Replacing OpenSSL, one step at a time

RustNL 2024

this talk

❶	❷	❸	❹
recent rustls rundown	rustls-libssl: why	rustls-libssl: what	rustls-libssl: how

recent rustls rundown

Funding!

Joe @ctz and Daniel @cpu full time

Adolfo @aochagavia and Ferrous Systems project contracts

Funded by ISRG Prossimo project: memorysafety.org

recent rustls rundown

Shipped features!

Revocation support with CRLs

Pluggable cryptography providers

FIPS140 support

`no_std` support

Post-quantum cryptography support

Unbuffered API

} experimental

Let's replace OpenSSL

rustls-libssl: why

non-Rust users *also* deserve memory-safe TLS!

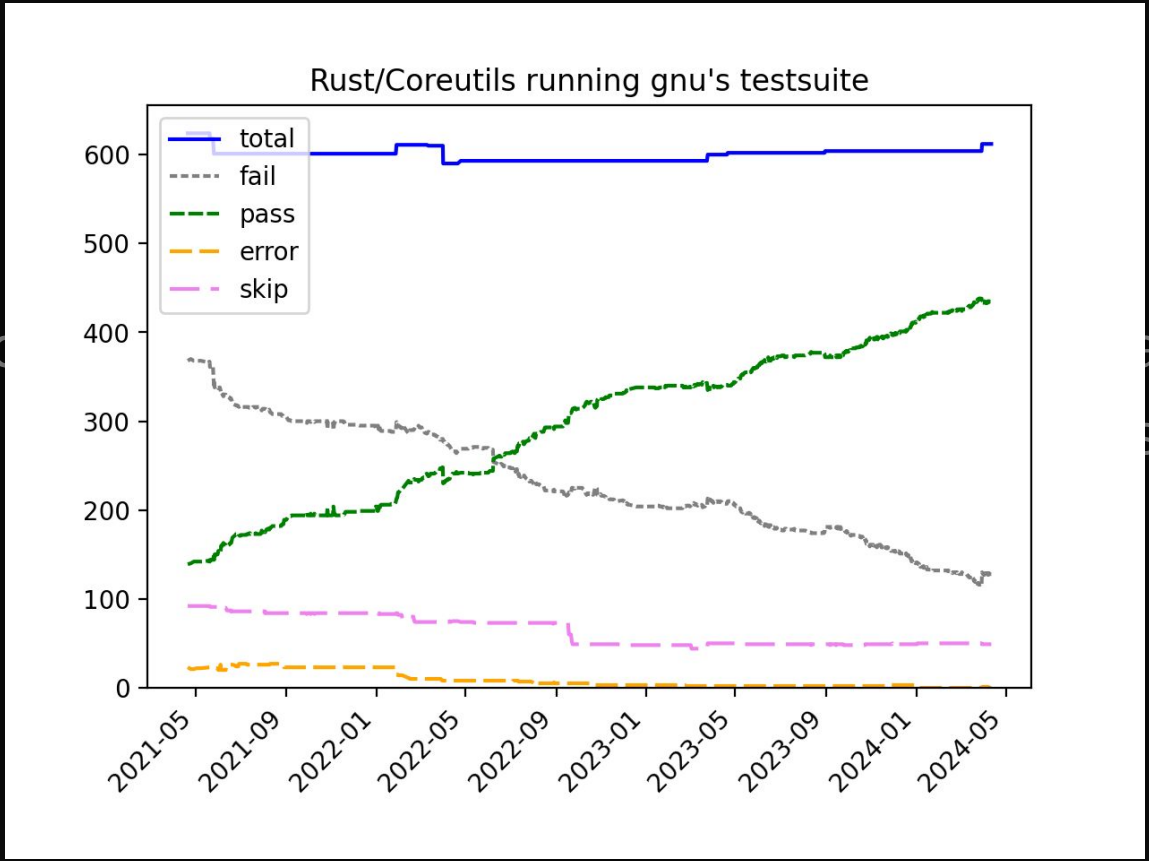
rustls-libssl: why

replacing a memory-unsafe component with a drop-in alternative is a quick way to reduce risks

