)

Tijuana, 22 may 2024

Sumario

Meta 5.1

Aleatoriedad en Software

Importancia de la Aleatoriedad

La aleatoriedad es esencial en la ciberseguridad porque muchos sistemas y protocolos de seguridad dependen de la generación de números aleatorios para funciones críticas como la encriptación y la autenticación. Cada vez que se inicia un dispositivo, se accede a una aplicación segura se generan números aleatorios para asegurar estas operaciones

Aleatoriedad

La generación de verdadera aleatoriedad es compleja. No basta con observar los resultados para evaluar la aleatoriedad. Esta dificultad ha provocado numerosos errores y vulnerabilidades en la implementación.

Tipos de generadores de números aleatorios

Generadores de Números Pseudo-Aleatorios (PRNGs)

Es un tipo de generador que produce números aleatorios de manera determinista. Esto significa que, aunque los resultados puedan parecer aleatorios, son generados por un algoritmo predefinido y, por lo tanto, son en realidad pseudo-aleatorios.

Generadores de Números Pseudo-Aleatorios Criptográficamente Seguros (CSPRNGs)

Es un tipo especial de PRNG diseñado específicamente para cumplir con altos estándares de seguridad. Estos generadores han sido estudiados exhaustivamente y sus características aseguran que los números producidos sean adecuados para usos

criptográficos.

Conclusiones

La generación de números aleatorios es una tarea crítica y difícil en la ciberseguridad. A pesar de los avances, los RNGs siguen siendo un área problemática con importantes implicaciones de seguridad. Por lo que debemos usar generadores que sean criptograficamente seguros.