

Evaluación de la capacidad de ejecución de atacantes en sistemas Unix usando Return Oriented Programming

Jaime Alconchel¹, Ricardo J. Rodríguez¹

¹Dpto. de Informática e Ingeniería de Sistemas, Universidad de Zaragoza, Spain

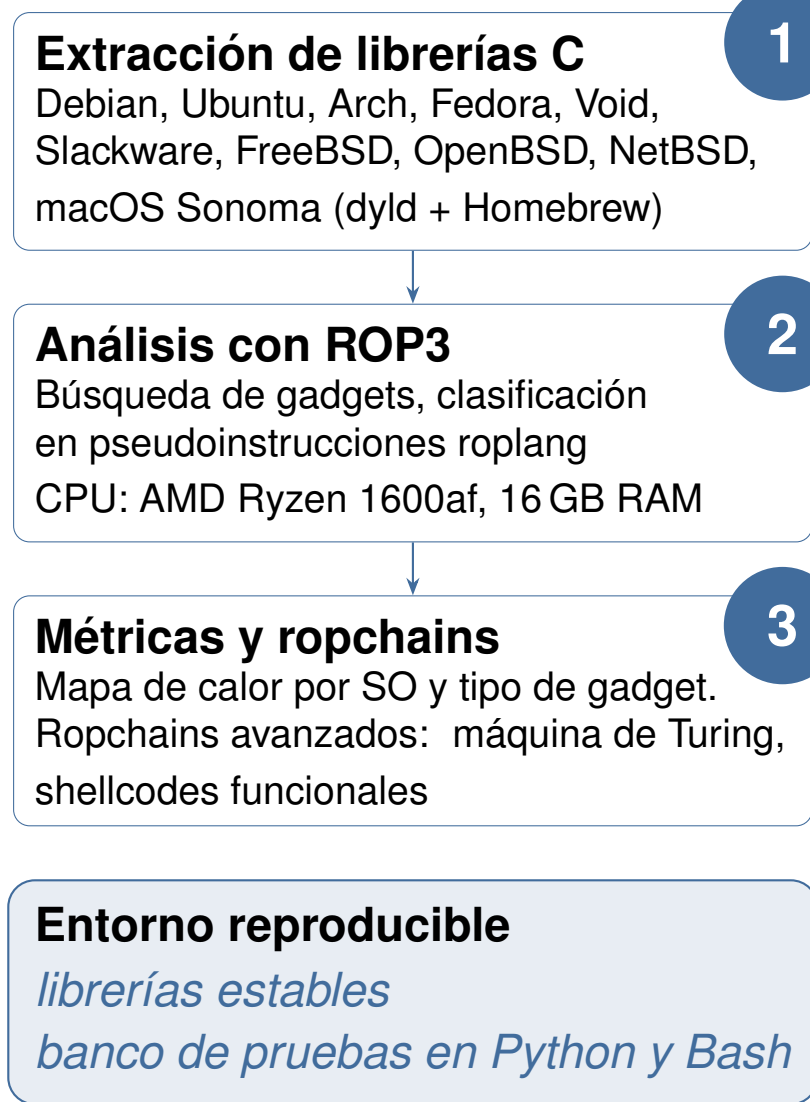
Programación orientada al retorno

- Técnica de reutilización de código que encadena secuencias (*gadgets*) terminadas en `ret` para lograr ejecución arbitraria sin inyectar nuevo código
- Evita protecciones DEP/NX al operar en secciones ejecutables ya presentes en los binarios
- Variante JOP: sustituye `ret` por `jmp` con un dispatcher dedicado
- Contramedidas: ASLR, CFI, ARM Pointer Authentication o Intel CET