rustls-lib

replac a

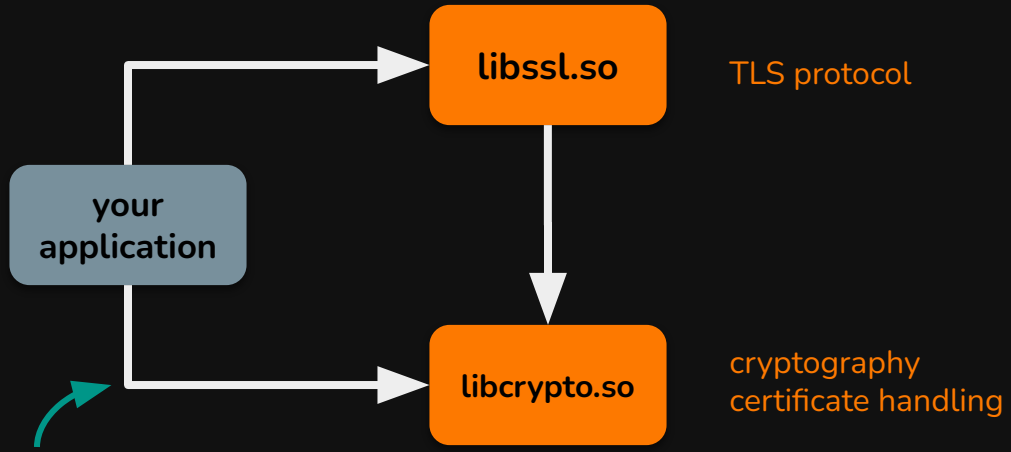
drop- sks



source: https://github.com/uutils/coreutils

rustls-libssl: what

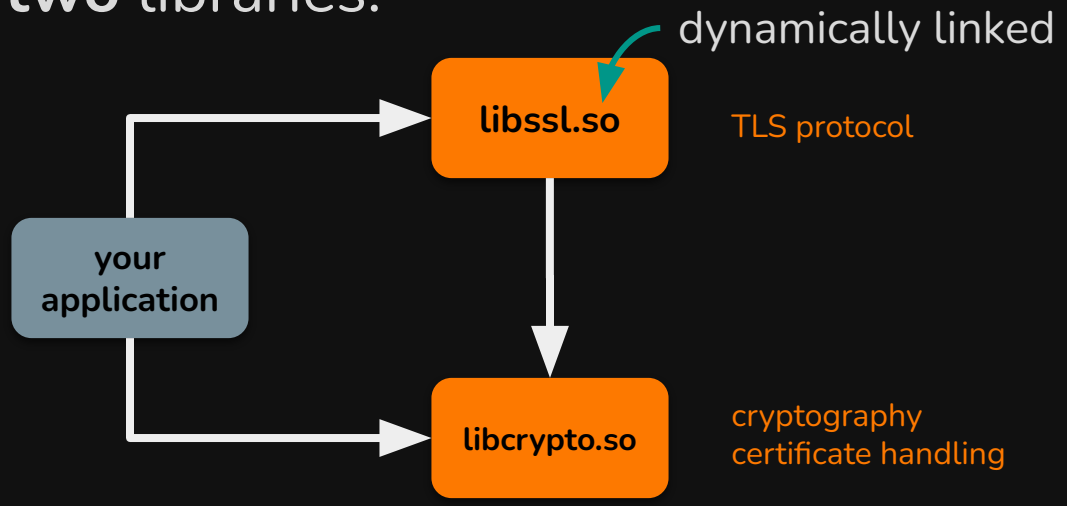
OpenSSL is **two** libraries:



Invariably an application that uses libssl also uses libcrypto

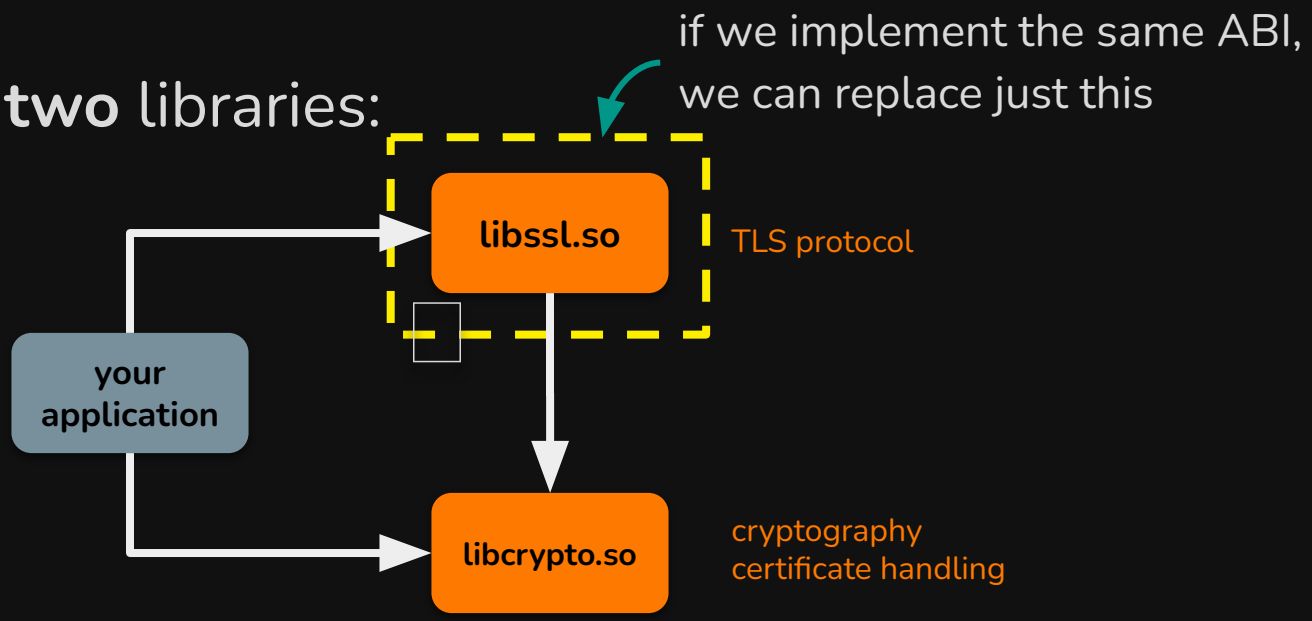
rustls-libssl: what

OpenSSL is **two** libraries:



rustls-libssl: what

OpenSSL is **two** libraries:



OpenSSL libssl is **big!**

522 functions!

```
BIO_f_ssl
BIO_new_buffer_ssl_connect
BIO_new_ssl
BIO_new_ssl_connect
BIO_ssl_copy_session_id
BIO_ssl_shutdown
d2i_SSL_SESSION
DTLS_client_method
DTLS_get_data_mtu
DTLS_method
DTLS_server_method
DTLS_set_timer_cb
DTLSv1_2_client_method
DTLSv1_2_method
DTLSv1_2_server_method
DTLSv1_client_method
DTLSv1_listen
DTLSv1_method
DTLSv1_server_method
ERR_load_SSL_strings
i2d_SSL_SESSION
OPENSSL_cipher_name
OPENSSL_init_ssl
OSSL_default_cipher_list
OSSL_default_ciphersuites
PEM_read_bio_SSL_SESSION
PEM_read_SSL_SESSION
PEM_write_bio_SSL_SESSION
PEM_write_SSL_SESSION
SRP_Calc_A_param
SSL_accept
SSL_add1_host
SSL_add1_to_CA_list
SSL_add_client_CA
SSL_add_dir_cert_subjects_to_stack
SSL_add_file_cert_subjects_to_stack
SSL_add_ssl_module
SSL_add_store_cert_subjects_to_stack
SSL_alert_desc_string
SSL_alert_desc_string_long
SSL_alert_type_string
SSL_alert_type_string_long
SSL_alloc_buffers
SSL_bytes_to_cipher_list
SSL_callback_ctrl
SSL_certs_clear
SSL_check_chain
SSL_check_private_key
SSL_CIPHER_description
SSL_CIPHER_find
SSL_CIPHER_get_auth_nid
SSL_CIPHER_get_bits
SSL_CIPHER_get_cipher_nid
SSL_CIPHER_get_digest_nid
SSL_CIPHER_get_handshake_digest
SSL_CIPHER_get_id
SSL_CIPHER_get_kx_nid
SSL_CIPHER_get_name
SSL_CIPHER_get_protocol_id
SSL_CIPHER_get_version
SSL_CIPHER_is_aead
SSL_CIPHER_standard_name
SSL_clear
SSL_clear_options
SSL_client_hello_get0_ciphers
SSL_client_hello_get0_compression_methods
SSL_client_hello_get0_ext
SSL_client_hello_get0_legacy_version
SSL_client_hello_get0_random
SSL_client_hello_get0_session_id
SSL_client_hello_get1_extensions_present
SSL_client_hello_isv2
SSL_client_version
SSL_COMP_add_compression_method
SSL_COMP_get0_name
SSL_COMP_get_compression_methods
SSL_COMP_get_id
SSL_COMP_get_name
SSL_COMP_set0_compression_methods
SSL_CONF_cmd
SSL_CONF_cmd_argv
SSL_CONF_cmd_value_type
SSL_CONF_CTX_clear_flags
SSL_CONF_CTX_finish
SSL_CONF_CTX_free
SSL_CONF_CTX_new
SSL_CONF_CTX_set1_prefix
SSL_CONF_CTX_set_flags
SSL_CONF_CTX_set_ssl
SSL_CONF_CTX_set_ssl_ctx
SSL_config
SSL_connect
SSL_copy_session_id
SSL_ct_is_enabled
SSL_ctrl
SSL_CTX_add1_to_CA_list
SSL_CTX_add_client_CA
SSL_CTX_add_client_custom_ext
SSL_CTX_add_custom_ext
SSL_CTX_add_server_custom_ext
SSL_CTX_add_session
SSL_CTX_callback_ctrl
SSL_CTX_check_private_key
SSL_CTX_clear_options
SSL_CTX_config
SSL_CTX_ct_is_enabled
SSL_CTX_ctrl
SSL_CTX_dane_clear_flags
SSL_CTX_dane_enable
SSL_CTX_dane_mtype_set
SSL_CTX_dane_set_flags
SSL_CTX_enable_ct
SSL_CTX_flush_sessions
SSL_CTX_free
SSL_CTX_get0_CA_list
SSL_CTX_get0_certificate
SSL_CTX_get0_ctlog_store
SSL_CTX_get0_param
SSL_CTX_get0_privatekey
SSL_CTX_get0_security_ex_data
SSL_CTX_get_cert_store
SSL_CTX_get_ciphers
SSL_CTX_get_client_CA_list
SSL_CTX_get_client_cert_cb
SSL_CTX_get_default_passwd_cb
SSL_CTX_get_default_passwd_cb_userdata
SSL_CTX_get_ex_data
SSL_CTX_get_info_callback
SSL_CTX_get_keylog_callback
SSL_CTX_get_max_early_data
SSL_CTX_get_num_tickets
SSL_CTX_get_options
SSL_CTX_get_quiet_shutdown
SSL_CTX_get_record_padding_callback_arg
SSL_CTX_get_recv_max_early_data
SSL_CTX_get_security_callback
SSL_CTX_get_security_level
SSL_CTX_get_ssl_method
SSL_CTX_get_timeout
SSL_CTX_get_verify_callback
SSL_CTX_get_verify_depth
SSL_CTX_get_verify_mode
SSL_CTX_has_client_custom_ext
SSL_CTX_load_verify_dir
SSL_CTX_load_verify_file
SSL_CTX_load_verify_locations
SSL_CTX_load_verify_store
SSL_CTX_new
SSL_CTX_new_ex
SSL_CTX_remove_session
SSL_CTX_sess_get_get_cb
SSL_CTX_sess_get_new_cb
SSL_CTX_sess_get_remove_cb
SSL_CTX_sessions
SSL_CTX_sess_set_get_cb
SSL_CTX_sess_set_new_cb
SSL_CTX_sess_set_remove_cb
SSL_CTX_set0_CA_list
SSL_CTX_set0_ctlog_store
SSL_CTX_set0_security_ex_data
SSL_CTX_set0_tmp_dh_pkey
SSL_CTX_set1_cert_store
SSL_CTX_set1_param
SSL_CTX_set_allow_early_data_cb
SSL_CTX_set_alpn_protos
SSL_CTX_set_alpn_select_cb
SSL_CTX_set_async_callback
SSL_CTX_set_async_callback_arg
SSL_CTX_set_block_padding
SSL_CTX_set_cert_cb
SSL_CTX_set_cert_store
SSL_CTX_set_cert_verify_callback
SSL_CTX_set_cipher_list
SSL_CTX_set_ciphersuites
