A ETHICAL CONSIDERATIONS

As is common in the computer security landscape, there is an intricate dance between defensive and offensive research. We have shared our results with AMD regarding the power of inference attacks, and have incorporated some of the feedback into the paper. This new class of attacks is a direct outcome of not having the ability to inspect main memory.

B INTROSPECTION ALGORITHM

The procedure we use to selectively hyper-step is presented in Algorithm 3.

Algorithm 3 Introspection using Trigger Points

```
Off-line: identify critical code section, generate profile, set candidate trigger $\Delta$
loop Introspection
    Identify target (§4.1) using profile
    if trigger point $\Delta$ reached then
        repeat
            Hyper-step (§4.2) the target
            Unveil likely instructions (§4.2.1)
            Locate fine-grained trigger $\Delta$'
            if $\Delta$' found then
                Set $\Delta$ = $\Delta$'
            end if
            Exfiltrate data
        until system call invocation
    end if
end loop
```

C NGINX PROCESS CONTROL

The procedure involved in spawning processes in Nginx is shown in Figure 5. The sequence of system calls spanning init, master, and workers processes (observable in the context of the SEV register inference attack) uniquely identify the target.

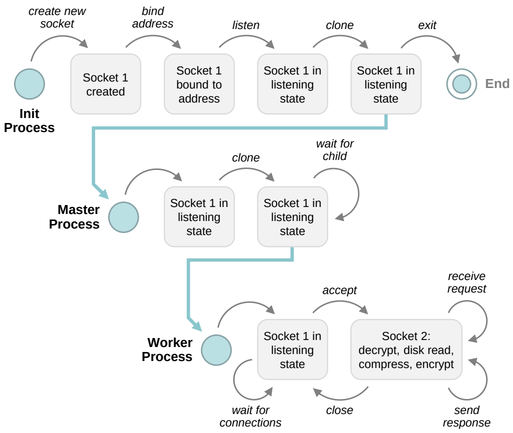
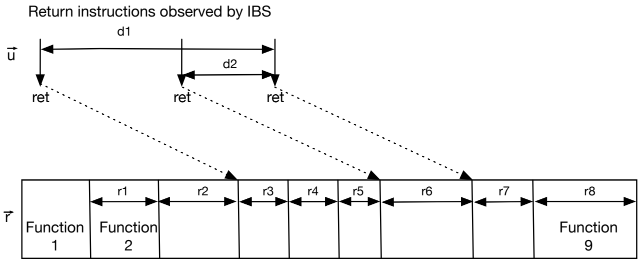

create new socket
bind address
listen
clone
exit
Init Process
Socket 1 created
Socket 1 bound to address
Socket 1 in listening state
Socket 1 in listening state
End
clone
wait for child
Master Process
Socket 1 in listening state
Socket 1 in listening state
accept
receive request
Worker Process
Socket 1 in listening state
Socket 2: decrypt, disk read, compress, encrypt
wait for connections
close
send response

Figure 5: Process control in Nginx.

D IBS BASED FINGERPRINT

In the example presented in Figure 6, the reference consists of eight distances for the nine functions in the application binary image.



Layout of an application obtained via disassembly. Each vertical line represents a return instruction.

Figure 6: Application reference and IBS based fingerprints