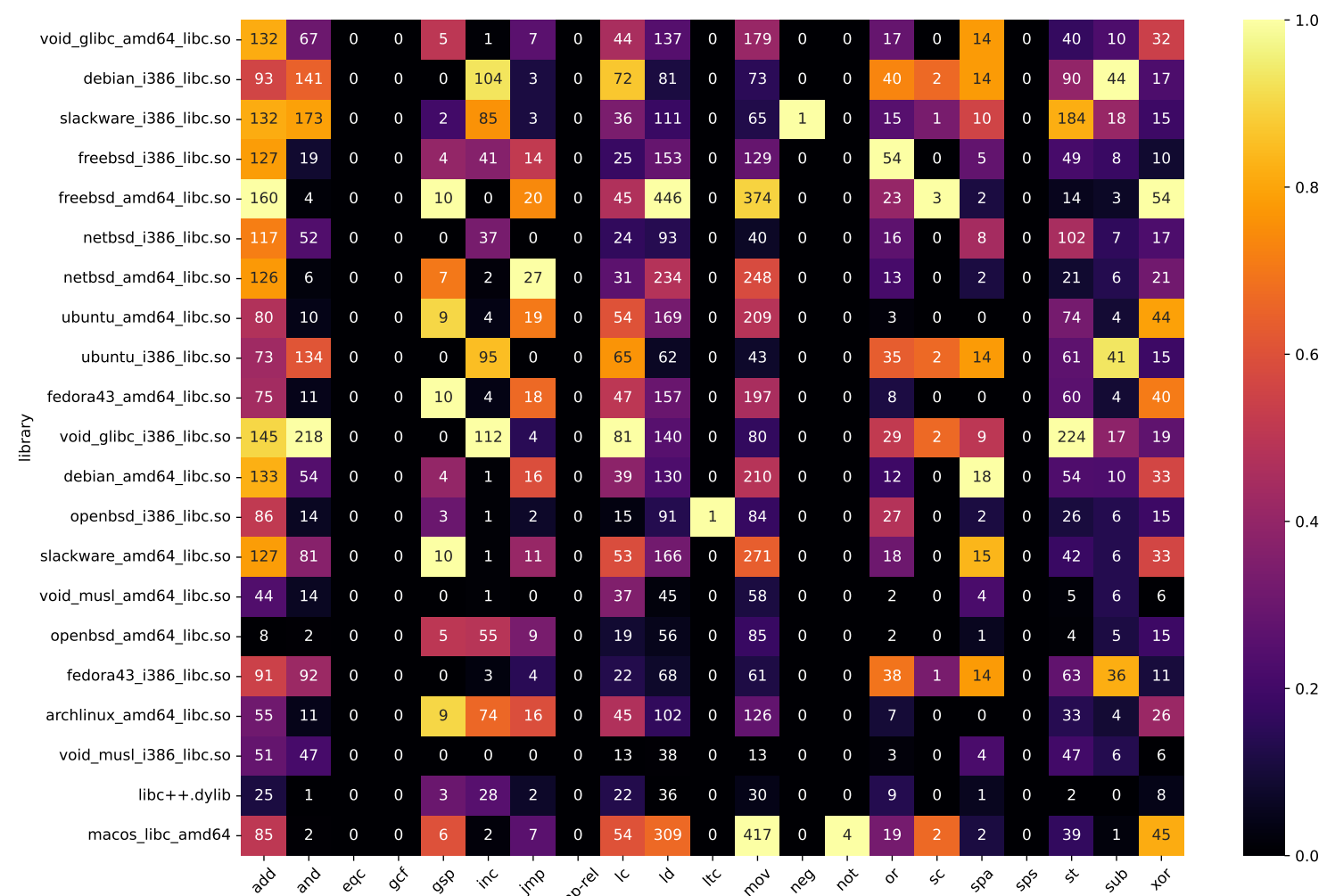
Herramienta ROP3 y lenguaje roplang

- ROP3 detecta y clasifica gadgets ROP/JOP en binarios, agrupándolos en pseudoinstrucciones del lenguaje roplang
- Permite medir el poder de ejecución: ejecución no condicional y condicional desde gadgets del binario
- Trabajo previo sobre Windows 10: ejecución no condicional completa en casi todos los binarios y ejecución condicional en los de mayor tamaño
- Extensión: soporte de formatos `ELF` (Linux/BSD) y `Mach-O` (macOS) y nueva estrategia de salto condicional `jmp`