SSL_CTX_set_client_CA_list
SSL_CTX_set_client_cert_cb
SSL_CTX_set_client_cert_engine
SSL_CTX_set_client_hello_cb
SSL_CTX_set_cookie_generate_cb
SSL_CTX_set_cookie_verify_cb
SSL_CTX_set_ctlog_list_file
SSL_CTX_set_ct_validation_callback
SSL_CTX_set_default_ctlog_list_file
SSL_CTX_set_default_passwd_cb
SSL_CTX_set_default_passwd_cb_userdata
SSL_CTX_set_default_read_buffer_len
SSL_CTX_set_default_verify_dir
SSL_CTX_set_default_verify_file
SSL_CTX_set_default_verify_paths
SSL_CTX_set_default_verify_store
SSL_CTX_set_ex_data
SSL_CTX_set_generate_session_id
SSL_CTX_set_info_callback
SSL_CTX_set_keylog_callback
SSL_CTX_set_max_early_data
SSL_CTX_set_msg_callback
SSL_CTX_set_next_protos_advertised_cb
SSL_CTX_set_next_proto_select_cb
SSL_CTX_set_not_resumable_session_callback
SSL_CTX_set_num_tickets
SSL_CTX_set_options
SSL_CTX_set_post_handshake_auth
SSL_CTX_set_psk_client_callback
SSL_CTX_set_psk_find_session_callback
SSL_CTX_set_psk_server_callback
SSL_CTX_set_psk_use_session_callback
SSL_CTX_set_purpose
SSL_CTX_set_quiet_shutdown
SSL_CTX_set_record_padding_callback
SSL_CTX_set_record_padding_callback_arg
SSL_CTX_set_recv_max_early_data
SSL_CTX_set_security_callback
SSL_CTX_set_security_level
SSL_CTX_set_session_id_context
SSL_CTX_set_session_ticket_cb
SSL_CTX_set_srp_cb_arg
SSL_CTX_set_srp_client_pwd_callback
SSL_CTX_set_srp_password
SSL_CTX_set_srp_strength
SSL_CTX_set_srp_username
SSL_CTX_set_srp_username_callback
SSL_CTX_set_srp_verify_param_callback
SSL_CTX_set_ssl_version
SSL_CTX_set_stateless_cookie_generate_cb
SSL_CTX_set_stateless_cookie_verify_cb
SSL_CTX_set_timeout
SSL_CTX_set_tlsext_max_fragment_length
SSL_CTX_set_tlsext_ticket_key_evp_cb
SSL_CTX_set_tlsext_use_srtp
SSL_CTX_set_tmp_dh_callback
SSL_CTX_set_trust
SSL_CTX_set_verify
SSL_CTX_set_verify_depth
SSL_CTX_SRP_CTX_free
SSL_CTX_SRP_CTX_init
SSL_CTX_up_ref
SSL_CTX_use_cert_and_key
SSL_CTX_use_certificate
SSL_CTX_use_certificate_ASN1
SSL_CTX_use_certificate_chain_file
SSL_CTX_use_certificate_file
SSL_CTX_use_PrivateKey
SSL_CTX_use_PrivateKey_ASN1
SSL_CTX_use_PrivateKey_file
SSL_CTX_use_psk_identity_hint
SSL_CTX_use_RSAPrivateKey
SSL_CTX_use_RSAPrivateKey_ASN1
SSL_CTX_use_RSAPrivateKey_file
SSL_CTX_use_serverinfo
SSL_CTX_use_serverinfo_ex
SSL_CTX_use_serverinfo_file
SSL_dane_clear_flags
SSL_dane_enable
SSL_dane_set_flags
SSL_dane_tlsa_add
SSL_do_handshake
SSL_dup
SSL_dup_CA_list
SSL_enable_ct
SSL_export_keying_material
SSL_export_keying_material_early
SSL_extension_supported
SSL_free
SSL_free_buffers
SSL_get0_alpn_selected
SSL_get0_CA_list
SSL_get0_dane
SSL_get0_dane_authority
SSL_get0_dane_tlsa
SSL_get0_next_proto_negotiated
SSL_get0_param
SSL_get0_peer_CA_list
SSL_get0_peer_certificate
SSL_get0_peername
SSL_get0_peer_scts
SSL_get0_security_ex_data
SSL_get0_verified_chain
SSL_get1_peer_certificate
SSL_get1_session
SSL_get1_supported_ciphers
SSL_get_all_async_fds
SSL_get_async_status
SSL_get_certificate
SSL_get_changed_async_fds
SSL_get_cipher_list
SSL_get_ciphers
SSL_get_client_CA_list
SSL_get_client_ciphers
SSL_get_client_random
SSL_get_current_cipher
SSL_get_current_compression
SSL_get_current_expansion
SSL_get_default_passwd_cb
SSL_get_default_passwd_cb_userdata
SSL_get_default_timeout
SSL_get_early_data_status
SSL_get_error
SSL_get_ex_data
SSL_get_ex_data_X509_STORE_CTX_idx
SSL_get_fd
SSL_get_finished
SSL_get_info_callback
SSL_get_key_update_type
SSL_get_max_early_data
SSL_get_num_tickets
SSL_get_options
SSL_get_peer_cert_chain
SSL_get_peer_certificate
SSL_get_peer_finished
SSL_get_peer_signature_type_nid
SSL_get_peering_cipher
SSL_get_privatekey
SSL_get_psk_identity
SSL_get_psk_identity_hint
SSL_get_quiet_shutdown
SSL_get_rbio
SSL_get_read_ahead
SSL_get_record_padding_callback_arg
SSL_get_recv_max_early_data
SSL_get_rfd
SSL_get_security_callback
SSL_get_security_level
SSL_get_selected_srtp_profile
SSL_get_servername
SSL_get_servername_type
SSL_get_server_random
SSL_get_session
SSL_get_shared_ciphers
SSL_get_shared_sigalgs
SSL_get_shutdown
SSL_get_sigalgs
SSL_get_signature_type_nid
SSL_get_srp_g
SSL_get_srp_N
