Análisis y estudio comparativo de la aleatoriedad en la disposición del espacio de direcciones en Windows 10 y Ubuntu 18.04 LTS

Raquel Vázquez Díaz, Pilar Vila Avendaño, José Manuel Vázquez Naya

Abstract

Los sistemas operativos presentan actualmente técnicas de protección de memoria que dificultan la explotación de las vulnerabilidades existentes. Una de estas técnicas es ASLR (*Address Space Layout Randomization*), cuya función es introducir aleatoriedad en el espacio de direcciones virtuales de un proceso.

El objetivo de este proyecto es medir, analizar y comparar el comportamiento de ASLR en dos sistemas operativos actuales, Windows 10 y Ubuntu 18.04 LTS, en las versiones de 64 bits. Para ello, utilizando la metodología Kanban, se ha realizado una revisión de los artículos científicos publicados hasta la fecha sobre esta temática, y se ha desarrollado una herramienta con la que obtener las direcciones de memoria para las áreas principales de un proceso durante un número suficientemente elevado y representativo de iteraciones.

Una vez concluidas las ejecuciones, se ha realizado un análisis, apoyado en datos, gráficas y tablas, que ha conducido esencialmente al siguiente resultado: la implementación de ASLR ha mejorado notablemente en estos dos sistemas operativos respecto a versiones anteriores, ya que las direcciones cuentan con más bits de entropía y casi todas las áreas de memoria se aleatorizan. Sin embargo, existen aspectos, como las correlaciones parciales o una distribución de frecuencias no siempre uniforme, que todavía son susceptibles de mejora. En Windows el mayor problema reside en el tamaño de su espacio de direcciones, que conlleva que se produzcan correlaciones totales o parciales entre las principales áreas de memoria. En Linux, que presenta un tamaño de direccionamiento mayor, teóricamente sí podría mejorarse la implementación de ASLR evitando por completo las correlaciones, pues existe espacio de direccionamiento suficiente para ello.

Por tanto, se demuestra que ASLR en la actualidad se comporta de manera mucho más eficiente que en sistemas operativos anteriores, pero sigue sin ser, de todas formas, óptimo. Este estudio podría extenderse tanto desde una perspectiva sincrónica, añadiendo nuevos sistemas operativos al análisis y comparación, como diacrónica, analizando y comparando los sistemas estudiados con otras versiones de Windows y Ubuntu anteriores. Asimismo, también se podría profundizar en las causas concretas que limitan la eficiencia de estas implementaciones de ASLR.