Introducción a la programación para ingeniería de computadores

Software Seguro

Gustavo Romero López

Updated: 24 de septiembre de 2024

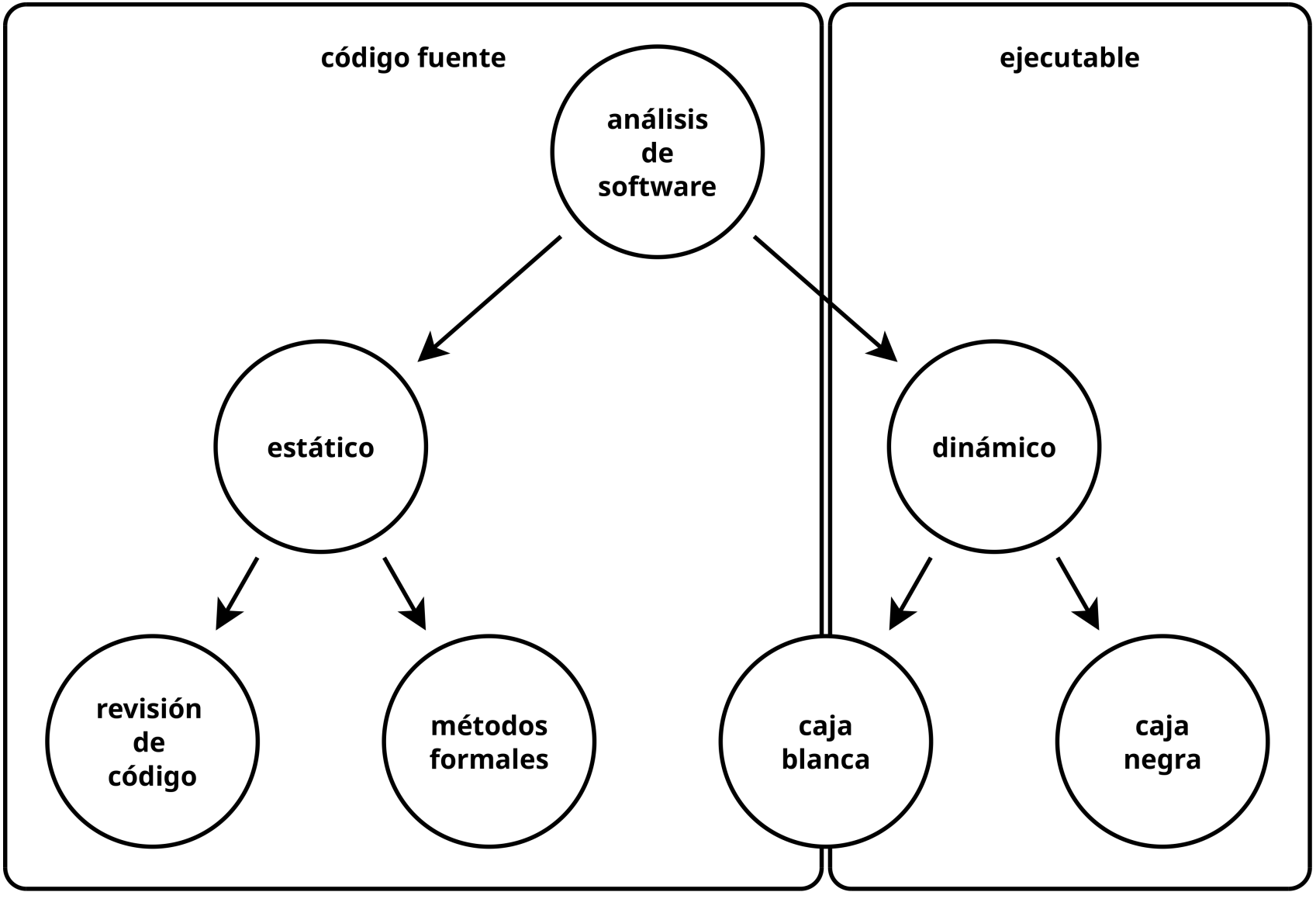
Arquitectura y Tecnología de Computadores

Ejemplo: seguridad de la memoria

Típicos errores de memoria en C/C++

```
char *p = new char[20];
p[20] = ... // fuera del límite
delete[] p;
p[ 0] = ... // memoria liberada
```

Resumen de las técnicas para mejorar la seguridad



Técnicas para mejorar la seguridad

- Análisis de código fuente
  - Detección de patrones vulnerables
  - Verificación formal
- Verificación de código binario
  - Desinfectantes: añadir comprobaciones
  - Fuzzing: proporcionar entradas pseudoaleatorias
  - Etiquetado de memoria, http://llvm.org/devmtg/2018-10/slides/Serebryany-Stepanov-Tsyrklevich-Memory-Tagging-Poster-LLVM-2018.pdf, https://seqred.pl/en/memory-tagging-extension/
  - Técnicas combinadas, ej: desinfectantes + fuzzing

Análisis estático

- `gcc -Wall/-Werror` gnu/llvm
  - es la forma más básica de análisis estático
  - detección de malas prácticas
  - `https://gcc.gnu.org/onlinedocs/gcc/Warning-Options.html`
- `gcc -fanalyzer` gnu
  - analizador de calidad
  - informe en texto plano
  - `https://gcc.gnu.org/onlinedocs/gcc-10.1.0/gcc/Static-Analyzer-Options.html`
- `scan-build` llvm
  - analizador de calidad
  - informe en html
  - `https://clang-analyzer.llvm.org/scan-build.html`

Desinfectantes

- En lugar de intentar evitar los fallos, como hace el análisis estático, instrumentaliza el código binario para intentar detectarlos:
  - `int a[100];`
  - `a[i] --> (i < 100)? echo a[i] : avisar_del_error()`
- Tipos:
  - direcciones: use after free, heap buffer overflow, stack buffer overflow, global buffer overflow, use after return, use after scope, initialization order bugs, memory leaks,...
  - hebras: condiciones de carrera, interbloqueos, circulos viciosos,...
  - memoria: uso de memoria sin inicializar,...

Fuzzing

- Técnica para localizar errores basada en la repetida introducción de datos.
- Funcionan mediante la instrumentación del código binario o el empleo de máquinas virtuales.
- Suele utilizarse en conjunción con desinfectantes para mejorar su efectividad.
- Tipos:
  - programa: America Fuzzy Lop
  - función: LibFuffer
- Ejemplos:
  - `https://int21.de/slides/bornhack2016-fuzzing`
  - `https://int21.de/slides/sha2017-fuzzing`
  - `https://int21.de/slides/troopers2017-fuzzing`