SSL_get_srp_userinfo
SSL_get_srp_username
SSL_get_srtp_profiles
SSL_get_SSL_CTX
SSL_get_ssl_method
SSL_get_state
SSL_get_verify_callback
SSL_get_verify_depth
SSL_get_verify_mode
SSL_get_verify_result
SSL_get_version
SSL_get_wbio
SSL_get_wfd
SSL_group_to_name
SSL_has_matching_session_id
SSL_has_pending
SSL_in_before
SSL_in_init
SSL_is_dtls
SSL_is_init_finished
SSL_is_server
SSL_key_update
SSL_load_client_CA_file
SSL_load_client_CA_file_ex
SSL_new
SSL_new_session_ticket
SSL_peek
SSL_peek_ex
SSL_pending
SSL_read
SSL_read_early_data
SSL_read_ex
SSL_renegotiate
SSL_renegotiate_abbreviated
SSL_renegotiate_pending
SSL_rstate_string
SSL_rstate_string_long
SSL_select_next_proto
SSL_sendfile
SSL_SESSION_dup
SSL_SESSION_free
SSL_SESSION_get0_alpn_selected
SSL_SESSION_get0_cipher
SSL_SESSION_get0_hostname
SSL_SESSION_get0_id_context
SSL_SESSION_get0_peer
SSL_SESSION_get0_ticket
SSL_SESSION_get0_ticket_appdata
SSL_SESSION_get_compress_id
SSL_SESSION_get_ex_data
SSL_SESSION_get_id
SSL_SESSION_get_master_key
SSL_SESSION_get_max_early_data
SSL_SESSION_get_max_fragment_length
SSL_SESSION_get_protocol_version
SSL_SESSION_get_ticket_lifetime_hint
SSL_SESSION_get_time
SSL_SESSION_get_timeout
SSL_SESSION_has_ticket
SSL_SESSION_is_resumable
SSL_SESSION_new
SSL_SESSION_print
SSL_SESSION_print_fp
SSL_SESSION_print_keylog
SSL_session_reused
SSL_SESSION_set1_alpn_selected
SSL_SESSION_set1_hostname
SSL_SESSION_set1_id
SSL_SESSION_set1_id_context
SSL_SESSION_set1_master_key
SSL_SESSION_set1_ticket_appdata
SSL_SESSION_set_cipher
SSL_SESSION_set_ex_data
SSL_SESSION_set_max_early_data
SSL_SESSION_set_protocol_version
SSL_SESSION_set_time
SSL_SESSION_set_timeout
SSL_SESSION_up_ref
SSL_set0_CA_list
SSL_set0_rbio
SSL_set0_security_ex_data
SSL_set0_tmp_dh_pkey
SSL_set0_wbio
SSL_set1_host
SSL_set1_param
SSL_set_accept_state
SSL_set_allow_early_data_cb
SSL_set_alpn_protos
SSL_set_async_callback
SSL_set_async_callback_arg
SSL_set_bio
SSL_set_block_padding
SSL_set_cert_cb
SSL_set_cipher_list
SSL_set_ciphersuites
SSL_set_client_CA_list
SSL_set_client_CA_file
SSL_set_connect_state
SSL_set_cert_validation_callback
SSL_set_debug
SSL_set_default_passwd_cb
SSL_set_default_passwd_cb_userdata
SSL_set_default_read_buffer_len
SSL_set_ex_data
SSL_set_fd
SSL_set_generate_session_id
SSL_set_hostflags
SSL_set_info_callback
SSL_set_max_early_data
SSL_set_msg_callback
SSL_set_not_resumable_session_callback
SSL_set_num_tickets
SSL_set_options
SSL_set_post_handshake_auth
SSL_set_psk_client_callback
SSL_set_psk_find_session_callback
SSL_set_psk_server_callback
SSL_set_psk_use_session_callback
SSL_set_purpose
SSL_set_quiet_shutdown
SSL_set_record_padding_callback
SSL_set_record_padding_callback_arg
SSL_set_recv_max_early_data
SSL_set_rfd
SSL_set_security_callback
SSL_set_security_level
SSL_set_session
SSL_set_session_id_context
SSL_set_session_secret_cb
SSL_set_session_ticket_ext
SSL_set_session_ticket_ext_cb
SSL_set_shutdown
SSL_set_srp_server_param
SSL_set_srp_server_param_pw
SSL_set_SSL_CTX
SSL_set_ssl_method
SSL_set_tlsext_max_fragment_length
SSL_set_tlsext_use_srtp
SSL_set_tmp_dh_callback
SSL_set_trust
SSL_set_verify
SSL_set_verify_depth
SSL_set_verify_result
SSL_set_wfd
SSL_shutdown
SSL_SRP_CTX_free
SSL_SRP_CTX_init
SSL_srp_server_param_with_username
SSL_stateless
SSL_state_string
SSL_state_string_long
SSL_test_functions
SSL_trace
SSL_up_ref
SSL_use_cert_and_key
SSL_use_certificate
SSL_use_certificate_ASN1
SSL_use_certificate_chain_file
SSL_use_certificate_file
SSL_use_PrivateKey
SSL_use_PrivateKey_ASN1
SSL_use_PrivateKey_file
SSL_use_psk_identity_hint
SSL_use_RSAPrivateKey
SSL_use_RSAPrivateKey_ASN1
SSL_use_RSAPrivateKey_file
SSLv3_client_method
SSLv3_method
SSLv3_server_method
SSL_verify_client_post_handshake
SSL_version
SSL_waiting_for_async
SSL_want
SSL_write
SSL_write_early_data
SSL_write_ex
TLS_client_method
TLS_method
TLS_server_method
TLSv1_1_client_method
TLSv1_1_method
TLSv1_1_server_method
TLSv1_2_client_method
TLSv1_2_method
TLSv1_2_server_method
TLSv1_client_method
TLSv1_method
TLSv1_server_method
```

