# Tema: A novel method of software vulnerability detection based on fuzzing technique.

## Síntesis:

Las vulnerabilidades por desbordamiento de buffer han sido largamente explotadas por piratas informáticos. En este apartado se nos muestra un método para perfeccionar la detección de este tipo de vulnerabilidades.

Actualmente, las técnicas de detección de vulnerabilidades de seguridad del software se pueden dividir en dos categorías:

* Código fuente
* Archivos ejecutables.

No obstante, el software empresarial no ofrece código fuente y el último tipo de detección es más eficaz.

En el artículo se nos muestran varias técnicas como:

* **Fuzzing**. La cual es una técnica de prueba que esta automatizada y ha logrado muchos beneficios en pruebas de seguridad.
* **Auditoria de Código fuente**. Esta técnica consiste en escanear el Código fuente para detectar posibles vulnerabilidades de software, sin embargo, solo se limita a posibles vulnerabilidades de cadenas, comprobación y asignación.
* **Auditoría de código de ensamblaje basada en IDA**. Esta técnica detecta las vulnerabilidades en los archivos ejecutables, infortunadamente tiene una desventaja, se requiere de conocimiento en ingeniería inversa.
* **Comparación de parches binarios**. Esta técnica su función recae en que una vez que se encuentran las vulnerabilidades, los proveedores las reparan mediante parches o actualizaciones de software.
* **Análisis inverso de productos de seguridad**. Consiste en un método para obtener vulnerabilidades de seguridad desconocidas a través del análisis inverso de productos de seguridad.

La técnica fuzzing posee un alto grado de automatización, mientras que otras técnicas se basan demasiado en las experiencias del trabajo humano.

Los fuzzers son herramientas creadas para detectar las vulnerabilidades del software basadas en la técnica de fuzzing y acogen diferentes enfoques de forma selectiva para construir paquetes mal formados. El sistema prototipo solo detecta vulnerabilidades de desbordamiento de búfer, por lo que no genera paquetes para detectar vulnerabilidades de desbordamiento/subdesbordamiento de enteros o vulnerabilidades de cadenas de formato.

Referencia: Zhang, X., Shao L., & Zheng, J., “A novel method of software vulnerability detection based on fuzzing technique”, Faculty of Computer Science and Engineering, UESTC, 2008, pp. 270 – 273.