CHALMERS | UNIVERSITY OF GOTHENBURG

Proyecto de tesis: una librería para proveer un análisis de manchas

Las aplicaciones Web a menudo presentan agujeros de seguridad que permiten a atacantes, or personas maliciosas, obtener información confidencial o acceso no autorizado. La mayoría de estos ataques son a menudo el resultado de la falta de validación en los datos de entrada provisto por los usuarios. Para ayudar a descubrir tales vulnerabilidades, análisis basados en manchas (o *taint analysis* en Ingles) han sido desarrollados para lenguajes populares de programación en la web (Perl, Ruby, PHP, Python). Teniendo en cuenta la entrada del usuario como datos poco fiables o manchados, el análisis de manchas determina cómo estos valores se propagan dentro de las aplicaciones. Si un valor manchado es utilizado en una operación que puede afectar la seguridad del sistema, el análisis levanta una alarma para indicar un posible vulnerabilidad o, alternativamente, que una validación de datos es necesaria. Una vez que un dato manchado es validado, se lo considera limpio, libre de cualquier mancha. Hay funciones especificas designadas para validar datos. Estas funciones garantizan la ausencia de ciertos patrones o datos que puedan producir inseguridades en el sistema.

Análisis basados en manchas se aplica a menudo en tiempo de ejecución mediante un monitor. Para ello, interpretes tiene que ser adaptados no solo para realizar los computos de los programas escritos en el lenguajes, sino también para proveer un análisis basado en manchas. Sin embargo, modificar un intérprete puede ser una tarea importante y dificultosa por si misma. A diferencia de trabajos anteriores, proveer un análisis basado de manchas mediante una librería no ha sido considerado previamente. Contar con una librería que provee un análisis basado en manchas evita cualquier modificación en el interprete e incrementa las chances para que este análisis sea adoptado masivamente.

Alumno: Ing. Juan José Conti

Objetivos: diseñar e implementar una librería que provee un análisis de manchas para Python. Algunas de las abstracción encontradas en el languaje Python hace que este lenguaje sea apropiado para implementar dicha librería de una manera elegante y minimalista.

Plan de acción: Estudiar análisis basados en manchas para los lenguajes Perl, Ruby, Python, y PHP entre otros. Diseñar e implementar la librería para Python. Evaluar el desempeño, ventajas y desventajas de la librería en un caso de estudio.

Dr. Alejandro Russo

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
Chalmers University of Technology | University of Gothenburg
SE-412 96 Gothenburg, Sweden
Phone: +46 31-772 1098
Mobile:+46 705-110896
E-mail: russo@chalmers.se

Chalmers tekniska högskola AB
Reg.No: 556479-5598 VAT No: SE556479559801