136 additional functions are multiplexed!

```
#define SSL_CTX_sess_get_cache_size(ctx) \
        SSL_CTX_ctrl(ctx,SSL_CTRL_GET_SESS_CACHE_SIZE,0,NULL)
```

(`SSL_CTX_ctrl`, `SSL_ctrl`, `SSL_CTX_callback_ctrl` and `SSL_callback_ctrl` are magic like this.)

Fortunately, most of this API surface is rarely used.

eg. curl[1] uses just 57 functions:

```
BIO_f_ssl
OPENSSL_init_ssl
SSL_alert_desc_string_long
SSL_CIPHER_get_name
SSL_connect
SSL_ctrl
SSL_CTX_add_client_CA
SSL_CTX_check_private_key
SSL_CTX_ctrl
SSL_CTX_free
SSL_CTX_get_cert_store
SSL_CTX_load_verify_dir
SSL_CTX_load_verify_file
SSL_CTX_new
SSL_CTX_sess_set_new_cb
SSL_CTX_set_alpn_protos
SSL_CTX_set_cipher_list
SSL_CTX_set_ciphersuites
SSL_CTX_set_default_passwd_cb
SSL_CTX_set_default_passwd_cb_userdata
SSL_CTX_set_keylog_callback
SSL_CTX_set_msg_callback
SSL_CTX_set_next_proto_select_cb
SSL_CTX_set_options
SSL_CTX_set_post_handshake_auth
SSL_CTX_set_srp_password
SSL_CTX_set_srp_username
SSL_CTX_set_verify
SSL_CTX_use_certificate_chain_file
SSL_CTX_use_certificate_file
SSL_CTX_use_certificate
SSL_CTX_use_PrivateKey_file
SSL_CTX_use_PrivateKey
SSL_free
SSL_get0_alpn_selected
SSL_get1_peer_certificate
SSL_get_certificate
SSL_get_current_cipher
SSL_get_error
SSL_get_ex_data
SSL_get_peer_cert_chain
SSL_get_privatekey
SSL_get_shutdown
SSL_get_verify_result
SSL_get_version
SSL_new
SSL_pending
SSL_read
SSL_SESSION_free
SSL_set_bio
SSL_set_connect_state
SSL_set_ex_data
SSL_set_fd
SSL_set_session
SSL_shutdown
SSL_write
TLS_client_method
```

