ExecVus

Alexandru Totolici
What? Why? How?

a way to visualize control-flow in software execution
What? Why? How?

underlying data collected by Tralfamadore

http://tralfamadore.cs.ubc.ca/
What? Why? How?

existing visualization...
lock_sock(sk);
TCP_CHECK_TIMER(sk);
flags = msg->msg_flags;
timeo = sock_sndtimeo(sk, flags & MSG_DONTWAIT);

/* Wait for a connection to finish. */
if (((1 << sk->sk_state) & ~(TCPF_ESTABLISHED | TCPF_CLOSE_WAIT))
    if ((err = sk_stream_wait_connect(sk, &timeo)) != 0)
goto out_err;

/* This should be in poll */
clear_bit(SOCK_ASYNC_NOSPACING, &sk->sk_socket->flags);
mss_now = tcp_current_mss(sk, !(flags & MSG_OOB));
call tcp_current_mss(114) tcp_current_mss(28) tcp_current_mss(23) tcp_current_mss(23)
tcp_current_mss(4) tcp_current_mss(3) tcp_current_mss(2) tcp_current_mss(1)
tcp_current_mss(1) tcp_current_mss(1)
iovlen = msg->msg_iovlen;
iov = msg->msg_iov;
copied = 0;
err = -EPIPE;
if (sk->sk_err || (sk->sk_shutdown & SEND_SHUTDOWN))
goto do_error;
while (--iovlen >= 0) {
    int seglen = iov->iov_len;
    unsigned char __user *from = iov->iov_base;
    inline tcp_mark_urg
    iov++;
}
What? Why? How?

but:

occlusion (of paths)
What? Why? How?
What? Why? How?

but:

occlusion (of paths)

selection (of flow)
What? Why? How?
What? Why? How?

but:

occlusion (of paths)
selection (of flow)
location (in execution)
What? **Why?** How?

control-flow is non-trivial to “see”
What? **Why?** How?

scenario 1: debug
What? **Why?** How?

scenario 2: malware
What? Why? **How?**

code collapse
What? Why? **How?**

code reordering
What? Why? **How?**

improve selection of execution path
What? Why? **How?**

“zoom” in and out (in the control-flow)
What? Why? How?
What? Why? How?
What? Why? How?

Mercurial, jQuery, Python, Cappuccino