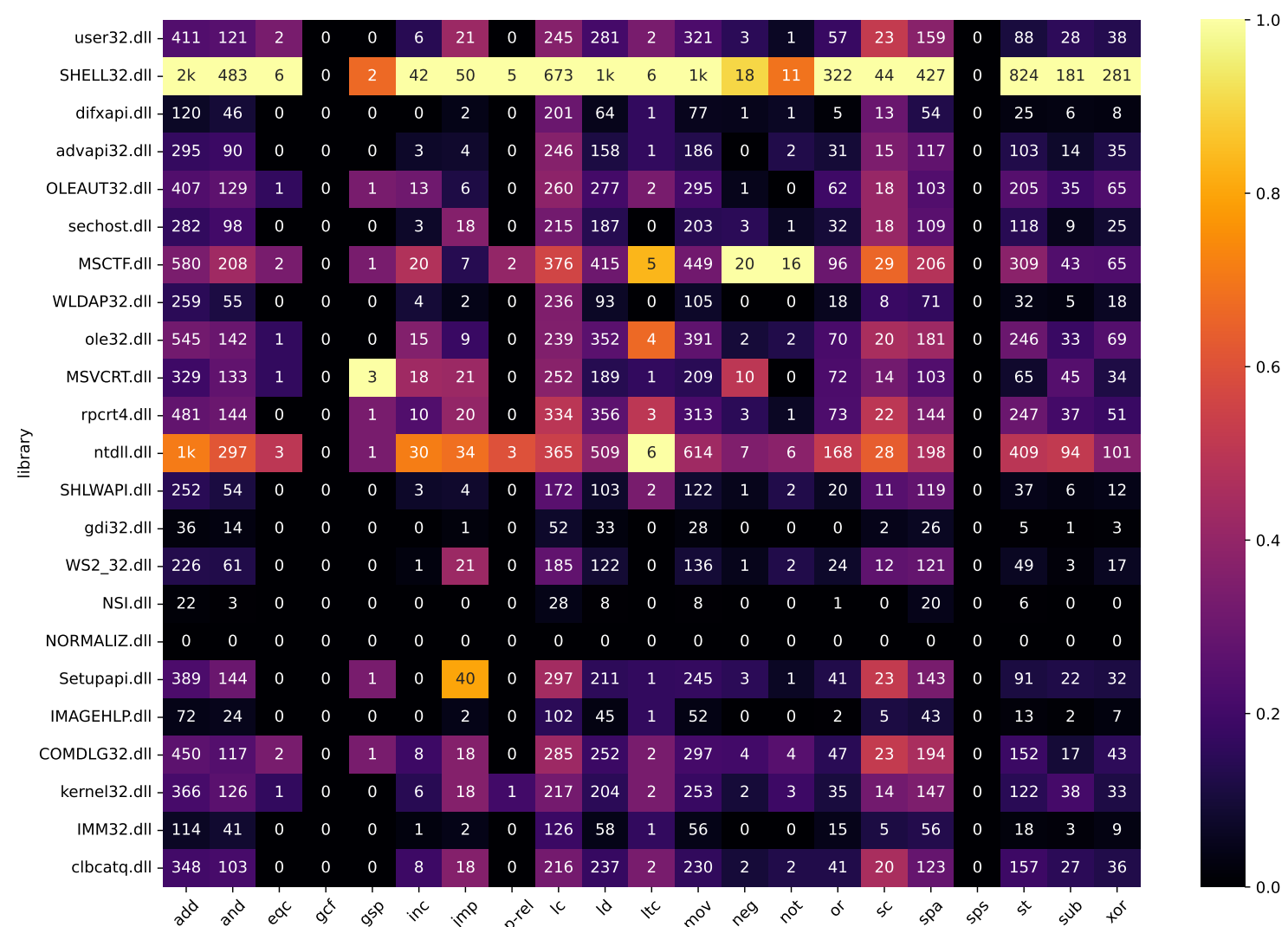
Metodología



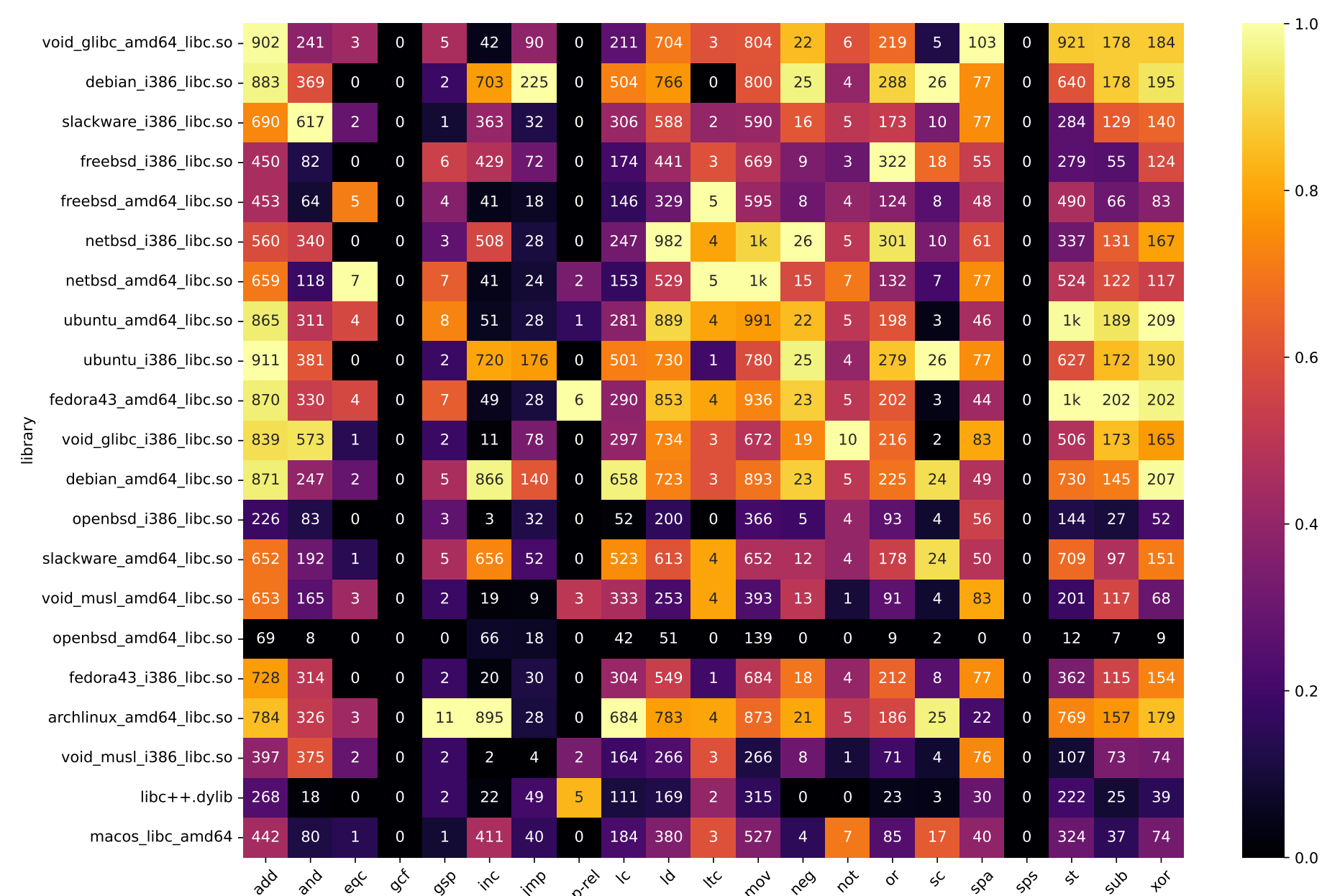
JOP — libc



ROP — Windows 10 x64



ROP — libc



Ropchains en grandes librerías

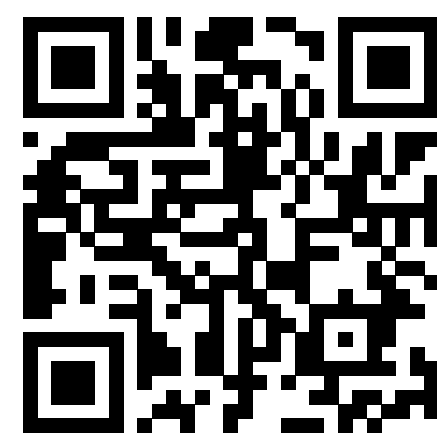
Bibliotecas	ROPchains									
	decoder	decoder	loop	syscall	exec	syscall	exec	relative	turing	
libc (1.83MB)	■	■	■	■	■	■	■	■	■	
libcurl (0.68MB)	■	■	■	■	■	■	■	■	■	
libxul (156.29MB)	■	■	■	■	■	■	■	■	■	
libssl (0.66MB)	■	■	■	■	■	■	■	■	■	
libz (0.12MB)	■	■	■	■	■	■	■	■	■	
libsqlite3 (1.37MB)	■	■	■	■	■	■	■	■	■	
libmergedlo (66.27MB)	■	■	■	■	■	■	■	■	■	
libwebkit2gtk (87.95MB)	■	■	■	■	■	■	■	■	■	
libLLVM-15 (111.87MB)	■	■	■	■	■	■	■	■	■	
libnghttp2 (0.18MB)	■	■	■	■	■	■	■	■	■	

Se extraen varias librerías populares de los repositorios de Debian para 64 bits (Trixie y Bookworm) y se analiza la presencia en ellos de *ropchains* complejos

Conclusiones

- La herramienta ROP3 se extiende con éxito a los formatos `ELF` y `Mach-O`, cubriendo sistemas operativos Unix de forma reproducible
- Las librerías C de Unix ofrecen una cantidad equivalente de operaciones roplang a la encontrada en binarios Windows, confirmando que ROP es un vector válido en todos los sistemas principales
- La nueva estrategia de salto condicional mejora significativamente los resultados del diseño original (`jmp-rel`), con ejecución condicional completa en la mayoría de las librerías
- Se demuestra la Turing completitud de algunas librerías mediante una máquina de Turing funcional construida exclusivamente con gadgets de las librerías analizadas

Código



Agradecimientos

Este trabajo ha sido parcialmente financiado por el Programa de Becas y Ayudas del Instituto de Investigación en Ingeniería de Aragón (I3A) y por la Cátedra Inetum.