[1] curl 7.81.0-1ubuntu1.15 as shipped on Ubuntu 22.04LTS

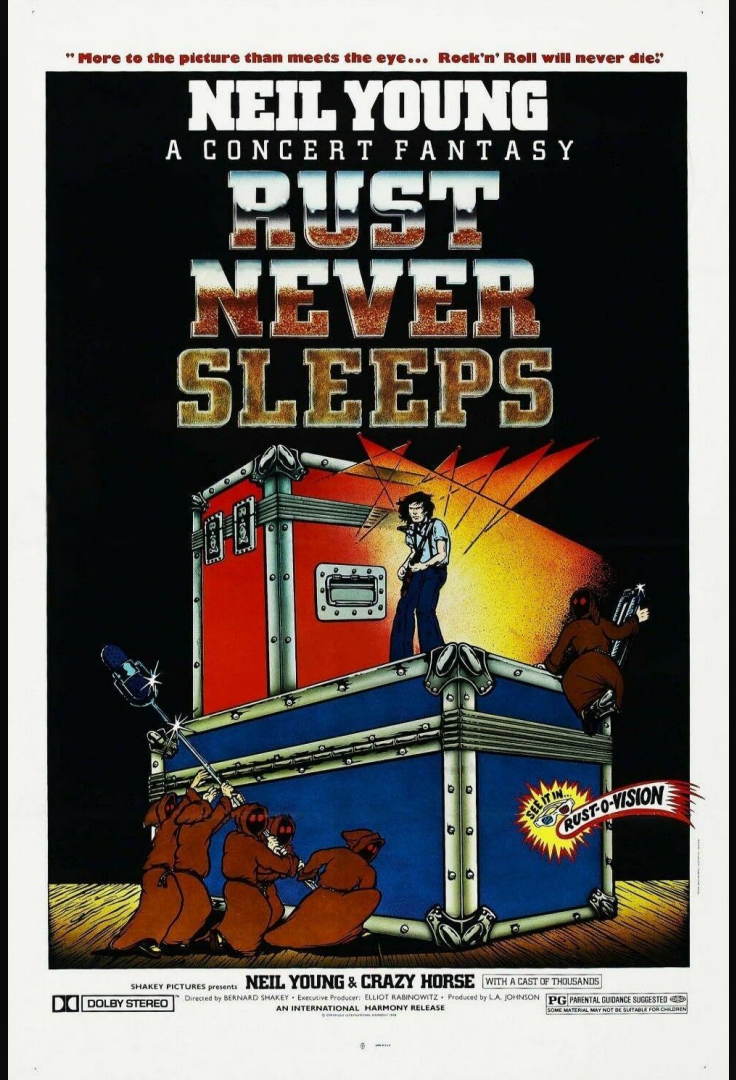
nginx[1] uses 90 functions.

significant overlap with curl: 114 functions cover both

that feels achievable!

[1] nginx 1.18.0-6ubuntu14.4 as shipped on Ubuntu 22.04LTS

let's make
libssl.so
(but in rust)



ingredients

✅ build a C-ABI dynamic library

Cargo.toml:

```
[lib]
name = "ssl"
crate-type = ["cdylib"]
```

ingredients

- ✅ build a C-ABI dynamic library
- ✅ with correctly-versioned symbols

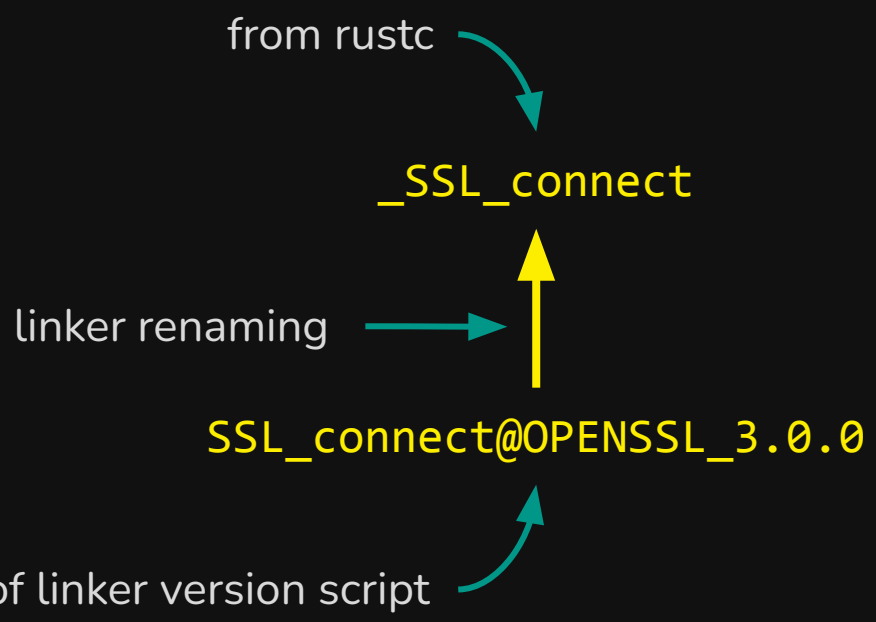
build.rs:

```
let filename = write_version_file();

println!("cargo:rustc-cdylib-link-arg="
         "-Wl,--version-script={filename}");

for symbol in ENTRYPOINTS {
    println!(
        "cargo:rustc-cdylib-link-arg="
        "-Wl,--defsym={}=_{}",
        symbol, symbol
    );
}
```

