Jan Kopański

include/uapi/linux/ptrace.h

Dodane zostały tutaj definicje stałych PTRACE_RUN_SYSCALL oraz struktury ptrace_run_syscall_args. Dodane zostały także definicje stałych PTRACE_SYSCALL_*, które służą do określania jaki syscall został przekazany do wywołania przez ptrace.

include/linux/sched.h

Dodana została definicja struktury ptrace_syscall, która służy do przenoszenia danych pomiędzy procesem procesem śledzącym a śledzonym. Struktura task_struct została rozszerzona o pole struct ptrace_syscall ptrace_syscall.

kernel/ptrace.c

Wewnątrz funkcji ptrace_request, w switchu dodany został nowy case obsługujący PTRACE_RUN_SYSCALL i wywołujący funkcję run_syscall, zdefiniowana w tym samym pliku.

Funkcja run syscall:

1) Kopiuje dane z przestrzeni użytkownika do przestrzeni jądra
2) Sprawdza ich poprawność i zajmuje się ewentualną obsługą błędów
3) Wypełnia pola struktury ptrace_syscall, należącej do procesu śledzącego
4) Budzi proces śledzony
5) Czeka na completion event: child->ptrace_syscall.event
6) Przekazuje wynik syscalla do przestrzenie użytkownika

arch/x86/entry/common.c

Wewnątrz funkcji exit_to_usermode_loop po obsłużeniu wszystkich sygnałów wywoływana jest funkcja ptrace_run_syscall, zdefiniowana w tym samym pliku.

Funkcja ptrace_run_syscall:

1) Wywołuje przez proces śledzony syscall przekazany do ptrace

2) Po wywołaniu syscalla powiadamia o tym proces śledzący, czyli zwalnia blokadę, na której czekał

3) Zatrzymuje ponownie proces śledzony

W przypadku syscalla exit kroki 2 i 3 są pomijane

kernel/exit.c

Na końcu funkcji do_exit dodane zostało zwalnianie blokady, na której czeka proces śledzący.

kernel/fork.c

Wewnątrz funkcji _do_fork, jeżeli proces został utworzony poprzez wysłanie syscalla fork przez ptrace, pomijane jest wywołanie funkcji ptrace_event_pid. Funkcja ptrace_event_pid ma powiadomić proces śledzący o tym, że nowo utworzony proces zaczął działać, co realizuje poprzez blokowanie się i czekanie na akcje ze strony procesu śledzącego. Proces śledzący jednakże w tym samym czasie czeka na zakończenie wywoływania syscalla, co prowadzi do zakleszczenia.