(and then use ldd)

ingredients

- ✅ build a C-ABI dynamic library
- ✅ with correctly-versioned symbols



ingredients

- ✅ build a C-ABI dynamic library
- ✅ with correctly-versioned symbols
- ✅ write some rust functions with C linkage

ingredients

- ✅ build a C-ABI dynamic library
- ✅
- ✅

#[no_mangle] and extern "C"

```
entry! {
    pub fn _SSL_alert_desc_string(value: c_int) -> *const c_char {
        crate::constants::alert_desc_to_short_string(value).as_ptr() as *const c_char
    }
}
```

ingredients

- ✅ build a C-ABI dynamic library
- ✅ with correctly-versioned symbols
- ✅ write some rust functions with C linkage
- ✅ and avoid undefined behaviour!

ingredients

- ✅ build a C-ABI dynamic library
- ✅
- ✅
- ✅

also wrap the whole function body in `std::panic::catch_unwind`

```
entry! {
    pub fn _SSL_alert_desc_string(value: c_int) -> *const c_char {
        crate::constants::alert_desc_to_short_string(value).as_ptr() as *const c_char
    }
}
```

differential testing

- write some simple C programs that use OpenSSL

```c
#include <stdio.h>

#include <openssl/ssl.h>

int main(void) {
  for (int i = -1; i < 260; i++) {
    printf("%d: '%s' '%s'\n", i,
           SSL_alert_desc_string(i),
           SSL_alert_desc_string_long(i));
  }
  return 0;
}
```

differential testing

- 📐 write some simple C programs that use OpenSSL
- 📃 have them print all return values and data

```
-1: 'UK' 'unknown'
0: 'CN' 'close notify'
1: 'UK' 'unknown'
2: 'UK' 'unknown'
3: 'UK' 'unknown'
4: 'UK' 'unknown'
5: 'UK' 'unknown'
6: 'UK' 'unknown'
7: 'UK' 'unknown'
...
```

should be deterministic: so no pointer values, or randomised data!

differential testing

- 📐 write some simple C programs that use OpenSSL
- 📃 have them print all return values and data
- 💥 run them against the real libssl.so and ours

```
$ ./target/constants > original

$ LD_LIBRARY_PATH=target/debug
  ./target/constants > ours
```

differential testing

- 📐 write some simple C programs that use OpenSSL
- 📃 have them print all return values and data
- 💥 run them against the real libssl.so and ours
- ✅ the output *should* be identical!

```
$ ./target/constants > original

$ LD_LIBRARY_PATH=target/debug
  ./target/constants > ours

$ diff -su original ours
Files original and ours are identical
```

miri with FFI calls

miri works very well for pure-rust libraries

...but not if you make an FFI call

miri with FFI calls

miri works very well for pure-rust libraries

...but not if you make an FFI call

```
error: unsupported operation: can't call foreign function `X509_STORE_new` on OS `linux`
    --> src/x509.rs:242:27
     |
242  |             raw: unsafe { X509_STORE_new() },
     |                           ^^^^^^^^^^^^^^^^ can't call foreign function
     |                                            `X509_STORE_new` on OS `linux`
     |
     = help: this is likely not a bug in the program; it indicates that the program
       performed an operation that the interpreter does not support
```

miri with FFI calls

miri works very well for pure-rust libraries

...but not if you make an FFI call

Let's send a pull request to miri

```
error: unsupported operation: can't call foreign                                    linux`
    --> src/x509.rs:242:27
     |
242  |             raw: unsafe { X509_STORE_new() },
     |                           ^^^^^^^^^^^^^^^^ can't call foreign function
     |                                            `X509_STORE_new` on OS `linux`
     |
     = help: this is likely not a bug in the program; it indicates that the program
       performed an operation that the interpreter does not support
```

miri with FFI calls

miri *already* looks in your crate for native function definitions!

```
#[cfg(miri)]
mod miri {
    pub struct X509_STORE(());

    #[no_mangle]
    pub extern "C" fn X509_STORE_new() -> *mut X509_STORE {
        Box::into_raw(Box::new(X509_STORE(())))
    }

    #[no_mangle]
    pub extern "C" fn X509_STORE_free(ptr: *mut X509_STORE) {
        if ptr.is_null() { return; }
        drop(unsafe { Box::from_raw(ptr) });
    }
}
```

conclusions

- 🦀 we've made a memory-safe[1] replacement for openssl 3.0 libssl.so

[1] mostly

conclusions

- we've made a memory-safe[1] replacement for openssl 3.0 libssl.so
- written in rust, using rustls

[1] mostly

conclusions

- we've made a memory-safe[1] replacement for openssl 3.0 libssl.so
- written in rust, using rustls
- applications don't need recompilation

[1] mostly

conclusions

- we've made a memory-safe[1] replacement for openssl 3.0 libssl.so
- written in rust, using rustls
- applications don't need recompilation
- supports a small subset of the openssl 3.0 libssl API

  (but enough for nginx and curl[2])

[1] mostly
[2] ubuntu 22.04 LTS versions

conclusions

- and it's easy to try:

```
$ with-rustls-libssl curl https://rustls.horse/

or

# rustls-libssl-nginx enable
# systemctl daemon-reload
# service nginx restart
```

thanks!

Repo: https://github.com/rustls/rustls-openssl-compat

Mastodon: @jpixton@octodon.social

Mail: jbp@jbp.io

Slides: https://github.com/ctz/talks